



Отчет Microsoft «Цифровая защита 2022»

Описание среды угроз и расширение
возможностей цифровой защиты.



Содержание

Данные, аналитические сведения и события в этом отчете относятся к периоду с июля 2021 г. по июнь 2022 г. (2022 финансовый год корпорации Microsoft), если не указано иное.

Для оптимального просмотра и навигации по этому отчету мы рекомендуем использовать приложение Adobe Reader, которое можно скачать бесплатно с веб-сайта Adobe.

Введение	02	Возможности северокорейских кибергрупп, используемые для достижения 3 основных целей режима	49	Киберустойчивость	86
Состояние киберпреступности	06	Кибернаемники угрожают стабильности киберпространства	52	Обзор киберустойчивости	87
Обзор состояния киберпреступности	07	Введение в действие норм кибербезопасности в интересах мира и безопасности в киберпространстве	53	Введение	88
Введение	08	Устройства и инфраструктура	56	Киберустойчивость: важнейший принцип информационного общества	89
Программышантажисты и вымогательство: угроза национального уровня	09	Обзор устройств и инфраструктуры	57	Важность модернизации систем и архитектуры	90
Аналитические сведения о программах шантажистах от специалистов по безопасности	14	Введение	58	Базовый уровень безопасности — определяющий фактор эффективности передовых решений	92
Киберпреступность как сервис	18	Правительства, принимающие меры по повышению безопасности и устойчивости критически важной инфраструктуры	59	Поддержание работоспособности удостоверений имеет основополагающее значение для благополучия организации	93
Развивающаяся среда фишинговых угроз	21	Уязвимости IoT и OT: тенденции и атаки	62	Параметры безопасности операционной системы по умолчанию	96
Хронология удаления ботнетов с первых дней сотрудничества корпорации Microsoft	25	Взлом цепочки поставок и встроенного ПО	65	Акцент на цепочке поставки ПО	97
Злоупотребление инфраструктурой киберпреступниками	26	Обзор уязвимостей встроенного ПО	66	Повышение устойчивости к новым DDoS-атакам, атакам навев-приложения и сети	98
Хактивисты с нами надолго?	28	Разведывательные атаки на OT-устройства	68	Разработка сбалансированного подхода к безопасности данных и киберустойчивости	101
Угрозы национального уровня	30	Кибероперации по распространению влияния	71	Устойчивость к кибероперациям по распространению влияния: человеческое измерение	102
Обзор угроз национального уровня	31	Обзор киберопераций по распространению влияния	72	Укрепление человеческого фактора за счет развития навыков	103
Введение	32	Введение	73	Уроки, извлеченные из нашей программы ликвидации программшантажистов	104
Справочная информация оданных об угрозах национального уровня	33	Тенденции в сфере киберопераций по распространению влияния	74	Необходимость немедленного принятия мер по защите квантовых вычислений	105
Пример кибергрупп национального уровня и их деятельности	34	Обзор операций по распространению влияния во время COVID-19 и вторжения России в Украину	76	Интеграция бизнесподразделений, отдела безопасности и ИТотдела для повышения устойчивости	106
Развивающаяся среда угроз	35	Отслеживание индекса российской пропаганды	78	Колоколообразная кривая киберустойчивости	108
Цепочка поставок ИТ как шлюз в цифровую экосистему	37	Синтетические медиа	80	Команды, внесшие свой вклад	110
Быстрая эксплуатация уязвимостей	39	Комплексный подход к защите от киберопераций по распространению влияния	83		
Кибертактика российских государственных кибергрупп военного времени угрожает Украине и другим странам	41				
Китай расширяет глобальные операции для получения конкурентного преимущества	44				
Иран становится агрессивнее после смены правительства	46				

Вступительное слово Тома Берта (Tom Burt),
корпоративного вице-президент по безопасности клиентов и доверию

«Триллионы сигналов из нашей глобальной экосистемы продуктов и сервисов, которые мы анализируем, показывают свирепость, область и масштабы цифровых угроз по всему миру»

Снимок нашей среды...

Область и масштаб среды угроз

Объем атак паролей вырос до 921 атаки в секунду, что на 74 % больше, чем в прошлом году.

Ликвидация киберпреступности

На сегодняшний день корпорация Microsoft удалила больше 10 000 доменов, используемых киберпреступниками, и 600, используемых национальными кибергруппами.

Устранение уязвимостей

93 % наших мероприятий по реагированию на атаки программ-шантажистов выявили недостаточный контроль привилегированного доступа и горизонтального перемещения.

23 февраля 2022 года мир кибербезопасности вступил в новую эпоху — эпоху гибридной войны.

В тот день за несколько часов до запуска ракет и пересечения танками через границы российские кибергруппы начали массированную разрушительную атаку против целей из числа украинских государственных учреждений, технологических и финансовых организаций. Чтобы узнать больше об этих атаках и уроках, которые можно из них извлечь, прочитайте главу «Угрозы национального уровня» третьего ежегодного издания отчета Microsoft «Цифровая защита». Главный из этих уроков состоит в том, что облако обеспечивает лучшую физическую и логическую защиту от кибератак и позволяет добиться прогресса в области анализа угроз и защиты конечных точек, которые подтвердили свою ценность в Украине.

Любое исследование событий этого года в области кибербезопасности должно начинаться с этого, но отчет за данный год позволяет понять гораздо больше. В первой главе мы рассмотрим действия киберпреступников, а во второй главе изучим угрозы, исходящие от иностранных государств. Обе группы существенно усовершенствовали свои атаки, что резко усилило их результаты. Хотя Россия заняла все заголовки новостей, но и иранские кибергруппы также после смены президента усилили атаки на Израиль, а также операции по вымогательству, взлому и утечке, нацеленные на критически важную инфраструктуру США. Китай также расширил шпионские операции в Юго-Восточной Азии и в других странах южного полушария, стремясь противостоять влиянию США и красть критически важные данные и информацию.

Иностранные субъекты также используют высокоэффективные методы для проведения пропагандистских операций по распространению влияния в регионах всего мира, что рассматривается в третьей главе. Например, Россия упорно старалась убедить своих граждан и граждан многих других стран в том, что вторжение в Украину оправдано, а также сея пропаганду, дискредитирующую вакцины от COVID на Западе и одновременно подтверждающую их эффективность у себя в стране. Кроме того, кибергруппы все чаще ориентируются на устройства Интернета вещей (IoT) или устройства управления операционными технологиями (OT), выбирая их в качестве точек входа в сети и критическую инфраструктуру, что обсуждается в четвертой главе. Наконец, в последней главе мы описываем сделанные выводы и уроки, которые мы извлекли за последний год, защищаясь от атак, направленных на корпорацию Microsoft и наших клиентов, на фоне события этого года в области киберустойчивости.

В каждой главе приводятся основные извлеченные уроки и выводы, основанные на уникальной точке зрения Microsoft. Триллионы сигналов из нашей глобальной экосистемы продуктов и сервисов, которые мы анализируем, показывают свирепость, область и масштабы цифровых угроз по всему миру. Корпорация Microsoft принимает меры для защиты клиентов и цифровой экосистемы от подобных угроз, и вы можете узнать о наших технологиях, которые выявляют и блокируют миллиарды попыток фишинга, кражи личных данных и других угроз для наших клиентов.

Вступительное слово Тома Берта (Tom Burt)

Продолжение

Мы также используем юридические и технические средства для захвата и уничтожения инфраструктуры, используемой киберпреступниками и национальными кибергруппами, и уведомляем клиентов, если они подвергаются угрозам или атакам со стороны иностранных государств. Мы разрабатываем улучшенные функции и сервисы, использующие технологии ИИ и машинное обучение для выявления и блокировки киберугроз, а специалисты по безопасности защищаются от кибервторжений и идентифицируют их быстрее и эффективнее.

Возможно, самое главное, что на протяжении всего отчета мы предлагаем рекомендации по действиям, которые отдельные лица и организации могут выполнить для защиты от этих растущих цифровых угроз. Применение эффективных мер киберпрофилактики будет лучшим способом защиты и может значительно снизить риск кибератак.

Состояние киберпреступности

Киберпреступники продолжают действовать как квалифицированные прибыльные компании. Они ищут и применяют новые способы реализации атак и усложняют инфраструктуру для проведения своих кампаний. В то же время киберпреступники становятся экономнее. Чтобы снизить накладные расходы и повысить видимость легитимности, злоумышленники взламывают бизнес-сети и устройства для проведения фишинговых кампаний, установки вредоносного ПО и использования вычислительных ресурсов жертв для майнинга криптовалюты.

[> Подробнее на стр. 6](#)

«Появление кибероружия в гибридной войне в Украине символизирует рассвет новой эпохи конфликтов».

Угрозы национального уровня

Злоумышленники национального уровня проводят изощренные кибератаки, чтобы избежать обнаружения, для продвижения своих стратегических приоритетов. Появление кибероружия в гибридной войне в Украине символизирует рассвет новой эпохи конфликтов. Россия также поддерживает войну операциями информационного влияния, используя пропаганду для воздействия на общественное мнение в России, Украине и во всем мире. За пределами Украины субъекты национального уровня усилили активность и начали использовать достижения в сфере автоматизации, облачной инфраструктуры и технологий удаленного доступа для атаки на широкий спектр целей. Корпоративные цепочки поставок ИТ, которые могут предоставить доступ к конечным целям, часто были целью атак. Киберпрофилактика стала еще важнее, так как злоумышленники быстро использовали неисправленные уязвимости, как сложные методы, так и методы прямого перебора для кражи учетных данных и скрывали свои операции с помощью ПО открытого исходного кода или подлинного ПО. Кроме того, Иран, как и Россия, начал использовать разрушительное кибероружие, в том числе программы-шантажисты, в качестве основного метода атак.

В результате необходимо срочно внедрить согласованную международную платформу, которая отдает приоритет правам человека и защищает людей от безрассудного поведения государств в Интернете. Все страны должны совместно работать над внедрением норм и правил ответственного поведения государств.

[> Подробнее на стр. 30](#)

Устройства и инфраструктура

Быстрое внедрение устройств с доступом в Интернет ускорило цифровую трансформацию, а пандемия значительно расширила возможные направления атак на цифровой мир. И киберпреступники, и иностранные государства быстро пытаются воспользоваться этим. Безопасность ИТ-оборудования и ПО укрепилась за последние годы, но IoT- и OT-устройства не поспевают за ними. Злоумышленники используют такие устройства для доступа к сетям и горизонтального перемещения, чтобы закрепиться в цепочке поставок или нарушить OT-операции целевой организации.

[> Подробнее на стр. 56](#)



Вступительное слово Тома Берта (Tom Burt)

Продолжение

Кибероперации по
распространению влияния

Иностранные государства все чаще используют сложные операции по распространению влияния для пропаганды и воздействия на общественное мнение как внутри страны, так и на международном уровне. Эти кампании подрывают доверие, усиливают поляризацию общества и угрожают демократическим процессам. Квалифицированные продвинутые активные манипуляторы используют традиционные СМИ вместе с Интернетом и социальными сетями, чтобы существенно увеличить масштаб, область и эффективность своих кампаний, а также свое влияние на глобальную информационную экосистему. В прошлом году мы видели такие операции в рамках гибридной войны России с Украиной, но также наблюдали, как Россия и другие страны, в том числе Китай и Иран, все чаще обращались к пропагандистским операциям в социальных сетях для расширения глобального влияния в различных областях.

[> Подробнее на стр. 71](#)


Киберустойчивость

Безопасность — важнейший фактор технологического успеха. Инноваций и повышения производительности можно достигнуть только после внедрения мер безопасности, которые сделают организации максимально устойчивыми к современным атакам. Из-за пандемии корпорации Microsoft пришлось изменить методы и технологии обеспечения безопасности для защиты наших сотрудников, где бы они ни работали. В прошлом году злоумышленники продолжали использовать уязвимости, обнаруженные во время пандемии и перехода к гибридной рабочей среде. С тех пор наша главная задача — контролировать распространение и растущую сложность различных методов атак, а также повышенную активность иностранных государств. В этой главе мы подробно описываем проблемы, с которыми столкнулись, и средства защиты, которую мы применили с 15 000 партнеров.

[> Подробнее на стр. 86](#)

Наша уникальная выигрышная позиция

37 млрд

угроз по элект-
ронной почте
заблокировано

34,7 млрд

угроз идентификации
заблокировано

43 трлн

сигналов генерируются ежедневно, используя сложную аналитику данных и алгоритмы ИИ для оценки цифровых угроз и преступной киберактивности и защиты от них.

Больше 8500

инженеров, исследователи, специалистов по обработке и анализу данных, экспертов по кибербезопасности, специалистов по угрозам, геополитических аналитиков, следователей и специалистов по реагированию в 77 странах.

Больше 15 000

партнеров в нашей экосистеме безопасности, которые повышают киберустойчивость наших клиентов.

2,5 млрд

сигналов об угрозах
анализируется
ежедневно

С 1 июля 2021 г. по 30 июня 2022 г.

Вступительное слово Тома Берта (Tom Burt)

Продолжение

Мы считаем, что корпорация Microsoft — независимо и в рамках тесного сотрудничества с другими представителями частного сектора, государственного сектора и гражданского общества — несет ответственность за защиту цифровых систем, которые лежат в основе социальной структуры нашего общества и способствуют созданию безопасных вычислительных сред для всех людей, где бы они ни находились. Поэтому мы каждый год публикуем отчет MDDR, начиная с 2020 года. Он представляет собой кульминацию анализа большого объема данных и всесторонних исследований корпорации Microsoft. В нем представлено наше мнение о том, как развивается среда цифровых угроз, и о важнейших мерах, которые можно принять сегодня для улучшения безопасности экосистемы.

Мы надеемся вызвать у читателей ощущение острой потребности, чтобы они немедленно приняли меры на основе данных и идей, которые мы представляем как здесь, так и в наших многочисленных публикациях по кибербезопасности в течение года. Анализируя серьезность угрозы цифровой среде (и ее последствия для физического мира), важно помнить, что мы все можем сделать что-то, чтобы защитить себя и наши организации от таких угроз.

Благодарим вас за то, что нашли время ознакомиться с отчетом Microsoft «Цифровая защита» за этот год. Надеемся, что вы найдете полезную информацию и рекомендации, которые помогут нам всем вместе защитить цифровую экосистему.

Том Берт (Tom Burt),
корпоративный вице-президент
по безопасности клиентов и доверию

У этого отчета 2 цели:

- ① Описать меняющуюся среду цифровых угроз для наших клиентов, партнеров и заинтересованных сторон, представляющих комплексную экосистему, проливая свет как на новые кибератаки, так и на тенденции исторически активных угроз.
- ② Позволить нашим клиентам и партнерам повысить киберустойчивость и реагировать на эти угрозы.



Состояние кибер- преступности

По мере улучшения инструментов киберзащиты и применения упреждающего подхода к предотвращению угроз все большим числом организаций злоумышленники адаптируют свои методы.

Обзор состояния киберпреступности	07
Введение	08
Программы шантажисты и вымогательство: угроза национального уровня	09
Аналитические сведения о программах-шантажистах от специалистов по безопасности	14
Киберпреступность как сервис	18
Развивающаяся среда фишинговых угроз	21
Хронология удаления ботнетов с первых дней сотрудничества корпорации Microsoft	25
Злоупотребление инфраструктурой киберпреступниками	26
Хактивисты с нами надолго?	28

Обзор

СОСТОЯНИЯ киберпреступности

По мере улучшения инструментов киберзащиты и применения упреждающего подхода к предотвращению угроз все большим числом организаций злоумышленники адаптируют свои методы.

Киберпреступники продолжают действовать как квалифицированные прибыльные компании. Они ищут и применяют новые способы реализации атак и усложняют инфраструктуру для проведения своих кампаний. В то же время киберпреступники становятся экономнее. Чтобы снизить накладные расходы и повысить видимость легитимности, злоумышленники взламывают бизнес-сети и устройства для проведения фишинговых кампаний, установки вредоносного ПО и использования вычислительных ресурсов жертв для майнинга криптовалюты.

Киберпреступность продолжает расти, так как индустриализация экономики киберпреступности снижает барьер для входа, расширяя доступ к инструментам и инфраструктуре, необходимым злоумышленникам.

➤ Подробнее на стр. 18

Угроза заражения программами-шантажистами и вымогательства становится все острее — теперь атаки нацелены на государственные учреждения, коммерческие предприятия и критически важную инфраструктуру.

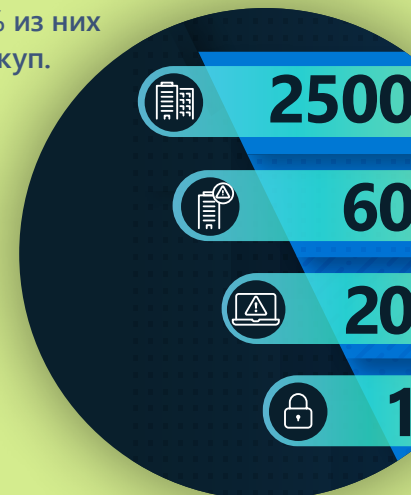


➤ Подробнее на стр. 9

Злоумышленники все чаще угрожают раскрыть конфиденциальные данные, чтобы заставить жертву заплатить выкуп.

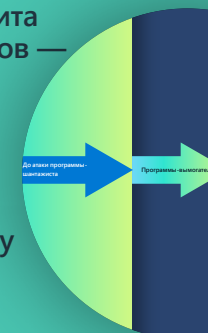
➤ Подробнее на стр. 10

Программы-шантажисты, управляемые человеком, — самые распространенные угрозы, так как 1/3 целей успешно скомпрометирована преступниками с использованием этих атак, а 5 % из них платят выкуп.



➤ Подробнее на стр. 9

Самая эффективная защита от программ-шантажистов — это многофакторная аутентификация, регулярная установка исправлений системы безопасности и применение принципа «Никому не доверяй» в сетевой архитектуре.



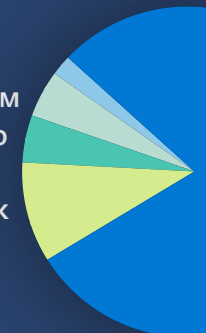
➤ Подробнее на стр. 13

Схемы фишинга учетных данных, которые нацелены на все почтовые ящики, находятся на подъеме, а компрометация корпоративной электронной почты, в том числе мошенничество со счетами, представляет значительный киберриск для организаций.

➤ Подробнее на стр. 21

Чтобы разрушить вредоносные инфраструктуры киберпреступников и национальных кибергрупп, корпорация Microsoft применяет инновационные юридические подходы и полагается на сотрудничество с государственными учреждениями и частными компаниями.

➤ Подробнее на стр. 25



Введение

Киберпреступность продолжает расти, используя как случайные, так и нацеленные атаки.

Средства киберзащиты улучшаются, и все больше государственных и частных организаций применяют упреждающий подход к предотвращению угроз, и мы видим, что злоумышленники используют 2 стратегии для получения доступа, необходимого для проведения атак. Первая из них — это кампания с широкими целями, которая зависит от объема. Вторая заключается в наблюдении и избирательном выборе цели для повышения прибыльности. Даже цель — это не получение дохода (например, действия национальных кибергрупп в геополитических целях), используются как случайные, так и нацеленные атаки. В прошлом году киберпреступники продолжали использовать социальную инженерию и острые общественные вопросы для повышения шансов на успех своих кампаний. Например, фишинговых писем на тему COVID стало меньше, но мы наблюдали рост запросов пожертвований для поддержки граждан Украины.

Они ищут и применяют новые способы реализации атак и усложняют инфраструктуру для проведения своих кампаний. Мы видим, что киберпреступники становятся экономнее и больше не платят за технологии. Чтобы снизить накладные расходы и повысить видимость легитимности, некоторые из них все чаще пытаются взломать бизнес-сети и устройства для проведения фишинговых кампаний, установки вредоносного ПО и использования вычислительных ресурсов жертв для майнинга криптовалюты.

В этой главе мы также рассмотрим рост движения хактивистов — действий обычных граждан, проводящими кибератаки для достижения социальных или политических целей. Тысячи людей по всему миру, как экспертов, так и новичков, с февраля 2022 года начали проводить такие атаки, как отключение веб-сайтов и кража данных из-за российско-украинской войны. Сейчас еще слишком рано прогнозировать, сохранится ли эта тенденция после окончания активных боевых действий.

Организации должны регулярно проверять и укреплять контроль доступа, а также внедрять стратегии безопасности для защиты от кибератак. Однако это не все, что они могут сделать. Мы расскажем, как наше подразделение по борьбе с киберпреступлениями (DCU) использовало гражданские иски для захвата контроля над вредоносной инфраструктурой, используемой киберпреступниками и национальными кибергруппами. Мы должны бороться с этой угрозой вместе, сотрудничая как с государственными, так и с частными организациями. Мы надеемся, что, поделившись тем, что мы узнали за последние 10 лет, мы поможем другим понять и принять активные меры для защиты себя и всей экосистемы от постоянно растущей угрозы киберпреступности.

Эми Хоган-Берни (Amy Hogan-Burney)

Генеральный директор, подразделение по борьбе с киберпреступлениями

Программы-шантажисты и вымогательство: угроза национального уровня

Атаки программ-шантажистов представляют серьезную опасность для всех, так как критически важная инфраструктура, компании всех размеров, а также государственные и местные органы власти становятся целью для преступников, использующих растущую экосистему киберпреступности.

За последние 2 года громкие инциденты с программами-шантажистами, такие как атаки на критически важную инфраструктуру, медицинские организации и поставщики ИТ-сервисов, привлекли значительное внимание общественности. Так как подобные атаки стали масштабнее, их последствия также расширились. Вот примеры атак, которые мы уже наблюдали в 2022 году:

- В феврале атака на 2 компании затронула систему обработки платежей сотен автозаправочных станций на севере Германии¹.
- В марте атака на почтовую службу Греции временно прервала доставку почты и обработку финансовых транзакций².
- В конце мая из-за атаки программы-шантажиста на государственные учреждения Коста-Рики правительству пришлось объявить чрезвычайное положение в стране, после того как больницы были закрыты, а обработка таможенных и налоговых сборов была нарушена³.

- Другая атака в мае вызвала задержки и отмены рейсов одной из крупнейших авиакомпаний Индии, в результате сотни пассажиров оказались в затруднительном положении⁴.

Успех этих атак и степень их реального воздействия стали результатом индустриализации экономики киберпреступности, получения доступа к инструментам и инфраструктуре, а также расширения возможностей киберпреступников за счет снижения барьера для входа.

В последние годы программы-шантажисты перешли от модели, в которой одна и та же группа разрабатывает и распространяет полезную нагрузку вымогателей, к модели «программа-шантажист как сервис» (RaaS). RaaS позволяет одной группе разрабатывать полезную нагрузку программы-шантажиста и предоставлять сервисы для получения оплаты и вымогательства посредством утечки данных другим киберпреступникам, которые фактически проводят атаки — их называют «партнерами», потому что они получают часть прибыли. Такой франчайзинг экономики киберпреступности расширил пул злоумышленников. Индустриализация инструментов для киберпреступников упростила вторжения, извлечение данных и развертывание программ-шантажистов.

Программы-шантажисты, управляемые человеком⁵ (это термин, придуманный исследователями Microsoft для описания угроз, управляемых людьми, которые принимают решения на каждом этапе атак в зависимости от того, что они обнаруживают в сети жертвы, и отличает эту угрозу от атак обычных программ-шантажистов) остаются серьезной угрозой для организаций.

Выбор цели и модель результативности программ-шантажистов, управляемых человеком



Модель основана на данных Microsoft Defender для конечной точки (EDR) (январь–июнь 2022 г.).

Программы-шантажисты и вымогательство: угроза национального уровня

Продолжение

Атаки программы-шантажистов стали еще эффективнее, так как стратегия монетизации двойного вымогательства стала, по сути, стандартом. Она включает в себя извлечение данных со взломанных устройств, шифрование данных на устройствах и последующую публикацию украденных данных или угрозу публичного размещения, чтобы заставить жертв заплатить выкуп.

Хотя большинство злоумышленников развертывают программы-шантажисты в любой сети, к которой получают доступ, некоторые из них покупают доступ у других киберпреступников, используя связи между брокерами доступа и операторами программ-шантажистов.

Уникальный набор данных сигналов, доступный нам, собирается из нескольких источников, таких как системы идентификации, электронной почты, конечных точек и облака, и дает представление о растущей экономике программ-шантажистов и системе партнеров, которая включает в себя инструменты, предназначенные для злоумышленников без технического опыта.

Расширение отношений между киберпреступниками-специалистами увеличило темпы, сложность и коэффициент успеха атак программ-шантажистов. Это привело к превращению экосистемы киберпреступников в взаимосвязанных субъектов с различными методами, целями и навыками, которые поддерживают друг друга при первоначальном доступе к целям, платежным сервисам, сайтам, инструментам расшифровки и публикации.

Теперь операторы программ-шантажистов могут покупать доступ к организациям или правительственным сетям в даркнете или получать учетные данные и доступ благодаря связи с брокерами, основная цель которых заключается исключительно в извлечении прибыли от доступа, который они получили.

Затем операторы используют приобретенный доступ для развертывания полезной нагрузки программ-шантажистов, купленной в магазинах или на форумах даркнета. Во многих случаях переговоры с жертвами ведет команда RaaS, а не сами операторы. Эти преступные транзакции почти неуязвимы, и шанс попасть в руки правоохранительных органов и предстать в суде очень мал из-за анонимности даркнета и трудностей с транснациональным обеспечением соблюдения законов.

Для успешной борьбы с этой угрозой необходимы общегосударственная стратегия и тесное сотрудничество с частным сектором.



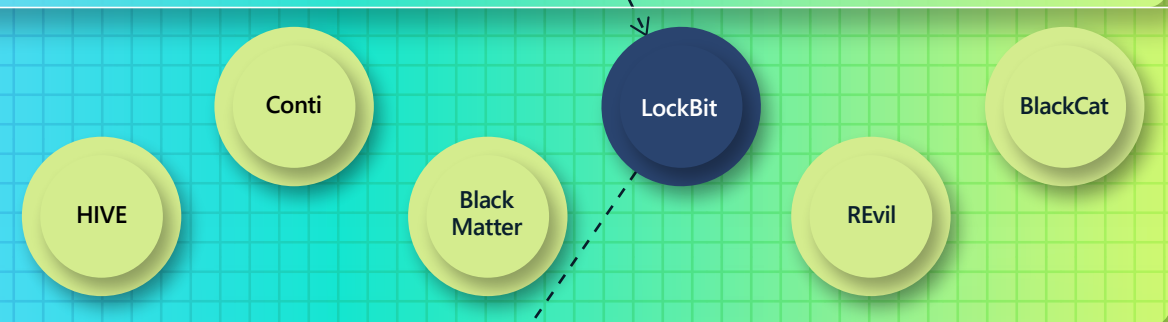
Активность цифровых угроз достигла исторического пика, а сложность кибератак растет с каждым днем.

Общие сведения об экономике программ-шантажистов

Операторы



Программа RaaS (или синдикат) — это соглашение между **оператором** и партнером. Оператор RaaS разрабатывает и поддерживает инструменты для атак программ-шантажистов, в том числе разработчиков, которые создают полезные нагрузки и платежные.



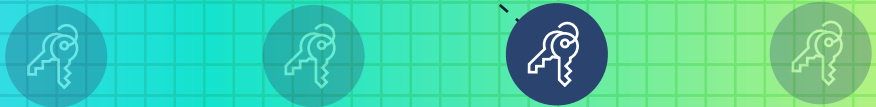
Программа RaaS (или синдикат) — это соглашение между оператором и партнером. Оператор RaaS разрабатывает и поддерживает инструменты для атак программ-шантажистов, в том числе разработчиков, которые создают полезные нагрузки и платежные порталы для связи с жертвами. Многие программы RaaS также включают набор дополнительных услуг по обеспечению вымогательства, включая размещение сайтов с утечками и интеграцию в записки о выкупе, а также услуги по расшифровке переговоров, принуждению к оплате и осуществлению криптовалютных транзакций.

Партнеры



Партнеры, как правило, представляют собой небольшие группы людей, «связанных» с одной или несколькими программами RaaS. Их роль заключается в развертывании полезных данных программы RaaS. Партнеры перемещаются в сети по горизонтали, сохраняются в системах и извлекают данные. У каждого партнера уникальные характеристики, такие как различные способы получения данных.

Брокеры доступа



Брокеры продают доступ к сети другим киберпреступникам или получают доступ сами с помощью вредоносных кампаний, метода перебора или уязвимостей. Брокера доступа могут быть как крупными, так и небольшими группами. Брокеры доступа верхнего уровня специализируются на доступе к сети крупных компаний, а у брокеров нижних уровней в даркнете может быть только 1-2 набора ценных краденых учетных данных для продажи.



Организации и частные лица со слабой киберпрофилактикой подвергаются большому риску кражи сетевых учетных данных.

Вопреки тому, как программы-шантажисты иногда изображаются в СМИ, очень редко один вариант программы-шантажиста контролируется только одной группой вымогателей. На самом деле существуют отдельные группы, которые разрабатывают вредоносное ПО, получают доступ к жертвам, развертывают программы-шантажисты и занимаются переговорами о выкупе. Индустриализация криминальной экосистемы привела к появлению следующих специализированных групп злоумышленников:

- Брокеры доступа, которые взламывают системы и передают возможности доступа («доступ как сервис»).
- Разработчики вредоносного ПО, которые продают инструменты.
- Преступные операторы и партнеры, которые проводят вторжения.
- Поставщики сервисов шифрования и вымогательства, которые берут на себя монетизацию для партнеров (RaaS).

Все управляемые человеком кампании программ-шантажистов зависят от слабых мест в системе безопасности. В частности, злоумышленники, как правило, пользуются недостаточными мерами киберпрофилактики организации, например отсутствием регулярной установки исправлений и многофакторной аутентификации (MFA).

Пример: противодействие Conti

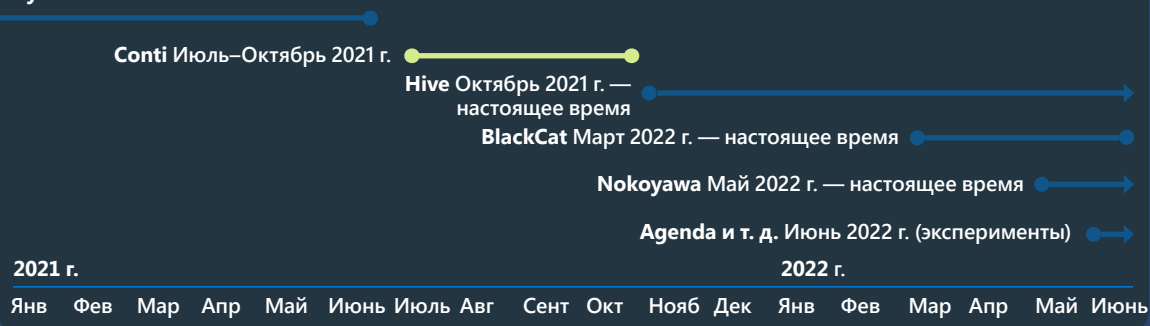
Conti — это один из самых распространенных вариантов программ-шантажистов за последние 2 года. Его применение начало падать в середине 2022 года, а Microsoft Threat Intelligence Center (MSTIC) наблюдал значительное снижение активности в конце марта и начале апреля. Мы наблюдали за последними развертываниями программ-шантажистов Conti в середине апреля. Однако, как и в случае с другими программами-шантажистами, закрытие Conti не оказало серьезного влияния на развертывание программ-шантажистов. Так специалисты MSTIC наблюдали, что партнеры Conti перешли на развертывание других полезных нагрузок, таких как BlackBasta, Lockbit 2.0, LockbitBlack и HIVE. Это согласуется с данными за предыдущие годы лет и дает возможность предположить, что когда группы вымогателей на какое-то время пропадают, они появляются вновь через несколько месяцев или передают свои технические возможности и ресурсы новым группам.

Команды аналитиков угроз в Microsoft отслеживают злоумышленников, использующих программы-шантажисты, как отдельные группы (отмеченные как DEV) на основе применяемых инструментов, а не вредоносных программ, которые они используют. Поэтому, когда партнеры Conti пропали с радаров, мы продолжили отслеживать эти группы DEV по использованию других инструментов или наборов RaaS. Например:

- Группа DEV-0230, связанная с ботнетом Trickbot, часто использовала Conti. В конце апреля специалисты MSTIC заметили, что она применяла программу-шантажист QuantumLocker.
- Группа DEV-0237 перешли от набора Conti к HIVE и NokoYawa, в том числе использовав HIVE в атаке 31 мая на государственные учреждения Коста-Рики.
- Группа DEV-0506, еще один поклонник набора инструментов Conti, использовала BlackBasta.

Пример партнера (DEV-0237), быстро переключающегося между программами RaaS

Рынок 2020 г. — Июнь 2021 г.



После того как программа RaaS, такая как Conti, закрывается, партнеры почти сразу переходят к другой программе (например, Hive).

RaaS развивает экосистему программ-шантажистов и усложняет идентификацию злоумышленников

Так как программы-шантажисты, управляемые человеком, контролируются отдельными операторами, модели подобных атак варьируются в зависимости от цели и меняются на протяжении всей атаки. Раньше мы видели тесную связь между начальным направлением атаки, инструментами и выбором полезной нагрузки программ-шантажистов в каждой кампании одного штамма. Это упрощало идентификацию злоумышленников. Однако партнерская модель RaaS разрывает эти связи. В результате корпорация Microsoft отслеживает партнеров, развертывающих полезную нагрузку в конкретных атаках, а не разработчиков полезной нагрузки программ-шантажистов в качестве операторов.

Другими словами, мы больше не предполагаем, что разработчик HIVE — это оператор атаки программы-шантажиста HIVE. Скорее всего, это партнер разработчика.

Участники отрасли кибербезопасности изо всех сил пытались точно определить такое разграничение между разработчиками и операторами. В отрасли по-прежнему часто сообщают об инциденте с программами-шантажистами, указывая название полезной нагрузки. Это создает ложное впечатление, что за всеми атаками с этой конкретной полезной нагрузкой стоит одна группа вымогателей, и все инциденты, связанные с ней, имеют общие методы и инфраструктуру. Для поддержки специалистов по безопасности сети важно узнать больше об этапах, предшествующих атакам различных партнеров, таких как извлечение данных и дополнительные механизмы сохранения в системе, а также о возможностях обнаружения и защиты, которые можно применять.

Злоумышленникам нужны учетные данные больше, чем вредоносное ПО, чтобы успешно проводить атаки. Успешное заражение программой-шантажистом, управляемой человеком, всей организации зависит от доступа к привилегированной учетной записи.

Обзор атаки программ-шантажистов, управляемых человеком

В прошлом году эксперты Microsoft по программам-шантажистам провели тщательные расследования 100 инцидентов, управляемых человеком, чтобы отследить методы злоумышленников и понять, как лучше защитить наших клиентов.

Следует отметить, что результаты анализа, которые мы приводим здесь, возможен только для управляемых устройств, подключенных к системе управления устройствами. Неуправляемые устройства — наименее защищенные аппаратные активы организации.

Самые распространенные методы, используемые программами-шантажистами на этапе развертывания:

75 %

Использование инструментов администрирования.

75 %

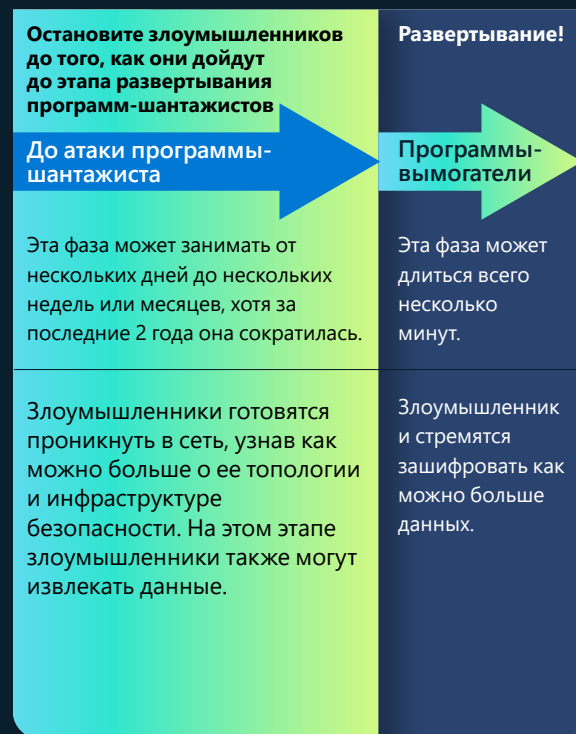
Использование приобретенной в даркнете скомпрометированной учетной записи пользователя с повышенными привилегиями для распространения вредоносных полезных данных по протоколу SMB.

99 %

Попытка подделать обнаруженные продукты для обеспечения безопасности и резервного копирования с помощью встроенных инструментов ОС.

Типичная атака, управляемая человеком

Атаки программ-шантажистов, управляемые человеком, можно разделить на фазу до установки программы-шантажиста и фазу развертывания программы-шантажиста. На первом этапе злоумышленники подготавливают проникновение в сеть, изучая топологию и инфраструктуру безопасности организации.



Наши расследования показали, что большинство участников атак программ-шантажистов, управляемых человеком, используют аналогичные недостатки системы безопасности и распространенные шаблоны и методы атак.

Надежная стратегия безопасности

Для борьбы с атаками такого рода и их предотвращение организациям нужно изменить менталитет, чтобы сосредоточиться на комплексной защите, необходимой для замедления и блокировки злоумышленников, прежде чем они смогут перейти к фазе развертывания программ-шантажистов.

Компании должны согласованно и агрессивно применять рекомендации по безопасности в своих сетях для предотвращения таких типов атак. Так как решения в итоге принимает человек, эти атаки могут генерировать множественные, казалось бы, не связанные оповещения в продуктах по обеспечению безопасности, которые могут легко затеряться или на которые специалист могут среагировать несвоевременно. Усталость от оповещений — реальный феномен, и центры информационной безопасности (SOC) могут упростить их жизнь, анализируя тенденции оповещений или группируя их в инциденты, чтобы получить расширенное представление. Затем центры информационной безопасности могут обрабатывать оповещения, используя возможности усиления безопасности, такие как правила уменьшения возможных направлений атаки. Защита от распространенных угроз может не только уменьшить число предупреждений, но и остановить многих злоумышленников, прежде чем они получат доступ к сетям.

Организации должны поддерживать высокие стандарты безопасности и профилактики сети, чтобы защититься от атак программ-шантажистов, управляемых человеком.

Практические рекомендации

Злоумышленники, использующие программ-шантажисты, руководствуются жадной легкой наживой, поэтому повышение их затрат за счет усиления безопасности является ключевым фактором разрушения экономики киберпреступников.

- 1 Сформируйте культуру профилактических мер для защиты учетных данных. Злоумышленникам нужны учетные данные больше, чем вредоносное ПО, чтобы успешно проводить атаки. Для успешного заражения всей организации программой-шантажистом, управляемой человеком, необходимы доступ к высокопривилегированной учетной записи, такой как администратор домена, или возможность редактирования групповой политики.
- 2 Проводите аудит раскрытых учетных данных.
- 3 Сделайте развертывание обновлений Active Directory приоритетом.
- 4 Назначьте приоритеты способов укрепления безопасности облака.
- 5 Сократите возможные направления атаки.
- 6 Укрепите защиту ресурсов, подключенных к Интернету, и оцените свой периметр.
- 7 Уменьшите усталость сотрудников центра информационной безопасности от предупреждений, укрепив защиту сети, чтобы уменьшить объем оповещений и сохранить ресурсы для реагирования на инциденты с высоким приоритетом.

Ссылки на дополнительную информацию

- > RaaS: понимание экономики свободного заработка киберпреступников и того, как защитить себя | Блог Microsoft Security
- > Атаки программ-шантажистов, управляемые человеком: предотвратимая катастрофа | Блог Microsoft Security

Аналитические сведения о программах-шантажистах от специалистов по безопасности

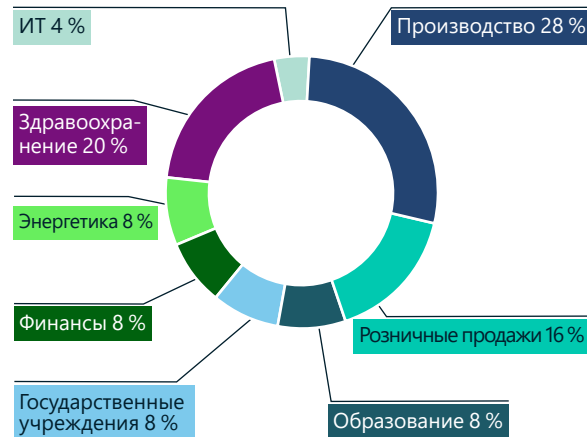
Организации во всем мире столкнулись с устойчивым ростом атак программ-шантажистов, начиная с 2019 года. Однако операции правоохранительных органов и геополитические события в прошлом году оказали серьезное влияние на киберпреступные организации.

Служба безопасности Microsoft поддерживает клиентов на протяжении всей кибератаки — от расследования до успешного сдерживания и восстановления. Сервисы реагирования и восстановления предлагаются 2 тесно интегрированными командами, одна из которых сосредоточена на расследовании и подготовке к восстановлению, а вторая — на сдерживании и восстановлении. В этом разделе представлен обзор выводов, сделанных на основе действий программ-шантажистов в прошлом году.

93 %

расследований Microsoft во время операций по восстановлению после атаки программ-шантажистов выявили недостаточные средства контроля привилегированного доступа и горизонтального перемещения.

Инциденты с программами-шантажистами и восстановление после них по отраслям

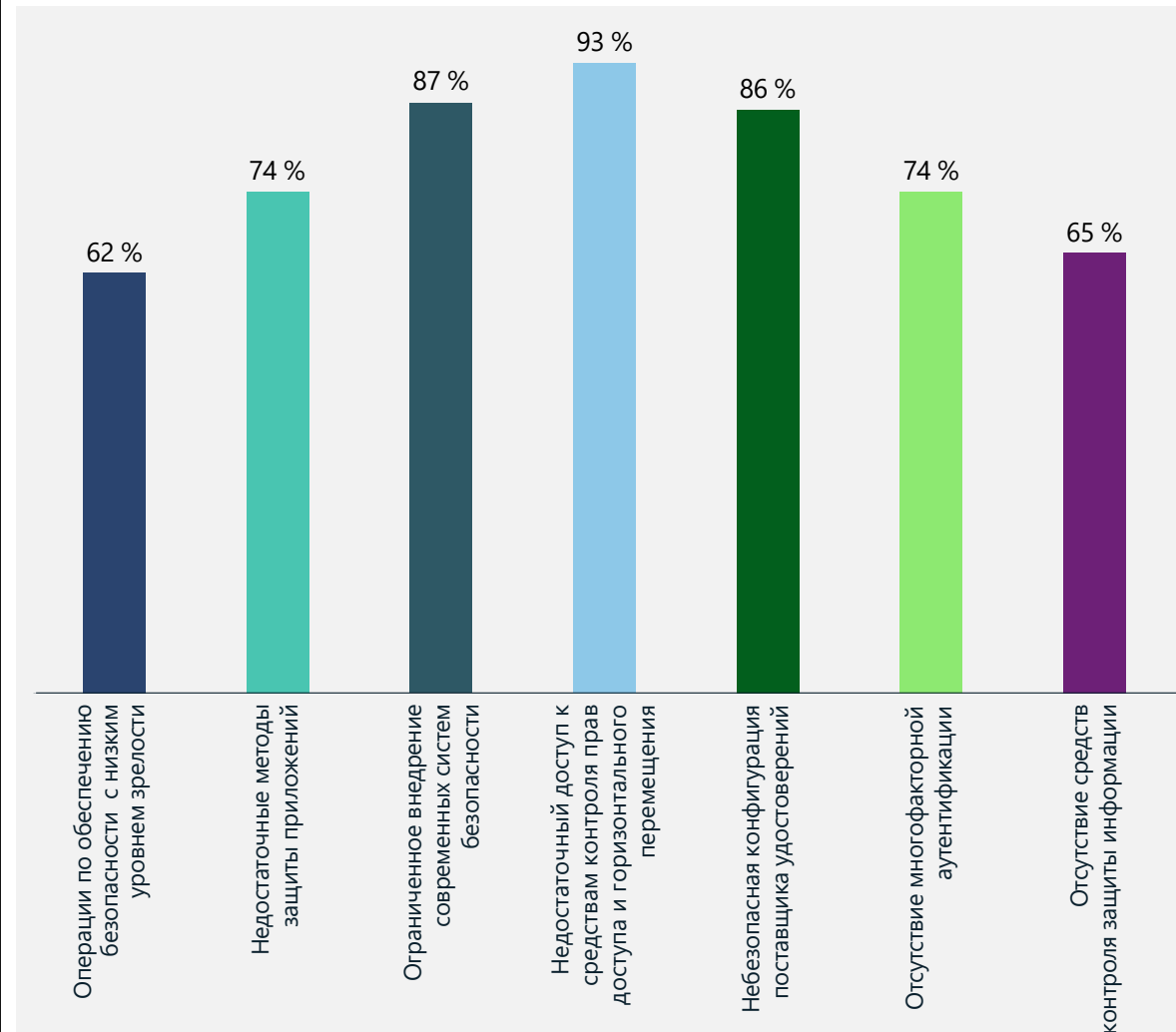


Из-за появления новых небольших групп киберпреступников и угроз специалисты по безопасности должны быть в курсе новых программ-шантажистов, защищаясь от ранее неизвестных семейств вредоносного ПО. Быстрый подход к разработке, используемый группами киберпреступников, привел к созданию интеллектуальных программ-шантажистов, упакованных в простые в использовании наборы. Это повышает гибкость при проведении масштабных атак на множество целей.

Далее представлен подробный обзор наиболее часто наблюдаемых факторов, способствующие слабой защите от программ-шантажистов, разделенных на 3 категории:

1. Слабые средства защиты удостоверений
2. Неэффективные процессы обеспечения безопасности
3. Ограниченная защита данных

Обзор самых распространенных выводов, сделанных на основе реагирования на атаки программ-шантажистов



Основной вывод, который сделали специалисты по реагированию на инциденты с программами-шантажистами, состоит в том, что атаки были вызваны недостаточными средствами контроля привилегированного доступа и горизонтального перемещения.

Аналитические сведения о программах-шантажистах от специалистов по безопасности

Продолжение

3 основных фактора, влияющих на наши операции реагирования на местах:

① **Слабые средства контроля идентификации:** атаки с целью кражи учетных данных остаются одним из главных факторов, способствующих этому

② **Неэффективные процессы обеспечения безопасности не только открывают возможности для злоумышленников, но и значительно влияют на время восстановления**

③ **В конечном итоге все сводится к данным — организациям не удается внедрить эффективную стратегию защиты данных, которая бы соответствовала потребностям их бизнеса**

① Слабые средства защиты удостоверений

Программы-шантажисты, управляемые человеком, продолжают развиваться и используют методы кражи учетных данных и горизонтального перемещения, традиционно связанные с нацеленными атаками. Успешные атаки часто являются результатом длительных кампаний, включающих в себя взлом систем идентификации, таких как Active Directory (AD), которые позволяют операторам красть учетные данные, получать доступ к системам и сохранять присутствие в сети.

Безопасность Active Directory (AD) и Azure AD security

88 %

затронутых клиентов не использовали рекомендации по безопасности AD и Azure AD. Это стало распространенным вектором атаки, так как злоумышленники используют неправильные конфигурации и слабые места в системе безопасности критически важных систем идентификации, чтобы получить расширенный доступ и возможность влияния на бизнес.

Принцип наименьших привилегий и использование рабочих станций с привилегированным доступом (PAW)

Ни одна из затронутых организаций не реализовала надлежащее разделение административных учетных данных и принцип доступа с наименьшими привилегиями через выделенные рабочие станции для управления критически важной системой идентификации и ценными ресурсами, такими как проприетарные системы и критически важные бизнес-приложения.

Безопасность привилегированных учетных записей

88 %

атак связаны с отсутствием MFA для конфиденциальных и привилегированных учетных записей, из-за чего злоумышленники смогли воспользоваться уязвимостью системы безопасности, чтобы скомпрометировать учетные данные и провести дальнейшие атаки уже с использованием подлинных учетных данных.

84 %

Администраторы в 84 % организаций не использовали средства контроля привилегий удостоверений, такие как ограниченный по времени доступ, чтобы предотвратить дальнейшее вредоносное использование скомпрометированных привилегированных учетных данных.

Аналитические сведения о программах-шантажистах от специалистов по безопасности

Продолжение

② Неэффективные процессы обеспечения безопасности

Согласно нашим данным, у организаций, пострадавших от атак программ-шантажистов, есть значительные недостатки в процессах обеспечения безопасности, инструментах и управлении жизненным циклом ИТ-ресурсов. Чаще всего мы наблюдали следующие недостатки:

Исправления:

68 %

пострадавших организаций не применяли эффективный процесс управления уязвимостями и исправлениями, а высокая зависимость от процессов, выполняемых вручную, и отсутствие автоматизированной установки исправлений привели к возникновению критических уязвимостей. Производство и критически важная инфраструктура сталкиваются с трудностями при обслуживании устаревших систем операционных технологий (ОТ) и установке исправлений.

Отсутствие инструментов для обеспечения безопасности:

Большинство организаций сообщили об отсутствии полной прозрачности состояния безопасности из-за отсутствия или неправильной конфигурации инструментов безопасности, что привело к снижению эффективности обнаружения и реагирования.

60 %

организаций сообщили о том, что не используют инструмент EDR⁶ — важнейшую технологию обнаружения и реагирования.

60 %

организаций не инвестировали в систему управления информацией о безопасности и событиях (SIEM), что привело к разрозненности мониторинга, ограниченной способности обнаружения сложных угроз и неэффективным процессам обеспечения безопасности. Автоматизация остается ключевым недостатком инструментов и процессов центров информационной безопасности, из-за чего сотрудникам приходится тратить много времени на изучение данных телеметрии.

84 %

пострадавших организаций не интегрировали мультиоблачные среды с инструментами для обеспечения безопасности.

Процессы реагирования и восстановления:

76 %

Отсутствие эффективного плана реагирования стало критически важным аспектом, который коснулся 76 % затронутых организаций. Это помешало надлежащим образом подготовиться к кризису и негативно повлияло на время реагирования и восстановления.

③ Ограниченная защита данных

Во многих скомпрометированных организациях отсутствовали надлежащие процессы защиты данных, что серьезно влияло на время восстановления и возобновления бизнес-процессов. Вот некоторые из самых распространенных недостатков:

Неизменяемые резервные копии:

44 %

организаций не создали неизменяемые резервные копии для затронутых систем. Согласно данным, у администраторов не было планов резервного копирования и восстановления для критически важных ресурсов, таких как AD.

Предотвращение потери данных:

Как правило, злоумышленники находят способ взломать системы, используя уязвимости в организации, извлекая критически важные данные для требования выкупа, кражи интеллектуальной собственности или продажи.

92 %

затронутых организаций не использовали эффективные средства предотвращения потери данных для снижения этих рисков, что привело к потере критически важных данных.

Количество программ-шантажистов уменьшилось в некоторых регионах и увеличилось в других.

В этом году мы наблюдали снижение общего числа атак программ-шантажистов, о которых сообщали наши команды реагирования в Северной Америке и Европе, по сравнению с предыдущим годом. Но число атак, зарегистрированных в Латинской Америке, возросло.

Этот факт можно объяснить тем, что киберпреступники переключили внимание с областей, которые могут вызвать реакцию правоохранительных органов, на не такие строгие цели. Так как специалисты Microsoft не заметили значительного улучшения безопасности корпоративных сетей во всем мире, то объяснить снижение обращений в службу поддержки, связанных с программами-шантажистами, можно сочетанием деятельности правоохранительных органов в 2021 и 2022 годах, которая увеличила затраты киберпреступников, а также некоторыми геополитическими событиями 2022 года.

Одна из самых масштабных операций RaaS связана с русскоязычной группой киберпреступников REvil (также известной как Sodinokibi), которая действует с 2019 года. В октябре 2021 года серверы REvil были отключены в рамках международной правоохранительной операции GoldDust⁷. В январе 2022 года Россия арестовала 14 предполагаемых участников REvil и провела рейды в 25 местах, связанных с ними⁸. Это был первый раз, когда Россия действовала против операторов программ-шантажистов на своей территории.

Хотя действия правоохранительных органов, вероятно, и замедлили частоту атак в 2022 году, злоумышленники вполне могут разработать новые стратегии, чтобы не попасться в будущем.

В 2 раза

сократилось число атак программ-шантажистов в некоторых регионах, но требуемый выкуп удвоился.

Хотя действия правоохранительных органов, вероятно, и замедлили частоту атак в 2022 году, злоумышленники вполне могут разработать новые стратегии, чтобы не попасться в будущем. Кроме того, напряженные отношения России и США из-за вторжения в Украину, похоже, положили конец зарождающемуся сотрудничеству России в глобальной борьбе с программами-шантажистами. После короткого периода неопределенности, последовавшего за арестами участников REvil, США и Россия прекратили сотрудничество в преследовании киберпреступников, что означает, что они снова могут рассматривать Россию как безопасное убежище.

Мы прогнозируем, что темпы деятельности программ-шантажистов будут зависеть от ответов на следующие важные вопросы:

1. Будут ли правительства принимать меры, чтобы помешать вымогателям действовать в своих границах, или пытаться помешать субъектам, действующим с иностранной территории?
2. Изменяют ли злоумышленники тактику, чтобы устранить необходимость в программах-шантажистах и использовать атаки с вымогательством?
3. Смогут ли организации модернизировать и трансформировать ИТ-операции быстрее, чем преступники смогут воспользоваться уязвимостями?
4. Заставят ли достижения в отслеживании выплат выкупа злоумышленникам изменить тактику и переговоры?

Практические рекомендации

1. Сосредоточьтесь на комплексных стратегиях безопасности, так как все семейства программ-шантажистов используют одни и те же уязвимости, чтобы попасть в сеть.
2. Обновляйте систему безопасности и принимайте базовые меры профилактики, чтобы повысить уровень защиты и модернизировать процессы обеспечения безопасности. Переход в облако позволяет быстрее обнаруживать угрозы и реагировать на них.

Ссылки на дополнительную информацию

- > Защитите свою организацию от программ-шантажистов | Microsoft Security
- > 7 способов защитить среду от компрометации | Блог Microsoft Security
- > Улучшение защиты с помощью ИИ для борьбы с атаками программ-шантажистов, управляемых человеком | Исследовательская команда Microsoft 365 Defender
- > Security Insider: ознакомьтесь с последними аналитическими сведениями и новостями в области кибербезопасности | Microsoft Security

Киберпреступность как сервис

Киберпреступность как сервис (СaaS) — это растущая и развивающаяся угроза для клиентов по всему миру. Подразделение Microsoft по борьбе с киберпреступлениями (DCU) наблюдало продолжающееся расширение экосистемы СaaS с увеличением числа онлайн-сервисов, упрощающих различные киберпреступления, такие как ВЕС и атаки программ-шантажистов, управляемые человеком. Фишинг остается предпочтительным методом атаки, так как киберпреступники могут извлечь существенную выгоду от успешной кражи и продажи украденных учетных записей.

В ответ на расширение рынка СaaS подразделение DCU усовершенствовало системы прослушивания для обнаружения и идентификации предложений СaaS во всей экосистеме, включающей в себя Интернет, даркнет, ограниченные форумы⁹, специализированные веб-сайты, онлайн-форумы обсуждений и платформы обмена сообщениями.

Сейчас киберпреступники сотрудничают друг с другом в разных часовых поясах и на разных языках для достижения конкретных результатов. Например, один веб-сайт СaaS, которым управляет пользователь из Азии, поддерживает операции в Европе и создает вредоносные учетные записи в Африке. Международный характер этих операций создает сложности с точки зрения охраны правопорядка и правоприменения. В ответ на это подразделение DCU концентрируется на отключении вредоносной криминальной инфраструктуры, используемой для атак СaaS, и сотрудничестве с правоохранительными органами по всему миру для привлечения преступников к ответственности.

Киберпреступники все чаще используют аналитику для увеличения охвата, масштаба и прибыли. Веб-сайты СaaS, как и обычный бизнес, должны подтверждать эффективность своих продуктов и сервисов для поддержания хорошей репутации. Например, веб-сайты СaaS регулярно автоматизируют доступ к взломанным учетным записям, чтобы подтвердить свою возможность предоставления доступа. Киберпреступники прекращают продажу определенных учетных записей после сброса паролей или установки исправлений. Все чаще мы выявляем веб-сайты СaaS, предоставляющие покупателям возможность проверки по требованию как процесс контроля качества. В результате покупатели могут быть уверены, что веб-сайт СaaS продает активные учетные записи и пароли, одновременно снижая потенциальные расходы для продавца СaaS, если украденные учетные данные будут исправлены до продажи.

