Microsoft

2022 Microsoft 디지털 방어 보고서

위협 환경을 조명하고
및 디지털 방어를 강화합니다.

목차

이 보고서의 데이터, 인사이트, 이벤트는 달리 명시되지 않는 한 2021년 7월부터 2022년 6월(2022년 Microsoft 회계 연도)까지입니다.

최적의 환경에서 이 보고서를 보고 살펴보려면 Adobe 웹 사이트에서 무료로 다운로드할 수 있는 Adobe Reader를 사용하는 것이 좋습니다.

Tom Burt의 소개말

고객 보안 및 신뢰 부문 기업 부사장

"전 세계 제품 및 서비스 생태계를 통해 분석하는 수조 개의 신호는 전 세계 디지털 위협의 흉포함, 범위, 규모를 보여줍니다."

환경을 보여 주는 스냅샷...

위협 환경의 범위 및 규모

비밀번호 공격의 양은 초당 약 921건으로 증가했는데, 이는 단 1년 만에 74% 증가한 수치입니다.

사이버 범죄의 해제

현재까지 Microsoft는 사이버 범죄자가 사용하는 10,000개 이상의 도메인과 국가 차원의 공격자가 사용하는 600개 이상의 도메인을 제거했습니다.

취약점 해결

랜섬웨어 인시던트 대응 참여의 93%는 권한 액세스 및 측면 이동에 대한 제어가 충분하지 않은 것으로 나타났습니다.

2022년 2월 23일, 사이버 보안 세계는 하이브리드 전쟁의 시대인 새로운 시대에 접어들었습니다. 이날, 미사일이 발사되고 탱크가 국경을 넘기 몇 시간 전 러시아 공격자들은 우크라이나 정부 기관, 기술, 금융 기관을 목표로 대규모 파괴적인 사이버 공격을 시작했습니다. 해당 공격과 이로부터 배울 수 있는 교훈에 대한 자세한 내용은 MDDE(Microsoft Digital Defense Report, Microsoft 디지털 방어 보고서)의 세 번째 연판의 국가 차원의 위협 장에서 확인할 수 있습니다. 이러한 교훈 중 핵심은 클라우드가 사이버 공격에 대응할 수 있는 최적의 물리적 및 논리적 보안을 제공하고 우크라이나에서 가치가 입증된 위협 인텔리전스 및 엔드포인트 보호의 발전을 지원한다는 점입니다.

올해 진행하는 사이버 보안 발전에 대한 모든 설문 조사는 이 부분에서 시작해야 하지만, 올해 보고서는 훨씬 더 많은 내용을 심층적으로 제공합니다. 보고서의 첫 번째 장에서는 사이버 범죄자의 활동에 초점을 맞추고 2장에서는 국가 차원의 위협에 중점을 둡니다. 두 그룹 모두 공격의 정교함을 크게 증가시켜 행동이 미치는 영향을 극적으로 증가시켰습니다. 러시아가 언론의 헤드라인을 장식하는 동안 이란 공격자들은 대통령 권력이 이양된 후 공격을 확대하여 이스라엘을 겨냥한 파괴적인 공격과 미국의 주요 기반 시설을 목표로 한 랜섬웨어 및 해킹 및 유출 작전을 시작했습니다. 중국 역시 동남아시아와 남반구의 다른 지역에서 스파이 활동을 강화하여 미국의 영향력에 대응하고 중요한 데이터와 정보를 훔치기 위해 노력했습니다.

외국 공격자들도 세 번째 장에서 다룬 것처럼 전 세계 여러 지역에서 선전 영향력 작전을 지원하기 위해 매우 효과적인 기술을 사용하고 있습니다. 예를 들어, 러시아는 자국 시민들과 타국 시민들에게 우크라이나 침공이 정당하다고 설득하기 위해 열심히 노력했으며, 이와 동시에 서방에서 코로나 백신을 불신하도록 선전을 뿌리면서 국내에서는 그 효과에 대해 홍보했습니다. 또한 공격자들은 4장에서 논의되는 네트워크 및 주요 인프라의 진입점으로 IoT(사물 인터넷) 디바이스 또는 OT(운영 기술) 제어 디바이스를 점점 더 목표로 삼고 있습니다. 마지막으로, 마지막 장에서는 사이버 회복탄력성 분야에서 올해 거둔 발전에 대해 검토하면서 Microsoft와 고객을 표적으로 삼은 공격을 방어하기 위해 지난 한 해 동안 배운 인사이트 및 교훈을 제공합니다.

각 장에서는 Microsoft만의 고유한 관점을 기반으로 배운 주요 교훈과 인사이트를 제공합니다. 전 세계 제품 및 서비스 생태계를 통해 분석하는 수조 개의 신호는 전 세계 디지털 위협의 사나움, 범위, 규모를 보여줍니다. Microsoft는 이러한 위협으로부터 고객과 디지털 생태계를 보호하기 위한 조치를 취하고 있으며, 고객에 대한 수십억 건의 피싱 시도, ID 도용, 기타 위협을 식별하고 차단하는 Microsoft 기술에 대해 읽을 수 있습니다.

Tom Burt의 소개말

계속

Microsoft는 또한 법적 및 기술적 수단을 사용하여 사이버 범죄자 및 국가 차원의 공격자들이 사용하는 인프라를 점유 및 종료하고 국가 차원의 공격자로부터 위협이나 공격을 받을 때 고객에게 알립니다. AI/ML 기술을 사용하여 사이버 위협을 식별 및 차단하고 보안 전문가가 사이버 침공을 보다 빠르고 효과적으로 방어하고 식별할 수 있는, 점점 더 효과적인 기능과 서비스를 개발하기 위해 노력합니다.

아마도 가장 중요한 점은 MDDR 전반에 걸쳐 개인, 조직, 기업이 이처럼 증가하는 디지털 위협을 방어하기 위해 취할 수 있는 조치에 대한 최적의 조언을 제공한다는 점일 것입니다. 좋은 사이버 방역 관행을 채택하는 것이 최선의 방어이며 이를 통해 사이버 공격의 위험을 크게 줄일 수 있습니다.

사이버 범죄 현황

사이버 범죄자들은 계속해서 수익 기업으로서 정교한 방식으로 활동하고 있습니다. 공격자들은 기술을 구현하는 새로운 방법을 채택 및 모색하고 있어 캠페인 운영 인프라를 호스팅하는 방법과 위치의 복잡성이 높아지고 있습니다. 동시에 사이버 범죄자들은 더욱 검소해지고 있습니다. 오버헤드를 낮추고 합법성을 높이기 위해 공격자들은 비즈니스 네트워크와 디바이스를 침해하여 피싱 캠페인 및 맬웨어를 호스팅하거나 컴퓨팅 성능을 사용하여 암호화폐를 채굴합니다.

> **6페이지에서 자세히 알아보기**

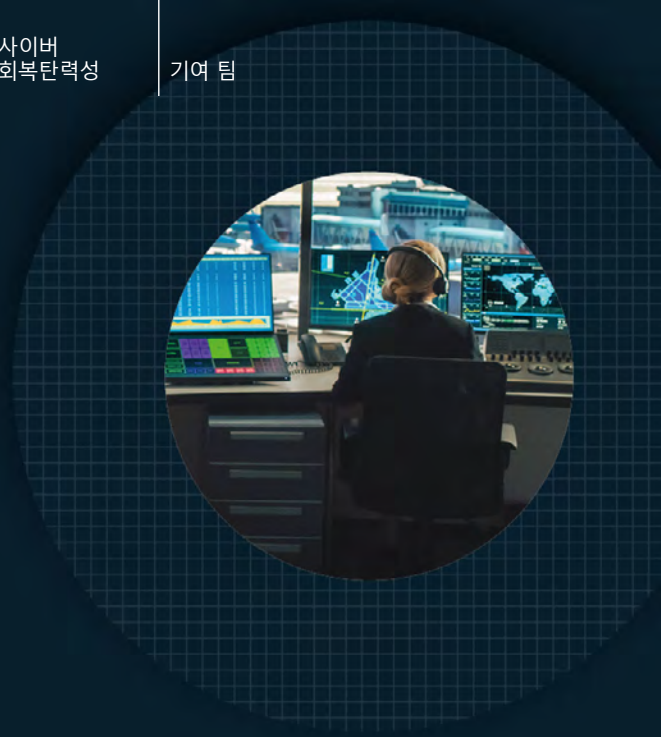
"우크라이나의 하이브리드 전쟁에서 사이버 무기 배치의 출현은 새로운 갈등 시대의 시작을 의미합니다."

국가 차원의 위협

국가 차원의 공격자들은 탐지를 피하고 전략적 우선순위를 높이기 위해 점점 더 정교한 사이버 공격을 시작하고 있습니다. 우크라이나의 하이브리드 전쟁에서 사이버 무기 배치의 출현은 새로운 갈등 시대의 시작을 의미합니다. 러시아는 또한 선전을 활용하여 러시아, 우크라이나, 전 세계 여론에 영향을 미치는 정보 영향력 작전으로 전쟁을 지원했습니다. 우크라이나 이외의 지역에서는 국가 차원의 공격자들이 더욱 활발하게 활동하고 자동화, 클라우드 인프라, 원격 액세스 기술의 발전을 활용하여 더 광범위한 대상을 공격하기 시작했습니다. 최종 목표물에 액세스할 수 있는 기업 IT 공급망이 빈번하게 공격을 받았습니다. 사이버 보안 방역은 공격자가 패치되지 않은 취약점을 신속하게 악용하고, 정교하면서도 무차별적인 공격 기술을 사용하여 개인 인증 정보를 훔치고, 오픈 소스 또는 합법적인 소프트웨어를 활용하여 작전을 난독화함에 따라 더욱 중요해졌습니다. 또한 이란은 러시아와 함께 랜섬웨어를 포함한 파괴적인 사이버 무기를 공격의 주요 요소로 사용하고 있습니다.

이러한 발전은 인권을 우선시하고 온라인에서 무모한 국가 행동으로부터 사람들을 보호하는 일관적인 글로벌 프레임워크를 긴급하게 채택해야 합니다. 모든 국가는 책임 있는 국가 행동을 위한 규범과 규칙을 이행하기 위해 협력해야 합니다.

> **30페이지에서 자세히 알아보기**



디바이스 및 인프라

팬데믹은 디지털 트랜스포메이션을 가속화하는 구성 요소로 모든 종류의 인터넷 연결 디바이스를 빠르게 채택함에 따라 디지털 세계의 공격 표면을 크게 증가시켰습니다. 그 결과, 사이버 범죄자와 국가 차원의 공격자들이 이를 빠르게 이용하고 있습니다. 최근 몇 년 동안 IT 하드웨어 및 소프트웨어의 보안이 강화되었지만 IoT 보안 및 OT 디바이스 보안은 이러한 속도를 따라가지 못했습니다. 위협 행위자들은 이러한 디바이스를 악용하여 네트워크에 대한 액세스를 구축하고 측면 이동을 지원하거나, 공급망에 발판을 마련하거나, 대상 조직의 OT 운영을 방해합니다.

> **56페이지에서 자세히 알아보기**

Tom Burt의 소개말
계속

사이버 영향력 작전

국가 차원의 공격자들은 선전을 배포하고 국내외 여론에 영향을 미치기 위해 점점 더 정교한 영향력 작전을 많이 사용하고 있습니다. 이러한 캠페인은 신뢰를 침식하고 양극화를 심화하며 민주적 절차를 위협합니다. 숙련된 첨단 지속적 조작 공격자(Advanced Persistent Manipulator)는 인터넷 및 소셜 미디어와 함께 전통 미디어를 활용하여 캠페인의 범위, 규모, 효율성을 크게 높이고 글로벌 정보 생태계에 미치는 막대한 영향을 크게 높이고 있습니다. 지난 한 해 동안 이러한 작전은 우크라이나에 대한 러시아의 하이브리드 전쟁의 일환으로 사용되는 경우가 많았지만, 러시아와 중국, 이란을 포함한 다른 국가들이 다양한 문제에서 국제적인 영향력을 확대하기 위해 소셜 미디어로 구동되는 선전 작전을 점점 더 많이 펼쳤습니다.

71페이지에서 자세히 알아보기

사이버 회복탄력성

보안은 기술 성공의 핵심 요소입니다. 혁신과 생산성 강화는 조직이 최신 공격에 최대한 탄력적으로 대처할 수 있도록 하는 보안 조치를 도입해야만 달성할 수 있습니다. 팬데믹은 Microsoft에서 근무하는 모든 곳에서 직원을 보호하기 위해 보안 관행과 기술을 전환해야 하는 과제를 던져주었습니다. 지난 한 해 동안 사이버 공격자들은 팬데믹과 하이브리드 업무 환경으로의 전환 도중 노출된 취약점을 계속 활용했습니다. 그 이후로 Microsoft의 주요 과제는 다양한 공격 방법의 보급과 복잡성을 관리하고 국가 차원의 활동을 증가시키는 것이었습니다. 이 장에서는 Microsoft에서 직면한 어려움과 15,000명 이상의 파트너와 함께 대응하기 위해 동원한 방어에 대해 자세히 설명하겠습니다.

86페이지에서 자세히 알아보기

Microsoft만의 유리한 점

370억
차단된 이메일 위협 수

347억
차단된 ID 위협

43조
개의 신호가 정교한 데이터 분석 기능 및 AI 알고리즘을 활용하여 매일 합성되어 디지털 위협 및 사이버 범죄 활동을 이해하고 이로부터 조직과 개인을 보호합니다.

25억
하루에 분석되는 엔드포인트 신호 수

8,500+
77개국에 8,500명 이상의 엔지니어, 연구원, 데이터 과학자, 사이버 보안 전문가, 위협 헌터, 지정학적 분석가, 조사관, 최전선 대응자가 있습니다.

15,000+
고객의 사이버 회복탄력성을 높일 수 있는 15,000명 이상의 파트너가 Microsoft 보안 생태계에 있습니다.

2021년 7월 1일부터 2022년 6월 30일까지

Tom Burt의 소개말
계속

Microsoft는 독립적으로 그리고 민간 산업, 정부 기관, 시민 사회의 다른 사람들과의 긴밀한 파트너십을 통해 우리 사회의 사회적 구조를 뒷받침하는 디지털 시스템을 보호하고 모든 사람이 어디에 있든 안전한 컴퓨팅 환경을 조성할 책임이 있다고 믿습니다. 이러한 책임감으로 인해 2020년부터 매년 MDDR을 발표했습니다. 이 보고서는 Microsoft의 방대한 데이터와 포괄적인 연구의 정점입니다. 디지털 위협 환경이 어떻게 진화하고 있고 생태계의 보안을 개선하기 위해 오늘날 취할 수 있는 중요한 조치에 대한 고유한 인사이트를 공유합니다.

Microsoft는 긴박감을 전달하길 원하기 때문에 독자들은 이 보고서와 일 년 내내 다양한 사이버 보안 간행물에서 제시하는 데이터와 인사이트를 기반으로 즉각적인 조치를 취합니다. 디지털 환경에 대한 위협의 심각성과 물리적 세계로의 전환을 고려하면 우리 모두는 디지털 위협으로부터 우리 자신, 조직, 기업을 보호하기 위한 조치를 취할 권한이 있다는 사실을 기억하는 것이 중요합니다.

시간을 내어 올해 Microsoft 디지털 방어 보고서를 살펴봐 주셔서 감사합니다. 이 보고서에서 제공하는, 디지털 생태계를 공동으로 방어하는 데 도움이 되는 귀중한 인사이트와 권장 사항을 알게 되시길 바랍니다.

Tom Burt 고객 보안 및 신뢰 부문 기업 부사장

이 보고서의 목적은 두 가지입니다.

1. 광범위한 생태계에 걸쳐 고객, 파트너, 이해관계자를 위해 진화하는 디지털 위협 환경을 조명하고 새로운 사이버 공격과 역사적으로 지속된 위협의 진화하는 추세를 조명합니다.
2. 고객과 파트너가 사이버 회복탄력성을 개선하고 이러한 위협에 대응할 수 있도록 지원합니다.

사이버 범죄 현황

사이버 방어가 개선되고 더 많은 조직이 예방에 대한 선제적인 접근 방식을 취함에 따라 공격자는 기술을 채택하고 있습니다.

사이버 범죄 현황

개요

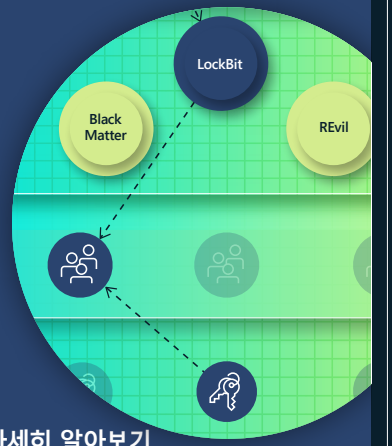
사이버 방어가 개선되고 더 많은 조직이 예방에 대한 선제적인 접근 방식을 취함에 따라 공격자는 기술을 채택하고 있습니다.

사이버 범죄자들은 계속해서 수익 기업으로서 정교한 방식으로 활동하고 있습니다. 공격자들은 기술을 구현하는 새로운 방법을 채택 및 모색하고 있어 캠페인 운영 인프라를 호스팅하는 방법과 위치의 복잡성이 높아지고 있습니다. 동시에 사이버 범죄자들은 더욱 검소해지고 있습니다. 오버헤드를 낮추고 합법성을 높이기 위해 공격자들은 비즈니스 네트워크와 디바이스를 침해하여 피싱 캠페인 및 맬웨어를 호스팅하거나 컴퓨팅 성능을 사용하여 암호화폐를 채굴합니다.

사이버 범죄 경제의 산업화를 통해 도구와 인프라에 대한 더 많은 액세스를 제공함으로써 진입 기술 장벽을 낮추면서 사이버 범죄가 계속 증가하고 있습니다.

18페이지에서 자세히 알아보기

랜섬웨어 및 갈취의 위협은 정부 기관, 기업, 주요 인프라를 표적으로 삼은 하는 공격으로 인해 더욱 대담해지고 있습니다.

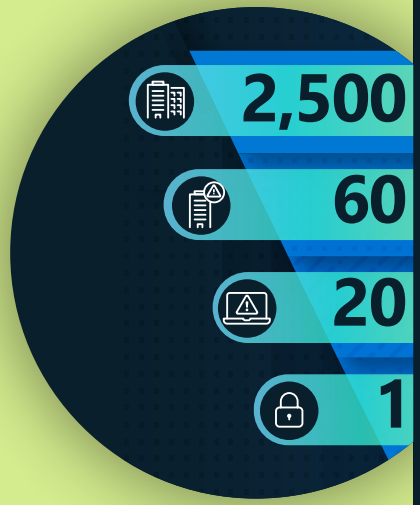


9페이지에서 자세히 알아보기

공격자들은 점점 더 몸값 지불을 강요하기 위해 민감한 데이터를 공개하겠다고 위협하고 있습니다.

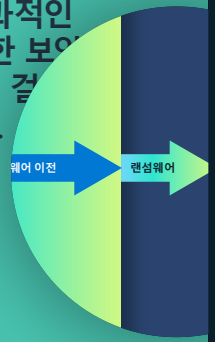
10페이지에서 자세히 알아보기

대상의 1/3이 이러한 공격을 사용하는 범죄자에 의해 성공적으로 침해되고 그중 5%가 몸값을 받기 때문에 사람이 운영하는 랜섬웨어가 가장 널리 퍼져 있습니다.



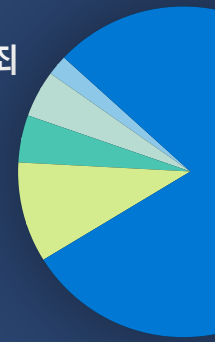
9페이지에서 자세히 알아보기

랜섬웨어에 대한 가장 효과적인 방어로는 다중 인증, 빈번한 보 네트워크 아키텍처 전반에 걸 트러스트 원칙이 있습니다.



13페이지에서 자세히 알아보기

무차별적으로 모든 받은 편지함을 표적으로 삼은 개인 인증 정보 피싱 수법이 증가하고 있으며 송장 사기를 포함한 비즈니스 이메일 침해는 기업에 심각한 사이버 범죄 위험을 초래합니다.



21페이지에서 자세히 알아보기

사이버 범죄자 및 국가 차원 공격자의 악의적인 인프라를 중단하기 위해 Microsoft는 혁신적인 법적 접근 방식과 공공 및 민간 파트너십에 의존합니다.

25페이지에서 자세히 알아보기

서문

무차별적인 공격과 표적 공격이 모두 증가함에 따라 사이버 범죄는 계속 증가하고 있습니다.

사이버 방어가 개선되고 더 많은 정부 기관 및 기업이 예방에 대한 선제적인 접근 방식을 취함에 따라 공격자가 사이버 범죄를 촉진하는 데 필요한 액세스 권한을 얻기 위해 두 가지 전략을 사용한다는 사실을 알 수 있습니다. 한 가지 접근 방식은 양에 의존하는 광범위한 타깃을 가진 캠페인입니다. 다른 한 가지 접근 방식은 감시와 보다 선별적인 타겟팅을 사용하여 수익률을 높입니다. 수익 창출이 목적이 아닌 경우에도(예: 지정학적 목적을 위한 국가 활동), 무차별적인 공격과 표적 공격 모두 사용됩니다. 작년 한 해 동안 사이버 범죄자들은 캠페인의 성공을 극대화하기 위해 사회 공학과 시사 문제를 계속해서 악용했습니다. 예를 들어, 코로나를 주제로 한 피싱 미끼는 덜 사용되었지만 우크라이나 시민을 지원하기 위해 기부를 요청하는 내용의 미끼가 증가했다는 사실을 발견했습니다.

공격자들은 기술을 구현하는 새로운 방법을 채택 및 모색하고 있어 캠페인 운영 인프라를 호스팅하는 방법과 위치의 복잡성이 높아지고 있습니다. 우리는 사이버 범죄자들이 점점 더 검소해지고 공격자들이 더 이상 기술에 대한 비용을 지불하지 않는다는 사실을 발견했습니다. 오버헤드를 낮추고 합법성을 높이기 위해 일부 공격자들은 점점 더 비즈니스를 침해하는 방법을 모색하여 피싱 캠페인 및 맬웨어를 호스팅하거나 컴퓨팅 성능을 사용하여 암호화폐를 채굴합니다.

이 장에서는 사회적 또는 정치적 목표를 달성하기 위해 사이버 공격을 수행하는 민간 시민으로 인해 발생되는 혼란인 핵티비즘 (hacktivism)의 성장에 대해서도 살펴보겠습니다. 전 세계 수천 명의 개인(전문가와 초보자 모두 포함)이 2022년 2월부터 러시아 및 우크라이나 간 전쟁의 일환으로 웹 사이트 비활성화 및 도난당한 데이터 유출과 같은 공격을 시작하기 위해 동원되었습니다. 적극적인 적대 행위가 끝난 후에도 이러한 추세가 계속될지 예측하기에는 너무 이릅니다.

조직은 액세스 제어를 정기적으로 검토 및 강화하고 사이버 공격을 방어하기 위한 보안 전략을 구현해야 합니다. 하지만, 이 외에도 다른 일을 할 수 있습니다. DCU(Digital Crimes Unit, 디지털 범죄 부서)가 민사 사건을 사용하여 사이버 범죄자와 국가 차원의 공격자가 사용하는 악성 인프라를 점유한 방법에 대해 설명하겠습니다. 우리는 공공 및 민간 파트너십을 통해 이 위협에 맞서 함께 싸워야 합니다. 지난 10년 동안 학습한 내용을 공유함으로써 다른 사람들이 지속적으로 증가하는 사이버 범죄의 위협으로부터 자신과 더 넓은 생태계를 보호하기 위해 취할 수 있는 선제적인 조치에 대해 이해하고 이를 고려하는 데 도움이 되길 바랍니다.

Amy Hogan-Burney
DCU(디지털 범죄 부서) 총괄 관리자

랜섬웨어 및 공격: 국가 차원의 위협

랜섬웨어 공격은 성장하는 사이버 범죄 생태계를 활용하는 범죄자에 의해 주요 인프라, 모든 규모의 기업, 주 및 지방 정부 기관 표적이 되기 때문에 모든 개인의 위험이 증가됩니다.

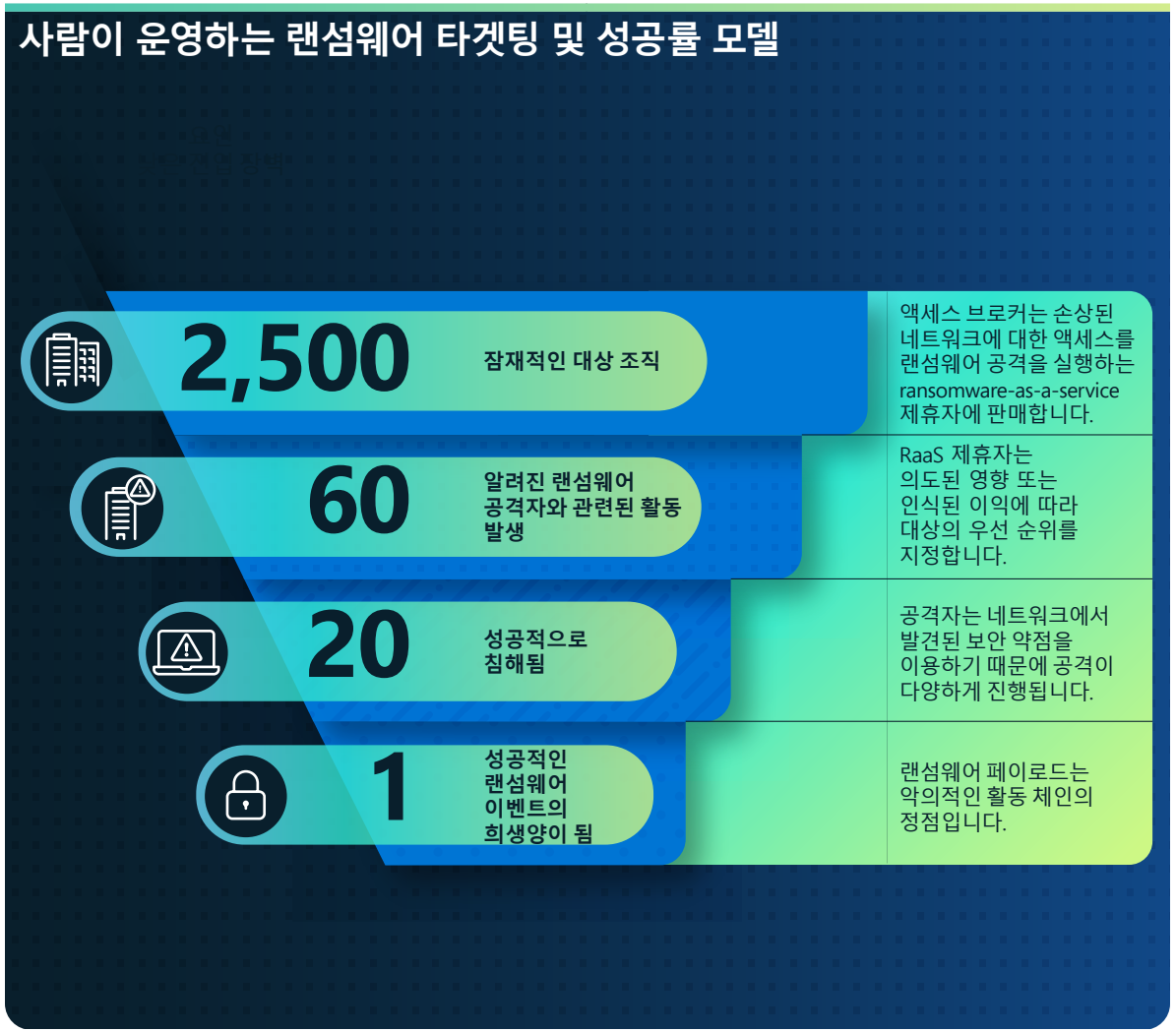
지난 2년 동안 주요 인프라, 의료, IT 서비스 제공자 등과 관련된 세간의 이목을 끄는 랜섬웨어 사건은 대중의 이목을 끌었습니다. 랜섬웨어 공격의 범위가 더욱 대담해짐에 따라 그 영향은 더욱 광범위해졌습니다. 다음은 이미 2022년에 진행된 공격의 예입니다.

- 2월, 두 회사에 대한 공격은 독일 북부에 있는 수백 개의 주유소의 지불 처리 시스템에 영향을 미쳤습니다.[1]
- 3월, 그리스 우편 서비스에 대한 공격으로 일시적으로 우편 배송이 중단되고 금융 거래 처리에 영향을 미쳤습니다.[2]
- 5월 말, 코스타리카 정부 기관에 대한 랜섬웨어 공격으로 여러 병원이 폐쇄되고 세관 및 세금 징수가 중단되어 국가 비상사태가 선포되었습니다.[3]
- 5월, 공격으로 인해 인도 최대 항공사 중 한 곳의 항공편이 지연되고 취소되어 수백 명의 승객이 발이 묶였습니다.[4]

이러한 공격의 성공과 실제 미친 영향력의 정도는 사이버 범죄 경제의 산업화로 인한 결과이며, 도구 및 인프라에 대한 액세스를 지원하고 진입 기술 장벽을 낮추어 사이버 범죄 역량을 확장합니다.

최근 몇 년 동안 랜섬웨어는 단일 '갱'이 랜섬웨어 페이로드를 개발하고 배포하는 모델에서 RaaS(서비스로서의 랜섬웨어) 모델로 전환했습니다. RaaS를 사용하면 단일 그룹이 랜섬웨어 페이로드의 개발을 관리하고 데이터 유출을 통해 실제로 랜섬웨어 공격을 시작하는 다른 사이버 범죄자(수익 삭감을 위해 '계열사'라고 함)에게 지불 및 갈취를 위한 서비스를 제공할 수 있습니다. 이러한 사이버 범죄 경제의 프랜차이즈는 공격자 풀을 확장했습니다. 사이버 범죄 도구의 산업화로 인해 공격자가 침입을 수행하고, 데이터를 유출하며, 랜섬웨어를 배포하는 것이 더 쉬워졌습니다.

사람이 운영하는 랜섬웨어[5](Microsoft 연구원이 대상 네트워크에서 발견한 내용을 기반으로 공격의 모든 단계에서 결정을 내리고 상용 랜섬웨어 공격의 위협을 설명하는 사람이 주도하는 위협을 설명하기 위해 만든 용어)는 조직에 여전히 중요한 위협입니다.



Microsoft EDR(엔드포인트용 Defender) 데이터를 기반으로 하는 모델(2022년 1월~6월)

랜섬웨어 및 갈취: 국가 차원의 위협

계속

랜섬웨어 공격은 이중 갈취 수익 창출 전략의 채택이 표준 관행이 됨에 따라 더욱 영향력이 커졌습니다. 여기에는 침해된 디바이스에서 데이터를 추출하고 디바이스의 데이터를 암호화한 다음 피해자가 몸값을 지불하도록 압력을 가하기 위해 도난당한 데이터를 공개적으로 게시하거나 게시하겠다고 위협하는 것이 포함됩니다.

대부분의 랜섬웨어 공격자는 액세스 권한이 있는 네트워크라면 어디든 랜섬웨어를 기회적으로 배포하지만 일부 공격자는 액세스 브로커와 랜섬웨어 운영자 간의 연결을 활용하여 다른 사이버 범죄자로부터 액세스 권한을 구매합니다.

Microsoft의 고유한 신호 인텔리전스는 ID, 이메일, 엔드포인트, 클라우드와 같은 여러 소스에서 수집되며 기술적으로 덜 숙련된 공격자를 위해 설계된 도구가 포함된 제휴 시스템을 통해 성장하는 랜섬웨어 경제에 대한 인사이트를 제공합니다.

전문화된 사이버 범죄자 간의 관계가 확대되면서 랜섬웨어 공격의 속도, 정교함, 성공이 증가했습니다. 이로 인해 사이버 범죄 생태계는 대상, 지불 서비스, 비밀번호 해독 또는 게시 도구나 사이트에 대한 초기 액세스에서 서로를 지원하는 다양한 기술, 목표, 기술을 가진 커넥티드 플레이어로 진화했습니다.

랜섬웨어 운영자는 현재 온라인으로 조직 또는 정부 기관 네트워크에 대한 액세스 권한을 구매하거나 확보한 액세스 권한으로 수익을 창출하는 것이 주요 목표인 브로커와의 대인 관계를 통해 개인 인증 정보 및 액세스 권한을 얻을 수 있습니다.

그런 다음 운영자는 구매한 액세스 권한을 사용하여 다크 웹 마켓플레이스 또는 포럼을 통해 구매한 랜섬웨어 페이로드를 배포합니다. 대부분의 경우 피해자와의 협상은 운영자 자신이 아닌 RaaS 팀에서 수행합니다. 이러한 범죄 거래는 완벽하며 참가자는 다크 웹의 익명성과 초국가적 법률 집행의 어려움으로 인해 체포 및 기소될 가능성이 거의 없습니다.

이러한 위협에 대한 지속 가능하고 성공적인 노력을 위해서는 민간 부문과의 긴밀한 파트너십을 통해 범정부 전략을 실행해야 합니다.

이따금씩 랜섬웨어가 미디어에서 묘사되는 방식과는 달리, 단일 랜섬웨어 변종이 단일 엔드 투 엔드 '랜섬웨어 갱'에 의해 관리되는 경우는 드뭅니다. 대신 맬웨어를 구축하고, 피해자에 대한 액세스 권한을 확보하고, 랜섬웨어를 배포하고, 강탈 협상을 처리하는 별도의 엔터티가 있습니다. 범죄 생태계의 산업화는 다음과 같은 결과를 낳았습니다.

- 침입하여 액세스 권한을 전달하는 액세스 브로커(서비스로서의 액세스)
- 도구를 판매하는 맬웨어 개발자
- 침입을 수행하는 범죄 운영자 및 계열사
- 제휴자로부터 수익 창출을 인수하는 암호화 및 갈취 서비스 제공자(RaaS)

사람이 운영하는 모든 랜섬웨어 캠페인은 보안 약점에 대한 공통된 종속성을 공유합니다. 특히 공격자는 일반적으로 조직의 열악한 사이버 위생을 이용하며, 여기에는 빈번하지 않은 패치 및 MFA(다중 인증) 구현 실패가 포함됩니다.

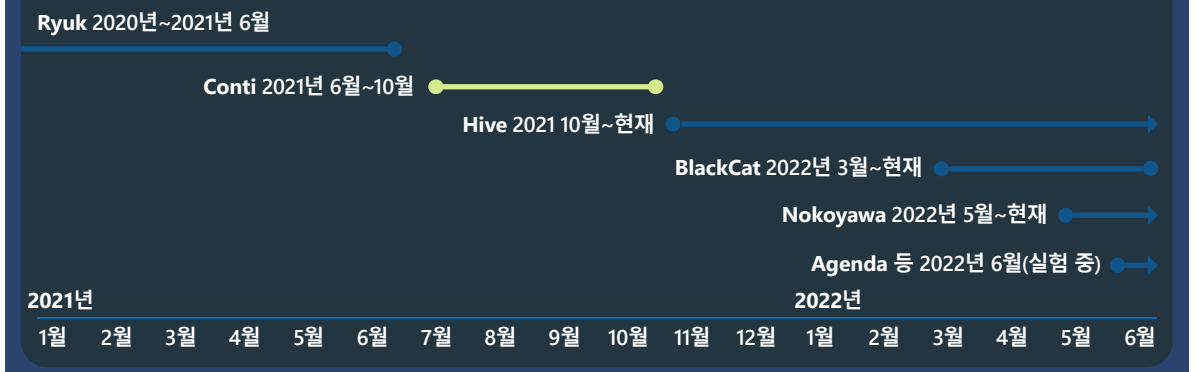
사례 연구: Conti의 해체

지난 2년 동안 최고의 랜섬웨어 변종 중 하나인 Conti는 2022년 중반에 운영을 중단하기 시작했으며 MSTIC(Microsoft Threat Intelligence Center, Microsoft 위협 인텔리전스 센터)는 3월 말과 4월 초에 활동이 크게 감소한 사실을 발견했습니다. 4월 중순에 Conti 랜섬웨어가 마지막으로 배포되었다는 사실을 발견했습니다. 그러나 다른 랜섬웨어 운영의 종료와 마찬가지로 MSTIC는 Conti 계열사가 BlackBasta, Lockbit 2.0, LockbitBlack, HIVE를 포함한 다른 랜섬웨어 페이로드를 배포하기 위해 선회하는 모습을 확인했기 때문에 Conti의 해체는 랜섬웨어 배포에 큰 영향을 미치지 않았습니다. 이는 이전 연도의 데이터와 일치하며 랜섬웨어 갱이 오프라인 상태가 되면 몇 달 후에 다시 나타나거나 기술 역량 및 리소스를 새로운 그룹에 재배포한다는 사실을 시사합니다.

Microsoft 위협 인텔리전스 팀은 랜섬웨어 위협 행위자를 이들이 사용하는 맬웨어로 추적하는 대신 특정 도구를 기반으로 개별 그룹(DEV로 레이블 지정)으로 추적합니다. 즉, Conti의 계열사가 분산되었을 때에도 다른 도구 또는 RaaS 키트를 사용하여 이러한 DEV를 계속 추적할 수 있었습니다. 예를 들면 다음과 같습니다.

- Trickbot과 제휴한 DEV-0230은 Conti의 다작 사용자였습니다. 4월 말, MSTIC는 QuantumLocker를 활용하여 이를 발견했습니다.
- DEV-0237은 5월 31일 코스타리카 정부 기관을 표적으로 삼은 공격에 HIVE를 활용한 것을 포함하여 Conti의 랜섬웨어 키트에서 HIVE 및 Nokoyawa로 전환했습니다.
- Conti 랜섬웨어 키트의 또 다른 다작 사용자인 DEV-0506은 BlackBasta를 통해 발견되었습니다.

RaaS 프로그램 간에 빠르게 전환하는 제휴자(DEV-0237)의 예



Conti와 같은 RaaS 프로그램이 종료된 후 랜섬웨어 제휴자는 거의 바로 다른 프로그램(Hive)으로 이동합니다.

RaaS는 랜섬웨어 생태계를 발전시키고 기여도를 방해합니다

사람이 운영하는 랜섬웨어는 개별 운영자에 의해 구동되기 때문에 공격 패턴은 대상에 따라 다르며 공격 기간 동안 번갈아 나타납니다. 과거에는 단일 랜섬웨어 부담의 각 캠페인에서 초기 진입 벡터, 도구, 랜섬웨어 페이로드 선택 간에 밀접한 관계가 있다는 사실을 발견했습니다. 이로 인해 기여도가 더 쉬워졌습니다. 그러나 RaaS와 연계된 모델은 이 관계를 분리합니다. 그 결과, Microsoft는 랜섬웨어 페이로드 개발자를 운영자로 추적하는 대신 특정 공격에서 페이로드를 배포하는 랜섬웨어 계열사를 추적합니다.

다시 말해, 우리는 더 이상 HIVE 개발자가 HIVE 랜섬웨어 공격의 운영자라고 가정하지 않고 운영자는 계열사일 가능성이 더 큽니다.

사이버 보안 업계는 개발자와 운영자 간의 이러한 구분을 적절하게 포착하기 위해 고군분투했습니다. 업계에서는 여전히 페이로드 이름으로 랜섬웨어 인시던트를 보고하는 경우가 많아 특정 랜섬웨어 페이로드를 활용하는 모든 공격의 배후에 단일 엔터티 또는 랜섬웨어 갱이 있으며 이와 관련된 모든 인시던트가 공통 기술과 인프라를 공유한다는 잘못된 인상을 줍니다. 네트워크 방어자를 지원하려면 데이터 반출 및 추가 지속성 메커니즘과 같이 다양한 계열사의 공격에 선행하는 단계와 존재할 수 있는 탐지 및 보호 기회에 대해 자세히 알아보는 것이 중요합니다.

맬웨어보다 공격자가 작업을 성공적으로 수행하려면 개인 인증 정보가 필요합니다. 전체 조직에서 사람이 운영하는 랜섬웨어 감염을 성공적으로 진행하기 위해서는 높은 권한의 계정에 대한 액세스에 의존합니다.

사람이 운영하는 랜섬웨어 공격에 대한 집중 조명

지난 한 해 동안 Microsoft의 랜섬웨어 전문가들은 100건 이상의 사람이 운영하는 랜섬웨어 인시던트에 대한 심층 조사를 수행하여 공격자의 기술을 추적하고 고객을 더 잘 보호하는 방법을 이해했습니다.

여기서 공유하는 분석 내용은 온보딩되고 관리되는 디바이스에서만 가능하다는 점에 유의해야 합니다. 온보딩되지 않고 관리되지 않는 디바이스는 조직의 하드웨어 자산에서 가장 안전하지 않은 부분을 나타냅니다.

가장 널리 사용되는 랜섬웨어 단계 기술:

75%
관리 도구를 사용합니다.

75%
획득한 높은 수준의 침해된 사용자 계정을 사용하여 SMB 프로토콜을 통해 악성 페이로드를 확산합니다.

99%
OS 구축 도구를 활용하여 검색된 보안 및 백업 제품을 변조하려고 시도합니다.

사람이 운영하는 일반적인 공격

사람이 운영하는 랜섬웨어 공격은 랜섬웨어 이전 단계와 랜섬웨어 배포 단계로 분류할 수 있습니다. 랜섬웨어 이전 단계에서 공격자는 조직의 유형 및 보안 인프라에 대해 학습하여 네트워크에 침투할 준비를 합니다.

랜섬웨어 배포 단계에 도달하기 전에 공격자를 차단합니다.	배포!
랜섬웨어 이전	**랜섬웨어**
이 단계는 며칠에서 몇 주 또는 몇 달까지 걸릴 수 있지만 지난 2년 동안 기간이 단축되었습니다.	이 단계는 몇 분만 지속될 수 있습니다.
공격자는 토폴로지 및 보안 인프라에 대해 가능한 한 많이 학습하여 네트워크에 침투할 준비를 합니다. 공격자는 이 단계에서 데이터를 유출할 수도 있습니다.	공격자는 가능한 한 많은 데이터를 암호화하는 것을 목표로 합니다.

Microsoft에서 실시한 조사에 따르면 사람이 운영하는 랜섬웨어 공격의 배후에 있는 대부분의 공격자는 유사한 보안 약점을 이용하고 일반적인 공격 패턴과 기술을 공유합니다.

지속 가능한 보안 전략

이러한 성격의 공격에 대처하고 이를 방지하려면 랜섬웨어 이전 단계에서 랜섬웨어 배포 단계로 이동하기 전에 공격자의 속도를 늦추고 차단하는 데 필요한 포괄적인 보호에 집중하도록 조직의 사고방식을 전환해야 합니다.

기업은 공격 클래스를 완화하기 위해 네트워크에 보안 모범 사례를 일관적이며 적극적으로 적용해야 합니다. 인간의 의사 결정으로 인해 이러한 랜섬웨어 공격은 쉽게 손실되거나 제시간에 응답하지 않을 수 있는, 이질적으로 보이는 여러 보안 제품 경고를 생성할 수 있습니다. 경고 피로는 실제로 발생하며 SOC(Security Operations Center: 보안 운영 센터)는 경고의 추세를 확인하거나 경고를 인시던트로 그룹화하여 더 큰 그림을 볼 수 있어 삶을 더 쉽게 만들 수 있습니다. 그런 다음 SOC는 공격 표면 감소 규칙과 같은 강화 기능을 활용하여 경고를 완화할 수 있습니다. 일반적인 위협에 대한 강화는 경고의 양을 줄일 뿐만 아니라 많은 공격자가 네트워크에 액세스하기 전에 차단합니다.

조직은 사람이 운영하는 랜섬웨어 공격으로부터 스스로를 보호하기 위해 지속적으로 높은 수준의 보안 태세와 네트워크 방역을 유지해야 합니다.

실행 가능한 인사이트

랜섬웨어 공격자는 쉬운 수익으로 동기 부여를 받기 때문에 보안 강화를 통해 비용을 추가하는 것이 사이버 범죄 경제를 혼란에 빠뜨리는 열쇠입니다.

1. 개인 인증 정보 위생을 구축합니다. 맬웨어보다 공격자가 작업을 성공적으로 수행하려면 개인 인증 정보가 필요합니다. 전체 조직에서 사람이 운영하는 랜섬웨어 감염을 성공적으로 진행하기 위해서는 도메인 관리자와 같은 높은 권한의 계정에 대한 액세스 또는 그룹 정책 편집 기능에 의존합니다.
2. 개인 인증 정보 노출을 감사합니다.
3. Active Directory 업데이트 배포의 우선순위를 지정합니다.
4. 클라우드 강화의 우선순위를 지정합니다.
5. 공격 표면을 줄입니다.
6. 인터넷 연결 자산을 강화하고 경계를 파악합니다.
7. 네트워크를 강화하여 양을 줄이고 우선순위가 높은 인시던트에 대한 대역폭을 보존함으로써 SOC 경고 피로를 줄입니다.

추가 정보에 대한 링크

- RaaS: 사이버 범죄 각 경제 이해 및 자신을 보호하는 방법 | Microsoft Security 블로그
- 사람이 운영하는 랜섬웨어 공격: 예방 가능한 재해 | Microsoft Security 블로그

최전선 대응자의 랜섬웨어 인사이트

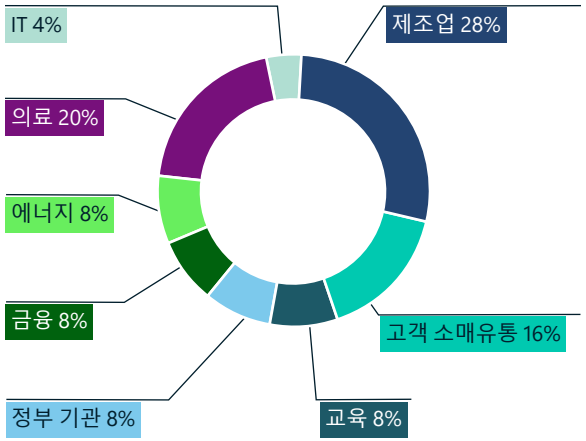
전 세계 조직에서는 2019년부터 사람이 운영하는 랜섬웨어 공격이 꾸준히 증가했습니다. 그러나 작년의 법 집행과 지정학적 사건은 사이버 범죄 조직에 상당한 영향을 미쳤습니다.

Microsoft의 Security Service Line은 조사에서 성공적인 억제 및 복구 활동에 이르기까지 전체 사이버 공격 과정에서 고객을 지원합니다. 대응 및 복구 서비스는 복구를 위한 조사 및 기초 작업에 중점을 둔 팀과 격리 및 복구에 중점을 둔 두 팀 등 고도로 통합된 두 팀에서 제공됩니다. 이 섹션에서는 지난 한 해 동안의 랜섬웨어 참여를 기반으로 한 결과에 대해 요약된 내용을 제공합니다.

93%

랜섬웨어 복구 참여 중 Microsoft 조사의 93%가 권한 액세스 및 측면 이동 제어가 충분하지 않은 것으로 나타났습니다.

산업별 랜섬웨어 인시던트 및 복구 참여

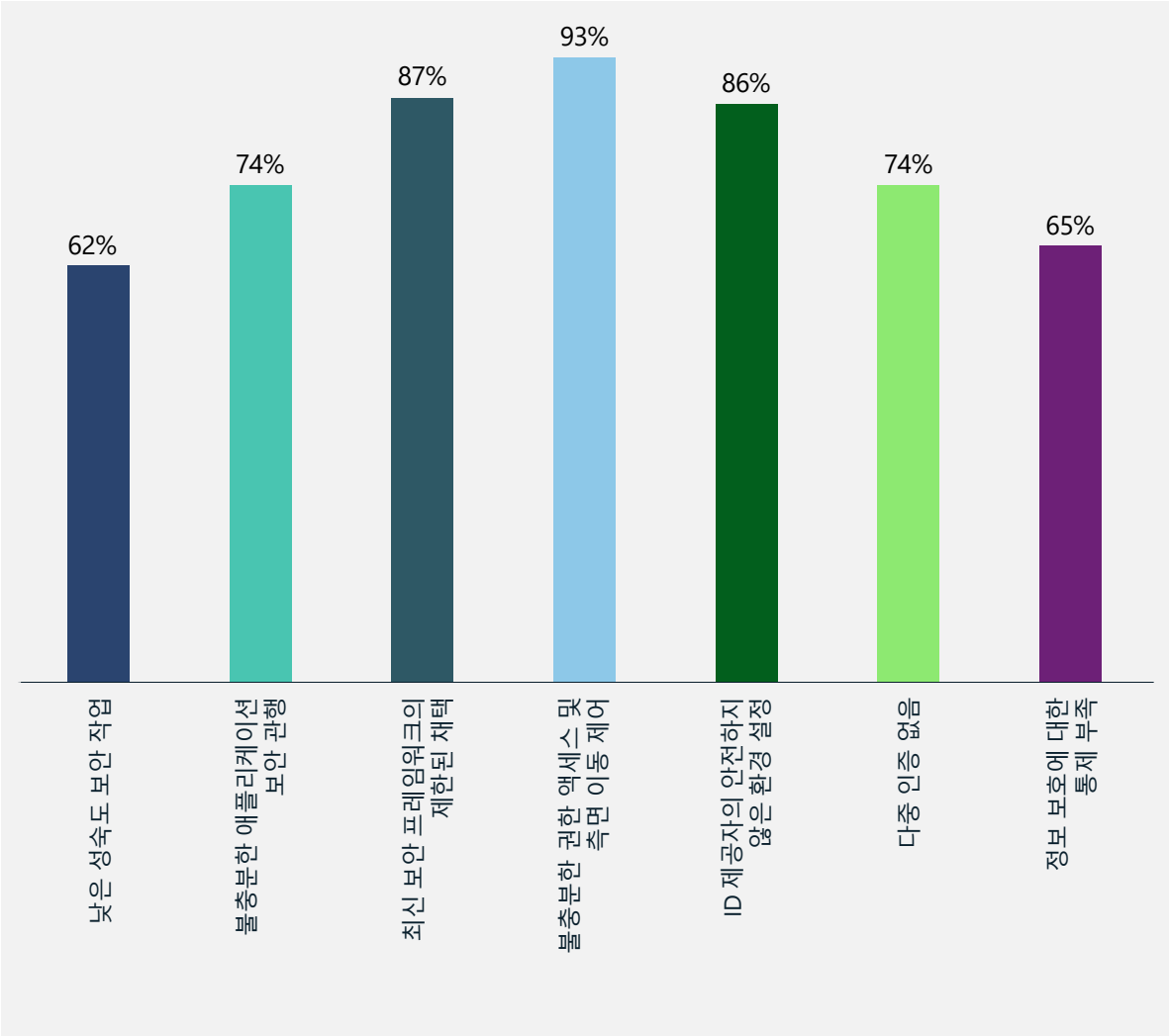


새로운 소규모 그룹과 위협이 부상함에 따라 방어 팀은 진화하는 랜섬웨어 위협을 인식하는 동시에 이전에 알려지지 않은 랜섬웨어 맬웨어 제품군으로부터 보호해야 합니다. 범죄 집단이 사용하는 신속한 개발 접근 방식은 사용하기 쉬운 키트에 패키지된 인텔리전트한 랜섬웨어의 생성으로 이어졌습니다. 이로 인해 더 많은 대상에 대해 광범위한 공격을 시작할 수 있는 유연성이 높아집니다.

이어지는 페이지에서는 랜섬웨어에 대한 취약한 보호에 기여하는 가장 일반적으로 발견되는 요인을 세 가지 범주의 결과로 그룹화하여 자세히 살펴보겠습니다.

1. 취약한 ID 제어
2. 비효율적인 보안 운영
3. 제한적인 데이터 보호

랜섬웨어 대응 참여에서 가장 일반적인 결과 요약 내용



랜섬웨어 인시던트 대응 참여 중 가장 일반적으로 발견된 것은 불충분한 권한 액세스 및 측면 이동 제어였습니다.

최전선 대응자의 랜섬웨어 인사이트

계속

현장 대응 참여에서 볼 수 있는 세 가지 주요 기여 요인:

① **취약한 ID 제어:** 개인 인증 정보 도난 공격은 여전히 가장 큰 기여 요인 중 하나입니다.

② **비효율적인 보안 운영** 프로세스는 공격자에게 기회를 제공할 뿐만 아니라 복구 시간에 상당한 영향을 미칩니다.

③ 결국 이는 데이터로 귀결됩니다. 조직은 자사 비즈니스 요구에 부합하는 효과적인 **데이터 보호 전략**을 구현하기 위해 고군분투합니다.

① 취약한 ID 제어

사람이 운영하는 랜섬웨어는 계속해서 진화하고 있으며 전통적으로 표적 공격과 관련된 개인 인증 정보 도난 및 측면 이동 방법을 사용합니다. 성공적인 공격은 종종 AD(Active Directory)와 같은 ID 시스템의 침해와 관련된 장기 실행 캠페인의 결과로, 이를 통해 사람 운영자는 개인 인증 정보를 훔치고 시스템에 액세스하며 네트워크에 영구적으로 있을 수 있습니다.

AD(Active Directory) 및 Azure AD 보안

88%

영향을 받는 고객의 88%가 AD 및 Azure AD 보안 모범 사례를 사용하지 않았습니다. 이는 공격자가 중요한 ID 시스템에서 잘못된 환경 설정과 취약한 보안 태세를 악용하여 비즈니스에 대한 광범위한 액세스와 영향을 얻으면서 일반적인 공격 벡터가 되었습니다.

최소 권한 액세스 및 PAW(Privileged Access Workstations, 권한 있는 액세스 워크스테이션) 사용

영향을 받는 조직 중 어떤 조직도 독점 시스템 및 비즈니스 크리티컬 애플리케이션과 같은 중요한 ID 및 고부가가치 자산을 관리하는 동안 전용 워크스테이션을 통해 적절한 관리 개인 인증 정보 분리 및 최소 권한 액세스 원칙을 구현하지 않았습니다.

권한 계정 보안

88%

참여의 88%에서 MFA가 중요하고 권한이 높은 계정에 대해 구현되지 않아 공격자가 개인 인증 정보를 침해하고 합법적인 개인 인증 정보를 활용하여 추가 공격을 피벗할 수 있는 보안 격차를 남겼습니다.

84%

조직의 84%에서 관리자는 침해된 권한 있는 개인 인증 정보의 악의적인 사용을 방지하기 위해 JIT(just-in-time) 액세스와 같은 권한 ID 제어를 사용하지 않았습니다.

최전선 대응자의 랜섬웨어 인사이트

계속

② 비효율적인 보안 운영

Microsoft 데이터에 따르면 랜섬웨어 공격을 받은 조직은 보안 운영, 도구, 정보 기술 자산 수명 주기 관리에 상당한 격차가 있습니다. 사용 가능한 데이터를 기반으로 하여 다음과 같은 차이가 가장 많이 발견되었습니다.

패치:

68%

영향을 받은 조직의 68%는 효과적인 취약점 및 패치 관리 프로세스가 없었고, 자동화된 패치 대비 수동 프로세스에 대한 의존도가 높아 중요한 문제가 발생하게 됐습니다. 제조 및 주요 인프라는 레거시 OT(운영 기술) 시스템의 유지 관리 및 패치로 인한 어려움을 계속해서 겪고 있습니다.

보안 운영 도구의 부족:

대부분의 조직은 부족한 보안 도구 또한 잘못된 환경 설정으로 인해 엔드 투 엔드 보안 가시성이 부족하여 탐지 및 대응 효율성이 감소했다고 보고했습니다.

60%

의 조직이 탐지 및 대응을 위한 기본 기술인 EDR[6] 도구를 사용하지 않는다고 보고했습니다.

60%

가 SIEM(보안 정보 및 이벤트 관리) 기술에 투자하지 않아 사일로 모니터링, 엔드 투 엔드 위협 탐지 능력 제한, 비효율적인 보안 운영으로 이어졌습니다. 자동화는 SOC 도구 및 프로세스의 핵심 격차로 여전히 남아 있기 때문에 SOC 직원은 보안 원격 분석을 이해하는 데 수많은 시간을 소비해야 합니다.

84%

영향을 받은 조직의 84%는 멀티클라우드 환경을 보안 운영 도구에 통합할 수 없었습니다.

대응 및 복구 프로세스:

76%

효과적인 대응 계획의 부족은 영향을 받은 조직 중 76%에서 발견된 중요한 영역으로, 위기에 적절하게 대비하는 조직을 방해하고 대응 및 복구 시간에 부정적인 영향을 미쳤습니다.

③ 제한적인 데이터 보호

침해된 많은 조직은 적절한 데이터 보호 프로세스가 부족하여 복구 시간과 비즈니스 운영으로 돌아갈 수 있는 기능에 심각한 영향을 받았습니다. 발생하는 가장 일반적인 격차는 다음과 같습니다.

변경 불가능한 백업:

44%

의 조직에는 영향을 받는 시스템에 대한 변경 불가능한 백업이 없었습니다. 또한 데이터에 따르면 관리자는 AD와 같은 중요한 자산에 대한 백업 및 복구 계획이 없었습니다.

데이터 손실 방지:

공격자는 일반적으로 조직의 취약점을 악용하고 강탈, 지적 재산권 도용 또는 수익 창출을 위해 중요한 데이터를 유출하여 시스템을 침해하는 방법을 찾습니다.

92%

영향을 받는 조직의 92%는 이러한 위험을 완화하기 위한 효과적인 데이터 손실 방지 제어를 구현하지 않아 중요한 데이터 손실이 발생했습니다.

랜섬웨어는 일부 지역에서 감소하고 다른 지역에서 증가했습니다

올 한 해 동안 Microsoft는 북미 및 유럽 대응 팀에 보고된 전체 랜섬웨어 사례 수가 전년도에 비해 감소한 사실을 확인했습니다. 이와 동시에 라틴 아메리카에서는 보고된 사례가 증가했습니다.

이러한 발견에 대한 한 가지 해석은 사이버 범죄자들이 더 쉬운 표적을 위해 법 집행 기관의 조사를 유발할 위험이 더 높은 것으로 인식되는 영역에서 멀어졌다는 것입니다. Microsoft는 랜섬웨어 관련 지원 요청의 감소를 설명하기 위해 전 세계적으로 엔터프라이즈급 네트워크 보안이 크게 개선된 것을 발견하지 못했기 때문에 가능성이 가장 높은 원인은 2022년 일부 지정학적 사건과 함께 2021년과 2022년의 법 집행 활동의 조합으로 범죄 활동 비용을 증가되었기 때문이라고 생각합니다.

가장 널리 퍼진 RaaS 작업 중 하나는 2019년부터 활동해 온 REvil(Sodinokibi라고도 함)이라는 러시아어를 사용하는 범죄 그룹의 작업입니다. 2021년 10월, REvil의 서버는 국제 법 집행 작전인 골드더스트의 일환으로 오프라인 상태가 되었습니다.[7] 2022년 1월, 러시아는 REvil 회원이라고 알려진 14명의 사람들을 체포하고 이들과 관련된 25곳을 급습했습니다.[8] 이는 러시아가 처음으로 자국 영토에서 랜섬웨어 운영자에 대해 조치를 취한 것입니다.

법 집행 활동으로 인해 2022년 공격 빈도가 줄어든 가능성이 있지만, 위협 행위자는 향후 잡히지 않도록 새로운 전략을 개발할 수 있습니다.

2배

일부 지역에서는 랜섬웨어 공격이 감소했지만 몸값 요구는 두 배 이상 증가했습니다.

법 집행 활동으로 인해 2022년 공격 빈도가 줄어든 가능성이 있지만, 위협 행위자는 향후 잡히지 않도록 새로운 전략을 개발할 수 있습니다. 뿐만 아니라, 러시아의 우크라이나 침공에 대한 러시아와 미국 간의 긴장은 랜섬웨어와의 국제적인 싸움에서 러시아의 초기 협력을 종식시킨 것으로 보입니다. REvil 체포 이후 잠깐의 불확실성 이후 미국과 러시아는 랜섬웨어 공격자 추적에 대한 협력을 중단했으며, 이로 인해 사이버 범죄자들이 러시아를 다시 한번 안전한 피난처로 볼 수 있다는 점을 시사합니다.

앞으로 랜섬웨어 활동의 속도는 다음과 같이 몇 가지 주요 질문의 결과에 따라 달라질 것으로 예측됩니다.

1. 정부 기관은 랜섬웨어 범죄자가 국경 내에서 활동하는 것을 방지하기 위한 조치를 취하거나 외국 영토에서 활동하는 공격자를 방해하기 위해 조치를 취할 것인가?
2. 랜섬웨어 그룹이 랜섬웨어의 필요성을 제거하고 갈취 스타일 공격에 의존하기 위해 전술을 변경할 것인가?
3. 조직은 범죄자가 취약점을 악용할 수 있는 것보다 더 빠르게 IT 운영을 현대화하고 혁신할 수 있는가?
4. 몸값 지불 추적의 발전으로 몸값 수령인이 전술과 협상 방식을 변경해야 하는가?

실행 가능한 인사이트

1. 모든 랜섬웨어 제품군이 동일한 보안 약점을 이용하여 네트워크에 영향을 미치므로 총체적인 보안 전략에 집중합니다.
2. 보안 기본 사항을 업데이트하고 유지 관리하여 심층 방어 기본 보호 수준을 높이고 보안 운영을 현대화합니다. 클라우드로 마이그레이션하면 위협을 더 빠르게 탐지하고 더 신속하게 대응할 수 있습니다.

추가 정보에 대한 링크

- 랜샘웨어로부터 조직 보호 | Microsoft Security
- 침해에 대비하여 조직 환경을 강화하는 7가지 방법 | Microsoft Security 블로그
- AI 기반 방어를 개선하여 사람이 운영하는 랜섬웨어 중단 | Microsoft 365 Defender 연구 팀
- 보안 인사이더: 최신 사이버 보안 인사이트 및 업데이트 살펴보기 | Microsoft Security

서비스로서의 사이버 범죄

CaaS(서비스로서의 사이버 범죄)는 성장하고 있으며 전 세계 고객에게 점점 더 위협이 되고 있습니다. Microsoft DCU(디지털 범죄 부서)는 BEC 및 사람이 운영하는 랜섬웨어를 비롯한 다양한 사이버 범죄를 촉진하는 온라인 서비스의 수가 증가함에 따라 CaaS 생태계가 지속적으로 성장하고 있음을 발견했습니다. 피싱은 사이버 범죄자가 도난당한 계정에 대한 액세스 권한을 성공적으로 훔치고 판매함으로써 상당한 가치를 얻을 수 있기 때문에 지속적으로 선호되는 공격 방법입니다.

확장되는 CaaS 시장에 대응하기 위해 DCU(디지털 범죄 부서)는 인터넷, 딥 웹, 검증된 포럼,[9] 전용 웹 사이트, 온라인 토론 포럼, 메시지 플랫폼의 전체 생태계에서 CaaS 제품을 탐지하고 식별할 수 있는 청취 시스템을 개선했습니다.

사이버 범죄자들은 이제 특정 결과를 제공하기 위해 시간대와 언어를 초월하여 협력하고 있습니다. 예를 들어, 아시아에서 한 개인이 관리하는 CaaS 웹 사이트는 유럽에서 운영을 유지하고 아프리카에서 악성 계정을 생성합니다. 이러한 운영의 다중 관할권 특성은 복잡성 높은 법률 및 집행 문제를 제기합니다. 이에 대응하여 DCU(디지털 범죄 부서)는 CaaS 공격을 용이하게 하는 데 사용되는 악성 범죄 인프라를 비활성화하고 전 세계 법 집행 기관과 협력하여 범죄자에게 책임을 묻는 데 노력을 집중하고 있습니다.

사이버 범죄자들은 도달 범위, 범위, 수익을 극대화하기 위해 점점 더 분석 기능을 많이 사용하고 있습니다. 합법적인 비즈니스와 마찬가지로 CaaS 웹 사이트는 확고한 평판을 유지하기 위해 제품 및 서비스의 유효성을 보장해야 합니다. 예를 들어 CaaS 웹 사이트는 침해된 개인 인증 정보의 유효성을 보장하기 위해 침해된 계정에 대한 액세스를 정기적으로 자동화합니다. 사이버 범죄자들은 비밀번호가 재설정되거나 취약점이 패치되면 특정 계정의 판매를 중단합니다. 품질 관리 프로세스로 구매자에게 온디맨드 검증 방식을 제공하는 CaaS 웹 사이트가 더 많아지는 사실을 확인했습니다. 그 결과, 구매자들은 CaaS 웹 사이트에서 활성 계정과 암호를 판매한다는 확신을 가짐과 동시에 도난당한 개인 인증 정보를 판매 전에 수정하면 CaaS 판매자의 잠재적 비용을 줄일 수 있습니다.

DCU(디지털 범죄 부서)는 또한 구매자들에게 특정 지리적 위치, 지정된 온라인 서비스 제공자, 특히 대상 개인, 직업 및 산업에서 침해된 계정을 구매할 수 있는 옵션을 제공하는 CaaS 웹 사이트를 발견했습니다. 빈번하게 주문되는 계정은 CFO 또는 '외상 매출금'과 같이 송장을 처리하는 전문가 또는 부서 관련 계정이 많습니다. 이와 마찬가지로, 공공 계약에 참여하는 산업은 공개 입찰 프로세스를 통해 제공되는 정보의 양으로 인해 표적이 되는 경우가 많습니다.

CaaS에 대한 DCU(디지털 범죄 부서) 조사를 통해 다음과 같은 여러 가지 주요 추세가 드러났습니다.

서비스의 수와 정교함이 증가하고 있습니다.

한 가지 예로는 일반적으로 피싱 공격을 자동화하는 데 사용되는 침해된 웹 서버로 구성된 웹 셸의 진화가 있습니다. DCU(디지털 범죄 부서)는 CaaS 리셀러가 전문 웹 대시보드를 통해 피싱 키트 또는 맬웨어의 업로드를 단순화하는 사실을 발견했습니다. CaaS 판매자는 지리적 위치 또는 직업 등 정의된 속성을 기반으로 스팸 메시지 서비스 및 특수 스팸 수신자 목록과 같은 대시보드를 통해 위협 행위자에게 추가 서비스를 판매하려고 시도하는 경우가 많습니다. 경우에 따라 단일 웹 셸이 여러 공격 캠페인에서 사용된다는 사실을 발견했으며, 이는 위협 행위자가 침해된 서버에 대한 지속적인 액세스를 유지할 수 있음을 시사합니다. 또한 CaaS 생태계의 일부로 사용할 수 있는 익명화 서비스와 VPN(가상 사설망) 및 VPS(가상 사설 서버) 계정에 대한 제안이 증가하는 것을 확인했습니다. 대부분의 경우, 제공되는 VPN/VPS는 처음에 도난당한 신용 카드를 통해 조달되었습니다. CaaS 웹 사이트는 또한 사이버 범죄 공격을 조율할 수 있는 플랫폼으로 사용하기 위해 더 많은 수의 RDP(원격 데스크톱 프로토콜), SSH(보안 셸), cPanel을 제공했습니다. CaaS 판매자는 RDP, SSH, cPanel을 적절한 도구와 스크립트로 환경 설정하여 다양한 유형의 사이버 공격을 용이하게 합니다.

동형이의어 도메인 생성 서비스는 점점 더 암호화폐로 지불을 요구하고 있습니다.

동형이의어 도메인은 다른 문자와 모양이 동일하거나 거의 동일해 보이는 문자를 활용하여 합법적인 도메인 이름을 사칭합니다. 이는 시청자가 동형이의어 도메인이 실제 도메인이라고 생각하도록 속이는 것을 목표로 합니다. 이러한 도메인은 유비쿼터스적인 위협이며 상당한 양의 사이버 범죄에 대한 게이트웨이 역할을 합니다. CaaS 사이트는 현재 사용자 맞춤형 동형이의어 도메인 이름을 판매하므로 구매자는 특정 회사 및 도메인 이름을 사칭하기 위해 요청할 수 있습니다. 결제가 완료되면 CaaS 판매자는 동형이의어 생성기 도구를 사용하여 도메인 이름을 선택한 다음 악성 동형이의어를 등록합니다. 이 서비스에 대한 지불금은 거의 독점적으로 암호화폐로 이루어집니다.

2,750,000

개의 사이트 등록이 올해 DCU(디지털 범죄 부서)에서 성공적으로 차단되어 국제 사이버 범죄에 가담하려는 범죄 공격자보다 앞서 나갔습니다.

서비스로서의 사이버 범죄

계속

CaaS 판매자는 구매할 수 있는 침해된 개인 인증 정보를 점점 더 많이 제공합니다.

침해된 개인 인증 정보를 사용하면 이메일 메시지 서비스, 회사 파일 공유 리소스, OneDrive for Business를 비롯한 사용자 계정에 무단으로 액세스할 수 있습니다. 관리자 개인 인증 정보가 침해되면 권한 없는 사용자가 기밀 파일, Azure 리소스, 회사 사용자 계정에 대한 액세스 권한을 확보할 수 있습니다. 대부분의 경우, DCU(디지털 범죄 부서) 조사에서 개인 인증 정보 확인을 자동화하기 위한 수단으로 여러 서버에서 동일한 개인 인증 정보를 무단으로 사용하는 것으로 확인되었습니다. 이 패턴은 침해된 사용자가 여러 피싱 공격의 피해자이거나 봇넷 키로거가 개인 인증 정보를 수집할 수 있도록 허용하는 디바이스 맬웨어가 있을 수 있음을 나타냅니다.

탐지를 피하기 위해 기능이 강화된 CaaS 서비스 및 제품이 새롭게 등장하고 있습니다.

한 CaaS 판매자는 탐지 및 방지 시스템을 우회하도록 설계된 복잡성 계층을 더한 피싱 키트와 탐지 및 방지 기능을 하루에 미화 달러로 제공합니다. 이 서비스는 다음 레이어 또는 사이트로의 트래픽을 허용하기 전에 검사를 수행하는 일련의 리디렉션을 제공합니다. 이 서비스 중 하나는 가상 머신인지 확인하는 등 디바이스의 지문을 90번 이상 확인하여 사용 중인 브라우저 및 하드웨어 등에 대한 세부 정보를 수집합니다. 모든 검사를 통과하면 트래픽은 피싱에 사용되는 방문 페이지로 전송됩니다.

엔드 투 엔드 사이버 범죄 서비스는 관리형 서비스에 대한 구독을 판매하고 있습니다.

일반적으로 온라인 범죄 실행의 각 단계는 운영 보안이 취약한 경우 위협 행위자를 노출시킬 수 있습니다. 여러 CaaS 사이트에서 서비스를 구매하는 경우 노출 및 식별 위험이 증가합니다. DCU(디지털 범죄 부서)는 다크 웹에서 소프트웨어 코드를 익명화하고 웹 사이트 텍스트를 일반화하여 노출을 줄이는 서비스가 증가하는, 걱정스러운 추세를 발견했습니다. 엔드 투 엔드 사이버 범죄 가입 서비스 제공자는 모든 서비스를 관리하고 결과를 보장하여 구독한 OCN에 대한 노출 위험을 더욱 줄입니다. 위험이 줄어듦에 따라 이러한 엔드 투 엔드 서비스의 인기는 높아졌습니다.