Подразделение DCU также выявило веб-сайты СaaS, предлагающие возможность покупать взломанные учетные записи, связанные с определенными регионами, поставщиками онлайн-сервисов, а также конкретными лицами, профессиями и отраслями. Часто покупатели

заказывают учетные записи специалистов или отделов, которые занимаются выставлением счетов, таких как финансовые директора или бухгалтеры. Аналогичным образом, отрасли, участвующие в государственных контрактах, часто становятся мишенью из-за объема информации, которая предоставляется в процессе публичных торгов.

Исследования DCU в отношении СaaS выявили несколько ключевых тенденций:

Число и сложность их сервисов растут.

Один из примеров — это развитие веб-оболочек, которые обычно состоят из скомпрометированных веб-серверов, используемых для автоматизации фишинговых атак. Подразделение DCU наблюдало, как реселлеры СaaS упрощают загрузку фишинговых наборов или вредоносного ПО через специализированные веб-панели. Продавцы СaaS часто затем пытаются продать злоумышленнику дополнительные сервисы через эти панели, такие как сервисы спам-сообщений и специализированные списки получателей спама на основе определенных атрибутов, таких как географическое расположение и профессия. В некоторых случаях мы видели, что одна веб-оболочка используется в нескольких кампаниях атак. Это говорит о том, что злоумышленники могут поддерживать постоянный доступ к скомпрометированному серверу. Мы также наблюдали рост числа сервисов анонимизации, доступных в экосистеме СaaS, а также предложений для виртуальных частных сетей (VPN) и виртуальных частных серверов (VPS). В большинстве случаев предлагаемые VPN/VPS первоначально приобретались с помощью краденых кредитных карт. На веб-сайтах СaaS также предлагалось множество протоколов удаленного рабочего стола (RDP), безопасной оболочки (SSH) и сPанелей в качестве платформы для проведения

кибератак. Продавцы СaaS настраивают RDP, SSH и сPанели с помощью соответствующих инструментов и скриптов для реализации различных типов кибератак.

Сервисы по созданию омоглифических доменов все чаще требуют оплаты в криптовалюте.

Омоглифические домены выдают себя за подлинные доменные имена, используя символы, которые внешне идентичны или почти идентичны другому символу. Их цель — обмануть пользователей, заставив их думать, что это подлинный домен. Это повсеместная угроза и точка входа для множества кибератак. Сайты СaaS теперь продают омоглифические доменные имена, что позволяет покупателям запрашивать конкретные компании и доменные имена для обмана пользователей. После получения платежа продавцы СaaS используют генератор омоглифов для выбора доменного имени, а затем регистрируют вредоносный домен. Этот сервис оплачивается практически только в криптовалюте.

2 750 000

попыток регистрации сайтов успешно заблокированы DCU в этом году, чтобы помешать злоумышленникам, которые планировали использовать их для киберпреступлений во всем мире.

Киберпреступность как сервис

Продолжение

Продавцы SaaS все чаще предлагают скомпрометированные учетные данные для продажи.

Скомпрометированные учетные данные предоставляют несанкционированный доступ к учетным записям пользователей, в том числе к сервисам электронной почты, корпоративным ресурсам обмена файлами и OneDrive для бизнеса. Если скомпрометированы учетные данные администратора, неавторизованные пользователи могут получить доступ к конфиденциальным файлам, ресурсам Azure и корпоративным учетным записям. Во многих случаях расследования DCU выявили несанкционированное использование одних и тех же учетных данных на нескольких серверах в качестве средства автоматизации проверки учетных данных. Это говорит о том, что скомпрометированный пользователь мог стать жертвой нескольких фишинговых атак или на устройстве установлено вредоносное ПО, с помощью которого клавиатурные шпионы ботнета собирают учетные данные.

Появляются сервисы и продукты SaaS с расширенными функциями, позволяющими избежать обнаружения.

Один продавец SaaS предлагает фишинговые наборы с повышенными уровнями сложности и функциями анонимизации, предназначенными для обхода систем обнаружения и предотвращения, всего за 6 долларов США в день. Сервис реализует последовательность перенаправлений, которые выполняют проверки, прежде чем разрешить

передачу трафика на следующий уровень или сайт. В рамках одного из таких процессов выполняется больше 90 проверок отпечатков устройства, в том числе проверка на виртуальную машину, сбор сведений об используемом браузере и оборудовании, а также многое другое. Если все проверки пройдены, трафик отправляется на целевую страницу, используемую для фишинга.

Комплексные сервисы киберпреступников продают подписки на управляемые сервисы.

Как правило, каждый шаг киберпреступления может выдать злоумышленников, если уровень операционной безопасности низкий. Риск обнаружения и идентификации растет, если сервисы приобретаются на нескольких сайтах SaaS. Подразделение DCU наблюдало тревожную тенденцию в даркнете: увеличивается число сервисов, предлагающих анонимизацию программного кода и обобщение текста веб-сайта для снижения риска обнаружения. Поставщики комплексных сервисов киберпреступников управляют всеми сервисами и гарантируют результаты, что еще больше снижает риск обнаружения подписывающейся ОСН. Благодаря этому популярность этих комплексных сервисов возросла.

Модель «фишинг как сервис» (PhaaS) — один из примеров комплексного сервиса киберпреступников. PhaaS — это результат развития полностью необнаруживаемых сервисов (FUD). Эти сервисы предлагаются по подписке. Типичные условия использования PhaaS включают в себя поддержание активности фишинговых веб-сайтов в течение месяца.

Специалисты DCU также обнаружили продавца SaaS, предлагающего DDoS-атаки по модели подписки. В рамках этой модели созданием и обслуживанием ботнета, необходимого для проведения атак, занимается продавец SaaS.

PhaaS: киберпреступники предлагают несколько сервисов в рамках одной подписки. В общем случае покупателю нужно выполнить всего лишь 3 действия:

1

Выбрать шаблон/дизайн фишингового сайта из сотен предложенных.

2

Указать адрес электронной почты для получения учетных данных, полученных от жертв фишинга.

3

Заплатить продавцу PhaaS в криптовалюте.

Как только эти действия будут выполнены, продавец PhaaS создает сервисы с 3 или 4 уровнями перенаправления и размещает ресурсы для атаки на конкретных пользователей. Затем кампания запускается, а учетные данные жертв собираются, проверяются и отправляются на адрес электронной почты, указанный покупателем. За дополнительную плату многие продавцы PhaaS могут размещать фишинговые сайты в публичном блокчейне, чтобы к ним мог получить доступ любой браузер, а перенаправления могли указывать пользователям на ресурс в распределенном реестре.

Каждый клиент с подпиской на DDoS получает зашифрованный сервис для повышения операционной безопасности и круглосуточную поддержку на 1 год. Этот DDoS-сервис поддерживает различные архитектуры и методы атаки, поэтому покупатель просто выбирает целевой ресурс, а продавец предоставляет доступ ко множеству скомпрометированных устройств в своем ботнете для проведения атаки. Стоимость подписки на DDoS-сервис составляет всего 500 долларов США.

Работа DCU по разработке инструментов и методов, которые выявляют и предотвращают деятельность киберпреступников SaaS, продолжается. Развитие SaaS-сервисов создает значительные проблемы, особенно для борьбы с незаконными криптовалютными платежами.

Преступное использование криптовалют

Криптовалюты становятся популярнее, и преступники все чаще используют их для уклонения от правоохранительных органов и мер по борьбе с отмыванием денег. Это усложняет правоохранительным органам отслеживание криптовалютных платежей киберпреступникам.

Глобальные расходы на блокчейн-решения выросли примерно на 340 % за последние 4 года, а число новых криптовалютных кошельков увеличилось приблизительно на 270 %. В мире больше 83 миллионов уникальных кошельков, а общая рыночная капитализация всех криптовалют составила примерно 1,1 триллиона долларов США по состоянию на 28 июля 2022 года¹⁰.



Источник: Twitter.com — @PeckShieldAlert (PeckShield — китайская компания, специализирующаяся на безопасности блокчейна).

Отслеживание платежей программ-шантажистов

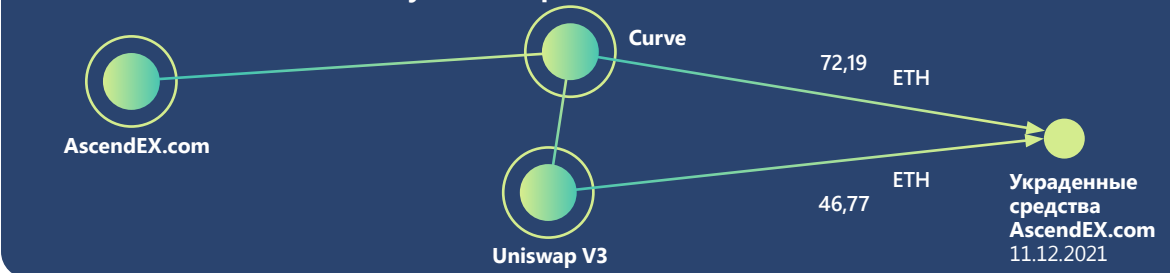
Программы-шантажисты — один из крупнейших источников незаконно полученной криптовалюты. Пытаясь разрушить вредоносную техническую инфраструктуру, используемую в атаках программ-шантажистов, например Zloader в апреле 2022 года¹¹, подразделение DCU корпорации Microsoft следит за кошельками преступников для отслеживания и восстановления криптовалюты.

Следователи DCU наблюдали, как злоумышленники, использующие программы-шантажисты, меняли тактику общения с жертвами, чтобы скрыть денежный след. Раньше киберпреступники указывали адреса биткоин-кошельков в записке о выкупе. Однако это упрощало отслеживание платежных транзакций в блокчейне, поэтому злоумышленники-шантажисты вместо этого начали добавлять адреса электронной почты или ссылки на чат-сайты для передачи адресов для выплаты выкупа жертвам. Некоторые даже создали уникальные веб-страницы и страницы входа для каждой жертвы, чтобы помешать специалистам по безопасности и правоохранительным органам узнать адреса кошельков преступников, притворяясь жертвами. Несмотря на попытки преступников скрыть следы, некоторые выплаты в счет выкупа все еще можно восстановить с помощью правоохранительных органов и криптоаналитиков, которые могут отслеживать движение средств в блокчейне.

Тенденция: отмывание незаконных доходов с помощью децентрализованных бирж (DEX)

Ключевой вопрос для киберпреступников заключается в конвертации криптовалюты в обычные деньги. У них есть несколько способов обмена, каждый из которых сопряжен с различными степенями риска. Один из методов снижения риска — это отмывание доходов через децентрализованную биржу (DEX) перед обналичиванием с помощью доступных вариантов вывода средств, таких как

Отслеживание незаконно полученной криптовалюты



Используя инструмент расследования криптовалют Chainalysis, подразделение по борьбе с киберпреступлениями Microsoft обнаружило, что хакеры AscendEX обменяли краденые средства на небольшой DEX-бирже Curve, в дополнение к Uniswap. На этой схеме показаны маршруты отмывания, выявленные нашей командой. Каждый круг представляет кластер кошельков, а цифры в каждой строке — общую сумму монет Ethereum, переданную для отмывания.

централизованные биржи (CEX), пиринговые (P2P) и внебиржевые сервисы обмена (OTC). Децентрализованные биржи — привлекательные ресурсы для преступников, потому что часто они не соблюдают меры по борьбе с отмыванием денег.

В декабре 2021 года хакеры атаковали глобальную криптовалютную торговую платформу AscendEX и похитили около 77,7 миллиона долларов США в криптовалюте, принадлежащей ее клиентам¹². Компания AscendEX наняла фирмы, занимающиеся анализом блокчейна и связалась с другими централизованными биржами, чтобы кошельки, на которые поступили украденные средства, можно было занести в черный список. Кроме того, адреса, на которые отправили украденную криптовалюту, поместили соответствующим образом в блокчейн-обозревателе Etherscan для криптовалюты Ethereum¹³. Чтобы не попасть в черный список, хакеры отправили Ethereum на 1,5 миллиона долларов США на одну из крупнейших в мире децентрализованных бирж Uniswap 18 февраля 2022 года¹⁴.

Принятие жестких мер по борьбе с отмыванием денег через DEX может ослабить эти процессы и заставить киберпреступников использовать

другие методы, такие как смешивание монет или нелицензированные биржи. Например, биржа Uniswap недавно объявила, что начнет использовать черные списки, чтобы не позволить кошелькам, которые участвуют в незаконной деятельности, выполнять транзакции на бирже¹⁵.

Практические рекомендации

- 1 Если вы стали жертвой киберпреступников и заплатили им криптовалютой, обратитесь в местные правоохранительные органы, которые помогут отследить и вернуть потерянные средства.
- 2 Ознакомьтесь с мерами по борьбе с отмыванием денег при выборе DEX-биржи.

Ссылки на дополнительную информацию

- Аппаратная защита от угроз от усложняющихся методов криптоджекинга | Исследовательская группа Microsoft 365 Defender

Развивающаяся среда фишинговых угроз

Схемы фишинга учетных данных набирают обороты и остаются серьезной угрозой для пользователей во всем мире, так как они нацелены на все почтовые ящики. Среди угроз, которые отслеживают и блокируют наши исследователи, объем фишинговых атак на порядки больше, чем все остальных.

Используя данные из Defender для Office, мы наблюдаем вредоносные электронные письма и действия со скомпрометированными удостоверениями. Сервис «Защита идентификации Azure Active Directory» предоставляет еще больше сведений с помощью оповещений о событиях, связанных со скомпрометированными удостоверениями. При использовании Defender для облачных приложений мы наблюдаем такие события, а Microsoft 365 Defender (M365D) коррелирует данные между продуктами. Метрика бокового перемещения взята из Defender для конечных точек (оповещения о поведении при атаке и событиях), Defender для Office (вредоносные письма) и опять M365D (для корреляции между продуктами).

710 млн

фишинговых писем блокируются за неделю.

1 ч 12 мин

Среднее время, необходимое злоумышленнику для доступа к личным данным, если вы станете жертвой фишингового письма¹⁶.

1 ч 42 мин

Среднее время, в течение которого злоумышленник начинает горизонтальное перемещение в корпоративной сети после взлома устройства¹⁷.

Учетные данные Microsoft 365 остаются одним из самых популярных среди злоумышленников типов учетных записей. После компрометации учетных данных для входа злоумышленники могут войти в компьютерные системы, связанные с корпоративной средой, чтобы упростить ее заражение вредоносными программами и программами-шантажистами, украсть конфиденциальные данные и информацию компании, получив доступ к файлам SharePoint, а также продолжить фишинговую атаку, отправляя вредоносные письма с помощью Outlook.

В дополнение к кампаниям с расширенными целями, фишингу для получения учетных данных, пожертвований и личной информации, злоумышленники выбирают отдельные компании для получения крупных выплат. Фишинговые атаки по электронной почте на организации с целью получения финансовой выгоды называют ВЕС-

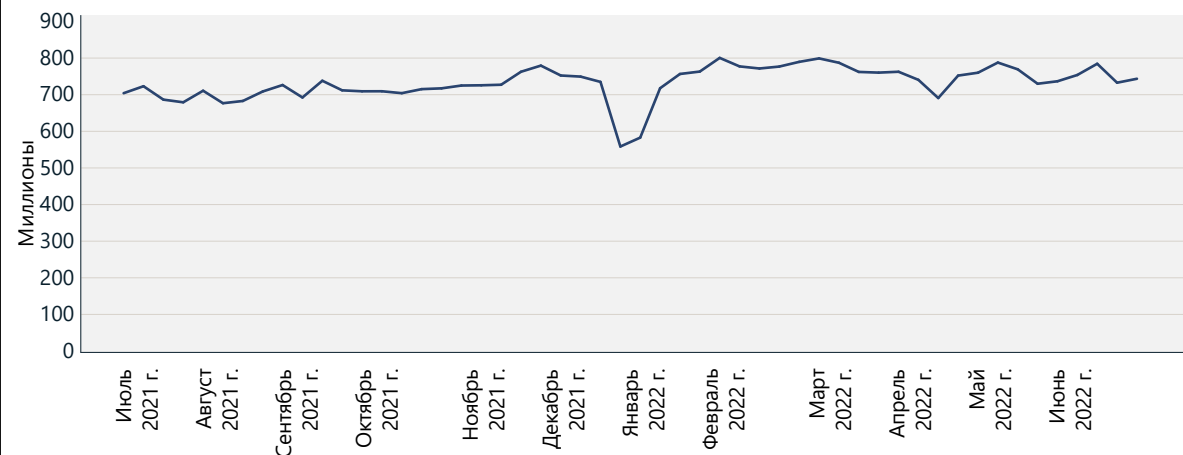
атаками. Корпорация Microsoft ежемесячно обнаруживает миллионы ВЕС-сообщений, что составляет 0,6 % от всех наблюдаемых фишинговых писем. В отчете IC3¹⁸, опубликованном в мае 2022 года, описывается тенденция роста ущерба из-за ВЕС-атак, сведения о которых раскрываются компаниями.

Методы, используемые в фишинговых атаках, становятся все сложнее. В ответ на меры защиты злоумышленники применяют новые способы реализации атак и усложняют инфраструктуру для проведения своих кампаний. Это значит, что организациям следует регулярно пересматривать стратегию внедрения решений безопасности для блокировки вредоносных писем и усиления контроля доступа для отдельных учетных записей пользователей.

531 000

В дополнение к URL-адресам, заблокированным Defender для Office, наше подразделение по борьбе с киберпреступлениями руководило удалением 531 000 уникальных фишинговых URL-адресов, размещенных за пределами решений Microsoft.

Обнаруженные фишинговые письма



Количество фишинговых писем, обнаруженных за неделю, продолжает расти. Снижение в декабре-январе — это ожидаемое сезонное падение, которое также отражено в прошлогоднем отчете. Источник: сигналы Exchange Online Protection.

Развивающаяся среда фишинговых угроз

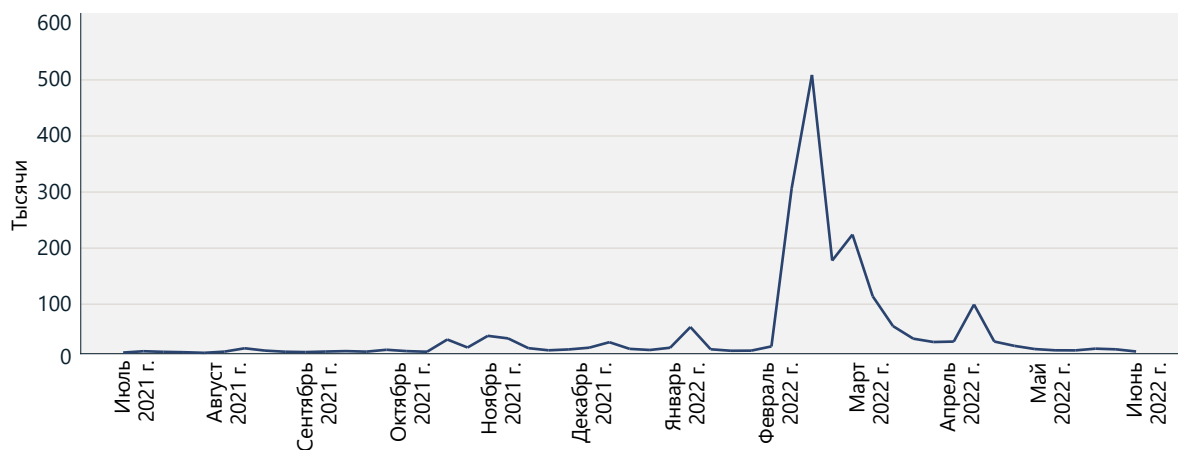
Продолжение

Мы продолжаем наблюдать устойчивый рост числа фишинговых писем с каждым годом. Переход на удаленную работу в 2020 и 2021 годах привел к резкому увеличению числа фишинговых атак, направленных на извлечение выгоды из меняющейся рабочей среды. Злоумышленники быстро применяют новые шаблоны писем, используя приманки, связанные с глобальными событиями, такими как пандемия COVID-19, и инструментами совместной работы и повышения производительности, такими как Google Диск или OneDrive. Число писем на тему COVID-19 снизилось, и с начала марта 2022 года новой приманкой война стала в Украине. Наши исследователи наблюдали резкое увеличение числа писем от злоумышленников, выдающих себя за настоящие организации и запрашивающих криптовалютные пожертвования в Bitcoin и Ethereum якобы для поддержки украинских граждан.

Всего через несколько дней после начала войны в конце февраля 2022 года число обнаруженных у корпоративных клиентов фишинговых писем, содержащих адреса Ethereum, резко возросло. Общее число обнаружений достигло пика в первую неделю марта — полмиллиона фишинговых писем содержали адрес кошелька Ethereum. До начала войны число адресов кошельков Ethereum в других письмах, отмеченных как фишинговые, было существенно меньше, — в среднем несколько тысяч писем в день.

Сейчас как никогда фишеры полагаются на подлинную инфраструктуру для своих атак, что приводит к росту фишинговых кампаний, направленных на компрометацию различных аспектов операций компаний, чтобы им

Фишинговые письма с адресами кошельков Ethereum



Общее число электронных писем, отмеченных как фишинговые и содержащие адреса кошельков Ethereum, увеличилось в начале украинско-российского конфликта и сократилось после первоначального всплеска.

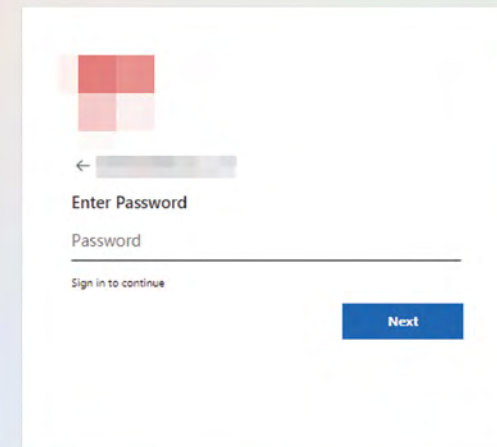
не приходилось покупать, размещать или управлять собственной инфраструктурой. Например, вредоносные письма могут исходить от скомпрометированных учетных записей отправителей. Злоумышленники извлекают выгоду от использования таких адресов с высокой оценкой репутации, которые считаются надежнее новых учетных записей и доменов. В некоторых продвинутых фишинговых кампаниях мы обнаружили, что злоумышленники предпочитают отправлять и подделывать домены, в которых функция DMARC¹⁹ настроена неправильно и не выполняет никаких действий при обнаружении инцидента, что позволяет подделывать электронные письма.

В масштабных фишинговых операциях обычно используются облачные сервисы и облачные виртуальные машины (VM) для проведения серьезных атак. Злоумышленники могут полностью автоматизировать развертывание

и доставку электронной почты с VM с помощью ретрансляторов SMTP или облачной инфраструктуры электронной почты, чтобы воспользоваться высокими показателями доставки и положительной репутацией этих сервисов. Если вредоносное письмо пройдет через эти облачные сервисы, специалисты по безопасности должны полагаться на надежные функции фильтрации электронной почты, чтобы не допускать письма в свою среду.

Учетные записи Microsoft остаются главной мишенью для фишеров, о чем свидетельствуют многочисленные фишинговые целевые страницы, которые имитируют страницу входа Microsoft 365. Например, фишеры пытаются воссоздать страницу входа Майкрософт в своих фишинговых наборах, создавая уникальный URL-адрес, адаптированный под получателя. Этот адрес указывает на вредоносную веб-страницу, созданную для сбора учетных данных, однако параметр в URL-адресе будет содержать адрес электронной почты конкретного получателя. Когда потенциальная жертва перейдет на страницу, фишинговый набор предварительно заполнит данные входа пользователя и корпоративный логотип, настроенный на получателя электронной почты, имитируя интерфейс страницы входа в Microsoft 365 целевой компании.

Фишинговая страница, выдающая себя за страницу входа Microsoft с динамическим контентом

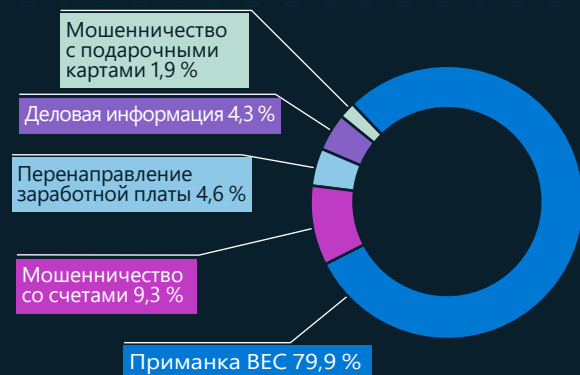


Акцент на компрометацию деловой электронной почты

Киберпреступники разрабатывают сложные схемы и методы, чтобы обойти стандартные механизмы безопасности, и нацеливаются на отдельных пользователей, коммерческие и иные организации. В ответ на это мы инвестируем значительные ресурсы в дальнейшее улучшение нашей программы защиты от ВЕС.

ВЕС — это самый дорогостоящий вид финансовых киберпреступлений. По оценкам, в 2021 году ущерб от них составит 2,4 миллиарда долларов США — это 59 % от 5 крупнейших категорий ущерба от интернет-преступности во всем мире²⁰. Чтобы понять масштаб проблемы и определить, как лучше всего защитить пользователей от ВЕС, исследователи безопасности Microsoft отслеживают самые распространенные темы, используемые в атаках.

Темы ВЕС (январь–июнь 2022 г.)



Темы ВЕС по проценту обнаружений

Тенденции ВЕС

В качестве точки входа злоумышленники ВЕС, как правило, пытаются начать разговор с потенциальными жертвами, чтобы установить контакт с ними. Выдавая себя за коллегу или делового знакомого, злоумышленник постепенно подводит беседу к денежному переводу. Вводные письма, которые мы считаем приманкой ВЕС, представляют около 80 % от обнаруженных писем ВЕС. Ниже представлены другие тенденции, выявленные исследователями безопасности Microsoft за последний год:

- Чаще всего для ВЕС-атак в 2022 году использовали спуфинг²¹ и имитацию²².
- Подтипом ВЕС-атак, наносивших самый большой финансовый ущерб жертвам, было мошенничество со счетами-фактурами (на основе объема и запрошенных сумм в долларах, наблюдаемых в наших расследованиях кампаний ВЕС).
- Кража деловой информации, такой как отчеты о кредиторской задолженности и контактные данные клиентов, позволяет злоумышленникам проводить убедительные атаки со счетами-фактурами.
- Большинство запросов на перенаправление заработной платы отправили из бесплатных почтовых сервисов, для этого редко использовались скомпрометированные учетные записи. Пик объема электронных писем от этих источников наблюдался 1-го и 15-го числа каждого месяца — это самые распространенные даты начисления заработной платы.
- Несмотря на то, что мошенничество с подарочными картами хорошо известно, на него пришлось только 1,9 % от числа обнаруженных ВЕС-атак.

Практические рекомендации

Защита от фишинга

Чтобы снизить риски фишинговых атак, ИТ-администраторам рекомендуется реализовать следующие политики и функции:

1. Требовать использования MFA во всех учетных записях для ограничения несанкционированного доступа.
2. Включить функции условного доступа для учетных записей с высокими привилегиями, чтобы не допускать доступ из стран, регионов и IP-адресов, которые обычно не генерируют трафик для вашей организации.
3. По возможности использовать физические ключи безопасности для руководителей, сотрудников, участвующих в платежных или закупочных операциях, и владельцев других привилегированных учетных записей.
4. Требовать использовать браузеры, поддерживающие такие сервисы, как Microsoft SmartScreen, для анализа URL-адресов на предмет подозрительного поведения и блокировки доступа к известным вредоносным веб-сайтам²³.
5. Использовать решение по безопасности на основе машинного обучения, которое с высокой точностью помещает на карантин фишинговые письма, а также проверяет URL-адреса и вложения в изолированной среде, прежде чем письмо попадет в папку «Входящие», такое как Microsoft Defender для Office 365²⁴.
6. Включить функции защиты от имитации и спуфинга во всей организации.
7. Настроить политики (DKIM) и DMARC, чтобы не допускать доставку электронных писем, не прошедших аутентификацию, которые могут имитировать подлинных отправителей.
8. Проводить аудит правил, созданных клиентом и пользователями, и удалять широкие исключения для доменов и IP-адресов. Эти правила часто обладают приоритетом и могут пропускать известные вредоносные письма через фильтры электронной почты.
9. Регулярно запускать симуляторы фишинга, чтобы оценить потенциальный риск организации, а также выявить и обучить уязвимых пользователей.

Ссылки на дополнительную информацию

- > От кражи файлов cookie до ВЕС: злоумышленники используют фишинговые сайты AiTM как точку входа для дальнейшего финансового мошенничества | исследовательская группа Microsoft 365 Defender, Microsoft Threat Intelligence Center (MSTIC)

Обман с использованием омоглифов

ВЕС и фишинг — это распространенные методы социальной инженерии, которая играет значительную роль в киберпреступности — она помогает убедить жертву начать общаться с преступником и довериться ему.

В традиционной торговле товарные знаки применяются для подтверждения происхождения продукта или услуги, а поддельные продукты производят с фальшивыми товарными знаками. Так и киберпреступники выдают себя за контактное лицо, знакомое цели во время фишинговой атаки, используя омоглифы для обмана потенциальных жертв.

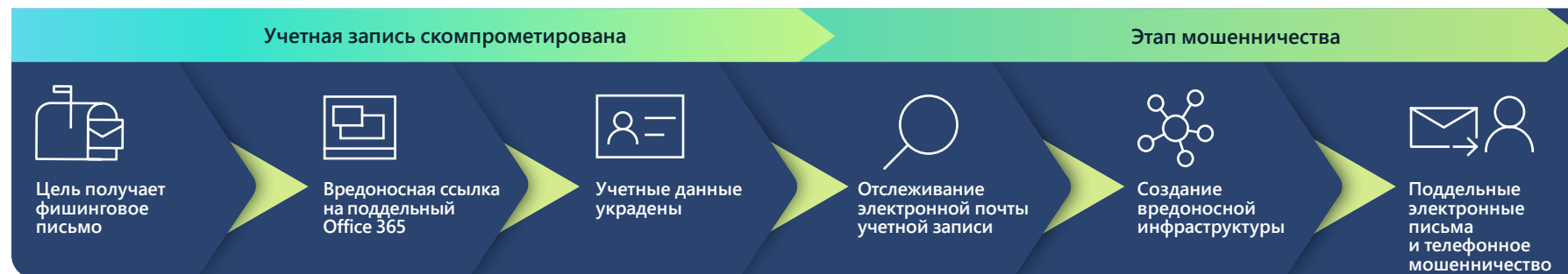
Омоглиф — это доменное имя, используемое для общения по электронной почте в ходе ВЕС-атаки, в котором символ заменяется на идентичный или почти идентичный по внешнему виду, чтобы обмануть цель.

Омоглифические методы, используемые в ВЕС-атаках

ВЕС-атака обычно проводится в 2 этапа, первый из которых включает в себя компрометацию учетных данных. Такие типы утечек учетных данных могут быть результатом фишинговых атак или масштабных утечек данных. После этого учетные данные продаются или выставляются в темной сети.

Вторая стадия — это этап мошенничества, когда злоумышленники используют скомпрометированные учетные данные для сложной атаки социальной инженерии с использованием омоглифических доменов электронной почты.

Ход ВЕС-атаки



Методы	% доменов, использующие омоглифические методы
замена I на l	25 %
замена l на i	12 %
замена g на q	7 %
замена m на rn	6 %
замена .com на .cam	6 %
замена o на 0	5 %
замена l на ll	3 %
замена i на ii	2 %
замена w на vv	2 %
замена ll на l	2 %
замена a на e	2 %
замена m на nn	1 %
замена I на ll, замена i на l	1 %
замена u на o	1 %

Анализ 1700 омоглифических доменов за период с января по июль 2022 года. Всего было использовано 170 омоглифических методов, но 75 % доменов использовали только 14 методов.

Омоглифы в действии

Омоглифический домен, который выглядит идентично почтовому домену, известному жертве, зарегистрирован в системе поставщика почтового сервиса с идентичным именем пользователя. Затем из поддельного домена отправляется электронное письмо с новыми инструкциями по оплате.

Используя средства аналитики с открытым исходным кодом и доступ к потокам электронной почты, преступники определяют лиц, которые отвечают за выставление счетов и платежи. Затем они создают олицетворение адреса электронной почты отправителя счетов-фактур. Это олицетворение состоит из идентичного имени пользователя и почтового домена, который омоглифом домена подлинного отправителя.

Злоумышленник копирует цепочку сообщений электронной почты, содержащую настоящий счет-фактуру, а затем добавляет в него собственные банковские реквизиты. После этого измененный счет-фактура повторно отправляется цели с поддельного адреса электронной почты. Так как контекст имеет смысл, а электронное письмо выглядит подлинным, цель часто следует инструкциям мошенников.

Практические рекомендации

1. Требовать использовать браузеры, поддерживающие сервисы анализа URL-адресов на предмет подозрительного поведения и блокировки доступа к известным вредоносным веб-сайтам, такие как Safe Links и SmartScreen²⁵.
2. Использовать решение по безопасности на основе машинного обучения, которое с высокой точностью помещает на карантин фишинговые письма, а также проверяет URL-адреса и вложения в изолированной среде, прежде чем письмо попадет в папку «Входящие».

Ссылки на дополнительную информацию

- > Internet Crime Complaint Center (IC3) | Business Email Compromise: The \$43 Billion Scam
- > Анализ спуфинга — Office 365 | Microsoft Docs
- > Анализ олицетворения — Office 365 | Microsoft Docs

Хронология удаления ботнетов с первых дней сотрудничества корпорации Microsoft

Уже больше 10 лет подразделение DCU прилагает все усилия, чтобы предотвратить киберпреступления, что привело к блокировке 26 вредоносных программ и атак национального масштаба. Команда DCU использует продвинутое тактики и инструменты для пресечения незаконных операций, и мы наблюдаем, что киберпреступники также развивают свои методики, чтобы быть на шаг впереди. Вот временная шкала с некоторыми ботнетами, устраненных DCU, и стратегиями, которые корпорация Microsoft использовала для их уничтожения.

Создано подразделение Microsoft по борьбе с киберпреступлениями

Сотрудничество: направлено на борьбу с киберпреступлениями, влияющими на экосистему Microsoft, за счет тесной совместной работы исследователей, юристов и инженеров.

Подход Microsoft: цель состоит в том, чтобы лучше понять технические аспекты различного вредоносного ПО и предоставить эти сведения юридическому отделу Microsoft для разработки эффективной стратегии разрушения.

Ботнет Sirefef/Zero Access

Описание: рекламный ботнет, перенаправляющий пользователей на опасные веб-сайты, которые устанавливают вредоносное ПО или крадут личную информацию; ботнет заразил 2 миллиона компьютеров и обошелся рекламодателям в 2,7 миллиона долларов США в месяц; основные цели атаки — в США и Западной Европе.

Сотрудничество: корпорация Microsoft тесно сотрудничала с ФБР и Центром киберпреступности Европола, чтобы вывести из строя P2P-инфраструктуру ботнета.

Ответ Microsoft: корпорация присоединилась к сети Zero Access, заменила вредоносные серверы C2 и успешно захватила домены сервера скачивания.

Акцент на разрушении инфраструктуры киберпреступников

Описание: за последний год корпорация Microsoft разрушила инфраструктуру 7 злоумышленников, не позволив им распространять другие вредоносные программы, контролировать компьютеры жертв и выбирать новых жертв.

Сотрудничество: вместе с интернет-провайдерами, правительствами, правоохранительными органами и частным сектором корпорация сервис-провайдер опубликовала информацию для исправления 17 миллионов жертв вредоносного ПО по всему миру.

2008 г.

Ботнет Conficker

Описание: быстро распространяющийся червь, нацеленный на ОС Windows, заражающий миллионы компьютеров и устройств в общей сети; вызвал сетевые сбои во всем мире.

Сотрудничество: создание рабочей группы Conficker — первого консорциума такого рода. Корпорация Microsoft объединила силы 16 организациями со всего мира, чтобы уничтожить ботнет.

Ответ Microsoft: группа работала во многих международных юрисдикциях и успешно уничтожила Conficker.

2009 г.

Ботнет Waledac

Описание: сложный спам-ботнет с доменами в США, который собирал адреса электронной почты и распространял спам, заражая до 90 000 компьютеров по всему миру²⁶.

Сотрудничество: был создан еще один консорциум, Центр Microsoft по защите от вредоносных программ Microsoft (MMPC), для тесного сотрудничества с учеными²⁷.

Ответ Microsoft: корпорация Microsoft применила многоуровневый подход к выводу из строя центра управления и удивила злоумышленников, захватив домены в США без предварительного уведомления²⁸. Корпорация Microsoft временно получила права собственности на почти 280 доменов, используемых серверами Waledac.

2011 г.

Ботнет Rustock

Описание: спам-бот/трояня, использующий черный ход и интернет-провайдеров в качестве основных центров управления; предназначен для продажи фармацевтических препаратов.

Сотрудничество: корпорация Microsoft объединила усилия с компанией Pfizer Pharmaceuticals, чтобы изучить препараты, продаваемые Rustock, и тесно сотрудничала с голландскими правоохранительными органами²⁹.

Ответ Microsoft: корпорация Microsoft обратилась к службе федеральных маршалов США и правоохранительным органам Нидерландов, чтобы вывести из строя серверы управления в этой стране. Были зарегистрированы и заблокированы все будущие алгоритмы генератора доменов (DGA).

2013 г.

Ботнет Trickbot

Описание: сложный ботнет с фрагментированной инфраструктурой по всему миру, ориентированный на индустрию финансовых услуг; использовался для взлома устройств Интернета вещей.

Сотрудничество: корпорация Microsoft объединила усилия с организацией Financial Services Information Sharing and Analysis Center (FS-ISAC), чтобы вывести из строя Trickbot³⁰.

Ответ Microsoft: подразделение DCU разработало систему для выявления и отслеживания инфраструктуры ботов, которая генерировала уведомления для активных интернет-провайдеров с учетом действующих законов в различных странах.

2019 г.

2022 г.

Взгляд в будущее

Подразделение DCU продолжает внедрять инновации и стремится использовать свой опыт борьбы с ботнетами для проведения скоординированных операций, выходящих за рамки вредоносного ПО. Для дальнейшего успеха требуются творческий подход, обмен информацией, инновационные правовые теории, а также сотрудничество с государственными и частными организациями.

Злоупотребление инфраструктурой киберпреступниками

Интернет-шлюзы как криминальная инфраструктура для управления

Устройства Интернета вещей (IoT) становятся популярной целью для киберпреступников, использующих широко распространенные ботнеты. Если на маршрутизаторах не установлены последние исправления и они доступны непосредственно из Интернета, злоумышленники могут воспользоваться ими для доступа к сетям, проведения атак и поддержки других своих операций.

Команда Microsoft Defender для Интернета вещей исследует различное оборудование — от устаревших контроллеров промышленных систем управления до современных датчиков IoT. Специалисты анализируют вредоносные программы, нацеленные на IoT и операционных технологии, чтобы внести свой вклад в составление общего списка индикаторов компрометации.

Маршрутизаторы особенно уязвимы для атак, так как они широко используются как дома, так и в офисах, подключенных к Интернету. Мы отслеживаем активность маршрутизаторов MikroTik — популярных во всем мире моделей для бытового и коммерческого использования, — определяя, как они используются для управления операциями киберпреступников, атак на систему доменных имен (DNS) и захвата оборудования для майнинга криптовалют.

В частности, мы обнаружили, как операторы Trickbot используют скомпрометированные маршрутизаторы MikroTik и перенастраивают их для работы в качестве части своей инфраструктуры управления. Популярность этих устройств усугубляет серьезность злоупотреблений ими со стороны Trickbot, а их уникальное аппаратное и программное обеспечение позволяет злоумышленникам обходить традиционные меры безопасности, расширять инфраструктуру и компрометировать все больше устройств и сетей.



Уязвимые маршрутизаторы подвержены риску использования потенциальных уязвимостей.

Отслеживая и анализируя трафик, содержащий команды Secure Shell (SSH), мы наблюдали, как злоумышленники использовали маршрутизаторы MikroTik для взаимодействия с инфраструктурой Trickbot после получения подлинных учетных данных для этих устройств. Они могли быть получены с помощью атак методом перебора, использования известных уязвимостей, для которых доступны исправления, и паролей по умолчанию. После доступа к устройству злоумышленник выполняет уникальную команду, которая перенаправляет трафик между 2 портами в маршрутизаторе, создавая линию связи

Цепочка атак Trickbot



Цепочка атак Trickbot, в которой показано использование IoT-устройств MikroTik в качестве прокси-серверов для центра управления.

между устройствами, затронутыми Trickbot, и центром управления.

Мы объединили полученные знания о различных методах атаки на устройства MikroTik, не только для Trickbot, а также известных общих уязвимостях и эксплойтов (CVE) в инструменте с открытым исходным кодом для устройств MikroTik, который может извлекать криминалистические артефакты, связанные с атаками на эти устройства³¹.

Устройства, работающие как обратные прокси-серверы для центров управления киберпреступников, существуют не только

для ботнета Trickbot и маршрутизаторов MikroTik. Вместе с командой Microsoft RiskIQ мы проследили путь до центра управления и наблюдали за SSL-сертификатами, что позволило выявить устройства Ubiquiti и LigoWave, которые также пострадали от этих атак³². Это верный признак того, что устройства Интернета вещей становятся активными компонентами скоординированных атак на национальном уровне и популярной целью для киберпреступников, использующих широко распространенные ботнеты.

Эксплуатация устройств Интернета вещей криптопреступниками

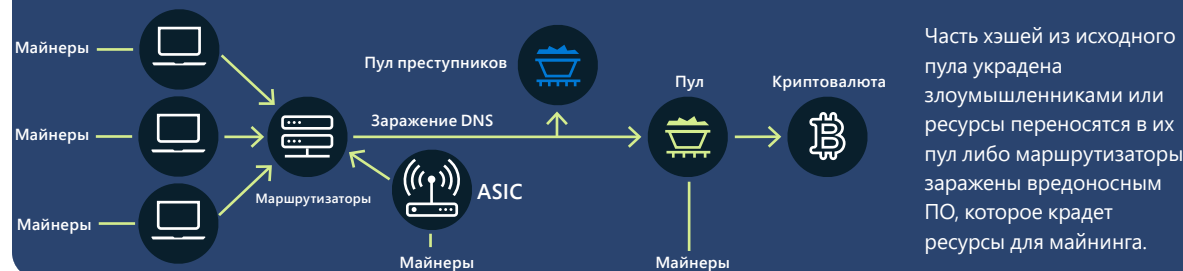
Аппаратные шлюзы становятся ценной целью для злоумышленников, так как число известных уязвимостей из года в год непрерывно растет. Они используются для майнинга криптовалют и других вредоносных операций.

Популярность криптовалют значительно выросла, и многие люди и организации выделили свои вычислительные и сетевые ресурсы таких устройств, как маршрутизаторы, для майнинга криптовалют в блокчейне. Однако это длительный и ресурсоемкий процесс с низкой вероятностью успеха. Чтобы повысить вероятность успеха, майнеры объединяются в распределенные, кооперативные сети, получая хэши, связанные с процентом монеты, которую они успешно добыли, с помощью подключенных ресурсов.

В прошлом году корпорация Microsoft обнаружила растущее число атак с эксплуатацией маршрутизаторов для перенаправления ресурсов на майнинг криптовалюты. Киберпреступники взламывают маршрутизаторы, подключенные к майнинговым пулам, и перенаправляют майнинг-трафик на связанные с ними IP-адреса с посредством отравления DNS-сервера, который изменяет параметры DNS целевых устройств. Затронутые маршрутизаторы регистрируют неверный IP-адрес для доменного имени, отправляя свои майнинг-ресурсы (или хэши) в пулы, используемые злоумышленниками. Эти пулы могут добывать анонимные монеты, связанные с преступной деятельностью, или использовать подлинные хэши, генерируемые майнерами, чтобы получить процент от добытых монеты, получая все плоды усилий майнеров.

Для половины известных уязвимостей, обнаруженных в 2021 году, нет доступных исправлений, поэтому обновление и защита маршрутизаторов в корпоративных и частных сетях остается серьезной проблемой для владельцев устройств и администраторов.

Взлом устройств для незаконного криптомайнинга.



Отравление DNS-сервера аппаратных шлюзов ставит под угрозу майнинг добропорядочных пользователей и перенаправляет ресурсы криптопреступникам.

Виртуальные машины как криминальная инфраструктура

Широко распространенный переход на облачные платформы затронул и киберпреступников, которые используют частные ресурсы невольных жертв, полученные с помощью фишинга или вредоносных программ, крадущих учетные данные. Многие киберпреступники предпочитают настраивать вредоносные инфраструктуры на облачных виртуальных машинах (VM), в контейнерах и микросервисах.

Когда киберпреступники получают доступ к системе, может произойти последовательность операций настройки инфраструктуры, например создание ряда VM с помощью скриптов и автоматизированных процессов. Эти процессы используются для выполнения вредоносных действий, таких как крупномасштабные спам-атаки по электронной почте, фишинговые кампании и веб-страницы с вредоносным контентом. Они даже могут включать в себя настройку масштабированной виртуальной среды для майнинга криптовалюты, в результате чего конечная жертва получает в конце месяца счет на сотни тысяч долларов.

Киберпреступники понимают, что время, в течение которого их вредоносные действия не будут обнаружены и заблокированы, ограничено. Поэтому они перешли на новый уровень и теперь учитывают непредвиденные обстоятельства. Мы видели, что они заранее готовят скомпрометированные учетные записи и следят за целевыми средами. Когда взломанную учетную запись (подготовленную с использованием сотен тысяч VM) обнаруживают, они переходят

к следующей учетной записи, уже подготовленной скриптами к немедленной активации, и их вредоносные действия продолжают практически без простоя.

Локальная инфраструктура, как и облачная инфраструктура, может использоваться в атаках с виртуальными локальными средами, которые неизвестны локальному пользователю. Для этого необходимо, чтобы первоначальная точка доступа была открытой и доступной. Киберпреступники также использовали частные локальные ресурсы для настройки дальнейшей цепочки облачной инфраструктуры, созданной для запутывания происхождения, чтобы избежать обнаружения создания подозрительной инфраструктуры.

Практические рекомендации

- 1 Внедрите эффективные принципы киберпрофилактики и организуйте обучение мерам кибербезопасности для сотрудников под руководством инструктора, чтобы они не попались на атаки с использованием социальной инженерии.
- 2 Регулярно проводите автоматизированные проверки аномального поведения пользователей с помощью масштабных обнаружений, чтобы сократить число этих атак.
- 3 Обновляйте и защищайте маршрутизаторы в корпоративных и частных сетях.

Хактивисты с нами надолго?

Хактивисты — это отнюдь не новое явление, но война в Украине привела к появлению множества хакеро-добровольцев, в том числе тех, кто был направлен правительствами на развертывание киберинструментов для нанесения ущерба репутации или ресурсам политических оппонентов, организаций и даже государств.

В феврале 2022 года украинское правительство призвало частных лиц по всему миру проводить кибератаки на Россию как часть их 300-тысячной «ИТ-армии»³³. В то же время созданные хактивистские группы, такие как Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans и RaidForum2 начали выполнять атаки в поддержку Украины. Другие группы, в том числе некоторые из числа создателей программы-шантажиста Conti, встали на сторону России³⁴.

В последующие месяцы действия группы Anonymous были очень заметны. Хакеры, действующие от ее имени (или от имени одного из ее партнеров) временно отключили тысячи российских и белорусских веб-сайтов, слили сотни гигабайт украденных данных, взломали российские телеканалы для показа проукраинского контента и даже предложили заплатить криптовалютой за сданные российские танки.

Рост числа гражданских хакеров

Социальные сети позволили быстро организовать и мобилизовать тысячи потенциальных гражданских хакеров, которые получили инструкции для проведения простых атак, таких как DDoS-атаки. Организаторы использовали Twitter, Telegram и частные форумы для объединения хакеров, координации операций и распространения инструкций по взлому.

Однако навыки большинства таких хакеров ограничены — даже с инструкциями. Поэтому в будущем возможны 2 варианта: 1) сотни или тысячи людей с базовыми техническими навыками используют шаблоны для проведения скоординированных или индивидуальных атак хактивистов на цели; 2) возможное окончание военных действий в Украине приведет к тому, что они оставят хактивизм позади, по крайней мере, до тех пор пока следующая политическая или социальная проблема не вдохновит их на действия.

Политизация хакеров

Повышенный риск, связанный с такой политической мобилизацией, состоит в развертывании технически подкованных хакеров, которые могут проводить кибератаки против целей иностранных правительств для поддержки собственных национальных приоритетов, — либо добровольно, либо по приказу своего правительства.

Иран, Китай и Россия уже используют хактивизм для вербовки в государственные хакерские группы. Например, в апреле 2022 года пророссийская хакерская группа Killnet провела DDoS-атаки на чешские железные дороги, региональные аэропорты и сервер государственной службы Чехии, хотя Чехия

напрямую не участвует в войне³⁵. В то же время некоторые правительства могут использовать хактивизм как прикрытие традиционного кибершпионажа или диверсионных операций, например иранских операций против Израиля.

В условиях участвовавших DDoS-атак, связанных с хактивизмом, технологическая отрасль должна быстро определять разницу между нормальным и ненормальным потоком трафика на веб-сайт. Корпорация Microsoft вместе с партнерами разработала набор инструментов, которые отличают вредоносный DDoS-трафик и отслеживают его происхождение. Кроме того, платформа Microsoft Azure может выявлять в своей среде компьютеры со слишком большим объемом исходящего трафика и отключать их.

Появление протестных программ

Протестные программы стали прямым результатом эмоциональной реакции на войну Россией и Украины. Некоторые разработчики ПО с открытым исходным кодом использовали популярность своих решений как средство высказать свое мнение или принять меры против этой геополитической ситуации. Например, на рабочем столе или в браузере открывались безвредные текстовые файлы для распространения призывов к миру. Но активисты также проводили целевые атаки на основе геолокации IP-адресов и выполняли разрушительные операции, такие как очистка жесткого диска. По мере развития других международных событий можно ожидать, что протестные программы снова проявятся в будущем. Так как чаще всего уважаемые разработчики ПО с открытым исходным кодом решают делать личные заявления, используя собственные компоненты, то на данный

момент нет никакого способа предотвратить такие изменения в пакетах исходных файлов, и пользователи должны быть в курсе потенциальных последствий.

Социальные сети позволили организовать и мобилизовать тысячи потенциальных гражданских хакеров, которые получили инструкции для проведения простых атак, таких как DDoS-атаки.

Практические рекомендации

- 1 Технологическая отрасль должна объединиться, чтобы разработать комплексные меры реагирования на эту новую угрозу.
- 2 Ведущие технологические компании, в том числе корпорация Microsoft, обладают инструментами для обнаружения вредоносного трафика, связанного с DDoS-атаками, и отключения виртуальных машин.
- 3 Пользователи ПО с открытым исходным кодом должны внимательно следить за происходящим во время геополитических кризисов.

Концевые сноски

1. <https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/>
2. <https://www.bleepingcomputer.com/news/security/greeces-public-postal-service-offline-due-to-ransomware-attack/>
3. <https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/>; <https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/>
4. <https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/>
5. <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>
6. Обнаружение и нейтрализации атак на конечные точки. <https://www.microsoft.com/en-us/security/business/threat-protection/>
7. https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html
8. <https://www.bbc.com/news/technology-59998925>
9. Vetted Forum — это дискуссионный веб-форум, для регистрации на котором текущий участник должен поручиться за нового.
10. <https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/>; <https://www.blockchain.com/charts/my-wallet-n-users>; <https://coinmarketcap.com>
11. <https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/>
12. <https://www.coindesk.com/business/2021/12/13/crypto-exchange-ascendex-hacked-losses-estimated-at-77m/>; <https://www.zdnet.com/article/after-77-million-hack-crypto-platform-ascendex-to-reimburse-customers/>
13. <https://etherscan.io/address/0x73326b6764187b7176ed3c00109ddc1e6264eb8b>
14. <https://finance.yahoo.com/news/ethereum-worth-over-1-5m-160249300.html>
15. <https://news.bitcoin.com/decentralized-finance-crypto-exchange-uniswap-starts-blocking-addresses-linked-to-blocked-activities/>
16. Источник данных: Defender для Office (вредоносные письма/скомпрометированное удостоверение), сервис «Защита идентификации Azure Active Directory» (события и оповещения о скомпрометированных удостоверениях), Defender для облачных приложений (события доступа к данным скомпрометированных удостоверений) и M365D (корреляция между продуктами).
17. Источник данных: Defender для конечной точки (оповещения/события, связанные с поведением при атаке), Defender для Office (вредоносные письма) и M365D (корреляция между продуктами).
18. <https://www.ic3.gov/Media/Y2022/PSA220504>
19. Domain-based Message Authentication, Reporting and Conformance (DMARC): протокол аутентификации, политики и отчетности для электронной почты, предоставляющий владельцам доменов электронной почты возможность защитить домен от несанкционированного использования.
20. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
21. <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/learn-about-spoof-intelligence?view=o365-worldwide>
22. <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/impersonation-insight?view=o365-worldwide>
23. <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview>
24. <https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365>
25. <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview>
26. Microsoft Corporation v. John Does 1-27, et. al., No. 1:10CV156, (E.D.Va. 22 февраля 2010 г.).
27. See Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 27 сентября 2011 г.
28. В частности, правило 65 Федеральных правил гражданского судопроизводства позволяет стороне добиваться такого средства правовой защиты, если: 1) стороне будет причинен немедленный и непоправимый ущерб, если защита не будет предоставлена, и 2) сторона попытается своевременно уведомить другую сторону. Кроме того, по закону требуется применять критерия балансировки, который уравнивает право ответчика на получение уведомления с объемом ущерба причиненного обществу.
29. Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D. Wa. 9 февраля 2011 г.).
30. Microsoft Corp. v. Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. 12 августа 2021 г.).
31. <https://github.com/microsoft/routeros-scanner>
32. RiskIQ: Ubiquiti Devices Compromised and Used as Malware C2 Reverse Proxies | RiskIQ Community Edition
33. <https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army>
34. <https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/>
35. <https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks>

Угрозы национального уровня

Злоумышленники национального уровня проводят изощренные кибератаки, чтобы избежать обнаружения, для продвижения своих стратегических приоритетов.

Обзор угроз национального уровня	31
Введение	32
Справочная информация о данных об угрозах национального уровня	33
Пример кибергрупп национального уровня и их деятельности	34
Развивающаяся среда угроз	35
Цепочка поставок ИТ как шлюз в цифровую экосистему	37
Быстрая эксплуатация уязвимостей	39
Кибертактика российских государственных кибергрупп военного времени угрожает Украине и другим странам	41
Китай расширяет глобальные операции для получения конкурентного преимущества	44
Иран становится агрессивнее после смены правительства	46
Возможности северокорейских кибергрупп, используемые для достижения 3 основных целей режима	49
Кибернаемники угрожают стабильности киберпространства	52
Введение в действие норм кибербезопасности в интересах мира и безопасности в киберпространстве	53

Обзор

угроз национального
уровня

Злоумышленники национального уровня проводят изощренные кибератаки, чтобы избежать обнаружения, для продвижения своих стратегических приоритетов. Появление кибероружия в гибридной войне в Украине символизирует рассвет новой эпохи конфликтов.

Россия также поддерживает войну операциями информационного влияния, используя пропаганду для воздействия на общественное мнение в России, Украине и во всем мире. Этот первый полномасштабный гибридный конфликт преподал нам и другие важные уроки. Во-первых, безопасность цифровых операций и данных (как в киберпространстве, так и в физическом пространстве) можно максимально эффективно обеспечить за счет перехода в облако. Первые атаки с российской стороны были нацелены на локальные сервисы (использовалось вредоносное ПО, удаляющее данные), а одна из первых запущенных ракет была нацелена на физические центры обработки данных.

Украина быстро перенесла рабочие нагрузки и данные в гипермасштабируемые облака, размещенные в центрах обработки данных за пределами страны. Во-вторых, достижения в области анализа киберугроз и защиты конечных точек на основе данных и передовых облачных сервисов ИИ и машинного обучения помогли Украине защититься от российских кибератак.