PhaaS(Phishing as a Service)는 엔드 투 엔드 사이버 범죄 서비스의 일례입니다. PhaaS는 FUD(완전히 탐지할 수 없는) 서비스로 알려진 이전 서비스가 진화한 것으로, 구독 기반으로 제공됩니다. 일반적인 PhaaS 용어로는 피싱 웹 사이트를 한 달 동안 활성 상태로 유지가 있습니다.

DCU(디지털 범죄 부서)는 또한 구독 모델에서 DDoS(분산 서비스 거부)를 제공하는 CaaS 판매자를 식별했습니다. 이 모델은 CaaS 판매자에게 공격을 수행하는 데 필요한 봇넷의 생성 및 유지 관리를 아웃소싱합니다. 각 DDoS 구독 고객은 운영 보안을 강화하기 위해 암호화된 서비스를 1년 동안 연중무휴로 제공받습니다. DDoS 구독 서비스는 다양한 아키텍처와 공격 방법을 제공하기 때문에 구매자는 공격할 리소스를 선택하기만 하면 판매자는 봇넷에서 침해된 디바이스 배열에 액세스하여 공격을 수행할 수 있습니다. DDoS 구독 비용은 미화 500달러에 불과합니다.

PhaaS 및 사이버 범죄자는 단일 구독 내에서 여러 서비스를 제공합니다. 일반적으로 구매자는 다음 세 가지 조치만 수행하면 됩니다.

1. 제공되는 수백 가지의 피싱 사이트 템플릿/디자인에서 선택합니다.
2. 피싱 피해자로부터 얻은 개인 인증 정보를 받을 이메일 주소를 제공합니다.
3. PhaaS 판매자에게 암호화폐로 지불합니다.

이러한 단계가 완료되면 PhaaS 판매자는 특정 사용자를 대상으로 하는 3개 또는 4개 계층의 리디렉션 및 호스팅 리소스로 서비스를 생성합니다. 이후에 캠페인이 시작되고 피해자 개인 인증 정보가 수집 및 확인되고 구매자가 제공한 이메일 주소로 전송됩니다. 프리미엄을 위해 수많은 PhaaS 판매자는 퍼블릭 블록체인에서 피싱 사이트를 호스팅하여 모든 브라우저에서 액세스할 수 있고 리디렉션은 사용자를 분산 원장의 리소스로 안내할 수 있습니다.

CaaS 사이버 범죄자를 식별하고 방해하는 도구와 기술을 개발하기 위한 DCU(디지털 범죄 부서)의 작업은 진행되고 있습니다. CaaS 서비스의 진화는 특히 암호화폐 결제를 방해하는 데 상당한 어려움이 있습니다.

범죄 목적으로 암호화폐 사용

암호화폐의 채택이 주류가 됨에 따라 범죄자들은 법 집행 및 AML(자금 세탁 방지) 조치를 피하기 위해 점점 더 많이 암호화폐를 사용하고 있습니다. 이로 인해 법 집행 기관이 사이버 범죄자들의 암호화폐 지불을 추적하는 데 대한 어려움이 높아집니다.

블록체인 솔루션에 대한 전 세계의 지출은 지난 4년 동안 약 340% 증가한 반면 새로운 암호화폐지갑은 약 270% 성장했습니다. 전 세계적으로 8,300만 개 이상의 고유 지갑이 있으며 모든 암호화폐의 총 시가총액은 2022년 7월 28일 현재 미화 약 1조 1천억 달러입니다.[10]

출처: Twitter.com—@PeckShieldAlert(PeckShield는 중국 기반 블록체인 보안 회사)

랜섬웨어 결제 추적

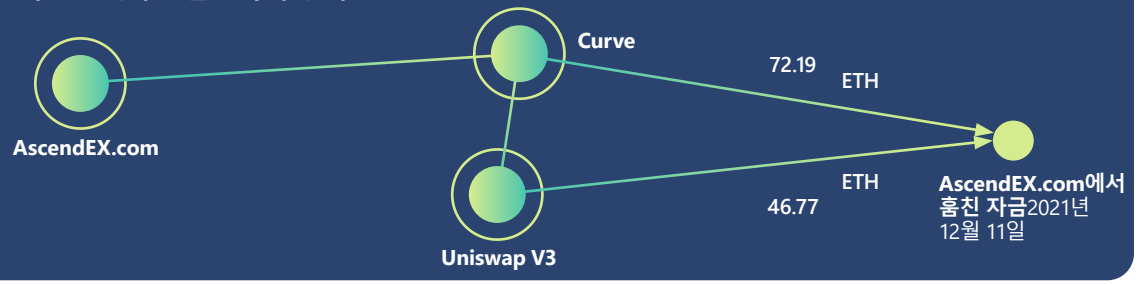
랜섬웨어는 불법적으로 얻은 암호화폐의 가장 큰 소스 중 하나입니다. 랜섬웨어 공격에 사용되는 악성 기술 인프라(예: 2022년 4월 Zloader의 중단[11])를 방해하기 위한 노력의 일환으로 Microsoft DCU(디지털 범죄 부서)는 범죄자들의 지갑을 추적하여 암호화폐 추적 및 복구 기능을 활성화합니다.

DCU(디지털 범죄 부서) 조사관들은 랜섬웨어 공격자가 자금 추적을 숨기기 위해 피해자와의 통신 전술을 발전시키는 모습을 발견했습니다. 원래 사이버 범죄자들은 몸값을 요청할 때 비트코인 주소를 포함했습니다. 그러나 이로 인해 블록체인에서 지불 거래를 쉽게 추적할 수 있게 되었기 때문에 랜섬웨어 공격자들은 지갑 주소를 포함하지 않는 대신 이메일 주소나 채팅 웹 사이트 링크를 추가하여 피해자에게 몸값을 보낼 주소를 전달했습니다. 일부 공격자들은 보안 연구원과 법 집행 기관이 피해자인 척하여 범죄자의 지갑 주소를 얻는 것을 방지하기 위해 피해자별 고유한 웹 페이지와 로그인 환경을 만들기도 했습니다. 자신의 흔적을 숨기려는 범죄자들의 노력에도 불구하고 일부 몸값은 블록체인에서 움직임을 추적할 수 있는 법 집행 기관 및 암호화 분석 회사와 협력하여 여전히 복구할 수 있습니다.

동향: 불법 수익금의 DEX 세탁

사이버 범죄자들이 겪는 주요 문제는 암호화폐를 전통 화폐로 전환하는 것입니다. 사이버 범죄자들에게는 몇 가지 잠재적인 전환 경로가 있으며, 각 경로는 다른 수준의 위험을 수반합니다. 위험을 줄이기 위해 사용되는 한 가지 방법은 CEX(탈중앙화거래소), P2P(피어 투 피어) 및 OTC(장외) 거래소와 같은 현금 인출 옵션을 통해 현금화하기 전 DEX(탈중앙화거래소)를 통해 수익금을 세탁하는 것입니다. DEX는 AML 조치를 따르지 않기 때문에 매력적인 자금 세탁 방법인 경우가 많습니다.

불법적으로 취득한 암호화폐 추적



Microsoft의 DCU(디지털 범죄 부서)는 암호화폐 조사 도구인 Chainalysis를 활용하여 AcendEX 해커들이 훔친 자금을 Uniswap 외에 Curve라는 소규모 DEX로 스왑한 사실을 발견했습니다. 이 다이어그램은 팀에서 발견한 자금 세탁 경로를 보여줍니다. 각 원은 지갑 클러스터를 나타내며 각 줄의 숫자는 자금 세탁 목적으로 전송된 Ethereum의 총량을 나타냅니다.

2021년 12월, 해커들은 국제 암호화폐 거래 플랫폼인 AscendEx를 공격하여 고객 소유의 암호화폐 미화 약 7,770만 달러를 훔쳤습니다.[12] AscendEx는 블록체인 분석 회사를 고용하고 다른 CEX에 연락하여 도난당한 자금을 받는 지갑이 블랙리스트에 오를 수 있도록 했습니다. 또한 코인이 전송된 주소는 Ethereum 블록체인 탐색기 Etherscan에서 이와 같이 표시되었습니다.[13] 경고 및 블랙리스트를 피하기 위해 해커들은 2022년 2월 18일 세계 최대 DEX 중 하나인 Uniswap에 Ethereum으로 미화 150만 달러를 보냈습니다.[14]

DEX가 더 강력한 AML 조치를 채택하면 플랫폼에서 자금 세탁 활동을 둔화시키고 사이버 범죄자들이 코인 텀블링 또는 무허가 교환과 같은 다른 난독화 방법을 사용하도록 할 수 있습니다. 예를 들어, Uniswap는 최근 블랙리스트를 사용하여 불법 활동에 연루된 것으로 알려진 지갑이 거래소에서 거래하는 것을 차단하기 시작할 것이라고 발표했습니다.[15]

실행 가능한 인사이트

1. 암호화폐를 사용하여 범죄자에게 돈을 지불한 사이버 범죄의 피해자인 경우 손실된 자금을 추적하고 복구하는 데 도움을 줄 수 있는 현지 법 집행 기관에 문의하세요.
2. DEX 선택 시, 적용되는 ALM 측정값을 숙지하세요.

추가 정보에 대한 링크

- 점점 더 복잡해지는 크립토재커에 대한 하드웨어 기반 위협 방어 | Microsoft 365 Defender 연구 팀

진화하는 피싱 위협 환경

개인 인증 정보 피싱 사기가 증가하고 있으며 무차별적으로 모든 받은 편지함을 표적으로 하기 때문에 모든 사용자에게 상당한 위협이 되고 있습니다. Microsoft 연구원들이 추적하고 보호하는 위협 중 피싱 공격의 양은 다른 모든 위협보다 훨씬 많습니다.

Defender for Office의 데이터를 활용하여 악성 이메일 및 침해된 ID 활동을 확인합니다. Azure Active Directory Identity Protection은 침해된 ID 이벤트 경고를 통해 더 많은 정보를 제공합니다. Defender for Cloud Apps를 활용하여 침해된 ID 데이터 액세스 이벤트를 확인하고 M365D(Microsoft 365 Defender)는 제품 간 상관관계를 제공합니다. 횡적 이동 메트릭은 Defender for Endpoint (공격 동작 경고 및 이벤트), Defender for Office(악성 이메일), M365D(제품 간 상관관계)에서 제공됩니다.

7억 1천만
매주 차단되는 피싱 이메일 수

1시간 12분
피싱 이메일의 피해자가 된 경우 한 공격자가 개인 데이터에 액세스하는 데 걸리는 중위 시간[16]

1시간 42분
디바이스가 침해된 후 한 공격자가 회사 네트워크 내에서 측면으로 이동하기 시작하는 데 걸리는 중위 시간[17]

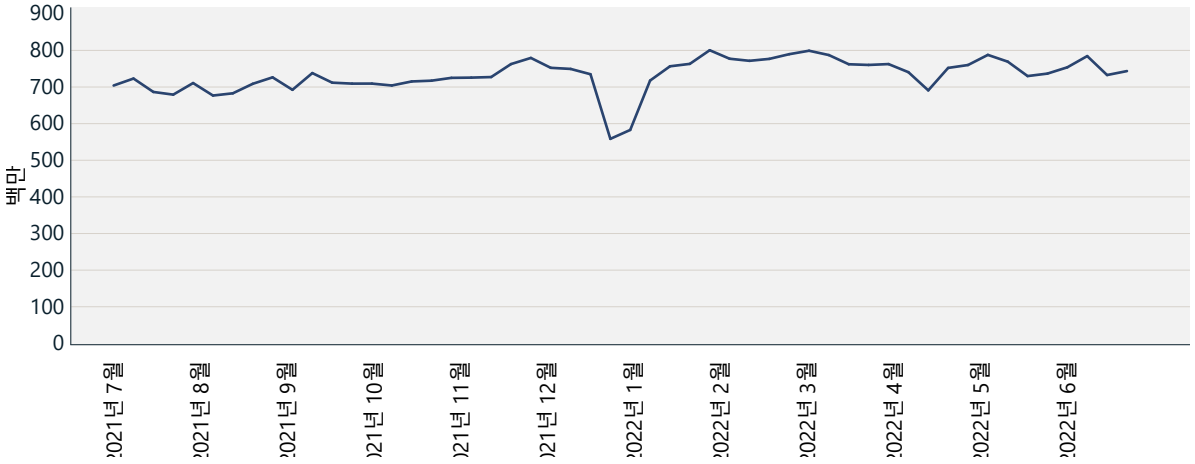
Microsoft 365 개인 인증 정보는 공격자들이 가장 많이 찾는 계정 유형 중 하나입니다. 로그인 개인 인증 정보가 침해되면 공격자들은 회사와 연결된 컴퓨터 시스템에 로그인하여 맬웨어 및 랜섬웨어 감염을 쉽게 하고, SharePoint 파일에 액세스하여 회사 기밀 데이터 및 정보를 훔치고, Outlook을 활용하여 추가 악성 이메일을 보내 피싱의 확산을 지속할 수 있습니다.

더 광범위한 대상, 그리고 개인 인증 정보, 기부, 개인 정보에 대한 피싱을 포함한 캠페인 외에도 공격자들은 더 큰 지불금을 위해 대상 비즈니스를 선별합니다. 금전적 이득을 위해 기업을 표적으로 하는 이메일 피싱 공격을 BEC 공격이라고 합니다. Microsoft는 매달 수백만 개의 BEC 이메일을 탐지하며, 이는 발견된 모든 피싱 이메일의 0.6%에 해당합니다. 2022년 5월에 발표된 IC3 보고서[18]에 따르면 BEC 공격으로 인한 노출 손실이 상승하는 추세입니다.

피싱 공격에 사용되는 기술은 계속해서 복잡해지고 있습니다. 대책에 대응하기 위해 공격자들은 기술을 구현하는 새로운 방법을 채택하고 캠페인 운영 인프라를 호스팅하는 방법과 위치의 복잡성을 높이고 있습니다. 즉, 조직은 악성 이메일을 차단하고 개별 사용자 계정에 대한 액세스 제어를 강화하기 위해 보안 솔루션을 구현하기 위한 전략을 정기적으로 재평가해야 합니다.

531,000
Defender for Office에서 차단한 URL 외에도 DCU(디지털 범죄 부서)는 Microsoft 외부에서 호스트되는 531,000개의 고유 피싱 URL을 삭제하도록 지시했습니다.

탐지된 피싱 이메일



주당 피싱 탐지 수는 계속 증가하고 있습니다. 12월~1월의 감소는 예견된 계절적 감소로, 작년 보고서에서도 보고되었습니다. 출처: Exchange Online Protection 신호

진화하는 피싱 위협 환경

계속

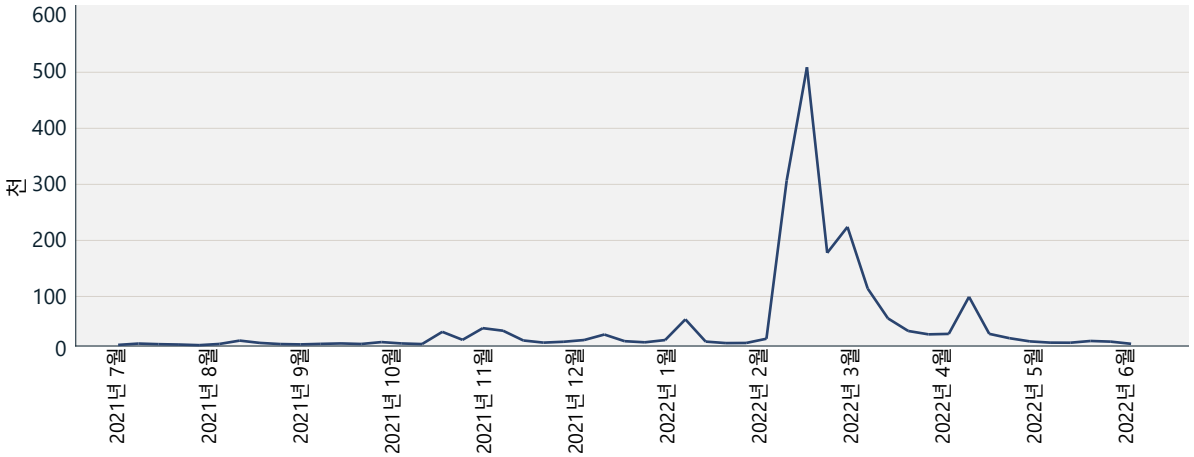
Microsoft는 피싱 이메일이 매년 꾸준히 증가하는 사실을 계속해서 발견하고 있습니다. 2020년과 2021년에 원격 근무로 전환하면서 작업 환경의 변화를 활용하기 위한 피싱 공격이 크게 증가했습니다. 피싱 공격자들은 코로나19 팬데믹과 같은 세계적인 주요 이벤트와 Google Drive 또는 OneDrive 파일 공유와 같은 협업 및 생산성 도구와 연결된 테마와 연관된 미끼로 새로운 이메일 템플릿을 빠르게 채택합니다. 코로나19 테마의 피싱은 줄어들었지만 우크라이나 전쟁은 2022년 3월 초부터 새로운 미끼가 되었습니다. Microsoft 연구원들은 우크라이나 시민을 지원하기 위해 비트코인과 Ethereum으로 암호화폐 기부를 요청하는 합법적인 조직을 사칭하는 이메일이 엄청나게 증가했다는 사실을 발견했습니다.

2022년 2월 말 우크라이나 전쟁이 시작된 지 불과 며칠 만에 기업 고객 사이에서 Ethereum 주소가 포함된 피싱 이메일이 탐지되는 경우가 급격히 증가했습니다. 총 이메일의 수는 3월 첫째 주 500만 개의 피싱 이메일에 Ethereum 지갑 주소가 포함되어 있을 때 최고조에 달했습니다. 전쟁이 시작되기 전에는 피싱으로 탐지된 다른 이메일의 Ethereum 지갑 주소 수가 훨씬 적어 하루 평균 수천 개의 이메일이 있었습니다.

피싱 공격자들은 그 어느 때보다 합법적인 인프라에 의존하여 운영하고 있어 운영의 다양한 측면을 침해하여 자체 구매, 호스팅 또는 운영할 필요가 없도록 하는 것을 목표로 하는 피싱 캠페인이 증가하고 있습니다. 예를 들어, 악성 이메일은 침해된 발신자 계정에서 시작될 수 있습니다. 공격자들은 평판 점수가 높고 새로 생성된 계정 및 도메인보다 더 신뢰할 수 있는 것으로 간주되는 이러한 이메일 주소를 사용하면 이점을 얻을 수 있습니다. 일부 고급 피싱 캠페인에서는 공격자가 DMARC[19]가 '조치 없음' 정책으로 잘못 설정된 도메인에서의 전송 및 스푸핑을 선호하여 이메일 스푸핑을 시작했다는 사실을 발견했습니다.

대규모 피싱 작업은 클라우드 서비스 및 클라우드 VM(가상 머신)을 사용하여 대규모 공격을 운영하는 경향이 있습니다. 공격자들은 SMTP 이메일 릴레이 또는 클라우드 이메일 인프라를 활용하여 VM에서 이메일을 배포하고 전달하는 프로세스를 완전히 자동화하여 이러한 합법적인 서비스의 높은 전달률과 긍정적인 평판의 이점을 누릴 수 있습니다. 악성 이메일이 이러한 클라우드 서비스를 통해 전송되도록 허용된 경우, 방어자들은 강력한 이메일 필터링 기능을 사용하여 이메일이 자신의 환경에 들어오지 못하도록 차단해야 합니다.

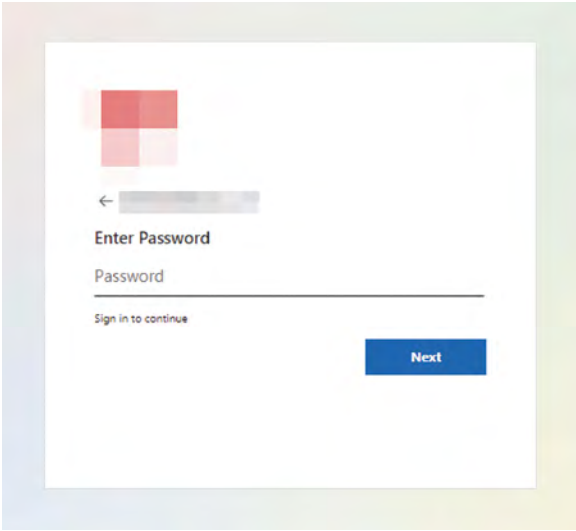
Ethereum 지갑 주소가 포함된 피싱 이메일



Ethereum 지갑 주소가 포함된 피싱으로 탐지된 총 이메일은 우크라이나 및 러시아 간 분쟁이 시작될 때 증가했으며 초기 푸시 이후 줄어들었습니다.

Microsoft 계정은 Microsoft 365 로그인 페이지를 사칭하는 수많은 피싱 랜딩 페이지에서 알 수 있듯이 피싱 운영자의 최고 타깃으로 남아 있습니다. 예를 들어, 피싱 공격자들은 수신자에게 사용자 맞춤화된 고유 URL을 생성하여 피싱 키트의 Microsoft 로그인 환경을 일치시키려고 시도합니다. 이 URL은 개인 인증 정보를 수집하기 위해 개발된 악성 웹 페이지를 가리키지만 URL의 매개 변수에는 특정 수신인의 이메일 주소가 포함됩니다. 대상이 페이지로 이동하면 피싱 키트는 사용자 로그인 데이터와 이메일 수신인에 따라 사용자 맞춤화된 회사 로고를 미리 채워 대상 회사의 사용자 맞춤형 Microsoft 365 로그인 페이지의 모양을 미러링합니다.

동적 콘텐츠로 Microsoft 로그인을 사칭하는 피싱 페이지

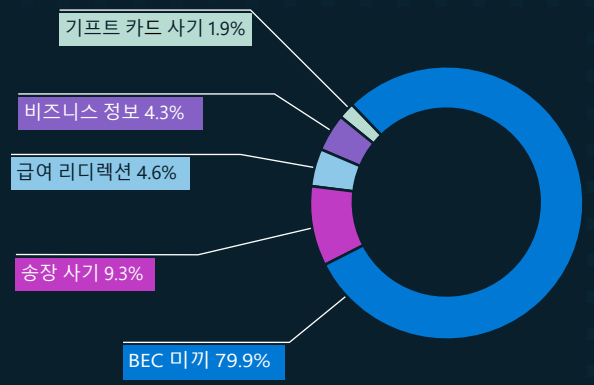


비즈니스 이메일 침해에 대한 집중 조명

사이버 범죄자들은 보안 설정을 무력화하고 개인, 기업, 조직을 표적으로 삼기 위해 점점 더 복잡성 높은 계획과 기술을 개발하고 있습니다. Microsoft는 이에 대응하여 BEC 시행 프로그램을 더욱 강화하기 위해 상당한 자원을 투자하고 있습니다.

BEC는 가장 비용이 많이 드는 금융형 사이버 범죄로, 2021년에 미화 약 24억 달러의 조정 손실이 발생했는데 이는 전 세계 상위 5개 인터넷 범죄 손실의 59% 이상을 차지합니다.[20] 문제의 범위와 BEC로부터 사용자를 보호하는 최선의 방법을 이해하기 위해 Microsoft 보안 연구원들은 공격에 사용되는 가장 일반적인 테마에 대해 추적하고 있습니다.

BEC 테마(2022년 1월~6월)



발생률에 따른 BEC 테마

BEC 추세

진입을 위해 BEC 공격자들은 일반적으로 관계 구축을 위해 잠재적인 피해자와 대화를 시작하려고 합니다. 공격자들은 동료 또는 업무상 지인으로 사칭하여 점진적으로 금전을 이체하는 방향으로 대화를 유도합니다. BEC 미끼로 추적하는 안내 이메일은 탐지된 BEC 이메일의 거의 80%를 차지합니다. 지난 한 해 동안 Microsoft 보안 연구원이 확인한 다른 추세는 다음과 같습니다.

- 2022년에 발견된 BEC 공격에서 가장 자주 사용된 기술은 스푸핑[21]과 사칭[22]이었습니다.
- 피해자에게 가장 큰 재정적 피해를 입힌 BEC 하위 유형은 송장 사기였습니다(BEC 캠페인 조사에서 본 양 및 요청된 달러 금액 기준).
- 지급 계정 보고서 및 고객 연락처와 같은 비즈니스 정보 도용을 통해 공격자들은 설득력 있는 송장 사기를 꾸밀 수 있습니다.
- 대부분의 급여 리디렉션 요청은 무료 이메일 서비스에서 전송되었으며 침해된 계정에서는 거의 전송되지 않았습니다. 이러한 소스에서 전송된 이메일의 양은 가장 일반적인 급여 날짜인 매월 1일과 15일경에 급증했습니다.
- 잘 알려진 사기 수단임에도 불구하고 기프트 카드 사기는 탐지된 BEC 공격의 1.9%에 불과했습니다.

실행 가능한 인사이트

피싱에 대한 방어

피싱에 대한 조직의 노출을 줄이려면 IT 관리자는 다음 정책 및 기능을 구현하는 것이 좋습니다.

1. 무단 액세스를 제한하기 위해 모든 계정에서 MFA를 사용해야 합니다.
2. 권한이 높은 계정에 대해 조건부 액세스 기능을 지원하여 일반적으로 조직에서 트래픽을 생성하지 않는 국가, 지역, IP의 액세스를 차단합니다.
3. 임원, 결제나 구매 활동에 관여하는 직원, 기타 권한 있는 계정에 대해 물리적 보안 키를 활용하는 것이 좋습니다.
4. Microsoft SmartScreen과 같은 서비스를 지원하는 브라우저를 사용하여 의심스러운 행동을 보이는 URL을 분석하고 알려진 악성 웹 사이트에 대한 액세스를 차단합니다.[23]
5. 이메일이 받은 편지함에 도달하기 전에 확률이 높은 피싱을 격리하고 샌드박스에서 URL 및 첨부 파일을 없애는 머신 러닝 기반 보안 솔루션(예: Microsoft Defender for Office 365)을 사용합니다.[24]
6. 조직 전체에서 사칭 및 스푸핑 방지 기능을 사용하도록 지원합니다.
7. DKIM(DomainKeys Identified Mail, 도메인키 식별 메일) 및 DMARC(Message Authentication Reporting & Conformance, 도메인 기반 메시지 인증 보고 및 적합성) 작업 정책을 환경 설정하여 스푸핑하는 것으로 알려진 전송자의 인증되지 않은 이메일이 전송되는 것을 방지합니다.
8. 테넌트 및 사용자가 생성한 허용 규칙을 감사하고 광범위한 도메인 및 IP 기반 예외를 없앱니다. 이러한 규칙은 우선시되며 이메일 필터링을 통해 알려진 악성 이메일을 허용하는 경우가 많습니다.
9. 피싱 시뮬레이터를 정기적으로 실행하여 조직 전체의 잠재적 위험을 측정하고 취약한 사용자를 식별 및 교육합니다.

추가 정보에 대한 링크

- 쿠키 도난에서 BEC까지: 공격자들은 AiTM 피싱 사이트를 금융 사기를 위한 추가 진입점으로 사용 | Microsoft 365 Defender 연구 팀, MSTIC(Microsoft 위협 인텔리전스 센터)

동형이의어 관련 속임수

BEC와 피싱은 일반적인 사회 공학 전술입니다. 사회 공학은 범죄에서 중요한 역할을 하여 표적이 신뢰를 얻음으로써 범죄자들과 상호 작용하도록 설득합니다.

실제 상거래에서 상표는 제품 또는 서비스의 출처에 대한 신뢰를 얻는 데 사용되며 위조 제품은 상표를 악용합니다. 마찬가지로 사이버 범죄자들은 피싱 공격 중 대상이 잘 아는 친숙한 연락처로 사칭하여 동형이의어로 잠재적 피해자를 속입니다.

동형이의어는 BEC에서 이메일 통신에 사용되는 도메인 이름으로, 대상을 속이기 위해 문자가 모양이 동일하거나 거의 동일한 문자로 대체됩니다.

BEC 시도에 사용되는 동형이의어 기술

BEC에는 일반적으로 두 단계가 있는데, 그 중 첫 번째 단계는 개인 인증 정보의 침해와 관련이 있습니다. 이러한 유형의 개인 인증 정보 유출은 피싱 공격 또는 대규모 데이터 침해로 인한 결과물일 수 있습니다. 그런 다음 개인 인증 정보는 다크 웹에서 판매되거나 거래됩니다.

두 번째 단계는 공격자들이 침해된 개인 인증 정보를 사용하여 동형이의어 이메일 도메인을 사용하여 정교한 사회 공학에 참여하는 사기 단계입니다.

BEC 공격의 진행

기술	동형이의어 기술을 보여 주는 도메인의 %
I 대신 l	25%
l 대신 i	12%
g 대신 q	7%
m 대신 rn	6%
.com 대신 .cam	6%
o 대신 0	5%
l 대신 ll	3%
i 대신 ii	2%
w 대신 vv	2%
ll 대신 l	2%
a 대신 e	2%
m 대신 nn	1%
I 대신 ll, i 대신 l	1%
u 대신 o	1%

2022년 1월부터 7월까지 1,700개 이상의 동형이의어 분석 결과로, 170개의 동형이의어 기술이 사용되었지만 도메인의 75%는 14개의 기술만 사용했습니다.

동형이의어의 실제 사례

피해자가 인식하는 메일 도메인과 동일하게 보이는 동형이의어 도메인은 동일한 사용자 이름으로 메일 제공자에 등록됩니다. 그런 다음 도난당한 도메인에서 새 결제 지침과 함께 도난당한 이메일이 전송됩니다.

범죄자는 오픈 소스 인텔리전스와 이메일 스레드에 대한 액세스를 활용하여 인보이스 발행 및 지불을 담당하는 개인을 식별합니다. 그런 다음 인보이스를 보내는 개인의 이메일 주소를 사칭합니다. 이러한 사칭은 동일한 사용자 이름과 실제 보낸 사람의 동형이의어 메일 도메인으로 구성됩니다.

공격자는 합법적인 인보이스가 포함된 이메일 체인을 복사한 다음 자체적으로 은행 세부 정보를 포함하도록 인보이스를 변경합니다. 그런 다음 이처럼 수정된 새 인보이스가 동형이의어로 사칭된 이메일을 통해 대상에게 재전송됩니다. 내용이 자연스럽고 이메일이 진짜처럼 보이기 때문에 대상이 사기성 지침을 따르는 경우가 많습니다.

실행 가능한 인사이트

1. 의심스러운 행동을 보이는 URL을 분석하는 서비스를 지원하는 브라우저를 사용하여 Safe Links 및 SmartScreen과 같이 알려진 악성 웹 사이트에 대한 액세스를 차단합니다.[25]
2. 이메일이 받은 편지함에 도달하기 전에 확률이 높은 피싱을 격리하고 샌드박스에서 URL 및 첨부 파일을 없애는 머신 러닝 기반 보안 솔루션을 사용합니다.

추가 정보에 대한 링크

- IC3(Internet Crime Complaint Center, 인터넷 범죄 신고 센터) | 비즈니스 이메일 침해: 미화 430억 달러 사기
- 스푸핑 인텔리전스 인사이트— Office 365 | Microsoft Docs
- 사칭 인사이트— Office 365 | Microsoft Docs

Microsoft의 협업 초기부터 봇넷 중단의 타임라인

DCU(디지털 범죄 부서)는 10년 이상 26건의 맬웨어 및 국가 차원의 중단을 발생시킨 사이버 범죄를 사전에 차단하기 위해 노력해 왔습니다. DCU(디지털 범죄 부서) 팀이 이러한 불법 작업을 차단하기 위해 고급 전술과 도구를 사용함에 따라 사이버 범죄자들도 한발 앞서 나가기 위해 접근 방법을 발전시키는 것을 볼 수 있습니다. 다음은 DCU(디지털 범죄 부서)에 의해 중단된 봇넷 샘플과 Microsoft가 봇넷을 종료하기 위해 채택한 전략을 보여 주는 타임라인입니다.

2008년

Conficker 봇넷

설명: Windows OS를 대상으로 빠르게 확산되는 웜으로, 공통 네트워크에 있는 수백만 대의 컴퓨터와 디바이스를 감염시켜 전 세계적으로 네트워크 중단을 일으켰습니다.

협업: 최초의 컨소시엄인 Conficker Working Group이 구성되었습니다. Microsoft는 봇을 물리치기 위해 전 세계 16개 조직과 파트너 관계를 맺었습니다.

Microsoft의 대응 방식: 이 그룹은 다양한 국제 관할권에서 협력했으며 Conficker를 성공적으로 중단시켰습니다.

2009년

Waledac 봇넷

설명: 이메일 주소를 수집하고 스팸을 배포하여 전 세계 최대 90,000대의 컴퓨터를 감염시킨 미국 도메인을 포함한 복잡성 높은 스팸 봇넷입니다.[26]

협업: 학계와의 긴밀한 협업에 중점을 둔 또 다른 컨소시엄인 MMPC(Microsoft Malware Protection Center, Microsoft 맬웨어 보호 센터)를 만들었습니다.[27]

Microsoft의 대응 방식: Microsoft는 C2의 계층화된 중단 접근 방식을 사용했으며 예고 없이 미국 기반 도메인을 점유하여 악의적인 공격자를 놀라게 했습니다.[28] Microsoft는 Waledac 서버에서 사용하는 거의 280개의 도메인에 임시 소유권을 부여했습니다.

2011년

Microsoft DCU(디지털 범죄 부서) 창단

협업: 조사관, 변호사, 엔지니어로 구성된 팀 간의 긴밀한 통합을 통해 Microsoft 생태계에 영향을 미치는 사이버 범죄를 차단하도록 설계되었습니다.

Microsoft의 접근 방식: 목표는 다양한 맬웨어의 기술적인 측면에 대한 이해도를 높이고 이러한 인사이트를 Microsoft의 법무 팀에 제공하여 효율적인 중단 전략을 개발하는 것입니다.

Rustock 봇넷

설명: 인터넷 제공자를 기본 C2로 사용하는 백도어 트로이 목마 스팸 이메일 봇으로, 의약품을 판매하도록 설계되었습니다.

협업: Microsoft는 Rustock에서 판매하는 약물을 이해하기 위해 Pfizer Pharmaceuticals와 파트너십을 구축하고 네덜란드 법 집행 기관과 긴밀히 협력했습니다.[29]

Microsoft의 대응 방식: Microsoft는 네덜란드의 미국의 마셜과 법 집행 기관과 협력하여 네덜란드의 C2 서버를 중단했습니다. 미래의 모든 DGA(도메인 생성기 알고리즘)을 등록하고 차단했습니다.

2013년

Sirefef/제로 액세스 봇넷

설명: 맬웨어를 설치하거나 개인 정보를 도용하는 위험한 웹 사이트로 사용자를 안내하도록 설계된 광고형 봇넷으로, 주로 미국과 서유럽에서 200만 대 이상의 컴퓨터를 감염시키고 광고주에게 매월 미화 270만 달러 이상의 비용을 사용하게 합니다.

협업: FBI 및 유로폴의 사이버 범죄 센터와 긴밀히 협력하여 P2P 인프라를 중단했습니다.

Microsoft의 대응 방식: 제로 액세스 네트워크에 가입하고, 범죄 C2 서버를 교체하고, 다운로드 서버 도메인을 성공적으로 점유했습니다.

2019년

Trickbot 봇넷

설명: 금융 서비스 산업을 대상으로 전 세계에서 파편화된 인프라를 갖춘 정교한 봇넷으로, IoT 디바이스가 침해되었습니다.

협업: Microsoft는 FS-ISAC(Financial Services Information Sharing and Analysis Center, 금융정보분석센터)와 제휴하여 Trickbot을 중단시켰습니다.[30]

Microsoft의 대응 방식: DCU(디지털 범죄 부서)는 다양한 국가의 특정 법을 고려하여 봇 인프라를 식별 및 추적하고 활성 인터넷 제공자에 대한 알림을 생성하는 시스템을 구축했습니다.

2022년

중단에 지속적으로 집중

설명: Microsoft는 지난 한 해 동안 7명의 위협 행위자들의 인프라를 중단하여 추가 맬웨어를 배포하고, 피해자의 컴퓨터를 제어하고, 추가 피해자를 대상으로 공격하지 못하도록 했습니다.

협업: Microsoft는 인터넷 서비스 제공자, 정부 기관, 법 집행 기관, 민간 기업과 협력하여 전 세계 1,700만 명 이상의 맬웨어 피해자들의 문제를 해결하기 위해 정보를 공유했습니다.

향후 전망

DCU(디지털 범죄 부서)는 계속해서 혁신을 거듭하고 있으며 봇넷 중단 경험을 활용하여 맬웨어를 뛰어넘는, 조정된 운영을 수행하려고 합니다. Microsoft가 지속적으로 성공하기 위해서는 창의적인 엔지니어링, 정보 공유, 혁신적인 법률 이론, 공공 및 민간 파트너십이 필요합니다.

사이버 범죄의 인프라 악용

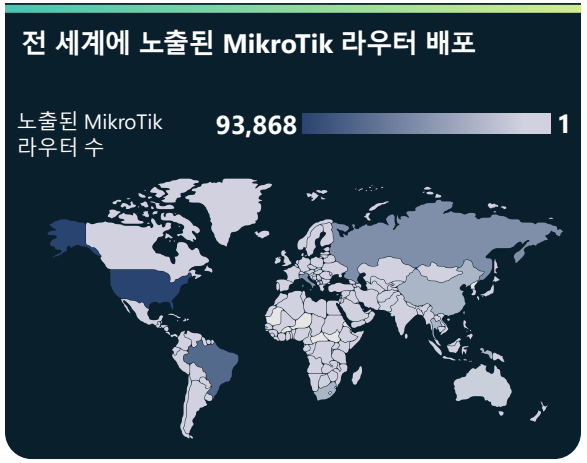
범죄 지휘 및 통제 인프라로서의 인터넷 게이트웨이

IoT 디바이스는 광범위한 봇넷을 활용하는 사이버 범죄자들에게 점점 더 인기 있는 표적이 되고 있습니다. 라우터가 패치되지 않고 인터넷에 직접 노출되면 위협 행위자들은 라우터를 악용하여 네트워크에 액세스하고 악의적인 공격을 실행하며 운영을 지원할 수도 있습니다.

Microsoft Defender for IoT 팀은 레거시 산업 제어 시스템 컨트롤러부터 최첨단 IoT 센서에 이르는 장비에 대한 연구를 수행합니다. 팀은 IoT 및 OT 관련 맬웨어를 조사하여 공유 침해 지표 목록에 기여합니다.

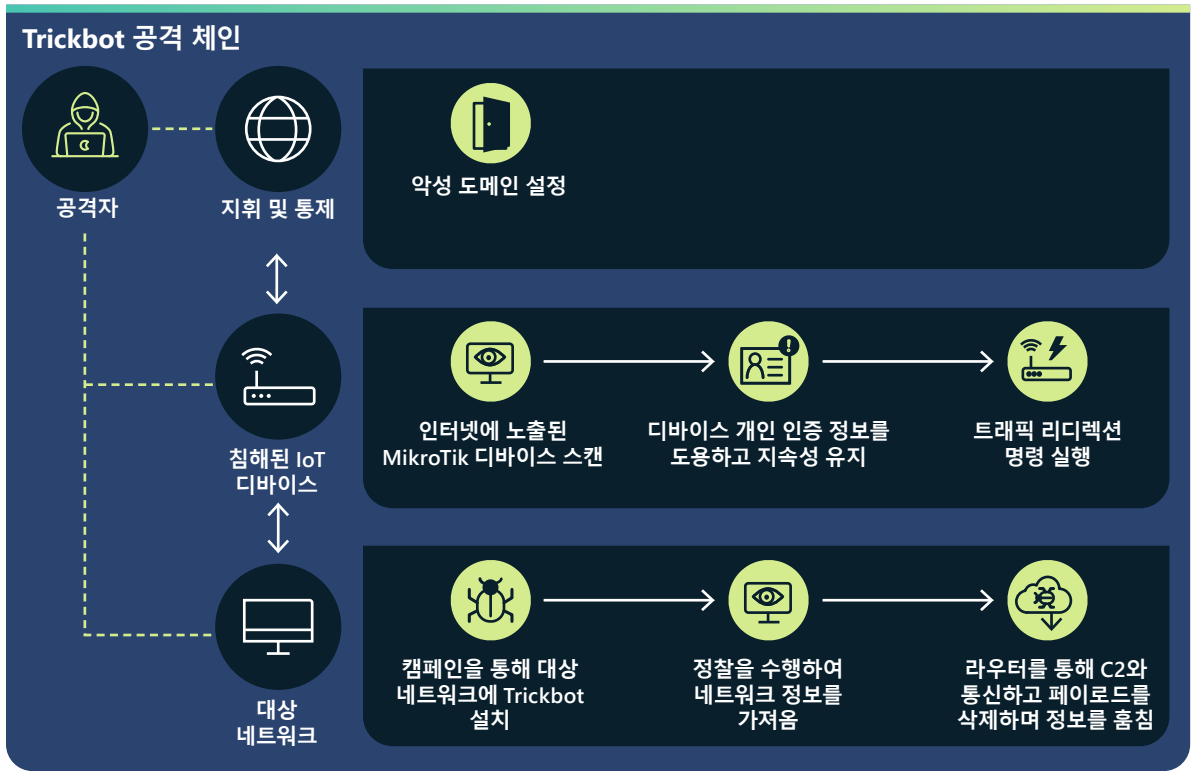
라우터는 인터넷에 연결된 가정과 조직 내 어디에나 있기 때문에 특히 취약한 공격 벡터입니다. Microsoft는 전 세계적으로 거주 및 상업적으로 인기 있는 라우터인 MikroTik 라우터의 활동을 추적하여 C2(지휘 및 통제), DNS(도메인 이름 시스템) 공격, 암호화폐 채굴 하이재킹에 어떻게 활용되는지 식별했습니다.

보다 구체적으로, Trickbot 운영자가 침해된 MikroTik 라우터를 활용하고 C2 인프라의 일부로 작동하도록 재구성하는 방법을 확인했습니다. 이러한 디바이스의 인기는 Trickbot에 의한 악용의 심각성을 더욱 악화시키고 고유한 자체 하드웨어 및 소프트웨어를 통해 위협 행위자들은 전통적인 보안 조치를 회피하고 인프라를 확장하며 더 많은 디바이스와 네트워크를 침해할 수 있습니다.



노출된 라우터는 잠재적인 취약점이 악용될 위험이 있습니다.

Microsoft는 SSH(보안 셸) 명령이 포함된 트래픽을 추적하고 분석하여 공격자가 디바이스에 대한 합법적인 개인 인증 정보를 얻은 후 MikroTik 라우터를 통해 Trickbot 인프라와 통신하는 것을 발견했습니다. 이러한 개인 인증 정보는 무차별 대입 공격, 쉽게 사용할 수 있는 패치로 알려진 취약점 악용, 기본 비밀번호를 사용하여 얻을 수 있습니다. 디바이스에 액세스하면 공격자는 라우터의 두 포트 간 트래픽을 리디렉션하는 고유한 명령을 실행하여 Trickbot의 영향을 받는 디바이스와 C2 간의 통신 회선을 설정합니다.



MikroTik IoT 디바이스를 C2의 프록시 서버로 사용하는 것을 보여 주는 Trickbot 공격 체인

Microsoft는 Trickbot뿐만 아니라 MikroTik 디바이스를 공격하는 다양한 방법과 알려진 CVE(공통 취약점 및 노출)에 대한 지식을 MikroTik 디바이스용 오픈 소스 도구로 집계하여 이러한 디바이스에 대한 공격과 관련된 포렌식 아티팩트를 추출할 수 있습니다.[31]

악성 소프트웨어 C2의 역방향 프록시 역할을 하는 디바이스는 Trickbot 및 MikroTik 라우터에만 고유한 것이 아닙니다. Microsoft RiskIQ 팀과 협력하여 관련 C2를 추적하고 SSL 인증서를 발견하여 영향을 받는 Ubiquiti 및 LigoWave 디바이스 역시 식별했습니다.[32] 이는 IoT 디바이스가 국가 차원의 조정 공격 내 활성화된 구성 요소가 되고 있으며 광범위한 봇넷을 활용하는 사이버 범죄자에게 인기가 높아지고 있다는 사실을 강력하게 나타냅니다.

IoT 디바이스를 악용하는 암호화폐 범죄자

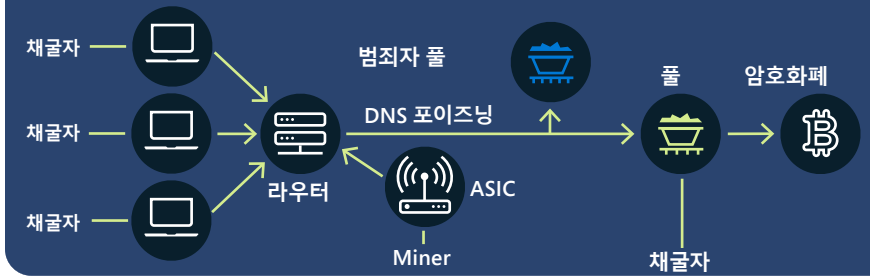
게이트웨이 디바이스는 알려진 취약점의 수가 매년 지속적으로 증가함에 따라 위협 행위자들에게 점점 더 가치 있는 표적이 되고 있습니다. 이러한 디바이스는 암호화폐 채굴 및 기타 유형의 악의적인 활동에 사용되고 있습니다.

암호화폐가 대중화됨에 따라 많은 개인과 조직이 라우터와 같은 디바이스의 컴퓨팅 성능과 네트워크 리소스에 투자하여 블록체인에서 코인을 채굴했습니다. 그러나 암호화폐 채굴은 성공 가능성이 낮은 시간 및 자원 집약적인 프로세스입니다. 코인 채굴 가능성을 높이기 위해 채굴자들은 분산된 협력 네트워크에 함께 모여 연결된 리소스로 채굴에 성공한 코인의 비율에 비례하여 해시를 받습니다.

작년에 Microsoft는 암호화폐 채굴 노력을 리디렉션하기 위해 라우터를 악용하는 공격이 증가한 사실을 발견했습니다. 사이버 범죄자들은 채굴 풀에 연결된 라우터를 침해하고 대상 디바이스의 DNS 설정을 변경하는 DNS 포이즈닝 공격을 통해 채굴 트래픽을 관련 IP 주소로 리디렉션합니다. 영향을 받은 라우터는 지정된 도메인 이름에 잘못된 IP 주소를 등록하여 채굴 리소스 또는 해시를 위협 행위자가 사용하는 풀로 보냅니다. 이러한 풀은 범죄 활동과 관련된 익명의 코인을 채굴하거나 채굴자가 생성한 합법적인 해시를 사용하여 채굴한 코인의 일정 비율을 보상으로 받을 수 있습니다.

> 2021년에 발견된 알려진 취약점의 절반 이상이 패치가 없기 때문에 회사 및 사설 네트워크에서 라우터를 업데이트하고 보호하는 것은 디바이스 담당자와 관리자에게 여전히 중요한 과제입니다.

불법 암호화폐 채굴을 위한 디바이스 침해



게이트웨이 디바이스의 DNS 포이즈닝은 합법적인 채굴 활동을 침해하고 리소스를 범죄 채굴 활동으로 리디렉션합니다.

범죄 인프라로서의 가상 머신

클라우드로의 광범위한 마이그레이션에는 피싱 또는 맬웨어 개인 인증 정보 도용을 통해 얻은 무의식적인 피해자의 개인 자산을 활용하는 사이버 범죄자가 포함됩니다. 많은 사이버 범죄자들이 클라우드 기반 VM(가상 머신), 컨테이너, 마이크로서비스에 악성 인프라를 설치하고 있습니다.

사이버 범죄자들이 액세스 권한을 갖게 되면 스크립팅 및 자동화된 프로세스를 통한 일련의 가상 머신과 같은 인프라를 설정하기 위한 일련의 이벤트가 발생할 수 있습니다. 이와 같이 스크립팅되고 자동화된 프로세스는 대규모 이메일 스팸 공격, 피싱 공격, 악의적인 콘텐츠를 호스팅하는 웹 페이지를 비롯하여 악의적인 활동을 시작하는 데 사용됩니다. 여기에는 암호화폐 채굴을 수행하는 확장된 가상 환경을 설정하여 최종 피해자에게 월말에 미화 수십만 달러의 청구서를 부과하는 것도 포함될 수 있습니다.

사이버 범죄자들은 악의적인 활동이 탐지되고 종료될 때까지 수명이 제한되어 있다는 사실을 이해합니다. 이로 인해 이들은 규모를 확장했으며 현재 비상 상황을 최우선으로 고려하여 사전 예방적인 자세로 운영합니다. 또한 침해된 계정을 미리 준비하고 환경을 모니터링합니다. 계정(수십만 개의 가상 머신을 사용하여 설정)이 탐지되는 즉시 다음 계정(이미 스크립트를 통해 바로 활성화될 준비가 되어 있는 계정)으로 이동하여 거의 또는 전혀 중단 없이 악의적인 활동을 지속합니다.

클라우드 인프라와 마찬가지로 온-프레미스 인프라는 온-프레미스 사용자에게 알려지지 않은 가상 로컬 환경을 활용한 공격에 사용할 수 있습니다. 이렇게 하려면 초기 액세스 포인트가 개방되어 있고 액세스 가능한 상태를 유지해야 합니다. 온-프레미스 프라이빗 자산은 또한 사이버 범죄자들에 의해 악용되어 의심스러운 인프라 생성 탐지를 피하기 위해 출처를 난독화하도록 설정된 클라우드 인프라의 후속 체인을 시작합니다.

실행 가능한 인사이트

1. 우수한 사이버 위생을 구현하고 직원들에게 사회 공학을 피하기 위한 지침과 함께 사이버 보안 교육을 제공합니다.
2. 대규모 검색을 통해 정기적으로 자동화된 사용자 활동 변칙 검사를 수행하여 이러한 유형의 공격을 줄입니다.
3. 회사 및 개인 네트워크에서 라우터를 업데이트하고 보호합니다.

핵티비즘(hacktivism)은 계속되는가?

핵티비즘(hacktivism)이 새로운 현상은 아니지만 우크라이나 전쟁에서 정부 기관이 정치적 적수, 조직, 심지어 국가 차원의 평판이나 자산을 침해하기 위해 사이버 도구를 배치하도록 지시하는 등 자발적인 해커들의 수가 급증했습니다.

2022년 2월 우크라이나 정부 기관은 전 세계 민간인들에게 3만 명의 강력한 'IT 부대'의 일환으로 러시아에 대한 사이버 공격을 수행할 것을 촉구했습니다.[33] 이와 동시에 Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans, RaidForum2와 같은 기존 핵티비스트 그룹이 우크라이나를 지원하기 위해 공격을 시작했습니다. 일부 Conti 랜섬웨어 갱을 비롯한 다른 그룹은 러시아 편에 섰습니다.[34]

그 후 몇 달 동안 Anonymous의 활동은 매우 눈에 띄었습니다. 그룹의 이름 또는 연합군의 이름으로 활동하는 해커들은 수천 개의 러시아 및 벨라루스 웹 사이트를 일시적으로 비활성화하고, 수백 기가바이트의 도난당한 데이터를 유출하며, 러시아 TV 채널을 해킹하여 친 우크라이나 콘텐츠를 재생했고, 항복한 러시아 탱크에 비트코인을 지불하겠다고 제안했습니다.

시민 해커들의 부상

소셜 미디어 플랫폼으로 인해 DDoS 공격과 같이 쉽게 실행할 수 있는 공격에 대한 수행 지침을 받은 수천 명의 시민 해커를 신속하게 조직하고 동원할 수 있었습니다. 주최자들은 트위터, 텔레그램, 비공개 포럼을 활용하여 해커를 결집하고, 작전을 구성하며, 해킹 지침 매뉴얼을 배포했습니다.

하지만, 이와 같은 지침이 있더라도 대부분의 해커들이 보유한 기술은 제한적일 수 있습니다. 이는 기본적인 기술 역량을 지닌 수백 또는 수천 명의 개인이 공격 템플릿을 사용하여 표적을 표적으로 하는 조직화된 공격 또는 개인적인 핵티비스트 공격을 수행하는 첫 번째 미래와 우크라이나를 향한 적대 행위가 결국 끝날 때 다음 정치적 또는 사회적 문제가 행동을 촉구할 때까지 핵티비즘을 뒤로하는 두 번째 미래 등 두 가지 가능한 미래 모습을 제시합니다.

해커들의 정치화

이러한 정치적 동원으로 인한 더 큰 위험은 기술에 정통한 해커들이 자체적으로 시작하거나 정부 기관의 요청에 따라 자국의 우선순위를 지원하기 위해 외국 정부 기관을 표적으로 삼은 사이버 공격을 계속해서 수행할 수 있다는 것입니다.

이란, 중국, 러시아는 이미 핵티비즘을 국가 해킹 그룹의 구성원으로 모집하고 있습니다. 예를 들어, 2022년 4월 친러시아 해킹 그룹인 Killnet은 체코가 전쟁에 직접 관여하지 않았음에도 불구하고 체코 철도, 지역 공항, 체코 공무원 서버를 표적으로 삼은 DDoS 공격을 시작했습니다.[35] 이와 동시에 일부 정부 기관은 핵티비즘을 전통적인 사이버 스파이 활동이나 사보타주 작전(예: 이스라엘에 대한 이란의 활동)을 은폐하는 데 사용할 수 있습니다.

핵티비즘과 관련된 DDoS 공격이 증가하는 환경에서 기술 산업은 웹 사이트로 들어오는 정상 트래픽 흐름과 비정상 트래픽 흐름의 차이를 신속하게 해독해야 하는 어려움에 직면해 있습니다. Microsoft와 파트너는 악성 DDoS 트래픽을 구별하고 트래픽의 출처를 추적하는 도구 모음을 개발했습니다. 또한 Microsoft의 Azure 플랫폼은 플랫폼에서 매우 높은 수준의 아웃바운드 트래픽을 생성하는 컴퓨터를 식별하고 종료할 수 있습니다.

시위웨어의 출현

시위웨어는 러시아와 우크라이나 간의 전쟁에 대한 감정적 반응의 직접적인 결과로 등장했습니다. 일부 오픈 소스 소프트웨어 개발자들은 소프트웨어의 인기를 전개되고 있는 지정학적 상황에 대해 발언하거나 관련 조치를 취하는 수단으로 사용했습니다. 여기에는 평화의 메시지를 전파하기 위해 데스크톱이나 브라우저에서 열리는 무해한 텍스트 파일이 있지만 IP 주소의 지리적 위치를 기반으로 한 표적 공격 및 하드 드라이브 삭제와 같은 파괴적인 작업도 포함되었습니다. 다른 국제적인 이벤트가 전개됨에 따라 향후 시위웨어가 다시 표면화될 것으로 기대할 수 있습니다. 일반적으로 존경받는 오픈 소스 관리자가 자신의 오픈 소스 구성 요소를 활용하여 개인적인 진술을 하기로 결정하여 발생하기 때문에 현재 소스 파일 패키지에서 이러한 유형의 변경이 발생하는 것을 막을 수 있는 보호 장치는 없으며 사용자는 이로 인한 잠재적인 영향이 있다는 사실을 인식해야 합니다.

소셜 미디어 플랫폼으로 인해 DDoS 공격과 같이 쉽게 실행할 수 있는 공격에 대한 수행 지침을 받은 수천 명의 시민 해커를 조직하고 동원할 수 있었습니다.

실행 가능한 인사이트

1. 기술 산업은 이와 같은 새로운 위협에 대한 포괄적인 대응을 설계하기 위해 함께 해야 합니다.
2. Microsoft를 비롯한 기술 분야의 선두 기업은 DDoS 공격과 관련된 악성 트래픽을 식별하고 해당 컴퓨터를 비활성화하는 도구를 보유하고 있습니다.
3. 오픈 소스 사용자는 지정학적 분쟁이 발생하는 동안 경계를 강화해야 합니다.

미주

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. EDR(엔드포인트 탐지 및 대응) 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 Forum은 기존 회원이 새 회원의 영입을 보증해야 하는 온라인 토론 포럼입니다.
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. 데이터 출처: Defender for Office(악성 이메일/침해된 ID 활동), Azure Active Directory Identity Protection(침해된 ID 이벤트/경고), Defender for Cloud Apps (침해된 ID 데이터 액세스 이벤트), M365D (제품 간 상관관계).
17. 데이터 출처: Defender for Endpoint(공격 동작 경고/이벤트), Defender for Office(악성 이메일), M365D(제품 간 상관관계).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. 도메인 기반 메시지 인증, 보고 및 적합성: 이메일 도메인 담당자에게 무단 사용으로부터 도메인을 보호할 수 있도록 설계된 이메일 인증, 정책, 보고 프로토콜입니다.
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. 2010년 2월 22일).
27. See Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 2011년 9월 27일.
28. 특히, 연방 민사소송규칙 제65조는 1) 구제가 승인되지 않을 경우 당사자가 즉각적이고 돌이킬 수 없는 피해를 입고, 2) 당사자가 상대방에게 적시에 통지를 제공하려고 하는 경우 당사자가 그러한 구제책을 추구할 수 있도록 허용합니다. 뿐만 아니라, 법에 의거하여 대중에 입힌 피해의 양에 대해 피고인의 통지 권리의 균형을 맞추는 균형 테스트를 적용해야 합니다.
29. Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D. Wa. 2011년 2월 9일).
30. Microsoft Corp. v. Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. 2021년 8월 12일).
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

국가 차원의 위협

국가 차원의 공격자들은 탐지를 피하고 전략적 우선순위를 높이기 위해 점점 더 정교한 사이버 공격을 시작하고 있습니다.

국가차원의 위협

개요

국가 차원의 공격자들은 탐지를 피하고 전략적 우선순위를 높이기 위해 점점 더 정교한 사이버 공격을 시작하고 있습니다. 우크라이나의 하이브리드 전쟁에서 사이버 무기 배치의 출현은 새로운 갈등 시대의 시작을 의미합니다.

러시아는 또한 선전을 활용하여 러시아, 우크라이나, 전 세계 여론에 영향을 미치는 정보 영향력 작전으로 전쟁을 지원했습니다. 이처럼 최초의 본격적인 하이브리드 분쟁은 다른 중요한 교훈을 가르쳐주었습니다. 첫째, 디지털 운영 및 데이터의 보안은 클라우드로 마이그레이션하면 사이버 공간과 물리적 공간 모두에서 가장 잘 보호될 수 있습니다. 초기 러시아 공격은 와이퍼 맬웨어로 온-프레미스 서비스를 표적으로 삼았고 최초로 발사된 미사일 중 하나가 물리적 데이터 센터를 표적으로 삼았습니다.

우크라이나는 워크로드와 데이터를 우크라이나 외부의 데이터 센터에서 호스팅되는 하이퍼스케일 클라우드로 빠르게 마이그레이션하여 대응했습니다. 둘째, 클라우드의 데이터와 고급 AI 및 ML 서비스로 구동되는 사이버 위협 인텔리전스 및 엔드포인트 보호의 발전은 우크라이나가 러시아 사이버 공격을 방어하는 데 도움이 되었습니다.

다른 곳에서는 국가 차원의 공격자들이 더욱 활발하게 활동하고 자동화, 클라우드 인프라, 원격 액세스 기술의 발전을 활용하여 더 광범위한 대상을 공격하고 있습니다. 최종 목표물에 액세스할 수 있는 기업 IT 공급망이 빈번하게 공격을 받았습니다. 사이버 보안 위생은 공격자가 패치되지 않은 취약점을 신속하게 악용하고, 정교하면서도 무차별적인 공격 기술을 사용하여 개인 인증 정보를 훔치고, 오픈 소스 또는 합법적인 소프트웨어를 활용하여 작전을 난독화함에 따라 더욱 중요해졌습니다. 또한 이란은 러시아와 함께 랜섬웨어를 포함한 파괴적인 사이버 무기를 공격의 주요 요소로 사용하고 있습니다.

이러한 발전은 인권을 우선시하고 온라인에서 무모한 국가 행동으로부터 사람들을 보호하는 일관적인 글로벌 프레임워크를 긴급하게 채택해야 합니다. 모든 국가는 책임 있는 국가 행동을 위한 규범과 규칙을 이행하도록 합의해야 합니다.

우크라이나 방어: 사이버 전쟁 초기의 교훈 — 문제에 대응하는 Microsoft

주요 인프라, 특히 IT 부문, 금융 서비스, 운송 시스템, 통신 인프라에 대한 타겟팅이 증대되고 있습니다.

35페이지에서 자세히 알아보기

IT 공급망이 대상에 액세스하기 위한 게이트웨이로 사용되고 있습니다.

NOBELIUM

36페이지에서 자세히 알아보기

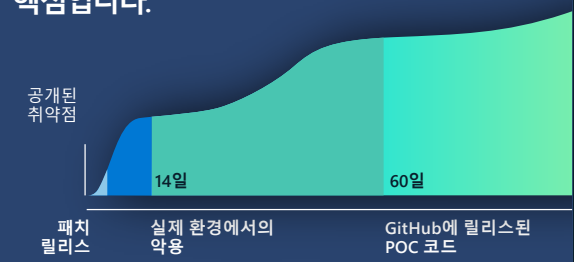
중국은 정보와 경쟁 우위를 확보하기 위해 특히 동남아시아의 소규모 국가를 대상으로 글로벌 타겟팅을 확대합니다.

44페이지에서 자세히 알아보기

이란은 권력 이양 이후 점점 더 공격적으로 성장했고, 랜섬웨어 공격 대상을 지역 내 적을 넘어 미국과 EU 희생자들로 확대했으며, 미국의 주요 인프라를 표적으로 삼았습니다.

46페이지에서 자세히 알아보기

패치되지 않은 취약점을 식별하고 신속하게 악용하는 것이 핵심 전술이 되었습니다. 보안 업데이트의 신속한 배포는 방어의 핵심입니다.



39페이지에서 자세히 알아보기

북한은 국방 건설, 경제 강화, 국내 안정 보장이라는 정권의 목표를 달성하기 위해 국방 및 항공우주 기업, 암호화폐, 언론사, 탈북자, 구호 단체를 표적으로 삼고 있습니다.

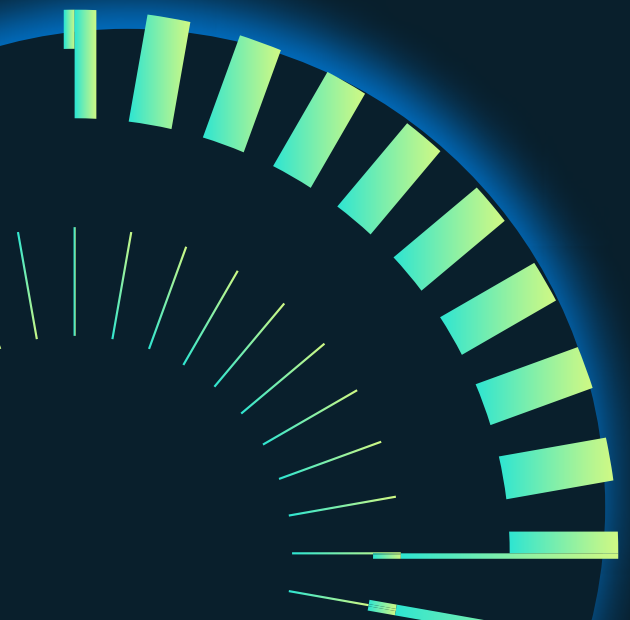
49페이지에서 자세히 알아보기

사이버 용병들은 성장하는 민간 기업 산업이 고객(종종 정부 기관)이 네트워크 및 디바이스에 침입할 수 있도록 고급 도구, 기술, 서비스를 개발하고 판매함에 따라 사이버 공간의 안정성을 위협합니다.

52페이지에서 자세히 알아보기

서문

2020년과 2021년, 세간의 이목을 끄는 공격에 이어 국가 차원의 위협 행위자들은 정교한 위협으로부터 방어하기 위해 조직에서 구현한 새로운 보안 보호에 적응하는 데 상당한 리소스를 소비했습니다.



엔터프라이즈급 조직과 마찬가지로 공격자들은 자동화, 클라우드 인프라, 원격 액세스 기술의 발전을 활용하여 더 광범위하게 공격 대상을 확장하기 시작했습니다. 이러한 전술적 변화는 기업 공급망을 표적으로 삼은 새로운 접근 방식과 대규모 공격으로 이어졌습니다. IT 보안 방역은 공격자들이 패치되지 않은 취약점을 신속하게 악용하고, 기업 네트워크를 침해하는 기술을 확장하며, 오픈 소스 또는 합법적인 소프트웨어를 활용하여 운영을 난독화하는 새로운 방법을 개발함에 따라 더욱 중요해졌습니다. 새로운 공격 기술은 표적의 네트워크에 액세스하기 위해 탐지하기 어려운 새로운 벡터를 제공했습니다. 마지막으로, 전시의 물리적 공격이 확대됨에 따라 사이버 공격이 군사 활동에서 중요한 역할을 하는 것을 보았습니다.

우크라이나의 분쟁은 사이버 공격이 지상에서의 군사적인 충돌과 병행하여 전 세계에 영향을 미치기 위해 진화하는 방법에 대한 너무나 신랄한 예를 제공했습니다. 전력 시스템, 통신 시스템, 언론, 기타 주요 인프라 모두 물리적 공격 및 사이버 공격의 표적이 되었습니다. 스파이 활동 및 정보 유출 캠페인의 일환으로 일반적으로 발견되는 네트워크 침해 시도는 주요 인프라 시스템에 대한 파괴적인 와이퍼 맬웨어 공격에 대한 하이브리드 전쟁에 집중되었습니다. 이러한 시스템의 보안을 클라우드에 연결하면 잠재적으로 파괴적인 공격을 조기에 탐지하고 중단할 수 있습니다.[1]

주요 사이버 이벤트에서 처음으로 머신 러닝을 활용하는 행동 탐지는 알려진 공격 패턴을 사용하여 인간이 위협을 인식하기도 전에 근본적인 맬웨어에 대한 사전 지식 없이도 추가 공격을 성공적으로 식별하고 차단했습니다. 또한 이러한 시스템을 보호하는 방어자와 실시간으로 위협 인텔리전스를 공유하여 활성 공격을 예측하고 방어하는 데 중요한 정보를 제공하는 것에 대한 가치를 확인했습니다.

전 세계의 국가 차원의 위협 행위자들은 새로운 방식 및 오래된 방식으로 계속해서 운영을 확장하고 있습니다. 중국, 북한, 이란, 러시아는 모두 Microsoft 고객을 표적으로 삼아 공격을 수행했습니다. IT 서비스 공급망은 공격자들이 여러 조직에 대한 액세스 포인트가 될 수 있는 업스트림 서비스로 주안점을 바꿈에 따라 공통 목표가 되었습니다. 우리는 공격자들로 인해 엔터프라이즈급 공급망에서 신뢰할 수 있는 관계를 계속 악용하여 인증 규칙의 포괄적인 적용, 지속적인 패치, 원격 액세스 인프라에 대한 계정 환경 설정, 진위 여부를 확인하기 위한 파트너 관계에 대한 빈번한 감사의 중요성을 강조될 것으로 예상합니다.

랜섬웨어 및 범죄 운영자와 마찬가지로 국가 차원의 공격자들은 잘못된 방식으로 환경 설정되거나 패치되지 않은 엔터프라이즈급 시스템(VPN/VPS 인프라, 온-프레미스 서버, 서드파티 소프트웨어)을 표적으로 삼아 지상 공격을 수행함으로써 노출 증가에 대응했습니다. 많은 공격자들이 악성 활동을 난독화하기 위해 상용 맬웨어와 오픈 소스 레드 팀 도구의 사용을 늘렸습니다.

결과적으로 우선순위가 지정된 패치를 통해 IT 보안 방역의 강력한 기준을 유지하고, 안티 템퍼 기능을 활성화하고, RiskIQ와 같은 공격 표면 관리 도구를 활용하여 공격 표면에 대한 외부 뷰를 확보하고, 기업 전체에서 다중 인증을 활성화하는 것이 수많은 정교한 공격자들로부터 사전에 방어하기 위한 기본 사항이 되었습니다.

국가 차원의 공격자들은 또한 공격 시 전술로서의 랜섬웨어 사용을 증가시켜, 해당 범죄 생태계에서 생성된 랜섬 맬웨어를 공격에 재사용하는 경우가 많아졌습니다. 이란과 북한에 기반을 둔 공격자들이 상용 랜섬웨어 도구를 활용하여 지역 경쟁자들 사이에서 주요 인프라를 포함한 표적 시스템을 침해했습니다. 마지막으로, 취약한 서드파티 솔루션에 대한 악용을 확대하기 위해 도구, 기술, 서비스를 개발하고 판매하는 사이버 용병의 위협이 증가했습니다. 국가 차원의 공격자들이 행하는 공격의 정교함과 민첩성은 매년 계속해서 진화할 것입니다. 조직은 이러한 공격자들의 변화에 대한 정보를 얻어 이에 대응함과 동시에 방어 역량을 개선해야 합니다.

John Lambert
Microsoft Threat Intelligence Center의 기업 부사장 겸 저명한 엔지니어

국가 차원의 데이터에 대한 배경

국가 차원의 사이버 위협은 국익을 증진하려는 명백한 의도를 가진 특정 국가에서 비롯된 사이버 위협 작업입니다. 국가 차원의 공격자들은 지적 재산권 도용, 스파이 활동, 감시, 개인 인증 정보 도용, 파괴적인 공격 등을 비롯하여 고객이 직면한 가장 지능적이고 지속적인 위협 중 일부를 제시합니다.