В других областях субъекты национального уровня усилили активность и используют достижения в сфере автоматизации, облачной инфраструктуры и технологий удаленного доступа для атаки на широкий спектр целей. Корпоративные цепочки поставок ИТ, которые могут предоставить доступ к конечным целям, часто были целью атак. Киберпрофилактика стала еще важнее, так как злоумышленники быстро использовали неисправленные уязвимости, как сложные методы, так и методы прямого перебора для кражи учетных данных и скрывали свои операции с помощью ПО открытого исходного кода или подлинного ПО. Кроме того, Иран, как и Россия, начал использовать разрушительное кибероружие, в том числе программы-шантажисты, в качестве основного метода атак.

В результате необходимо срочно внедрить согласованную международную платформу, которая отдает приоритет правам человека и защищает людей от безрассудного поведения государств в Интернете. Все страны должны совместно работать над внедрением согласованных норм и правил ответственного поведения государств.

» «Защита Украины: первые уроки кибервойны», Microsoft On the Issues

Усиленное внимание критически важной инфраструктуре, в частности, ИТ-сфере, финансовым услугам, транспортным системам и инфраструктуре связи.

» Подробнее на стр. 35

ИТ-цепочка поставок используется как ворота для доступа к целевым объектам.

NOBELIUM

» Подробнее на стр. 36

Китай расширяет глобальные операции, выбирая в качестве цели небольшие страны Юго-Восточной Азии, для сбора разведанных и получения конкурентного преимущества.

» Подробнее на стр. 44

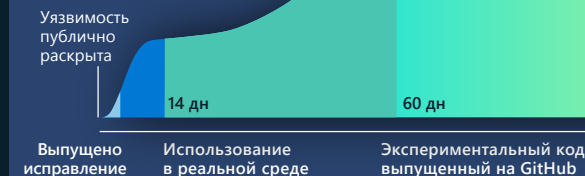
Кибернаемники угрожают стабильности киберпространства — эта растущая индустрия из частных компаний разрабатывает и продает расширенные инструменты, методы и сервисы, позволяющие клиентам (часто правительствам) проникать в сети и устройства.

» Подробнее на стр. 52

Иран становится агрессивнее после смены правительства, расширяя атаки программ-шантажистов за пределы региональных противников на США и ЕС, а также нацеливаясь на критически важную инфраструктуру США.

» Подробнее на стр. 46

Выявление и быстрое использование неисправленных уязвимостей стало ключевой тактикой злоумышленников. Для защиты от них требуется быстрое развертывание обновлений системы безопасности.



» Подробнее на стр. 39

Северная Корея нацелилась на оборонные и аэрокосмические компании, криптовалюты, новостные агентства, перебежчиков и организации по оказанию гуманитарной помощи для достижения следующих целей режима: выстраивание обороны, укрепление экономики и поддержка внутренней стабильности.

» Подробнее на стр. 49

Введение

После громких атак в 2020 и 2021 годах кибергруппы национального уровня выделили значительные ресурсы на адаптацию к новым средствам безопасности, реализованным организациями для защиты от сложных угроз.

Как и крупные предприятия, злоумышленники начали использовать достижения в сфере автоматизации, облачной инфраструктуры и технологий удаленного доступа, чтобы расширить цели своих атак. Подобные тактические корректировки привели к появлению новых подходов и крупномасштабным атакам на корпоративные цепочки поставок. Профилактика ИТ-безопасности стала еще важнее, так как хакеры разрабатывали новые способы быстрого использования неисправленных уязвимостей, расширяли методы компрометации корпоративных сетей и скрывали свои операции с помощью ПО с открытым исходным кодом или подлинного коммерческого ПО. Новые методы атаки создали новые, трудные для обнаружения векторы для доступа к сети цели. Наконец, во время войны наблюдается эскалация физических атак — мы увидели, что кибератаки играют важную роль в военных операциях.

Конфликт в Украине стал слишком очевидным примером того, как кибератаки видоизменяются, чтобы влиять на мир параллельно с военным конфликтом. Энергетические и телекоммуникационные системы, средства массовой информации и другая критическая инфраструктура стали целями как физических атак, так и кибератак. Попытки взлома сети, характерные для шпионажа и кампаний по извлечению информации, сосредоточились на гибридной войне с разрушительными атаками вредоносного ПО на критически важные инфраструктурные системы. Подключение системы безопасности этих решений к облаку позволило заранее обнаруживать потенциально разрушительные атаки и срывать их¹.

Впервые в рамках масштабной кибератаки средства обнаружения аномального поведения, использующие машинное обучение, применяли известные шаблоны атак для успешного выявления и предотвращения дальнейших атак без предварительных данных о базовом вредоносном ПО — еще до того, как кто-то узнал о таких угрозах. Мы также убедились в ценности обмена информацией об угрозах в реальном времени со специалистами по безопасности, защищающими эти системы, которая позволяет получать критически важные сведения для прогнозирования и защиты от активных атак.

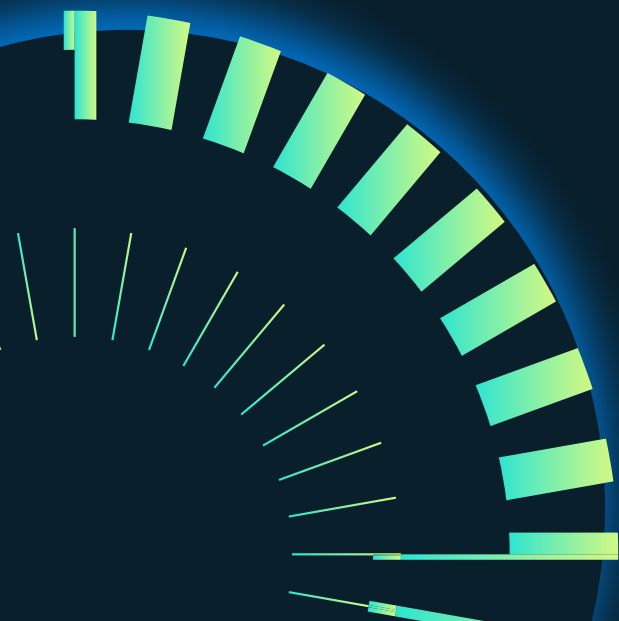
Кибергруппы национального уровня по всему миру продолжают расширять свои операции, используя как новые, так и старые методы. И Китай, и Северная Корея, и Иран, и Россия проводили атаки на клиентов Microsoft. Цепочка поставок ИТ-сервисов стала общей целью для них, так как злоумышленники сместили акцент на базовые сервисы, которые могут стать точкой доступа в несколько организаций. Мы ожидаем, что они и далее будут использовать доверительные отношения в корпоративных цепочках поставок, что подчеркивает важность комплексного применения правил аутентификации, надлежащей установки исправлений и настройки учетных записей для инфраструктуры удаленного доступа, а также регулярного аудита партнерских отношений для подтверждения надежности.

Кибергруппы национального уровня, как и создатели программ-шантажистов и другие киберпреступники, отреагировали на новые уязвимости, направив свои усилия на плохо настроенные или необновленные корпоративные системы (инфраструктура VPN/VPS, локальные серверы, стороннее ПО) для использования публичных инструментов для проведения атак. Многие стали использовать готовое вредоносное ПО и инструменты с открытым исходным кодом, чтобы скрыть следы своей деятельности.

В результате поддержание надежного базового уровня киберпрофилактики за счет приоритетной установки исправлений, включения защиты от несанкционированного доступа, использования инструментов управления возможными направлениями атаки, таких как RiskIQ, для анализа и реализации многофакторной аутентификации во всей организации стали основами для активной защиты от многих изоциренных злоумышленников.

Кибергруппы национального уровня также расширили использование программ-шантажистов в своих атаках, часто повторно применяя вредоносное ПО, созданное экосистемой киберпреступников. Мы наблюдали, как иранские и северокорейские кибергруппы использовали готовые программы-шантажисты для нанесения ущерба целевым системам региональных конкурентов, часто включающим в себя критическую инфраструктуру. Наконец, мы видим растущую угрозу от кибернаемников, создающих и продающих инструменты, методы и сервисы для расширения применения эксплойтов против уязвимых сторонних решений. Сложность и гибкость атак со стороны кибергрупп национального уровня будут расти с каждым годом. Организации должны реагировать на это, получая сведения об этих изменениях и параллельно развивая средства защиты.

Джон Ламберт (John Lambert)
Корпоративный вице-президент
и выдающийся инженер, Microsoft Threat
Intelligence Center



Справочная информация о данных об угрозах национального уровня

Угрозы национального уровня — это кибероперации, которые исходят из конкретной страны и явно связаны с национальными интересами.

Угрозы национального уровня представляют собой одни из самых продвинутых и постоянно активных видов угроз, с которыми сталкиваются наши клиенты, включая кражу интеллектуальной собственности, шпионаж, слежку, кражу учетных данных, разрушительные атаки и многое другое.

Мы инвестируем значительные ресурсы в обнаружение, анализ этих угроз и противодействие им. Когда организация или владелец учетной записи становятся целью или их взламывают кибергруппы национального уровня, корпорация Microsoft отправляет уведомление о национальной угрозе (NSN) напрямую клиенту, включая в него сведения, необходимые для расследования. По состоянию на июнь 2022 года мы отправили больше 67 000 NSN, с тех пор как они появились в 2018 году.

Данные оповещений NSN корпорации Microsoft представлены в этой главе, чтобы организации могли оценивать подобные угрозы. Уровень активности иностранных государств, показанный на диаграммах, основан на числе NSN, отправленных корпорацией Microsoft клиентам в ответ на обнаружение кибергрупп национального уровня, нацеленных или компрометирующих по крайней мере одну учетную запись в организации клиента.



4 основными иностранными государствами, кибергруппы которых мы включаем в этот отчет, являются Россия, Китай, Иран и Северная Корея. Это страны-источники чаще всего наблюдаемых кибергрупп, ориентированных на клиентов Microsoft за последний год. В отчете также представлены наши наблюдения о кибергруппах из Ливана и кибернаемниках или хакерах, работающих в частном секторе по найму.

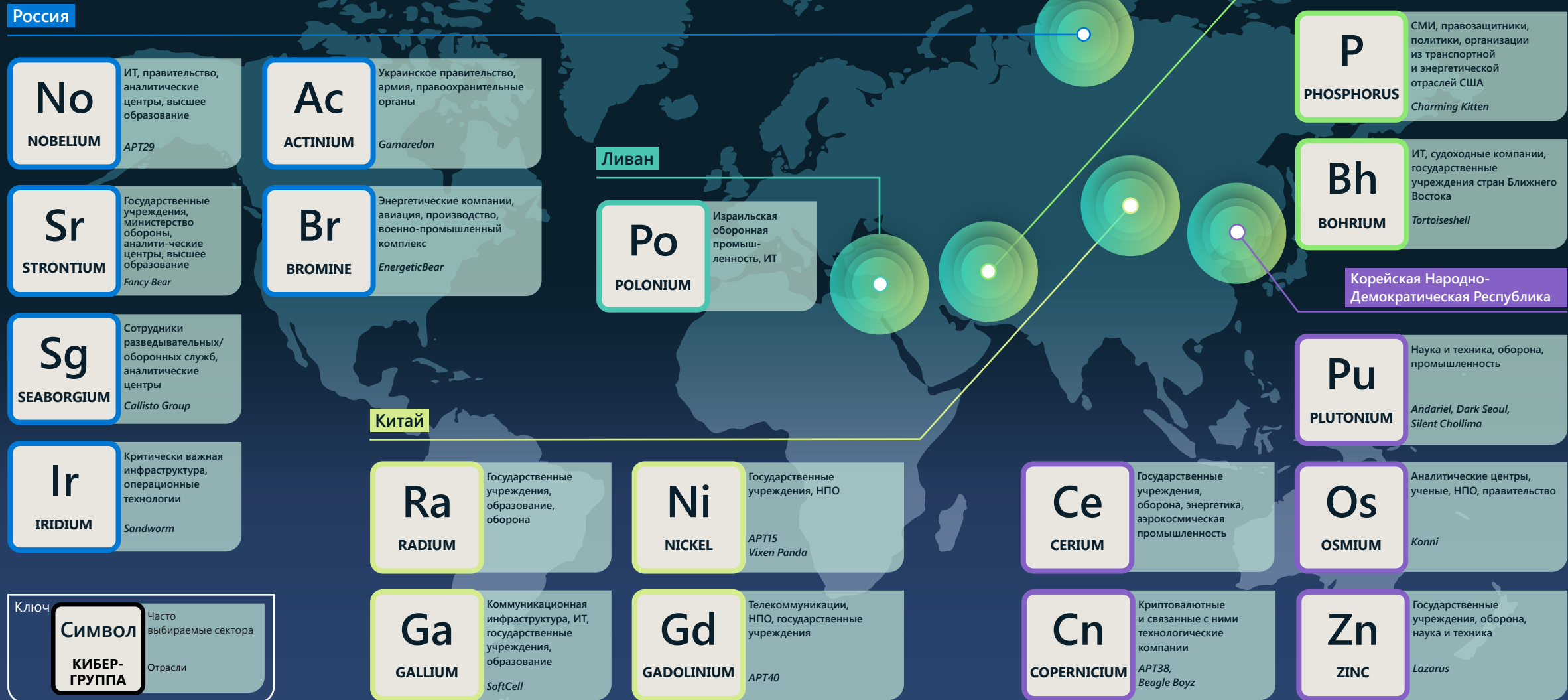
Корпорация Microsoft обозначает кибергруппы иностранных государств названиями химических элементов (например, NOBELIUM) — некоторые

из них показаны на следующей странице. Мы используем обозначения DEV-#### в качестве временного названия, данного неизвестному, появляющемуся или развивающемуся кластеру угроз, что позволяет отслеживать его как уникальный набор информации, пока мы не достигнем высокой степени уверенности в происхождении или личности субъекта, стоящего за действием.

Когда субъект DEV соответствует критериям, он преобразуется в именованного субъекта или объединяется с существующими. На протяжении

всей этой главы мы приводим примеры кибергрупп иностранных государств и групп DEV, чтобы получить глубокое представление о целях атаки, методах и анализе мотиваций. Хотя многие из этих групп используют те же инструменты, что и киберпреступники, они создают уникальные угрозы из-за специального вредоносного ПО, способности обнаруживать и извлекать выгоду из уязвимостей нулевого дня и юридической безнаказанности.

Пример кибергрупп национального уровня и их деятельности



Развивающаяся среда угроз

Стремление корпорации Microsoft к отслеживанию действий кибергрупп национального уровня и уведомлению клиентов, если мы видим, что они стали целью или были скомпрометированы, лежит в основе нашей миссии по защите клиентов от атак.

Такое уведомление — важная часть нашего обязательства сообщать клиентам о том, успешно ли предотвращаются наблюдаемые атаки с помощью наших средств защиты или же атаки оказались эффективны из-за неизвестных уязвимостей. Отслеживание уведомлений с течением времени помогает Microsoft выявлять меняющиеся тенденции угроз со стороны злоумышленников и выделять больше средств защиты на упреждающее устранение угроз для клиентов наших облачных сервисов.

Такое отслеживание также позволяет обмениваться данными и идеями о том, что мы видим. Аналитики, отслеживающие этих злоумышленников и следящие за их атаками, полагаются на сочетание технических индикаторов и геополитического опыта, чтобы понять мотивы, объединяя технический и глобальный контекст в новые выводы. Это дает уникальный взгляд на приоритеты кибергрупп национального уровня и на то, как их мотивация может зависеть от политических, военных и экономических государств, использующих их.

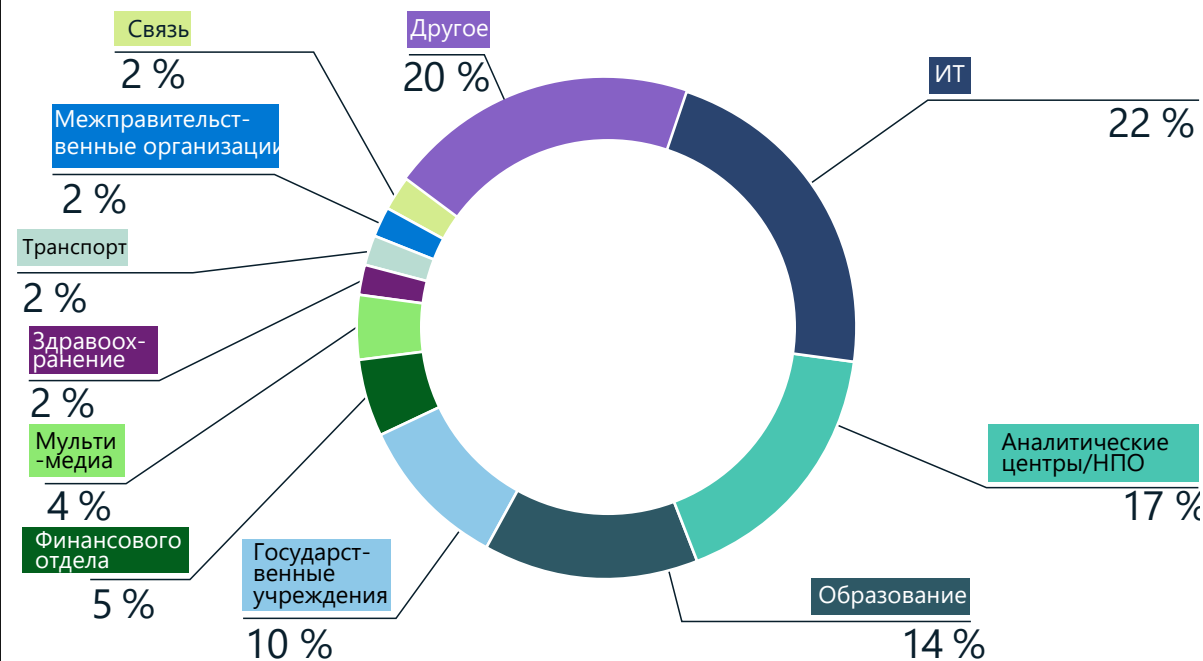
Политические события прошлого года определили приоритеты и допустимые риски спонсируемых государством кибергрупп во всем мире. По мере ухудшения геополитических отношений разрушаются, а «ястребы» получают больший контроль в некоторых странах, кибергруппы стали наглее и агрессивнее. Например:

- Россия непрерывно проводила атаки против украинского правительства и критически важной инфраструктуры страны, дополняя военные операции².
- Иран агрессивно стремился проникнуть в критически важную инфраструктуру США, такую как администрация транспортных центров.
- Северная Корея продолжила попытки кражи криптовалюты у финансовых и технологических компаний.
- Китай расширил глобальные операции кибершпионажа.

Хотя кибергруппы национального уровня могут быть хорошо технически оснащены и могут использовать широкий спектр тактик, их атаки часто можно предотвратить с помощью эффективной киберпрофилактики. Многие из этих злоумышленников полагаются на относительно низкотехнологичные средства, такие как целевые фишинговые письма, для доставки сложных вредоносных программ вместо разработки специализированных эксплойтов или использования целевой социальной инженерии для достижения своих целей.

Угрозы национального уровня

Отраслевые секторы, на которые нацелены кибергруппы национального уровня



Кибергруппы национального уровня были ориентированы на целый ряд секторов. Российские и иранские кибергруппы нацелились на ИТ-отрасль как средство доступа к клиентам ИТ-компаний. Аналитические центры, неправительственные организации (НПО), университеты и государственные учреждения были другими общими целями таких злоумышленников.

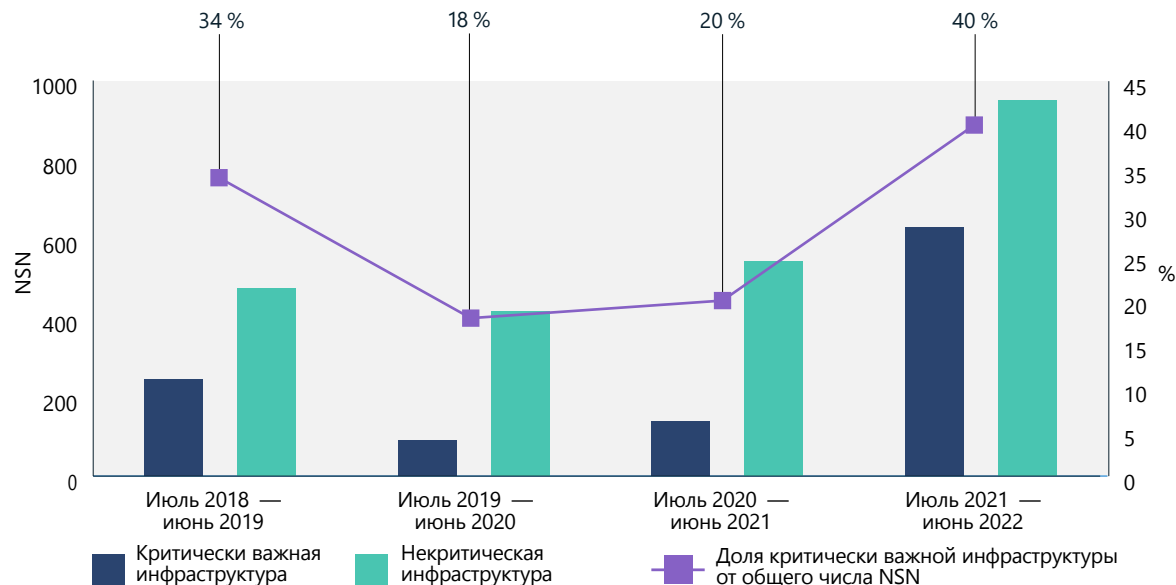
Их у кибергрупп может быть много, поэтому они могут выбирать в качестве жертвы конкретные группы организаций или отдельных лиц. В прошлом году количество атак на цепочки поставок выросло, и особый акцент был сделан на ИТ-компании. Взламывая системы поставщиков ИТ-сервисов, злоумышленники часто могут добиться первоначальной цели за счет доверительных отношений с компанией, которая управляет

подключенными системами, или могут расширить масштаб атаки, скомпрометировав сотни клиентов за одну попытку. После ИТ-сектора самыми популярными у злоумышленников целевыми организациями были аналитические центры, ученые при университетах и правительственные чиновники. Это желательные «мягкие цели» для шпионажа с целью сбора разведанных по геополитическим вопросам.

Развивающаяся среда угроз

Продолжение

Тенденции, связанные с критически важной инфраструктурой



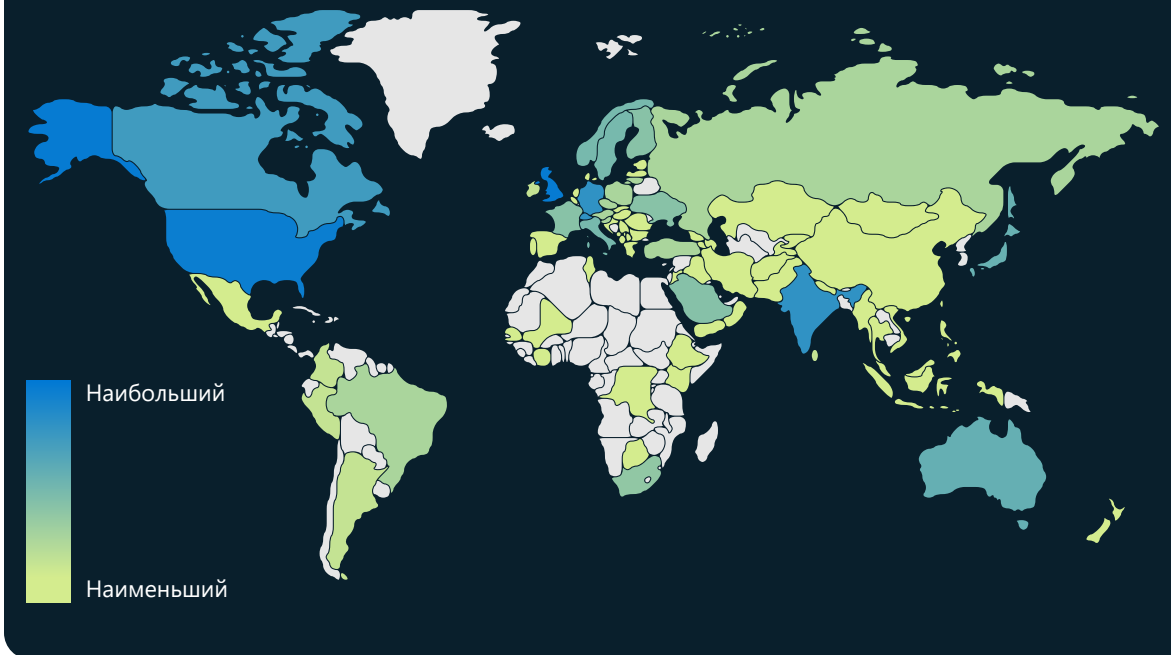
Кибергруппы национального уровня в прошлом году стали чаще выбирать критически важную инфраструктуру³, при этом они сосредоточились на компаниях из ИТ-сектора, финансовой индустрии услуг, транспортных системах и инфраструктуре связи.

«До вторжения в Украину правительства думали, что данные должны оставаться внутри страны, чтобы им ничего не угрожало. После вторжения миграция данных в облако и их перенос за пределы территориальных границ стали частью планирования устойчивости и надлежащего управления».

Кристин Флинн Гудвин (Cristin Flynn Goodwin),

заместитель генерального юрисконсульта, подразделение безопасности клиентов и доверия

Географический выбор целей кибергруппами национального уровня



В прошлом году кибергруппы национального уровня выбирали цели по всему миру с особенно сильным акцентом на американские и британские предприятия. Организации из Израиля, ОАЭ, Канады, Германии, Индии, Швейцарии и Японии также были одними из наиболее часто атакуемых, согласно данным NSN.

Практические рекомендации

- 1 Определите и защитите потенциальные ценные цели в области данных, технологий, информации и бизнес-операций, подверженные риску, которые могут соответствовать стратегическим приоритетам кибергрупп национального уровня.
- 2 Используйте облачные инструменты защиты для выявления и устранения известных и новых угроз сети в любом масштабе.

Цепочка поставок ИТ как шлюз в цифровую экосистему

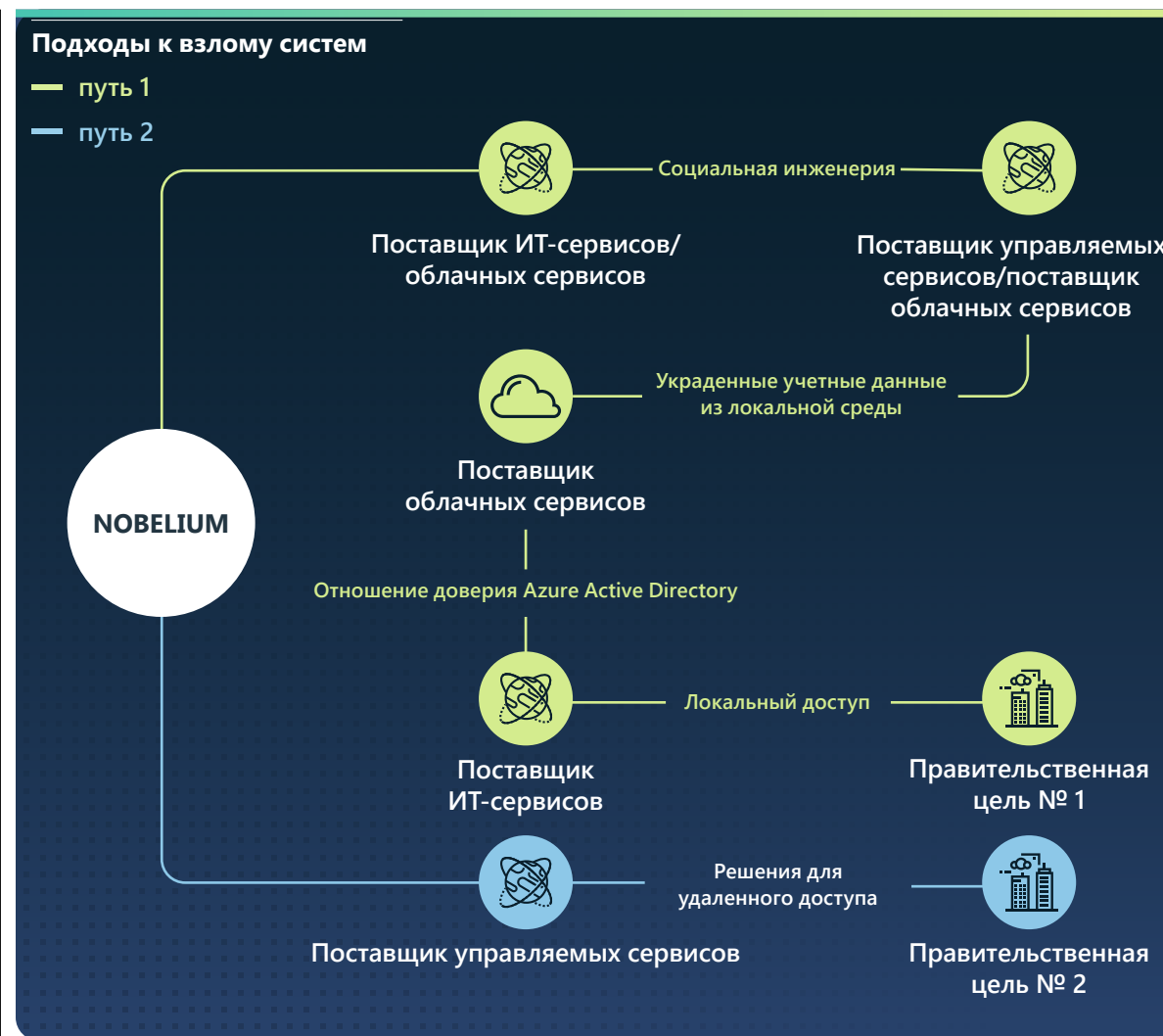
Атаки национальных кибергрупп на поставщиков ИТ-сервисов может позволить им эксплуатировать другие интересующие их организации, используя доверие и доступ, предоставленные этим поставщикам цепочек поставок. В прошлом году кибергруппы национального уровня нацелились на поставщиков ИТ-сервисов, чтобы атаковать сторонние цели и получить доступ к нижестоящим клиентам, связанным с государственными учреждениями, политическими организациями и критически важной инфраструктурой.

Поставщики ИТ-сервисы — привлекательные промежуточные цели, так как они обслуживают сотни прямых и тысячи косвенных клиентов, представляющих интерес для иностранных разведывательных служб. В случае их взлома стандартные бизнес-процессы и делегированные права администратора, которыми пользуются эти фирмы, могут позволить злоумышленникам получить доступ к сетям клиентов поставщиков ИТ-сервисов и манипулировать ими без инициации оповещений системы безопасности.

В прошлом году кибергруппа NOBELIUM попыталась скомпрометировать и использовать привилегированные учетные записи облачных решений и поставщиков других управляемых сервисов, чтобы попытаться получить доступ, в основном, к государственным учреждениям США и Европы, а также к политическим организациям.

Группа NOBELIUM показала, как подход «взломать одного значит взломать многих» можно использовать против предполагаемого геополитического противника. В прошлом году эта кибергруппа проводила как косвенные, так и прямые вторжения в важные организации из стран НАТО, которое российское правительство воспринимает как экзистенциальную угрозу. С июля 2021 года до начала июня 2022 года 48 % уведомлений клиентов Microsoft об угрозах российской деятельности в отношении клиентов онлайн-сервисов поступило ИТ-компаниям из стран НАТО — вероятно, в качестве промежуточных точек доступа. В целом, 90 % уведомлений о деятельности российских кибергрупп за тот же период поступили клиентам из стран НАТО, в первую очередь для ИТ-компаний, аналитических центров и неправительственных организаций (НПО), а также государственных учреждений. На основании этого можно предположить, что стратегию группы заключается в использовании нескольких средств первоначального доступа к целям.

Произошел переход от использования цепочки поставок ПО к использованию цепочки поставок ИТ-сервисов, при этом злоумышленники нацеливаются на поставщиков облачных решений и управляемых сервисов для получения доступа к их клиентам.



На этой диаграмме показан многовекторный подход кибергруппы NOBELIUM к взлому конечных целей и нанесению сопутствующего ущерба другим жертвам на пути. В дополнение к действиям, показанным выше, кибергруппа NOBELIUM инициировала распыление паролей и фишинговые атаки против связанных организаций, даже нацеливаясь на личный кабинет по крайней мере одного государственного служащего в качестве еще одного потенциального пути к компрометации.

Цепочка поставок ИТ как шлюз в цифровую экосистему

Продолжение

В течение года сотрудники Microsoft Threat Intelligence Center (MSTIC) обнаруживали все больше иранских государственных кибергрупп и связанных с Ираном злоумышленников, взламывающих ИТ-компании. Во многих случаях злоумышленники крали учетные данные для входа, чтобы получить доступ к клиентам жертва для достижения целого ряда целей — от сбора разведанных до ответных разрушительных атак.

- В июле и августе 2021 года кибергруппа DEV-0228 взломала систему израильского поставщика ПО для бизнеса, чтобы позже скомпрометировать клиентов в оборонном, энергетическом и юридическом секторах Израиля⁴.
- С августа по сентябрь 2021 года корпорация Microsoft обнаружила всплеск активности иранских кибергрупп, нацеленных на ИТ-компании в Индии. Отсутствие насущных геополитических проблем, которые вызвали бы такое изменение, позволяет предположить, что цель этих атак — косвенный доступ к дочерним компаниям и клиентам за пределами Индии.

- В январе 2022 года кибергруппа DEV-0198, которая, по нашему мнению, связана с правительством Ирана, взломала израильского поставщика облачных решений. По оценкам Microsoft, злоумышленники, вероятно, использовали скомпрометированные учетные данные поставщика для аутентификации в израильской логистической компании. Специалисты MSTIC наблюдали, как та же группа пыталась провести разрушительную кибератаку против логистической компании в конце того же месяца.
- В апреле 2022 года кибергруппа POLONIUM из Ливана, которая, по нашему мнению, сотрудничала с иранскими кибергруппами в области методов компрометации цепочки поставок ИТ-сервисов, взломала другую израильскую ИТ-компанию, чтобы получить доступ к израильским оборонным и юридическим организациям⁵.

Прошедший год демонстрирует, что злоумышленники, такие как NOBELIUM и DEV-0228, знают среду доверительных отношений организации лучше, чем сами организации. Эта возросшая угроза подчеркивает необходимость понимания и укрепления границ и точек входа в цифровые инфраструктуры. Кроме того, это указывает на то, что поставщикам ИТ-сервисов необходимо тщательно отслеживать собственную кибербезопасность. Например, организациям следует применить политики многофакторной проверки подлинности и условного доступа,

которые затрудняют злоумышленникам взлом привилегированных учетных записей или распространение по сети.

Тщательный анализ и аудит партнерских отношений помогает минимизировать ненужные разрешения между вашей организацией и поставщиками, а также немедленно заблокировать доступ для любых организаций, которые выглядят незнакомыми. Анализ журналов действий и просмотр доступных мер упрощает выявление аномалий, которые могут инициировать дальнейшее расследование.

**Выбор кибергруппами
национального уровня третьих
сторон позволяет эксплуатировать
чувствительные организации,
пользуясь доверием и доступом
в цепочке поставок.**

Практические рекомендации

- 1 Проводите анализ и аудит отношений между поставщиками сервисов и делегированных прав доступа, чтобы свести к минимуму ненужные разрешения. Заблокируйте доступ для любых партнеров, которые выглядят незнакомыми или еще не были проверены⁶.
- 2 Включите ведение журнала и проверяйте любые операции аутентификации для инфраструктуры удаленного доступа и виртуальных частных сетей (VPN), делая акцент на учетные записи с однофакторной аутентификацией, для подтверждения подлинности и расследования аномальных действий.
- 3 Включите MFA для всех учетных записей (в том числе учетных записей сервисов) и убедитесь, что MFA применяется для всех удаленных подключений.
- 4 Используйте решения без пароля для защиты учетных записей⁷.

Ссылки на дополнительную информацию

- > Кибергруппа NOBELIUM нацелена на получение делегированных прав администратора для проведения масштабных атак | Microsoft Threat Intelligence Center (MSTIC)
- > Иранские кибергруппы все чаще выбирают ИТ-сектор | Microsoft Threat Intelligence Center (MSTIC), подразделение цифровой безопасности Microsoft
- > Разоблачение деятельности кибергруппы POLONIUM и инфраструктуры, нацеленной на израильские организации | Microsoft Threat Intelligence Center (MSTIC)

Быстрая эксплуатация уязвимостей

По мере того как организации укрепляют кибербезопасность, национальные кибергруппы в ответ применяют новые тактики для проведения атак и уклонения от обнаружения. Выявление и эксплуатация ранее неизвестных уязвимостей, которые называют уязвимостями нулевого дня, — основная тактика таких операций.

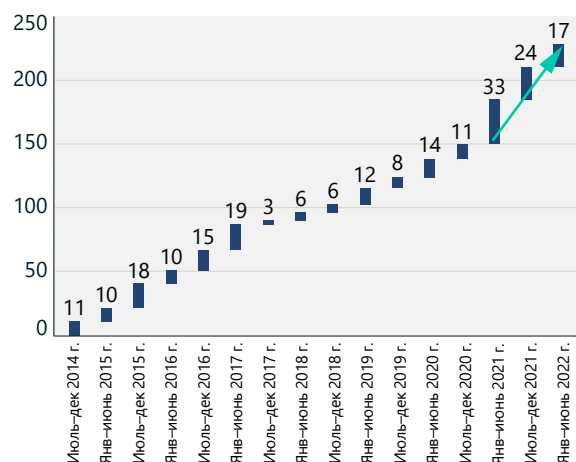
Уязвимости нулевого дня особенно эффективны для первоначального использования эксплоитов. После публичного раскрытия уязвимости могут быть быстро повторно использованы другими национальными кибергруппами и киберпреступниками. Число публично раскрытых уязвимостей нулевого дня за последний год аналогично показателю предыдущего года, который был самым высоким за всю историю наблюдений.

По мере того как злоумышленники — как национального уровня, так и киберпреступники — все лучше осваивают эти уязвимости, мы наблюдаем сокращение времени между объявлением об уязвимости и ее использованием. Поэтому организациям необходимо немедленно исправлять эксплоиты. Кроме того, крайне важно, чтобы организации или отдельные лица, которые раскрывают новые уязвимости, сообщали о них публично или уязвимым поставщикам как можно скорее в соответствии с скоординированными процедурами раскрытия уязвимостей.

Это гарантирует своевременное выявление уязвимостей и разработку исправлений для защиты клиентов от угроз, неизвестных ранее.

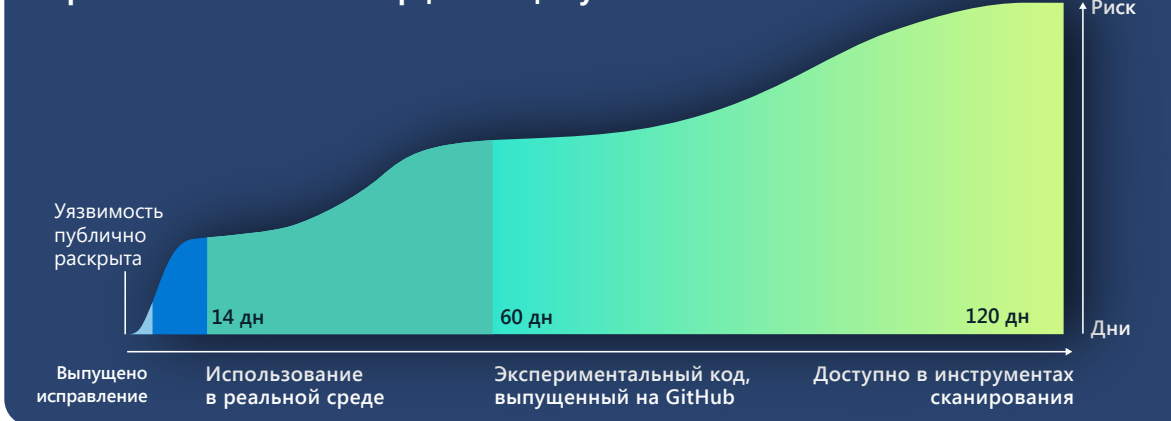
Многие организации предполагают, что у них мало шансов стать жертвами атак нулевого дня, если управление уязвимостями встроено в систему сетевой безопасности. Однако коммерциализация эксплоитов приводит к тому, что их используют гораздо быстрее. Эксплоиты нулевого дня часто обнаруживают другие злоумышленники и широко используются в течение короткого периода времени, оставляя под угрозой системы без установленных исправлений. Несмотря на то, что эксплоит нулевого дня может быть трудно обнаружить, действия злоумышленников после его использования часто легче обнаружить. Если же их источник — ПО с последними исправлениями, это может служить признаком компрометации.

Исправления, выпущенные для уязвимостей нулевого дня



Число публично раскрытых эксплоитов нулевого дня из списка распространенных уязвимостей и рисков (CVE).

Скорость и масштабы коммерциализации уязвимостей



В среднем требуется всего 14 дней, чтобы эксплоит стал доступен в экосистеме киберпреступников после публичного раскрытия уязвимости. На этом графике представлен анализ сроков использования уязвимостей нулевого дня, а также число систем, уязвимых для этих эксплоитов и активных в Интернете после первого публичного раскрытия.

Атаки с использованием уязвимостей нулевого дня обычно сперва нацелены на ограниченный набор организаций, но их быстро внедряют в масштабную экосистему злоумышленников. После этого среди них начинается своего рода соревнование в попытке использовать уязвимость как можно шире, прежде чем потенциальные жертвы установят исправления.

Мы наблюдаем, как многие кибергруппы национального уровня разрабатывают эксплоиты на основе неизвестных уязвимостей, но кибергруппы из Китая особенно искусны в обнаружении и разработке эксплоитов нулевого дня. Китайские нормативные требования к информированию об уязвимостях вступили

в силу в сентябре 2021 года — впервые в мире правительство потребовало сообщать об уязвимостях государственному органу, до того как о уязвимости будет извещен владелец продукта или сервиса. Это новое требование может позволить лицам, связанным с китайским правительством, накапливать обнаруженные уязвимости для их применения. Рост использования уязвимостей нулевых дней за последний год со стороны китайских кибергрупп, вероятно, связан с тем, что прошел целый год после вступления в силу требований к раскрытию уязвимостей, и это важный шаг в приоритетном использовании эксплоитов нулевого дня со стороны государства. Уязвимости, описанные далее, были впервые разработаны и развернуты китайскими кибергруппами национального уровня, прежде чем они были обнаружены и распространены среди других злоумышленников в масштабной экосистеме угроз.

Быстрая эксплуатация уязвимостей

Продолжение

Даже у организаций, которые не являются целью кибергрупп национального уровня, будет ограниченное время для исправления уязвимостей нулевого дня в затронутых системах, прежде чем они будут использованы в широкой экосистеме злоумышленников.

Эти примеры недавно выявленных уязвимостей показывают, что у организаций в среднем есть 60 дней с момента выпуска исправления уязвимости и публикации пилотного кода в Интернете. Часто другие кибергруппы начинают применять эти уязвимости повторно. Также у организаций есть в среднем 120 дней до того, как уязвимость станет доступна в автоматизированных инструментах сканирования уязвимостей и эксплойтов, таких как Metasploit, что часто приводит к ее массовому использованию. Это подчеркивает, что даже у организаций, которые не являются целью кибергрупп национального уровня, будет ограниченное время для исправления уязвимостей нулевого дня в затронутых системах, прежде чем они будут использованы в широкой экосистеме злоумышленников.

CVE-2021-35211 SolarWinds Serv-U

В июле 2021 года компания SolarWinds выпустила рекомендации по безопасности для уязвимости CVE-2021-35211, поблагодарив корпорацию Microsoft за уведомление⁸. В то время мы обнаружили, что национальная кибергруппа DEV-0322 активно использует уязвимость SolarWinds Serv-U. Наша команда RiskIQ отследила 12 646 IP-адресов, на которых были размещены подключенные к Интернету версии затронутых устройств в период с 15 июня по 9 июля.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

В сентябре 2021 года наши исследователи наблюдали, как связанные с Китаем кибергруппы использовали уязвимость Zoho ManageEngine в нескольких организациях из США. Общественности стало известно об этой уязвимости 6 сентября под именем CVE-2021-40539 Zoho ManageEngine ADSelfService Plus — организации обычно используют эту функцию для сброса пароля⁹. Кибергруппа DEV-0322

воспользовалась уязвимостью позднее в сентябре, применив ее в качестве начального закрепления в сетях и выполнения дополнительных действий, таких как сброс учетных данных, установка двоичных файлов и удаление вредоносных программ для сохранения в среде. На момент раскрытия команда RiskIQ обнаружила 4011 экземпляр этих систем, активно действующих в Интернете.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

В конце октября 2021 года мы обнаружили, как кибергруппа DEV-0322 использует уязвимость CVE-2021-44077 во втором продукте Zoho ManageEngine, ServiceDesk Plus — программном обеспечении службы ИТ-поддержки с возможностями управлением активами. Кибергруппа DEV-0322 использовала эту уязвимость для компрометации организаций из сферы здравоохранения, ИТ, высшего образования и критически важных производственных секторах. 2 декабря Федеральное бюро расследований (ФБР) и Агентство по кибербезопасности и безопасности инфраструктуры (CISA) выпустили совместное консультативное предупреждение для общественности о том, что кибергруппы национального уровня используют эту уязвимость. На момент публикации команда RiskIQ обнаружила 7956 экземпляров этих систем, активно действующих в Интернете.

CVE-2021-42321 Microsoft Exchange

Эксплойт нулевого дня для уязвимости CVE-2021-42321 в Exchange был выявлен во время Tianfu Cup, международного саммита по кибербезопасности и хакерского соревнования, состоявшегося 16 и 17 октября 2021 года в Чэнду, Китай. Исследователи безопасности из корпорации Microsoft обнаружили использование уязвимости Exchange 21 октября, всего 3 три дня после ее обнаружения. На момент публикации

команда RiskIQ обнаружила 61 559 экземпляров этих систем, активно действующих в Интернете. Мы продолжали наблюдать активность эксплойта вплоть до ноября 2021 года.

CVE-2022-26134 Confluence

У связанной с Китаем кибергруппы, вероятно, был код эксплойта нулевого дня для уязвимости Confluence (CVE-2022-26134) за 4 дня до того, как она была публично раскрыта 2 июня. Вероятно, злоумышленники использовали ее против американской организации. На момент публикации команда RiskIQ обнаружила 53 621 экземпляр уязвимых к Confluence систем в Интернете.

Уязвимости выявляются и используются в большом масштабе и во все более короткие сроки.

Практические рекомендации

- 1 Сделайте установку исправлений уязвимостей нулевого дня приоритетом, как только они будут выпущены — не ждите развертывания в соответствии с циклом управления исправлениями.
- 2 Документируйте и проводите инвентаризацию всех аппаратных и программных ресурсов организации, чтобы оценить риски и быстро определить, когда устанавливать исправления.

Кибертактика российских государственных кибергрупп военного времени угрожает Украине и другим странам

В этом году российские кибергруппы начали кибероперации в дополнение к военным действиям во время вторжения России в Украину, часто используя те же тактику и методы, что и против целей за пределами Украины. Очень важно, чтобы организации во всем мире приняли меры по укреплению киберзащиты против цифровых угроз, исходящих от кибергрупп, связанных с Россией.

Ситуация на местах продолжает изменяться по мере продолжения военного конфликта, поэтому Украина и ее союзники должны быть готовы защититься, если российские кибергруппы увеличат частоту или интенсивность вторжений в соответствии с военными целями. В первые 4 месяца войны корпорация Microsoft наблюдала, как злоумышленники, связанные с российской армией, запускали несколько волн разрушительных кибератак против почти 50 различных украинских учреждений и предприятий, а также выполняли шпионские операции против многих других организаций. За исключением операций против клиентов онлайн-сервисов, 64 % российских атак

в отношении известных целей были направлены на украинские организации в период с конца февраля по июнь.

Для каждой операции российские злоумышленники использовали многие тактики, методы и процедуры (TTP), которые мы наблюдали перед вторжением, против целей как внутри Украины, так и за ее пределами. Они стремились уничтожить данные и вывести украинские правительственные учреждения из равновесия в начале конфликта. Затем их целью было помешать перевозке военной и гуманитарной помощи в Украину, блокировка доступа общественности к сервисам и СМИ, а также кража информации с долгосрочной разведывательной или экономической ценностью для России.

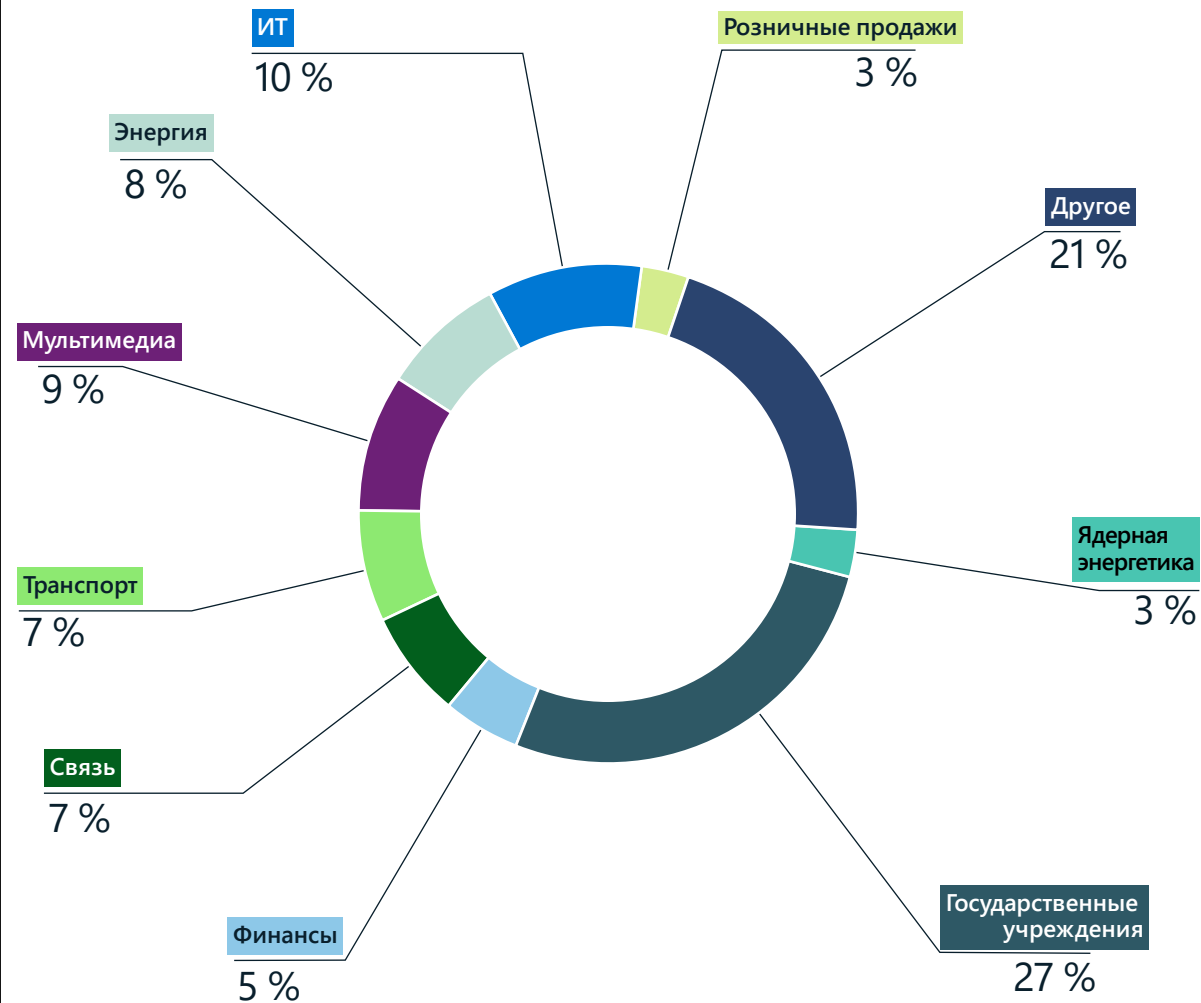
Атаки на транспорт — это угроза критически важной области для украинских граждан, пытающихся выжить в конфликте. Согласно опросу, проведенному по заказу ЮНИСЕФ в мае, респонденты в затронутых конфликтом городских районах больше всего беспокоились о транспорте и топливе, перебоях в поставках, безопасности и ограниченном доступе к продовольствию, медицинскому обслуживанию и финансовым услугам¹⁰. В июне координатор ООН по кризисным ситуациям в Украине заявил, что как минимум 15,7 миллиона человек в Украине срочно нуждаются в гуманитарной помощи, и их количество будет расти по мере продолжения войны¹¹.

За пределами Украины корпорация Microsoft обнаружила российские попытки вторжения в сети 128 организаций в 42 странах с конца февраля по июнь. США были главной целью для России. Польша, через которую проходит большая часть международной военной и гуманитарной помощи Украине, также была важной целью в течение этого периода. Злоумышленники, связанные с российским правительством, атаковали организации в странах Балтии и компьютерные сети в Дании, Норвегии, Финляндии и Швеции в апреле и мае.

Угрозы
национального
уровня

Кибероперации
по распростра-
нению влияния

Отрасли в Украине, чаще всего выбираемые злоумышленниками в качестве цели после вторжения



Федеральные, региональные и местные администрации в Украине оставались приоритетной целью для российских государственных и связанных с государством кибергрупп на протяжении всего конфликта. Акцент на транспортных, энергетических, финансовых и медийных организациях подчеркивает риски, которые эти кибероперации представляют для сервисов, от которых зависят граждане Украины.

Кибертактика российских государственных кибергрупп военного времени угрожает Украине и другим странам

Продолжение

Мы наблюдали рост аналогичных действий в отношении министерств иностранных дел стран НАТО.

Российские кибергруппы остались заинтересованы во взломе критической инфраструктуры как внутри, так и за пределами Украины. Группа IRIDIUM развернула вредоносную программу Industroyer 2 в неудачной попытке оставить миллионы людей в Украине без электричества. За пределами Украины в начале 2022 года кибергруппа BROMINE атаковала производственные организации и промышленные системы управления.

В этом году российские кибергруппы и связанные с ними злоумышленники проводили кибероперации против Украины, ее союзников и других целей, представляющих разведывательную ценность, используя многие из следующих тактик, методов и процедур:

Целевой фишинг с помощью вредоносных вложений или ссылок

Российские государственные и связанные с Россией кибергруппы, такие как ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM и IRIDIUM, проводили фишинговые кампании для получения доступа к желаемым учетным записям и сетям в организациях внутри и за пределами

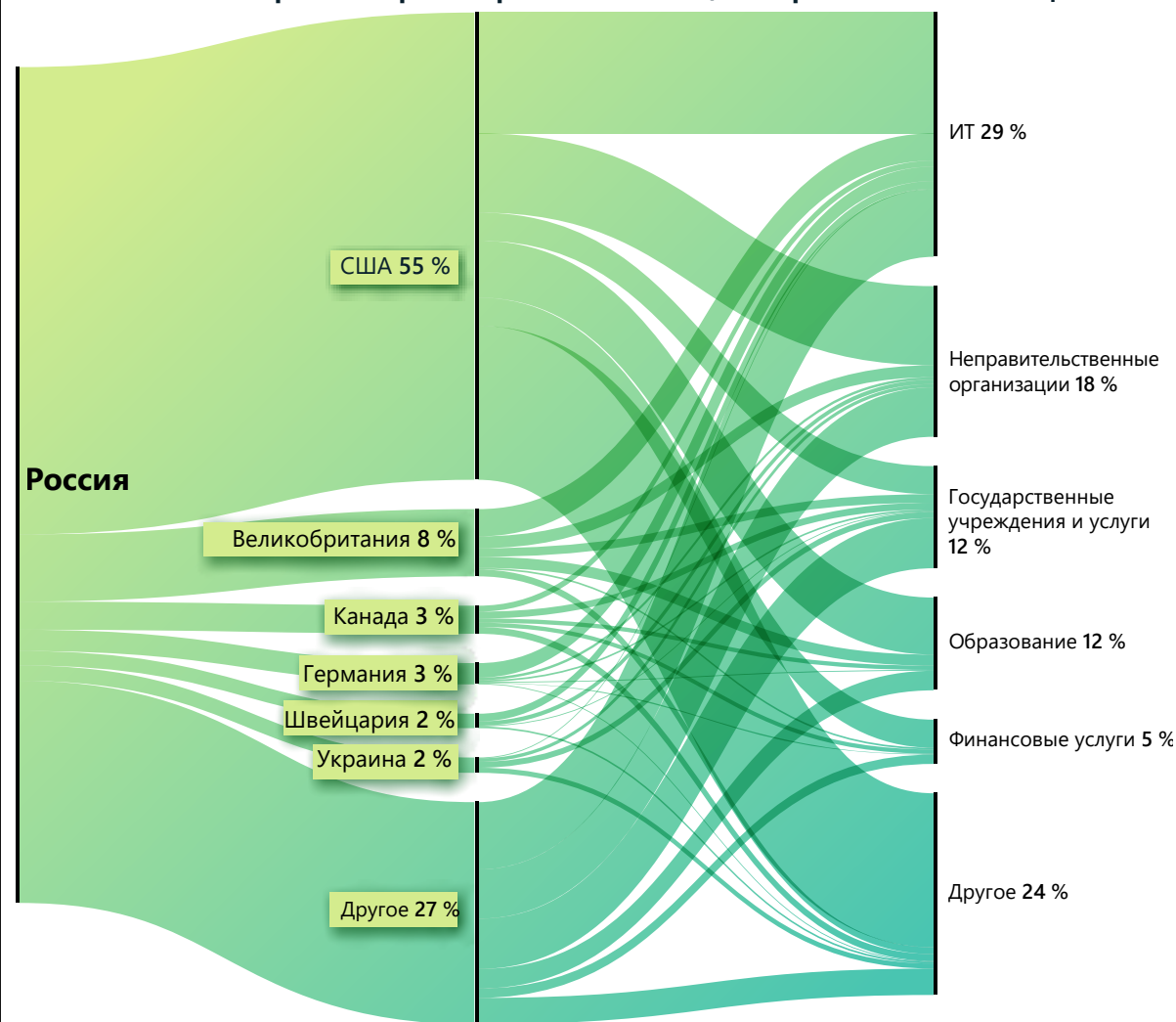
Украины. Для многих кампаний применялись скомпрометированные или поддельные учетные записи в целевых организациях или в той же отрасли и убедительные темы, чтобы заманить жертв в ловушку. Группа NOBELIUM использовал скомпрометированные дипломатические учетные записи для отправки фишинговых писем, замаскированных под дипломатические сообщения, сотрудникам министерств иностранных дел по всему миру. Кибергруппа STRONTIUM создала поддельные учетные записи на основе общедоступных имен владельцев учетных записей в аналитических центрах в США и отправляла фишинговые письма, чтобы получить доступ к учетным записям в этих центрах. Группа SEABORGIUM проводила фишинговые атаки с использованием приманок, связанных с освещением конфликта в Украине, чтобы получить доступ к учетным записям международных аналитических центров в странах Северной Европы.