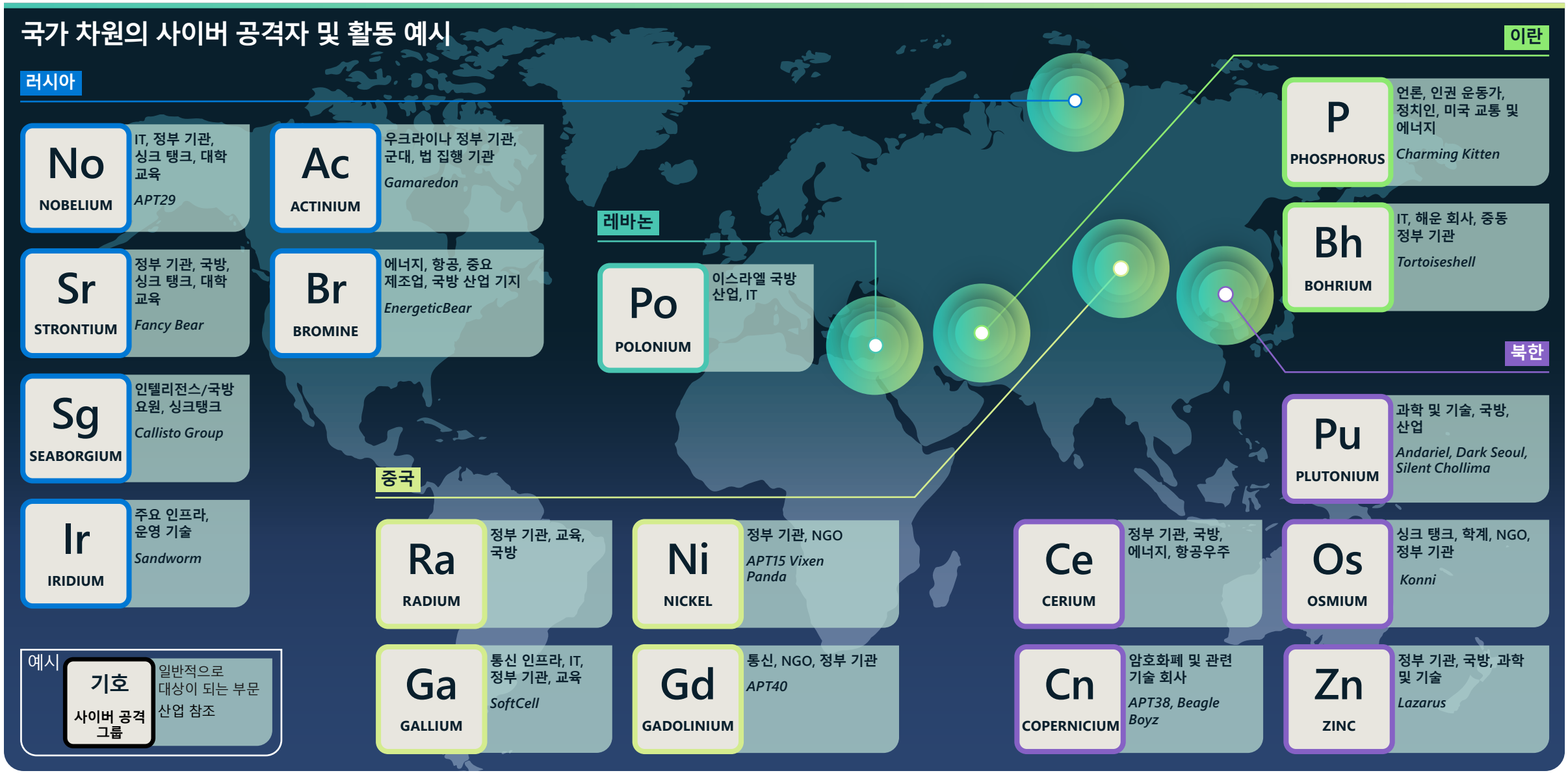
Microsoft는 이러한 위협을 발견하고 이해하며 이에 대응하는 데 상당한 리소스를 투자합니다. 조직 또는 개인 계정 담당자가 발견된 국가 차원 공격자들의 대상이 되거나 이들로 인해 침해된 경우 Microsoft는 공격 활동을 조사하는 데 필요한 정보를 포함하여 NSN(Nation State Notification, 국가 차원의 알림) 형식으로 고객에게 직접 경고를 전달합니다. 2018년에 시작한 이래, 2022년 6월 기준으로 67,000개 이상의 NSN을 제공했습니다.

이 장에서는 Microsoft NSN 경고 데이터를 제공하여 측정 가능한 활동에 대한 알아봅니다. 차트에 표시된 국가 차원의 활동 수준은 고객 조직에서 하나 이상의 계정을 표적으로 삼거나 침해하는 국가 차원의 공격자들의 탐지에 대한 대응으로 Microsoft에서 고객에게 발급한 NSN 수를 기반으로 합니다.

이 보고서에 포함된 위협 그룹 중 주요 4개국은 러시아, 중국, 이란, 북한입니다. 이는 지난 한 해 동안 Microsoft 고객을 표적으로 하는, 가장 일반적으로 발견된 공격자들의 출신 국가를 나타냅니다. 이 보고서에는 레바논과 사이버 용병 또는 민간 부문의 공격자들의 위협 그룹에 대한 발견 내용도 포함되어 있습니다.

Microsoft는 화학 원소 이름(예: NOBELIUM)으로 국가 그룹을 식별하며, 그중 일부만 다음 페이지에 표시되었습니다. DEV-#### 지정은 알려지지 않거나 새롭게 부상하거나 개발 중인 위협 활동 클러스터에 지정된 임시 이름으로 사용하기 때문에 활동 뒤에 있는 공격자들의 출신 국가 또는 신원에 대한 높은 확신이 들 때까지 고유한 정보 집합으로 추적할 수 있습니다.

기준을 충족하면 DEV는 지명된 공격자로 전환되거나 기존 공격자와 병합됩니다. 이 장 전체에서 공격 대상, 기술, 동기 분석에 대한 심층적인 시각을 제공하기 위해 국가 차원 및 DEV 그룹의 예를 인용합니다. 이들 중 대다수의 그룹은 사이버 범죄자들과 동일한 도구를 사용하지만 맞춤형 맬웨어, 제로 데이의 취약점을 발견하고 활용하는 기능, 법적 처벌의 형태로 고유한 위협을 제시합니다.


국가 차원의 사이버 공격자 및 활동 예시
러시아
No
NOBELIUM
IT, 정부 기관, 싱크 탱크, 대학 교육
APT29
Ac
ACTINIUM
우크라이나 정부 기관, 군대, 법 집행 기관
Gamaredon
Sr
STRONTIUM
정부 기관, 국방, 싱크 탱크, 대학 교육
Fancy Bear
Br
BROMINE
에너지, 항공, 중요 제조업, 국방 산업 기지
EnergeticBear
Sg
SEABORGIUM
인텔리전스/국방 요원, 싱크탱크
Callisto Group
Ir
IRIDIUM
주요 인프라, 운영 기술
Sandworm
레바논
Po
POLONIUM
이스라엘 국방 산업, IT
이란
P
PHOSPHORUS
언론, 인권 운동가, 정치인, 미국 교통 및 에너지
Charming Kitten
Bh
BOHRIUM
IT, 해운 회사, 중동 정부 기관
Tortoiseshell
북한
Pu
PLUTONIUM
과학 및 기술, 국방, 산업
Andariel, Dark Seoul, Silent Chollima
중국
Ra
RADIUM
정부 기관, 교육, 국방
Ni
NICKEL
정부 기관, NGO
APT15 Vixen Panda
Ce
CERIUM
정부 기관, 국방, 에너지, 항공우주
Os
OSMIUM
싱크 탱크, 학계, NGO, 정부 기관
Konni
Ga
GALLIUM
통신 인프라, IT, 정부 기관, 교육
SoftCell
Gd
GADOLINIUM
통신, NGO, 정부 기관
APT40
Cn
COPERNICIUM
암호화폐 및 관련 기술 회사
APT38, Beagle Boyz
Zn
ZINC
정부 기관, 국방, 과학 및 기술
Lazarus
예시
기호
사이버 공격 그룹
일반적으로 대상이 되는 부문 산업 참조

진화하는 위협 환경

국가 차원의 공격자 활동을 추적하고 대상이 되거나 침해되는 것을 발견할 때 고객에게 알리는 Microsoft의 사명은 공격으로부터 고객을 보호한다는 사명에 뿌리를 두고 있습니다.

이러한 알림은 발견된 공격이 Microsoft의 보안 관련 제품을 통한 보호로 성공적으로 방지되는지 또는 알려지지 않은 보안 약점으로 인해 공격이 효과적인지 여부를 고객에게 알리기 위한 노력의 중요한 부분입니다. 시간에 따른 알림 추적은 Microsoft가 공격자별로 진화하는 위협 추세를 식별하고 클라우드 서비스 전반에서 고객에 대한 위협을 사전에 완화하는 데 제품 보호에 집중하는 데 도움이 됩니다.

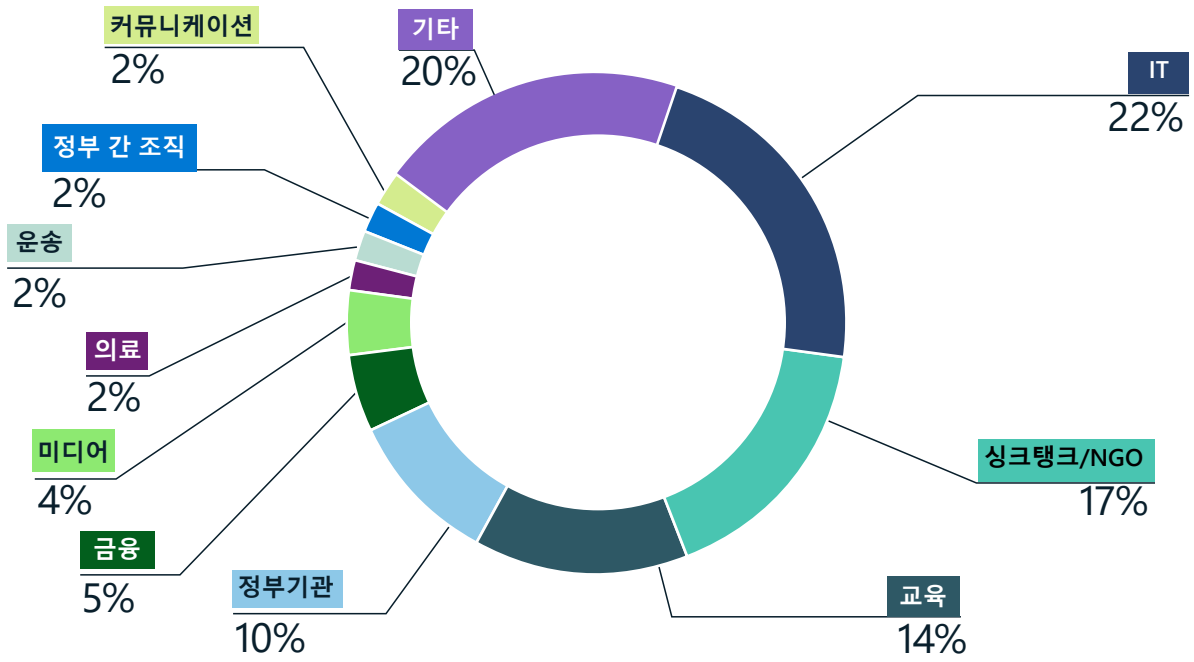
이 추적을 통해 우리가 보는 것에 대한 데이터와 인사이트를 공유할 수도 있습니다. 분석가들은 이러한 공격자와 공격을 추적하여 기술 지표와 지정학적 전문 지식의 조합에 의존하여 공격자들의 동기를 이해하고 기술 및 국제적인 컨텍스트를 새로운 인사이트로 결합합니다. 이처럼 엄선된 정보는 국가 차원의 사이버 공격자들의 우선순위와 이들의 동기가 이들을 고용하는 국가의 정치적, 군사적, 경제적 우선순위를 어떻게 반영할 수 있는지에 대한 독특한 관점을 제공합니다.

지난 한 해 동안 발전한 정치는 전 세계적으로 국가가 후원하는 위협 그룹의 우선순위와 위험 허용 범위를 형성했습니다. 지정학적 관계가 무너지고 일부 국가에서 강경파들이 더 많은 통제권을 획득함에 따라 사이버 공격자들은 더욱 뻔뻔스럽고 공격적으로 변했습니다. 예를 들면 다음과 같습니다.

- 러시아는 지상 군사 작전을 보완하기 위해 우크라이나 정부 기관과 국가의 중요한 기반 시설을 가차 없이 표적으로 삼았습니다.[2]
- 이란은 항만과 같은 미국의 중요 기반 시설에 적극적으로 침투하려고 했습니다.
- 북한은 금융 및 기술 회사로부터 암호화폐를 훔치는 캠페인을 지속했습니다.
- 중국은 국제 사이버 스파이 활동을 확대했습니다.

국가 차원의 공격자들은 기술적으로 정교하고 다양한 전술을 사용할 수 있지만 이러한 공격은 좋은 사이버 방역을 통해 완화되는 경우가 많습니다. 이러한 공격자들 중 다수는 사용자 맞춤형 악용 방식을 개발하거나 표적 사회 공학을 활용하여 목표를 달성하는 데 투자하는 대신 스피어 피싱 이메일과 같은 상대적으로 낮은 기술 수단에 의존하여 정교한 맬웨어를 제공합니다.

국가 차원의 공격자들이 목표로 하는 산업 부문



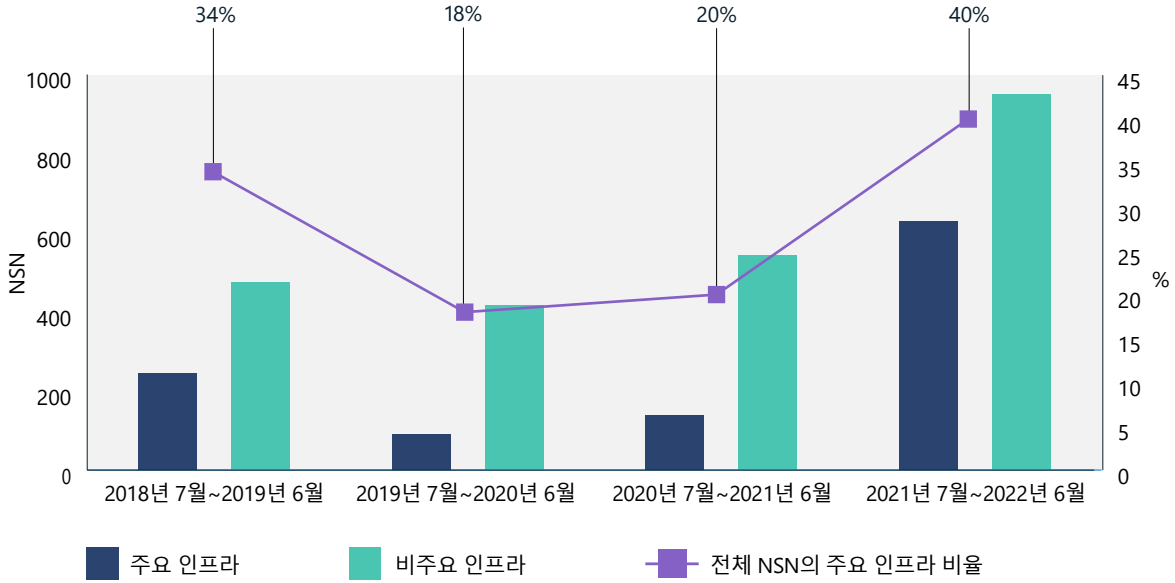
국가 차원의 그룹은 다양한 부문을 목표로 했습니다. 러시아와 이란의 국가 차원 공격자들은 IT 기업의 고객에게 접근하기 위한 수단으로 IT 산업을 표적으로 삼았습니다. 싱크 탱크, NGO(비정부기구), 대학, 정부 기관은 국가 차원 공격자들의 다른 공통 목표로 남아있었습니다.

국가 차원의 공격자들에게는 특정 그룹의 조직 또는 개인을 표적으로 삼을 수 있는 다양한 목표가 있습니다. 작년에는 공급망 공격이 증가했으며 특히 IT 회사에 집중되었습니다. 위협 행위자는 IT 서비스 제공자를 침해함으로써 연결된 시스템을 관리하는 회사와의 신뢰할 수 있는 관계를 통해 원래 대상에 도달하거나 한 번의 공격으로 수백 명의 다운스트림 고객을 침해하여 훨씬 더 큰 규모의 공격을 실행할 수 있습니다. IT 부문 다음으로 가장 빈번하게 표적이 된 그룹은 싱크 탱크, 대학 부속 학자, 정부 기관 관료였습니다. 이들은 지정학적 문제에 대한 정보를 수집하기 위한 스파이 활동의 바람직한 '소프트 타깃'입니다.

진화하는 위협 환경

계속

주요 인프라 동향

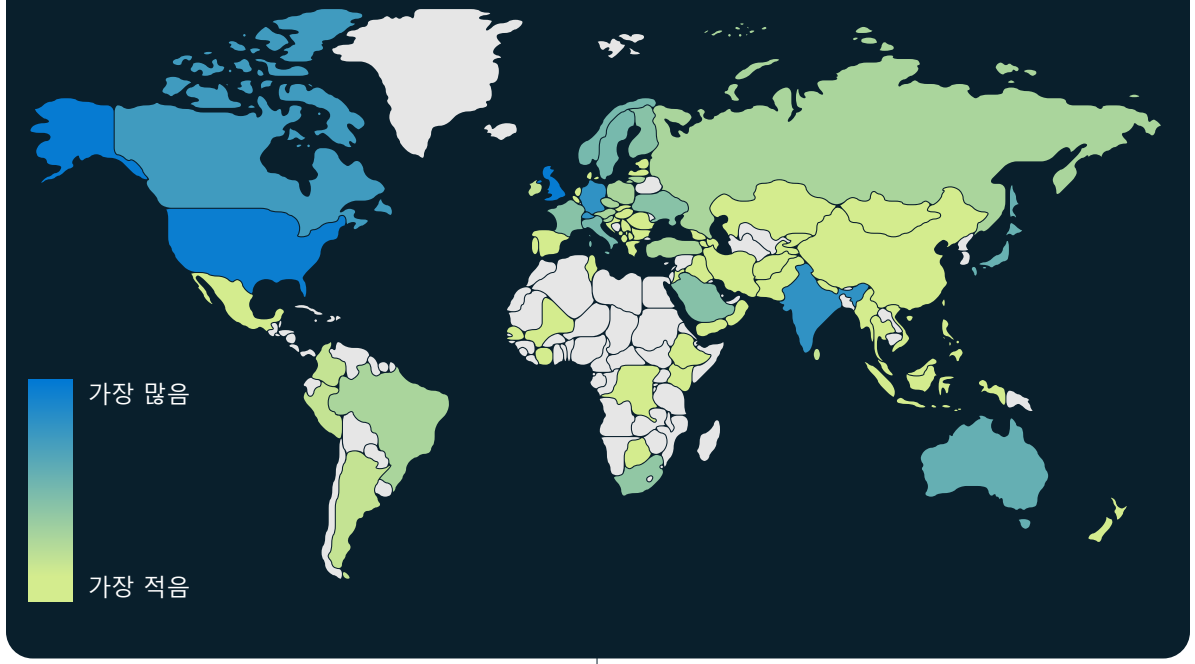


국가 차원 그룹의 주요 인프라 타겟팅[3]은 작년에 증가했으며 공격자들은 IT 부문, 금융 서비스, 운송 시스템, 통신 인프라의 기업에 중점을 두었습니다.

"우크라이나 침공 이전에 정부 기관은 데이터를 보호하기 위해 국가 내에 있어야 한다고 생각했습니다. 침공 후 데이터를 클라우드로 마이그레이션하고 영토 경계 외부로 이동하는 것은 이제 회복탄력성 계획 및 우수한 거버넌스의 일부가 되었습니다."

Cristin Flynn Goodwin,
고객 보안 및 신뢰 부문 준법률 고문

국가 차원 공격자의 지리적 타겟팅



국가 차원 그룹의 사이버 타겟팅은 작년에 전 세계를 표적으로 삼았으며 특히 미국과 영국 기업에 중점을 두었습니다. Microsoft NSN 데이터에 따르면 이스라엘, 아랍에미리트, 캐나다, 독일, 인도, 스위스, 일본의 조직 역시 가장 빈번한 표적 중 하나였습니다.

실행 가능한 인사이트

1. 국가 차원 그룹의 전략적 우선순위와 일치할 수 있는 잠재적인 고부가가치 데이터 대상과 위험에 처한 기술, 정보, 비즈니스 운영을 식별하고 보호합니다.
2. 클라우드 보호를 지원하여 네트워크에 대한 알려진 위협과 새로운 위협을 대규모로 식별하고 완화합니다.

디지털 생태계로 가는 관문으로서의 IT 공급망

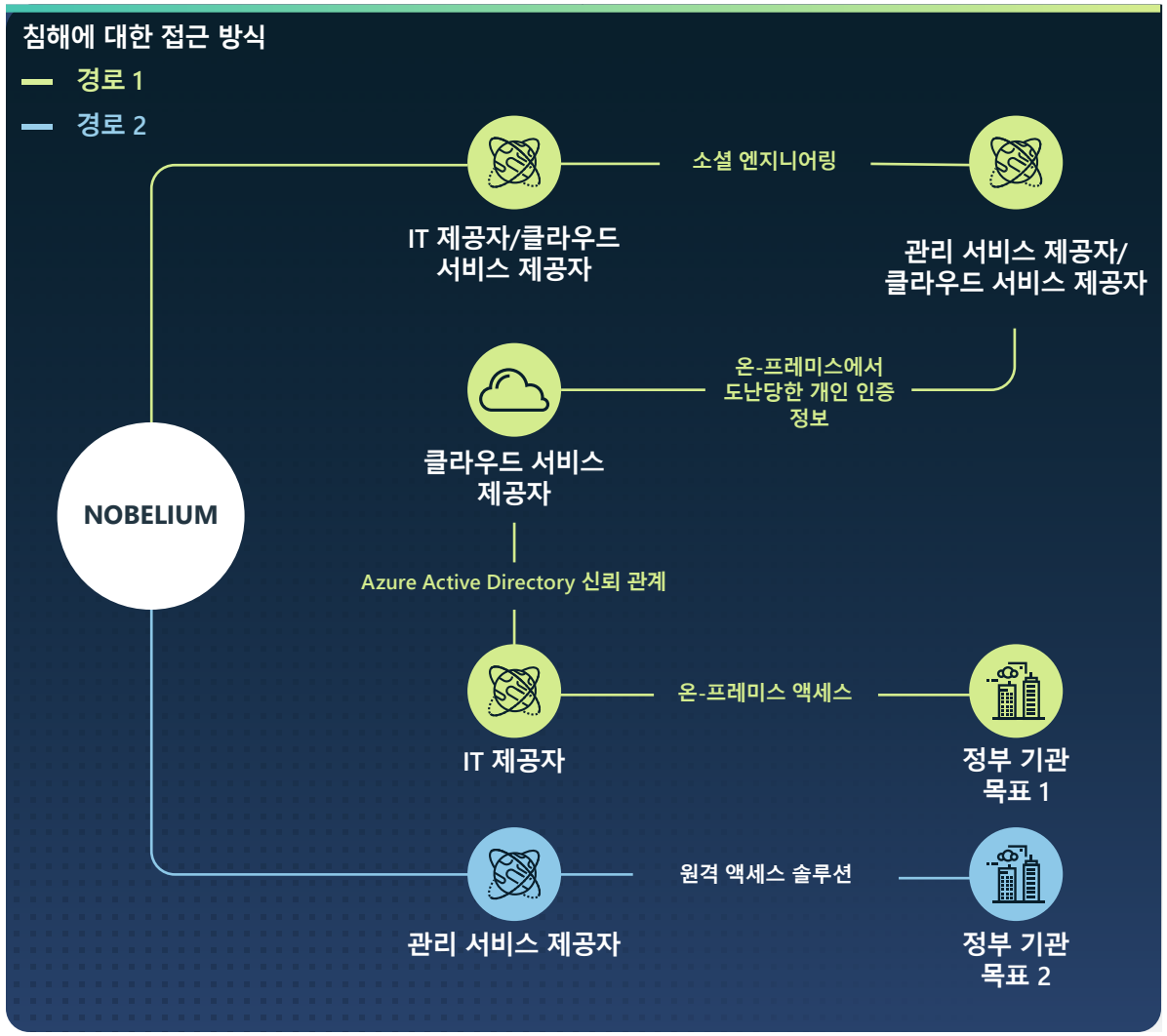
IT 서비스 제공자에 대한 국가 차원의 타겟팅을 통해 위협 행위자들은 이러한 공급망 제공자에게 부여된 신뢰와 액세스를 활용하여 관심 있는 다른 조직을 악용할 수 있습니다. 작년에 국가 차원의 사이버 위협 그룹은 IT 서비스 제공자를 표적으로 삼아 서드파티 대상을 공격하고 정부 기관, 정책, 주요 인프라 부문의 다운스트림 클라이언트에 대한 액세스 권한을 확보했습니다.

IT 서비스 제공자는 외국 정보 서비스에 관심이 있는 수백 명의 직접 고객 및 수천 명의 간접 고객에게 서비스를 제공하기 때문에 매력적인 중개 대상입니다. 이러한 제공자들이 악용될 경우 일상적인 비즈니스 관행과 이러한 회사가 누리는 위임된 관리 권한으로 인해 악의적인 공격자가 즉시 경고를 트리거하지 않고 IT 서비스 제공자 클라이언트 네트워크에 액세스하고 이를 조작할 수 있습니다.

작년에 NOBELIUM은 클라우드 솔루션 및 기타 관리 서비스 제공자의 권한 있는 계정을 침해하고 활용하여 주로 미국과 유럽 정부 기관 및 정책 고객에 대한 대상 다운스트림 액세스를 시도했습니다.

NOBELIUM은 '많은 것을 침해하기 위해 하나를 침해하는' 접근 방식이 인식된 지정학적 공격자에게 어떠한 방식으로 향하는지 보여 주었습니다. 작년에 위협 행위자는 러시아 정부가 실존적 위협으로 인식하는 NATO(북대서양조약기구) 회원국에 기반을 둔 민감한 조직에 대한 제삼자 및 직접 침입을 추구했습니다. 2021년 7월부터 2022년 6월 초까지 온라인 서비스 고객을 표적으로 삼은 러시아 위협 활동에 대한 Microsoft의 고객 알림 중 48%가 중개 액세스 지점으로 NATO 회원국에 기반을 둔 IT 부문 회사에 전달되었습니다. 전반적으로 같은 기간 동안 러시아 위협 활동에 대한 알림 중 90%는 주로 IT, 싱크 탱크, NGO(비정부기구), 정부 기관 부문 내 NATO 회원국에 기반을 둔 고객에게 전달되었습니다. 이는 이러한 대상에 대한 다양한 초기 액세스 수단을 추구하는 전략을 시사합니다.

> 소프트웨어 공급망의 악용에서 IT 서비스 공급망 악용으로 방식이 전환되어 클라우드 솔루션 및 관리 서비스 제공자를 표적으로 하여 다운스트림 고객에게 도달했습니다.



이 다이어그램은 궁극적인 대상과 그 과정에서 다른 희생자에 대한 부수적 피해를 침해하는 NOBELIUM의 다중 벡터 접근 방식을 보여줍니다. 위에서 볼 수 있는 작업 외에도 NOBELIUM은 관련 엔터티에 대해 암호 스프레이 및 피싱 공격을 시작하여 심지어 또 다른 잠재적 침해 경로로 한 명 이상의 공무원 개인 계정을 표적으로 삼았습니다.

디지털 생태계로 가는 관문으로서의 IT 공급망

계속

한 해 동안 MSTIC(Microsoft 위협 인텔리전스 센터)는 IT 회사를 침해하는 이란 국가 및 이란과 연계된 공격자들의 수가 증가하고 있음을 탐지했습니다. 많은 경우 공격자들은 인텔리전스 수집에서 보복적 파괴 공격에 이르기까지 다양한 목표를 위해 다운스트림 클라이언트에 액세스할 수 있도록 로그인 개인 인증 정보를 훔치는 것으로 탐지되었습니다.

- 2021년 7월과 8월에 DEV-0228은 이스라엘 비즈니스 소프트웨어 제공자를 침해하여 이후 이스라엘 국방, 에너지, 법률 부문의 다운스트림 고객을 침해했습니다.[4]
- 2021년 8월부터 9월까지 Microsoft는 인도에 기반을 둔 IT 회사를 표적으로 하는 이란 차원의 공격자들의 급증을 탐지했습니다. 이러한 변화를 촉발할 긴급한 지정학적 문제가 없다는 사실은 이러한 목표가 인도 외부에 있는 자회사 및 고객에 대한 간접적인 접근을 위한 것임을 시사합니다.
- 2022년 1월, 이란 정부 기관과 연계된 것으로 보이는 그룹인 DEV-0198은 이스라엘 클라우드 솔루션 제공자를 침해했습니다. Microsoft는 공격자가 제공자의 침해된 개인 인증 정보를 사용하여 이스라엘 물류 회사에 인증했을 가능성이 있다고 봅니다. MSTIC는 동일한 공격자가 그달 말에 물류 회사를 대상으로 파괴적인 사이버 공격을 시도한 모습을 발견했습니다.
- 2022년 4월, 레바논에 기반을 두고 IT 공급망 기술에 대해 이란 차원의 그룹과 협력한 것으로 보이는 POLONIUM은 다른 이스라엘 IT 회사를 침해하여 이스라엘 국방 및 법률 조직에 액세스했습니다.[5]

지난 한 해 동안의 활동을 통해 NOBELIUM 및 DEV-0228과 같은 위협 행위자가 조직보다 조직의 신뢰할 수 있는 관계 환경을 더 잘 알고 있다는 사실을 알 수 있습니다. 이와 같은 위협의 증가는 조직이 디지털 자산의 경계와 진입점을 이해하고 강화해야 할 필요성을 강조합니다. 또한 IT 서비스 제공자가 자체적으로 사이버 보안 상태를 엄격하게 모니터링하는 것이 중요하다는 사실 역시 강조합니다. 예를 들어, 조직은 악의적인 공격자들이 권한 있는 계정을 캡처하거나 네트워크 전체에 분산하는 것을 어렵게 만드는 다중 인증 및 조건부 액세스 정책을 구현해야 합니다.

파트너 관계를 철저히 검토하고 감사하면 조직과 업스트림 제공자 간의 불필요한 권한을 최소화하고 친숙하지 않은 관계에 대한 액세스 권한을 즉시 제거할 수 있습니다. 활동 로그에 익숙해지고 사용 가능한 활동을 검토하면 추가 조사를 촉발할 수 있는 변칙을 더 쉽게 발견할 수 있습니다.

> 제삼자를 표적으로 하는 국가 차원의 공격자들은 공급망에서 신뢰와 액세스를 활용하여 민감한 조직을 악용할 수 있습니다.

실행 가능한 인사이트

1. 업스트림 및 다운스트림 서비스 제공자 관계와 위임된 권한 액세스를 검토하고 감사하여 불필요한 권한을 최소화합니다. 친숙하지 않거나 아직 감사되지 않은 파트너 관계에 대한 액세스 권한을 제거합니다.[6]
2. 로깅을 사용하도록 설정하고 단일 요소 인증으로 환경 설정된 계정을 중심으로 원격 액세스 인프라 및 VPN(가상 사설망)에 대한 모든 인증 작업을 검토하여 신뢰성을 확인하고 비정상적인 활동을 조사합니다.
3. 모든 계정(서비스 계정 포함)에 대해 MFA를 지원하고 모든 원격 연결에 MFA가 적용되는지 확인합니다.
4. 비밀번호 없는 솔루션을 사용하여 계정을 보호합니다.[7]

추가 정보에 대한 링크

- 광범위한 공격을 용이하게 하기 위해 위임된 관리 권한을 표적으로 하는 NOBELIUM | MSTIC(Microsoft 위협 인텔리전스 센터)
- 성장하는 IT 부문을 타겟으로 한 이란 | MSTIC(Microsoft 위협 인텔리전스 센터), Microsoft DCU(디지털 범죄 부서)
- 이스라엘 조직을 표적으로 삼은 POLONIUM 활동 및 인프라 노출 | MSTIC(Microsoft 위협 인텔리전스 센터)

신속한 취약점 악용

조직이 사이버 보안 태세를 강화함에 따라 국가 차원의 공격자들은 공격을 제공하고 탐지를 피하기 위해 고유한 신규 전술을 추구하여 대응합니다. 이전에 알려지지 않은 취약점(제로 데이 취약점으로 알려짐)을 식별하고 악용하는 것이 이러한 노력의 핵심 전술입니다.

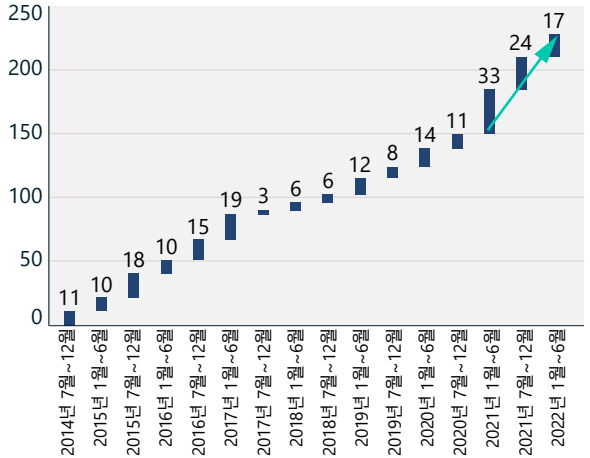
제로 데이 취약점은 초기 악용에 특히 효과적인 수단이며, 일단 공개적으로 노출되면 취약점은 다른 국가 차원의 공격자 및 범죄 공격자에 의해 신속하게 재사용될 수 있습니다. 지난 한 해 동안 공개된 제로데이 취약점의 수는 전년도와 비슷하며 사상 최고치를 기록했습니다.

사이버 위협 행위자(국가 및 범죄자 모두)가 이러한 취약점을 활용하는 데 더 능숙해짐에 따라 취약점 발표와 해당 취약점이 상품화되는 기간이 단축된다는 사실을 발견했습니다. 따라서 조직은 악용을 즉시 패치해야 합니다. 마찬가지로, 새로운 취약점을 발견한 조직이나 개인은 조정된 취약점 공개 절차에 따라 가능한 한 빨리 영향을 받는 제공자에 책임감 있게 공개하거나 보고하는 것이 중요합니다.

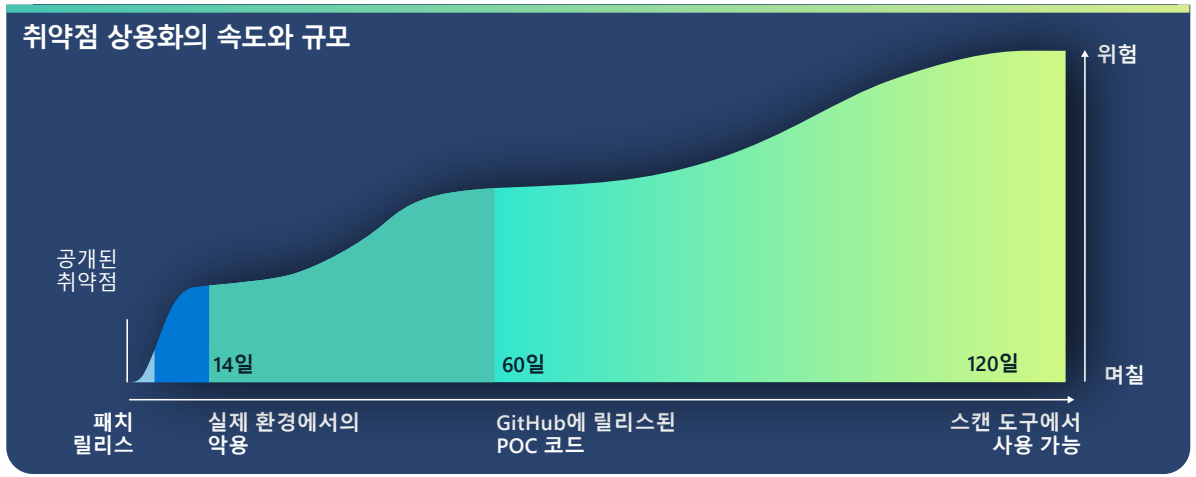
이를 통해 취약점을 식별하고 패치를 적시에 개발하여 이전에 알려지지 않은 위협으로부터 고객을 보호할 수 있습니다.

수많은 조직은 취약점 관리가 네트워크 보안에 필수적인 경우 제로 데이 악용 공격의 피해자가 될 가능성이 적다고 가정합니다. 하지만, 악용의 상품화로 인해 이러한 공격은 훨씬 더 빠른 속도로 이루어지고 있습니다. 제로 데이 악용은 다른 공격자에 의해 발견되고 단기간에 광범위하게 재사용되어 패치되지 않은 시스템을 위험에 빠뜨리는 경우가 많습니다. 제로 데이 악용은 탐지하기 어려울 수 있지만 공격자의 악용 후 작업은 탐지하기가 더 쉬운 경우가 많으며, 완전히 패치된 소프트웨어에서 발생하는 경우 침해에 대한 경고 신호로 작용할 수 있습니다.

제로 데이 취약점에 대해 릴리스된 패치



CVE(Common Vulnerabilities and Disclosures, 일반적인 취약점 및 공개) 목록에서 공개적으로 공개된 제로 데이 악용의 수입니다.



평균적으로 취약점이 공개된 후 실제 환경에서 사용할 수 있기까지는 14일밖에 걸리지 않습니다. 이러한 새로운 관점은 제로 데이 취약점을 악용하는 타임라인과 함께 지정된 악용에 취약하고 처음 공개된 시점부터 인터넷에서 활성화된 시스템 수에 대한 분석을 제공합니다.

제로 데이 취약점 공격은 처음에는 제한된 조직을 표적으로 하는 경향이 있지만 더 큰 위협 행위자 생태계에 빠르게 채택됩니다. 이로 인해 위협 행위자들이 잠재적인 대상이 패치를 설치하기 전에 가능한 한 광범위하게 취약점을 악용하기 위한 경쟁을 시작합니다.

다양한 국가 차원의 공격자들이 알려지지 않은 취약점에서 악용을 개발하는 사실을 발견하지만 중국에 기반을 둔 국가 차원의 위협 행위자들은 특히 제로 데이 악용을 발견하고 개발하는 데 능숙합니다. 중국의 취약점 보고 규정은 2021년 9월에 발효되어 세계 최초로 정부 기관이 취약점을 제품 또는 서비스 담당자와 공유하기 전에 정부 기관에 보고하도록 했습니다. 이처럼 새로운 규정은 중국 정부 기관이 무기화와 관련된 취약점 보고 내용을 구축할 수 있도록 할 수 있습니다. 작년에 중국에 기반을 둔 공격자들 간의 제로 데이 사용이 증가한 사실은 중국 보안 커뮤니티에 대한 중국의 취약점 공개를 요구한 첫해라는 사실과 제로 데이 악용을 국가 우선순위로 사용하는 주요 단계를 반영하는 것 같습니다. 아래에 설명된 취약점은 더 큰 위협 생태계의 다른 공격자들 사이에서 발견되어 확산되기 전 중국에 기반을 둔 국가 차원의 공격자들에 의해 처음 개발 및 배포된 취약점입니다.

신속한 취약점 악용

계속

심지어 국가 차원의 위협 행위자들의 공격 대상이 아닌 조직조차 취약점이 더 광범위한 공격자 생태계에 의해 악용되기 전 영향을 받는 시스템에서 제로 데이 취약점을 패치할 수 있는 기간이 제한되어 있습니다.

이와 같이 새로 식별된 취약점에 대한 예는 조직에서 취약점이 패치되고 PoC(개념 증명) 코드가 온라인으로 제공되기까지 평균 60일이 소요되며 다른 공격자들이 재사용했다는 사실을 보여줍니다. 이와 마찬가지로, 조직은 Metasploit과 같은 자동화된 취약점 검사 및 악용 도구에서 취약점을 사용할 수 있기까지 평균 120일이 소요되는데, 이로 인해 대규모로 악용되는 경우가 많습니다. 이는 국가 차원의 위협 행위자들의 대상이 아닌 조직조차 취약점이 더 광범위한 공격자 생태계에 의해 악용되기 전 영향을 받는 시스템에서 제로 데이 취약점을 패치할 수 있는 기간이 제한되어 있다는 사실을 강조합니다.

CVE-2021-35211 SolarWinds Serv-U

2021년 7월, SolarWinds는 CVE-2021-35211에 대한 보안 권고를 발표하여 Microsoft에 알림을 제공했습니다.[8] 당시 Microsoft는 국가 차원의 위협 행위자 DEV-0322가 SolarWinds Serv-U 취약점을 적극적으로 악용하고 있다는 사실을 발견했습니다. Microsoft의 RiskIQ 팀은 6월 15일~7월 9일에 영향을 받은 디바이스의 인터넷 연결 버전을 호스팅하는 12,646개의 IP 주소를 발견했습니다.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

2021년 9월, Microsoft 연구원들은 중국과 연계된 공격자들이 여러 미국 기반 기업에서 Zoho ManageEngine을 악용하는 사실을 발견했습니다. 이 취약점은 9월 6일 CVE-2021-40539 Zoho ManageEngine ADSelfService Plus로 공개적으로 보고되었으며, 이 조직은 일반적으로 암호 재설정을 처리하는 데 사용합니다.[9] 9월 말에 DEV-0322는 이 취약점을 악용하여 네트워크에서 발판을 마련하기 위한 초기 벡터로 사용하고 개인 인증 정보 덤핑, 사용자 맞춤형 바이너리 설치, 지속성 유지를 위한 맬웨어 삭제 등의 추가 작업을 수행했습니다. 공개 당시 RiskIQ는 이러한 시스템의 4,011개 인스턴스가 인터넷에 활성화되어 있었습니다.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

2021년 10월 말, Microsoft는 자산 관리 기능이 있는 IT 헬프 데스크 소프트웨어인 두 번째 Zoho ManageEngine 제품 ServiceDesk Plus에서 취약점(CVE-2021-44077)을 활용하는 DEV-0322를 발견했습니다. DEV-0322는 이 취약점을 사용하여 의료, 정보 기술, 대학 교육, 중요한 제조 부문의 엔터티를 표적으로 삼고 침해했습니다. 12월 2일, FBI(미국 연방수사국)와 CISA(Cybersecurity and Infrastructure Security Agency, 사이버 보안 및 인프라 보안국)는 대중을 표적으로 삼고 이 취약점을 악용하는 국가 차원의 공격자들에 대한 공동 주의보를 발표했습니다. 공개 당시 RiskIQ는 이러한 시스템의 7,956개 인스턴스가 인터넷에 활성화되어 있었습니다.

CVE-2021-42321 Microsoft Exchange

Exchange 취약점 CVE-2021-42321에 대한 제로 데이 악용은 중국 청두에서 2021년 10월 16일~17일에 개최된 국제 사이버 보안 정상 회담 및 해킹 대회인 Tianfu Cup에서 공개되었습니다. Microsoft의 보안 연구원들은 취약점이 밝혀진 지 불과 3일 후인 10월 21일에 실제로 Exchange 취약점이 악용되었다는 사실을 발견했습니다. 공개 당시 RiskIQ는 이러한 시스템의 61,559개 인스턴스가 인터넷에 활성화되어 있었습니다. Microsoft는 2021년 11월까지 계속해서 악용 활동에 대해 관찰했습니다.

CVE-2022-26134 Confluence

중국과 연계된 한 공격자는 6월 2일 취약점이 공개되기 4일 전에 Confluence 취약점(CVE-2022-26134)에 대한 제로 데이 악용 코드를 가지고 있었을 가능성이 있으며 미국 기반 엔터티를 표적으로 삼아 이를 활용했을 가능성이 있습니다. 공개 당시 RiskIQ는 취약점 Confluence 시스템의 53,621개 인스턴스가 인터넷에 활성화되어 있었습니다.

취약점은 점점 더 짧은 시간 내에 대규모로 발견되어 악용되고 있습니다.

실행 가능한 인사이트

1. 제로 데이 취약점이 릴리스되는 즉각적인 패치의 우선순위를 지정합니다. 패치 관리 주기가 배포될 때까지 기다리지 마세요.
2. 모든 엔터프라이즈급 하드웨어 및 소프트웨어 자산을 문서화하고 인벤토리화하여 위험을 파악하고 패치에 대한 조치를 신속하게 결정합니다.

전시 사이버 전술을 통해 우크라이나와 그 이상을 위협하는 러시아 차원의 공격자들

올해 러시아 차원의 공격자들은 러시아의 우크라이나 침공 중 군사 행동을 보완하기 위해 사이버 작전을 시작했으며, 우크라이나 외부 대상을 목표로 배치된 것과 동일한 전술과 기술을 사용했습니다. 전 세계 조직이 러시아와 연계된 위협 행위자들로부터 비롯된 디지털 위협에 대해 사이버 보안을 강화하기 위한 조치를 취하는 것이 중요합니다.

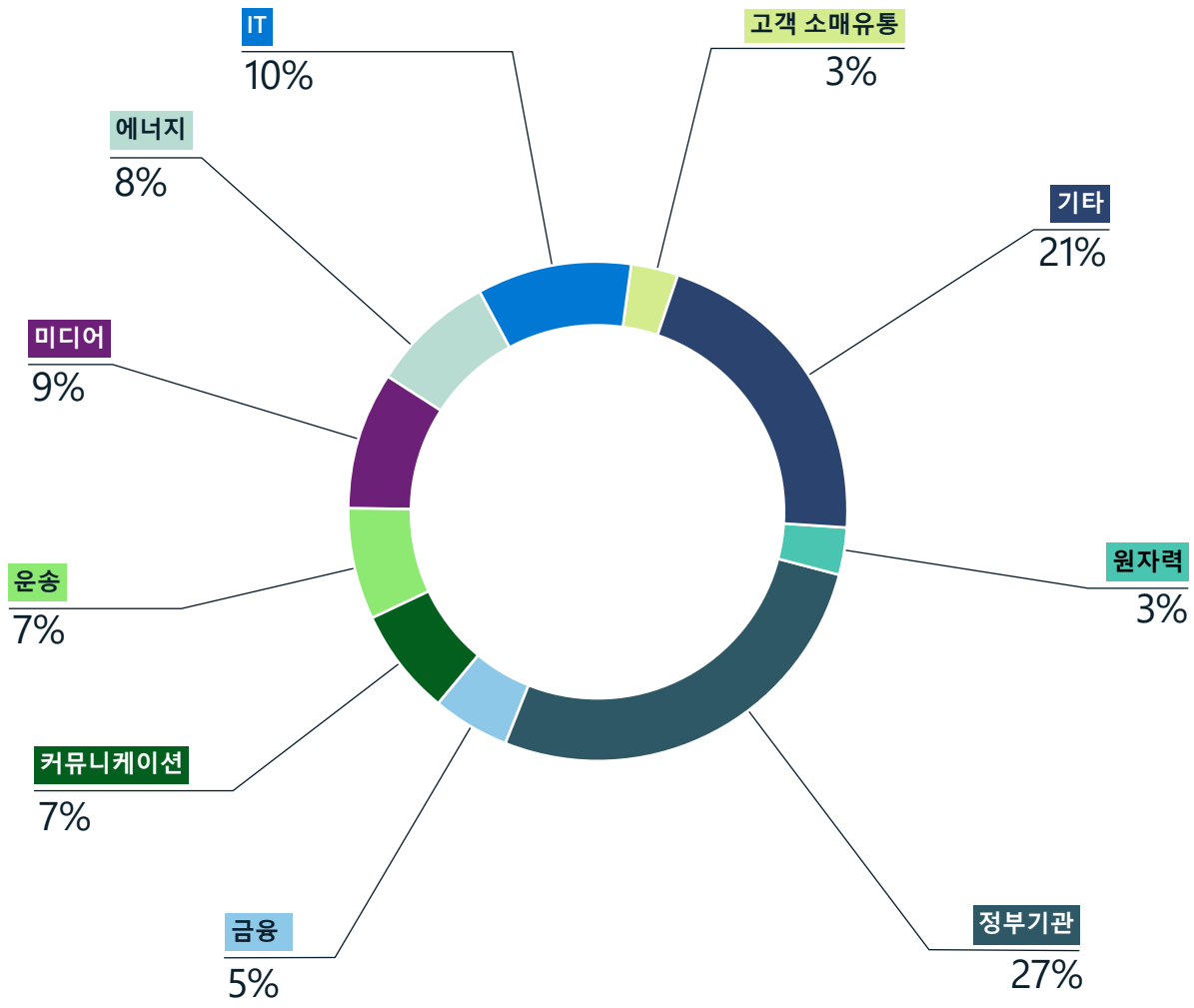
군사 분쟁이 지속됨에 따라 지상의 상황은 계속 변동하고 있으며 러시아 차원의 사이버 공격자들이 군사 목표에 따라 침공 빈도 또는 강도를 높이면 우크라이나와 동맹국은 스스로를 방어할 준비가 되어 있어야 합니다. 전쟁이 시작된 지 4개월 동안 Microsoft는 러시아 군대와 관련된 위협 행위자들이 거의 50개의 우크라이나 기관 및 기업에 대해 여러 차례 파괴적인 사이버 공격을 시작하고 다른 많은 기관에 대해 스파이 중심의 침공을 시작한다는 사실을 발견했습니다. 온라인 서비스 고객에 대한 작전을 제외하고 알려진 표적에 대한 러시아 위협 활동 중 64%는 2월 말부터 6월까지 우크라이나 기반 조직을 표적으로 삼았습니다.

각 작전에서 러시아 위협 행위자들은 우크라이나 안팎의 목표물에 대한 침공 전에 사용되는 것으로 발견된 많은 TTP(전술, 기술, 절차)를 사용했습니다. 이러한 공격자들은 분쟁 초기에 데이터를 파괴하고 우크라이나 정부 기관의 균형을 무너뜨리려고 했습니다. 이후 이들은 우크라이나에 대한 군사 및 인도 주의적 지원의 수송을 방해하고, 서비스 및 언론에 대한 대중의 접근을 방해하며, 러시아를 위해 장기 정보 또는 경제적 가치가 있는 정보를 훔치려고 노력했습니다.

교통수단을 목표로 삼는 것은 분쟁에서 살아남으려는 우크라이나 시민들에게 매우 중요한 영역을 위협하는 것입니다. 지난 5월 유니세프에서 진행한 한 설문조사에 따르면 분쟁 피해 도시 지역의 응답자들은 운송 및 연료, 공급 중단, 보안, 식량, 의료 서비스 및 금융 서비스에 대한 제한적인 접근에 대해 가장 우려하고 있었습니다.[10] 6월에 우크라이나의 유엔 위기 조정관은 우크라이나에서 최소 1,570만 명이 인도적 지원이 시급히 필요하며 전쟁이 계속됨에 따라 그 수는 증가할 것이라고 말했습니다.[11]

우크라이나 이외의 지역에서 Microsoft는 2월 말에서 6월까지 42개국의 128개 조직을 표적으로 삼은 러시아 네트워크의 침입 노력을 탐지했습니다. 미국은 러시아의 제1의 표적이었습니다. 우크라이나에 대한 국제 군사 및 인도 주의적 지원의 대부분이 통과하는 폴란드 역시 이 기간 동안 중요한 목표였습니다. 러시아 국가와 연계된 위협 행위자들은 4월과 5월에도 발트해 연안 국가의 조직과 덴마크, 노르웨이, 핀란드, 스웨덴의 컴퓨터 네트워크를 추적했습니다.

침공 이후 우크라이나에서 가장 표적이 된 산업 부문



우크라이나의 연방, 주, 지방 정부 조직은 분쟁 기간 동안 러시아 국가 및 주와 연계된 위협 그룹의 최우선 목표였습니다. 운송, 에너지, 금융, 언론 부문 조직에 대한 초점은 이러한 사이버 작전이 우크라이나 시민이 의존하는 서비스에 미치는 위험을 강조합니다.

전시 사이버 전술을 통해 우크라이나와 그 이상을 위협하는 러시아 차원의 공격자들

계속

NATO 국가의 외교부를 표적으로 삼은 유사한 활동이 증가했습니다.

러시아 차원의 위협 그룹은 작년 한 해 동안 계속해서 우크라이나 안팎의 중요한 기반 시설을 침해하는 데 관심을 보였습니다. IRIDIUM은 Industroyer2 맬웨어를 배포했지만 수백만 명의 우크라이나 사람들의 전력을 빼앗는 데 실패했습니다. 우크라이나 외부에서 BROMINE은 2022년 초에 제조 및 산업 제어 시스템과 관련된 조직에 침입했습니다.

러시아 차원의 공격자들 및 러시아와 연계된 공격자들은 다음 TTP 중 다수의 TTP를 사용하여 올해 우크라이나, 동맹국, 기타 가치 있는 정보를 표적으로 삼은 사이버 작전을 지시했습니다.

악성 첨부 파일 또는 링크를 사용한 스피어 피싱

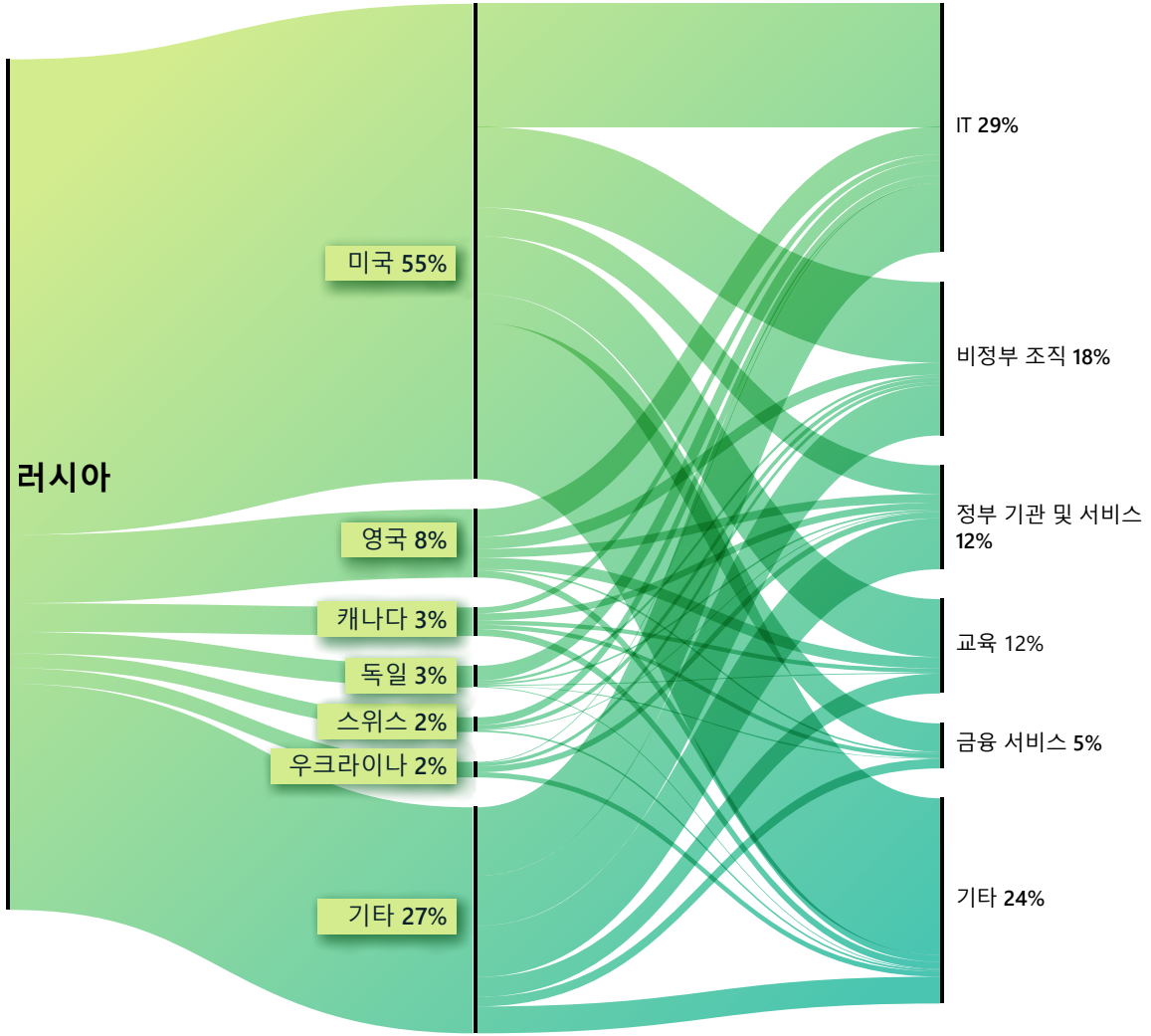
ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM, IRIDIUM과 같은 러시아 차원의 그룹 및 러시아와 연계된 그룹 모두 피싱 캠페인을 사용하여 우크라이나 내외의 조직에서 원하는 계정 및 네트워크에 대한 초기 액세스 권한을 확보했습니다. 수많은 캠페인이 대상 조직 또는 동종 업계 내 도용되거나 스푸핑된 계정을 활용했으며 피해자를 유인하기 위해 매력적인 주제를 사용했습니다. NOBELIUM은 침해된 외교 관련 계정을 사용하여 외교 관련 통신으로 위장한 피싱 이메일을 전 세계 외교부 직원에게 보냈습니다. STRONTIUM은 미국 싱크 탱크의 계정 담당자 이름을 기반으로 스푸핑 계정을 생성하고 해당 싱크 탱크의 계정에 대한 액세스 권한을 얻기 위해 피싱 메시지를 보냈습니다. SEABORGIUM은 북유럽 국가의 국제 문제 관련 싱크 탱크의 계정에 대한 초기 액세스 권한을 얻기 위해 우크라이나 분쟁에 대한 보고와 관련된 미끼를 사용하여 피싱했습니다.

IT 서비스 공급망을 활용하여 다운스트림 고객에게 영향

2021년 말, 러시아 차원의 공격자들은 IT 서비스 제공자를 침해하고 이 액세스를 사용하여 1월 DEV-0586 웹 사이트 변조 및 파괴적인 Whispergate 맬웨어 배포를 손쉽게 했습니다.[12] 또한 DEV-0586은 우크라이나 국방부와 통신 및 운송 부문의 기타 조직을 위한 자원 관리 시스템을 구축한 IT 회사의 네트워크를 침해하였는데, 이는 공격 그룹이 해당 부문에서도 제삼자 공격 옵션을 모색하고 있다는 사실을 나타냅니다.

전 세계적으로, 특히 미국과 서유럽에서 NOBELIUM은 2021~2022년 내내 정부 기관 및 기타 민감한 네트워크에 대한 액세스 권한을 얻을 수 있도록 IT 서비스 제공자를 표적으로 삼았습니다(이 장 앞부분의 공급망 취약점에 대한 논의 참조).

러시아: 상위 표적 국가 및 산업 부문



2022년 초부터 우크라이나 기반 조직에 대해 관심을 집중했음에도 불구하고 북미와 서유럽에 기반을 둔 기업은 여전히 러시아 공격자들이 가장 많이 목표로 삼은 온라인 서비스 고객이었습니다. IT 부문에 대한 NOBELIUM의 캠페인은 작년에 가장 많이 표적이 된 부문이 되었습니다.

전시 사이버 전술을 통해 우크라이나와 그 이상을 위협하는 러시아 차원의 공격자들

계속

네트워크에 대한 초기 액세스 권한을 얻기 위해 퍼블릭 애플리케이션 악용

최소 2021년 말부터 STRONTIUM은 Microsoft Exchange 서버와 같은 공용 서비스를 악용하여 정보를 훔치는 기능을 개발하고 강화하기 위해 노력했습니다. STRONTIUM은 패치되지 않은 Exchange 서버를 악용하여 우크라이나 정부 기관 계정은 물론 미국, 레바논, 페루, 루마니아의 군사 및 국방 산업 관련 조직과 아르메니아, 보스니아, 코소보, 말레이시아에 기반을 둔 기타 정부 기관에 액세스했습니다. 러시아 군대와 연계되기도 한 DEV-0586은 Confluence 서버 취약점을 악용하여 우크라이나 및 기타 동유럽 국가의 정부 기관 및 IT 부문 조직에 대한 초기 액세스 권한을 얻었습니다.

러시아 차원의 공격자들 및 연계된 위협 행위자들은 전쟁과 평화의 시기에 관심 있는 조직을 침해시키기 위해 동일한 TTP를 많이 사용합니다.

관리 계정 및 프로토콜, 네트워크 검색 및 측면 이동을 위한 기본 유틸리티 사용

네트워크에 대한 초기 액세스 권한을 얻은 후 Microsoft는 가능한 한 오랫동안 탐지를 피하도록 기본 유지 관리 작업을 수행하는 데 사용되는 합법적인 계정 및 소프트웨어 유틸리티를 활용하는 러시아 차원의 공격자들을 발견했습니다. 이들은 관리 기능과 유효한 관리 프로토콜, 도구, 방법을 갖춘 침해된 ID에 의존하여 자동화된 모니터와 네트워크 방어자의 관심을 즉시 끌지 않고 네트워크 내에서 측면으로 이동했습니다.

기본적인 사이버 방역과 엔드포인트 탐지 및 대응 도구의 사용은 평시와 전쟁 중에 이러한 작전 유형의 부정적인 영향을 완화하는 데 도움이 될 수 있습니다.

진행 중인 분쟁의 예측 불가능성으로 인해 전 세계 조직은 러시아 차원의 공격자들 및 러시아와 관련된 위협 행위자들로부터 비롯된 디지털 위협을 대상으로 사이버 보안을 강화하기 위한 조치를 취해야 합니다.

실행 가능한 인사이트

1. MFA ID 보호 도구를 구현하고 최소 권한 액세스를 적용하여 가장 중요하고 권한이 있는 계정 및 시스템을 보호하여 사용자의 ID를 보호함으로써 개인 인증 정보 도난 및 계정 남용을 최소화합니다.
2. 업데이트를 적용하여 모든 시스템이 가능한 한 빨리 최고 수준의 보호를 받고 최신 상태로 유지되도록 합니다.
3. 맬웨어 방지, 엔드포인트 탐지, ID 보호 솔루션을 조직 전체에 배포합니다. 숙련되고 유능한 인력과 심층 방어 보안 솔루션을 결합하여 조직이 비즈니스에 영향을 미치는 침입을 식별, 탐지, 방지할 수 있도록 지원합니다.
4. 중요한 시스템을 백업하고 로깅을 지원하여 환경에 대한 위협을 탐지하거나 알림을 받는 경우 조사 및 복구를 사용하도록 합니다. 인시던트 대응 계획을 수립하는 것이 좋습니다.

추가 정보에 대한 링크

- 우크라이나 방어: 사이버 전쟁 초기의 교훈 | 문제에 대응하는 Microsoft
- 우크라이나의 하이브리드 전쟁 | 문제에 대응하는 Microsoft
- 우크라이나의 사이버 위협 활동: 분석 및 리소스 | MSRC(Microsoft Security Response Center, Microsoft 보안 대응 센터)
- 우크라이나를 겨냥한 사이버 공격 중단 | 문제에 대응하는 Microsoft
- 우크라이나 정부 기관을 표적으로 삼은 맬웨어 공격 | 문제에 대응하는 Microsoft
- MagicWeb: 누구나 인증할 수 있는 NOBELIUM의 침해 후 속임수 | MSTIC(Microsoft 위협 인텔리전스 센터), DART(Detection and Response Team, 탐지대응팀), Microsoft 365 Defender 연구 팀

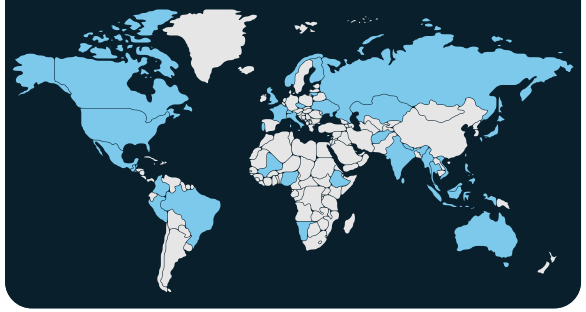
경쟁 우위를 위한 글로벌 타겟팅을 확대하는 중국

오늘날 복잡성 높은 지정학적 환경에서 사이버 작전을 수행하는 중국 국가 차원의 공격자들 및 중국과 연계된 위협 행위자들은 경쟁 우위를 확보하기 위한 목표의 일환으로 중국의 전략적 군사, 경제, 외교 목표를 달성하는 것을 목표로 하는 경우가 많습니다. 작년에 Microsoft는 전 세계 국가를 표적으로 하는 중국의 광범위한 위협 활동을 발견했습니다.

2021년 중반부터 중국은 2년 만에 최악의 코로나19 급증세를 보인 가운데, 경제 및 금융 안정성을 보장하기 위해 노력하고 있습니다.[13] 중국은 러시아와의 '무한한' 파트너십 간 균형 유지 등과 같은 지정학적 사건에 대한 자신의 입장을 교묘하게 표명하고 [14] 세계 무대에서 자신의 입지를 유지하기 위해 계속해서 노력해왔습니다.[15] 또한 대만[16]과 남중국해에 대한 미국과 미국의 동맹국들에 향한 중국의 입장은 수많은 국가와의 외교 관계에 긴장감을 계속해서 불어넣었습니다.[17]

중국 국가 차원의 위협 그룹 및 중국과 연계된 위협 그룹은 모든 면에서 경쟁 우위를 확보하기 위해 동남아시아를 중심으로 전 세계에서 더 많은 소규모 국가를 표적으로 삼았습니다.

중국 국가 차원의 공격자 및 중국과 연계된 단체의 표적이 된 국가

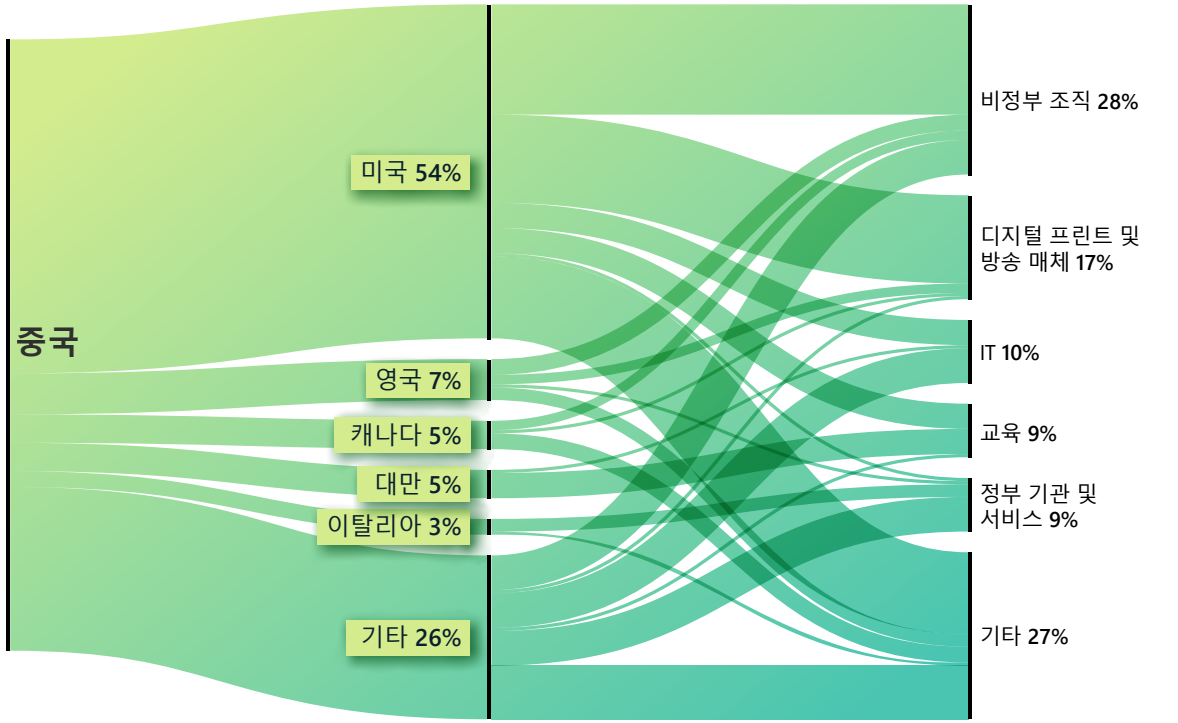


중국은 또한 이전에 구축한 BRI(Belt and Road Initiatives, 일대일로 이니셔티브)를 통해 전 세계에 경제적인 영향력을 계속해서 확대하고, EU와의 포괄적인 투자 프레임워크를 되살리려고 시도하고,[18] 아시아 태평양 지역의 15개국과 역내 포괄적 경제동반자협정으로 알려진 새로운 지역 무역 협정을 협상했습니다.[19] Microsoft에서는 중국이 관측된 사이버 작전과 표적이 되는 광범위한 엔터티로 인해 전략적인 정치적, 군사적, 경제적 목표를 달성하는 데 도움이 되는 도구로 사이버 수집을 계속 활용할 것이라고 평가합니다.

경제적 및 군사적 수익을 증진시킬 가능성이 있는 사이버 표적

Microsoft는 중국 국가 차원의 위협 그룹 및 중국과 연계된 위협 그룹이 전 세계 소규모 국가를 광범위하게 표적으로 삼고 있다는 사실을 발견했으며, 이는 중국이 사이버 스파이 활동을 국제 경제 및 군사 영향력의 구성 요소로 사용하고 있음을 시사합니다.

중국: 상위 표적 국가 및 산업 부문



싱크 탱크/NGO, 언론, IT, 정부 기관, 교육 부문은 아마도 지속적인 정보 수집 및 정찰을 위해 중국에 기반을 둔 위협 그룹의 가장 많은 표적이 된 분야 중 하나였습니다.

표적으로는 아프리카, 카리브해, 중동, 오세아니아, 남아시아 국가가 포함되지만 이에 국한되지 않으며 특히 동남아시아 및 태평양 제도 국가에 중점을 둡니다.

중국의 BRI 전략에 따라 중국에 기반을 둔 위협 그룹은 아프가니스탄, 카자흐스탄, 모리셔스, 나미비아, 트리니다드 토바고의 기업을 표적으로 삼았습니다.[20] 예를 들어, 트리니다드 토바고는 2018년에 중국의 BRI 전략을 지지한 최초의 카리브해 국가였으며 중국은 트리니다드 토바고를 해당 지역의 중요한 파트너로 간주합니다. NICKEL은 2021년부터 트리니다드 토바고를 표적으로 삼고 네트워크 작전을 지속해왔습니다. 예를 들어, 2022년 3월 NICKEL은 정보 수집 목적으로 정부 기관을 대상으로 정찰 활동을 수행했습니다.

경쟁 우위를 위한 글로벌 타겟팅을 확대하는 중국

계속

한편 Microsoft는 중국이 이 지역에 대한 미국의 새로운 관심에 대처하기 위해 군사 및 경제적 우선순위를 전환함에 따라 중국 국가 차원의 위협 그룹 및 중국과 연계된 위협 그룹이 동남아시아 기업에 대한 네트워크 작전에 집중하고 태평양 섬 국가로 확장하는 것을 발견했습니다. 2022년 1월, Microsoft는 RADIUM이 베트남의 에너지 회사 및 에너지 관련 정부 기관과 인도네시아 정부 기관을 표적으로 삼는다는 사실을 발견했습니다. RADIUM의 활동은 남중국해 내 중국의 전략적 목표와 일치할 가능성이 높습니다.[21] 2월 말과 3월 초에 GALLIUM은 동남아시아 지역의 저명한 IGO(정부간기구)와 100개 이상의 관련 계정을 침해했습니다. GALLIUM이 이 지역에서 IGO를 목표로 하는 시기는 미국과 지역 지도자들 간의 예정된 회담의 발표와 일치했습니다. GALLIUM 공격자들은 이벤트 전에 통신을 모니터링하고 정보를 수집하는 임무를 맡았을 것입니다.

중국이 태평양 섬 국가에서 영향력을 확대함에 따라 중국 위협 단체의 활동이 뒤따랐습니다. 4월에 중국과 솔로몬제도는 '평화와 안보를 증진'하기 위한 안보 협정에 서명했습니다. 이 협정은 잠재적으로 중국이 솔로몬 제도에 무장 경찰과 군대를 배치할 수 있도록 허용합니다.[22] 5월에 중국은 피지에서 제2차 중국 및 PIC(태평양 지역 도서 국가) 간의 외교부 장관 회의를 주최하고 정치, 문화, 사회, 안보, 기후 변화 수익을 증진하고 팬데믹과 싸우기 위해 '포괄적인 전략적 파트너십'을 발전시킬 것을 제안했습니다.[23]

5월 같은 시기에 Microsoft는 솔로몬제도 정부 기관 시스템에서 GADOLINIUM의 맬웨어를 발견했습니다. RADIUM은 또한 파푸아뉴기니의 한 통신 회사 시스템에서 악성 코드를 실행했습니다. Microsoft에서는 이러한 활동이 중국의 전반적인 지역 전략을 지원하기 위한 정보 수집을 목적으로 할 가능성이 있다고 평가합니다.