Использование цепочки поставок ИТ-сервисов для воздействия на их клиентов

В конце 2021 года российские государственные кибергруппы скомпрометировали поставщиков ИТ-сервисов и использовали их для подделки веб-сайтов и развертывания разрушительной вредоносной программы Whispergate (DEV-0586) в январе¹². Группа DEV-0586 также взломала сеть ИТ-компания, которая создавала системы управления ресурсами для министерства обороны Украины и других организаций в секторах связи и транспорта, указывая на то, что группа также изучает варианты сторонних атак в этих секторах.

Во всем мире, но особенно в США и Западной Европе, в течение 2021–2022 годов группа NOBELIUM атаковала поставщиков ИТ-сервисов, чтобы получить доступ к правительственным и другим важным сетям (см. обсуждение уязвимостей цепочки поставок ранее в этой главе).

Россия: основные страны и отрасли промышленности, выбираемые в качестве цели



Несмотря на повышенное с начала 2022 года внимание к украинским организациям, предприятия из Северной Америки и Западной Европы по-прежнему были клиентами онлайн-сервисов, которых чаще всего атаковали российские кибергруппы. Кампания NOBELIUM против ИТ-сектора сделала его основной целью в прошлом году.

Кибертактика российских государст- венных кибергрупп военного времени угрожает Украине и другим странам

Продолжение

Использование публичных приложений для первоначального доступа к сетям

По крайней мере, с конца 2021 года кибергруппа STRONTIUM работала над развитием и совершенствованием своих возможностей по использованию публичных сервисов, таких как серверы Microsoft Exchange, для кражи данных. Группа STRONTIUM использовала серверы Exchange без установленных исправлений для доступа к украинским правительственным учетным записям, а также к военным и оборонным организациям в США, Ливане, Перу и Румынии и другим государственным учреждениям в Армении, Боснии, Косово и Малайзии. Группа DEV-0586, также связанная с российскими военными, использовала уязвимости сервера Confluence для первоначального доступа к государственным организациям и ИТ-компаниям в Украине и других странах Восточной Европы.

Российские государственные и связанные с ними кибергруппы используют многие из тех же тактик, методов и процедур для компрометации организаций, представляющих интерес в военное и мирное время.

Использование административных учетных записей и протоколов, а также собственных утилит для обнаружения сетевых ресурсов и горизонтального перемещения

После первоначального доступа к сети корпорация Microsoft наблюдала, как российские государственные кибергруппы применяют подлинные учетные записи и программные утилиты, предназначенные для выполнения базовых задач обслуживания, чтобы избежать обнаружения в течение как можно большего времени. Они использовали скомпрометированные удостоверения с правами администратора, а также стандартные протоколы, инструменты и методы администрирования для горизонтального перемещения внутри сетей, не привлекая внимание автоматизированных средств мониторинга и защиты сети.

Базовая киберпрофилактика и использование инструментов обнаружения конечных точек и реагирования позволят смягчить негативное воздействие таких операций в мирное и военное время.

Из-за непредсказуемости продолжающегося конфликта организации во всем мире приняли меры по укреплению кибербезопасности против цифровых угроз от российских государственных и связанных с Россией кибергрупп.

Практические рекомендации

- 1 Сведите к минимуму возможности кражи учетных данных и злоупотребления учетными записями, защитив удостоверения пользователей с помощью средств защиты удостоверений MFA и реализации доступа с минимальными привилегиями для защиты конфиденциальных и привилегированных учетных записей и систем.
- 2 Устанавливайте обновления, чтобы все системы были защищены на высочайшем уровне как можно скорее и были в актуальном состоянии.
- 3 Разверните в организации решения для защиты от вредоносных программ, обнаружения конечных точек и защиты удостоверений. Сочетание решений для глубокой защиты в сочетании с обученным и эффективным персоналом позволит вашей организации выявлять, обнаруживать и предотвращать вторжения, влияющие на бизнес.
- 4 Организуйте проведение расследований и восстановление в случае обнаружения или получения уведомления об угрозе для среды за счет резервного копирования критически важных систем и ведения журналов. Настоятельно рекомендуется создать план реагирования на инциденты.

Ссылки на дополнительную информацию

- > Защита Украины: первые уроки кибервойны | Microsoft On the Issues
- > Гибридная война в Украине | Microsoft On the Issues
- > Киберугрозы в Украине: анализ и ресурсы | Microsoft Security Response Center (MSRC)
- > Предотвращение кибератак, направленных против Украины | Microsoft On the Issues
- > Вредоносные атаки, нацеленные на правительство Украины | Microsoft On the Issues
- > MagicWeb: трюк NOBELIUM после взлома для аутентификации от имени любого пользователя | Microsoft Threat Intelligence Center (MSTIC), Detection and Response Team (DART), команда исследователей Microsoft 365 Defender

Китай расширяет глобальные операции для получения конкурентного преимущества

В современном сложном геополитическом климате китайские государственные и связанные с ними кибергруппы часто стремятся продвигать стратегические военные, экономические и международные отношения страны в рамках цели Китая по получению конкурентного преимущества. В прошлом году корпорация Microsoft наблюдала масштабную атаку из Китая, нацеленную на страны по всему миру.

С середины 2021 года Китай маневрирует в попытках обеспечить экономическую и финансовую стабильность на фоне худшего всплеска числа заболеваний COVID-19 за 2 года¹³. Китай продолжал проявлять гибкость касательно геополитических событий, таких как балансировка своего «безграничного» партнерства с Россией¹⁴ и сохранение своих позиций на мировой арене¹⁵. Кроме того, позиция Китая в отношении США и их союзников по отношению к Тайваню¹⁶ и Южно-Китайского моря продолжала держать международные отношения со многими странами в напряжении¹⁷.

Китайские государственные и связанные с ними кибергруппы стали чаще выбирать в качестве цели небольшие страны по всему миру с акцентом на Юго-Восточную Азию, чтобы получить конкурентное преимущество на всех фронтах.

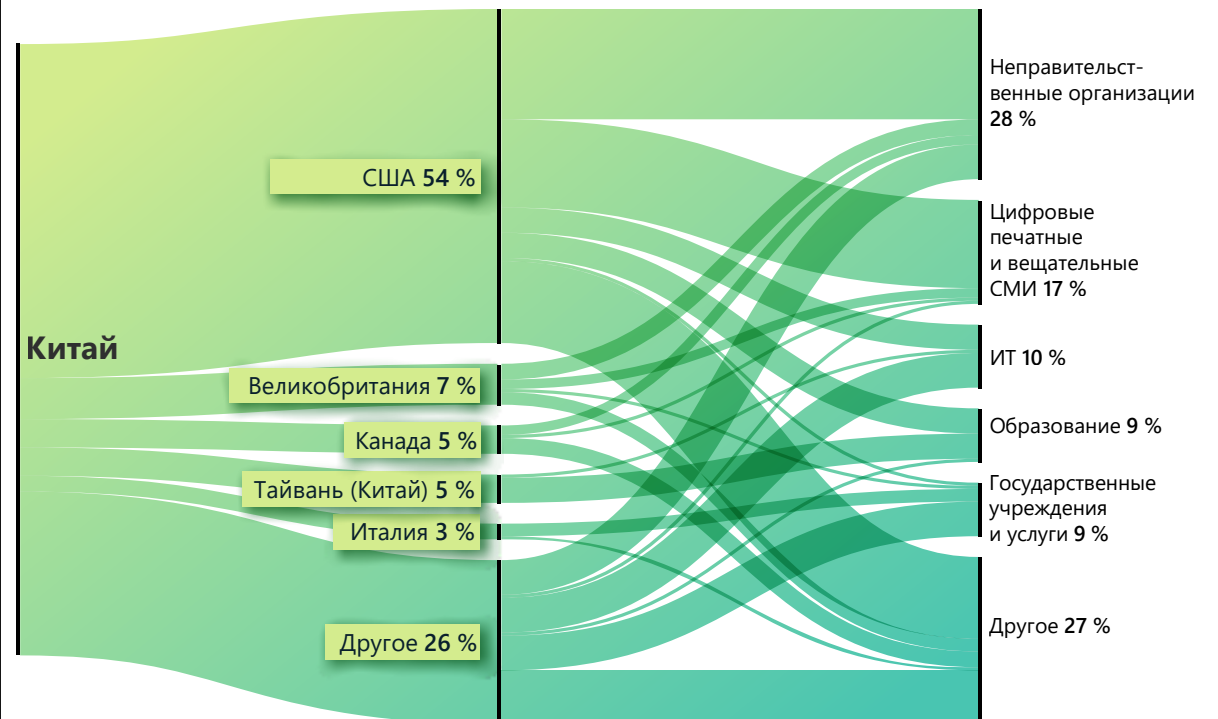


Китай также продолжал расширять экономическое влияние во всем мире в рамках программы «Один пояс — один путь» (BRI), пытаясь возродить комплексную инвестиционную платформу с ЕС¹⁸ и ведя переговоры о новом региональном торговом соглашении с 15 странами Азиатско-Тихоокеанского региона, известном как соглашение о Всеобъемлющем региональном экономическом партнерстве¹⁹. По оценкам Microsoft, Китай продолжит использовать кибероперации сбора данных для продвижения своих стратегических политических, военных и экономических целей, о чем говорят выявленные кибероперации и широта выбора целевых организаций.

Кибератаки, вероятно, будет продвигать экономические и военные интересы.

Корпорация Microsoft наблюдала масштабные атаки на небольшие страны по всему миру со стороны китайских государственных и связанных с ними кибергруппами. Вероятно, Китай использует кибершпионаж как метод распространения глобального экономического и военного влияния.

Китай: основные страны и отрасли промышленности, выбираемые в качестве цели



Аналитические центры/НПО, СМИ, ИТ-компании, государственные и образовательные учреждения были одними из главных целей базирующихся в Китае кибергрупп угроз, вероятно, для постоянного сбора разведанных и рекогносцировки.

В число целей входили страны Африки, Карибского бассейна, Ближнего Востока, Океании и Южной Азии, но особый акцент был сделан на страны Юго-Восточной Азии и Океании.

В соответствии с программой BRI китайские кибергруппы атаковали организации из Афганистана, Казахстана, Маврикия, Намибии, Тринидада и Тобаго²⁰. Например, Тринидад и Тобаго стал первой карибской страной, которая одобрила

программу BRI в 2018 году, и Китай считает это государство важным партнером в регионе. Кибергруппа NICKEL проводит непрерывные сетевые операции, нацеленные на Тринидад и Тобаго, с 2021 года. Например, в марте 2022 года группа NICKEL провела разведывательную операцию, нацеленную на государственное учреждение, вероятно, для сбора разведанных.

Китай расширяет глобальные операции для получения конкурентного преимущества

Продолжение

Между тем, корпорация Microsoft наблюдала, как китайские государственные и связанные с ними кибергруппы направили сетевые атаки на организации в Юго-Восточной Азии и затем расширили их на страны Океании, так как Китай изменил военные и экономические приоритеты, чтобы справиться с проблемами, вызванными возобновлением интереса США к этому региону. В январе 2022 года корпорация Microsoft наблюдала, как кибергруппа RADIUM атаковала энергетическую компанию и связанное с энергетикой государственное учреждение во Вьетнаме, а также индонезийское государственное учреждение. Операции RADIUM, вероятно, соответствовали стратегическим целям Китая в Южно-Китайском море²¹. В конце февраля и начале марта кибергруппа GALLIUM взломала больше 100 учетных записей, связанных с известной в Юго-Восточной Азии межправительственной организацией (МПО). Сроки атаки GALLIUM на МПО в этом регионе совпали с объявлением о запланированной встрече между США и региональными лидерами. Группе GALLIUM, вероятно, поручили отслеживать коммуникации и собирать разведданные до этого мероприятия.

По мере расширения влияния Китая в странах Океании началась волна операций китайских кибергрупп. В апреле Китай и Соломоновы Острова подписали соглашение, призванное «содействовать миру и безопасности». Оно позволяет Китаю развернуть полицию и вооруженные силы на Соломоновых островах²². В мае на Фиджи состоялась вторая встреча министров иностранных дел Китая и стран Океании, на которой Китай предложил развивать «всеобъемлющее стратегическое партнерство» для продвижения политических, культурных, социальных интересов, а также интересов в области безопасности и изменения климата, а также для борьбы с пандемией²³. Примерно в то же время в мае корпорация Microsoft обнаружила вредоносное ПО GADOLINIUM в правительственных системах Соломоновых Островов. Кибергруппа RADIUM также загрузила вредоносный код в системы телекоммуникационной компании в Папуа-Новой Гвинее. Мы считаем, что эти действия были направлены на сбор разведданных для поддержки общей региональной стратегии Китая.

Корпорация Microsoft мешает операциям NICKEL, но кибергруппа демонстрирует настойчивость.

В декабре 2021 года подразделение Microsoft по борьбе с киберпреступлениями (DCU) подало ходатайства в окружной суд Восточного округа штата Вирджиния с просьбой разрешить конфисковать 42 домена центра управления, контролируемых кибергруппой NICKEL. Эти домены использовали в операциях против государственных и дипломатических учреждений, а также НПО в Центральной и Южной Америке, Карибском бассейне, Европе и Северной Америке с сентября 2019 года²⁴. С помощью этих операций NICKEL удалось получить долгосрочный доступ

к нескольким организациям и извлечь данные из систем некоторых жертв с конца 2019 года.

По мере того как Китай продолжает развивать двусторонние экономические отношения со множеством стран (часто в рамках соглашений, связанных с BRI), глобальное влияние Китая будет расти. По нашей оценке, китайские государственные и связанные с ними кибергруппы будут преследовать цели в государственном, дипломатическом и неправительственном секторах, чтобы получить новую информацию, вероятно, с целью экономического шпионажа или традиционного сбора разведданных. После вмешательства корпорации Microsoft кибергруппа NICKEL нацелилась на несколько государственных учреждений, вероятно, пытаясь восстановить потерянный доступ. С конца марта по май 2022 года NICKEL удалось повторно взломать не меньше 5 государственных учреждений по всему миру. Это говорит о том, что у группы были дополнительные точки входа в эти организации или что она восстановила доступ через новые домены центра управления. Настойчивый взлом кибергруппой NICKEL одних и тех же государственных учреждений во всем мире указывает на важность задачи на высоком уровне.

Китай становится агрессивнее касательно своей позиции по внешней политике. Мы считаем, что экономический шпионаж и сбор разведданных с помощью киберопераций, вероятно, будут продолжаться.

Практические рекомендации

- 1 Укрепите киберзащиту для упреждающей борьбы с киберугрозами. Из-за настойчивости китайских кибергрупп организациям необходимо своевременно выявлять, обнаруживать возможные вторжения и реагировать на них.
- 2 Злоумышленники злоупотребляют запланированными задачами²⁵ в качестве распространенного метода сохранения и уклонения от механизмов защиты, поэтому убедитесь, что в вашей среде используются дополнительные рекомендации по безопасности для защиты от этого метода²⁶.
- 3 Мы продолжаем наблюдать использование веб-оболочек как начального направления атаки в сетях целей²⁷. Организации должны защитить системы от атак с помощью веб-оболочек, которые могут дать злоумышленникам доступ для выполнения удаленных команд²⁸.

Ссылки на дополнительную информацию

- > Кибергруппа NICKEL атакует государственные учреждения в Латинской Америке и Европе | Microsoft Threat Intelligence Center (MSTIC), подразделение цифровой безопасности Microsoft
- > Защита пользователей от недавних кибератак | Microsoft On the Issues

Иран становится агрессивнее после смены правительства

Корпорация Microsoft наблюдала, как иранские государственные и связанные с ними кибергруппы увеличивают темпы и масштабы кибератак против Израиля, расширяют атаки программ-шантажистов на США и ЕС, выбирая в качестве цели критически важную инфраструктуру США, чтобы, по крайней мере, подготовиться к потенциальным разрушительным кибератакам.

Растущая активность иранских государственных кибергрупп последовала за сменой президента в Иране. Летом 2021 года радикальный политик Ибрагим Раиси сменил умеренного президента Хасана Роухани. В отличие от Раиси, который является протеем Верховного лидера Ирана и близким союзником Корпуса стражей исламской революции (КСИР), склонность бывшего президента Роухани к дипломатии часто вызывала противоречия с Верховным лидером и руководителями КСИР²⁹. Ястребиные взгляды администрации Раиси, по-видимому, повысили готовность иранских кибергрупп к смелым действиям против Израиля и Запада, особенно США, несмотря на возобновление дипломатического взаимодействия для продолжения ядерной сделки с Ираном.

Увеличение темпов и масштабов иранских кибератак против Израиля

Через несколько недель после формирования внешнеполитической команды президентом Раиси³⁰ иранские государственные кибергруппы возобновили разрушительные кибератаки против Израиля, проводя их быстрее, чем в предыдущем году. Атаки программ-шантажистов и попытки кражи данных осуществлялись каждые несколько недель начиная с сентября. В них участвовали по меньшей мере 3 связанных с Ираном кибергруппы. Возможно, атаки могли быть частью общенациональной кампании возмездия против Израиля. По крайней мере в одном случае корпорация Microsoft предположила, что атака программ-шантажистов против израильской организации в конце 2021 года была направлена на сокрытие основной атаки, нацеленной на удаление данных. Анализ вредоносного ПО, проведенный корпорацией Microsoft, показал, что программа-шантажист, доставленная жертве, выполняла код для уничтожения данных после шифрования.

К 2022 году иранские кибератаки расширились с точки зрения целей и типов атак. В феврале кибергруппа DEV-0198 попыталась провести серьезную атаку на израильскую критически важную инфраструктуру. Корпорация Microsoft также предполагает, что связанная с Ираном кибергруппа, скорее всего, несет ответственность за сложную кибератаку, из-за которой в июне в Израиле сработали сирены противоракетной обороны. Вероятно, использовалось программное обеспечение, которое корректирует звук по IP-сетям.

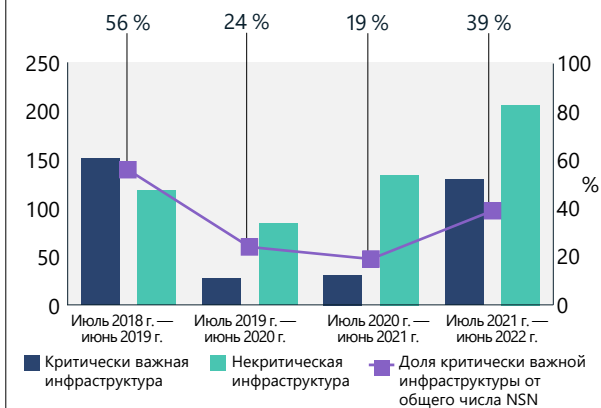
Угрозакритически важной инфраструктуре США и Израиля со стороны Ирана росла в течение всего года

По оценкам Microsoft, иранские государственные кибергруппы, связанные с КСИР (PHOSPHORUS и DEV-0198), атаковали важную инфраструктуру США и Израиля с конца 2021 года до середины 2022 года. Вероятная цель заключалась в том, чтобы позволить Тегерану нанести ответный удар по тем же секторам, в атаку на которых руководители КСИР обвиняли США и Израиль³¹. По нашим оценкам, эти операции связаны с заявлениями, сделанными в конце октября 2021 года генералом КСИР Голамреза Джалали, начальником управления гражданской обороны Ирана, который повторил обвинения других влиятельных фигур режима в том, что США и Израиль проводили кибератаки на иранские порты, железные дороги и автозаправочные станции³². Джалали выступил с этим обвинением во второй раз во время постановочной пятничной молитвенной речи на трибуне с изображением ракеты, перечеркивающей слово «США». Это говорит о том, что старшие руководители придерживались той же точки зрения³³.

В октябре 2021 кибергруппа PHOSPHORUS начал масштабное сканирование американских организаций года на наличие неисправленных уязвимостей Fortinet и ProxyShell. После компрометации эти уязвимые системы использовались для проведения атак программ-шантажистов, а в нескольких случаях — против критически важной инфраструктуры в США и других западных странах. Это были первые подтвержденные случаи атак программ-шантажистов, связанных с иранским государством, за пределами Ближнего Востока. После кибератаки на автозаправочные станции Ирана в конце октября корпорация Microsoft наблюдала всплеск атак иранских программ-шантажистов на американские компании, что говорит о возможной корреляции.

В то же время кибергруппа PHOSPHORUS перешла к направленным атакам, часто используя целевой фишинг, на крупные инфраструктурные компании в США, в том числе морские порты и аэропорты, транспортные системы, коммунальные и нефтегазовые компании. Эти атаки, часто проводимые с помощью целевого фишинга, продолжались до середины 2022 года. Цели были напрямую связаны с секторами, в атаке на которые Тегеран обвинил США и Израиль, что могло послужить причиной для операции возмездия. Компрометация почти идентичных целей позволит сдерживать такие атаки в будущем в попытке избежать эскалации за счет информирования о причине атаки без признания вины.

Возобновление иранских атак на инфраструктуру



Иранские атаки на критически важную инфраструктуру достигли самых высоких показателей, наблюдаемых с конца 2018 года до начала 2019 года. Мы использовали директиву президента США 21 (PPD-21), чтобы определить, соответствует ли компания критериям критически важной для инфраструктуры организации (июль 2021 г.—июль 2022 г.).

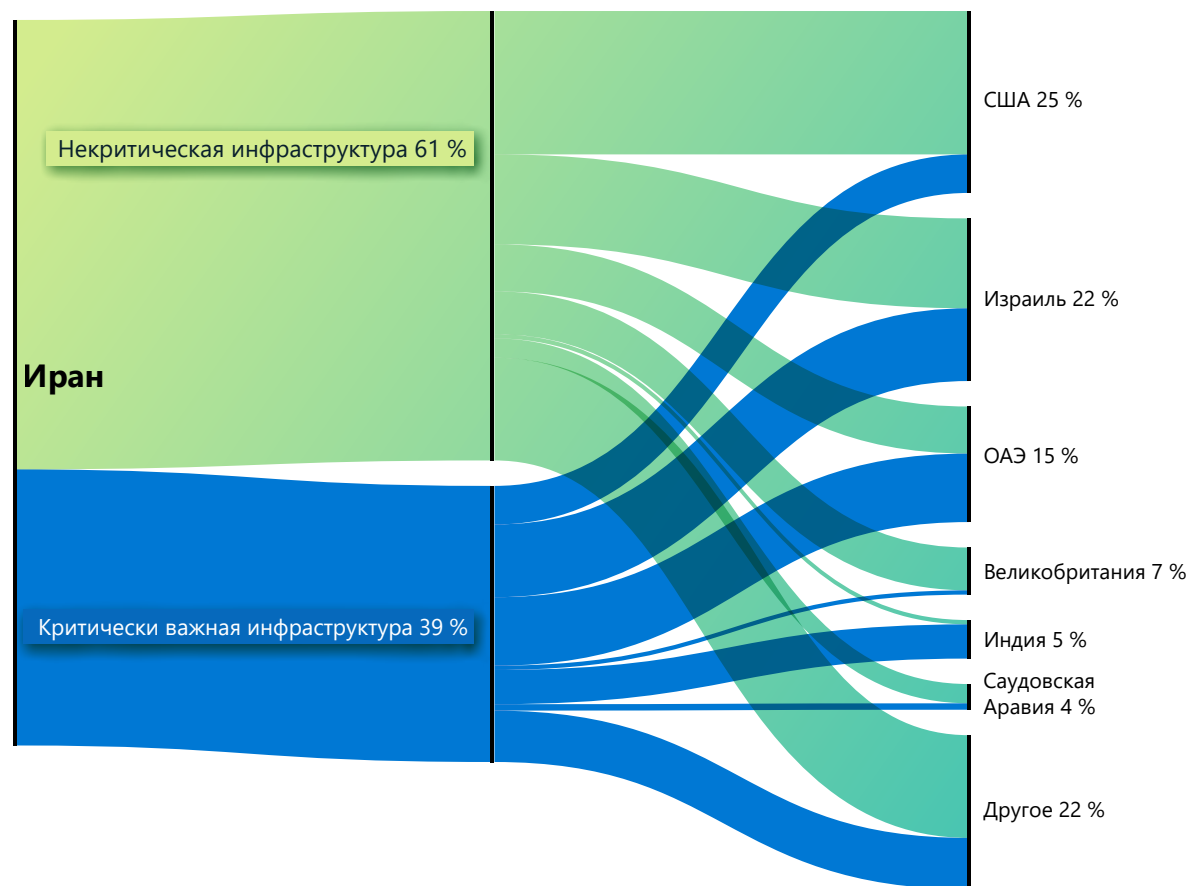
Иран становится агрессивнее после смены правительства

Продолжение

В Израиле кибергруппа DEV-0198 атаковала железные дороги, логистические компании, поставщиков ПО логистических компаний и топливные компании с акцентом на автозаправочные станции. В начале 2022 года группа организовала разрушительную атаку на сеть крупной израильской логистической компании, что вынудило ее отключить компьютеры и прервать некоторые операции для сдерживания атаки. В другом случае мы наблюдали, как группа попыталась получить доступ к сети крупного израильского транспортного предприятия с помощью украденных или повторно использованных учетных данных. В то же время другая иранская кибергруппа DEV-0343 (нацеленная на организации из таких секторов, как оборона, морские перевозки и спутниковые снимки, что позволяет предположить ее связь с КСИР) взломала учетные записи израильских транспортных и портовых организаций в начале 2021 года.

Иранские кибергруппы, скорее всего, останутся угрозой для американских и израильских транспортных и энергетических компаний, особенно в связи с тем, что дипломатические усилия по возобновлению иранской ядерной сделки ослабевают, а Вашингтон, Тель-Авив и Тегеран ищут альтернативные принудительные способы, чтобы выторговать уступки.

Иранские атаки на критически важную инфраструктуру по странам



Иранские атаки на критически важную инфраструктуру происходили чаще всего против организаций из Израиля, ОАЭ и США.

Иранские кибергруппы, скорее всего, останутся угрозой для американских и израильских транспортных и энергетических компаний в наступающем году.

Иранские кибергруппы распространили атаки программ-шантажистов за пределы региональных противников и нацелились на критически важные объекты инфраструктуры в Израиле и США.

Практические рекомендации

- 1 Улучшите общую киберпрофилактику организации, используя решения без пароля, такие как MFA, и обеспечив их применение для всех удаленных подключений, чтобы устранить угрозу от потенциально скомпрометированных учетных данных.
- 2 Оценивайте подлинность всего входящего трафика электронной почты, чтобы убедиться в подлинности адресов отправителей.
- 3 Устанавливайте исправления заранее и регулярно³⁴.
- 4 Проводите проверку и аудит каждого партнерского отношения с сервис-провайдерами, чтобы свести к минимуму ненужные разрешения между вашей организацией и поставщиками. Корпорация Microsoft рекомендует немедленно блокировать доступ любых партнеров, которые выглядят незнакомыми или еще не были проверены³⁵.

Ссылки на дополнительную информацию

- > Иранские кибергруппы все чаще выбирают ИТ-сектор | Microsoft Threat Intelligence Center (MSTIC), подразделение цифровой безопасности Microsoft (DSU)
- > Связанная с Ираном кибергруппа DEV-0343 проводит атаки на такие сектора как оборона, ГИС и морские перевозки | Microsoft Threat Intelligence Center (MSTIC), подразделение цифровой безопасности Microsoft (DSU)

Базирующаяся в Ливане кибергруппа, связанная с Ираном, атакует цели в Израиле

Корпорация Microsoft отслеживает действия, связанные с киберугрозами, независимо от платформы, цели или географического региона. Мы поддерживаем прозрачность и ведем активный поиск угроз во всем мире, чтобы предоставлять клиентам самые эффективные способы обнаружения.

Хотя угрозы со стороны России, Китая, Ирана и Северной Кореи составляют большую часть нашей наблюдаемой активности национальных кибергруппы, мы также отслеживаем угрозы со стороны стран-членов НАТО и демократических стран и сообщаем о них. В прошлом году мы продемонстрировали операции турецкой (SILICON) и вьетнамской (BISMUTH) кибергрупп. В этом году мы расширяем анализ ливанской кибергруппы, результаты которого мы опубликовали ранее³⁶.

Корпорация Microsoft обнаружила ранее незафиксированную ливанскую кибергруппу, о которой можно с умеренной уверенностью заявить, что она действовала в координации с группами, связанными с министерством разведки и безопасности Ирана (MOIS). Такое сотрудничество или руководство со стороны Тегерана соответствует известиям о том, что правительство Ирана использует третьи стороны для проведения кибератак, о чем сообщили в конце 2020 года, вероятно, чтобы укрепить возможность Ирана отрицать свою причастность к ним.

Как мы наблюдали, группа POLONIUM нацелилась или скомпрометировала больше 20 израильских организаций и 1 МПО, выполняя операции из Ливана с февраля по май 2022 года, прежде чем корпорация Microsoft нарушила и публично раскрыла их деятельность. Почти половина

этих организаций были частью оборонной промышленности Израиля или имели связи с израильскими оборонными компаниями. Это говорит о том, что интересы кибергруппы совпадают с иранскими — это сбор разведанных или прямое противодействие Израилю³⁷.

Предполагаемые связи POLONIUM с кибергруппами MOIS основаны на совпадении жертв, инструментов и методов.

- Совпадение жертв: иранская кибергруппа, связанная с MOIS, которую корпорация Microsoft отслеживает как MERCURY, ранее скомпрометировала нескольких жертв POLONIUM. Это указывает на совпадение требований операций или возможную «передачу» жертв между группами.
- Общие инструменты и методы: специалисты MSTIC обнаружили, что кибергруппа DEV-0588 (также известная как CopyKittens), как и POLONIUM, обычно использует AirVPN для операций, а группа DEV-0133 (также известный как Lyceum³⁸) использует OneDrive для управления и извлечения данных. Подобно иранским государственным кибергруппам, участники POLONIUM использовали поставщика облачных решений для взлома израильской авиационной компании и юридической фирмы³⁹.

Кибергруппа POLONIUM развернула серию пользовательских имплантатов с использованием облачных сервисов для управления и извлечения данных, в частности в OneDrive и DropBox. Участники POLONIUM часто создавали уникальные приложения OneDrive для целей, вероятно, чтобы избежать обнаружения.

К июню 2022 года корпорация Microsoft приостановила работу больше 20 приложений OneDrive, созданных POLONIUM, уведомила затронутые организации и развернула ряд обновлений средств аналитики безопасности для постановки на карантин инструмент, разработанных POLONIUM.

Корпорация Microsoft успешно обнаружила и отключила использование сервиса OneDrive в качестве центра управления кибергруппы POLONIUM.

Практические рекомендации

- 1 Обновите антивирусные инструменты⁴⁰ и убедитесь, что облачная защита⁴¹ включена для обнаружения соответствующих индикаторов.
- 2 Для клиентов, связанных с сервис-провайдерами, проведите проверку и аудит всех партнерских отношений, чтобы свести к минимуму ненужные разрешения между вашей организацией и поставщиками⁴². Немедленно заблокируйте доступ любых партнеров, которые выглядят незнакомыми или еще не были проверены.

Ссылки на дополнительную информацию

- > Разоблачение деятельности кибергруппы POLONIUM и инфраструктуры, нацеленной на израильские организации | Microsoft Threat Intelligence Center (MSTIC), подразделение цифровой безопасности Microsoft (DSU)
- > Кибергруппа MERCURY использует уязвимости Log4j 2 в неисправленных системах для атаки на израильские организации | Microsoft Threat Intelligence Center (MSTIC), исследовательская команда Microsoft 365 Defender, Microsoft Defender Threat Intelligence

Возможности северокорейских кибергрупп, используемые для достижения 3 основных целей режима

Киберприоритеты Северной Кореи за последний год отражали заявленные правительством глобальные приоритеты. В нескольких выступлениях Ким Чен Ын выделил 3 приоритета: наращивание оборонного потенциала, укрепление экономики страны и обеспечение внутренней стабильности⁴³. Действия, предпринятые северокорейскими государственными кибергруппами ясно указывают на то, что киберпространство используется для достижения этих 3 целей.

Северокорейские государственные кибергруппы применяли различные тактики, чтобы проникнуть в аэрокосмические компании по всему миру.

Северокорейские государственные кибергруппы, в первую очередь CERIUМ и ZINC, использовали различные тактики, чтобы проникнуть в сети оборонных и аэрокосмических компаний по всему миру. В первой половине 2022 года Северная Корея приступила к самому агрессивному периоду ракетных испытаний и использовала кибершпионаж, чтобы помочь своим исследователям получить информацию о разработке систем обороны и контрмер для атаки противников.

Мы наблюдали, как кибергруппа COPERNICIUM атаковала различные компании, связанные с криптовалютой, во всем мире, часто успешно, чтобы помочь поддержать испытывающую трудности экономику Северной Кореи. Хотя мы не можем подтвердить, смогла ли группа получить деньги после компрометации, мы наблюдали, как COPERNICIUM заражает десятки машин, отправляя вредоносные документы, маскирующиеся под предложения других криптовалютных компаний.

Наконец, группа, которую корпорация Microsoft отслеживает как DEV-0215, работала над поддержанием стабильности и лояльности в Северной Кореи, нацеливаясь на новостные организации, которые сообщают о проблемах КНДР. У этих СМИ есть источники как в Северной Кореи, так и в общинах перебежчиков, которых Пхеньян считает экзистенциальной угрозой. Кроме того, группа пыталась получить доступ к сетям корейскоязычных христианских групп, которые обычно открыто выступают против КНДР и активно работают с северокорейскими перебежчиками.

Атаки на оборонные и аэрокосмические компании

Северокорейские государственные кибергруппы под предводительством CERIUМ и ZINC приложили значительные усилия для разработки тактики, направленной на проникновение в оборонные и аэрокосмические компании. Кибергруппа CERIUМ неоднократно исследовала южнокорейские виртуальные частные сети (VPN), скачивая клиенты и ища слабые места. Она также скачивала популярные приложения, используемые южнокорейскими военными и государственными учреждениями, вероятно, в поисках уязвимостей. Группа внимательно следила за текущими событиями и создавала новые документы-приманки, в которых использовались громкие темы, чтобы заставить потенциальных жертв щелкнуть вредоносные исполняемые файлы и ссылки.

И ZINC, и CERIUМ использовали в своих кампаниях социальные сети и социальную инженерию. ZINC особенно преуспела в создании поддельных профилей на LinkedIn и в других профессиональных социальных сетях — операторы выдавали себя за менеджеров по найму крупных оборонных и аэрокосмических компаний. Используя эти профили, они отправляли ссылки или вредоносные файлы потенциальным жертвам как прямые сообщения в социальных сетях или электронные письма.

В дополнение к сотрудникам корпораций, кибергруппа CERIUМ также нацеливалась на южнокорейских военных, проявляя особый интерес как к военным академиям, так и к военнослужащим, работающим в научных учреждениях.

Атаки на криптовалютные ресурсы для балансировки потерь

С тех пор как в 2016 году против КНДР были введены санкции ООН, в экономике страны продолжался спад, что усугублялось стихийными бедствиями, такими как наводнения⁴⁴ и засуха⁴⁵, а также почти полным закрытием границ для импорта с начала пандемии COVID-19 в начале 2020 года⁴⁶. Хотя Северная Корея ненадолго открыла свои границы для торговли с Китаем в начале 2022 года, вскоре они были снова закрыты⁴⁷. В середине мая Северная Корея сообщила о первом внутреннем случае заболевания COVID-19⁴⁸. С тех пор в стране применили китайскую стратегию массовой изоляции для борьбы с вирусом, что негативно повлияло на и без того хрупкую экономику КНДР.

Северокорейская государственная кибергруппа COPERNICIUM попыталась компенсировать часть потерянных доходов за счет кражи средств (как правило, в виде криптовалюты) у любой компании, в сети которой они смогли проникнуть. Мы обнаружили десятки скомпрометированных компьютеров, принадлежащих компаниям, связанным с криптовалютой, в США, Канаде, Европе и всей Азии. COPERNICIUM даже удалось взломать компьютеры, принадлежащие компаниям, связанным с криптовалютой, своего самого сильного союзника — Китая, — как на материке, так и в Гонконге. Группа по большей части использовала социальные сети для разведки и приближения к целям. Злоумышленники создавали профили, притворяясь разработчиками или старшими сотрудниками компаний, связанных с криптовалютой. Затем они развивали отношения с теми, кто работал в отрасли, отправляя вредоносные ссылки или файлы, как только налаживали взаимопонимание.

Возможности северокорейских кибергрупп, используемые для достижения 3 основных целей режима

Продолжение

Группа, связанная с PLUTONIUM, разрабатывает и разворачивает программы-шантажисты

Группа злоумышленников из Северной Кореи, которую корпорация Microsoft отслеживает как DEV-0530, начала разрабатывать и использовать программы-шантажисты в атаках в июне 2021 года. Эта группа, назвавшаяся H0lyGh0st, применяла полезную нагрузку программ-шантажистов с тем же названием для своих кампаний и успешно скомпрометировала малые предприятия в нескольких странах уже в сентябре 2021 года.

Корпорация Microsoft оценила, что у DEV-0530 были связи с другой северокорейской группой, отслеживаемой как PLUTONIUM (также известная как DarkSeoul или Andariel). Хотя использование программы-шантажиста H0lyGh0st в кампаниях является уникальной отличительной чертой DEV-0530, специалисты MSTIC обнаружили связь между 2 группами, а также то, что группа DEV-0530 применяла инструменты, разработанные PLUTONIUM.

Нельзя быть полностью уверенным в том, что деятельность DEV-0530 спонсировалась правительством. Хотя атаки программ-шантажистов могли быть заказаны правительством по той же причине, по которой оно поддерживает

кражу у криптовалютных компаний, также возможно, что участники DEV-0530 действовали независимо, чтобы заработать деньги для себя. Если бы это были северокорейские хакеры, действующие независимо, это объяснило бы, почему их операции не были такими масштабными по сравнению со спонсируемыми правительством кражами средств криптовалютных компаний.

Атаки на северокорейские новостные агентства, перебежчиков, религиозные группы и гуманитарные организации

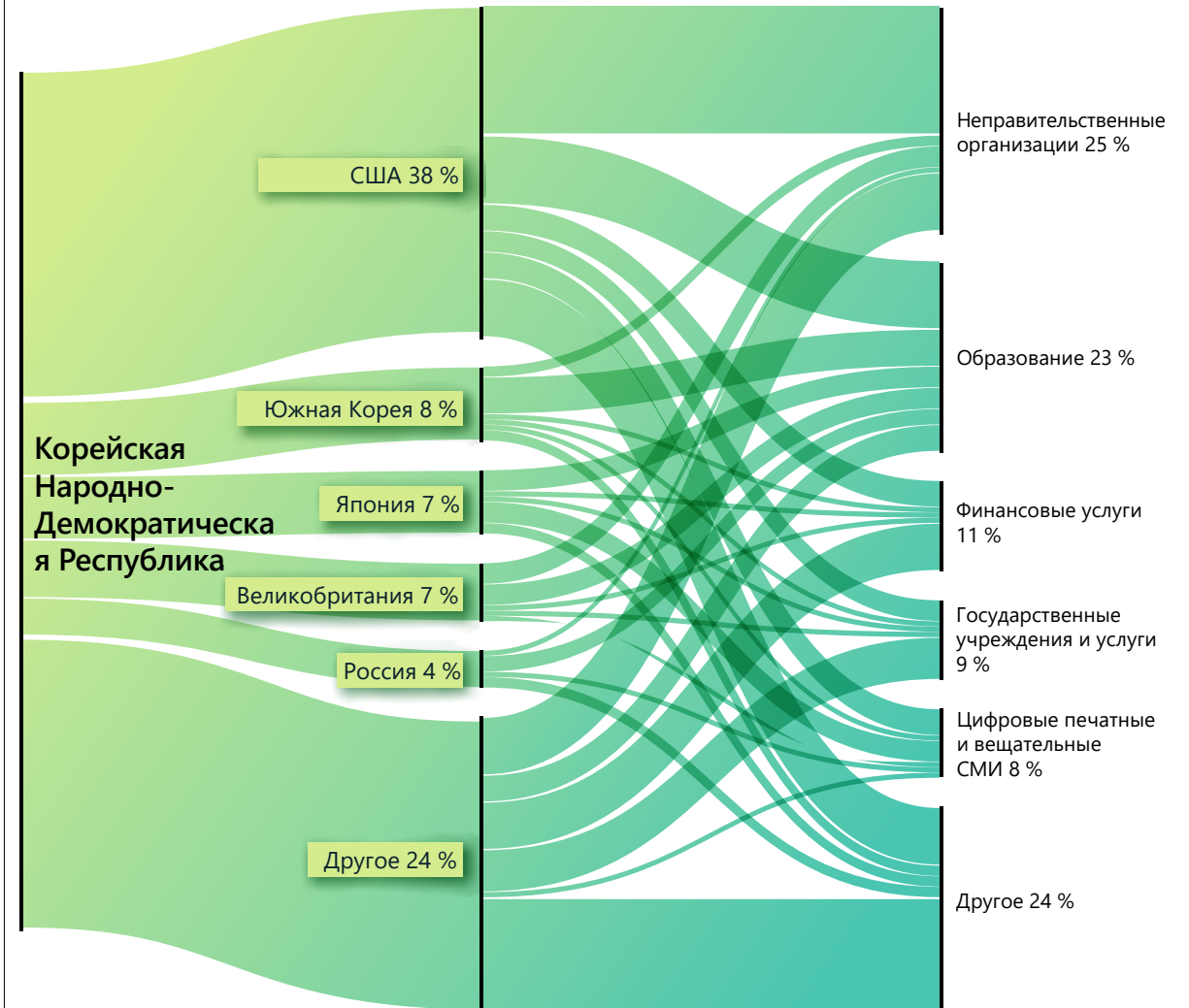
В прошлом году Верховный лидер КНДР Ким Чен Ын публично высказался о концентрации на внутренней безопасности и лояльности, чем на ракетах и ядерном оружии. В соответствии с этой озабоченностью внутренними проблемами по крайней мере 2 северокорейские государственные кибергруппы сосредоточились на аспектах, которые режим рассматривает как внутренние угрозы.

Первой из них была группа, которую корпорация Microsoft отслеживает как DEV-0215. Она нацелена на СМИ, которые внимательно следят за северокорейскими новостями. Одной из вероятных причин этого нападения было то, что эти СМИ получают сведения от северокорейских перебежчиков, китайских граждан, которые тесно сотрудничают с Северной Кореей, и даже некоторых северокорейских граждан, живущих в стране, используя различные методы общения с внешним миром. Правительство КНДР считает эти группы экзистенциальной угрозой, особенно граждан внутри Северной Кореи, которые рассматриваются как предатели и шпионы. Вероятно, группа DEV-0215 пыталась выявить источники этих СМИ, чтобы нейтрализовать потенциальные утечки информации.

Угрозы национального уровня

Кибероперации по распространению влияния

Северная Корея: основные целевые отрасли и сектора



Северная Корея рассматривает США, Южную Корею и Японию как своих главных врагов. Хотя Россия является давним союзником КНДР, северокорейские злоумышленники направляют свои атаки и на российские аналитические центры, ученых и дипломатов, чтобы получить разведанные о российских взглядах на глобальные события.

Возможности северокорейских кибергрупп, используемые для достижения 3 основных целей режима

Продолжение

Корпорация Microsoft также получила подтверждение того, что группа DEV-0215 нацелена на корейскоговорящие христианские общины. Большинство евангельских христианских корейских церквей критически относятся как к правительству Северной Кореи, так и к правительству Южной Кореи, которое выступает за диалог с Северной Кореей. Эти церкви могут проводить разъяснительную работу с перебежчиками, а некоторые из них участвуют в гуманитарной помощи Северной Корее. КНДР считает их угрозой, потому что они часто играют решающую роль в оказании помощи перебежчикам несмотря на то, что их поток почти иссяк во время пандемии⁴⁹. Группа DEV-0215 создала поддельные документы о христианских конференциях для корейскоговорящих граждан в качестве приманки, чтобы выяснить, кто помогает организовывать перебежки.

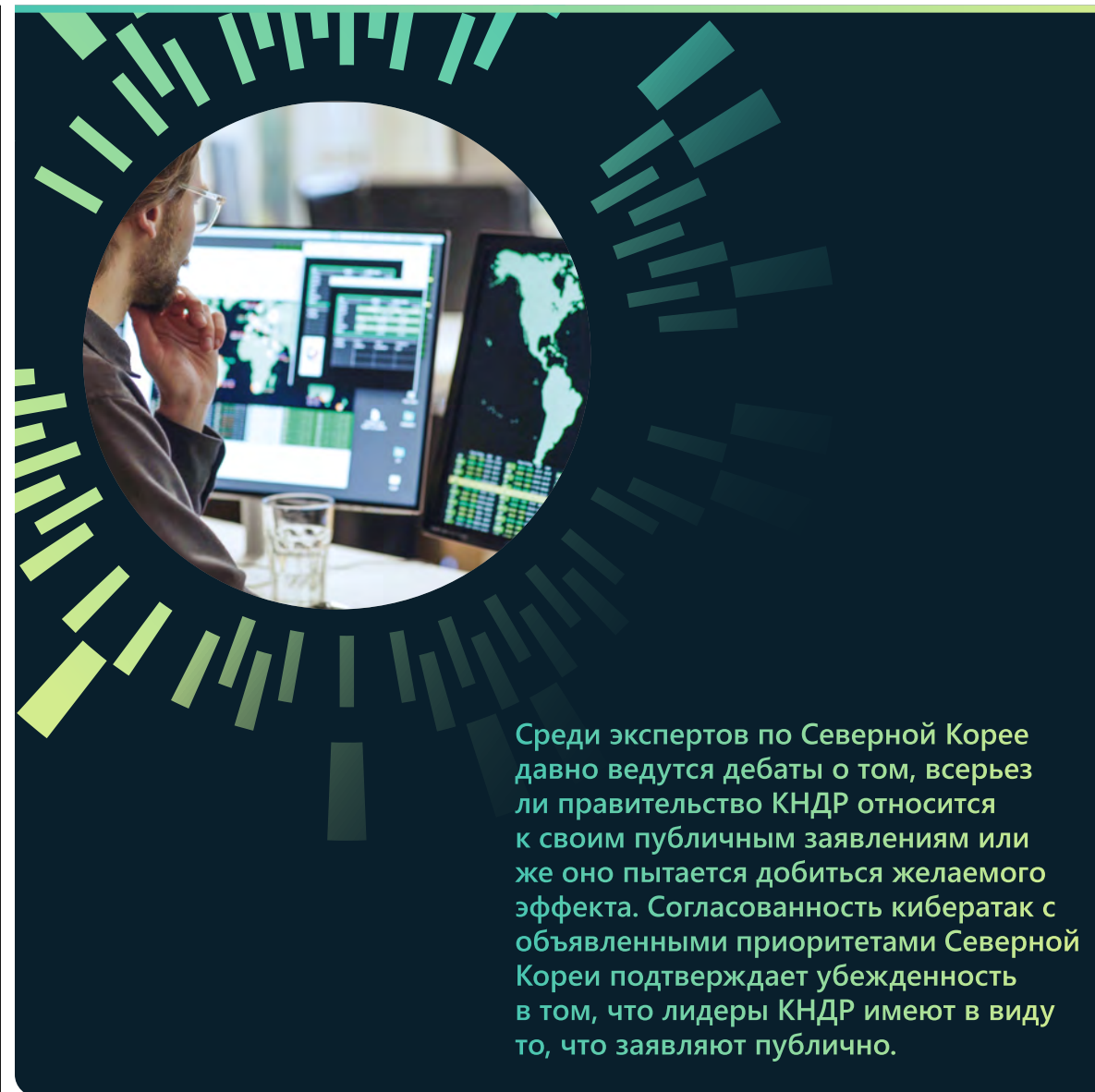
Наконец, государственная кибергруппа OSMIUM в течение года проявляла устойчивый интерес к международным гуманитарным организациям, в том числе к тем, которые помогали Северной Корее в прошлом. Хотя КНДР, как правило, не принимает предложения о помощи из-за пределов страны, но сейчас, особенно после вспышки COVID-19⁵⁰, правительство может рассматривать возможность согласиться на получение помощи, но опасается последствий для безопасности, связанных с допуском иностранных гуманитарных работников в страну. КНДР может проникать в сети гуманитарных организаций по всему миру, чтобы определить, разрешать ли такую помощь в собственной стране.

Практические рекомендации

- 1 Участники северокорейских государственных кибергрупп квалифицированы, неутомимы и креативны, но от них можно защититься.
- 2 Большинство успешных атак можно остановить с помощью базовых мер киберпрофилактики, таких как двухфакторная аутентификация или запрет открывать вложения от неизвестных лиц в виртуальной среде.

Ссылки на дополнительную информацию

- > Северокорейская кибергруппа атакует малый и средний бизнес с помощью программы-шантажиста H0lyGh0st | Microsoft Threat Intelligence Center (MSTIC), подразделение цифровой безопасности Microsoft (DSU)



Среди экспертов по Северной Корее давно ведутся дебаты о том, всерьез ли правительство КНДР относится к своим публичным заявлениям или же оно пытается добиться желаемого эффекта. Согласованность кибератак с объявленными приоритетами Северной Кореи подтверждает убежденность в том, что лидеры КНДР имеют в виду то, что заявляют публично.

Кибернаемники угрожают стабильности киберпространства

Сейчас вырастает целая индустрия из частных компаний, которые разрабатывают и продают инструменты, методы и сервисы, позволяющие их клиентам — часто государственным учреждениям — проникать в сети, компьютеры, телефоны и устройства, подключенные к Интернету. Эти компании как актив для иностранных государств часто подвергают опасности диссидентов, правозащитников, журналистов, защитников гражданского общества и других граждан. Мы называем их кибернаемниками или злоумышленниками из частного сектора.

Мир, в котором частные компании создают и продают кибероружие, опаснее для потребителей, предприятий всех размеров и государственных учреждений. Эти вредоносные инструменты могут использоваться способами, который не соответствуют нормам и ценностям демократии. Корпорация Microsoft считает защиту прав человека важнейшим обязательством, к которому мы относимся серьезно, ограничивая применение модели «наблюдение как сервис» по всему миру.

Корпорация Microsoft оценила некоторых государственных субъектов в демократических и авторитарных режимах, передающих на аутсорсинг разработку или использование технологии «наблюдение как сервис». Так они избегают ответственности и надзора, а также получают возможности, которые сложно создавать у себя в стране.

Такое кибероружие предоставляет иностранным государствам возможности наблюдения, которые они не смогли бы разработать сами.

Рынок, на котором действуют кибернаемники, нельзя назвать прозрачным. Тем не менее мы продолжаем наблюдать, как эти группы используют эксплойты нулевого дня и даже эксплойты типа «zero-click», которые вообще не требуют взаимодействия с жертвой, что позволяет осуществлять наблюдение как сервис.

Недавно корпорация Microsoft объявила о европейском кибернаемнике, отслеживаемого как KNOTWEED, — австрийской кибергруппе DSIRF. Многочисленные новостные сообщения связывают компанию с разработкой и попыткой продажи набора инструментов вредоносного ПО Subzero⁵¹. К его жертвам относятся юридические фирмы, банки и стратегические консалтинговые компании в таких странах, как Австрия, Великобритания и Панама⁵².

Так как эти вредоносные программы для наблюдения не являются строго засекреченными, созданными оборонными и разведывательными агентствами средствами, а скорее коммерческими продуктами, которые продают компаниям и частным лицам, любой режим регулирования кибероружия должен выйти за рамки экспортного контроля. Воздействие такого кибероружия может быть разрушительным.

Когда кибер-наемник использует уязвимость в продукте или сервисе, он подвергает риску всю вычислительную экосистему. Когда о уязвимостях сообщают публично, компании стараются как можно быстрее выпустить исправление, до того как начнутся широкомасштабные атаки (см. наше предыдущее обсуждение использования уязвимостей). Это опасный и сложный цикл как для поставщиков ПО (которые должны быстро разрабатывать исправления), так и для потребителей продуктов (которые должны немедленно их установить).

Корпорация Microsoft как один из учредителей Cybersecurity Tech Accord⁵³ — ведущего альянса, объединяющего 150 технологических компаний, — взяла на себя обязательство не участвовать во вредоносных операциях в Интернете. Мы поддерживаемся этого обязательства и наших обязанностей в области прав человека. Мы занимаемся техническими сбоями и юридическими проблемами, чтобы подчеркнуть негативные последствия, вызванные сервисами кибернаемников, и будем продолжать защищать клиентов, когда обнаружим злоупотребления.

Кибернаемники создают и предоставляют возможности по модели «наблюдение как сервис» — это технологически сложными и широко доступные решения, использующие вредоносные программы и широкий спектр методов.

Практические рекомендации для государственных учреждений

- 1 Внедрите требования к прозрачности и надзора за применением модели «наблюдение как сервис», особенно в области закупок, включая запрет на взаимодействие с этими субъектами, как это сделало министерство торговли США, добавившее их в санкционный список юридических лиц.
- 2 Установите ограничения, действующие после трудоустройства, для бывших работников из этого сектора.
- 3 Выполняйте обязательства по проверке клиентов и убеждайте компании соблюдать обязательства в области прав человека.

Ссылки на дополнительную информацию

- > Распутывание клубка KNOTWEED: европейский злоумышленник из частного сектора использует эксплойты нулевого дня | Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), RiskIQ (Microsoft Defender Threat Intelligence)
- > Продолжение борьбы с кибероружием частного сектора | Microsoft On the Issues

Введение в действие норм кибербезопасности в интересах мира и безопасности в киберпространстве

Нам срочно требуется внедрить согласованную международную платформу, которая отдает приоритет правам человека и защищает людей от безрассудного поведения государств в Интернете. Нигде это не проявляется так сильно, как в продолжающейся войне в Украине. В дополнение к глобальным стратегическим усилиям, правительства могут принять меры уже сейчас, чтобы оказать немедленное положительное воздействие.

5 лет назад корпорация Microsoft призвала к созданию «Цифровой Женевской конвенции» для продвижения ответственности и обязательств между секторами по защите мира и безопасности в Интернете. Киберпространство становилось отдельной и нестабильной областью конфликтов и конкуренции между государствами, причем атаки становились все масштабнее даже в мирное время.

Сейчас по-прежнему есть острая потребность в такой платформе, что подтверждают российские кибератаки против Украины в рамках вторжения России. Эта война создала новую линию фронта, которая резко отличается от всего, что мы видели раньше.