Microsoft는 NICKEL의 작전을 중단하지만 위협 그룹은 지속성을 보입니다.

2021년 12월, Microsoft DCU(디지털 범죄 부서)는 NICKEL에서 제어하는 42개의 C2(지휘 및 통제) 도메인을 압수할 수 있는 권한을 요청하는 탄원서를 버지니아 동부 지방 법원에 제출했습니다. 이러한 C2 도메인은 2019년 9월부터 중남미, 카리브해, 유럽, 북미 전역의 정부 기관, 외교 기관, NGO를 표적으로 삼은 작전에 사용되었습니다.[24] 이러한 작전을 통해 NICKEL은 여러 기관에 장시간 액세스할 수 있었고 2019년 말부터 일부 피해자의 데이터를 지속적으로 유출했습니다.

중국이 더 많은 국가와 양자 경제 관계를 지속적으로 구축함에 따라(BRI와 관련된 협정으로 구축하는 경우가 많음) 전 세계에 미치는 중국의 영향력은 계속해서 커질 것입니다. Microsoft에서는 중국 국가 차원의 공격자들 및 중국과 연계된 위협 행위자들이 경제 스파이 활동이나 전통적인 정보 수집을 목표로 새로운 인사이트를 확보하기 위해 정부 기관, 외교, NGO 부문을 표적할 것이라고 평가합니다. Microsoft에서 중단한 이후 NICKEL은 잃어버린 액세스 권한을 되찾기 위해 여러 정부 기관을 표적으로 삼았습니다. 2022년 3월 말에서 5월 사이에 NICKEL은 전 세계에서 최소 5개의 정부 기관을 다시 침해했습니다. 이는 NICKEL에 해당 엔터티에 대한 추가 진입점이 있거나 새 C2 도메인을 통해 액세스 권한을 다시 얻었다는 사실을 나타냅니다. 전 세계적으로 동일한 정부 기관을 반복적으로 침해하는 NICKEL의 끈기는 높은 수준에서의 작업의 중요성을 보여줍니다.

중국은 외교 정책에 대해 더욱 적극적인 입장을 취하고 있습니다. Microsoft는 계속해서 사이버 기반 경제 스파이 활동을 평가하고 정보를 수집할 것입니다.

실행 가능한 인사이트

1. 사이버 방어를 강화하여 사이버 위협을 사전에 완화합니다. 중국 위협 행위자들의 지속성에 따라 조직은 가능한 침입을 적시에 식별, 보호, 탐지하고 이에 대응해야 합니다.
2. 위협 행위자들은 예약된 작업[25]을 지속성 및 방어 회피의 일반적인 방법으로 남용하기 때문에 조직 환경에서 추가 보안 지침을 사용하여 일반적으로 사용되는 이러한 기술로부터 보호해야 합니다.[26]
3. Microsoft는 웹 셸을 타겟 네트워크에 대한 초기 벡터로 사용하는 행태를 계속해서 관찰합니다.[27] 조직은 공격자들에게 원격 명령을 실행할 수 있는 액세스 권한을 제공할 수 있는 웹 셸 공격에 대한 시스템을 강화해야 합니다.[28]

추가 정보에 대한 링크

- 라틴 아메리카 및 유럽 전역의 정부 기관을 표적으로 하는 NICKEL | MSTIC(Microsoft 위협 인텔리전스 센터), Microsoft DSU(Digital Security Unit, 디지털 보안부)
- 최근 사이버 공격으로부터 사용자 보호 | 문제에 대응하는 Microsoft

권력 이양 후 점점 더 공격적으로 성장하고 있는 이란

Microsoft는 이란 차원의 그룹 및 이란과 연계된 공격자들이 이스라엘에 대한 사이버 공격의 속도와 범위를 늘리고, 랜섬웨어 공격 대상을 지역 내 적을 넘어 미국 및 EU로 확대하고, 세간의 이목을 끄는 미국의 주요 인프라를 표적으로 삼아 적어도 잠재적인 파괴적인 사이버 공격에 대한 사전 위치를 확보한다는 사실을 발견했습니다.

이란 차원의 공격자들의 사이버 공격이 성장함에 따라 대통령의 권력이 이양되었습니다. 2021년 여름, 온건파 하산 로하니 대통령 대신 강경파 이브라힘 라이시가 대통령이 되었습니다. 최고 지도자의 제자이자 IRGC(Islamic Revolutionary Guard Corps, 이란혁명수비대)의 가까운 동맹인 라이시와 뚜렷한 대조를 이루는 로하니 전 대통령의 외교 성향은 최고 지도자 및 IRGC 고위 지도자들과 갈등을 빚는 경우가 많았습니다.[29] 라이시 행정부의 매파적 견해는 이란과의 핵 협정을 되살리기 위한 외교적 개입의 재개에도 불구하고 이란 공격자들이 이스라엘과 서방, 특히 미국에 대해 더 대담한 조치를 취하려는 의지를 높인 것으로 보입니다.

이스라엘에 대한 이란의 사이버 공격 속도 및 범위 증가

라이시가 외교 정책 팀을 구성한 지 몇 주 만에[30] 이란 차원의 공격자들은 전년도보다 더 빠른 속도로 이스라엘에 대한 파괴적인 사이버 공격을 재개했습니다. 이러한 랜섬웨어 및 hack-and-leak(해킹 및 유출) 공격은 9월을 시작으로 몇 주에 한 번씩 수행되었으며 최소 3명의 이란과 연계된 공격자들이 연루됨에 따라 공격은 이스라엘에 대한 전국적인 보복 캠페인의 일부였을 수 있다는 사실을 시사합니다. 최소 한 가지 사례에서 Microsoft는 2021년 말 이스라엘 조직에 대한 랜섬웨어 공격이 기본 데이터 삭제 공격을 숨기기 위한 공격이라고 평가했습니다. Microsoft 맬웨어 분석에 따르면 피해자에게 전달된 랜섬웨어는 암호화 후 와이퍼 맬웨어를 실행하도록 프로그래밍되었습니다.

2022년까지 이란의 사이버 공격은 표적 선택지 및 공격 형태에서 확대되었습니다. 2월에 DEV-0198은 이스라엘의 중요 기반 시설에 대한 파괴적인 공격을 시도했습니다. Microsoft는 또한 이란과 연계된 한 공격자가 IP 네트워크를 통해 오디오를 조정하는 소프트웨어를 사용하여 6월 이스라엘에서 비상 로켓 사이렌을 울린 정교한 사이버 공격에 책임이 있을 가능성이 가장 높다고 평가합니다.

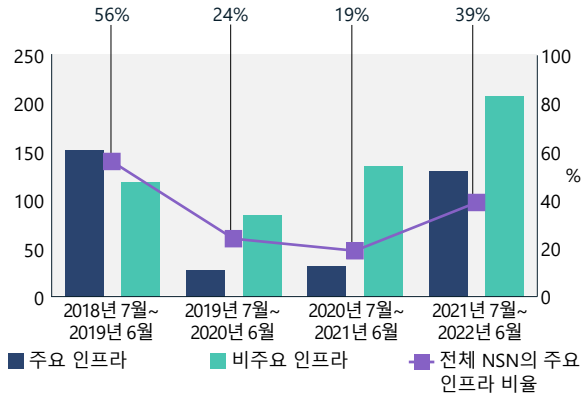
일 년 내내 증가한 미국과 이스라엘의 주요 인프라에 대한 이란의 위협

Microsoft가 평가하는 이란 차원의 공격자들은 2021년 말부터 2022년 중반까지 미국과 이스라엘의 주요 인프라를 표적으로 한 IRGC(PHOSPHORUS 및 DEV-0198)와 연계하고 있습니다. 가능한 목표는 IRGC 고위 관리들이 이란을 방해하고 있다고 미국과 이스라엘을 비난한 것과 동일한 부문에서 보복할 수 있는 옵션을 테헤란에 제공하는 것이었습니다.[31] Microsoft는 이러한 활동이 미국과 이스라엘 정권 내 영향력 있는 기타 인물이 이란의 항구, 철도, 주유소를 표적으로 삼고 사이버 공격을 자행했다고 계속해서 비난한 이란 IRGC의 수동적 국방 기구의 수장 Gholamreza Jalali 장군이 지난 2021년 10월 말 발표한 성명과 관련이 있다고 평가합니다.[32] Jalali는 금요일 기도 연설에서 'USA'라는 단어를 타격하는 미사일 그림과 함께 다시 한번 이러한 내용의 비난을 전달하며 자신의 상관들 역시 동일한 견해를 갖고 있음을 시사합니다.[33]

PHOSPHORUS는 2021년 10월 패치되지 않은 Fortinet 및 ProxyShell 취약점에 대해 미국 조직에 대한 광범위한 스캔을 시작했습니다. 일단 침해되면 이와 같이 패치되지 않은 시스템은 미국 및 기타 서방 국가의 주요 인프라에 대한 랜섬웨어 공격을 실행하는 데 사용되었습니다. 이는 중동 이외의 지역에서 이란 국가와 연계된 랜섬웨어 공격을 확인한 첫 번째 사례였습니다. 10월 말 이란의 주유소에 대한 사이버 공격 이후 Microsoft는 미국 기업에 대한 이란 랜섬웨어 공격이 급증한 것을 발견하며 이에 대한 연관성을 시사했습니다.

이와 동시에, PHOSPHORUS는 주요 항구 및 진입점의 공항, 대중교통 시스템, 유틸리티 회사, 석유 및 가스 회사를 포함한 미국의 유명한 주요 인프라 회사를 스피어 피싱을 통해 직접 표적한 경우가 많았습니다. 스피어 피싱을 통해 종종 수행되는 이 표적은 2022년 중반까지 지속되었습니다. 표적은 테헤란이 이란에 공격한 미국과 이스라엘을 비난한 부문과 직접적으로 일치하며 이란에 보복 옵션을 제공했을 가능성이 높습니다. 거의 동일한 표적을 침해하는 것은 향후 이와 같은 공격을 억제할 수 있는 기회를 제공하는 동시에 죄를 인정하지 않고 공격의 원인을 암시하여 문제 제기를 회피하려는 것입니다.

이란의 인프라 타겟팅 부활



주요 인프라를 표적으로 삼는 이란의 행태는 2018년 말부터 2019년 초까지 최고 수준으로 증가했습니다. Microsoft는 미국 PPD-21(Presidential Policy Directive 21, 대통령 정책 지침 21)을 사용하여 회사가 주요 인프라 기준에 부합하는지 여부를 결정했습니다. (2021년 7월~2022년 6월).

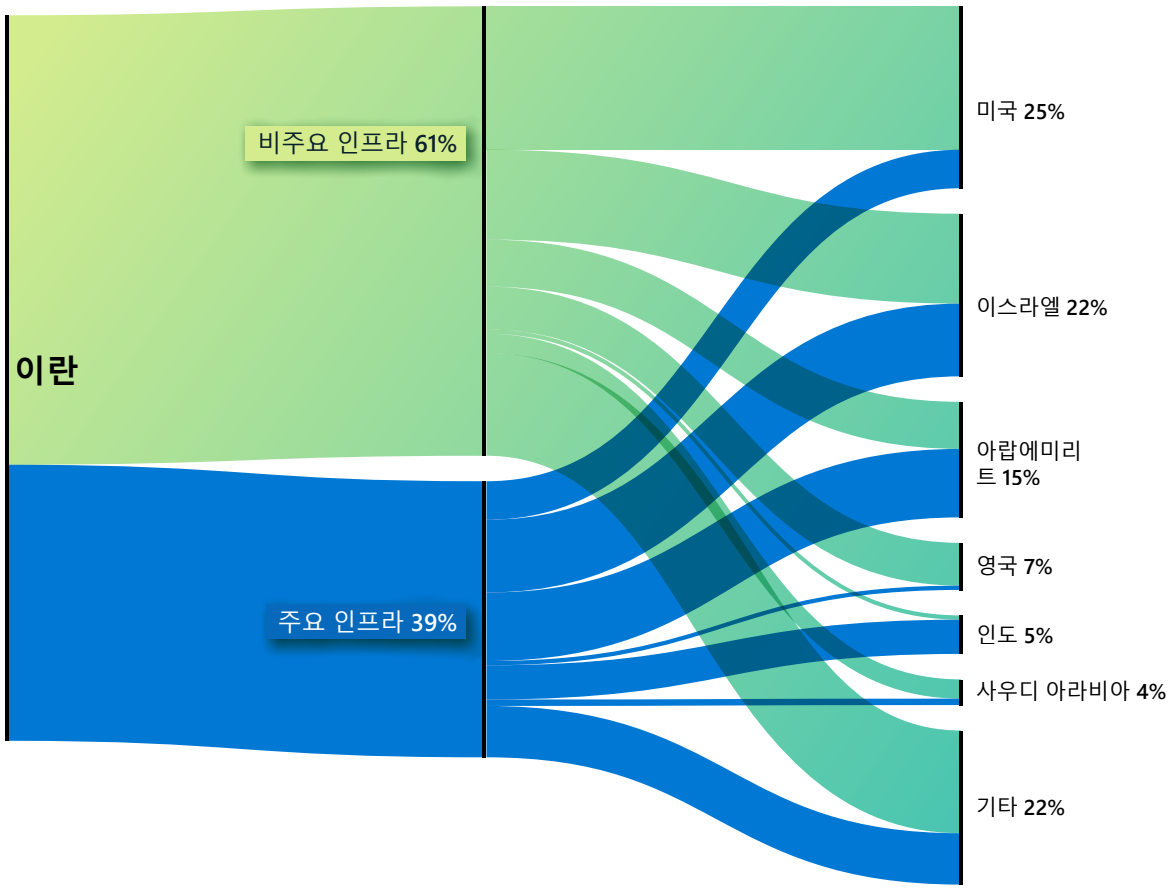
권력 이양 후 점점 더 공격적으로 성장하고 있는 이란

계속

이스라엘에서 DEV-0198은 주유소를 중점으로 두고 이스라엘 철도, 물류 회사, 물류 회사의 소프트웨어 제공 업체, 연료 회사를 표적으로 삼았습니다. 2022년 초, 이 그룹은 주요 이스라엘 물류 회사의 네트워크에 대한 파괴적인 공격을 수행하여 회사는 공격을 억제하기 위해 컴퓨터와 일부 작업을 종료해야 했습니다. 다른 사례를 통해 Microsoft는 그룹이 도난당하거나 재사용된 개인 인증 정보를 통해 주요 이스라엘 운송 제공 업체의 네트워크에 액세스하려고 시도한 사실을 발견했습니다. 한편, 국방, 해상 운송, 위성 이미지 회사를 표적으로 삼아 IRGC와의 연관성을 시사하는 또 다른 이란 공격자인 DEV-0343은 2021년 초 내내 이스라엘 운송 및 항구 관련 기관의 계정을 침해했습니다.

이란의 위협 그룹은 특히 이란 핵 협정을 되살리려는 외교적 노력이 줄어들고 워싱턴, 텔아비브, 테헤란이 양허를 활용할 대안적인 강압 수단을 모색함에 따라 미국과 이스라엘의 운송 및 에너지 회사에 위협이 될 가능성이 높습니다.

국가별 이란의 주요 인프라 표적



이란은 이스라엘, 에미리트, 미국 내 조직에서 가장 두드러지게 주요 인프라를 표적으로 삼았습니다.

이란 공격자들은 내년에도 미국과 이스라엘의 운송 및 에너지 회사에 위협이 될 것입니다.

이란 그룹은 랜섬웨어 공격을 지역 내 적을 넘어 확장했으며 미국과 이스라엘의 주요 인프라를 표적으로 삼고 있습니다.

실행 가능한 인사이트

1. MFA와 같은 비밀번호 없는 솔루션을 지원하고 모든 원격 연결에 해당 솔루션을 강제적으로 사용하여 잠재적으로 침해된 개인 인증 정보를 완화하여 조직의 전반적인 사이버 위생을 개선합니다.
2. 모든 인바운드 이메일 트래픽의 신뢰성을 평가하여 발신자 주소가 합법적인지 확인합니다.
3. 일찍 그리고 자주 패치합니다.[34]
4. 각 서비스 제공자와의 파트너 관계를 검토하고 감사하여 조직과 업스트림 제공자 간의 불필요한 권한을 최소화합니다. Microsoft에서는 친숙하지 않거나 아직 감사되지 않은 파트너 관계에 대한 액세스 권한을 즉시 제거하는 것을 권장합니다.[35]

추가 정보에 대한 링크

- 성장하는 IT 부문을 타겟으로 한 이란 | MSTIC(Microsoft 위협 인텔리전스 센터), Microsoft DSU(디지털 보안부)
- 국방, GIS, 해양 부문을 겨냥한 이란 관련 DEV-0343 | MSTIC(Microsoft 위협 인텔리전스 센터), Microsoft DSU(디지털 보안부)

이스라엘을 표적으로 하는 이란과 연관된 레바논 기반의 그룹

Microsoft는 플랫폼, 표적이 된 피해자 또는 지리적 지역과 관계없이 사이버 위협 활동을 모니터링합니다. 전 세계적으로 가시성 및 적극적인 위협 헌팅을 유지하여 고객을 위한 더 나은 탐지를 작성합니다.

러시아, 중국, 이란, 북한의 위협이 Microsoft에서 발견한 국가 차원의 공격자 활동의 대부분을 차지하지만, Microsoft는 NATO 회원국과 민주주의 국가의 위협 역시 추적하고 이에 대해 소통합니다. 작년에는 터키 기반의 공격자(SILICON)와 베트남 기반의 공격자(BISMUTH)의 활동에 대해 소개했습니다. 올해 Microsoft는 이전에 공개적으로 공개한 레바논 기반 그룹의 세부 내용을 발전시키고 있습니다.[36]

Microsoft는 이전에 문서화되지 않은 레바논 기반 그룹을 발견했으며, 이란의 MOIS(정보보안부)와 연계된 공격자들과 협력하여 중간 정도의 접근성을 통해 이 그룹을 평가합니다. 테헤란의 이러한 협력 또는 지침은 2020년 말 이란 정부 기관이 사이버 작전을 수행하기 위해 제삼자와 협력하고 있다는 내용의 폭로와 일치하며, 이는 이란이 그럴듯한 변명을 하며 부인할 가능성이 높습니다.

관찰된 활동에서 POLONIUM은 Microsoft가 활동을 중단하고 공개적으로 이들의 활동을 공개하기 전인 2022년 2월과 5월 사이에 24개의 이스라엘 기반 조직과 1개의 레바논 기반 IGO를 표적으로 삼거나 침해했습니다. 이스라엘 조직의 거의 절반이 이스라엘 국방 산업의 일환이거나 이스라엘 국방 산업체와 연관이 있는데, 이는 이 그룹이 이스라엘에 대한 정보 수집 및/또는 이스라엘에 직접 대응하는 데 있어 이란과 유사한 이해관계를 가지고 있음을 나타냅니다.[37]

MOIS 그룹에 대한 POLONIUM의 평가된 링크는 관찰된 피해자 중복과 도구 및 기술의 공통성을 기반으로 합니다.

- 피해자 중복: Microsoft에서 MERCURY라고 추적하는 이란의 MOIS와 연관된 이란 차원의 한 그룹은 과거 POLONIUM의 여러 희생자를 침해했는데, 이는 임무 요구 사항의 수렴 또는 그룹 간 희생자의 '승인' 가능성을 나타냅니다.
- 일반적인 도구 및 기술: POLONIUM과 유사하게 MSTIC는 DEV-0588(CopyKittens라고도 함)이 일반적으로 작전 시 AirVPN을 사용하고 DEV-0133(Lyceum[38]이라고도 함)은 C2 및 유출 시 OneDrive를 사용합니다. 이란 차원의 공격자들과 마찬가지로 POLONIUM은 클라우드 서비스 제공자를 사용하여 이스라엘 항공 회사와 법률 회사를 침해했습니다.[39]

POLONIUM은 C2 및 데이터 유출을 위해 클라우드 서비스(특히 OneDrive 및 DropBox)를 사용하여 일련의 사용자 맞춤형 임플란트를 배포했습니다. POLONIUM은 탐지를 피하기 위해 표적 고유의 OneDrive 애플리케이션을 생성하는 경우가 많았습니다.

2022년 6월 현재 Microsoft는 POLONIUM에서 생성한 20개 이상의 OneDrive 애플리케이션을 일시 중단하고, 영향을 받는 조직에 알리며, POLONIUM에서 개발한 도구를 격리하기 위해 일련의 보안 인텔리전스 업데이트를 배포했습니다.

Microsoft는 OneDrive를 C2로 남용하는 POLONIUM의 행위를 성공적으로 탐지하고 비활성화했습니다.

실행 가능한 인사이트

1. 바이러스 백신 도구[40]를 업데이트하고 클라우드 보호[41]를 켜 관련 지표를 탐지하도록 합니다.
2. 서비스 제공자와 관계를 맺고 있는 고객의 경우, 모든 파트너 관계를 검토하고 감사하여 조직과 업스트림 제공자 간의 불필요한 권한을 최소화해야 합니다.42 친숙하지 않거나 감사되지 않은 파트너 관계에 대한 액세스 권한을 즉시 제거합니다.

추가 정보에 대한 링크

- 이스라엘 조직을 표적으로 삼은 POLONIUM 활동 및 인프라 노출 | MSTIC(Microsoft 위협 인텔리전스 센터), Microsoft DSU(디지털 보안부)
- 패치되지 않은 시스템의 Log4j 2 취약점을 활용하여 이스라엘 조직을 표적으로 삼는 MERCURY | MSTIC(Microsoft 위협 인텔리전스 센터), Microsoft 365 Defender 연구 팀, Microsoft Defender 위협 인텔리전스

북한 정권의 3대 목표 달성에 활용된 사이버 역량

지난 한 해 동안 북한의 사이버 우선순위는 북한 정부 기관에서 명시한 국제적인 우선순위를 반영했습니다. 김정은은 주요 연설에서 여러 번 국방 역량의 구축, 어려움을 겪고 있는 국가 경제의 강화, 국내 안정의 보장이라는 세 가지 우선순위를 강조했습니다.[43] 북한 차원의 공격자들이 취한 조치는 이 세 가지 목표를 달성하기 위해 사이버 환경이 활용되고 있음을 분명히 보여줍니다.

북한 차원의 공격자들은 다양한 전술을 사용하여 전 세계 항공우주 기업에 침투했습니다.

주로 CERIUM 및 ZINC를 중심으로 한 북한 차원의 위협 그룹들은 다양한 전술을 사용하여 전 세계 국방 및 항공우주 기업 네트워크에 침투했습니다. 북한은 2022년 상반기에 역사상 가장 공격적으로 미사일 시험에 착수하면서 사이버 스파이 활동을 통해 북한 연구원들이 적국의 발전에 대한 북한만의 방어 시스템과 대응책을 개발하는 데 우위를 점할 수 있도록 지원했습니다.

Microsoft는 COPERNICIUM이 전 세계 다양한 암호화폐 관련 회사를 표적으로 삼고 종종 성공을 거두어 어려움을 겪고 있는 북한의 경제를 지원한다는 사실을 발견했습니다. 이 그룹이 침해 이후 돈을 빼낼 수 있었는지는 확인할 수 없지만 COPERNICIUM이 다른 암호화폐 회사의 제안으로 가장한 악성 문서를 보내 수십 대의 기계를 감염시켰다는 사실을 발견했습니다.

마지막 그룹은 Microsoft가 북한 문제를 보도하는 뉴스 조직을 표적으로 삼아 북한 내 안정성과 충성도를 유지하기 위해 노력하는 것으로 추적되는 DEV-0215입니다. 이러한 매체들은 북한 및 탈북자 공동체 내에 정보원이 있으며, 평양은 이를 실존적 위협으로 보고 있습니다. 또한 이 그룹은 북한을 노골적으로 반대하고 탈북자들과 적극적으로 협력하는 한국 기독교 단체의 네트워크에 접근하기 위해 노력했습니다.

국방 및 항공우주 기업 표적

CERIUM 및 ZINC에서 이끄는 북한 차원의 공격자들은 국방 및 항공우주 기업에 침투할 수 있는 전술 개발에 상당한 노력을 기울였습니다. CERIUM은 클라이언트를 다운로드하고 약점을 찾아 한국의 VPN(가상 사설망)을 반복적으로 조사했습니다. 또한 한국군 및 정부 기관 고객이 사용하는 일반적인 애플리케이션을 다운로드하여 취약점을 찾았습니다. 이 그룹은 현재 진행되고 있는 이벤트를 면밀히 추적하고 표적이 맬웨어 실행 파일과 링크를 클릭하도록 하기 위해 세간의 이목을 끄는 주제를 미끼로 사용하는 새로운 미끼 문서를 작성했습니다.

ZINC와 CERUM은 모두 캠페인에서 소셜 미디어와 소셜 엔지니어링을 사용했습니다. ZINC는 특히 LinkedIn 및 기타 전문 소셜 미디어 사이트에서 가짜 프로필을 만드는 데 능숙했으며, 공격자들은 주요 국방 및 항공 우주 회사의 채용 담당자로 사칭했습니다. 이러한 프로필을 통해 소셜 미디어의 다이렉트 메시지나 이메일을 활용하여 잠재적인 피해자에게 링크나 악성 첨부 파일을 보냈습니다.

CERIUM은 기업 직원 외에도 한국군을 광범위하게 표적으로 삼아 육군사관학교 및 학계에서 일하는 모든 군인에게 특별한 관심을 보였습니다.

손실 균형을 맞추기 위한 암호화폐 표적

2016년 유엔 제재가 가해진 이후 북한 경제는 2020년 초 코로나19 팬데믹이 시작된 이래 홍수[44], 가뭄[45]과 같은 자연재해와 거의 전면적인 국경의 수입품 봉쇄로 인해 계속 위축되고 있습니다.[46] 북한은 2022년 초에 중국과의 무역을 위해 잠시 국경을 개방했지만 곧 다시 폐쇄했습니다.[47] 5월 중순, 북한은 국내에서 첫 코로나19 확진자가 발생했다고 보고했습니다.[48] 그 이후 이미 취약한 북한 경제에 부정적인 영향을 미친 바이러스와 맞서 싸우기 위해 전면 폐쇄라는 중국식 '제로 코로나' 전략을 채택했습니다.

북한 차원의 그룹인 COPERNICIUM은 침투할 수 있는 모든 회사 네트워크로부터 돈(일반적으로 암호화폐 형태)을 훔쳐 손실된 수익의 일부를 상쇄하려고 했습니다. 이들은 미국, 캐나다, 유럽, 아시아 전역의 암호화폐 관련 회사의 수십 대 기계를 침해했습니다. 심지어 COPERNICIUM 북한의 가장 강력한 동맹국인 중국 본토와 홍콩의 암호화폐 관련 회사 소유의 기계까지 침해했습니다. 이 그룹은 초기 정찰 및 표적에 접근하기 위해 소셜 미디어에 크게 의존했습니다. 공격자들은 암호화폐와 관련된 비즈니스의 개발자 또는 고위 임원을 사칭하는 프로필을 작성했습니다. 그런 다음 업계 관계자들과 관계를 구축한 다음 악성 링크 또는 파일을 보냅니다.

북한 정권의 3대 목표 달성에 활용된 사이버 역량

계속

PLUTONIUM 관련 그룹에서 랜섬웨어 개발 및 배포

Microsoft에서 DEV-0530으로 추적하는, 북한에서 시작된 공격자 그룹은 2021년 6월에 랜섬웨어를 개발하여 공격에 사용하기 시작했습니다. 스스로 H0lyGh0st라고 하는 이 그룹은 캠페인에 동일한 이름의 랜섬웨어 페이로드를 활용했으며 이미 2021년 9월에 여러 국가 내 중소기업을 성공적으로 침해했습니다.

Microsoft는 DEV-0530이 PLUTONIUM(DarkSeoul 또는 Andariel이라고도 함)으로 추적되는 또 다른 북한 기반 그룹과 관련이 있다고 평가했습니다. 캠페인에서 H0lyGh0st 랜섬웨어를 사용하는 것은 DEV-0530에만 해당되지만 MSTIC는 DEV-0530이 PLUTONIUM에서 독점적으로 생성한 도구를 사용하는 사실뿐만 아니라 두 그룹이 커뮤니케이션한다는 사실을 발견했습니다.

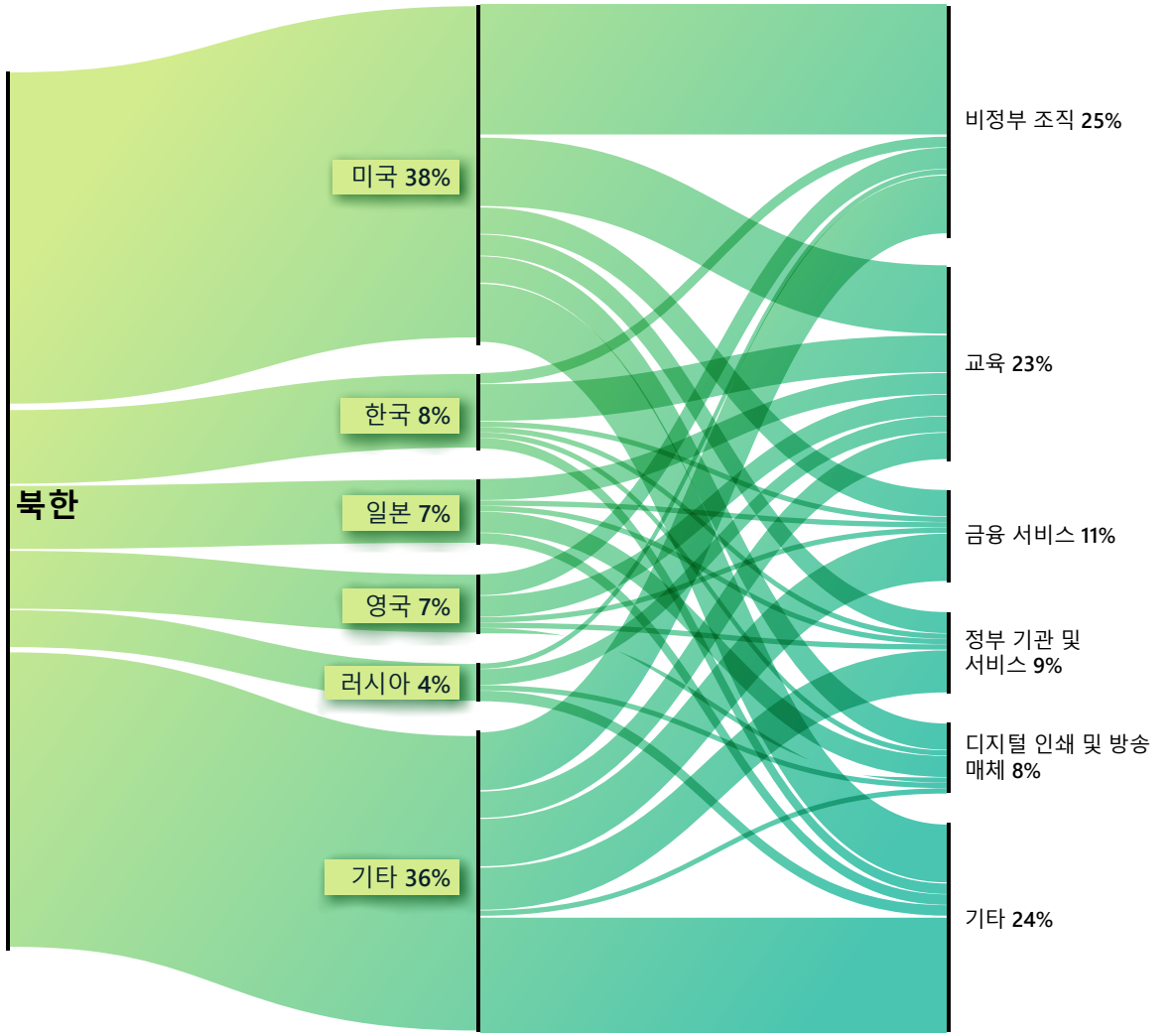
DEV-0530 활동이 정부 기관의 후원을 받았는지는 확실하지 않습니다. 랜섬웨어 공격은 암호화폐 회사의 절도를 후원하는 것과 같은 이유로 정부 기관에서 명령을 받아 진행되었을 수 있지만, DEV-0530의 배후에 있는 공격자들이 돈을 벌기 위해 독립적으로 행동했을 수도 있습니다. 북한 해커들이 독립적으로 활동한다면, 정부 기관에서 후원하는 암호화폐 기업에 대한 절도 작전에 비해 활동이 널리 퍼지지 않은 이유를 설명할 수 있을 것입니다.

북한 언론사, 탈북자, 종교 단체, 구호 단체를 표적으로

작년에 최고 지도자 김정은은 공개적으로 미사일과 핵무기보다 내부 안보와 충성도에 더 중점을 두었습니다. 국내 문제에 몰두하는 이러한 기조를 반영하여, 적어도 두 개의 북한 차원의 그룹은 북한 정권이 국내 위협으로 간주할 측면에 초점을 맞췄습니다.

첫 번째 그룹은 Microsoft에서 DEV-0215로 추적하는 그룹으로, 북한 뉴스를 밀접하게 따르는 언론사 조직을 표적으로 삼습니다. 언론사를 표적으로 하는 이유 중 하나는 이러한 언론사가 외부 세계와 커뮤니케이션하는 다양한 방법을 활용하여 탈북자, 북한과 긴밀히 협력하는 중국 시민, 심지어 북한에 거주하는 일부 북한 시민으로부터 뉴스거리를 입수하기 때문입니다. 북한 정부 기관은 이들, 특히 북한 내에서 반역자 및 스파이로 간주되는 북한 주민들을 생존에 대한 실존적인 위협으로 보고 있습니다. DEV-0215는 잠재적인 정보 유출을 무력화할 수 있도록 이러한 정보원들을 식별하려고 했을 것입니다.

북한: 상위 표적 국가 및 산업 부문



북한은 미국, 한국, 일본을 주적으로 보고 있습니다. 러시아는 오랜 동맹국이지만 북한 차원의 위협 행위자들은 러시아 싱크 탱크, 학계, 외교 관계자를 표적으로 삼아 국제 문제에 대한 러시아의 견해에 대한 정보를 얻습니다.

북한 정권의 3대 목표 달성에 활용된 사이버 역량

계속

Microsoft는 또한 한국 기독교 공동체를 표적으로 삼은 DEV-0215의 증거를 확인했습니다. 한국의 복음주의 기독교 교회들은 북한, 그리고 북한과의 우호적인 관계를 형성하는 한국 정부 기관에 대해 비판적인 경향이 있습니다. 이 교회들은 탈북자들을 대상으로 전도 활동을 할 가능성이 높으며, 일부는 북한을 대상으로 인도주의적 활동을 하고 있습니다. 북한은 이들을 위협으로 보고 있는데, 팬데믹 기간 동안 북한의 탈북자들이 거의 없었지만,[49] 이와 같은 기독교 단체들은 탈북자들의 탈출을 돕는 데 중요한 역할을 하는 경우가 많기 때문입니다. DEV-0215는 한국인 연사들을 표적으로 삼아 기독교 컨퍼런스에 대한 가짜 문서를 생성하여 이들을 표적으로 삼고 탈북에 도움을 주는 사람을 알아내기 위한 미끼로 사용했습니다.