Для обеспечения стабильности в киберпространстве потребуется укрепить и изменить институты глобального управления, чтобы сделать их пригодными для этой цели. Киберпространство принципиально отличается от других областей — это безграничная, синтетическая среда, которая в основном поддерживается частными компаниями.

Это значит, что необходимо обратиться к технологической отрасли с просьбой взять на себя большую ответственность как за безопасность продуктов и сервисов, так и за цифровую экосистему в целом. Хотя на всех фронтах был достигнут заметный прогресс, проблемы резко стали острее.

Мы должны удвоить коллективные усилия по защите безопасности в киберпространстве. Нельзя воспринимать права и свободы, которые мы привыкли ожидать в Интернете, как должное. Когда мы изо всех сил пытаемся решить проблемы, злоумышленники планируют свой следующий удар, используя искусственный интеллект, дезинформацию и ища способы подорвать молодую метавселенную. Правозащитники, технологическая индустрия и уважающие права человека правительства должны вместе разработать позитивную концепцию безопасного и надежного онлайн-мира. Этот путь будет долгим, но есть меры, которые правительства могут принять уже сейчас, чтобы немедленно улучшить экосистему кибербезопасности:

- Необходимо указывать нормативные акты, законы и последствия при публикации источников киберугроз. Одним из основных улучшений за последние 5 лет стала скорость и координация указания источников кибератак правительством. Вместо обычной публичной огласки и порицания в своих заявлениях необходимо подчеркнуть, какие международные законы или нормы нарушаются и какие последствия это предполагает, чтобы способствовать укреплению признания международных ожиданий.
- Уточнить толкование международного права в Интернете. Хотя правительства согласны с тем, что международное право применяется и в Интернете, при этом остаются вопросы о том, как оно действует в конкретных ситуациях. Это особенно актуально после вторжения в Украину. Правительства могут добиться многого для определения ожиданий, предотвращения

недоразумений и укрепления доверия, публично объявив, как они понимают свои обязательства по международному праву.

- Консультироваться с другими заинтересованными сторонами. По мере того как международные форумы продолжают выявлять лучшие способы содействия активному вовлечению многих заинтересованных сторон, правительства могут поддерживать эффективный диалог путем консультаций с сообществами с участием многих заинтересованных сторон, в частности с технологической индустрией, чтобы этот диалог приносил пользу тем, кто обладает уникальным опытом.
- Сформировать постоянный надзорный орган для поддержки ответственного поведения государств в киберпространстве. Работа международных дипломатических форумов по продвижению ответственного поведения государств в Интернете никогда не была такой важной. Существует очевидная необходимость в постоянном механизме ООН, позволяющего рассматривать киберпространство как область конфликта.
- Определить новые нормативные требования для развивающихся угроз. Угрозы в киберпространстве постоянно развиваются вместе с технологиями. Хотя международные нормы должны быть технологически нейтральными, их следует обновлять и корректировать в зависимости от изменений в среде угроз и того, как мы используем технологии. Даже сегодня мы наблюдаем случаи злоупотребления пробелами в существующих международных нормах. Государства должны взять на себя обязательство напрямую защищать базовые процессы, лежащие в основе цифровой экосистемы, которые сейчас не защищены, такие как процесс обновления ПО. Кроме того, отдельные области заслуживают дополнительной защиты. Например, как мы узнали во время пандемии, нормы защиты здравоохранения имеют важнейшее значение.

Объем и сложность атак национальных государственных кибергрупп продолжают расти, что создает опасную ситуацию.

Необходимы немедленные действия — есть меры, которые правительства могут принять уже сейчас, чтобы немедленно улучшить экосистему кибербезопасности, такие как внедрение согласованных норм и правил поведения государств в киберпространстве и сотрудничество с многосторонним сообществом для устранения возникающих недостатков.

Необходимо переосмыслить межотраслевые объединения для решения проблемы кибератак со стороны иностранных государств.

Ссылки на дополнительную информацию

- Момент расплаты: необходимость сильного и глобального ответа на киберугрозы | Microsoft On the Issues
- Кибератаки, нацеленные на здравоохранение, необходимо прекратить | Microsoft On the Issues
- Будущее кибердипломатии в ООН все ближе | Microsoft On the Issues

Концевые сноски

1. <https://www.microsoft.com/en-us/cybersecurity/content-hub/cloud-security>
2. <https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/>
3. Критически важная инфраструктура в этой главе определяется в соответствии с политической директивой 21 Президента США (PPD-21), Critical Infrastructure Security and Resilience (февраль 2013 г.).
4. <https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/>
5. <https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/>
6. <https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/>
7. <https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-passwordless-authentication>
8. <https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211>
9. <https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release>
10. <https://reliefweb.int/report/ukraine/unicef-ukraine-humanitarian-situation-report-no-13-10-17-may-2022>
11. <https://news.un.org/en/story/2022/06/1119672>
12. <https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r;>
<https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>
13. <https://www.cnn.com/2022/03/14/economy/china-jan-feb-economy-challenges-ahead-intl-hnk/index.html>
14. <https://www.wsj.com/articles/russias-vladimir-putin-meets-with-chinese-leader-xi-jinping-in-beijing-11643966743>
15. <https://www.washingtonpost.com/world/2022/04/01/china-eu-summit/>
16. <https://twitter.com/MoNDefense>
17. <https://news.usni.org/2022/01/24/2-u-s-aircraft-carriers-now-in-south-china-sea-as-chinese-air-force-flies-39-aircraft-near-taiwan>
18. [https://ec.europa.eu/trade/policy/in-focus/eu-china-agreement/;](https://ec.europa.eu/trade/policy/in-focus/eu-china-agreement/) <https://www.usnews.com/news/world/articles/2022-02-28/eu-plans-summit-with-china-on-april-1-to-address-tensions>
19. <https://www.wsj.com/articles/u-s-on-sidelines-as-china-and-other-asia-pacific-nations-launch-trade-pact-11641038401>
20. <https://greenfdc.org/chinas-two-sessions-2022-what-it-means-for-economy-climate-biodiversity-green-finance-and-the-belt-and-road-initiative-bri/>
21. <https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea>
22. <https://www.theguardian.com/world/2022/apr/30/the-china-solomons-security-deal-has-been-signed-time-to-move-on-from-megaphone-diplomacy>
23. https://www.fmprc.gov.cn/eng/zxxx_662805/202205/t20220531_10694928.html
24. [https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/;](https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/)
<https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/>
25. <https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/>
26. <https://attack.mitre.org/techniques/T1053/>
27. <https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/>
28. <https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/>
29. [https://www.timesofisrael.com/in-rare-criticism-of-irgc-rouhani-slams-anti-israel-slogans-on-test-missiles/;](https://www.timesofisrael.com/in-rare-criticism-of-irgc-rouhani-slams-anti-israel-slogans-on-test-missiles/) <https://www.theguardian.com/world/2017/may/05/iran-president-hassan-rouhani-nuclear-agreement-sabotaged;> [https://d2071andvip0wj.cloudfront.net/184-iran-s-priorities-in-a-turbulent-middle-east_1.pdf;](https://d2071andvip0wj.cloudfront.net/184-iran-s-priorities-in-a-turbulent-middle-east_1.pdf) [https://www.aljazeera.com/news/2016/3/9/iran-launches-ballistic-missiles-during-military-drill;](https://www.aljazeera.com/news/2016/3/9/iran-launches-ballistic-missiles-during-military-drill) [https://www.usatoday.com/story/news/world/2015/04/25/iran-yemen-weapons/26367493/;](https://www.usatoday.com/story/news/world/2015/04/25/iran-yemen-weapons/26367493/) [https://www.armscontrol.org/blog/ArmsControlNow/2016-03-14/The-Iranian-Ballistic-Missile-Launches-That-Didnt-Happen;](https://www.armscontrol.org/blog/ArmsControlNow/2016-03-14/The-Iranian-Ballistic-Missile-Launches-That-Didnt-Happen) [https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/;](https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/)
30. [https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/;](https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/) <https://www.france24.com/en/live-news/20210825-iran-s-parliament-approves-president-s-cabinet-choices>

Продолжение концевых сносок

31. <https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-inintelligence-operations>; <https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential>; <https://miburo.substack.com/p/iran-disinfo-privatized?s=r>.
32. <https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/>
33. <https://www.tasnimnews.com/en/news/2021/11/05/2602361/us-military-action-off-the-table-iranian-general>
34. В частности, исправлены уязвимости ProxyShell (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 и CVE-2021-27065, CVE-2021-34473) серверов Exchange. Кроме того, обязательно установите исправления для уязвимостей VPN-устройств Fortinet FortiOS SSL.
35. <https://docs.microsoft.com/en-us/microsoft-365/commerce/manage-partners?view=o365-worldwide>
36. <https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/>
37. <https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/>
38. <https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign>
39. <https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/>
40. <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-baselines-microsoft-defender-antivirus?view=o365-worldwide>
41. <https://docs.microsoft.com/microsoft-365/security/defender-endpoint/cloud-protection-microsoft-defender-antivirus>
42. <https://docs.microsoft.com/microsoft-365/commerce/manage-partners?view=o365-worldwide>
43. <https://www.marketwatch.com/story/kim-jong-un-calls-for-improved-living-conditions-in-north-korea-01633920099>
<https://www.bbc.com/news/world-asia-59845636>
<https://kcnawatch.org/newstream/1650963237-449932111/respected-comrade-kim-jong-un-makes-speech-at-military-parade-held-in-celebration-of-90th-founding-anniversary-of-kpra/>
44. <https://www.theguardian.com/world/2021/aug/06/north-korea-homes-wreckeddamaged-and-bridges-washed-away-in-floods>
45. <https://www.reuters.com/world/asia-pacific/nkorea-mobilises-office-workers-fight-drought-amid-food-shortages-2022-05-04/>
46. https://www.washingtonpost.com/world/asia_pacific/north-korea-kim-pandemic/2021/09/08/31adfd74-ff53-11eb-87e0-7e07bd9ce270_story.html
47. <https://news.yahoo.com/china-halts-freight-train-traffic-102451425.html>
48. <https://www.cnn.com/2022/05/11/asia/north-korea-covid-omicron-coronavirus-intl-hnk/index.html>
49. <https://www.csis.org/analysis/number-north-korean-defectors-drops-lowest-level-two-decades>
50. <https://www.aljazeera.com/economy/2022/5/20/north-korea-shuns-outside-help-as-covid-catastrophe-looms>
51. Ян-Филипп Хайн (Jan-Philipp Hein), In the mystery of creepy spy software, the trail leads via Wirecard to the Kremlin, FOCUS Online, (2022), https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html; Шугар Миззи (Sugar Mizzy), We unveil the “Subzero” state trojan from Austria, Europe-cities (2021), <https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/>; Андре Майстер (Andre Meister), We unveil the state Trojan “Subzero” from Austria, Netzpolitik.org (2022), <https://netzpolitik.org/2021/dsif-wir-enthuellenden-staatstrojaner-subzero-aus-oesterreich>.
52. Как отмечается в нашем техническом блоге, обнаружение целей в определенной стране не обязательно означает, что клиент DSIRF находится в той же стране, так как часто цели находятся в разных странах.
53. Home | Cybersecurity Tech Accord (cybertechaccord.org)

Устройства и инфраструктура

С ускорением цифровой трансформации безопасность цифровой инфраструктуры становится важной как никогда.

Обзор устройств и инфраструктуры	57
Введение	58
Правительства, принимающие меры по повышению безопасности и устойчивости критически важной инфраструктуры	59
Уязвимости IoT и OT: тенденции и атаки	62
Взлом цепочки поставок и встроенного ПО	65
Обзор уязвимостей встроенного ПО	66
Разведывательные атаки на OT-устройства	68

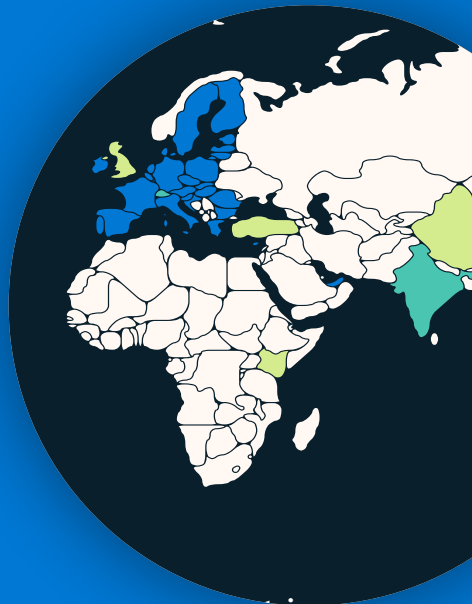
Обзор

устройств и инфраструктуры

Быстрое внедрение устройств с доступом в Интернет ускорило цифровую трансформацию, а пандемия значительно расширила возможные направления атак на цифровой мир.

И киберпреступники, и иностранные государства быстро пытаются воспользоваться этим. Безопасность ИТ-оборудования и ПО укрепились за последние годы, но устройства Интернета вещей (IoT) и операционных технологий (OT) не поспевают за ними. Злоумышленники используют такие устройства для доступа к сетям и горизонтального перемещения, чтобы закрепиться в цепочке поставок или нарушить OT-операции целевой организации.

Правительства во всем мире переходят к защите критически важной инфраструктуры, улучшая безопасность IoT и OT.

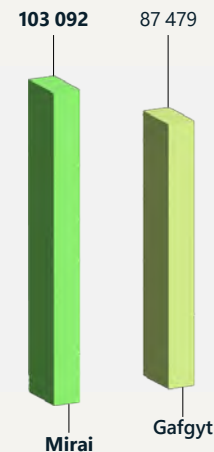


[Подробнее на стр. 59](#)

Для повсеместного внедрения средств защиты необходимы согласованные и совместимые на глобальном уровне политики безопасности.

[Подробнее на стр. 59](#)

Использование модели «вредоносное ПО как сервис» переросло в масштабные операции против уязвимых IoT- и OT-устройств в инфраструктуре, коммунальных и корпоративных сетях.



[Подробнее на стр. 63](#)

Число атак на устройства с удаленным управлением растет: в мае 2022 года было зарегистрировано свыше 100 миллионов атак, что в 5 раз больше, чем в прошлом году.

[Подробнее на стр. 62](#)



Злоумышленники все чаще применяют уязвимости встроенного ПО устройств IoT для проникновения в корпоративные сети и проведения разрушительных атак.

[Подробнее на стр. 65](#)

32 % проанализированных образцов встроенного ПО содержали как минимум 10 известных критических уязвимостей.



[Подробнее на стр. 66](#)

Введение

Ускорение цифровой трансформации увеличило риски кибербезопасности для критически важной инфраструктуры и киберфизических систем.

За последние годы в цифровом мире произошли невиданные ранее изменения. Организации трансформируются, чтобы использовать достижения в области вычислительной техники, такие как интеллектуальное облако и интеллектуальные технологии. Из-за пандемии компании были вынуждены ускорить цифровую трансформацию, чтобы выжить и соответствовать темпам внедрения устройств, подключенных к Интернету, что привело к росту возможных направлений атак в геометрической прогрессии.

Сообщество специалистов по безопасности оказалось неспособно поспеть за такой быстрой миграцией. В прошлом году мы наблюдали угрозы, использующие устройства во всех частях организации — от традиционного ИТ-оборудования до контроллеров операционных технологий (ОТ) или простых датчиков Интернета вещей (IoT). Хотя безопасность ИТ-оборудования в последние годы усилилась, но об IoT- и ОТ-устройствах этого сказать нельзя. Злоумышленники используют такие устройства для доступа к сетям и горизонтального перемещения, чтобы нарушить ОТ-операции целевой организации. Мы видели атаки на электросети, атаки программ-шантажистов, нарушающие ОТ-операции, использование маршрутизаторов IoT для сохранения присутствия в сети и атаки, нацеленные на уязвимости встроенного ПО.

Распространенность уязвимостей IoT и ОТ — это проблема для всех организаций, но критически важная инфраструктура подвергается повышенному риску, так как злоумышленники поняли, что отключение базовых сервисов служб является мощным рычагом давления. Атака программы-шантажиста на Colonial Pipeline Company в 2021 году показала, как киберпреступники могут прервать работу критически важной службы, чтобы повысить вероятность получения выкупа. Кибератаки России против Украины демонстрируют, что некоторые государства рассматривают кибератаки на критически важную инфраструктуру как приемлемый метод саботажа для достижения своих военных целей.

Однако надежда все-таки есть. Политики и специалисты по защите сетей стараются улучшить кибербезопасности критически важной инфраструктуры, в том числе устройств IoT и ОТ, на которые они полагаются. Законодатели ускоряют разработку законов и нормативных актов для укрепления общественного доверия к кибербезопасности критически важной инфраструктуры и устройств.

Корпорация Microsoft сотрудничает с правительствами по всему миру, чтобы воспользоваться этой возможностью для укрепления кибербезопасности, и мы приветствуем возросшую вовлеченность с этой стороны. Однако нас беспокоит то, что непоследовательные, индивидуальные или слишком сложные требования могут оказать непреднамеренные последствия, такие снижение уровня безопасности в некоторых случаях за счет отвлечения и без того скудных ресурсов безопасности на соблюдение нескольких дублирующихся сертификатов.

С точки зрения безопасности защитники сети используют несколько подходов к улучшению уровня безопасности IoT и ОТ в своей организации. Один из них — это внедрение непрерывного мониторинга устройств IoT и ОТ. Другой подход — это «сдвиг влево», то есть требование и внедрение передовых методов кибербезопасности для самих устройств IoT и ОТ. Третий подход состоит в реализации решения для мониторинга безопасности, которое охватывает как ИТ-, так и ОТ-сети. Такой комплексный дает существенное преимущество, поддерживая критически важные организационные процессы, такие как устранение разрозненности между ОТ и ИТ, что, в свою очередь, позволяет организации повысить уровень безопасности и одновременно достичь бизнес-целей.

Михал Браверман-Блюменстик (Michal Braverman-Blumenstyk)

Корпоративный вице-президент, технический директор, подразделение безопасности облачных технологий и искусственного интеллекта

Правительства, принимающие меры по повышению безопасности и устойчивости критически важной инфраструктуры

Правительства во всем мире разрабатывают и развивают политики управления рисками кибербезопасности для критически важной инфраструктуры. Многие из них также принимают политики для укрепления безопасности устройств IoT и ОТ. Глобальная волна политических инициатив открывает огромные возможности для улучшения кибербезопасности, но также создает проблемы для заинтересованных сторон во всей экосистеме.

Разработка комплексного представления об управлении киберрисками критически важной инфраструктуры имеет решающее значение, но это сложная задача, особенно взаимосвязь между технологиями и глобальными поставщиками, диапазон использования технологий и связанных с ними рисков, а также необходимость инвестиций как в краткосрочные, так и в долгосрочные стратегии. Политики с оптимальной областью действия, которые стимулируют последовательное обучение и улучшение, а также поддерживают глобальную межотраслевую совместимость, помогут справиться с трудностями и осуществить безопасную цифровую трансформацию. Но фрагментарный подход к законодательству может привести к дублированию

и непоследовательности нормативных требований. Это может сказаться на ресурсах и, в конечном итоге, помешать достижению целей в области безопасности. Например, вместо инноваций и обеспечения безопасности организации могут выделять ресурсы на формальные мероприятия по обеспечению соответствия.

Корпорация Microsoft стремится сотрудничать с правительствами по всему миру для создания эффективных политик кибербезопасности критически важной инфраструктуры, углубленного понимания проблем и возможностей, а также поддержки инициатив, направленных на улучшение защиты от коллективных рисков.

Развитие политик управления рисками кибербезопасности критически важной инфраструктуры

В прошлом году несколько юрисдикций, в том числе Австралия, Чили, Европейский союз (ЕС), Япония, Сингапур, Соединённое Королевство и США, разработали, обновили или ввели в действие межотраслевые или отраслевые требования к кибербезопасности¹. Многие из них, а также другие правительства, такие как Индия² и Швейцария³, уже выпустили или разрабатывают требования к отчетности об инцидентах кибербезопасности для критически важной инфраструктуры и поставщиков базовых сервисов⁴.

В прошлом году в Австралии, ЕС, Индонезии и США произошел ряд важных политических событий. Австралия приняла 2 закона для управления межотраслевыми рисками кибербезопасности критически важной инфраструктуры. Среди прочего, в них определяются новые сектора критически важной инфраструктуры, требования к разработке планов управления рисками и отчетности об инцидентах кибербезопасности. Они дают правительству возможность вмешиваться, если будет определено, что оператор критически важной инфраструктуры не желает или не может адекватно реагировать на инцидент.



ЕС работал над обновлением Директивы NIS 2016 года, которая закладывает основу для регулирования технологических сервисов и продуктов, считающихся критически важными для экономики и функционирования общества государствах-членах ЕС. Предлагаемая директива NIS 2 содержит изменения, определяющие новую категорию критически важной цифровой инфраструктуры, строгие требования к отчетности о киберинцидентах и дополнительные требования к управлению рисками кибербезопасности. ЕС также разработал предлагаемое обновление к Закону о цифровой операционной устойчивости (DORA), вводя новые требования к информационно-коммуникационным технологиям, используемым в секторе финансовых услуг.

В мае Индонезия выпустила президентское постановление о защите критически важной информационной инфраструктуры («IIV»), которое вступит в силу в мае 2024 года и охватит такие сектора, как энергетика, транспорт, финансы и здравоохранение. Цель этого законодательного акта — защитить непрерывность внедрения IIV, предотвратить кибератаки и повысить готовность к реагированию на киберинциденты. Поставщики IIV будут нести ответственность за обеспечение надежной защиты, внедрение эффективного управления киберрисками и информирование о результатах кибератак соответствующим государственным органам. Постановление включает в себя требование сообщать о киберинцидентах в течение 24 часов.

Правительства, принимающие меры по повышению безопасности и устойчивости критически важной инфраструктуры

Продолжение

Конгресс США принял закон, который уполномочил Агентство кибербезопасности и безопасности инфраструктуры (CISA) США издавать нормативные акты, требующие отчетности о киберинцидентах от операторов критически важной инфраструктуры, а Администрация транспортной безопасности (TSA) США выпустила новые отраслевые требования к кибербезопасности в транспортном секторе. В 2021 году TSA выпустила 2 директивы безопасности для операторов трубопроводов опасных жидкостей и природного газа в ответ на атаку вымогателей на Colonial Pipeline Company:

- Первая директива требует, чтобы операторы назначали координатора по кибербезопасности, сообщали о киберинцидентах в течение 12 часов и проводили оценку уязвимости своих систем.
- Вторая директива, которую TSA пересмотрела в 2022 году, требовала от них принятия конкретных мер по смягчению последствий для защиты от атак программ-шантажистов и других известных угроз для ИТ- и ОТ-систем, разработки и реализации плана реагирования на чрезвычайные ситуации и реагирования в области кибербезопасности в течение 30 дней и проведения ежегодной проверки проекта архитектуры кибербезопасности.

Основываясь на нормативных требованиях для трубопроводов, администрация TSA выпустила 2 дополнительные директивы безопасности позже в 2021 году, которые содержали требования к кибербезопасности для грузовых железнодорожных, пассажирских железнодорожных перевозчиков и железнодорожных транзитных систем. Директивы требовали, чтобы соответствующие операторы назначали координаторов по кибербезопасности, сообщали об инцидентах кибербезопасности в течение 24 часов, разработали и внедрили план реагирования на инциденты кибербезопасности и проводили оценку уязвимостей системы кибербезопасности. Одновременно в TSA объявили, что в программы авиационной безопасности были добавлены требования к операторам аэропортов и авиакомпаний выполнять первые 2 положения (назначить координатора и сообщать об инцидентах в течение 24 часов).

Развитие политик безопасности устройств IoT и ОТ

Правительства десятков стран активно разрабатывают требования для повышения кибербезопасности продуктов и сервисов информационно-коммуникационных технологий (ИКТ), в том числе устройств IoT и ОТ. Наибольшими проблемами для продуктов и сервисов ИКТ являются безопасность цепочки поставок ПО и безопасность IoT.

- Европейская комиссия предложила Закон о киберустойчивости, который определит требования к кибербезопасности для автономного ПО, подключенных устройств и вспомогательных сервисов⁵. Соответствующими методами для поставщиков ПО являются использование безопасного жизненного цикла разработки ПО⁶ и предоставление спецификации ПО⁷.

Новые требования к безопасности будут применяться к подключенным устройствам, и всем производителям потребуется управлять скоординированными процессами раскрытия уязвимостей⁸ для выпущенных продуктов.

Законодатели уделили внимание распространению устройств IoT и устройств ОТ, подключенных к сети.

- Законопроект о безопасности продуктов и телекоммуникационной инфраструктуры в Великобритании потребует от производителей потребительских подключаемых к сети продуктов, таких как телевизоры Smart TV, прекратить использование паролей по умолчанию, которые становятся легкой мишенью для киберпреступников, сформулировать политику раскрытия уязвимостей (например, способ получения уведомления о недостатках системы безопасности) и обеспечить прозрачность в отношении минимального периода времени, в течение которого они будут предоставлять обновления системы безопасности⁹.
- В ЕС внедряются новые стандарты или требования к безопасности с помощью нескольких законодательных инструментов, таких как делегированный акт для Директиве о радиооборудовании, который применяется к беспроводным устройствам и направлен на повышение устойчивости сети, защиту конфиденциальности потребителей и снижение риска мошенничества с денежными средствами¹⁰. Кроме того, может потребоваться использование схемы облачной сертификации¹¹, которая сейчас разрабатывается после принятия Закона ЕС о кибербезопасности 2019 года¹².

Необходимость согласованности

Во многих случаях законодательные инициативы в различных регионах, секторах, технологических областях и областях управления операционными рисками разрабатываются одновременно. Это приводит к потенциальному дублированию усилий или непоследовательности в области охвата, требований и затрудняет ситуацию для организаций, которые хотят соблюдать требования или продемонстрировать соответствие. Без общепринятого определения IoT область применения особенно сложна для нормативных требований для устройств IoT и ОТ. Приведенные выше примеры могут быть применимы к «подключенным к сети продуктам и вспомогательным сервисам», «потребительским подключаемым продуктам» и «беспроводным устройствам». В то же время многие правительства стремятся внедрить надежные режимы оценки, чтобы лучше понять, соответствуют ли организации и продукты текущим и новым требованиям и как они смогут их соблюдать. По мере объединения этих тенденций сложность будет только расти. Обнадешивает то, что вопросы, заданные в ходе консультаций по Закону о киберустойчивости ЕС, затронули то, как новые нормативные требования могут взаимодействовать с существующими нормативными актами в области кибербезопасности, чтобы избежать появления конфликтующих требований.

Итеративные подходы, основанные на рисках и ориентированные на результат или процесс (в отличие от ориентированных на конкретные реализации), помогут повысить уровень кибербезопасности и будут способствовать непрерывному совершенствованию. Аналогичным образом акцент на обеспечении совместимости между секторами, регионами и областями политик позволит последовательно повышать уровень кибербезопасности во взаимосвязанных глобальных цепочках поставок.

Правительства, принимающие меры по повышению безопасности и устойчивости критически важной инфраструктуры

Продолжение

Сейчас в разных регионах, секторах и отраслях разрабатываются политики кибербезопасности критически важной инфраструктуры, которые становятся все сложнее. Эта открывает прекрасные возможности, но и создает серьезные проблемы. То, как будут действовать правительства, окажет решающее значение на будущее цифровой трансформации и безопасность всей экосистемы.

Ускорение инвестиций в масштабах всей экосистемы в безопасность цепочки поставок ПО и архитектуру «Никому не доверяй»

Указ Президента США (EO) 14028 об улучшении кибербезопасности стал катализатором для ускорения текущих инициатив корпорации Microsoft по совершенствованию безопасности цепочки поставок нашей компании и экосистемы в целом, чтобы позволить нашим клиентам реализовать принцип «Никому не доверяй».

Мы давно считаем, что для улучшения цепочки поставок ПО требуются необходимые знания и рекомендации — начиная с публикации жизненного цикла разработки безопасности Microsoft около 15 лет назад.

Кроме того, мы тесно сотрудничаем с National Cybersecurity Center of Excellence, чтобы продемонстрировать подходы к архитектуре «Никому не доверяй», применяемые как к локальным, так и к облачным технологиям, и чтобы создать новые возможности продуктов, такие как принудительная аутентификация в гибридных и мультиоблачных средах для защиты от фишинга.

Сегодня мы выходим за рамки требований указа Президента США по демонстрации соответствия требованиям к безопасности цепочки поставок ПО и предоставлению информации о спецификации ПО 2 способами:

1. Мы публикуем версию генератора спецификации ПО с открытым исходным кодом, который мы создали для простой интеграции с конвейерами CI/CD. Инструмент поддерживает сборки на платформах Windows, Linux, Mac, iOS и Android¹³.
2. Мы вносим свой вклад в разработку отраслевых стандартов целостности, прозрачности и доверия в цепочке поставок (SCITT). Это позволит автоматизировать обмен поддающейся проверке информацией о цепочке поставок, такой как артефакты, которые подтверждают соответствие требованиям, в том числе представленным в руководстве по цепочке поставок ПО, описанном в указе Президента США.

Практические рекомендации

1. Необходимо переосмыслить межотраслевые объединения для решения проблемы кибератак со стороны иностранных государств.
2. Разработайте политики кибербезопасности, согласованные и совместимые между различными регионами, секторами и областями.

Ссылки на дополнительную информацию

- > Продолжение инвестиций в безопасность цепочки поставок в поддержку указа Президента США о кибербезопасности | Техническое сообщество Microsoft
- > Правительство США устанавливает стратегию и требования к архитектуре «Никому не доверяй» | Блог Microsoft Security
- > CYBER EO | Microsoft Federal
- > Supply Chain Integrity, Transparency, and Trust | github.com
- > Implementing a Zero Trust Architecture | NCCoE (nist.gov)

Уязвимости IoT и OT: тенденции и атаки

В эпоху повсеместного подключения сети устройства быстро подключаются к Интернету, взаимодействуя с крупными системами, собирая данные и обеспечивая прозрачность в ранее невидимых областях. Это открывает возможности как для организаций, так и для злоумышленников. При этом киберпреступность становится многомиллиардной индустрией — и многомиллиардным риском для бизнеса.

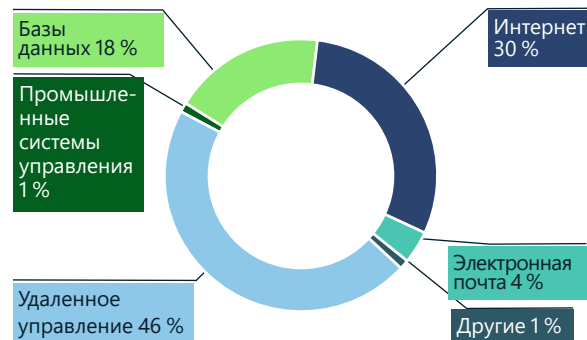
Устройства IoT — от принтеров и веб-камер до устройств климат-контроля и систем контроля доступа к зданиям — создают уникальные риски безопасности для отдельных лиц, организаций и сетей. Многие организации просто не могут работать без них, однако они могут быстро превратиться в угрозу безопасности и стать причиной судебного разбирательства. Быстрое внедрение IoT-решений практически во всех отраслях расширило возможные направления атаки и увеличило риск для организаций.

Использование модели «вредоносное ПО как сервис» переросло в масштабные операции против гражданской инфраструктуры и коммунальных услуг (среди целей — больницы, нефтегазовые предприятия, электрические сети, транспортные компании и другая критически важная инфраструктура), а также корпоративных сетей. Злоумышленникам приходится прилагать значительные усилия для выявления и взлома конфигурации операционных сред и встроенных устройств IoT и OT.

Устройства IoT создают уникальные риски безопасности, так как их можно использовать как точки входа и сохранения присутствия в сети. Миллионы устройств IoT не содержат исправлений или предоставляют открытый доступ.

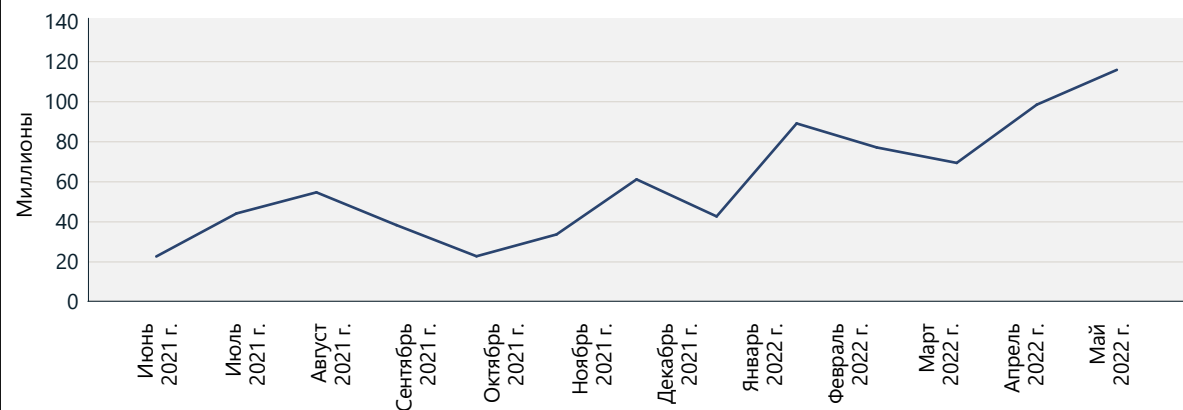
Устройства с открытым доступом можно обнаружить с помощью инструментов поиска в Интернете, определив сервисы, прослушивающие открытые сетевые порты. Эти порты часто используются для удаленного управления устройствами. Без правильной защиты открытое для доступа устройство IoT может использоваться как точка входа на другой уровень корпоративной сети, так как неавторизованные пользователи могут удаленно получать доступ к портам. Мы видели множество злоумышленников, пытающихся использовать уязвимости в устройствах, доступным из Интернета, начиная от камер до маршрутизаторов и термостатов. Однако несмотря на риски миллионы устройств остаются уязвимыми или открытыми для доступа.

Обзор типов атак на IoT/OT



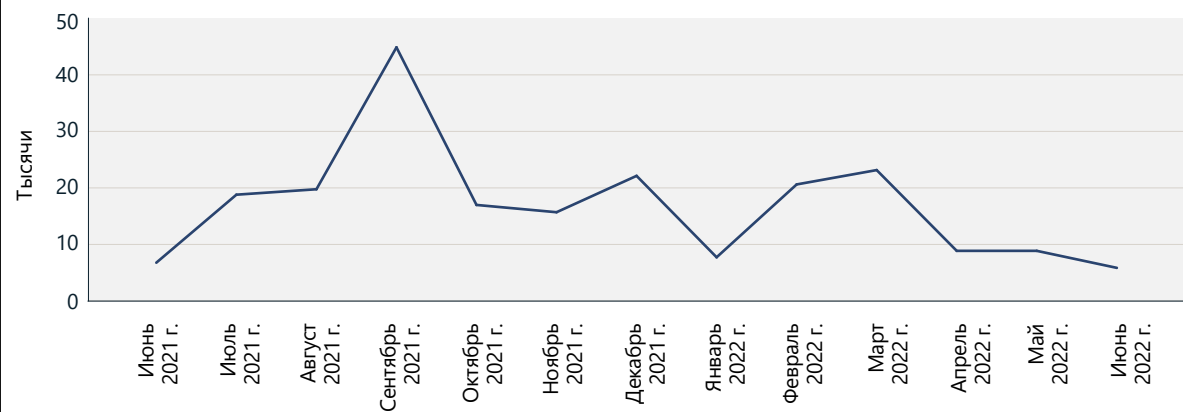
Типы атак, обнаруженные с помощью сети датчиков MSTIC. Самыми распространенными были атаки на устройства с удаленным управлением, атаки через Интернет и атаки на базы данных (метод прямого перебора или эксплойты).

Атаки на устройства с удаленным управлением



С течением времени число атак на порты удаленного управления растет, что демонстрируют данные сети датчиков MSTIC.

Веб-атаки на IoT и OT



Объем веб-атак с течением времени, видимый с помощью сети датчиков MSTIC. Так как число устройств, напрямую подключенных к Интернету, продолжает снижаться, возможности злоумышленников для их обнаружения будут ограничены.

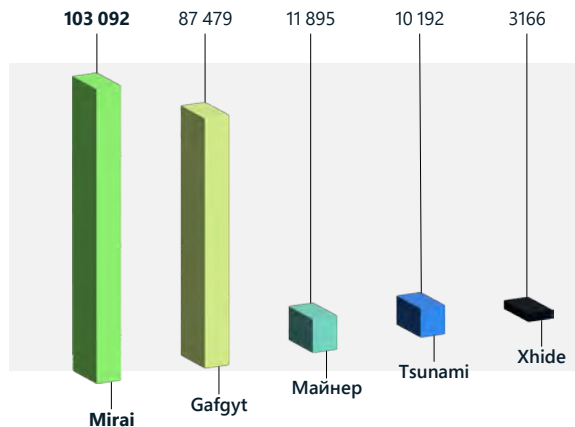
Уязвимости IoT и OT: тенденции и атаки

Продолжение

Обновленное вредоносное ПО

Группы киберпреступности развиваются и меняют способы развертывания вредоносного ПО и выбора целей. В прошлом году мы обнаружили, что число атак на обычные протоколы IoT, такие как Telnet, существенно сократилось — в некоторых случаях до 60 %. В то же время киберпреступники и национальные кибергруппы перепрофилировали ботнеты под новые задачи. Сохранение вредоносных программ, таких как Mirai, в системах подчеркивает модульный характер этих атак и возможности адаптации существующих угроз.

Основные вредоносные программы IoT, обнаруженные в ИТ-средах



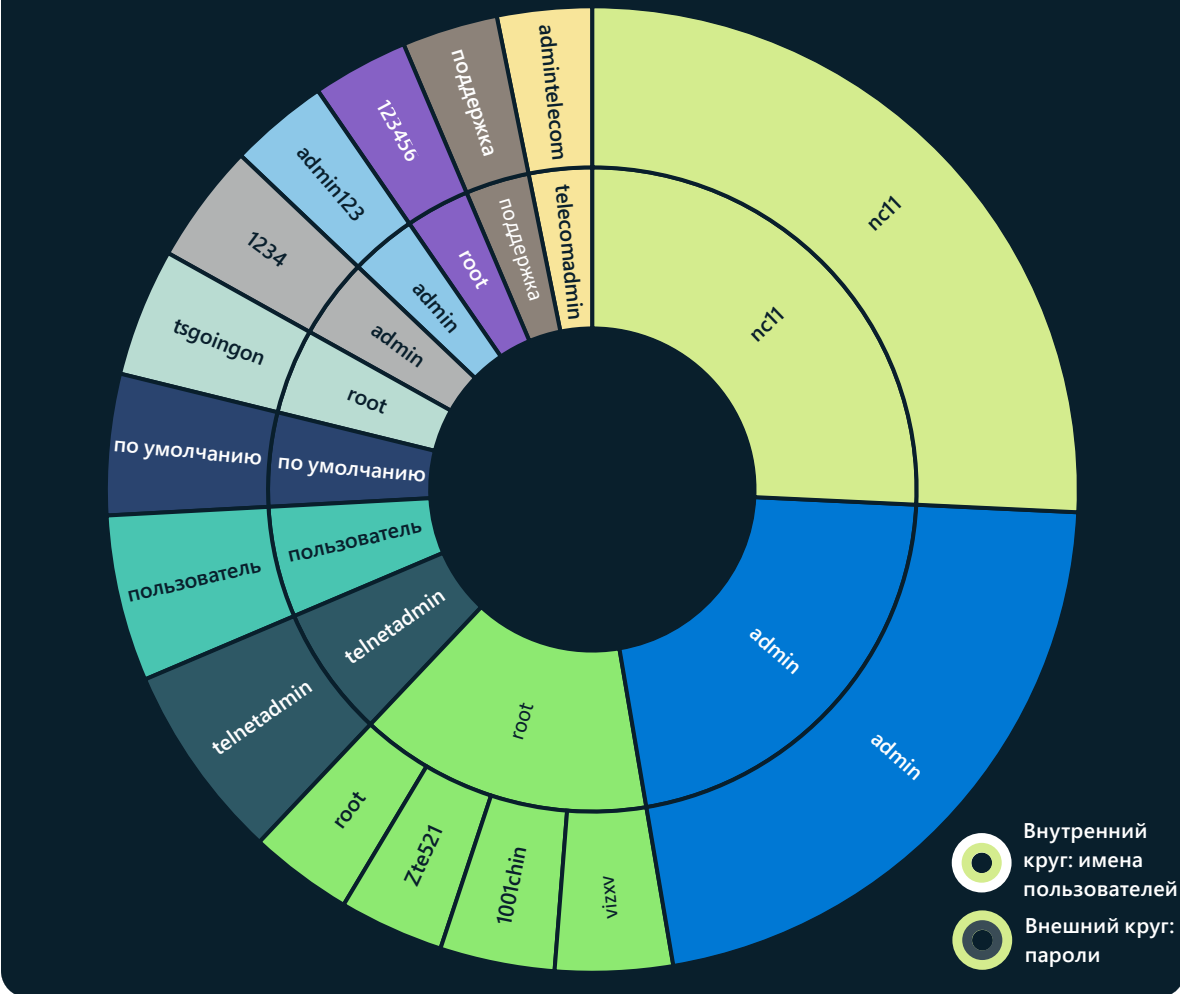
Вредоносная программа Mirai была изменена для заражения широкого спектра устройств IoT, таких как IP-камеры, цифровые видеорегистраторы систем видеонаблюдения и маршрутизаторы. Вектор атаки вышел за пределы устаревших средств управления безопасностью и теперь направлен на конечные точки в сети. Злоумышленники используют дополнительные уязвимости и перемещаются по сети горизонтально. Вредоносная программа Mirai была несколько раз переработана для создания вариантов, адаптированным к различным архитектурам и использующим как известные уязвимости, так и уязвимости нулевого дня для применения новых векторов атак.

За последний год использование Mirai выросло как среди 32-, так и среди 64-разрядных архитектур процессоров x86. Эта вредоносная программа получила новые возможности, которые быстро начали использовать национальные кибергруппы и киберпреступники. Национальные кибергруппы теперь используют новые варианты существующих ботнетов в распределенных атаках типа «отказ в обслуживании» (DDoS) на иностранных противников.

Так как прибыль от атак на устройства IoT в 2022 году снизилась, мы обнаружили, что несколько групп злоумышленников используют уязвимости, такие как Log4j и Spring4Shell, для доставки вредоносной полезной нагрузки на такие устройства, как серверы, заражая и добавляя их в крупные ботнеты, осуществляющие DDoS-атаки. Обновленное вредоносное ПО, предназначенного для атаки на уязвимые устройства IoT, вызывает серьезные последствия как для организаций, так и для целых стран, так как горизонтальное перемещение может создать бэкдор для дополнительной полезной нагрузки и доступ к другим устройствам в сетях.

Многие протоколы промышленных систем управления не отслеживаются, поэтому они уязвимы для атак на OT-устройства. Это может привести к повышенному риску для критически важной инфраструктуры.

Относительная распространенность пар имени пользователя и пароля, наблюдаемых на устройствах IoT/OT в сигналах датчиков за 45 дней



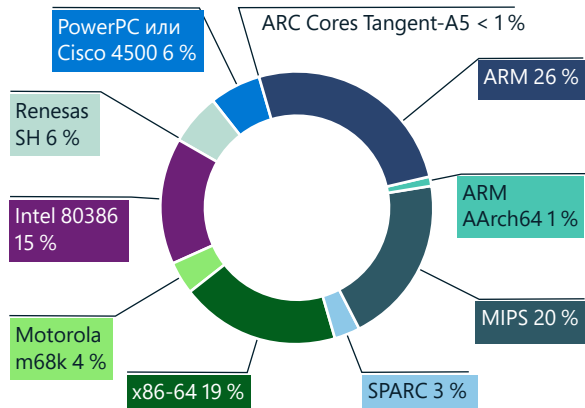
Использование распространенных пар имени пользователя и пароля повышает риск взлома. 20 % из 39 миллионов устройств IoT и OT используют идентичные имена пользователей и пароли.

Уязвимости IoT и OT: тенденции и атаки

Продолжение

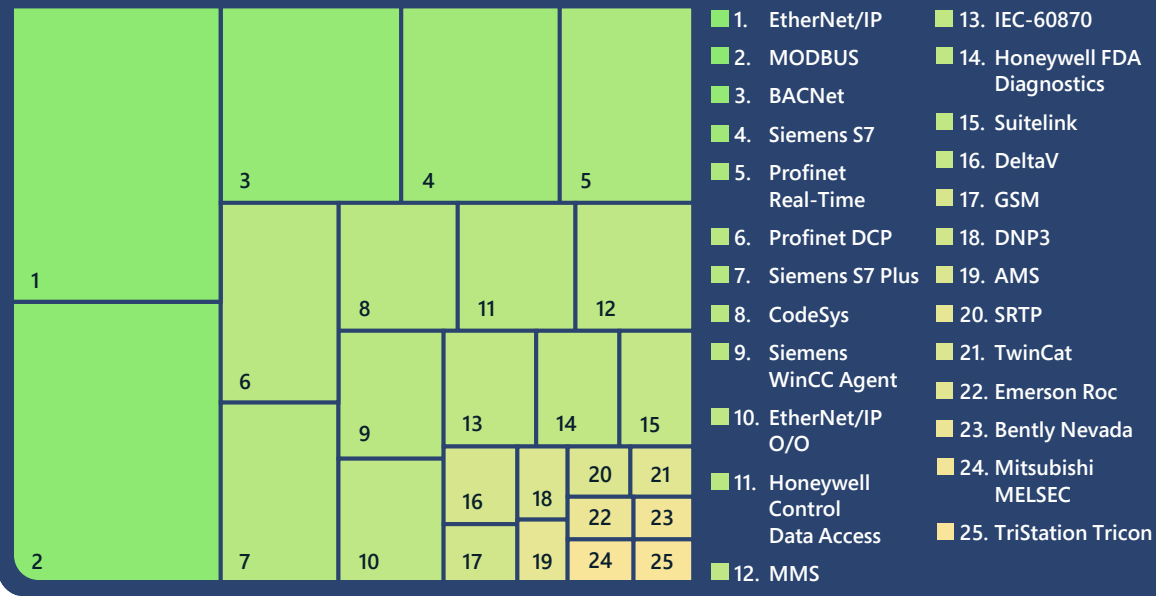
Слабые конфигурации и стандартные учетные данные по умолчанию по-прежнему представляют опасность для сетей, но корпорация Microsoft наблюдала множество веб-эксплоитов, использующих протокол HTTP. Мы видели рост числа атак на веб-сервисы с использованием старых ботнетов. В то же время уменьшилось число открытых портов telnet в Интернете — это положительный сигнал для сетевой безопасности, так как ботнеты, которые ранее представляли риск для устройств, теряют свою актуальность. Несмотря на это мы все еще наблюдали постоянные ботнеты в сетях датчиков.

Распространение вредоносных программ Интернета вещей с использованием уязвимостей архитектуры ЦП



Корпорация Microsoft отметила, что устройства Интернета вещей на базе процессоров ARM больше всего подвержены заражению вредоносным ПО, за которыми следуют архитектуры MIPS, X86-64 и процессор Intel 80386.

Распространенность протокола промышленных систем управления



Уязвимости протокола промышленных систем управления

Мы изучили операционные данные с облачных датчиков, обнаружив самые распространенные протоколы промышленных систем управления (ICS). Они дают представление о характере этих устройств и возможных направлениях атак. Это особенно актуально для обеспечения безопасности критически важной инфраструктуры. Вот некоторые из главных выводов:

1. Большинство протоколов проприетарные, поэтому стандартные инструменты мониторинга ИТ-среды не обеспечивают требуемую прозрачность для этих устройств и протоколов. В результате сети остаются без мониторинга, что делает их уязвимыми к атакам, специфичным для операционных технологий.

2. Существует множество различных протоколов, зависящих от поставщика. Это значит, что решения по обеспечению безопасности конкретных поставщиков не смогут охватить всю сеть полностью. Корпорация Microsoft делает ставку на подход, не зависящий от поставщика, чтобы защитить широкий спектр различных устройств.
3. Организации должны убедиться, что эти протоколы не будут доступны непосредственно в Интернете из их сетей. Такая доступность может создать серьезную угрозу безопасности из-за уязвимостей и слабой защиты этих протоколов.

Вредоносные программы, такие как Mirai, сохраняется в среде за счет добавления новых возможностей и внедряется киберпреступниками и национальными кибергруппами с помощью новых вариантов существующих ботнетов, проводящих DDoS-атаки на иностранных противников.

Практические рекомендации

1. Убедитесь, что устройства надежны, устанавливая исправления, изменяя пароли по и порты SSH по умолчанию.
2. Сократите возможные направления атаки, удалив ненужные интернет-соединения и открытые порты, ограничив удаленный доступ, блокируя порты, запрещая удаленный доступ и используя VPN-сервисы.
3. Используйте сетевое решение для обнаружения и реагирования с поддержкой IoT/OT и систему управления информацией о безопасности и событиях (SIEM)/оркестрации безопасности и автоматизации реагирования (SOAR) для отслеживания аномального или несанкционированного поведения устройств, такого как взаимодействие с неизвестными хостами.
4. Сегментируйте сети, чтобы ограничить возможность горизонтального перемещения злоумышленников и компрометации ресурсов после первоначального вторжения. Устройства IoT и OT-сети должны быть изолированы от корпоративных ИТ-сетей с помощью брандмауэров.
5. Убедитесь, что протоколы промышленных систем управления не доступны напрямую из Интернета.

Взлом цепочки поставок и встроенного ПО

Почти у любого устройства, подключенного к Интернету, есть встроенное ПО. Это специальная программа, закодированная в оборудование или печатную плату устройства. За последние несколько лет мы видим все больше попыток взлома встроенного ПО для проведения масштабных атак. Так как встроенное ПО, скорее всего, останется ценной мишенью для злоумышленников, организации должны защитить его от взлома.

Встроенное ПО реализует основные функции устройства, такие как подключение к сети и хранение данных. Оно есть в маршрутизаторах, камерах, телевизорах и других устройствах, используемых предприятиями (IoT), наряду с промышленным управляющим оборудованием (OT), используемым в критически важной инфраструктуре. Так сложилось, что встроенное ПО разрабатывали, применяя незащищенный код, что создает значительные уязвимости, которые могут использоваться для захвата контроля над устройством или внедрения вредоносного кода.

Этот риск становится еще серьезнее, когда дело доходит до цепочки поставок. Большинство устройств создаются с использованием программных и аппаратных компонентов от множества производителей, а также библиотек с открытым исходным кодом. Во многих случаях у операторов устройств нет четкого представления об аппаратной и программной спецификации материалов (H/SBOM) для оценки риска цепочки поставок устройств в сети. В июне 2020 года были раскрыты уязвимости в сетевом стеке, который использовался множеством производителей. Они затрагивали сотни миллионов потребительских и промышленных устройств IoT¹⁴. Иногда поставщики изменяли название сетевого стека, что скрывало какие-либо признаки уязвимости устройства. Мы наблюдаем все большую угрозу от злоумышленников, нацеленных на эту цепочку поставок программного и аппаратного обеспечения устройств IoT/OT для компрометации организаций.

Процесс обновления встроенного ПО сильно зависит от устройства, а сложность и логистика обновления влияют на его частоту. Не всегда можно определить, работает ли устройство с последней версией ПО, что затрудняет специалистам по безопасности мониторинг и защиту устройств IoT и OT. Кроме того, у встроенного ПО некоторых устройств нет криптографической подписи, что позволяет обновлять их без подтверждения пользователя. Эти недостатки делают устройства еще уязвимее для атак на цепочку поставок по всей производственной и распределительной цепочке.

Для борьбы с этими угрозами корпорация Microsoft инвестирует значительные средства в обеспечение безопасности и целостности встроенного ПО на различных этапах цепочки поставок, а также в подтверждение того, что оно не было модифицировано во время получения или передачи. Это обеспечит уровень доверия между каждым сегментом конвейера и сертифицированную и проверенную цепочку ответственности для каждого компонента, который мы отправляем клиентам. Вместе с партнерами мы прилагаем все усилия, чтобы гарантировать безопасность на всем пути, от чипа к облаку, на всех устройствах в корпоративной и OT-сети.

«Поставщики ИКТ-инфраструктуры все чаще становятся целью злоумышленников, потому что они могут стать источником масштабной атаки. В то же время международное законодательство, нормативные требования и потребности клиентов в безопасности и отказоустойчивости цепочки поставок становятся строже, а требования часто различаются.

Для решения этой проблемы необходимо сотрудничество. Корпорация Microsoft вместе с поставщиками и правительствами разных стран стремится защитить всю экосистему цепочки поставок, превосходя требования как клиентов, так и надзорных органов. Для этого мы применяем комплексный подход к безопасности и операционной устойчивости, который гибко разворачивается во всей цепочке поставок.

Обеспечение целостности встроенного ПО от этапа проектирования до начала использования устройства — важнейший аспект нашего коллективного подхода. Поддержка SDL-процессов поставщиков и развертывание инновационного аппаратного корневого узла — это примеры того, как мы можем «встроить» целостность в цепочку поставок.

Наше сообщество применяет результаты коллективных исследований и разработок, включающие в себя новые методы защиты от изменения кода и криптографические механизмы, в дополнение к непрерывному мониторингу и обнаружению аномалий. Вместе мы успешно снижаем привлекательность цепочки поставок как возможного направления атаки».

Эдна Конуэй (Edna Conway),
вице-президент, директор по безопасности и рискам, облачная инфраструктура

Обзор уязвимостей встроенного ПО

Злоумышленники все чаще применяют уязвимости встроенного ПО устройств IoT для проникновения в корпоративные сети. В отличие от традиционных конечных точек, которые используют агенты XDR для поиска слабых мест, уязвимости в устройствах IoT/OT гораздо сложнее обнаружить.

Недавний опрос, проведенный корпорацией Microsoft и Ponemon Institute, подчеркивает как возможности, так и проблемы устройств IoT/OT в области безопасности на предприятии¹⁵. 68 % респондентов считают, что внедрение IoT/OT имеет решающее значение для стратегической цифровой трансформации, при этом 60 % признают, что IoT/OT — один из наименее защищенных аспектов ИТ/OT-инфраструктуры.

Пример применения уязвимостей встроенного ПО устройств IoT для проникновения в сеть — это троян Trickbot, который использовал пароли по умолчанию и уязвимости в маршрутизаторах Mikrotik¹⁶ для обхода корпоративных систем защиты. Фундаментальная проблема встроенного ПО устройств IoT заключается в отсутствии сведений о состоянии их безопасности и уязвимостей.

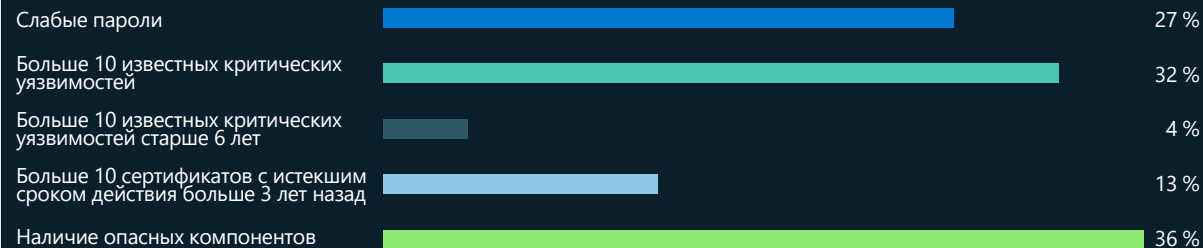
Хотя решения для производства безопасных устройств есть, но миллиарды незащищенных устройств уже развернуты на предприятиях. Их называют действующими устройствами. В 2021 году корпорация Microsoft приобрела компанию ReFirm Labs, чтобы проанализировать безопасность действующих устройств и позволить разработчикам устройств улучшить защиту своих продуктов. ReFirm Labs анализирует двоичный образ встроенного ПО и создает подробный отчет о потенциальных уязвимостях безопасности¹⁷. Эта технология включена в будущий выпуск Microsoft Defender для Интернета вещей.

В прошлом году мы изучили агрегированные результаты уникального встроенного ПО, проверенного нашими клиентами. Хотя использовать можно не все обнаруженные слабые места, они подчеркивают фундаментальную проблему с безопасностью встроенного ПО устройств.

Обратите внимание, что типы слабых мест в устройствах IoT/OT никогда не будут допустимыми для традиционных конечных точек под управлением Windows или Linux.

- Слабые пароли: 27 % процентов сканируемых образов встроенного ПО содержали учетные записи с паролями, закодированными с помощью слабых алгоритмов (MD5/DES), которые легко взломать.

Проанализированные слабые места безопасности в образах встроенного ПО



- Известные уязвимости: во встроенном ПО устройств IoT/OT, как и в других системах, широко используются библиотеки с открытым исходным кодом. Однако устройства часто поставляются с устаревшими версиями этих компонентов. Согласно нашему анализу, 32 % образов содержали по крайней мере 10 известных уязвимостей (CVE) критического уровня (9,0 или выше). 4 % содержали не меньше 10 критических уязвимостей возрастом больше 6 лет.
- Просроченные сертификаты: сертификаты используются для аутентификации подключений и удостоверений, а также для защиты конфиденциальных данных, однако 13 % проанализированных образов содержали не меньше 10 сертификатов, срок действия которых истек больше 3 лет назад.
- Программные компоненты: 36 % образов содержали программные компоненты, которые корпорация Microsoft рекомендует исключить из устройств IoT, таких как инструменты захвата пакетов (tcpdump, libpcap), которые могут использоваться для разведки сети в рамках цепочки атак.

Атаки на встроенное ПО в реальном мире

Viasat: использование уязвимости встроенного ПО для атаки на спутниковую связь

В феврале 2022 года после инцидента со спутниковой сетью была отключена стратегическая коммуникационная сеть, последствия чего ощутили во всей Европе. Система KA-SAT компании Viasat получила большой объем трафика, что вывело из строя многие модемы, после чего против сети началась атака типа «отказ в обслуживании». Так как фиксированная широкополосная связь была нарушена, тысячи ветряных турбин стали недоступными для удаленных операторов, а вредоносное ПО, удаляющее данные, было развернуто на затронутых модемах. Сбой затронул 30 000 спутниковых терминалов, используемых различными организациями для связи.

Cyclops Blink: использование атаки на цепочку поставок встроенного ПО для взлома шлюзов брандмауэра

Развитие и расширение инфраструктуры управления и атак — важнейший компонент успеха для злоумышленников. Потребность в стабильной инфраструктуре управления выросла, поэтому маршрутизаторы стали желанным вектором атаки, так как на них редко устанавливают исправления, а комплексных решений безопасности просто нет.

Корпорация Microsoft сотрудничает с государственными и коммерческими организациями для разработки технологии анализа встроенного ПО, которая позволит лучше оценивать безопасность устройств и обеспечить полную защиту жизненного цикла для сборщиков и операторов устройств.

С июня 2019 года связанная с государством группа постоянно активных угроз (APT) использовала модульное вредоносное ПО Cyclops Blink для взлома уязвимых устройств брандмауэра WatchGuard и маршрутизаторов ASUS, устанавливая вредоносные обновления и добавляя их в масштабный ботнет. Вредоносная программа успешно заражает устройства, используя известную уязвимость, которая дает возможность повысить привилегии и удаленно управлять устройством. После заражения вредоносная программа может устанавливать дополнительные модули и отклонять обновления встроенного ПО. Скомпрометированные устройства подключались к серверам управления, размещенным на других устройствах WatchGuard. Выдавая множество SSL-сертификатов для центра управления на различных TCP-портах, операторы Cyclops Blink получали привилегированный удаленный доступ к сетям, устанавливая вредоносные обновления встроенного ПО и уклоняясь от традиционных механизмов защиты, таких как сканирование.

Как корпорация Microsoft повышает уровень безопасности цепочки поставок

Корпорация Microsoft сотрудничает с государственными и коммерческими организациями для решения этих проблем с безопасностью устройств IoT и OT ([см. обсуждение на странице 66](#)). Наш вклад будет включать в себя использование технологии анализа встроенного ПО для предоставления операторам устройств сведений о состоянии безопасности устройств в сети. Это позволит клиентам выявлять устройства, требующие дополнительную защиту, обновление или замену, назначать им приоритеты, а также стимулировать сборщиков устройств инвестировать средства в их безопасность. В то же время мы поддерживаем производителей, предоставляя им комплексные решения для проектирования защищенных устройств и применения безопасных жизненных циклов разработки.

Другой важный аспект — это предоставление разработчикам и операторам надежной инфраструктуры, позволяющей обновлять встроенное ПО устройств при обнаружении и устранении проблем с безопасностью. Корпорация Microsoft объединяет анализ встроенного ПО и Defender для Интернета вещей с Центром обновления устройств для Центра Интернета вещей, чтобы создать решение для поддержки полного жизненного цикла безопасности устройств IoT и OT. Это важные меры по реализации нашей концепции защиты инфраструктуры клиентов путем внедрения устройств, которые применяют принцип «Никому не доверяй» к своим решениям IoT и OT¹⁸.

Злоумышленники все чаще используют уязвимости встроенного ПО устройств IoT для проникновения в корпоративные сети.

Практические рекомендации

- 1 Получите подробное представление об устройствах IoT/OT в сети и приоритезируйте их по риску для организации в случае компрометации.
- 2 Используйте инструменты сканирования встроенного ПО для анализа потенциальных уязвимостей и сотрудничайте с поставщиками, чтобы определить, как снизить риски для уязвимых устройств.
- 3 Требуйте от поставщиков применения рекомендаций по обеспечению безопасности жизненного цикла разработки, чтобы усилить защиту устройств IoT/OT.

Ссылки на дополнительную информацию

- > [Assessment of the Critical Supply Chains Supporting the US Information and Communications Technology Industry](#)

Разведывательные атаки на OT-устройства

В сложных цепочках поставок для планирования фактической системы используется проектная информация. Из множества ресурсов, из которых состоит эта проектная информация, самым конфиденциальным является файл проекта, который определяет среду и все ресурсы. Это важная стратегическая цель для злоумышленников, которые хотят получить доступ к системе и успешно провести атаку, полностью адаптированную под целевую среду.

Атаки на промышленные системы для нарушения операционных процессов состоят из 2 этапов.


1. Сначала злоумышленник должен получить доступ к OT-сети. Для этого можно войти в систему через устройства IoT на корпоративной стороне сети (уровень 4 модели Пердью) и перейти границу между ИТ и ОТ, традиционно разделенную брандмауэрами и сетевым оборудованием, чтобы попасть на уровни эксплуатации и управления.
2. Затем необходимо идентифицировать сетевые устройства. В промышленных системах используются стандартные устройства и компоненты в специализированных архитектурах, специально разработанных для производственных сред. Одно из таких стандартных устройств — это программируемый логический контроллер (ПЛК). Каждый производитель создает уникальные интерфейсы и функции для ПЛК — важных компонентов промышленных систем, — и эти устройства дополняются специализированными схемами для сред клиентов.

Уникальная конфигурация каждого ПЛК описана в файле проекта, содержащем определение среды и ее ресурсов, многоступенчатую логику и многое другое.

Анализ показывает, что в большинстве сред с признаками атаки время подготовки намного превышает продолжительность самой атаки. Злоумышленники часто месяцами проводят удаленное моделирование среды и ее ресурсов, повторяя попытки построить модель и подготовить атаку. Так как среды постоянно меняются и в них добавляются новые устройства, уязвимости создаются именно в связи с данными проекта и файлами конфигурации. Кража файла проекта может ускорить атаку на несколько недель или месяцев, а также позволить злоумышленникам быстро и точно смоделировать целевую среду, что усложнит обнаружение вредоносных действий.

Industroyer и Incontroller

Мы наблюдали рост числа атак на организации, критически важную инфраструктуру и правительственные цели со стороны спонсируемых государством злоумышленников с использованием модульных вредоносных программ и платформ атак. Новые попытки вмешаться в критически важные операции в Украине подчеркивают растущую угрозу разведывательных атак на OT-устройства, которые сильно адаптированы под целевые среды. Расширенные фазы разведки и исследования, проводимые кибергруппами национального уровня, указывают на стратегию использования кибервойны для удаленного нанесения ущерба инфраструктуре и достижения конкретных стратегических или оперативных целей в гибридных киберкинетических операциях и политической стратегии.



Мы наблюдаем растущую угрозу разведывательных атак на OT-устройства, которые специально адаптированы под целевые среды.

Разведывательные атаки на ОТ-устройства

Продолжение

В начале 2022 года были выявлены 2 адаптирующиеся атаки на критически важную ОТ-инфраструктуру. Атака, совмещающая кибероперации и физические действия, на электрические подстанции и защитные реле в Украине была осуществлена с помощью специализированного вредоносного ПО, в том числе варианта Industroyer — программы, которая вызвала перебои в подаче электроэнергии в Украине после развертывания в 2016 году.

Industroyer 2 — это первое известное повторное развертывание вредоносного ПО, предназначенного для ОТ-инфраструктуры, на новую цель. Эта угроза использовала протокол IEC104 (стандартный протокол для мониторинга и контроля системы питания), разработанный для Industroyer и предназначенный для удаленных терминальных блоков, подобных ПЛК, с номером модели ABB RTU540/560. Создатель этой вредоносной программы использовал знания о среде жертвы для выполнения множества команд заранее определенным выводам, чтобы их было невозможно включить вручную. Это увеличило длительность перебоев в подаче электроэнергии и усилило разрушительное воздействие атаки.

Incontroller — это модульная вредоносная платформа, выявленная в тот же период, которая представляет собой модульный набор инструментов, значительно ускоряющих проникновение и атаки на ОТ-устройства, минуя устаревшие механизмы безопасности. Этот набор общего назначения поддерживает возможности сбора данных, разведки и атаки, которые легко настраиваются для различных сред и могут серьезно повлиять на фазу исследования для атаки на ОТ-инфраструктуру, ускоряя разведку и упрощая моделирование сред за счет извлечения информации об устройствах и их конфигурациях.

Платформа Incontroller поддерживает протоколы для ПЛК Schneider Electric и Omron, а также собирает такую информацию, как версия встроенного ПО, тип модели и подключенные устройства. Набор инструментов может выполнять команды для изменения конфигурации, включения и выключения выводов контроллера. После доступа к среде платформа может добавлять бэкдоры в устройства для загрузки дополнительной полезной нагрузки, создавая уязвимости для увеличения числа точек доступа, загрузки многоступенчатой логики и проведения DoS-атак. Благодаря своей универсальности набор инструментов позволяет злоумышленнику быстро атаковать среду, не создавая новые атаки для каждого ПЛК или расположения. Это дает возможность легко взаимодействовать с различными типами устройств во многих отраслях.



Практические рекомендации

- 1 Избегайте передачи файлов, содержащих определения системы, по незащищенным каналам или сотрудникам без соответствующих полномочий.
- 2 Если передача таких файлов все-таки необходима, обязательно отслеживайте действия в сети и защищайте ресурсы.
- 3 Защищайте инженерные станции с помощью решений EDR.
- 4 Используйте упреждающий подход к реагированию на инциденты в ОТ-сетях.
- 5 Разверните решение для непрерывного мониторинга, такое как Defender для Интернета вещей.

Концевые сноски

1. Смотрите, например, Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe's digital future (europa.eu); <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1>; Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (homeaffairs.gov.au); Chile: Bill for cybersecurity and critical information infrastructure introduced in Senate | News post | DataGuidance; Japan passes economic security bill to guard sensitive technology | The Japan Times; Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs (csa.gov.sg); Proposal for legislation to improve the UK's cyber resilience—GOV.UK (www.gov.uk); Telecommunications (Security) Act 2021 (legislation.gov.uk); Updating the NIST Cybersecurity Framework—Journey To CSF 2.0 | NIST
2. Cert-In — домашняя страница
3. Initiation of consultation on introduction of cyberattack reporting obligation (admin.ch)
4. Смотрите, например, untitled (house.gov)
5. Cyber Resilience Act | Shaping Europe's digital future (europa.eu)
6. Смотрите, например, Жизненный цикл разработки Microsoft Security
7. Смотрите, например, Создание спецификаций на программное обеспечение (SBM) с помощью SPDX в корпорации Microsoft — Engineering@Microsoft, The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. Смотрите, например, <https://www.microsoft.com/en-us/msrc/cvd>
9. The Product Security and Telecommunications Infrastructure (PSTI) Bill—product security factsheet—GOV.UK (www.gov.uk)
10. Commission strengthens cybersecurity of wireless devices and products (europa.eu)
11. Cloud Certification Scheme: Building Trusted Cloud Services Across Europe — ENISA (europa.eu)
12. Certification — ENISA (europa.eu)
13. <https://github.com/microsoft/sbom-tool> GitHub - Microsoft/sbom-tool: инструмент SBOM — это высокомасштабируемый и готовый к использованию на предприятии инструмент для создания SBOM, соответствующих требованиям SPDX 2.2, для любых артефактов.
14. <https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come>
15. Инновации в сфере IoT/OT критически важны, но связаны со значительными рисками (декабрь 2021 г.): <https://www.microsoft.com/security/blog/2021/12/08/new-research-shows-iot-and-ot-innovation-is-critical-to-business-but-comes-with-significant-risks/>
16. Выявление использования ботнетом Trickbot устройств IoT в инфраструктуре центра управления (март 2022 г.): <https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/>
17. IoT Show в Channel 9: эпизод о сканировании встроенного ПО устройств Интернета вещей (май 2022 г.): <https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot>
18. Как применить принцип «Никому не доверяй» к решениям Интернета вещей (май 2021 г.): <https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/>

Кибероперации по распрост- ранению влияния

В современных операциях иностранных государств по распространению своего влияния применяются новые методы и технологии, что делает их кампании, направленные на подрыв доверия, эффективнее и результативнее.

Обзор киберопераций по распространению влияния	72
Введение	73
Тенденции в сфере киберопераций по распространению влияния	74
Обзор операций по распространению влияния во время COVID-19 и вторжения России в Украину	76
Отслеживание индекса российской пропаганды	78
Синтетические медиа	80
Комплексный подход к защите от киберопераций по распространению влияния	83

Обзор

киберопераций по распространению влияния

В современных операциях иностранных государств по распространению своего влияния применяются новые методы и технологии, что делает их кампании, направленные на подрыв доверия, эффективнее и результативнее.

Иностранные государства все чаще используют сложные операции по распространению влияния для пропаганды и воздействия на общественное мнение как внутри страны, так и на международном уровне. Эти кампании подрывают доверие, усиливают поляризацию общества и угрожают демократическим процессам. Квалифицированные продвинутые активные манипуляторы используют традиционные СМИ вместе с Интернетом и социальными сетями, чтобы существенно увеличить масштаб, область и эффективность своих кампаний, а также свое влияние на глобальную информационную экосистему. В прошлом году мы видели такие операции в рамках гибридной войны России с Украиной, но также наблюдали, как Россия и другие страны, в том числе Китай и Иран, все чаще обращались к пропагандистским операциям в социальных сетях для расширения глобального влияния.

Кибероперации по распространению влияния становятся все сложнее, так как все больше государств используют их для формирования общественного мнения, дискредитации противников и разжигания разногласий.

Ход иностранных киберопераций по распространению влияния

Предварительная подготовка

Запуск

Усиление

Подробнее на стр. 74

Вторжение России в Украину продемонстрировало кибероперации по распространению влияния, интегрированные с традиционными кибератаками и военными операциями для максимального воздействия.

Подробнее на стр. 76

Россия, Иран и Китай использовали пропагандистские кампании на протяжении всей пандемии COVID-19, часто в качестве стратегического инструмента для достижения широких политических целей.

Подробнее на стр. 76

Синтетические медиа распространяются все шире из-за роста числа инструментов, которые легко создают и публикуют высокореалистичные искусственные изображения, видео и аудио. Технологии подтверждения цифрового происхождения, которые сертифицируют происхождение медиаресурсов, как обещают, сможет бороться с неправильным использованием таких видов медиа.

Подробнее на стр. 80

Комплексный подход к защите от киберопераций по распространению влияния

Корпорация Microsoft опирается на свою уже зрелую инфраструктуру аналитики киберугроз для борьбы с кибероперациями по распространению влияния. Наша стратегия состоит в выявлении, срыве, защите и сдерживании пропагандистских кампаний иностранных агрессоров.

Подробнее на стр. 83

- Производство
Целевое и
использова
- Распредел
Беспрецед
скорость
- Последств
Снижение

Введение

Для успеха демократии необходима достоверная информация. Главная область внимания для Microsoft — операции по распространению влияния, разрабатываемые и проводимые иностранными государствами. Эти кампании подрывают доверие, усиливают поляризацию общества и угрожают демократическим процессам.

Такие операции всегда были угрозой для информационной экосистемы. Однако в эпоху Интернета и социальных сетей есть ряд отличий: значительно возросший размах, масштаб и эффективность кампаний, а также сильное влияние, которое они могут оказать на работоспособность глобальной информационной экосистемы.

Старая поговорка «Ложь может обойти половину мира, прежде чем правда сможет надеть штаны» теперь подтверждается данными. Исследование Массачусетского технологического института (MIT)¹ показало, что ложь на 70 % чаще ретвитят, чем правду, и что она в 6 раз быстрее достигает первых 1500 человек. Информационная экосистема становится сомнительной, так как в Интернете и социальных сетях процветают пропагандистские кампании, которые подрывают доверие к традиционным новостям. В исследовании, проведенном в 2021 году², только 7 % взрослых американцев заявили, что «сильно» доверяют газетам, телевидению и радионовостям, в то время как 34 % сообщили, что «совсем не доверяют им».

Корпорация Microsoft стремится выявлять основных субъектов, угрозы и тактики в пространстве иностранного кибервлияния и обмениваться полученным опытом. В июне этого года мы опубликовали подробный отчет об уроках, извлеченных из опыта Украины, с обзором киберопераций России по распространению влияния³.

Мы также изучаем, как новые технологии, такие как дипфейки, могут использоваться в качестве оружия, чтобы подорвать доверие к журналистам. Мы сотрудничаем с компаниями, правительством и учеными, чтобы разработать эффективные способы обнаружения синтетических медиа и восстановления доверия, такие как системы искусственного интеллекта (ИИ), которые могут обнаруживать подделки.

Быстрое изменение информационной экосистемы и онлайн-пропаганды иностранных государств, в том числе объединение традиционных кибератак с операциями по распространению влияния и вмешательством в демократические выборы, требует всеобщего подхода для борьбы с угрозами демократии как в Интернете, так и за его пределами.

Корпорация Microsoft стремится поддерживать работоспособную информационную экосистему с подлинными новостями и информацией. Мы разрабатываем средства и функции обнаружения угроз для борьбы с растущим риском операций по распространению влияния, проводимых иностранными государствами. Для этого мы недавно приобрели компанию Miburo Solutions, сотрудничаем со сторонними контролирующими организациями, такими как Global Disinformation Index и NewsGuard, и участвуем в многосторонних партнерских объединениях (а иногда и возглавляем их), таких как Coalition for Content Provenance and Authenticity (C2PA). Только вместе мы сможем успешно бороться с теми, кто хочет подорвать демократические процессы и институты.

Тереза Хатсон (Teresa Hutson)

Вице-президент по технологиям и корпоративной ответственности

Тенденции в сфере киберопераций по распространению влияния

Кибероперации по распространению влияния становятся все сложнее по мере быстрого развития технологий. Мы видим пересечение функций и расширение инструментов для традиционных кибератак на кибероперации по распространению влияния. Кроме того, мы наблюдаем усиление координации и повышение интенсивности со стороны иностранных государств.

Корпорация Microsoft инвестировала средства в борьбу с операциями иностранного влияния в этом году, приобретя компанию Miburo Solutions, которая специализируется на анализе операций подобного рода. Объединив этих аналитиков со специалистами Microsoft по анализу контекста угроз, корпорация Microsoft сформировала Центр анализа цифровых угроз (DTAC). DTAC анализирует и сообщает об угрозах со стороны иностранных государств — как о кибератаках, так и об операциях по распространению влияния, — объединяя информацию и аналитические сведения об угрозах с геополитическим анализом, чтобы получить данные для эффективного реагирования и защиты.

Больше 75 % людей во всем мире заявили, что они обеспокоены превращением информации в оружие⁴, и наши данные подтверждают, что эти опасения не безосновательны. Корпорация Microsoft и ее партнеры отслеживают, как кибергруппы национального уровня используют операции по распространению влияния для достижения своих стратегических и политических целей. В дополнение к разрушительным кибератакам и кибершпионажу, авторитарные режимы все чаще проводят кибероперации по распространению влияния для формирования общественного мнения, дискредитации противников, разжигания страха, сеяния разногласий и искажения реальности.

Такие операции обычно проходят за 3 этапа:

Предварительная подготовка

Подобно предварительному развертыванию вредоносного ПО в компьютерной сети организации, кибероперации по распространению влияния закладывают ложные нарративы в публичном домене в Интернете. Такая тактика уже давно помогает традиционным кибероперациям, особенно если ИТ-администраторы сканируют свою последние действия в сети. Вредоносные программы, которое длительное время находится в сети в спящем режиме, может сделать его последующее использование эффективнее. Ложные нарративы, которые остаются незамеченными в Интернете, могут сделать последующие тезисы правдоподобными.

Запуск

Часто, когда момент наиболее способствует достижению целей субъекта, начинается скоординированная кампания по распространению нарративов через поддерживаемые правительством и находящиеся под влиянием СМИ и каналы социальных сетей.

Усиление

Наконец, контролируемые иностранным государством СМИ и его ставленники усиливают нарративы для целевой аудитории. Во многих случаях технические платформы невольно расширяют охват этих нарративов. Например, интернет-реклама может помочь финансировать такие операции, а координированные системы доставки контента могут заполнить поисковые системы спущенными сверху тезисами.

Этот трехэтапный подход применили в конце 2021 года для поддержки российского нарратива о предполагаемом биологическом оружии и биологических лабораториях в Украине. Впервые подобный контент был загружен на YouTube 29 ноября 2021 года на канале регулярного англоязычного шоу американского экспатрианта, живущего в Москве, который утверждал, что финансируемые США биологические лаборатории в Украине связаны с разработкой биологического оружия. Несколько месяцев эта история по сути незамеченной. 24 февраля 2022 года, когда российские танки пересекли границу, нарратив был отправлен в бой. Команда аналитиков данных Microsoft выявила 10 новостных сайтов, контролируемых Россией или зависящих от нее, которые одновременно 24 февраля опубликовали отчеты, ссылающиеся на «прошлогодний отчет» с целью придать ему достоверность. Кроме того, представители министерства иностранных дел России провели пресс-конференции, на которых также представили ложные утверждения о биологических лабораториях США, которые распространились по информационной среде. Спонсируемые Россией команды работали над усилением нарратива в социальных сетях и на веб-сайтах.

Мы видим, как авторитарные режимы во всем мире работают вместе, чтобы загрязнить информационную экосистему для взаимной выгоды. Например, на протяжении пандемии COVID-19 Россия, Иран и Китай использовали пропаганду и операции по распространению влияния, применяя сочетание открытых, полужакрытых и скрытых методов пропаганды среди демократических стран и пытаясь добиться других геополитических целей ([что обсуждается далее на стр. 76](#)). 3 режима использовали экосистемы обмена сообщениями и информации друг друга, чтобы продвигать собственные нарративы. Большая часть этого контента состояла из критики или теорий заговора о США и их союзниках, распространяемых правительственными деятелями в официальных заявлениях, и одновременно продвигала собственные вакцины и меры борьбы с COVID-19 как превосходящие меры, принятые в США и других демократиях. Усиливая друг друга, государственные СМИ создали экосистему, в которой негативное освещение демократий — или позитивное освещение России, Ирана и Китая, — со стороны одного государственного СМИ, было усилено другими.

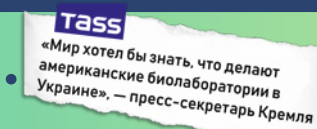
Ход иностранных киберопераций по распространению влияния⁵

Предварительная подготовка



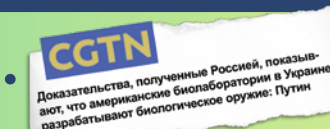
Пресс-конференция

Запуск



Освещение в российской экосистеме СМИ

Усиление



Усиление в зарубежных СМИ

Иллюстрация того, как нарративы о биологических лабораториях США и биологическом оружии распространяются в рамках 3 фаз многих иностранных операций по распространению влияния — предварительная подготовка, запуск и усиление.

Тенденции в сфере киберопераций по распространению влияния

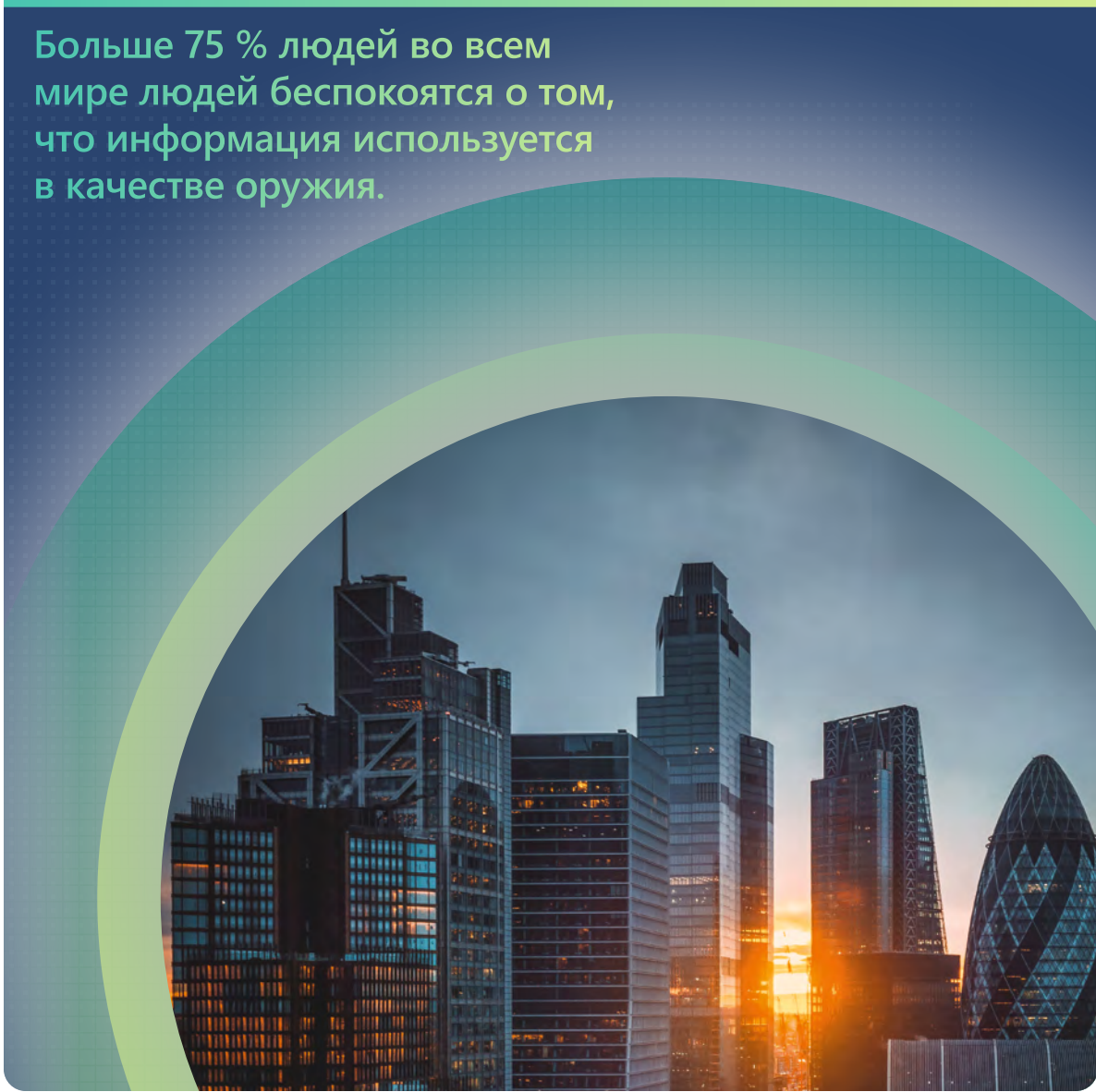
Продолжение

Кроме того, частные технологические компании могут стать невольными участниками этих кампаний. К ним могут относиться компании, которые регистрируют интернет-домены, размещают веб-сайты, продвигают контент в социальных сетях и на поисковых сайтах, направляют трафик и помогают финансировать эти операции с помощью цифровой рекламы. Организации должны знать об инструментах и методах, используемых авторитарными режимами для киберопераций по распространению влияния, чтобы обнаруживать, а затем и предотвращать распространение таких кампаний. Кроме того, растет потребность в том, чтобы помочь потребителям развить способность точно выявлять иностранные операции по распространению влияния и ограничивать взаимодействие с их нарративами или контентом.

Кибероперации по распространению влияния, в том числе пропаганда авторитарных режимов, представляют угрозу для демократий во всем мире, так как они подрывают доверие, усиливают поляризацию общества и угрожают демократическим процессам.

Усиление координации и обмена информацией между правительством, частным сектором и гражданским обществом необходимо для улучшения прозрачности, а также для выявления и срыва этих кампаний по распространению влияния.

Больше 75 % людей во всем мире людей беспокоят о том, что информация используется в качестве оружия.



Обзор операций по распространению влияния во время COVID-19 и вторжения России в Украину

Иностранные государства, которые стремились взять под свой контроль информационную среду во время пандемии и во время российского вторжения в Украину, — это яркие примеры того, как авторитарные режимы смешивают кибер- и информационные операции.

Пропаганда, связанная с COVID-19

Россия, Иран и Китай использовали пропаганду и кампании по распространению влияния в течение всей пандемии COVID-19. Пандемия играла важную роль в этих кампаниях 2 основными способами:

1. Представления о самой пандемии.
2. Кампании, которые использовали COVID-19 как стратегический инструмент для достижения широких политических целей.

Общая цель этих кампаний имеет 2 стороны: во-первых, подорвать демократии, демократические институты и имидж США и их союзников на мировой арене; во-вторых, укрепить собственные позиции внутри страны и на международном уровне.

Пример подобного поведения можно увидеть в сообщениях известных российских аккаунтов и СМИ, ориентированных на англоязычных читателей, по сравнению с тем, как российское правительство общалось с собственным народом о вакцине и серьезностью заболевания COVID-19.

Темы, рассмотренные в 10 самых просматриваемых историях о коронавирусе на сайте RT.com (октябрь 2021 г. — апрель 2022 г.)

Пропаганда против вакцинации нацелена на читателей за пределами России

Русский

«Локдаун и дополнительные прививки предотвращают распространение»

«Российские знаменитости получили положительный результат теста»

«В России растет число случаев заболевания и смертей»

«Вакцина Sputnik V очень эффективна»

«Для поездок на общественном транспорте требуется предъявить документ о вакцинации»

Английский

«Вакцинация не сможет помещать распространению вируса и неэффективна против новых штаммов»

«У вакцины Pfizer опасные побочные эффекты»

«Массовая вакцинация политически мотивирована»

«Pfizer и Moderna проводят нерегулируемые клинические испытания»

Российское освещение COVID-19 с разными формулировками.

Кампании, которые стремились скрыть происхождение вируса COVID-19, служат еще одним примером. С самого начала пандемии российская, иранская и китайская пропаганда усиливала тезисы друг друга, чтобы подчеркнуть эти центральные темы. Большая часть подобного контента состояла из пропаганды критики или теорий заговора о США. Регулярно усиливая друг друга, государственные СМИ создали экосистему, в которой негативное освещение демократий — или позитивное освещение России, Ирана и Китая, — со стороны одного государственного СМИ, было усилено другими.

Один из таких примеров — раннее предположение российских и иранских государственных СМИ о том, что вирус COVID-19 может быть биологическим оружием, созданным США. Это утверждение распространилось на маргинальных конспирологических сайтах в начале пандемии после интервью с профессором права, который утверждал, что вирус COVID-19 был создан в качестве оружия⁶. После публикации интервью на нескольких веб-сайтах с ограниченной аудиторией, историю подхватили государственные СМИ. PressTV, иранское англо- и франкоязычное издание, спонсируемое иранским правительством⁷, опубликовало в феврале 2020 года англоязычную статью под названием «Является ли коронавирус

оружием биологической войны США, как считает Фрэнсис Бойл?»⁸. В статье говорилось, что именно США стояли за вспышкой COVID-19: «Во всех войнах США использует радиологическое, химическое, биологическое и другое запрещенное оружие, которое вызывает разрушительные потери в затронутых районах»⁸. Российские государственные СМИ и аккаунты китайского правительства поддержали это мнение. Russia Today (RT) — государственное издание, известное своей ролью в распространении кремлевской пропаганды⁹, опубликовало, по крайней мере, одну историю, которая продвигала заявления иранских официальных лиц, утверждающих, что COVID-19 может быть «результатом биологической атаки США, направленной на Иран и Китай»¹⁰, и сделало публикации в социальных сетях о том же самом. Например, твит RT от 27 февраля 2020 года гласил: «Поднимите руку те, кто не удивится, если когда-нибудь выяснится, что коронавирус — это биологическое оружие?»¹¹

Война в Украине — пропаганда как оружие войны

Вторжение России в Украину — этой яркий пример того, как кибероперации по распространению влияния можно объединить с традиционными кибератаками и военными операциями, чтобы повысить их воздействие.

Перед вторжением в Украину аналитики угроз из Microsoft заметили, что по меньшей мере 6 отдельных кибергрупп, связанных с Россией, совершили больше 237 кибератак против Украины. Их целью было нарушение работы сервисов и организаций, предотвращение доступа украинцев к достоверной информации и сеяние сомнений в руководителях страны.

Обзор операций по распространению влияния во время COVID-19 и вторжения России в Украину

Продолжение

В отчете Microsoft, опубликованном в апреле 2022 года, мы показали, как в явной попытке контролировать информационную среду в Киеве Россия нанесла ракетный удар по телебашне в Киеве в тот же день, когда она использовала разрушительное вредоносное ПО против крупной украинской медиакомпании¹².

Другим примером того, как объединяются кибератаки и операции по распространению влияния, служит то, что российский злоумышленник отправлял украинским гражданам электронные письма (якобы от жителей Мариуполя), обвиняя украинское правительство в эскалации войны и призывая соотечественников дать отпор правительству. Эти письма были адресованы по имени тем, кто получал электронное письмо. Это говорит о том, что их контактные данные могли быть украдены в ходе предыдущей кибератаки, связанной со шпионажем. В письмах не было никаких вредоносных ссылок. Это свидетельствует о том, что целью этой кампании было исключительное распространение влияния.

Использование контента, полученного в ходе хакерского взлома, утечки данных или иной операции, — это распространенная тактика, используемая российскими субъектами в операциях по распространению влияния. На протяжении всей войны в Украине пророссийские каналы в социальных сетях публиковали, по их словам, полученные в результате утечки сведения или иные чувствительные материалами из украинских источников. Такой контент применяется

пророссийскими каналами и СМИ в рамках широкой стратегии распространения влияния, направленной на снижение доверия к демократическим институтам и постановку под сомнение основных нарративов. Этой информацией можно манипулировать, чтобы создать пропаганду, нацеленную на Украину и Запад, уменьшить доверие к цифровой безопасности и подорвать поддержку помощи Украине со стороны западных стран.

Россия использовала другие информационные атаки для формирования общественного мнения после военных операций, чтобы скрыть факты или подорвать доверие. Например, 7 марта Россия подготовила нарратив, сообщив в ООН о том, что родильный дом в Мариуполе был опустошен и используется в качестве военного объекта. 9 марта Россия разбомбила роддом. После того, как стало известно о бомбежке, представитель России в ООН Дмитрий Полянский написал в Twitter, что освещение взрыва было «фейковыми новостями», и сослался на предыдущие заявления России о предполагаемом использовании роддома в качестве военного объекта. Затем Россия широко распространяла этот нарратив на контролируемых Россией веб-сайтах в течение 2 недель после атаки.



Дмитрий Полянский @Dpol_un

Так рождаются #fakenews. В нашем заявлении от 7 марта (russia.ru/en/news/070322n) мы предупреждали, что радикалы превратили эту больницу в военный объект. очень тревожно, что ООН распространяет эту информацию без проверки #Mariupol #Mariupolhospital



1



4

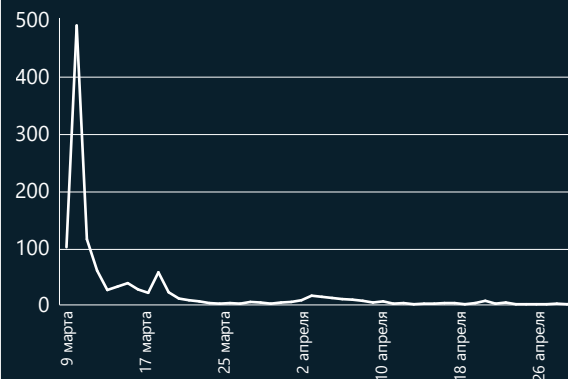


8



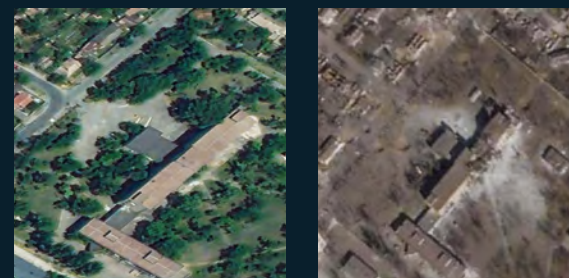
Домены с трафиком

(9 марта 2022 г. — 30 апреля 2022 г.)



Пропагандистские сайты публиковали рассказы о роддоме около 2 недель с коротким всплеском, который начался 1 апреля 2022 г. Источник: Microsoft AI for Good Lab.

Спутниковые снимки роддома в Мариуполе в феврале и марте 2022 г.



Собственный анализ спутниковых снимков Microsoft показал, что роддом подвергся бомбардировке. Первая фотография от 24 февраля 2022 года, а вторая — от 24 марта 2022 года. Источник: Planet Labs.

Обеление Россией подобных операций продолжается по мере развития войны. Например, в конце июня 2022 года российские СМИ и влиятельные лица описали бомбежку торгового центра как оправданную и необходимую, ложно утверждая, что он использовался не в качестве торгового центра, а скорее в качестве оружейного склада для украинских сил территориальной обороны¹³. Несколько прокремлевских блогеров в Telegram разместили контент, усиливающий нарратив об «атаке под чужим флагом», причем блогеры указали на предполагаемые признаки подтасовки, такие как присутствие людей в военной форме на кадрах с места происшествия¹⁴ и отсутствие женщин на кадрах¹⁵. Россия начала кампании, опираясь на выстроенную систему пропагандистских мессенджеров и сред. Усиление этих историй в Интернете позволяет России переложить вину на международную арену и избежать ответственности.

Иностранные государства, такие как Россия, понимают ценность использования информации, полученной из закрытых источников, для влияния на общественное мнение и используют кампании «взлома и утечки» для распространения контрнарративов и подрыва доверия.

Ссылки на дополнительную информацию

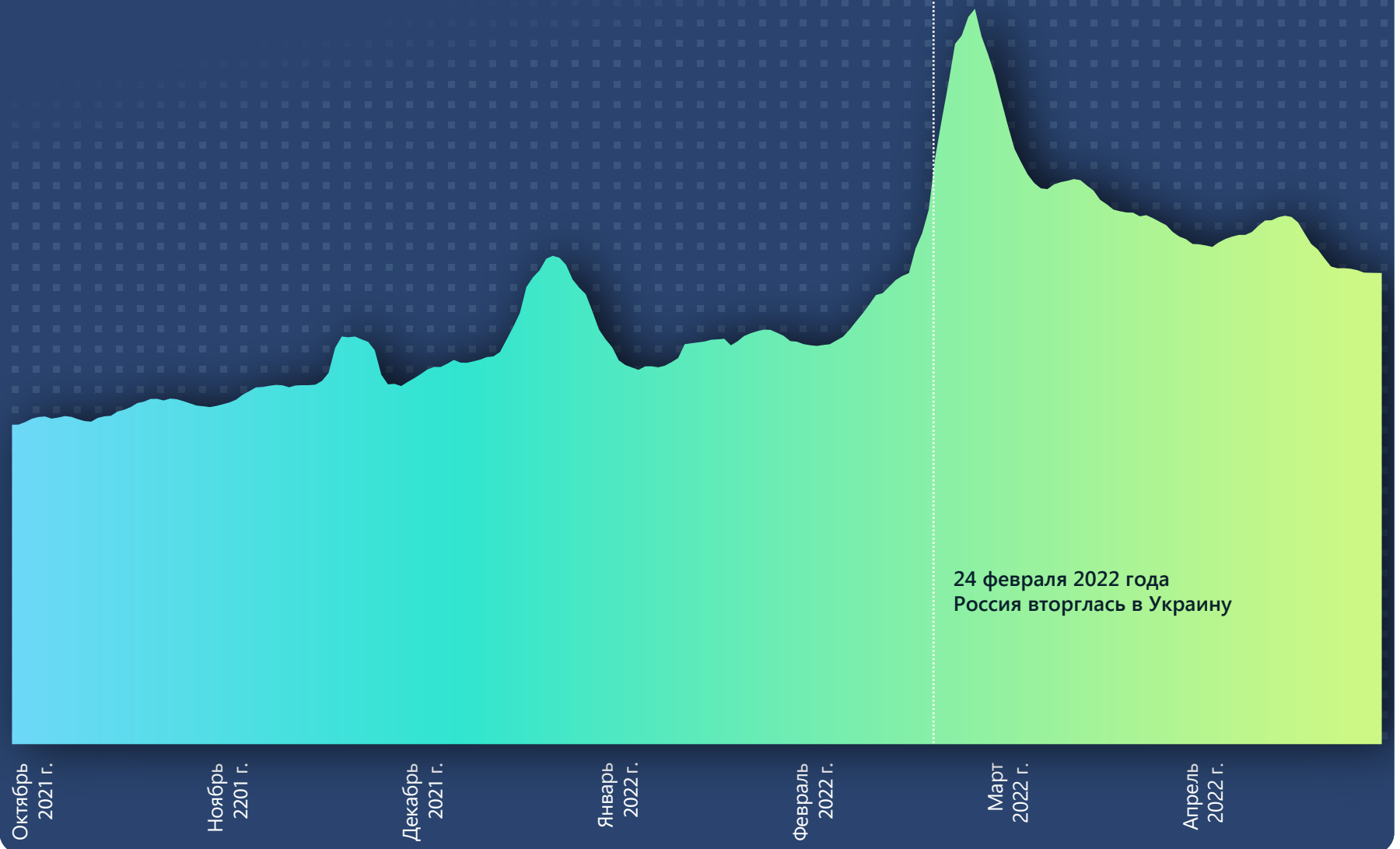
- Защита Украины: первые уроки кибервойны | Microsoft On the Issues
- Обзор кибератак России в Украине | Специальный отчет Microsoft
- Предотвращение кибератак, направленных против Украины | Microsoft On the Issues

Отслеживание индекса русской пропаганды

В январе 2022 года почти 1000 американских веб-сайтов ссылались на российские пропагандистские сайты. Самыми популярными темами для российских пропагандистских сайтов, ориентированных на американскую аудиторию, были война с Украиной, внутренняя политика США (либо за Трампа, либо за Байдена), пандемия COVID-19 и связанные с вакцинами нарративы.

Индекс русской пропаганды (RPI) отслеживает поток новостей из контролируемых и спонсируемых государством русских новостных агентств и усилителей как долю от общего новостного трафика в Интернете. RPI можно использовать для составления графика потребления русской пропаганды в Интернете и в разных регионах на точной временной шкале. Однако корпорация Microsoft отмечает, что мы можем наблюдать только русскую пропаганду, размещенную на ранее идентифицированных веб-сайтах. У нас нет сведений о пропаганде на других типах веб-сайтов, таких как новостные сайты авторитарных режимов, неидентифицированные веб-сайты и группы в социальных сетях.

Индекс русской пропаганды в США
(октябрь 2021 г. — апрель 2022 г.)



Отслеживание индекса российской пропаганды

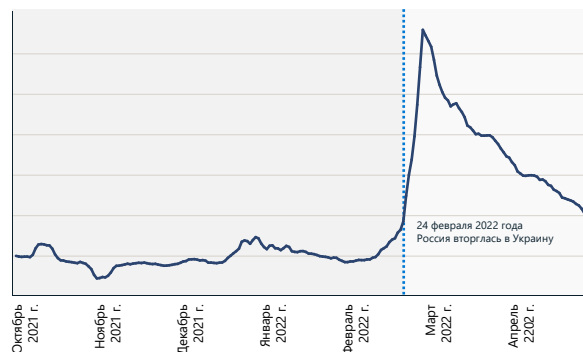
Продолжение

Индекс российской пропаганды: Украина

Когда началась война в Украине, объем российской пропаганды вырос на 216 %, а пик пришелся на 2 марта. На следующей диаграмме показано, как это внезапное увеличение совпало с вторжением. На 2 графиках показан рост объема российской пропаганды вскоре после начала вторжения.

RPI, Украина

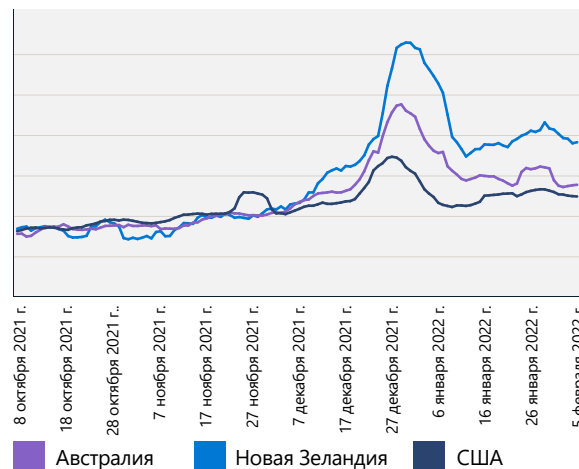
(7 октября 2021 г. — 30 апреля 2022 г.)



Индекс российской пропаганды: Новая Зеландия, Австралия и США

Оценка RPI в Новой Зеландии показала всплеск в конце 2021 года, связанный с пропагандой по теме пандемии COVID-19. Данный всплеск потребления российской пропаганды в Новой Зеландии предшествовал росту общественных протестов в начале 2022 года в Веллингтоне. Второй всплеск был определенно связан с российским вторжением в Украину и превысил RPI Австралии и США.

RPI, Новая Зеландия, Австралия и США



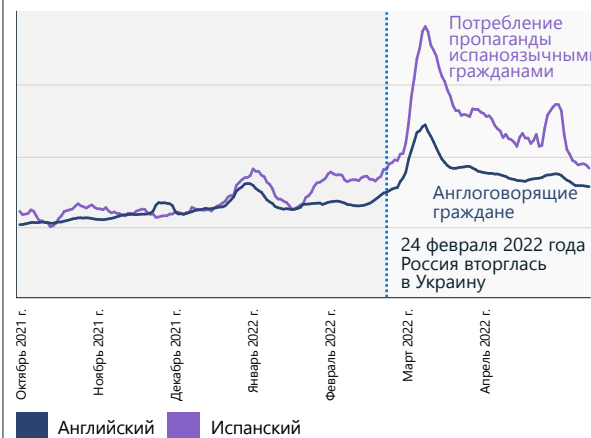
Потребление российской пропаганды в Новой Зеландии аналогично австралийскому до первой недели декабря 2021 года. Затем потребление российской пропаганды в Новой Зеландии увеличилось на 30 % по сравнению с Австралией и США.

Индекс российской пропаганды в США: английский и испанский языки

RPI также отслеживает пропаганду на разных языках. Несколько СМИ, в том числе RT и Sputnik News, доступны на 20 языках. К ним относятся английский, испанский, немецкий, французский, греческий, итальянский, чешский, польский, сербский, латышский, литовский, молдавский, белорусский, армянский, осетинский, грузинский, азербайджанский, арабский, турецкий, персидский и дари.

На следующем графике показано, что RPI для новостей на испанском языке в США намного выше, чем для новостей на английском языке.

Потребление российской пропаганды в 2 раза выше среди испаноговорящих граждан



Потребление российской пропаганды в США в 2 раза выше среди испаноговорящих граждан.

Высокий уровень потребления российской пропаганды в Латинской Америке



RT на испанском языке — это международное новостное издание с наибольшим количеством просмотров страниц и подписчиков в Facebook.

Источник: Microsoft AI for Good Research Lab

Синтетические медиа

Мы вступаем в золотую эпоху создания и манипулирования СМИ с помощью ИИ. Аналитики Microsoft отмечают, что это обусловлено 2 основными тенденциями: распространением простых в использовании инструментов и сервисов для искусственного создания высокореалистичных синтетических изображений, видео, аудио и текста, а также возможностью быстрого распространения контента, оптимизированного для конкретной аудитории.

Ни одна из этих технологий сама по себе не представляет проблемы. Технологию на базе ИИ можно использовать для создания веселого и интересного цифрового контента, например для создания синтетического или улучшения существующего контента. Эти средства широко используются компаниями для рекламы и коммуникаций, а также частными лицами для создания привлекательного контента для своих подписчиков. Однако синтетические медиа, создаваемые и распространяемые с вредоносными целями, могут нанести серьезный ущерб отдельным лицам, компаниям, учреждениям и обществу в целом. Корпорация Microsoft была движущей силой в разработке технологий и методик как внутри компании, так и в широкой экосистеме медиа, чтобы ограничить потенциальный ущерб.

В этом разделе рассматриваются результаты анализа корпорацией Microsoft текущего состояния современных технологий создания вредного синтетического контента, потенциальном ущербе при широком распространении этого контента и технических мерах по смягчению последствий, которые могут защитить нас от киберугроз на основе синтетических медиа.

Создание синтетических медиа

Область синтетического текста и мультимедиа развивается очень быстро, так как методы, которые когда-то были доступны только крупным киностудиям с огромными вычислительными ресурсами, теперь интегрированы в приложения для телефонов. В то же время эти средства становятся проще в использовании и могут генерировать контент с таким уровнем реализма, который может обмануть даже специалистов. Мы очень близки к моменту, после которого каждый будет иметь возможность создать синтетическое видео с любым человеком, кто говорит или делает что-либо. Вполне разумно полагать, что мы вступаем в эпоху, когда существенная часть контента, который мы видим в Интернете, будет полностью или частично создана синтетически с помощью ИИ.

Из-за появления простых в использовании и широко доступных инструментов с дополнительными возможностями создание синтетического контента продолжает совершенствоваться, и скоро он будет неотличим от реальности.

Доступно много высококачественных бесплатных и коммерческих средств редактирования изображений, видео и аудио. С их помощью можно вносить простые, но потенциально опасных изменения в цифровой контент, например добавлять вводящий в заблуждение текст, заменять лица, удалять или изменять контекст. Такие «дешевые подделки» широко используются для распространения вредоносного контента, продвижения политических идеологий и нанесения ущерба репутации. Хорошо известным примером является видео 2019 года¹⁶, в котором спикер Палаты представителей США Нэнси Пелоси

невнятно произносит свою речь и выглядит пьяной. Хотя было быстро определено, что видео было замедлено, чтобы создать такой эффект, эта «дешевая подделка» распространилась повсеместно, пока не появилось исходное видео и контекст.

Продвинутые подходы к изменению медиаконтента включают в себя использование передовых методов ИИ для (а) создания чисто синтетических медиа и (б) сложного редактирования существующих медиа. Термин «дипфейк» часто применяется к синтетическим медиа, которые были созданы на основе ИИ (название происходит от глубоких нейронных сетей, которые иногда используются в этих целях). Такие технологии выпускаются как отдельные приложения, инструменты и сервисы и интегрируются в популярные коммерческие инструменты редактирования и решения с открытым исходным кодом.

Злоумышленники используют подобные технологии в качестве оружия в надежде нанести ущерб отдельным лицам и учреждениям. Ниже перечислены примеры методов использования дипфейков:

- **Замена лица (видео, изображения)** — замена лица одного человека в видео на другое. Этот метод может использоваться для шантажа человека, компании или учреждения, а также для размещения людей в неловких местах или ситуациях.
- **Кукловодство (видео, изображения)** — использование видео для анимации неподвижного изображения или создания другого видео. При этом может создаваться впечатление, что человек сказал что-то неловкое или вводящее в заблуждение.
- **Генеративно-состязательные сети (видео, изображения)** — семейство методов создания фотореалистичных изображений.

- **Модели-трансформеры (видео, изображения, текст)** — создание реалистичных изображений на основе текстового описания.

Такие передовые методы на основе ИИ еще не широко используются в киберкампаниях по распространению влияния, но мы ожидаем, что проблема будет расти, по мере того как инструменты становятся проще в использовании и доступнее.

Влияние манипуляций с синтетическими медиа

Информационные операции не впервые используются для нанесения ущерба или расширения влияния. Однако скорость, с которой информация может распространяться, и способность быстро отделить факты от вымысла означают, что воздействие и ущерб дипфейков и других вредоносных синтетических медиа могут быть намного шире, что продемонстрировал пример с Нэнси Пелоси.

Мы рассматриваем несколько категорий ущерба: манипулирование рынком, мошенничество с платежами, голосовой фишинг, имитация, ущерб бренду, репутационный ущерб и ботнеты. Для многих из этих категорий есть реальные примеры, которые могут подорвать нашу способность отделять факты от вымысла.

Долгосрочная и коварная угроза заключается в нашем понимании того, что истинно, если мы больше не можем доверять тому, что видим и слышим. Из-за этого любое компрометирующее изображение, аудио или видео публичной или частной фигуры можно назвать подделкой — это называют «дивидендом лжеца»¹⁷. Согласно недавнему исследованию¹⁸, что эти технологии уже используются для атак на финансовые системы, хотя возможны и многие другие сценарии злоупотреблений.

Синтетические медиа

Продолжение

Обнаружение синтетических медиа

Сейчас в промышленности, правительстве и научных кругах предпринимаются усилия по разработке эффективных способов обнаружения и устранения последствий использования синтетических медиа и восстановления доверия. Есть несколько многообещающих путей развития, а также препятствия, которые следует рассмотреть.

Один из подходов заключается в создании систем на базе ИИ, которые могут обнаруживать подделки. Это, по сути, «оборонительные» ИИ-системы для противодействия наступательным ИИ-системам. В этой области активно проводятся исследования: современные системы для создания синтетического аудио и видео оставляют артефакты, которые могут обнаружить обученные медиааналитики и автоматизированные инструменты.

Хотя текущие подделки имеют явные недостатки, но, к сожалению, такие артефакты обычно уникальны для конкретного инструмента или алгоритма. Это значит, что обучение на известных подделках обычно не обобщается на другие

алгоритмы, как это было показано в открытом конкурсе в 2020 году по созданию детекторов дипфейк-изображений¹⁹. Есть большой соблазн увеличить инвестиции в разработку продвинутых детекторов, но корпорация Microsoft совсем не уверена, что это приведет к значительным улучшениям, по 2 причинам:

Во-первых, у нас есть превосходные физические модели, отражающие реальный мир. Текущие создатели подделок срезают углы, что приводит к обнаружению артефактов, но новые модели станут еще реалистичнее. В реальной сцене, снятой камерой, нет ничего особенного, что не мог бы смоделировать компьютер.

Во-вторых, продвинутые алгоритмы создания подделок используют генеративно-сопоставительные сети (GAN) как часть процесса. GAN запускает 2 ИИ-системы друг против друга, используя генератор для создания подделки и дискриминатор для обнаружения поддельных изображений и обучения генератора. Любые инвестиции в разработку улучшенного детектора только позволят генератору повысить качество подделок.

Среда синтетических медиа

	Факторы Низкий барьер для входа	Удобные инструменты	Инструменты повышенной сложности	Простое распространение
	Производители Целевое и вредоносное использование	Организации и учреждения	Физические лица и потребители	Злоумышленники, стремящиеся нанести вред
	Распределение Беспрецедентная скорость	Усиление через социальные сети	Таргетированные электронные письма и реклама	Аудиофайлы по голосовой почте Напрямую из источника
	Последствия Снижение доверия	Ущерб репутации личности	Мошенничество и другой финансовый ущерб	Ущерб организации или бренду Манипулирование рынком
	Устранение Перспективные решения	Передовые системы ИИ для обнаружения	Определение цифрового происхождения	Межотраслевые усилия

Синтетические медиа

Продолжение

Определение происхождения цифровых ресурсов

Если обнаружение подделок — ненадежный процесс, как можно защититься от вредоносного использования синтетических медиа? Одна из важных новых технологий в этой сфере — это технология подтверждения цифрового происхождения. Это механизм, позволяющий создателям цифровых медиа сертифицировать ресурсы, чтобы потребители могли определить, был ли ресурс подделан. Технология подтверждения цифрового происхождения особенно важна в контексте современных социальных сетей, учитывая скорость, с которой контент может передаваться по Интернету, и простоту манипуляций с контентом со стороны злоумышленников.

Технология подтверждения цифрового происхождения — это современная версия криптографической подписи документов, предназначенная для определения источника, редактирования истории и метаданных объектов по мере их прохождения через Интернет. Концепция и технические методы для реализации такого типа сквозной сертификации медиа с защитой от подделки были разработаны командой, состоящей из исследователей и ученых корпорации Microsoft. Мы возглавляем межотраслевое объединение, направленное на реализацию технологии подтверждения цифрового происхождения в рамках программы Project Origin (созданной совместно Microsoft, BBC, CBC/Radio-Canada и New York Times) и участвуем в инициативе Content Authenticity Initiative (созданной компанией Adobe). Кроме того, корпорация Microsoft вместе с партнерами из сферы технологий и мультимедийных сервисов создала организацию Coalition for Content Provenance and Authenticity (C2PA). C2PA — это организация по стандартизации, которая недавно опубликовала самую продвинутую спецификацию технологии подтверждения цифрового происхождения, которую можно применять к медиаресурсам, таким как изображения, видео, аудио и текст.

Объект с поддержкой C2PA содержит манифест, который защищает объект и метаданные от подделки, а сопутствующий сертификат идентифицирует издателя.

Синтетические медиа изначально не были предназначены для нанесения вреда, но злоумышленники используют их как оружие, пытаясь подорвать доверие к отдельным лицам и организациям.

Подтверждение цифрового происхождения — это многообещающая новая технология, которая поможет восстановить доверие к медиаконтенту в Интернете за счет сертификации происхождения медиаресурсов.

Публичные решения, основанные на спецификации C2PA, появляются либо как новая функция существующих продуктов, либо как новые отдельные приложения и сервисы. Мы ожидаем, что большинство популярных инструментов съемки, редактирования и разработки будут поддерживать C2PA через несколько лет. Это дает компаниям возможность определить свои потребности и методы использования технологии подтверждения цифрового происхождения и потребовать применять такой дополнительный уровень защиты в инструментах, которые они используют в текущих рабочих процессах.

Практические рекомендации

- 1 Принимайте профилактические меры для защиты организации от угроз дезинформации путем упреждающего рассмотрения пресс-релизов и ответов в СМИ.
- 2 Используйте технологию подтверждения происхождения для защиты официальных сообщений.

Ссылки на дополнительную информацию

- > Многообещающий шаг вперед в борьбе с дезинформацией | Microsoft On the Issues
- > A Milestone Reached, 31 января 2022 г.
- > Project Origin | Microsoft ALT Innovation
- > Coalition for Content Provenance and Authenticity (C2PA)
- > Изучите технические сведения о системе, используемой Project Origin для проверки подлинности мультимедиа | Microsoft ALT Innovation

900 %

в годовом исчислении увеличивается распространение дипфейков с 2019 года²⁰.

Комплексный подход к защите от киберопераций по распространению влияния

Корпорация Microsoft опирается на свою зрелую инфраструктуру анализа киберугроз для получения широкого и инклюзивного представления о кибероперациях по распространению влияния.

Мы используем платформу для предлагаемых стратегий реагирования и смягчения последствий, чтобы бороться с угрозой, создаваемой операциями, которые можно разделить на 4 ключевых категории: выявление, срыв, защита и сдерживание.

Кроме того, корпорация Microsoft применяет 4 принципа для поддержки нашей работы в этой области. Первый принцип — это обязательство уважать свободу выражения мнений и поддерживать способность клиентов создавать, публиковать и искать информацию с помощью наших платформ, продуктов и сервисов. Второй принцип состоит в том, что мы активно работаем над тем, чтобы наши платформы и продукты не использовались для усиления иностранных сайтов и контента киберопераций по распространению влияния. Третий принцип гласит, что мы не будем умышленно извлекать выгоду из контента или субъектов иностранных киберопераций по распространению влияния. Наконец, мы уделяем приоритетное внимание поиску контента для противодействия иностранным операциям по распространению влияния, используя внутренние данные о наших продуктах и сведения от проверенных партнеров.

Обнаружение

Как и в случае с киберзащитой, первый шаг в противодействии иностранным кибероперациям по распространению влияния — это развитие возможностей для их обнаружения. Ни одна организация не может надеяться в одиночку добиться необходимого прогресса. Новое расширенное сотрудничество в технологическом секторе окажет решающее значение, так как прогресс в сфере анализа и оповещений о кибероперациях по распространению влияния во многом зависит от роли гражданского общества, в том числе научных кругов и некоммерческих организаций.

Понимая эту роль, исследователи Джейк Шапиро (Jake Shapiro) и Алисия Уонлесс (Alicia Wanless) из Принстонского университета и Фонда Карнеги за международный мир соответственно запланировали запуск нового «Института исследований информационной среды» (IRIE). При поддержке Microsoft, Knight Foundation и Craig Newmark Philanthropies институт IRIE организует инклюзивное многофункциональное научно-исследовательское учреждение, смоделированное по образцу Европейской организации ядерных исследований (ЦЕРН). В нем будут объединены эксперты по обработке и анализу данных, чтобы ускорить и масштабировать новые открытия в этой сфере. Результаты будут публиковаться для информирования политиков, технологических компаний и потребителей.

Защита

Второй стратегический принцип — это укрепление защиты демократии, что давно является приоритетной целью, для достижения которой сейчас необходимы инвестиции и инновации. При этом следует учитывать проблемы, которые технологии создали для демократии, и возможности, которые технологии открывают для эффективной защиты демократических обществ.

Структура стратегии Microsoft направлена на то, чтобы помочь заинтересованным из различных секторов сторонам выявлять, срывать, защищать и сдерживать пропаганду, особенно кампании иностранных агрессоров.

Будет логично начать с одного из самых серьезных технологических вызовов нашего времени — влияния Интернета и цифровой рекламы на традиционную журналистику. С 1700-х годов свободная и независимая пресса играла особую роль в поддержке каждой демократии на планете, разоблачая коррупцию, документируя войны и освещая крупнейшие социальные проблемы этой и любой другой эпохи. Однако Интернет практически уничтожил местные новости, пожирая доходы от рекламы и переманивая платных подписчиков. Многие местные газеты закрылись. Один из многих выводов из нашей недавней работы состоит в том, что города, в которых нет газеты, неосознанно и неизбежно подвергаются большему, чем в среднем, объему иностранной пропаганды. Поэтому одно из важнейших направлений защиты демократии — это укрепление традиционной журналистики и свободной прессы, особенно на местном уровне. Для этого понадобятся постоянные инвестиции и непрерывные инновации, соответствующие потребностям различных стран и континентов. Эти непростые задачи, и они требуют многосторонних подходов, которые корпорация Microsoft и другие технологические компании поддерживают все чаще.

Нам также необходимы инновации в государственной политике, которые

должны стать общественным приоритетом. Это могут быть законы, позволяющие издателям вести переговоры о доходах от рекламы совместно с технологическими компаниями, и законодательство, предоставляющее льготы, освобождающие местные редакции от части их налогов на заработную плату для журналистов, которых они нанимают. Журналистам требуется множество других инструментов для своей работы, в том числе возможность разделять контент от подлинных и мошеннических источников.

Кроме того, быстро растет потребность помогать потребителям развить эффективную способность выявлять информационные операции, контролируемые иностранными государствами. Эта задача может показаться нерешаемой, но она напоминает усилия, которые технологический сектор уже давно прилагает для борьбы с другими киберугрозами. Подумайте о том, чтобы научить потребителей внимательнее смотреть на адрес электронной почты, чтобы они могли обнаружить спам или другие мошеннические сообщения. Инициативы в США, такие как News Literacy Project и Trusted Journalism

Долгосрочная и коварная угроза заключается в нашем понимании того, что истинно, если мы больше не можем доверять тому, что видим и слышим.

Комплексный подход к защите от киберопераций по распространению влияния

Продолжение

Program, помогают повысить осведомленность потребителей новостей и информации. Во всем мире новые технологии, такие как подключаемый модуль для браузера компании NewsGuard, могут ускорить реализацию таких инициатив.

Это также должно напомнить нам о том, что один из основополагающих принципов демократии — это образование в области гражданского общества. Как всегда, все должно начинаться в школах. Однако мы живем в мире, в котором гражданское образование должно длиться всю жизнь. Новая программа Civics at Work, разработанная организацией Center for Strategic and International Studies, партнером и первым подписантом которой стала корпорация Microsoft, направлена на повышение гражданской осведомленности в корпоративных сообществах. Это хороший пример широты возможностей для укрепления защиты демократии.

Срыв

В последние годы подразделение Microsoft по борьбе с цифровыми преступлениями (DCU) усовершенствовало свою тактику и разработало средства для предотвращения киберугроз — от программ-шантажистов до ботнетов и атак иностранных государств. Мы извлекли много ценных уроков, начиная с роли активного срыва в противодействии широкому спектру кибератак.

При противодействии кибероперациям по распространению влияния срыв может стать еще важнее, и самый эффективный подход к срыву становится все очевиднее. Наиболее эффективный антидот от масштабного обмана — это прозрачность. Именно поэтому корпорация Microsoft расширила возможности по обнаружению и пресечению операций по распространению влияния иностранных государств, приобретя Miburo Solutions — ведущую компанию по анализу и исследованию киберугроз, которая специализируется на обнаружении иностранных киберопераций по распространению влияния и реагировании на них.

Наш опыт показывает, что государственные учреждения, технологические компании и НПО должны приписывать кибератаки той или иной стороне с осторожностью и достаточным объемом доказательств. Понимание последствий такого срыва критически важно и может стать еще полезнее в срыве киберопераций по распространению влияния. Посмотрите на передачу информации правительством США перед вторжением России в Украину, который позволил превратить прозрачность в эффективные меры, такие как разоблачение российских планов, в том числе конкретных кампании, например попытку использовать поддельное видео насильственного характера.

Как было показано в опубликованной прошлым летом статье CyberPeace Institute (Женева) о продолжающихся кибератаках внутри и за пределами Украины, у широкого круга гражданских организаций и частного сектора есть возможность повысить прозрачность в отношении киберопераций по распространению влияния. Надежные отчеты о недавно обнаруженных и хорошо задокументированных операциях помогут гражданам лучше оценивать то, что они читают, видят и слышат — особенно в Интернете. С этой целью корпорация Microsoft будет использовать

существующие киберотчеты и дополнять их, а также будет выпускать новые отчеты, данные и обновления, связанные с тем, что мы узнаем о кибероперациях по распространению влияния, включая в них заявления о возможных источниках операций, когда это необходимо. Мы будем публиковать годовой отчет, использующий данные для анализа всей компании на распространенность иностранных информационных операций и описывающий дальнейшие действия для постепенного улучшения ситуации. Мы также будем приводить дополнительные шаги, основанные на таком типе прозрачности.

Роль цифровой рекламы очень важна, например реклама может помочь финансировать иностранные операции, одновременно создавая видимость легитимности пропагандистских сайтов, спонсируемых из-за рубежа. Для борьбы с этими финансовыми потоками потребуются новые усилия.

Задержка

Наконец, нельзя ожидать, что страны изменят поведение, если не будет ответственности за нарушение международного права. Обеспечение такой подотчетности — исключительная обязанность правительства. Однако все чаще действия с многосторонним участием играют важную роль в укреплении и расширении международных норм. Больше 30 онлайн-платформ, рекламодателей и издателей, в том числе корпорация Microsoft, подписали недавно обновленный Свод правил Европейской комиссии по дезинформации, согласившись на усиление обязательств по решению этой растущей проблемы. Подобно недавнему Парижскому призыву, Призыву Крайстчерч и Декларации обудущем Интернета, многосторонние действия помогут объединить правительства и общество демократических стран. После этого правительства смогут опираться на эти нормы и законы для поддержки подотчетности, в которой нуждаются мировые демократии и которой они заслуживают.

Благодаря радикальной прозрачности демократические правительства и общества смогут эффективно противодействовать кампаниям по распространению влияния, приписывая их иностранным государствам, информируя общественность и укрепляя доверие к гражданским институтам.

Мы расширили технические возможности обнаружения и пресечения операций по распространению иностранного влияния и поддерживаем прозрачную отчетность о подобных операциях, таких как наши отчеты о кибератаках.

Практические рекомендации

- 1 Используйте эффективные методы цифровой профилактики в вашей организации.
- 2 Рассмотрите способы противодействия любой непреднамеренной поддержки киберкампаний по распространению влияния вашими сотрудниками или бизнес-процессами. К ним относится сокращение поставок контента на известные зарубежные пропагандистские сайты.
- 3 Необходимо поддерживать кампании информационной грамотности и гражданского участия в качестве ключевого компонента, помогающего обществу защищаться от пропаганды и иностранного влияния.
- 4 Напрямую взаимодействуйте с группами, связанными с вашей отраслью, которые стремятся противодействовать операциям по распространению влияния.

Концевые сноски

1. <https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections?msclkid=8dc75d6abcfe11ecad9946a058d581c9>
2. <https://news.gallup.com/poll/355526/americans-trust-media-dips-second-lowest-record.aspx>
3. Защита Украины: первые уроки кибервойны (microsoft.com)
4. [https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf](https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022%20Edelman%20Trust%20Barometer%20FullReport.pdf)
5. Официальный представитель МИД России Мария Захарова: <https://tass.com/politics/1401777>; Лавров: <https://www.cnn.com/2022/05/05/opinions/sergey-lavrov-hitler-comments-ukraine-kauders/index.html>, Kirill Kudryavtsev/Pool/AFP/Getty Images
6. <https://apnews.com/article/conspiracy-theories-iran-only-on-ap-media-misinformation-bfca6d5b236a29d61c4dd38702495ffe>
7. <https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib>
8. <https://www.presstv.ir/Detail/2020/02/04/617877/Is-the-coronavirus-a-US-bioweapon>
9. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf
10. <https://www.rt.com/news/482405-iran-coronavirus-us-biological-weapon/>
11. https://web.archive.org/web/20220319124125/https://twitter.com/RT_com/status/1233187558793924608?s=20
12. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd>
13. Russia's Kremenchuk Claims Versus the Evidence—bellingcat
14. https://t.me/oddr_info/39658
15. <https://t.me/voenacher/23339>
16. Fact check: "Drunk" Nancy Pelosi video is manipulated | Reuters
17. <https://lawcat.berkeley.edu/record/1136469>
18. <https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237>
19. Deepfake Detection Challenge Results: An open initiative to advance AI (facebook.com)
20. Deepfakes 2020: The Tipping Point, Johannes Tammekänd, John Thomas, and Kristjan Peterson, октябрь 2020 г.

Киберустой- чивость

Понимание рисков и преимуществ модернизации становится решающим для комплексного подхода к устойчивости.

Обзор киберустойчивости	87
Введение	88
Киберустойчивость: важнейший принцип информационного общества	89
Важность модернизациисистем и архитектуры	90
Базовый уровень безопасности — определяющий фактор эффективности передовых решений	92
Поддержание работоспособности удостоверений имеет основополагающее значение для благополучия организации	93
Параметры безопасности операционной системы по умолчанию	96
Акцент на цепочке поставки ПО	97
Повышение устойчивости к новым DDoS-атакам, атакам на веб-приложения и сети	98
Разработка сбалансированного подхода к безопасности данных и киберустойчивости	101
Устойчивость к кибероперациям по распространению влияния: человеческое измерение	102
Укрепление человеческого фактора за счет развития навыков	103
Уроки, извлеченные из нашей программы ликвидации программшантажистов	104
Необходимость немедленного принятия мер по защите квантовых вычислений	105
Интеграция бизнесподразделений, отдела безопасности и ИТ-отдела для повышенияустойчивости	106
Колоколообразная кривая киберу стойчивости	108

Обзор киберустойчивости

Кибербезопасность — важнейший фактор технологического успеха. Инноваций и повышения производительности можно достигнуть только после внедрения мер безопасности, которые сделают организации максимально устойчивыми к современным атакам.

Из-за пандемии нам пришлось изменить методы и технологии обеспечения безопасности для защиты сотрудников Microsoft, где бы они ни работали. В прошлом году злоумышленники продолжали использовать уязвимости, обнаруженные во время пандемии и перехода к гибридной рабочей среде. С тех пор наша главная задача — контролировать распространение и растущую сложность различных методов атак, а также повышенную активность иностранных государств.

Для эффективного обеспечения киберустойчивости необходим комплексный, адаптивный подход, позволяющий бороться с меняющимися угрозами для базовых сервисов и инфраструктуры.

[➤ Подробнее на стр. 89](#)

Модернизированные системы и архитектура важны для борьбы с угрозами в эпоху повсеместного подключения к сети.

[➤ Подробнее на стр. 90](#)

Базовый уровень безопасности — определяющий фактор эффективности передовых решений.

[➤ Подробнее на стр. 92](#)

Атаки на основе паролей остаются основной причиной компрометации учетных данных, но появляются и другие типы атак.

[➤ Подробнее на стр. 93](#)

Человеческое измерение устойчивости к кибероперациям по распространению влияния — это наша способность сотрудничать и кооперироваться.

[➤ Подробнее на стр. 102](#)

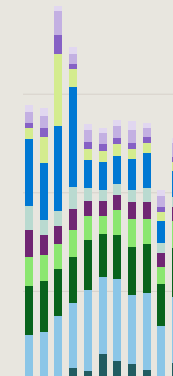
Подавляющее большинство успешных кибератак можно предотвратить с помощью базовых профилактических мер.

[➤ Подробнее на стр. 108](#)



В прошлом году в мире наблюдалась беспрецедентная по объему, сложности и частоте активность DDoS-атак.

[➤ Подробнее на стр. 98](#)



Введение

Из-за пандемии нам пришлось изменить методы и технологии обеспечения безопасности для защиты сотрудников Microsoft, где бы они ни работали. В прошлом году злоумышленники продолжали использовать уязвимости, обнаруженные во время пандемии и перехода к гибридной рабочей среде. С тех пор наша главная задача — контролировать распространение и растущую сложность различных методов атак, а также повышенную активность иностранных государств.

Активность цифровых угроз и сложность кибератак растут с каждым днем. Многие из современных сложных атак сосредоточены на компрометации архитектур идентификации, цепочек поставок и третьих сторон с системами безопасности различного уровня. Мы обнаружили, что фишинговые атаки на удостоверения — это явная и реальная угроза. Однако такие типы атак, как правило,

оказываются безуспешными при надлежащем управлении идентификацией, контроле фишинга и управлении конечными точками. Поэтому мы все должны помнить основы: 98 % атак можно остановить с помощью базовых профилактических мер. Корпорация Microsoft управляет удостоверениями и устройствами в рамках подхода «Никому не доверяй», согласно которому необходимо применять принципа наименьших привилегий и стойкие к фишингу учетные данные, чтобы эффективно предотвращать кибератаки и защищать данные.

Сегодня даже злоумышленники без продвинутых технических навыков могут проводить невероятно разрушительные атаки, так как передовые тактики, методы и процедуры становятся широкодоступны в экономике киберпреступности. Война в Украине показала, как национальные кибергруппы активизировали наступательные кибероперации за счет широкого использования программ-шантажистов. На данный момент программы-шантажисты превратились в сложную индустрию, в которой злоумышленники используют тактику двойного или тройного вымогательства для получения выплаты, а разработчики применяют модель «программа-шантажист как сервис» (RaaS). При этом злоумышленники используют партнерскую сеть для проведения атак, что снижает барьер для входа не таких квалифицированных киберпреступников и, в конечном счете, расширяет пул злоумышленников.

В ответ на это корпорация Microsoft разработала программу уничтожения программ-шантажистов. Ее цель — устранение пробелов в контроле и охвате, содействие улучшению функций сервисов и разработка сценариев восстановления нашего центра информационной безопасности и инженерных команд в случае атаки программ-шантажистов.

Недавние атаки на цепочку поставок и сторонних поставщиков указывают на серьезную точку перегиба во всей отрасли. Сбои, которые эти атаки вызывают у наших клиентов, партнеров, государственных учреждений и корпорации Microsoft, продолжают увеличиваться. Это подчеркивает важность мер киберустойчивости и сотрудничества заинтересованных сторон в области безопасности. Злоумышленники также атакуют локальные системы, что усиливает потребность организаций в управлении уязвимостями, связанными с устаревшими системами, за счет модернизации и переноса инфраструктуры в облако с повышенным уровнем безопасности.

Мы живем во времена, когда безопасность — это важнейший фактор технологического успеха. Инноваций и повышения производительности можно достигнуть только после внедрения мер безопасности, которые сделают организации максимально устойчивыми к современным атакам. По мере развития и распространения цифровых угроз крайне важно встроить киберустойчивость в структуру каждой организации.

Брет Арсено (Bret Arsenault)
Директор по информационной безопасности

Киберустойчивость: важнейший принцип информационного общества

Цифровая революция привела к тому, что организации трансформируются, стремясь усилить взаимосвязь рабочих процессов и предлагаемых услуг. Из-за быстрого роста числа киберугроз встраивание киберустойчивости в структуру организации так же важно, как финансовая и операционная устойчивость.

Цифровая трансформация навсегда изменила методы взаимодействия организаций с клиентами, партнерами, сотрудниками и другими заинтересованными сторонами. Новые технологии открывают невероятные возможности для взаимодействия с людьми, трансформации продуктов и оптимизации операций. Пандемия ускорила цифровую трансформацию, стимулируя внедрение инновационных технологий, которые позволяют сотрудничать по-новому и из любого места.

По мере распространения киберугроз по всему миру, предотвращение атак становится все сложнее в нашем «всегда подключенном к сети» мире. Киберустойчивость — это способность организации продолжать работу и поддерживать развитие, несмотря на множество атак. Необходим баланс между методами предотвращения атак с одной стороны и возможностями сохранения работоспособности и восстановления с другой.

Государственные учреждения и частные организации создают комплексные модели, которые выходят за рамки безопасности и конфиденциальности для защиты активов, данных и других ресурсов в рамках киберустойчивости.

Разработка комплексного подхода к киберустойчивости

Для киберустойчивости необходим комплексный, адаптивный и глобальный подход, позволяющий бороться с меняющимися угрозами для базовых сервисов и инфраструктуры, включающий в себя:

- Базовые меры киберпрофилактики, описанные в нашей колоколообразной кривой киберустойчивости.
- Понимание компромисса между рисками/преимуществами цифровой трансформации и управление им.
- Возможности реагирования в реальном времени, позволяющие заранее обнаруживать угрозы и уязвимости.
- Защита от известных атак и профилактические меры против новых и ожидаемых направлений атак с возможностью автоматического исправления.
- Снижение воздействия атак и сбоев за счет изоляции неисправностей и сегментации сети.
- Автоматическое восстановление и резервирование в случае сбоя.
- Приоритизация операционного тестирования для выявления недостатков и понимания общих обязанностей и зависимостей от внешних ресурсов, таких как облачные решения по обеспечению безопасности.

Эффективная программа киберустойчивости начинается с фундаментальных аспектов, таких как понимание доступных сервисов и наличие надежного каталога ресурсов, которые можно использовать в случае сбоя. Применяя их в качестве основы, программа должна оценивать собственную эффективность, оценивать производительность критически важных

сервисов и их зависимостей, тестировать и проверять возможности локальных и облачных сервисов, а также поддерживать непрерывное улучшение на протяжении всего цифрового жизненного цикла организации.

Для реализации комплексного подхода мы сотрудничаем с организациями, чтобы выявить наиболее важные локальные и онлайн-сервисы, бизнес-процессы, зависимости, сотрудников и поставщиков. Мы также стремимся определить активы и ресурсы, связанные с ожиданиями клиентов и рынка, нормативными и договорными обязательствами и внутренними процессами. По мере выявления этих важных ресурсов параллельно следует обнаруживать и отслеживать угрозы, сбои, возможные направления атак, а также уязвимости в системах и процессах. Возможности для решения этой задачи на фоне дефицита квалифицированных специалистов ограничены, поэтому необходимо тщательно определить приоритеты на основе общего риска для организации.

Такой тип комплексного подход должен поддерживать адаптацию из-за постоянно меняющейся среды угроз для повышения производительности, ускорения обнаружения, реагирования и восстановления, а также уменьшения радиуса воздействия в случае сбоя. Этот подход должен также учитывать растущую взаимосвязанность угроз. Например, инцидент безопасности может привести к утечке данных с последствиями для конфиденциальности, что потребует совместной работы многих внутренних и внешних команд для быстрого реагирования и минимизации ущерба.

Киберустойчивость — это способность организации продолжать работу и поддерживать развитие, несмотря на сбои, в том числе кибератаки.

Практические рекомендации

- 1 Создавайте и контролируйте технологические системы, которые ограничивают влияние атаки и позволяют им продолжать работать безопасно и эффективно, даже если атака была успешной. Уделите внимание распространенным важным ресурсам, поддержке гибкости и адаптивной архитектуре (например, гибридной и мультиоблачной или мультиплатформенной), сократите возможные направления атак (например, удалите неиспользуемые приложения и излишние права доступа), всегда предполагайте, что ресурсы уже взломаны, и ожидайте эволюции злоумышленников.
- 2 При планировании цифровых проектов учитывайте потенциальные угрозы вместе с возможностями и разделяйте ответственность за устойчивость по всей цепочке поставок цифровых технологий, в том числе для облачных решений по обеспечению безопасности.
- 3 Создавайте решения со встроенной системой безопасности и принимайте меры для прогнозирования, обнаружения, предотвращения будущих угроз, адаптации мер защиты и реагирования на эти атаки.
- 4 Убедитесь, что бизнес-лидеры консультируются с отделами безопасности при необходимости, чтобы понимать риски, связанные с новыми разработками. В свою очередь, отделы безопасности должны учитывать бизнес-цели и информировать лидеров о том, как их достигать безопасным образом.
- 5 Убедитесь в наличии четких операционных методов и процедур для обеспечения киберустойчивости организации.

Важность модернизации систем и архитектуры

По мере разработки новых возможностей для эпохи повсеместного подключения к сети нам необходимо контролировать угрозы, которые создают устаревшие системы и ПО.

Устаревшие системы, разработанные до распространения современных инструментов подключения, такие как смартфоны, планшеты и облачные сервисы, представляют риск для организаций, которые по-прежнему их используют. Этот риск подтверждают выводы команды сервисов безопасности Microsoft для реагирования на инциденты — группы специалистов по безопасности, которая помогает клиентам реагировать на атаки и восстанавливаться после них.

За последний год проблемы, обнаруженные у клиентов, восстанавливающихся после атак, были связаны с 6 категориями, представленными на диаграмме на этой странице. На следующей странице описаны практические меры, которые необходимо принять для повышения устойчивости.

Больше 80 % инцидентов безопасности можно проследить до нескольких недостающих элементов, которые можно исправить с помощью современных подходов к безопасности.

Основные проблемы, влияющие на киберустойчивость



На этой схеме показана доля затронутых клиентов без базовых средств безопасности, которые имеют решающее значение для повышения киберустойчивости организации. Эти результаты основаны на операциях Microsoft за последний год.

«Лидеры должны считать киберустойчивость важнейшим аспектом устойчивости бизнеса. Они должны планировать реагирование на киберсбои так же, как для стихийных бедствий и других непредвиденных событий, а также объединять внутренние заинтересованные стороны, такие как операционный отдел, отдел коммуникаций, юридический отдел и т. д., для разработки стратегий. Это поможет им как можно быстрее вернуть в строй критически важные бизнес-системы, чтобы возобновить бизнес-операции.

Но это еще не все. Многие организации полагаются на сторонних поставщиков и сервис-провайдеров, поэтому лидеры должны распространить процесс планирования киберустойчивости на всю цепочку создания стоимости, чтобы обеспечить непрерывность и устойчивость бизнеса».

Энн Джонсон (Ann Johnson), корпоративный вице-президент по безопасности, соответствию, идентификации и управлению развитием бизнеса

Важность модернизации систем и архитектуры

Продолжение

Есть четкие проблемные области, которые компании могут улучшить для модернизации подхода и методов защиты от угроз:

Проблема	Практические действия
<p>Небезопасная конфигурация поставщика удостоверений</p> <p>Неправильная конфигурация и доступность платформ идентификации и их компонентов — это распространенное направление атаки для получения несанкционированного доступа с высокими привилегиями.</p>	<p>Соблюдайте базовые показатели конфигурации безопасности и рекомендации при развертывании и обслуживании систем идентификации, таких как AD и Azure AD.</p> <p>Реализуйте ограничения доступа, применяя разделение привилегий и принцип наименьших привилегий. Используйте рабочие станции с привилегированным доступом (PAW) для управления системами идентификации.</p>
<p>Недостаточный доступ к средствам контроля прав доступа и горизонтального перемещения</p> <p>Администраторы обладают чрезмерными разрешениями в цифровой среде, и часто их учетные данные доступны на рабочих станциях, подверженных различным рискам.</p>	<p>Защитите и ограничьте административный доступ, чтобы сделать среду устойчивее и ограничить область действия атаки. Используйте средства управления привилегированным доступом, такие как ограничение по времени и принцип необходимого минимума.</p>
<p>Отсутствие многофакторной аутентификации (MFA)</p> <p>Современные злоумышленники не взламывают систему, а входят в нее.</p>	<p>MFA — это критически важный и фундаментальный механизм контроля доступа пользователей, который должен быть реализован во всех организациях. В сочетании с условным доступом MFA может оказаться неоценимым в борьбе с киберугрозами.</p>
<p>Операции по обеспечению безопасности с низким уровнем зрелости</p> <p>Большинство пострадавших от злоумышленников компаний использовали традиционные инструменты обнаружения угроз и не обладали актуальной аналитической информацией для своевременного реагирования и устранения.</p>	<p>Для внедрения комплексной стратегии обнаружения угроз необходимы инвестиции в системы расширенного обнаружения угроз и реагирования на них (XDR) и современные облачные инструменты, использующие машинное обучение для отделения шума от подлинных сигналов. Модернизируйте инструменты управления безопасностью, используя систему XDR, которая будет анализировать безопасность во всей цифровой среде.</p>
<p>Отсутствие средств контроля защиты информации</p> <p>Организации по-прежнему сталкиваются с трудностями при разработке комплексных средств контроля защиты информации, которые бы обеспечивали полный охват различных сред хранения данных, сохраняли эффективность на протяжении всего жизненного цикла информации и были согласованы с уровнем важности данных для бизнеса.</p>	<p>Выявите критически важные бизнес-данные и их расположение. Проверяйте процессы жизненного цикла информации и применяйте средства защиты данных, обеспечивая непрерывность бизнеса.</p>
<p>Ограниченное внедрение современных систем безопасности</p> <p>Удостоверения — это новый периметр безопасности, обеспечивающий доступ к разрозненным цифровым сервисам и вычислительным средам. Интеграция принципа «Никому не доверяй», средств обеспечения безопасности приложений и других современных киберплатформ позволяет организациям активно управлять рисками, которые в противном случае они с трудом могли бы обнаружить.</p>	<p>Платформы на основе принципа «Никому не доверяй» применяют концепции наименьших привилегий, явной проверки всех попыток доступа и всегда предполагают компрометацию. Организациям также нужно внедрять средства контроля и методы обеспечения безопасности в DevOps и процессы жизненного цикла приложений для повышения надежности своих бизнес-систем.</p>

Базовый уровень безопасности — определяющий фактор эффективности передовых решений

В ходе анализа мы обнаружили широкое распространение общих слепых зон в защите организаций, которые позволяют злоумышленникам получить доступ, создать плацдарм и провести атаку даже при наличии передовых решений безопасности.

Часто исход кибератаки определяется задолго до ее начала. Злоумышленники используют уязвимые среды для получения первоначального доступа, наблюдения и нанесения ущерба посредством горизонтального перемещения, шифрования или извлечения данных. Если остановить злоумышленника на ранней стадии, существенно возрастает вероятность ограничить общий ущерб от атаки.

Корпорация Microsoft изучила определенные конфигурации систем безопасности, чтобы выявить самые распространенные недостатки этих сред. Так мы увидели наиболее распространенные уязвимости, используемые во время атак программ-шантажистов, управляемых человеком, которые позволили злоумышленникам получить доступ и перемещаться по сети незамеченными.

Базовые конфигурации безопасности всегда должны быть включены

Устройства организации, которые не подключены к системе управления или устарели (с точки зрения как уязвимостей, так и состояния агента безопасности), являются для злоумышленников потенциальными точками входа и способами получения доступа. Мы обнаружили, что подключение устройств к обновленному решению по обнаружению и нейтрализации атак на конечные точки¹ (EDR) и платформе защиты конечных точек² (EPP) является важным шагом, но оно не гарантирует защиту от программ-шантажистов.

Расширенные решения, такие как EDR и EPP, играют важную роль в обнаружении злоумышленника на ранней стадии атаки, автоматическом исправлении и защите. Но так как они полагаются на фундаментальную возможность обнаружения атаки, для их эффективного применения базовые конфигурации безопасности должны быть включены. На самом деле мы часто наблюдали, как работа продвинутых решений сводилась на нет из-за отсутствия базовых конфигураций безопасности.

Рекомендации по конфигурациям безопасности как индикатор устойчивости центра информационной безопасности

Мы наблюдали 70-процентное сокращение времени, необходимого аналитику центра информационной безопасности для просмотра оповещения и реагирования на него, в течение 6 месяцев среди наших клиентов и партнеров. Это хороший знак. Однако, хотя прозрачность конфигурации безопасности повысила производительность аналитиков безопасности, обеспечение прозрачности продуктов за счет подключения к системе управления и обновления устройств организации будет лучшим предиктором успешного предотвращения атак.

Риски, связанные с неизвестными устройствами

В отличие от облачных сетей, где клиенты знают, какие ресурсы запущены в тех или иных операционных системах, в локальных сетях может быть множество устройств, таких как устройства Интернета вещей, настольные компьютеры, серверы и сетевое оборудование, которые не отслеживаются и не контролируются организацией.

К типичной корпоративной сети подключено больше 3500 устройств, которые не защищены агентом EDR и могут получать доступ к корпоративным ресурсам или даже к ценным активам. Microsoft Defender для конечной точки (MDE) использует проверку сети для обнаружения устройств и предоставления информации о классификации устройств, подключенных к сети, такой как имя, дистрибутив операционной системы и тип устройства.

3500 —

среднее число подключенных к сети устройств в организации, которые не защищены агентом EDR.

Для устройств, не поддерживаемых агентом EDR, необходимо, по крайней мере, знать об их существовании и принимать меры для их защиты, оценивая уязвимости, а также ограничивая их доступ к сети.

Практические рекомендации

- 1 Даже самые передовые решения могут оказаться бесполезны при отсутствии базовых конфигураций безопасности.
- 2 Применяйте рекомендации по настройке конфигураций безопасности для защиты от будущих атак. Эти базовые параметры гарантируют огромную рентабельность инвестиций с точки зрения способности защиты от атак.
- 3 Подключите все соответствующие устройства к решению EDR.
- 4 Обязательно обновите агенты безопасности и обеспечьте защиту от несанкционированного доступа, чтобы улучшить прозрачность и защиту продуктов.

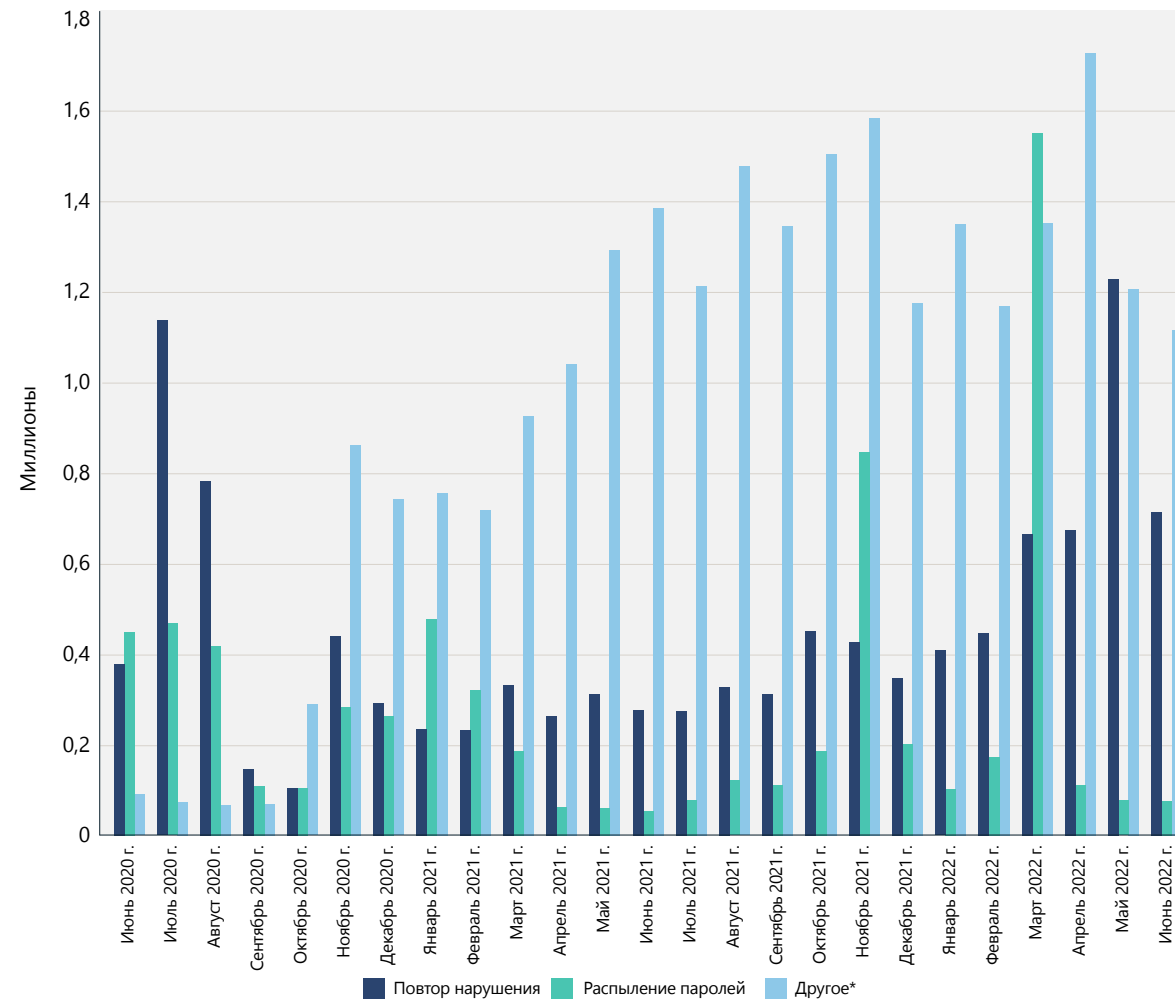
Поддержание работоспособности удостоверений имеет основополагающее значение для благополучия организации

Защита удостоверений сейчас важна как никогда. Атаки на основе паролей остаются основной причиной компрометации учетных данных, но появляются и другие типы атак. Число сложных атак продолжает расти по сравнению с прежней стандартной практикой распыления паролей и воспроизведения нарушений.

Атаки на основе паролей все еще распространены, и больше 90 % учетных записей, взломанных с помощью этих методов, не защищены строгой аутентификацией. Строгая аутентификация подразумевает использование нескольких факторов, например пароля, SMS-сообщения и ключей безопасности FIDO2.

Мы наблюдаем рост числа нацеленных атак с распылением паролей с очень большими всплесками объема вредоносного трафика, распространяющегося по тысячам IP-адресов.

Распределение скомпрометированных пользователей по категориям атак



Распределение скомпрометированных пользователей в месяц по категориям атак. Число атак с распылением паролей сильно менялось, как видно по всплескам в ноябре 2021 года и марте 2022 года. Эти пики представляют тысячи затронутых пользователей и тысячи IP-адресов. *В категории «Другое» представлены атаки, отличные от распыления паролей и воспроизведения нарушений, такие как фишинг, вредоносное ПО, «злоумышленник в середине», компрометация локального издателя токенов и другие. Источник: Azure AD Identity Protection.

4500

За время, которое требуется, чтобы прочитать это предложение, мы предотвратили 4500 атак с распылением паролей.

Поддержание работоспособности удостоверений имеет основополагающее значение для благополучия организации

Продолжение

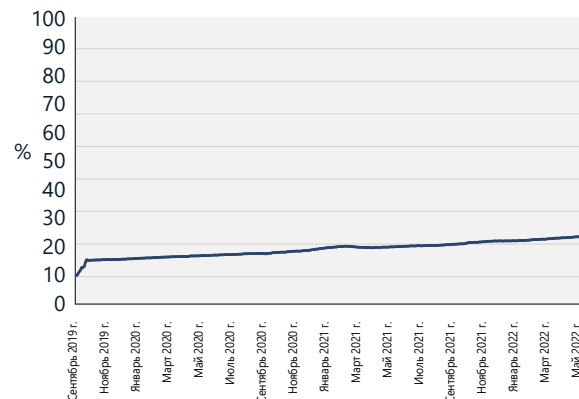
Внедрение строгой аутентификации

Из положительных моментов можно отметить устойчивый рост внедрения строгой аутентификации среди корпоративных клиентов Azure Active Directory (Azure AD). Для Azure AD ежемесячный объем активных пользователей строгой аутентификации (MAU) вырос с 19 % до 26 % в прошлом году, а MAU строгой аутентификации для учетных записей администраторов — с 30 % до примерно 33 %.

Эта положительная тенденция, но чтобы строгая аутентификация была распространена на большинство организаций, по-прежнему необходим значительный рост. Клиенты, которые еще не используют ее в своих средах, должны начать планирование и развертывание строгой аутентификации для защиты своих пользователей³.

При проектировании развертывания строгой аутентификации следует учитывать аутентификацию без пароля, так как это самый безопасный и удобный механизм, устраняющий риск атак на пароли.

Использование строгой аутентификации (сентябрь 2019 г. – май 2022 г.)

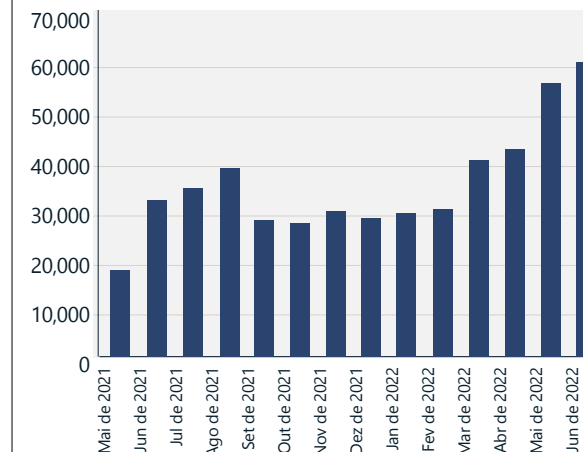


Применение строгой аутентификации удвоилось с 2019 года, но лишь 26 % пользователей и 33 % администраторов используют ее. Источник: Azure Active Directory.

Устойчивый рост числа атак с воспроизведением токена

Доля других типов атак увеличилась в 2022 году. Мы наблюдали рост нацеленных атак, которые специально избегают аутентификации на основе паролей, чтобы уменьшить вероятность обнаружения. Такие атаки используют файлы cookie системы единого входа (SSO) браузера или токены обновления, полученные с помощью вредоносных программ, фишинга и других методов. Иногда злоумышленники выбирают инфраструктуру рядом с целевым пользователем, чтобы еще больше снизить вероятность обнаружения. Мы наблюдаем устойчивый рост числа атак с воспроизведением токенов — их количество в Azure AD Identity Protection превысило 40 000 в месяц. Воспроизведение токенов означает использование токенов, которые были выданы авторизованному пользователю злоумышленником, обладающим указанными токенами. Часто токены получают с помощью вредоносного ПО, например получая файлы cookie из браузера пользователя или применяя расширенные методы фишинга.

Число обнаруженных атак с воспроизведением токенов



Число обнаруженных атак с воспроизведением токенов в месяц. Источник: Azure AD Identity Protection, уникальные сеансы, отмеченные при обнаружении аномальных токенов.

Поддержание работоспособности удостоверений имеет основополагающее значение для благополучия организации

Продолжение

Извлечение токенов

Для достижения своих целей злоумышленникам гораздо больше нужны не вредоносные программы, а учетные данные. На самом деле все атаки программ-шантажистов, управляемых человеком, применяют украденные учетные данные. В ходе многих изощренных вторжений используются учетные данные, приобретенные в даркнете, которые перед этим украли с помощью несложного и широко распространенного вредоносного ПО для кражи учетных данных. Этот класс вредоносного ПО теперь может красть и токены, в том числе данные сеанса и утверждения MFA. Это значит, что заражение домашних систем, из которых пользователи подключаются к корпоративным ресурсам, может привести к серьезным инцидентам в сетях организации.

Злоумышленники также могут извлекать токены с устройств жертв, применяя атаки типа «злоумышленник в середине», в ходе которых жертва переходит по вредоносной ссылке в фишинговом письме или мгновенном сообщении и перенаправляется на веб-сайт, который выглядит как подлинная страница входа поставщика удостоверений. На самом деле это веб-сервис, созданный злоумышленником, которая ретранслирует и перехватывает весь трафик между

пользователем и поставщиком удостоверений. Злоумышленник может перехватить имя пользователя и пароль, а также ретранслировать запросы защиты MFA. Маркеры, выданные поставщиком удостоверений и перехваченные злоумышленником, могут содержать утверждения MFA, которые можно использовать для удовлетворения требований MFA.

С начала 2022 года Microsoft Defender для облачных приложений обнаруживает в среднем 895 таких атак в месяц. Их можно предотвратить с помощью устойчивых к фишингу факторов MFA, таких как аутентификация на основе сертификатов, Windows Hello для бизнеса или ключи безопасности FIDO2.

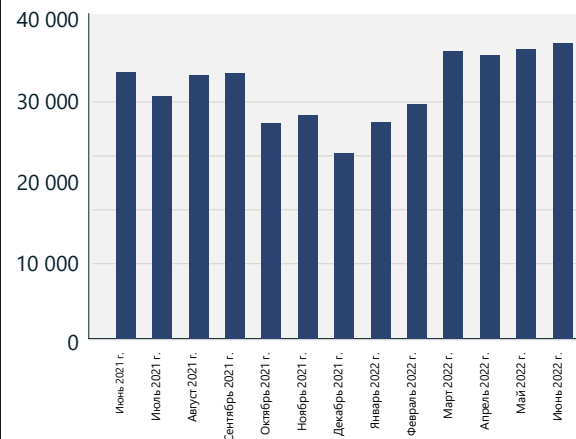
Атаки на основе паролей — этой основной метод взлома учетных записей.

Усталость от MFA

Используя концепцию «усталости от MFA», злоумышленники генерируют несколько запросов MFA для устройства жертвы, надеясь, что цель подтвердит запрос непреднамеренно или в результате усталости. Эту атаку можно предотвратить с помощью современных приложений для аутентификации, таких как Microsoft Authenticator, в сочетании с такими функциями, как сопоставление чисел⁴ и добавление дополнительного контекста⁵. По оценкам Azure AD Identity Protection, в месяц происходит 30 000 атак с использованием усталости от MFA.

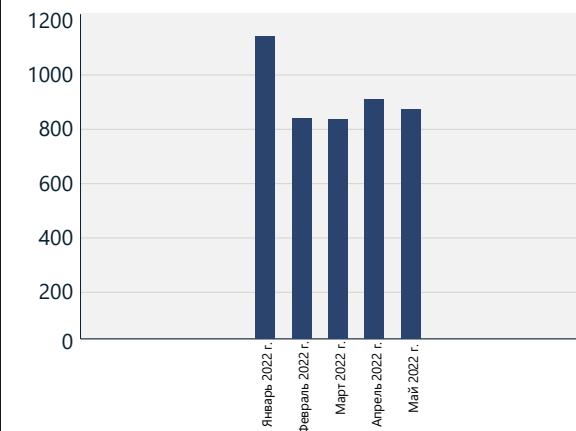
Доля сложных атак продолжает расти, что подчеркивает необходимость применения стойких к фишингу факторов MFA.

Предполагаемые случаи атак с использованием усталости от MFA



Источник: Azure AD Identity Protection.

Обнаруженные случаи фишинга с последующими атаками типа «злоумышленник в середине»



Источник: Microsoft Defender для облачных приложений.

Практические рекомендации

- 1 Убедитесь, что все учетные записи организации защищены строгой аутентификацией.
- 2 Аутентификация без пароля — это самый безопасный и удобный интерфейс, устраняющий риск стать жертвой атак на основе паролей.
- 3 Отключите устаревшую аутентификацию во всей организации.
- 4 Защитите ценные и административные учетные записи с помощью стойких к фишингу форм строгой аутентификации.
- 5 Перейдите с локального на облачного поставщика удостоверений и подключите к нему все приложения для согласованного взаимодействия с пользователем и усиления безопасности.

Ссылки на дополнительную информацию

- > Во Всемирный день паролей подумайте о том, чтобы полностью отказаться от паролей | Microsoft Security

Параметры безопасности операционной системы по умолчанию

Из-за непрерывно меняющейся среды угроз безопасности мы наблюдаем растущую потребность в конфигурации системы безопасности по умолчанию для повышения киберустойчивости. Хотя сейчас безопасность операционной системы стала как никогда критичной, сложной и важной для бизнеса, настроить и контролировать ее может быть довольно сложно.

Раньше система безопасности компьютеров и устройств предоставляла встроенные функции, которые клиент или ИТ-специалист должен был настроить по своему усмотрению. Теперь этот подход потерял актуальность, потому что злоумышленники используют продвинутые инструменты автоматизации, облачную инфраструктуру и технологии удаленного доступа для достижения своих целей. Критически важно, чтобы все уровни безопасности — от чипа до облака — были настроены с использованием конфигурации по умолчанию. Корпорация Microsoft перешла на настройку безопасности операционной системы Windows по умолчанию⁶.

Клиенты, которые используют глубокую защиту, в том числе многоуровневую систему безопасности, новые функции безопасности, регулярные и последовательные исправления

и обновления, а также проводят обучение и сеансы повышения осведомленности о фишинге и других мошенничествах, вправе ожидать меньше заражений вредоносным ПО.

Для упрощения глубокой защиты в Windows 11 по умолчанию включены тесно интегрированные аппаратные и программные средства защиты, такие как проверка целостности памяти, безопасная загрузка и Trusted Platform Module 2.0. Пользователи Windows 10 с соответствующим оборудованием также могут включить эти функции в приложении «Параметры Windows» или в меню BIOS.

У старых устройств во многих случаях нет такого сильного соответствия между аппаратной безопасностью и программными методами защиты. Устройства, на которых безопасность не включена по умолчанию, необходимо настроить вручную в параметрах, когда это возможно⁷.

Корпорация Microsoft рекомендует настроить параметры вручную устройств, на которых безопасность не включена по умолчанию, когда это возможно.

Применяйте упреждающий подход к установке обновлений операционной системы и исправлений системы безопасности, которые обеспечат защиту на протяжении всего жизненного цикла оборудования и ПО.

Практические рекомендации

- 1 Используйте решение без пароля, которое привязывает учетные данные для входа с Trusted Platform Module. В частности, выберите решение без пароля, соответствующее отраслевому стандарту Faster Identity Online (FIDO) Alliance⁸.
- 2 Своевременно удалите все неиспользуемые и устаревшие исполняемые файлы с устройств организации.
- 3 Защититесь от сложных атак на встроенное ПО, включив функцию проверки целостности памяти, безопасную загрузку и Trusted Platform Module 2.0, если они не включены по умолчанию. Это укрепит безопасность процесса загрузки с помощью возможностей, встроенных в современные процессоры.
- 4 Включите шифрование данных и защиту учетных данных.
- 5 Включите элементы управления приложениями и браузерами для надежной защиты от недоверенных приложений, а также другие встроенные средства защиты от эксплойтов.
- 6 Включите защиту доступа к памяти, чтобы предотвратить случайные физические атаки, таких как подключение вредоносного устройства к портам, доступным извне.

Ссылки на дополнительную информацию

- > Книга о безопасности Windows | Коммерческие организации
- > Новые функции безопасности Windows 11 помогут защитить работу в гибридной среде | Блог Microsoft Security

Акцент на цепочке поставки ПО

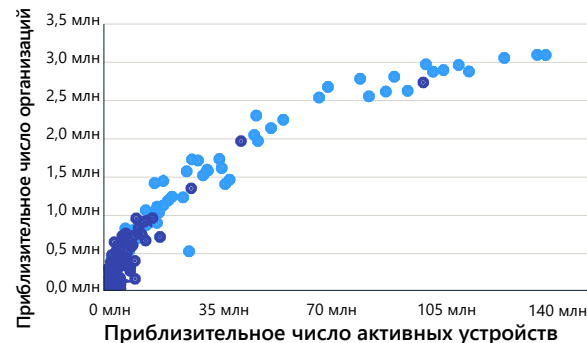
Атаки на сторонние приложения, подключаемые модули и расширения могут подорвать доверие клиентов к поставщикам, которые играют центральную роль в экосистеме поставок. Использование теории сетей для анализа центральности ПО дает возможность понять критичность исправления, особенно для базовых приложений.

Сеть приложений Windows, состоящая из 18 миллионов исполняемых файлов приложений, установлена и используется в 5 миллионах организаций, что дает нам общее представление экосистемы ПО. 97 % из 100 000 чаще всего используемых приложений разработаны сторонними поставщиками, которые выпускают соответствующие обновления и исправления системы безопасности. Это подчеркивает 2 важные черты нашей экосистемы коммерческих приложений.

Во-первых, в экосистеме коммерческих приложений Windows есть центральность. Только 100 000 (из 18 миллионов) приложений используются на 1000 или большем числе устройств. То есть чуть больше половины из 1 % этих приложений обладают таким широким охватом в экосистеме устройств.

Во-вторых, существует разнообразие методов управления этими приложениями: 10 000 крупнейших поставщиков управляют обновлениями и исправлениями системы безопасности чаще всего используемых коммерческих приложений. Это демонстрирует взаимозависимость компании от разнообразного набора средств контроля безопасности, соответствия требованиям и управления поставщиков ПО.

Коммерческое распространение чаще всего используемых приложений



Издатель ● Корпорация Microsoft ● Сторонние

Основные приложения используются миллионами организаций и десятками миллионов устройств. Так как они распространены почти везде, злоумышленники постоянно ищут в них уязвимости, которые могут повлиять на миллионы устройств в пользовательской базе.

Мы видим, что миллионы коммерческих устройств по-прежнему используют уязвимые версии приложений через много месяцев после выпуска исправлений или даже через несколько лет после прекращения поддержки продукта. Например, больше миллиона активных коммерческих устройств с Windows использует версия инструмента чтения PDF-файлов, которая не поддерживается с 2017 года.

Старые, неподдерживаемые версии приложений по-прежнему активно применяют на миллионах коммерческих устройств. Поэтому организации могут стать жертвой уязвимостей, которые не будут исправлены.

Для поддерживаемых версий приложений мы наблюдаем плато скорости установки критически важных исправлений, что противоречит тенденции, повышающей отказоустойчивость. Вместо этого кривая должна показывать экспоненциальное внедрение исправлений месяц за месяцем для достижения необходимой устойчивости.

Коэффициент развертывания критически важных исправлений



Изучив критическую уязвимость, которая затронула 134 версии набора браузеров, мы обнаружили, что 78 % (а это миллионы) устройств все еще использовали одну из уязвимых версий через 9 месяцев после выпуска исправления.

Мы использовали набор инструментов InterpretML⁹ для определения характеристик, коррелирующих с организациями, которые с большей вероятностью используют устройства с устаревшими версиями приложений. Вот важнейшие из этих факторов: небольшое время использования устройств, географические районы, такие как Азиатско-Тихоокеанский регион и Латинская Америка, отрасли, такие как автомобилестроение, химическая промышленность, телекоммуникации, транспорт и логистика, медицинское страхование (обработчики обращений) и иное страхование.

Поддержка отказоустойчивости ПО должна включать в себя регулярное отключение или удаление неиспользуемых приложений.

Безопасность и соответствие требованиям в организации зависят от ее собственных усилий и от мер, принимаемых поставщиками ПО.

Практические рекомендации

- 1 Своевременно устанавливайте обновления всех приложений и конечных точек в организации.
- 2 Своевременно удаляйте все неиспользуемые и устаревшие исполняемые файлы с устройств организации.

Ссылки на дополнительную информацию

- > Документация по Microsoft Intune | Документы Microsoft Docs
- > Управление приложениями | Microsoft Docs
- > Microsoft Defender для конечной точки | Microsoft Security
- > OSS Secure Supply Chain Framework | Microsoft Security Engineering
- > Microsoft Open Source Software Secure Supply Chain Framework | GitHub

Повышение устойчивости к новым DDoS-атакам, атакам на веб-приложения и сети

Ускоренная цифровая трансформация положила конец традиционной модели сети и безопасности на основе периметра. При переходе в облако организации должны внедрить облачную систему безопасности сети для защиты цифровых ресурсов.

Сложность, частота и объем атак продолжают расти, и они больше проводятся не только в праздники. Это указывает на то, что злоумышленники перешли круглогодичным атакам. Это подчеркивает важность непрерывной защиты за пределами традиционных периодов пикового трафика.

Распределенные атаки типа «отказ в обслуживании» (DDoS)

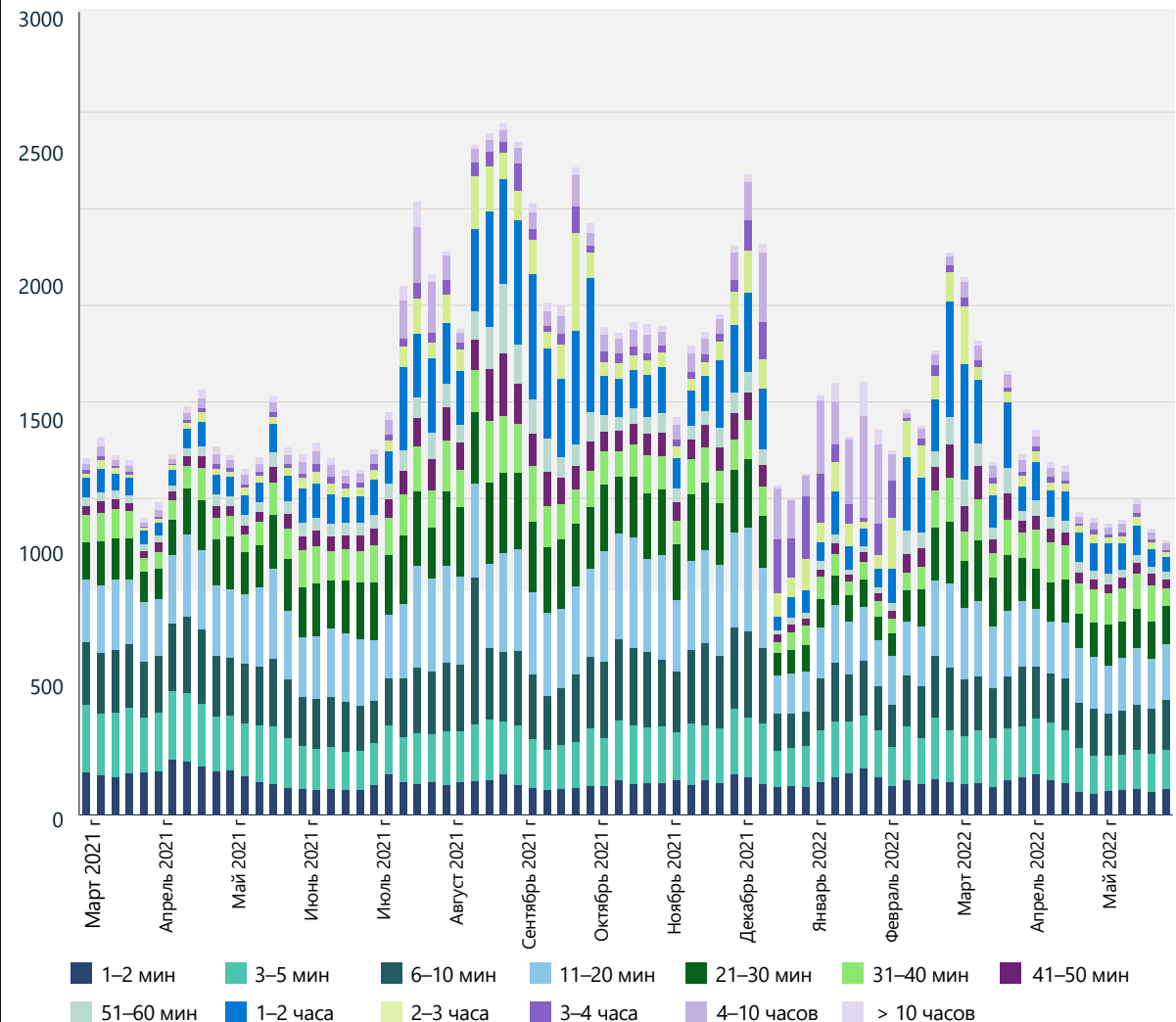
В прошлом году в мире наблюдалась беспрецедентная по объему, сложности и частоте активность DDoS-атак. Резкий всплеск числа DDoS-атак был вызван значительным увеличением киберопераций иностранных государств и распространением недорогих DDoS-сервисов. Корпорация Microsoft в среднем предотвращала 1955 атак в день, что на 40 % больше, чем в предыдущем году. В прошлом пиковое число атак приходилось на период праздников в конце года. Однако в этом году самое большое число атак было зафиксировано 10 августа 2021 года. Это может указывать на переход к круглогодичным атакам и подчеркивает важность непрерывной защиты за пределами традиционных периодов пикового трафика.

В ноябре 2021 года корпорация Microsoft сорвала масштабную DDoS-атаку с пропускной способностью 3,4 терабита в секунду (Тб/с) из примерно 10 000 источников из разных стран. Схожие по объему атаки с пропускной способностью больше выше 2 Тбит/с были устранены в 2022 году. Это говорит о том, что растет не только сложность, частота, но и объем (пропускная способность) атак.

Длительность атаки

Большинство атак, наблюдаемых за последний год, были краткосрочными. Примерно 28 % из них длились меньше 10 минут, 26 % — 10–30 минут, 14 % — 31–60 минут. 32 % атак длились больше 1 часа.

Число DDoS-атак и распределение их длительности (март 2021 г. — май 2022 г.)



Большинство атак в прошлом году были краткосрочными. Примерно 28 % атак длились меньше 10 минут.

Повышение устойчивости к новым DDoS-атакам, атакам на веб-приложения и сети

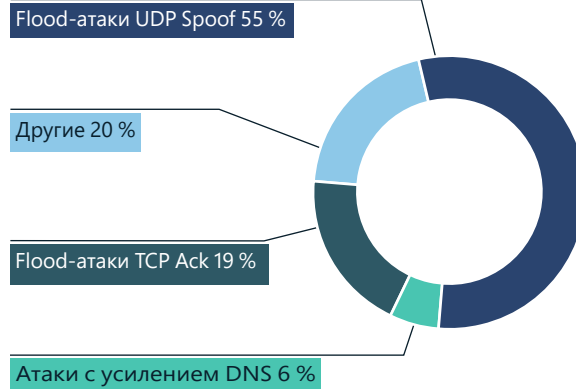
Продолжение

Направления DDoS-атак

В прошлом году самыми частыми направлениями атак стали отражение протокола UDP на порту 80 с использованием протокола SSDP, протокола CLDAP, системы доменных имен (DNS) и протокола NTP, которые составили единый пик. Мы также наблюдали рост числа DDoS-атак на уровне приложений, нацеленных на веб-сайты, с 16,3 миллиона пиковых запросов в секунду (RPS) и пиковым трафиком на уровне 9,89 Тбит/с.

В 2022 году корпорация Microsoft каждый день блокировала почти 2000 DDoS-атак и предотвратила крупнейшую в истории DDoS-атаку.

Направления DDoS-атак



Flood-атака UDP Spoof стала крупнейшей в первой половине 2022 года: ее показатель вырос с 16 % до 55 %. Показатель flood-атаки TCP Ack снизился с 54 % до 19 %.

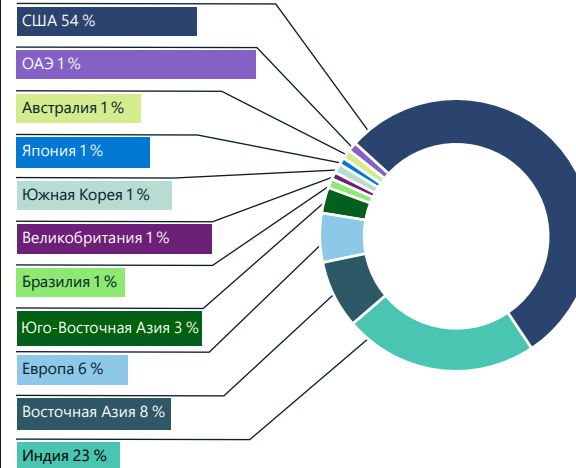


Игровая индустрия продолжает оставаться главной целью DDoS-атак, в основном с использованием мутаций ботнета Mirai и атак по протоколу UDP малого объема. Так как этот протокол часто применяется в игровых и стриминговых приложениях, подавляющее большинство направлений атак были flood-атаками UDP-спуфинга, в то время как небольшая часть были связаны с отражением и усилением по протоколу UDP.

Географические регионы, выбираемые в качестве цели

54 % DDoS-атак, обнаруженных за последний год, были проведены против целей в США. Эту тенденцию можно частично объяснить тем фактом, что большинство клиентов Azure и Microsoft находятся в США. Мы также наблюдали резкий всплеск атак на цели в Индии, при этом 2 % из них пришлось на вторую половину 2021 года, а 23 % — на первое полугодие 2022 года. Восточная Азия, в частности Гонконг, остается популярной целью на уровне 8 %. В Европе атаки были сосредоточены на Амстердам, Вена, Париж и Франкфурт.

Цели DDoS-атак

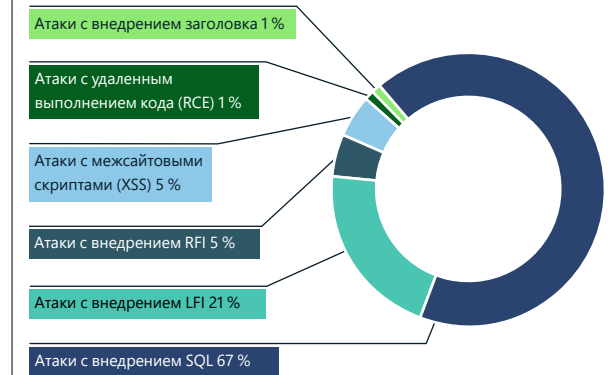


Мы связываем большой объем атак в Азии с большим числом игроков, особенно в Китае, Японии, Южной Корее и Индии. Это тенденция будет продолжаться, так как из-за распространения смартфонов растет популярность мобильных игр, а значит число атак на этот регион будет увеличиваться.

Эксплойты веб-приложений

Брандмауэр веб-приложений (WAF) в сочетании с защитой от DDoS-атак служит неотъемлемой частью стратегии глубокой защиты ресурсов веб-интерфейсов и интерфейсов прикладного программирования (API). Корпорация Microsoft наблюдала больше 300 миллиардов активаций правил WAF в месяц в Azure.

Распределение самых распространенных типов атак



Azure WAF ежедневно обнаруживает миллиарды 10 самых распространенных атак OWASP (Open Web Application Security Project) (OWASP)¹⁰. Согласно полученным сигналам, злоумышленники чаще всего пытались использовать атаки с внедрением SQL-кода, за которыми следовали попытки внедрения кода в локальные файлы и удаленных атак путем внедрения файлов. Это соответствует списку 10 основных атак OWASP, в котором атаки с внедрением являются третьим по распространенности типом веб-атак.

Кроме того, увеличилось число атак ботов на веб-приложения Azure: 1,7 миллиарда запросов ботов в среднем за месяц, 4,6 процента этого трафика составляют вредоносные боты.

Повышение устойчивости к новым DDoS-атакам, атакам на веб-приложения и сети

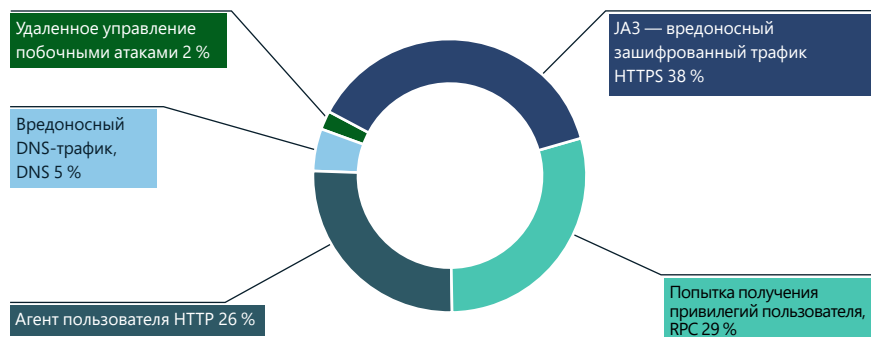
Продолжение

Из-за растущего количества ботов, проводящих атаки со вставкой учетных данных, мошенничество с кредитными картами, кампании кибер-влияния и атаки на цепочку поставок, мы ожидаем устойчивый рост атак ботов на веб-приложения.

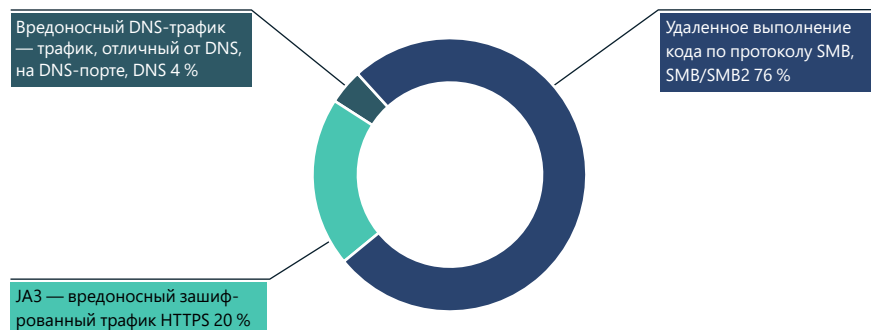
Вторжение в сеть: обнаружение и предотвращение

В 2022 году мы видели значительное увеличение числа эксплойтов сетевого уровня, особенно вредоносного ПО. Только в июне система обнаружения и предотвращения вторжений (IDPS) брандмауэра Azure заблокировала больше 150 миллионов подключений.

Причина блокировки трафика в IDPS



Причины оповещения о трафике в IDPS



Анализ оповещений и блокировки трафика в IDPS демонстрирует следующие подходы, используемые злоумышленниками. В категории «Блокировка трафика» мы видим, что злоумышленники используют протокол SSL для сокрытия своих действий, при этом число атак с удаленным выполнением кода растет. В категории «Оповещения о трафике» мы наблюдаем, что для атак с удаленным выполнением используются протоколы SMB/SMB2.

Практические рекомендации

- 1 Проверьте весь трафик между системами в центре обработки данных или облачном сервисе, а также трафик, стремящийся получить к ним доступ.
- 2 Разработайте надежную стратегию непрерывного реагирования на инциденты сетевой безопасности.
- 3 Используйте встроенные облачные сервисы безопасности для реализации надежной системы защиты сети на основе принципа «Никому не доверяй».

Ссылки на дополнительную информацию

- > Улучшите защиту от атак программ-шантажистов с помощью брандмауэра Azure | Блоги и обновления Azure | Microsoft Azure
- > Структура DDoS-атаки с усилением | Блог Microsoft Security
- > Интеллектуальная защита приложений от периметра до облака с помощью брандмауэра веб-приложений Azure | Блоги и обновления Azure | Microsoft Azure

Разработка сбалансированного подхода к безопасности данных и киберустойчивости

Цифровая трансформация привела к существенному росту объемов данных и рисков безопасности, соответствия требованиям и конфиденциальности. Киберустойчивые организации должны сбалансировать инвестиции в средства защиты данных, обеспечения соответствия требованиям и возможности восстановления, а также интегрировать их со специализированными процессами реагирования надзорных органов для устранения различных типов нарушений.

Вопрос состоит не в том, будет ли утечка данных, а в том, когда это произойдет. В исследовании «Cost of a Data Breach, 2021», проведенном IBM и Ponemon Institute, указано, что средний ущерб от утечки данных во всем мире составляет 4,24 миллиона долларов (на 10 процентов больше, чем в предыдущем году) и 9,05 миллиона долларов в США. Основным фактором, влияющим на сумму ущерба, оказались недостатки в соблюдении нормативных требований. И наоборот, снижение ущерба от утечки данных связано с применением рекомендаций, таких как планирование реагирования на инциденты (IR), зрелость развертывания модели «Никому не доверяй», ИИ, автоматизация процессов обеспечения безопасности и использование шифрования.

Утечки данных неизбежны. Организации, применяющие сбалансированный подход к обеспечению устойчивости, могут снизить частоту, воздействие нарушений и ущерб от них.

Управление данными, безопасность, соответствие требованиям и конфиденциальность взаимосвязаны

В последние годы мы видим, что данные становятся важнейшим механизмом создания ценности для организаций. В то же время из-за расширения нормативных требований, регулирующих как управление данными, так и безопасность, размылись границы между ролями, связанными с риском. Новые роли высшего звена, такие как директор по данным (CDO) или директор по конфиденциальности (CPO), напрямую заинтересованы в безопасности и соответствии требованиям, внедрение и использование средств защиты данных часто зависит от команд, возглавляемых ИТ-директорами (CIO) и (или) директором по информационной безопасности (CISO). Это не улица с односторонним движением, так как инициативы в области управления данными, которыми руководят CDO, также дают преимущества в сфере безопасности. В результате такой взаимосвязанности отделы ИТ, управления данными, безопасности, соответствия требованиям и конфиденциальности должны работать теснее для достижения эффективности и управления рисками.

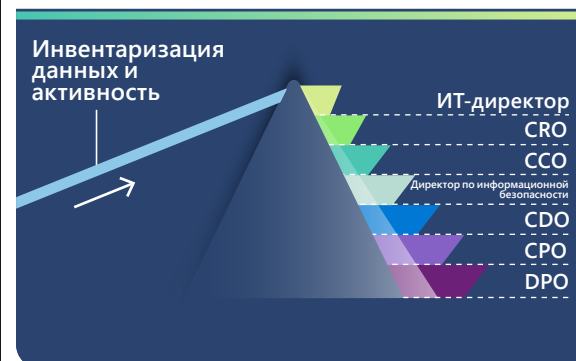
Единые платформы управления рисками для всего массива данных организации — это будущее

Согласование управляющих процессов отделов ИТ, управления данными, безопасности, соответствия требованиям и конфиденциальности затруднено из-за разрозненности приложений для каждого из этих

направлений и несогласованного охвата в типичном гибридном и мультиоблачном распределении данных организации. Мы считаем, что организациям нужна единая панель управления для поиска, просмотра и защиты данных, контроля доступа, использования и жизненного цикла данных, а также предотвращения потери данных во всей среде.

Работа с одними и теми же данными инвентаризации и сведениями об операциях упрощает межведомственное взаимодействие, дает полное представление о рисках и позволяет компаниям лучше подготовиться и оптимизировать реагирование на нарушение.

Единая панель управления должна стать своего рода призмой. Командам, участвующим в обеспечении безопасности данных, соответствия требованиям и конфиденциальности, необходимы разные, но согласованные представления одних и тех же данных инвентаризации и действий, чтобы они могли эффективно сотрудничать. К действиям с данными относятся доступ к данным, их изменение и перемещение — это важные переменные в процессе защиты данных.



Эффективные процессы управления данными, безопасности, соответствия требованиям и конфиденциальности взаимосвязаны и требуют сотрудничества между командами.

Практические рекомендации

- 1 Необходимо найти баланс между защитой и восстановлением, а также минимизировать влияние утечки данных, инвестируя средства и ресурсы в возможности обеспечения соответствия требованиям, защиты данных и реагирования на нарушения безопасности.
- 2 Разрабатывайте и внедряйте процессы и инструменты, которые устраняют разрозненность рисков и охватывают всю среду данных.

Ссылки на дополнительную информацию

- > Microsoft Purview — решения для защиты данных | Microsoft Security
- > Будущее соответствия требованиям и управления данными уже здесь: представьте Microsoft Purview | Блог Microsoft Security

Устойчивость к кибероперациям по распространению влияния: человеческое измерение

За последние 5 лет развитие графики и машинного обучения позволило получить простые в использовании инструменты, быстро создающие высококачественный реалистичный контент, который может широко распространяться по Интернету за считанные секунды.

Мы достигли точки развития, когда ни люди, ни алгоритмы не могут надежно отличить факты от вымысла, потому что о глобальных событиях сообщают с помощью текстового, звукового и визуального контента. Распространение таких средств и их результатов ставит под сомнение надежность всех цифровых средств массовой информации, искажая понимание местных и международных событий. Новые формы операций по распространению влияния, ставшие возможными благодаря технологическим достижениям, могут оказаться серьезными последствиями на демократические процессы¹¹.

Возникают вопросы о том, что можно сделать, чтобы сделать будущее устойчивее к подобным кибероперациям по распространению влияния. Но технологии — это лишь одна часть головоломки. Потребуется много усилий, в том числе обучение медиаграмотности, осведомленности и бдительности, инвестиции в качественную журналистику с настоящими профессионалами на местном, национальном и международном уровнях, сети обмена данными и оповещения об операциях по распространению влияния, а также новые нормативные требования, которые наказывают злоумышленников, создающих цифровые медиа или манипулирующие с целью обмана.

Мы также признаем, что восстановление доверия к цифровому контенту — это амбициозная цель, для достижения которой потребуются различные точки зрения и участники. Нет ни одной компании, учреждения или правительства, которое могло бы справиться с этими угрозами в одиночку. Наша сверхсила как людей — это способность работать вместе и кооперироваться. Это особенно важно сейчас, потому что это потребует от всех — правительств по всему миру, отраслей, ученых и особенно новостных, социальных и медийных организаций — совместной работы для улучшения нашего общества.



Ссылки на дополнительную информацию

- > Приложения на основе искусственного интеллекта в кибероперациях министерства обороны | Microsoft On the Issues
- > Artificial Intelligence and Cybersecurity: Rising Challenges and Promising Directions. Hearing on Artificial Intelligence Applications to Operations in Cyberspace before the Subcommittee on Cybersecurity, of the Senate Armed Services Committee, 117th Congress (3 мая 2022 г., выступление Эрика Хорвица (Eric Horvitz))

Укрепление человеческого фактора за счет развития навыков

Учет человеческого фактора необходим для любой стратегии развития навыков кибербезопасности. Согласно исследованию Kaspersky Human Factor in IT Security¹², 46 % инцидентов кибербезопасности связаны с небрежными или одетыми в форму сотрудниками, которые непреднамеренно способствуют атаке.

Команда Microsoft по образованию и повышению осведомленности из организации Digital Security and Resilience отвечает за укрепление человеческого фактора кибербезопасности, позволяя сотрудникам защищать собственные системы и данные, а также системы и данные наших клиентов. Наши цели:

- Снизить риски для Microsoft и наших клиентов, создав централизованный базовый набор навыков безопасности среди всех сотрудников компании.
- Укрепить знания сотрудников в области безопасности с помощью многоэтапного подхода для получения желаемого поведения.
- Стимулировать изменение культуры, сделав ориентированное на безопасность мышление неотъемлемой частью культуры Microsoft с помощью ежегодных тренингов и мероприятий по безопасности.

- Поддерживать универсальный централизованный веб-ресурс с рекомендациями, информацией о политике компании и отчетами об инцидентах по всем вопросам, связанным с кибербезопасностью.

Адаптированная централизованная программа обучения в области кибербезопасности затрагивает каждого сотрудника корпорации Microsoft не реже одного раза в год. Тренинги оптимизированы для поддержки текущих инициатив в области кибербезопасности и получения измеримых результатов. Совет Microsoft по управлению информационными рисками (IRMC) играет ключевую роль в определении важных результатов изменения поведения в области кибербезопасности, которых необходимо достичь с помощью обучения.

С помощью всех программ обучения в области кибербезопасности мы оцениваем эффективность, результативность и результаты решения, где это возможно. Например, результатом нашего тренинга по методам борьбы с внутренними угрозами стали 95-процентное соответствие требованиям к обучению, высокая удовлетворенность учащихся и существенное увеличение числа менеджеров, сообщающих о возможных случаях внутренних угроз с помощью инструмента Report It Now. Обучающая программа посвящена следующим темам:

Основы безопасности — централизованный курс по кибербезопасности и соответствию требованиям в масштабах всего предприятия, в котором рассматриваются базовые методы обеспечения безопасности и конфиденциальности. В этой долгожданной серии тренингов используется модель развлекательного образования, чтобы сделать изучение кибербезопасности привлекательным и интересным.

STRIKE — обязательный технический курс Microsoft для инженеров, которые разрабатывают и поддерживают бизнес-решения. Этот тренинг

с участием только по приглашениям охватывает своевременные и критически важные области киберпрофилактики и использует динамическую гибридную модель доставки, адаптированную к потребностям аудитории.

Специализированные программы — целевые учебные программы, которые поддерживают конкретные инициативы в области кибербезопасности, такие как теневые ИТ, внутренние угрозы и Microsoft Federal. Эти тренинги тесно интегрированы в общую стратегию взаимодействия для соответствующих инициатив в области кибербезопасности за счет поддержки со стороны руководства и отчетности по системам показателей, чтобы не допустить формальный подход к обучению.

MSProtect — централизованный веб-ресурс Microsoft содержит рекомендации, информацию о политике компании и отчеты об инцидентах по всем вопросам, связанным с кибербезопасностью. Этот ресурс, доступный по запросу, предназначен для сотрудников, не проходящих официальные учебные курсы.

Навыки обеспечения безопасности не следует рассматривать как формальную проверку «для галочки». Вместо этого необходимо сделать акцент на изменении поведения, чтобы отслеживать результаты по достижению целевого поведения, и создайте системы анализа для определения влияния обучения.

Практические рекомендации

- 1 Проводите обучение и предоставляйте ресурсы по безопасности для сотрудников, когда и где им это необходимо.
- 2 Разработайте централизованную стратегию обучения навыкам, основанную на заинтересованных сторонах со всей организации.
- 3 Отслеживайте и анализируйте влияние обучения на продуктивность (количество), эффективность (качество) и результаты (влияние на бизнес).

Ссылки на дополнительную информацию

- Корпорация Microsoft запускает следующий этап инициативы по развитию навыков, которая уже помогла 30 миллионам человек

Уроки, извлеченные из нашей программы ликвидации программ-шантажистов

За последние 5 лет корпорация Microsoft самостоятельно модель «Никому не доверяй»¹³, чтобы реализовать надежное управление удостоверениями и устройствами, а также обеспечить их работоспособность. По мере роста риска атак программ-шантажистов мы обработали огромные объемы данных для поддержки нашего подхода к защите компании и наших клиентов.

После тщательной внутренней оценки мы разработали программу борьбы с атаками программ-шантажистов, чтобы устранить недостатки в контроле и охвате, внести свой вклад в улучшение функций для таких сервисов, как Defender для конечной точки, Azure и M365, а также разработать руководства по восстановлению систем в случае атаки программ-шантажистов для наших центров информационной безопасности и инженерных команд.

Первым шагом стала оценка степени защиты от атаки программ-шантажистов, направленных на корпорацию Microsoft. Уже полным ходом шли развертывание Defender для конечной точки и перевод всех устройств на процессы управления и обеспечения соответствия на базе модели «Никому не доверяй». Но нам требовался способ оценки всех аспектов вопроса помасштабнее: сможем ли мы эффективно восстановиться после атаки? Чтобы получить ответ на него, мы изучили документ NIST 8374: Ransomware Risk Management: A Cybersecurity Framework (CSF) Profile¹⁴, который соответствует общей корпоративной политике по сравнению с известным списком механизмов контроля. В результате анализа мы быстро выявили пробелы в охвате.

Затем мы приоритизировали недостатки функций идентификации, обнаружения, защиты, реагирования и восстановления стандарта CSF. Мы обнаружили стратегическое соответствие модели «Никому не доверяй» и другим программам, а также обнаружили пробелы, которые не имели существующего рабочего потока. Оценив объем работы и усилий, необходимых для их устранения, мы разделили их на 2 категории:

- **Защита предприятия (PtE)** — определение задач, которые мы должны выполнять как организация, чтобы защитить себя и иметь возможность восстановиться после успешной атаки.
- **Защита клиента (PtC)** — добавление возможностей в наши предложения для защиты клиентов и нашего бизнеса.

Применение результатов в нашей организации

Чтобы устранить главные риски и защитить критически важные сервисы от атаки программ-шантажистов, мы планируем сосредоточить

инвестиции в течение следующих 6–12 месяцев на следующих 5 сценариях в рамках специальной программы борьбы с программ-шантажистами. После успешной реализации каждого из этих сценариев мы постепенно расширим охват программы, чтобы охватить все подразделения компании.

Сценарий 1. Сотрудники отдела безопасности понимают общие риски, связанные с атакой программ-шантажистов, им доступен формальный процесс для информирования руководителей о недостатках в контроле и анализе рисков.

Сценарий 2. У сотрудников отдела безопасности есть доступ к руководствам, которые помогут им и другим отделам Microsoft реагировать на атаки программ-шантажистов на критически важные сервисы и восстанавливать их.

Сценарий 3. У сотрудников подразделения Enterprise Resilience есть стандарт, которому необходимо следовать при резервном копировании критически важных систем. Созданы необходимые руководства, регулярно проводятся упражнения по резервному копированию и восстановлению, чтобы обеспечить возможность восстановления данных в случае атаки программ-шантажистов.

Сценарий 4. Владельцы сервисов понимают и реализуют необходимые средства контроля и политики безопасности и эксплуатации для защиты своих сервисов, данных клиентов, конечных точек и сетевых ресурсов от атак программ-шантажистов с особым акцентом на критически важные сервисы Microsoft.

Сценарий 5. Все сотрудники могут получить доступ к образовательным и учебным ресурсам, которые помогают распознать атаку программ-шантажистов, уведомить отдел безопасности и принять меры.

Практические рекомендации

- 1 Документируйте и проверяйте все операции восстановления и исправления, связанные с атаками программ-шантажистов на критически важные сервисы.
- 2 Привлекайте заинтересованные стороны к обновлению ваших руководств по управлению кризисными ситуациями, чтобы конкретные действия, процесс принятия решений и инструкции, связанные с атакой программ-шантажистов, позволяющие определить, следует ли платить вымогателям.
- 3 Расширьте охват средств обнаружения и защиты, включив возможности, доступные в развернутых продуктах обеспечения безопасности (например, правила сокращения возможных направлений атак Defender для конечной точки).
- 4 Вместе с командой по стандартизации процессов безопасности определите базовый уровень защиты от атаки программ-шантажистов, организуйте обучение и предоставьте документацию инженерным группам о том, как защититься от таких атак.
- 5 Используйте автоматизацию, чтобы упростить развертывание политик безопасности и операционных политик в командах DevOps, а также гарантировать быстрое обнаружение и устранение инцидентов в случае возникновения аномалий.

Ссылки на дополнительную информацию

- > Как корпорация Microsoft защищается от программ-шантажистов | Microsoft Inside Track

Необходимость немедленного принятия мер по защите квантовых вычислений

Угроза, которую квантовые вычисления представляют для современной криптографии и всего, что она защищает, очень серьезна, поэтому необходим способ ее контролировать. В недавно выпущенном министерством обороны США и организацией Intelligence Community Systems меморандуме об улучшении кибербезопасности национальной безопасности¹⁵, основанном на указе президента США № 10428¹⁶ об улучшении национальной кибербезопасности страны, подчеркивается, что безопасность цепочки поставок ПО имеет решающее значение для борьбы с будущими атаками иностранных государств.

Что такое квантовые компьютеры?

Квантовые компьютеры — это устройства, использующие свойства квантовой физики для хранения данных и выполнения вычислений. Они могут очень эффективно решать определенные задачи, значительно превосходя даже лучшие суперкомпьютеры. Квантовые вычисления уже открывают новые горизонты в области шифрования и обработки данных. Согласно исследованиям, квантовые вычисления станут многомиллиардной индустрией уже в 2030 году¹⁷. На самом деле квантовые вычисления и квантовая связь смогут трансформировать множество отраслей — от

здравоохранения и энергетики до финансов и безопасности.

Квантовые вычисления представляют угрозу для современной криптографии и всего, что она защищает.

Угроза современной криптографии

После разработки алгоритма Шора в 1994 году и появления промышленного квантового компьютера с несколькими миллионами физических кубитов все современные и широко распространенные криптографические алгоритмы с открытым ключом могут быть эффективно взломаны. Поэтому необходимо проанализировать, оценить и стандартизировать «квантово-безопасные» криптосистемы, которые будут эффективными, гибкими и защищенными от козлятательной квантовой атаки. Переход ПО на «постквантовую криптографию», а именно на существующие классические алгоритмы и протоколы, устойчивые к квантовым атакам, займет годы, если не десятилетие или больше¹⁸.

Это значит, что угроза для современной криптографии и всего, что она защищает, очень серьезна, поэтому необходим способ ее контролировать. Злоумышленники могут записать зашифрованные данные сейчас и использовать их позже, когда квантовый компьютер станет доступен. Ждать появления квантовых вычислений, прежде чем рассматривать их последствия для криптографии, бессмысленно.

Криптография используется во всей киберэкосистеме, то есть наши сервисы безопасности на основе криптографии могут быть скомпрометированы. Например, к ним относятся сервисы связи (TLS, IPSec), обмена сообщениями (электронная почта, веб-конференции), управления идентификацией и доступом, просмотра веб-страниц, подписи кода, платежных транзакций и другие сервисы, которые применяют криптографию для защиты.

По мере того как квантовые компьютеры становятся все ближе к реальности, также потребуется дополнительно изучить сторонние программные компоненты, содержащие реализации криптографических алгоритмов и возможностей. Для этого организации по всей цепочке создания стоимости должны внести свой вклад в обеспечение безопасности цепочки. Отраслевые организации и правительства наращивают усилия по определению требований к безопасности цепочки поставок ПО, а в некоторых случаях вводят новые требования для обеспечения безопасности цепочки. Документ National Security Memorandum NSM-8¹⁹ устанавливает требования и сроки внедрения постквантовой криптографии в системах национальной безопасности. В нем указано, что в течение 180 дней необходимо «запланировать модернизацию, использование неподдерживаемого шифрования, утвержденных уникальных протоколов, квантово-устойчивых протоколов и квантово-устойчивой криптографии там, где это необходимо».

Стандартизация — это долгосрочная инициатива по переходу к квантово-безопасной криптографии. Органы, которые работают над стандартами, использующими криптографию с открытым ключом, должны начать экспериментировать и адаптироваться к постквантовым алгоритмам уже сейчас.

Новые алгоритмы постквантовой криптографии (PQC) — это классические алгоритмы, которые считаются устойчивыми к квантовым атакам. Сейчас они рассматриваются в рамках проекта постквантовой стандартизации NIST²⁰. Эта работа повлияет на международные усилия органов по стандартизации. Хотя и будет определенное пересечение с набором алгоритмов правительства США, различные результаты выбора национальными и надзорными органами совместимых алгоритмов могут вызвать международные проблемы. Такая фрагментация, в свою очередь, усложнит проектирование продуктов и сервисов.

Новые криптографические алгоритмы, стойкие к квантовым атакам, находятся на рассмотрении в рамках программы стандартизации постквантовой криптографии NIST. Эта работа окажет влияние на международные усилия органов по стандартизации.

Практические рекомендации

Наряду с SAFECode и участвующими партнерами вся отрасль должна принять немедленные краткосрочные меры для подготовки к переходу на PQC²¹. К ним относятся:

- 1 Инвентаризация кода и продуктов, использующих криптографию.
- 2 Реализация в организации стратегия криптографической гибкости, которая включает в себя минимизацию модификации кода, необходимого при изменении криптографических алгоритмов.
- 3 Проверка использования потенциально квантово-безопасных алгоритмов в продуктах или сервисах, использующих криптографию.
- 4 Подготовка к применению различных алгоритмов с открытым ключом для шифрования, обмена ключами и подписи.
- 5 Тестирование приложений на предмет влияния очень больших размеров ключей, шифров и подписей.

Ссылки на дополнительную информацию

- > Корпорация Microsoft представила базовые физические концепции, необходимую для создания нового вида кубита | Microsoft Research

Интеграция бизнес-подразделений, отдела безопасности и ИТ-отдела для повышения устойчивости

Надежная киберустойчивость зависит от бизнес-лидеров, работающих с отделами безопасности над обеспечением безопасности в организации. По опыту корпорации Microsoft, руководство в области безопасности — сложная работа, которая требует поддержки со стороны лидеров организации для наиболее эффективной защиты организации.

Лидеры в области безопасности сталкиваются со множеством меняющихся проблем, связанных с рисками, технологиями, экономикой, организационными процессами, бизнес-моделями, трансформацией культуры, геополитическими интересами, шпионажем и соблюдением международных санкций. Все они обладают нюансами, которые следует тщательно изучить и контролировать.

Кроме того, лидеры в области безопасности должны препятствовать как опытным, хорошо финансируемым и мотивированным злоумышленникам, так и низкоквалифицированным, но эффективным киберпреступникам. Их команды должны защищать сложные технические среды, часто заложенные 30 лет назад, когда безопасности уделяли не такое внимание, как сейчас. Решения, принятые много лет назад, могут создавать риски сегодня, пока мы не

погасим технический долг и не устраним недостатки системы безопасности.

Лидеры организаций и надзорные органы могут оказать сильное положительное влияние на безопасность, активно поддерживая лидеров в этой области и помогая связать интегрированную систему безопасности и остальные части организации. По опыту корпорации Microsoft, клиенты, которые решили эту задачу, повышают свою устойчивость и гибкость для адаптации и внедрения инноваций.

Руководители организаций могут поддержать лидеров в области безопасности, сосредоточив внимание на 3 ключевых областях:

1. Реализация встроенной системы безопасности

Безопасность иногда рассматривают как препятствие или оставляют напоследок в бизнес-процессах. Часто ее начинают реализовывать в решениях, когда уже слишком поздно, потому что избежать рисков или исправить систему без значительных затрат уже невозможно.

Лидеры организаций и надзорные органы должны проследить за тем, чтобы они:

Реализовали систему безопасности новых инициатив с самых ранних этапов.

Новые инициативы цифровой трансформации и внедрения облачных технологий должны уделять особое внимание безопасности, чтобы риски для организации не росли с каждым новым приложением или цифровыми возможностями. После надежной реализации безопасности вы можете использовать эти процессы для модернизации устаревших систем, чтобы одновременно повысить уровень безопасности и производительности.

Сделали профилактические меры для обеспечения безопасности нормой.

Обеспечьте базовое обслуживание системы безопасности, например установку обновлений

и исправлений, а также использование безопасных конфигураций, с полной поддержки со стороны организации (включая бюджеты, запланированные простои, требования к приобретению для поддержки продуктов поставщиков и т. д.).

К сожалению, многие организации откладывают внедрение этих мер на потом или применяют их лишь частично. Это дает злоумышленникам широкие возможности. Необходимость в стандартизации мер безопасности отражена в документе US NIST 800-40²².

2. Взаимодействуйте со специалистами по безопасности

Лидеры организаций должны активно участвовать в важнейших процессах обеспечения безопасности и поддерживать их для приоритизации ресурсов и подготовки к нарушениям безопасности. К этим процессам относятся:

Выявление критически важных бизнес-активов.

Руководителям и отделам безопасности необходимо знать, какие активы критически важны для бизнеса, чтобы сосредоточить на них ресурсы безопасности. Многим организациям приходится делать это впервые, в том числе формулировать новые вопросы, которые ранее не рассматривались, и отвечать на них.

Процедуры непрерывности бизнеса и аварийного восстановления, связанные с кибербезопасностью.

Кибератаки могут стать масштабными событиями, которые прерывают или полностью останавливают все бизнес-операции или их большую часть. Если убедиться в готовности команд по всей организации к таким ситуациям, организации ускорят восстановление бизнес-операций, ограничат ущерб и смогут сохранить доверие клиентов, граждан и избирателей. Эту процедуру следует интегрировать с существующим процессом обеспечения непрерывности бизнеса и аварийного восстановления.

Решения о рисках безопасности должны принимать руководители бизнес-направлений или подразделений, которые обладают полной информацией о всех рисках и возможностях.



Интеграция бизнес-подразделений, отдела безопасности и ИТ-отдела для повышения устойчивости

Продолжение

3. Правильно позиционируйте безопасность

Способы структурирования отчетности о рисках безопасности в организациях часто приводит к принятию неверных решений. Такие решения о рисках лучше всего принимать руководителям бизнес-направлений или подразделений, которые обладают полной информацией о всех рисках и возможностях. Однако часто организации (явно или косвенно) назначают профильных экспертов из отделов безопасности ответственными за риски безопасности. Это создает лишнюю нагрузку на отделы безопасности, лишая бизнес-руководителей прозрачности и контроля над ключевым риском для их бизнеса. Организации могут исправить это следующими способами:

Подготовка бизнес-руководителей — расскажите бизнес-руководителям о рисках безопасности в целом и о том, как эти угрозы могут и будут влиять на их бизнес-направление. Непосредственное вовлечение отделов безопасности в эти инициативы также улучшит сотрудничество и общую гибкость бизнеса.

Назначение ответственности за риски безопасности бизнес-руководителям — когда бизнес-руководители получают достаточно информации, чтобы понять и принять риски безопасности, организация должна явно переложить на них ответственность за эти риски, в то же время возлагая на команды безопасности ответственность за управление этим риском и предоставление бизнес-руководителям экспертных знаний и рекомендаций.

Снижение риска за счет устранения разрозненности



«Киберустойчивость можно описать как динамическую шкалу, в начале которой идут классические процедуры обеспечения непрерывности бизнеса и аварийного восстановления с эффективным резервным копированием данных, возможности восстановления процессов, технологий и их зависимостей (в том числе пользователей и сторонних поставщиков), которые затем превращаются в непрерывно доступные самовосстанавливающиеся сервисы, устойчивость для критически важных ролей и отработку отказа для критически важных сторонних поставщиков. Самые устойчивые организации стимулируют интеграцию между ИТ-специалистами, бизнес-руководителями и специалистами по безопасности. Для достижения высокого уровня устойчивости необходимо учитывать ее с самого начала, реализуя безопасное управление изменениями и детализированную изоляцию сбоев. Киберустойчивость — это лишь один из сценариев эффективной программы планирования борьбы с любыми рисками. По мере роста киберрисков и усиления связи между кибербезопасностью и устойчивостью связь директора по информационной безопасности (CISO) с программой устойчивости организации становится прочнее и прочнее. С каждым годом все больше директоров по информационной безопасности берут на себя ответственность за устойчивость всей компании».

Лиза Решаур (Lisa Reshaur)

Генеральный директор по управлению рисками, Microsoft

Ссылки на дополнительную информацию

- > От традиционной к цифровой устойчивости: как организации используют цифровые технологии, чтобы благополучно пережить кризис в беспрецедентные времена | [Официальный блог Microsoft](#)
- > Как ИТ-отделы и отделы безопасности могут сотрудничать для укрепления безопасности конечных точек | [Microsoft Security](#)

Колоколообразная кривая киберустойчивости

Движущие факторы успешного обеспечения устойчивости, которые должна принять каждая организация

Как мы видели, многие кибератаки оказываются успешными просто потому, что не соблюдаются базовые меры киберпрофилактики. Вот минимальные стандарты, которые должны соблюдать все организации:

- **Включение многофакторной аутентификации (MFA)** — для защиты от взломанных паролей пользователей и обеспечения дополнительной устойчивости удостоверений.
- **Применение принципа «Никому не доверяй»** — неотъемлемый элемент любого плана обеспечения устойчивости, ограничивающего воздействие на организацию. Вот эти принципы:

- Явная проверка — убедитесь, что пользователям и устройства можно доверять, прежде чем разрешать им доступ к ресурсам.
- Доступ с наименьшими привилегиями — предоставляйте только те разрешения, которые необходимы для доступа к ресурсу.
- Предположение о взломе — всегда предполагайте, что защита взломана и системы могут быть скомпрометированы. Это означает, что необходимо вести непрерывный мониторинг среды на предмет возможной атаки.

- **Использование антивирусных программ для расширенного обнаружения и реагирования** — используйте ПО для обнаружения и автоматической блокировки атак и предоставления аналитических сведений отделу безопасности. Мониторинг информации из систем обнаружения угроз играет важную роль в своевременном реагировании на угрозы.
- **Установка обновлений** — неисправленные и устаревшие системы остаются основной причиной, по которой многие организации становятся жертвами атаки. Убедитесь, что все системы, в том числе встроенное ПО, операционные системы и приложения, своевременно обновляются.
- **Защита данных** — понимание того, какие из данных наиболее важны, где они находятся и используются ли необходимые системы для их защиты, имеет решающее значение для реализации соответствующей защиты.

98 %

Базовые меры безопасности по-прежнему защищают от 98 % атак.



Обозначения

- Включение многофакторной аутентификации
- Применение принципа «Никому не доверяй»
- Использование современных средств защиты от вредоносных программ
- Установка обновлений
- Защитите данные

Концевые сноски

1. Сервис обнаружения и нейтрализации атак на конечные точки (EDR) — это корпоративная платформа обеспечения безопасности конечных точек, предназначенная для предотвращения, обнаружения и анализа сложных угроз в корпоративных сетях, а также реагирования на них. Этот сервис поддерживает обнаружение атак практически в реальном времени и предоставляет возможности для их устранения. Аналитики безопасности могут эффективно приоритизировать оповещения, получать полное представление об уровне нарушения и принимать ответные меры для устранения угроз.
2. Платформа защиты конечных точек (EPP) — это решение, развернутое на конечных устройствах для предотвращения файловых вредоносных программ, обнаружения и блокировки вредоносных действий со стороны доверенных и ненадежных приложений, а также для предоставления возможностей расследования и исправления, необходимых для динамического реагирования на инциденты безопасности и оповещения.
3. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted>
4. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match>
5. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context>
6. Книга о безопасности Windows: коммерческие организации
7. Новые функции безопасности Windows 11 помогут защитить работу в гибридной среде | Блог Microsoft Security
8. FIDO Alliance: Open Authentication Standards More Secure than Passwords
9. <https://interpret.ml/>
10. OWASP Top Ten | OWASP Foundation
11. <https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/>
12. <https://www.kaspersky.com/blog/the-human-factor-in-it-security/>
13. <https://aka.ms/ZTatMSFT>
14. <https://csrc.nist.gov/publications/detail/nistir/8374/final>
15. <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/>
16. Executive Order 14028 Improving the Nation's Cybersecurity
17. <https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth>
18. The Long Road Ahead to Transition to Post-Quantum Cryptography, <https://cacm.acm.org/magazines/2022/1/257440-the-long-road-ahead-to-transition-to-post-quantum-cryptography/fulltext>
19. <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/>
20. <https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization>
21. <https://safecode.org/blog/preparing-for-post-quantum-cryptography-roadmap-initial-guidance/>
22. <https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final>

Команды, внесшие свой вклад

Команды, внесшие свой вклад

Данные и аналитические сведения в этом отчете были предоставлены разнообразной группой специалистов по безопасности, работающих во многих подразделениях Microsoft. Их общая цель состоит в защите корпорации Microsoft, ее клиентов и всего мира от кибератак. Мы гордимся тем, что делимся этими сведениями на условиях прозрачности, чтобы сделать мир безопасным местом для всех.

AI for Good Research Lab: использование возможностей данных и ИИ для решения многих международных проблем. Лаборатория сотрудничает с организациями за пределами Microsoft, применяя искусственный интеллект для повышения качества жизни и защиты окружающей среды. Ее приоритетными областями являются онлайн-безопасность (дезинформация, кибербезопасность, безопасность детей), реагирование на стихийные бедствия, экологическая устойчивость и использование ИИ для здравоохранения.

Azure Edge & Platform, Enterprise & OS Security: эта команда отвечает за безопасность базовой ОС и платформы в Windows, Azure и других продуктах Microsoft. Она внедряет ведущие в отрасли решения для обеспечения безопасности и аппаратные решения в платформы Microsoft, чтобы снизить число эксплойтов, удостоверений и вредоносных программ от чипа до облака. Создатели платформы Microsoft Secured-core для ПК, периметра сети и серверов, процессора Microsoft Pluton и многого другого.

Azure Networking, Core: команда специалистов по облачным сетям, специализирующаяся на глобальной сети Microsoft, сетях центров обработки данных и программно-определяемой сетевой инфраструктуре Azure, включающей в себя платформу DDoS, пограничную сетевую платформу и продукты сетевой безопасности, такие как Azure WAF, брандмауэр Azure и Azure DDoS Protection Standard.

Команда Cloud Security Research: защищая Microsoft Cloud, разрабатывая инновационные функции и продукты безопасности, а также проводя исследования, эта команда позволяет клиентам Microsoft безопасно трансформировать свои организации.

Customer Security and Trust (CST): междисциплинарная команда, постоянно совершенствующая средства обеспечения безопасности клиентов в продуктах и онлайн-сервисах Microsoft. Работая с инженерными группами и командами по безопасности по всей компании, CST стремится гарантировать соответствие требованиям, повысить уровень безопасности и прозрачности для защиты наших клиентов и укрепления глобального доверия к корпорации Microsoft.

Customer Success: отделы безопасности подразделения Customer Success работают напрямую с клиентами, чтобы делиться рекомендациями, извлеченными уроками и рекомендациями по ускорению трансформации и модернизации системы безопасности. Эта команда собирает и систематизирует рекомендации и уроки, извлеченные из опыта Microsoft и наших клиентов, в виде эталонных стратегий, архитектур, планов и т. д.

Операционный центр по киберзащите (CDOC): подразделение Microsoft, специализирующееся на кибербезопасности и защите, в котором объединены специалисты со всей компании для защиты корпоративной инфраструктуры Microsoft и облачной инфраструктуры, к которой у клиентов есть доступ. Сотрудники, реагирующие на инциденты, работают вместе со специалистами по анализу данных и инженерами по безопасности для разных сервисов продуктов и устройств корпорации Microsoft, чтобы защищать клиентов, обнаруживать угрозы и реагировать на них в круглосуточном режиме.

Democracy Forward Initiative: команда Microsoft, работающая над сохранением, защитой и развитием основ демократии путем продвижения безопасной информационной экосистемы, защиты открытых и безопасных демократических процессов и пропаганды корпоративной гражданской ответственности.

Подразделение по борьбе с киберпреступлениями (DCU): команда юристов, следователей, специалистов по обработке и анализу данных, инженеров, аналитиков и бизнес-специалистов, которые борются с киберпреступностью в глобальном масштабе с использованием технологий, криминалистики, гражданских исков, уголовных дел и сотрудничества с государственными и частными организациями.

Digital Diplomacy: международная команда из бывших дипломатов, законодателей и экспертов по юридическим вопросам, работающих над продвижением мирного, стабильного и безопасного киберпространства на фоне растущего конфликта национальных государств.

Digital Security & Resilience (DSR): подразделение, цель которого — корпорации Microsoft создавать самые надежные устройства и сервисы, сохраняя при этом нашу компанию в безопасности, а также защищая данные нашей компании и наших клиентов.

Подразделение цифровой безопасности (DSU): команда адвокатов и аналитиков по кибербезопасности, которые используют свои юридические, геополитические и технические знания для защиты корпорации Microsoft и ее клиентов. DSU укрепляет доверие к корпоративным средствам защиты Microsoft от продвинутых киберпреступников со всего мира.

Команды, внесшие свой вклад

Продолжение

Центр анализа цифровых угроз (DTAC): команда экспертов, которые анализируют и сообщают об угрозах иностранных государств, в том числе о кибератаках и операциях по распространению влияния. Команда объединяет информацию и аналитические сведения о киберугрозах с геополитическим анализом, чтобы предоставить нашим клиентам и корпорации Microsoft ценные данные для эффективного реагирования и защиты.

Enterprise and Security: команда, ориентированная на создание современной, безопасной и управляемой платформы для интеллектуального облака и интеллектуальных технологий.

Enterprise Mobility: команда, которая помогает создать современное рабочее место и современную систему управления для защиты данных в облаке и локальной среде. Решение Endpoint Manager предоставляет сервисы и средства, используемые корпорацией Microsoft и ее клиентами для контроля и мониторинга мобильных устройств, настольных компьютеров, виртуальных машин, встроенных устройств и серверов.

Enterprise Risk Management: команда, работающая в различных бизнес-подразделениях над определением приоритетов рисков для обсуждения с высшим руководством Microsoft. Команда ERM объединяет несколько групп операционных рисков, управляет структурой корпоративных рисков Microsoft и проводит внутреннюю оценку безопасности компании на основе стандарта NIST Cybersecurity Framework.

Global Cybersecurity Policy: команда, которая работает с правительствами, неправительственными организациями и отраслевыми партнерами для продвижения государственной политики кибербезопасности. Она помогает клиентам повысить уровень безопасности и отказоустойчивости по мере внедрения и использования технологий Microsoft.

Identity and Network Access (IDNA) Security: команда, работающая над защитой всех клиентов Microsoft от несанкционированного доступа и мошенничества. Она состоит из инженеров, менеджеров по продуктам, специалистов по обработке и анализу данных, а также исследователей безопасности.

M365 Security: подразделение, которое разрабатывает решения по безопасности, такие как Microsoft Defender для конечной точки (MDE), Microsoft Defender для удостоверений (MDI) и другие, для защиты корпоративных клиентов.

Комитет Microsoft по искусственному интеллекту, этике и последствиям проектирования и исследований (AETHER): консультативный совет корпорации Microsoft, целью которого является обеспечение ответственной разработки и внедрения новых технологий.

Microsoft Bing Search and Distribution: команда, занимающаяся поддержкой поисковой системы в Интернете мирового класса, позволяющей пользователям по всему миру быстро находить релевантные результаты и информацию, в том числе отслеживая темы и актуальные истории, которые важны для них, предоставляя пользователям контроль над конфиденциальностью.

Решения клиентов и партнеров Microsoft: единая коммерческая организация Microsoft по выходу на рынок, ответственная за такие роли, как выездные специалисты и консультанты по безопасности и техническим продажам.

Microsoft Defender Experts: крупнейшее глобальное подразделение Microsoft, состоящее из исследователей в области безопасности, ориентированных на продукты, прикладных специалистов и аналитиков угроз. Defender Experts предоставляет инновационные возможности обнаружения и реагирования в продуктах Microsoft 365 для обеспечения безопасности и управляемых сервисах Microsoft Defender Experts.

Microsoft Defender для Интернета вещей: команда, состоящая из экспертов, специализирующихся на обратном инжиниринге вредоносных программ, протоколов и встроенного ПО Интернета вещей/операционных технологий. Команда ищет связанные с этими технологиями угрозы, чтобы выявить вредоносные тенденции и кампании.

Microsoft Defender Threat Intelligence (RiskIQ): команда, которая занимается тактической аналитикой, исследуя обширную коллекцию внешних телеметрических данных Microsoft, создавая схему среды угроз по мере ее развития для обнаружения ранее неизвестной вредоносной инфраструктуры и добавления контекста к субъектам угроз и кампаниям. Команда регулярно публикует релевантные и полезные исследования, чтобы предоставить важные тактические сведения специалистам по безопасности.

Отдел развития бизнеса Microsoft в сфере безопасности: команда, которая отвечает за стратегию развития кибербезопасности в корпорации Microsoft, партнерские отношения и стратегические инвестиции.

Центр Microsoft по реагированию на угрозы (MSRC): команда, сотрудничающая с исследователями в области безопасности, которые занимаются защитой клиентов и партнерской экосистемы Microsoft. MSRC как неотъемлемая часть Операционного центра по киберзащите (CDOC) корпорации Microsoft объединяет

экспертов по реагированию на угрозы, чтобы обнаруживать угрозы и реагировать на них в режиме реального времени.

Сервисы безопасности Майкрософт для реагирования на инциденты: команда экспертов по кибербезопасности, помогающих клиентам на протяжении всего жизненного цикла кибератаки — от расследования до успешного сдерживания и восстановления. Сервисы предлагаются 2 тесно интегрированными командами: командой обнаружения и реагирования (DART), специализирующейся на расследовании и подготовке к восстановлению, и командой по восстановлению безопасности после компрометации (CRSP), которая отвечает за аспекты сдерживания и восстановления.

Microsoft Threat Intelligence Center (MSTIC): команда, сосредоточенная на выявлении, отслеживании и сборе аналитических данных о самых продвинутых злоумышленниках, влияющих на клиентов Microsoft, в том числе об угрозах национального, вредоносных программ и фишинге.

One Engineering System (1ES): команда, цель которой — создавать инструменты мирового уровня, чтобы помочь разработчикам Microsoft работать максимально продуктивно и безопасно. Команда отвечает за развитие центральной стратегии обеспечения безопасности всей цепочки поставок программного обеспечения Microsoft.

Operational Threat Intelligence Center (OpTIC): команда, отвечающая за контроль и распространение аналитики о киберугрозах, которая поддерживает деятельность операционного центра по киберзащите Microsoft (CDOC) для защиты нашей корпорации и наших клиентов.



Описание среды угроз и расширение
возможностей цифровой защиты.

→ Подробнее: <https://microsoft.com/mddr>

→ Узнавайте больше: <https://blogs.microsoft.com/on-the-issues/>

🐦 Оставайтесь на связи: [@msftissues](#) и [@msftsecurity](#)