마지막으로 국가 차원의 그룹인 OSMIUM은 한 해 동안 작년에 북한을 지원한 단체를 비롯하여 국제 구호 단체에 꾸준한 관심을 보였습니다. 북한은 대체로 국제 원조를 거절해왔지만, 특히 코로나19가 발생한 이후[50] 원조 제의를 받아들이는 것을 고려하고 있을 가능성이 있습니다. 그러나 해외 구호원들의 북한 입국 허용에 따른 안보 파급 효과를 경계하고 있습니다. 북한은 자국에 이와 같은 원조를 허용할지 결정하기 위해 전 세계 구호 단체의 네트워크에 침투하고 있을 수 있습니다.

실행 가능한 인사이트

1. 북한 차원의 공격자들은 숙련되고 가차 없고 창의적이지만 조직에서는 이들을 방어할 수 있습니다.
2. 대부분의 성공적인 공격은 2단계 인증 또는 가상 환경에서 알 수 없는 개인이 보낸 첨부 파일을 열지 않는 것과 같은 기본적인 사이버 방역으로 방지할 수 있습니다.

추가 정보에 대한 링크

- H0lyGh0st 랜섬웨어로 중소기업을 표적으로 삼는 북한 위협 행위자 | MSTIC(Microsoft 위협 인텔리전스 센터), Microsoft DSU(디지털 보안부)

북한 전문가들 사이에서는 북한 정부가 공개적인 성명을 진지하게 받아들이고 있는지 아니면 실효성을 주장하고 있는지에 대한 오랜 논쟁이 있어 왔습니다. 북한이 발표한 우선순위와 일치하는 사이버 공격은 북한이 자국의 목표에 대해 공개적으로 말할 때는 진지한 태도로 임한다는 사실을 입증합니다.

사이버 공간의 안정성을 위협하는 사이버 용병

고객(종종 정부 기관)이 네트워크, 컴퓨터, 전화, 인터넷 연결 디바이스에 침입할 수 있도록 지원하는 도구, 기술, 서비스를 개발하고 판매하는 민간 기업의 산업이 성장하고 있습니다. 국가 차원의 공격자들의 자산인 이러한 단체는 반체제 인사, 인권 옹호자, 언론인, 시민 사회 옹호자, 기타 민간 시민을 위험에 빠뜨리는 경우가 많습니다. Microsoft에서는 이들을 사이버 용병 또는 민간 부문 공격자라고 부릅니다.

민간 부문 기업이 사이버 무기를 만들고 판매하는 세상은 소비자, 다양한 규모의 기업, 정부 기관에 더 위험합니다. 이러한 공격적인 도구는 훌륭한 거버넌스와 민주주의의 규범과 가치와 일치하지 않는 방식으로 사용될 수 있습니다. Microsoft는 인권 보호가 기본적인 의무라고 생각하며 전 세계적으로 '서비스로서의 감시'를 축소함으로써 이를 진지하게 받아들입니다.

Microsoft는 민주주의 및 권위주의 정권의 특정 국가 차원의 공격자들이 '서비스로서의 감시' 기술의 개발 또는 사용을 아웃소싱하는 것을 평가했습니다. 이것이 바로 이들이 책임과 감독을 피하고 기본적으로 개발하기 어려운 능력을 습득하는 방법입니다.

> 이러한 사이버 무기는 국가가 단독으로 개발할 수 없었던 감시 기능을 제공합니다.

사이버 용병이 활동하는 시장은 불투명합니다. 그럼에도 불구하고 Microsoft에서는 제로 데이 악용과 피해자와의 상호 작용이 전혀 필요하지 않은 제로 클릭 악용을 활용하여 이러한 그룹을 계속해서 관찰하여 서비스로서의 감시를 지원합니다.

Microsoft는 최근 DSIRF라고 하는 오스트리아 기반 PSOA인 유럽 민간 부문 공격자, KNOTWEED에 대해 발표했습니다. 여러 뉴스 보도에 따르면 이 회사는 Subzero라는 맬웨어 도구 세트의 개발 및 판매 시도와 연관되어 있습니다.[51] 피해자로는 오스트리아, 영국, 파나마와 같은 국가 내 법률 회사, 은행, 전략 컨설팅 회사가 있습니다.[52]

이러한 공격 감시 기능은 더 이상 국방 및 정보 기관이 만든 고도로 기밀 기능이 아니라 현재 기업과 개인에게 제공되는 상업용 제품이기 때문에 사이버 무기에 대한 모든 규제 체제는 수출 통제를 넘어서야 합니다. 이러한 사이버 무기의 영향은 치명적일 수 있습니다.

사이버 용병이 제품이나 서비스의 취약점을 악용하면 전체 컴퓨팅 생태계가 위험에 처하게 됩니다. 취약점이 공개적으로 식별되면 기업은 광범위한 기반 공격이 발생하기 전에 앞다투어 보호 기능을 릴리스합니다(취약점 악용에 대한 이전 설명 참조). 이는 (패치를 편리하게 개발해야 하는) 소프트웨어 공급업체와 (패치를 즉시 구현해야 하는) 제품 소비자 모두에게 위험하고 어려운 시기입니다.

150개 이상의 기술 회사를 통합하는 선도적인 동맹인 Cybersecurity Tech Accord[53]의 창립 멤버인 Microsoft는 온라인에서 공격적인 활동에 관여하지 않기로 약속했습니다. Microsoft는 이러한 약속과 이 분야에서의 인권 책임을 지지합니다. Microsoft는 사이버 용병이 제공하는 서비스로 인한 부정적인 영향을 강조하기 위해 기술적 중단 및 법적 어려움에 함께했으며 남용된 경우를 목격했을 때 계속해서 고객을 보호할 것입니다.

> 사이버 용병은 고급 맬웨어 및 다양한 기술을 포함하여 기술적으로 정교하고 광범위하게 사용할 수 있는 '서비스로서의 감시' 기능을 생성하고 제공합니다.

정부 기관의 실행 가능한 인사이트

1. 이러한 공격자들에 대한 금지를 포함하여 미국이 상무부의 법인 목록에 있는 회사를 표적으로 삼았던 것처럼 특히 조달 부문에서 서비스로서의 감시에 대한 투명성 및 감독 요구 사항을 구현합니다.
2. 이 부문에서 근무했던 전직 직원을 대상으로 퇴직 후 제한 규칙을 설정합니다.
3. '고객에 대한 이해' 의무를 이행하고 기업이 인권 약속을 지키도록 장려하는 것을 목표로 합니다.

추가 정보에 대한 링크

- 엉킨 매듭 풀기: 제로 데이 악용을 사용하는 유럽 민간 부문의 공격자 | MSTIC(Microsoft 위협 인텔리전스 센터), MSRC(Microsoft 보안 대응 센터), RiskIQ(Microsoft Defender 위협 인텔리전스)
- 민간 부문 사이버 무기와의 지속적인 싸움 | 문제에 대응하는 Microsoft

사이버 공간의 평화와 안보를 위한 사이버 보안 규범 운영

인권을 우선시하고 온라인에서 무모한 국가 행동으로부터 사람들을 보호하는 일관적인 국제적인 프레임워크가 긴급하게 필요합니다. 이러한 사실은 우크라이나에서 현재 진행되고 있는 전쟁에서 가장 명확히 입증되었습니다. 국제 사회의 전략적인 노력 외에도 정부 기관은 긍정적인 영향을 즉각적으로 미치기 위해 지금 바로 행동에 나설 수 있습니다.

5년 전 Microsoft는 온라인 평화와 안보를 수호하기 위해 다양한 부문에 걸쳐 책임과 의무를 증진하기 위해 '디지털 제네바 협약'을 요구했습니다. 사이버 공간은 국가 간의 갈등과 경쟁이 뚜렷하게 발생하는 불안정한 영역으로 새롭게 떠오르고 있으며, 평시에도 공격이 더욱 보편화되었습니다.

오늘날에도 이러한 프레임워크에 대한 필요성은 러시아 침공의 일환으로 우크라이나를 표적으로 삼은 러시아의 사이버 공격으로 입증되었습니다. 이번 전쟁은 우리가 이전에 알고 있던 것과는 극적으로 다른 새로운 전선을 만들었습니다.

사이버 공간에 안정성을 가져오려면 목적에 맞춰 국제 거버넌스 기관을 강화하고 재구상해야 합니다. 사이버 공간은 국경이 없고 합성적인 특성이 있으며 주로 민간 산업에 의해 유지되는 등 다른 영역과 근본적으로 다릅니다. 이는 기술 산업이 제품 및 서비스의 보안과 더 넓은 디지털 생태계에 대해 더 큰 책임을 지도록 요청하는 것을 의미합니다. 모든 면에서 눈에 띄는 진전이 있었지만 그중 어려움은 극적으로 증가했습니다.

우리는 사이버 공간의 보안을 방어하기 위해 공동의 노력을 강화해야 합니다. 온라인에서 기대했던 권리와 자유를 당연하게 여길 수 없습니다. 어려움을 해결하기 위해 고군분투하는 동안 악의적인 공격자들은 AI를 활용하여 다음 공격 방법 및 위치를 계획하고, 허위 정보를 활용하고, 신생 메타버스를 훼손할 방법을 모색하고 있습니다. 인권 옹호자, 기술 산업, 인권 존중 정부 기관은 안전한 온라인 세계를 구성할 수 있는 긍정적인 비전을 향해 협력해야 합니다. 앞으로 가야 할 길은 멀지만 사이버 보안 생태계를 즉시 개선하기 위해 지금 당장 정부가 할 수 있는 일이 있습니다.

- 공격자 특정 시, 규범, 법률, 결과를 인용합니다. 지난 5년 동안 크게 개선된 점 중 하나는 사이버 공격의 공격자를 특정하는 정부 기관의 속도와 조정이었습니다. 이러한 진술을 통해 단순히 이름을 밝히고 망신을 주는 것 외에도 어떤 국제법이나 규범이 위반되고 어떤 방식으로 결과가 야기될지를 강조하여 국제적인 기대에 대한 인식을 강화하는 데 도움이 되어야 합니다.
- 온라인으로 국제법 해석을 명확히 합니다. 정부 기관은 국제법이 온라인에 적용된다는 데 동의하지만 특정 경우에 어떻게 적용되는지 의문이 남아 있습니다. 이는 특히 우크라이나 침공의 여파와 관련이 있습니다. 정부 기관은 국제법에 따른 의무를 어떻게 이해하는지 명시함으로써 기대치를 설정하고, 오해를 방지하고, 신뢰를 구축하는 데 큰 도움이 될 수 있습니다.
- 다른 이해관계자들과 협의합니다. 국제 포럼이 강력한 다중 이해관계자 포용을 촉진하는 최선의 방법을 계속해서 발견함에 따라 정부 기관은 다중 이해관계자 커뮤니티, 특히 기술 산업과 협의하여 정보에 입각한 대화를 지원함으로써 필수 전문 지식을 보유한 사람들과 대화를 나눌 수 있습니다.
- 사이버 공간에서 책임 있는 국가 행동을 지원하기 위해 상설 기구를 구성합니다. 온라인에서 책임 있는 국가 행동을 증진하기 위한 국제 외교 포럼의 작업이 그 어느 때보다 중요해졌습니다. 사이버 공간을 분쟁 영역으로 다루기 위한 영구적인 유엔 메커니즘이 분명히 필요합니다.
- 진화하는 위협에 대한 새로운 규범을 정의합니다. 사이버 공간 위협은 기술 혁신과 함께 끊임없이 진화하고 있습니다. 국제 규범은 기술 중립적이어야 하지만 위협 환경의 변화와 기술 사용 방식에 따라 업데이트되고 약화되어야 합니다. 현재에도 기존 국제 프레임워크의 격차가 남용되는 경우를 봅니다. 국가는 소프트웨어 업데이트 프로세스와 같이 현재 보호되지 않는 디지털 생태계를 뒷받침하는 핵심 프로세스를 명시적으로 보호하기 위해 노력해야 합니다. 뿐만 아니라, 특정 영역은 추가적인 보호가 필요합니다. 예를 들어, 팬데믹을 통해 배운 바와 같이 의료 보호를 위한 규범은 필수적입니다.

국가 차원의 공격자들과 이들의 공격은 규모와 정교함이 증가하여 견딜 수 없는 상황을 만들고 있습니다.

즉각적인 조치를 취해야 합니다. 현재 사이버 공간에서 국가 차원의 공격자들에 대한 합의된 규범 및 규칙을 구현하고 광범위한 다중 이해관계자 커뮤니티와 협력하여 새로운 격차를 해결하는 등 사이버 보안 생태계를 즉시 개선하기 위해 정부 기관이 할 수 있는 일이 있습니다.

다자간 기관은 국가 차원의 사이버 공격에 대한 긴급한 문제를 해결하기 위해 재구상되어야 합니다.

추가 정보에 대한 링크

- 심판의 순간: 강력하고 국제적인 사이버 보안 대응의 필요성 | 문제에 대응하는 Microsoft
- 의료 분야를 겨냥한 사이버 공격은 중단되어야 | 문제에 대응하는 Microsoft
- 손짓하는 유엔 사이버 외교의 다음 장 | 문제에 대응하는 Microsoft

미주

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. 이 장의 주요 인프라는 PPD-21(대통령 정책 지침 21)의 Critical Infrastructure Security and Resilience(2013년 2월)에 정의되어 있습니다.
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://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://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.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://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.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/;
30. 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

미주(계속)

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. 특히 Exchange 서버에 ProxyShell 취약점(CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, CVE-2021-34473)에 대한 패치를 적용합니다. 또한 Fortinet FortiOS SSL VPN 어플라이언스에 취약점을 패치해야 합니다.
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-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. Jan-Philipp Hein, In the mystery of creepy spy software, the trail leads via Wirecard to the Kremlin, FOCUS Online, (2022년), 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, Sugar Mizzy, We unveil the "Subzero" state trojan from Austria, Europe-cities (2021년), https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/, Andre Meister, We unveil the state Trojan "Subzero" from Austria, Netzpolitik.org (2022년), https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich.
52. Microsoft의 기술 블로그에서 언급한 바와 같이, 국제 표적이 일반적이기 때문에 한 국가 내 표적을 식별한다는 것이 반드시 DSIRF 고객이 동일한 국가에 거주한다는 의미는 아닙니다.
53. 홈 | 사이버보안 기술 협정(cybertechaccord.org)

디바이스 및 인프라

디지털 트랜스포메이션이 가속화됨에 따라 디지털 인프라의 보안이 그 어느 때보다 중요해졌습니다.

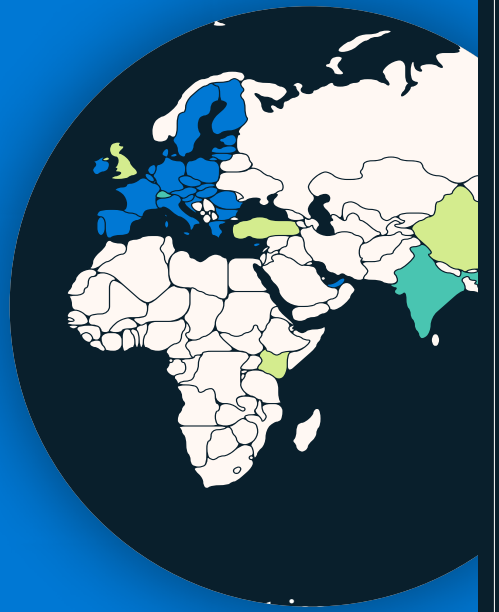
디바이스 및 인프라

개요

팬데믹은 디지털 트랜스포메이션을 가속화하는 구성 요소로 모든 종류의 인터넷 연결 디바이스를 빠르게 채택함에 따라 디지털 세계의 공격 표면을 크게 증가시켰습니다.

사이버 범죄자와 국가 차원의 공격자들이 이를 빠르게 이용하고 있습니다. 최근 몇 년 동안 IT 하드웨어 및 소프트웨어의 보안이 강화되었지만 IoT(사물 인터넷) 및 OT(운영 기술) 디바이스 보안은 이러한 속도를 따라가지 못했습니다. 위협 행위자들은 이러한 디바이스를 악용하여 네트워크에 대한 액세스를 구축하고 측면 이동을 지원하거나, 공급망에 발판을 마련하거나, 대상 조직의 OT 운영을 방해합니다.

전 세계적으로 정부 기관은 IoT 및 OT 보안을 개선하여 주요 인프라를 보호하기 위해 움직이고 있습니다.

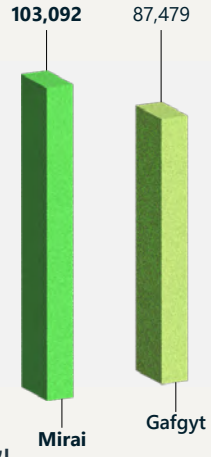


59페이지에서 자세히 알아보기

광범위한 채택을 보장하기 위해서는 전 세계적으로 일관되고 상호 운용 가능한 보안 정책이 필요합니다.

59페이지에서 자세히 알아보기

서비스로서의 맬웨어는 기업 네트워크뿐만 아니라 인프라 및 유틸리티에서 노출된 IoT 및 OT에 대응하기 위해 대규모 운영으로 전환했습니다.



63페이지에서 자세히 알아보기

원격 관리 디바이스에 대한 공격이 증가하고 있습니다. 2022년 5월에는 1억 건 이상의 공격이 관찰되었는데, 이는 작년에 비해 5배 증가한 수치입니다.

62페이지에서 자세히 알아보기

공격자들은 IoT 디바이스 펌웨어의 취약점을 점점 더 활용하여 기업 네트워크에 침투하고 파괴적인 공격을 시작하고 있습니다.

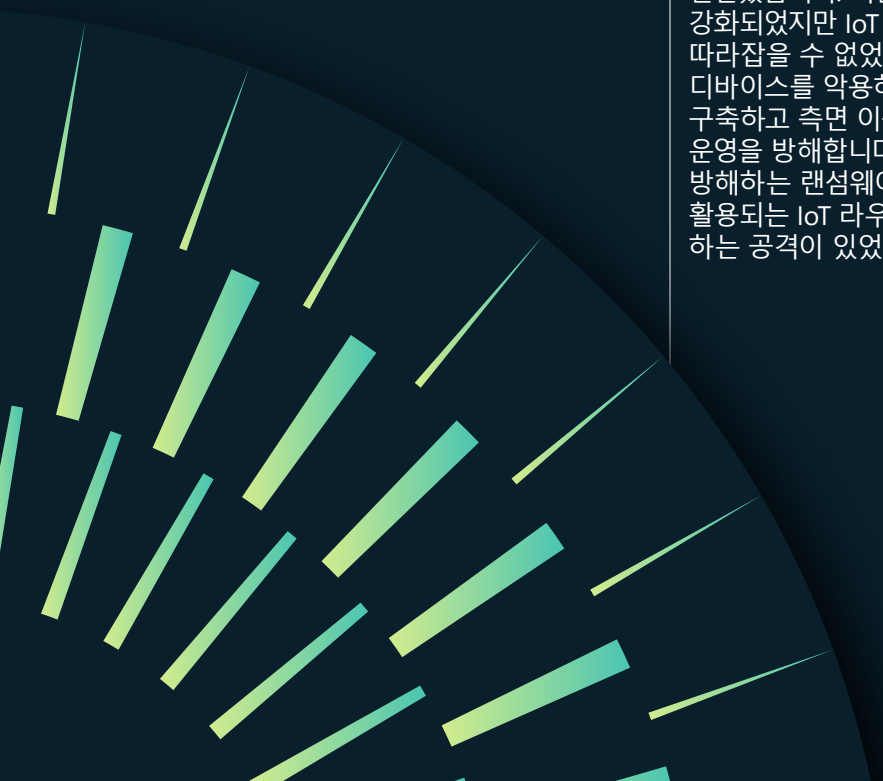
65페이지에서 자세히 알아보기

분석된 펌웨어 이미지 중 32%에는 최소 10개의 알려진 치명적인 취약점이 포함되어 있습니다.

66페이지에서 자세히 알아보기

서문

디지털 트랜스포메이션이 가속화되면서 주요 인프라와 사이버 물리 시스템에 대한 사이버 보안 위험이 증가했습니다.



지난 몇 년 동안 디지털 세계에서는 전례 없는 변화가 있었습니다. 조직은 인텔리전트한 클라우드 및 인텔리전트 엣지에서 모두 향상된 컴퓨팅 기능을 활용하기 위해 진화하고 있습니다. 팬데믹으로 인해 기업은 생존을 위해 디지털화해야 하고 전 세계 산업이 인터넷 연결 디바이스를 채택하는 속도로 인해 디지털 세계의 공격 표면은 기하급수적으로 증가하고 있습니다.

이와 같은 마이그레이션은 보안 커뮤니티가 따라잡을 수 없을 만큼 빠르게 진행되었습니다. 지난 한 해 동안 Microsoft에서는 전통적인 IT 장비에서 OT(운영 기술) 컨트롤러 또는 간단한 IoT(사물 인터넷) 센서에 이르기까지 조직의 모든 부분에서 디바이스를 악용하는 위협을 발견했습니다. 최근 몇 년 동안 IT 장비의 보안이 강화되었지만 IoT 및 OT 디바이스 보안은 그 속도를 따라잡을 수 없었습니다. 위협 행위자들은 이러한 디바이스를 악용하여 네트워크에 대한 액세스를 구축하고 측면 이동을 지원하거나 대상 조직의 OT 운영을 방해합니다. 전력망에 대한 공격, OT 운영을 방해하는 랜섬웨어 공격, 지속성 향상을 위해 활용되는 IoT 라우터, 펌웨어의 취약점을 표적으로 하는 공격이 있었습니다.

만연한 IoT 및 OT 취약점은 모든 조직에서 해결해야 할 과제이지만, 위협 행위자들이 주요 서비스의 비활성화가 강력한 수단이라는 것을 알았기 때문에 주요 인프라의 위험이 증가하고 있습니다. 2021년, Colonial Pipeline Company를 표적으로 삼은 랜섬웨어 공격은 범죄자들이 몸값을 받을 가능성을 높이기 위해 어떻게 주요 서비스를 방해할 수 있는지를 보여 주었습니다. 그리고 우크라이나에 대한 러시아의 사이버 공격은 일부 국가에서는 주요 기반 시설에 대한 사이버 공격을 국가의 군사 목표를 달성하기 위해 허용 가능한 방해 행위로 보고 있음을 보여줍니다.

그래도 희망은 있습니다. 정책 입안자들과 네트워크 방어자들은 자신들이 의존하는 IoT 및 OT 디바이스를 포함하여 주요 인프라의 사이버 보안을 개선하기 위해 행동하고 있습니다. 정책 입안자들은 주요 인프라 및 디바이스의 사이버 보안에 대한 대중의 신뢰를 구축할 수 있도록 법률 및 규정의 개발을 가속화하고 있습니다.

Microsoft는 전 세계 정부 기관들과 협력하여 이 기회를 통해 사이버 보안을 강화하고 있으며 추가적인 참여를 환영합니다. 그러나 경우에 따라 부족한 보안 리소스를 중복적인 여러 인증을 준수하도록 전환하여 보안을 저하시키는 등 일관성이 없거나 맞춤형이거나 복잡성 높은 요구 사항이 의도하지 않은 영향을 미칠 수 있습니다.

보안 운영 관점에서 네트워크 방어자들은 조직의 IoT/OT 보안 태세를 개선하기 위해 여러 가지 접근 방식을 취합니다. 한 가지 접근 방식은 IoT 및 OT 디바이스의 지속적인 모니터링을 구현하는 것입니다. 또 다른 접근 방식은 IoT 및 OT 디바이스 자체에 대한 더 나은 사이버 보안 관행을 요구하고 구현하는 것을 의미하는 '시프트 레프트'입니다. 세 번째 접근 방식은 IT 및 OT 네트워크를 모두 포괄하는 보안 모니터링 솔루션을 구현하는 것입니다. 이와 같은 총체적인 접근 방식은 OT와 IT 간의 "'사일로 제거'와 같은 중요한 조직 프로세스에 기여하는 상당한 추가적인 이점을 제공하며, 이를 통해 조직은 비즈니스 목표를 달성함과 동시에 강화된 보안 태세에 도달할 수 있습니다.

Michal Braverman-Blumenstyk
클라우드 및 AI 보안 부문 기업 부사장 겸 최고 기술 책임자

주요 인프라 보안 및 회복탄력성을 개선하기 위해 행동에 나서는 정부 기관

전 세계적으로 정부 기관은 주요 인프라 사이버 보안 위험을 관리하기 위한 정책을 개발하고 발전시키고 있습니다. 또한 많은 정부 기관에서 IoT 및 OT 디바이스 보안을 개선하기 위한 정책을 제정하고 있습니다. 전 세계적으로 정책 이니셔티브가 증가함에 따라 사이버 보안을 강화할 수 있는 엄청난 기회가 창출되고 있지만 생태계 전반의 이해관계자에게 문제를 발생시키기도 합니다.

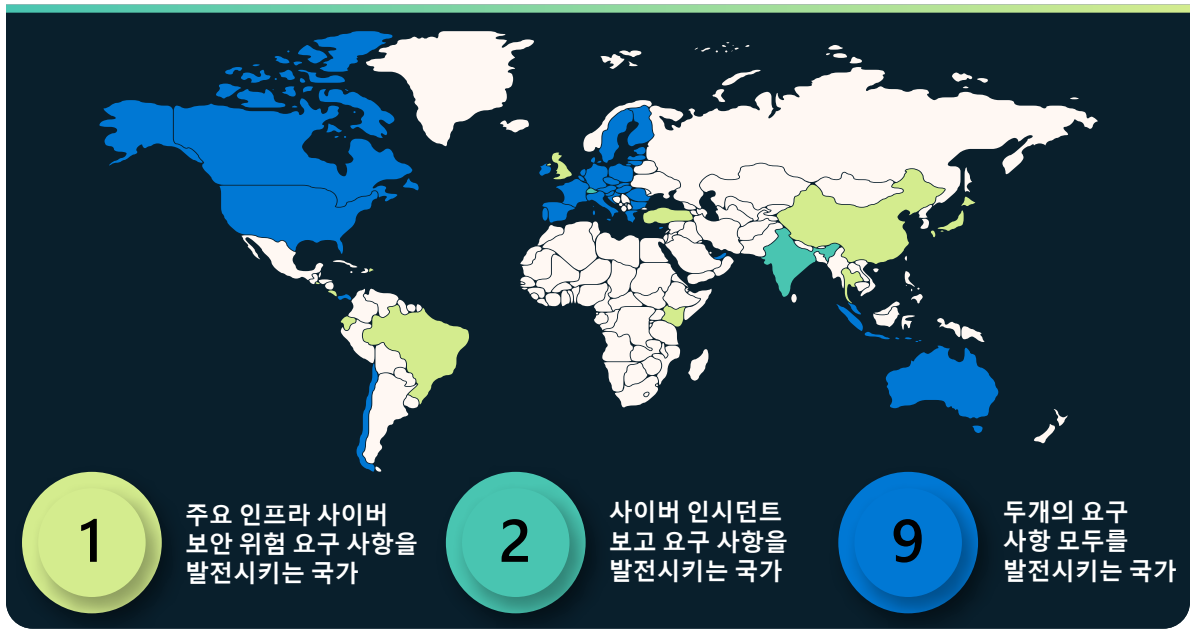
주요 인프라 사이버 위험을 관리하기 위한 총체적인 비전을 개발하는 것은 중요하지만, 특히 기술 및 글로벌 공급업체 간의 상호 연결 정도, 기술 사용 범위, 관련 위험, 장단기 전략에 대한 투자 필요성을 고려하면 복잡해집니다. 반복적인 학습 및 개선을 추진하고 글로벌 부문 간 상호 운용성을 지원하는 효과적인 범위의 정책은 복잡성을 관리하고 보다 보안에 민감한 디지털 트랜스포메이션을 지원하는 데 도움이 될 수 있습니다. 그러나 입법에 대한 단편적인 접근 방식은 중복되고 일관성 없는 규제 요구 사항으로 이어질 수 있습니다. 이는 리소스에 영향을 미치고 궁극적으로 보안 목표를 훼손할 수 있습니다. 예를 들어, 조직은 리소스를 혁신과 보안에서 형식주의적 규정 준수 연습으로 전환할 수 있습니다.

Microsoft는 전 세계 정부 기관과 협력하여 효과적인 주요 인프라 사이버 보안 정책을 추구하고, 해결 과제 및 기회에 대한 이해를 높이고, 집단적 위험 태세를 강화하기 위한 노력을 지원하고자 합니다.

주요 인프라 사이버 보안 위험 관리의 정책 개발

작년 한 해 동안 호주, 칠레, EU(유럽 연합), 일본, 싱가포르, UK(영국), 미국을 포함한 여러 관할 구역에서 교차 부문 또는 부문별 사이버 보안 요구 사항을 개발, 업데이트 또는 구현했습니다.[1] 이들 중 다수의 정부 기관, 그리고 인도[2] 및 스위스[3]와 같은 기타 정부 기관들은 주요 인프라 및 필수 서비스 제공자에 대한 사이버 보안 인시던트 보고 요구 사항을 이미 발표했거나 개발 중입니다.[4]

작년에 호주, EU, 인도네시아, 미국에서 몇 가지 주목할 만한 정책 발전이 이뤄졌습니다. 호주는 부문 간 주요 인프라 사이버 보안 위험을 관리하는 데 도움이 되는 두 가지 법률을 제정했습니다. 이 법률은 무엇보다도 새로운 주요 인프라 부문을 지정하고, 위험 관리 계획의 개발을 요구하고, 사이버 보안 인시던트 보고를 의무화하고, 주요 인프라 운영자가 인시던트에 적절하게 대응할 의사가 없거나 적절하게 대응할 수 없다고 판단되는 경우 정부 기관에서 개입할 수 있는 권한을 부여합니다.



EU는 2016년 NIS 지침을 업데이트하기 위해 노력했습니다. 이 지침은 EU 회원국이 경제와 사회 기능에 중요한 것으로 간주되는 기술 서비스 및 제품을 규제할 수 있는 프레임워크를 제공합니다. 제안된 NIS 2에는 주요 디지털 인프라의 새로운 범주를 생성하고, 사이버 인시던트 보고에 대한 요구 사항을 늘리고, 추가 사이버 보안 위험 관리 요구 사항을 부과하는 개정안이 포함되어 있습니다. EU는 또한 금융 서비스 부문에서 사용되는 정보 통신 기술에 대한 새로운 요구 사항을 만드는 DORA(Digital Operational Resilience Act, 디지털 업무 탄력성법)에 대한 업데이트를 제안했습니다.

5월 인도네시아는 에너지, 운송, 금융, 의료와 같은 부문에서 2024년 5월 발효 예정인 'IIV(주요 정보 인프라)' 보호에 관한 대통령 규정을 발표했습니다. 이 규정을 통한 인도네시아의 목표는 IIV 구현의 연속성을 보호하고, 사이버 공격을 방지하며, 사이버 인시던트 처리에 대한 준비를 강화하는 것입니다. IIV 제공자는 안전하고 신뢰할 수 있는 보호를 수행하고, 효과적인 사이버 위험 관리를 구현하고, 사이버 위험 결과를 해당 정부 기관에 보고할 책임이 있습니다. 이 규정에는 사이버 인시던트를 24시간 이내에 보고해야 하는 요구 사항이 포함되어 있습니다.

주요 인프라 보안 및 회복탄력성을 개선하기 위해 행동에 나서는 정부 기관

계속

미국 의회는 CISA(Cybersecurity and Infrastructure Security Agency, 사이버 보안 및 인프라 보안국)가 주요 인프라 운영자로부터 사이버 인시던트 보고를 요구하는 규정을 발행할 수 있는 권한을 부여하는 법률을 통과시켰고, 미국 TSA(Transportation Security Administration, 교통 안전국)는 운송 부문의 새로운 부문별 사이버 보안 요구 사항을 발표했습니다. 2021년 TSA는 Colonial Pipeline Company를 표적으로 삼은 랜섬웨어 공격에 대응하여 유해 액체 및 천연가스 파이프라인 운영자에게 두 가지 보안 지침을 발표했습니다.

- 첫 번째 지침은 운영자가 사이버 보안 코디네이터를 지정하고, 12시간 이내에 사이버 인시던트를 보고하며, 시스템의 취약성 평가를 수행하도록 요구하는 것입니다.
- TSA가 2022년에 개정한 두 번째 지침은 운영자가 랜섬웨어 공격 및 IT 및 OT 시스템에 대한 기타 알려진 위협으로부터 보호할 수 있는 특정 완화 조치를 구현하고, 30일 이내에 사이버 보안 비상 및 대응 계획을 개발 및 구현하고, 연례 사이버 보안 아키텍처 설계 검토를 거치도록 요구하는 것입니다.

TSA는 파이프라인에 대한 규정을 기반으로 2021년 후반에 화물 철도, 여객 철도 운송업체 또는 철도 운송 시스템에 대한 사이버 보안 요구 사항을 공표하는 두 가지 추가 보안 지침을 발표했습니다. 이 지침에 따르면 해당 운영자는 사이버 보안 코디네이터를 지정하고, 24시간 이내에 사이버 보안 인시던트를 보고하며, 사이버 보안 인시던트 대응 계획을 개발 및 구현하고, 사이버 보안 취약성 평가를 완료해야 합니다. TSA는 이와 동시에 공항 및 항공사 운영자가 처음 두 조항을 구현하여 코디네이터를 지정하고 24시간 이내에 인시던트를 보고하는 내용의 항공 보안 프로그램 업데이트를 발표했습니다.

IoT 및 OT 디바이스 보안의 정책 개발

수십 개 국가에서 정부 기관은 IoT 및 OT 디바이스를 포함한 ICT(정보 통신 기술) 제품 및 서비스의 사이버 보안을 발전시키기 위한 요구 사항을 적극적으로 개발하고 있습니다. ICT 제품 및 서비스의 맥락에서 가장 큰 관심사는 소프트웨어 공급망 보안 및 IoT 보안입니다.

- 유럽연합 집행위원회는 독립형 소프트웨어, 커넥티드 디바이스, 보조 서비스에 대한 사이버 보안 요구 사항을 설정하는 Cyber Resilience Act(사이버 회복탄력성법)를 제안했습니다.[5] 소프트웨어 공급업체에 대한 관련 관행으로는 안전한 소프트웨어 개발 수명 주기 활용[6] 및 SBOM(Software Bill of Materials, 소프트웨어 제품 명세서) 제공이 있습니다.[7] 새로운 보안 요구 사항은 커넥티드 디바이스에 적용되며 모든 제조업체는 릴리스된 제품에 대해 조정된 취약점 공개[8] 프로세스를 관리해야 합니다.

정책 입안자들은 또한 IoT 디바이스 및 네트워크 OT 디바이스의 지속적인 확산에 관심을 집중했습니다.

- 영국의 Product Security and Telecommunications Infrastructure Bill(제품 보안 및 통신 인프라 법) 초안은 스마트 TV와 같은 소비자와 연결 가능한 제품의 제조업체가 사이버 범죄자의 쉬운 표적이 되는 기본적인 암호 사용을 중단하고, 취약점 공개 정책(예: 보안 결함에 대한 통지를 받는 방법)을 수립하며, 보안 업데이트를 제공하는 최소 기간에 대한 투명성을 제공하도록 요구합니다.[9]
- EU에서는 무선 디바이스에 적용되고, 네트워크 회복탄력성 개선, 소비자 개인 정보 보호, 금전적 사기 위험 절감 방법을 모색하는 라디오 장비 지침에 위임된 법률을 비롯하여 여러 입법 도구를 통해 새로운 보안 표준 또는 요구 사항이 구현되고 있습니다.[10] 또한 2019 EU 사이버 보안법[12]의 결과로 현재 개발 중인 클라우드 인증 체제[11]를 사용해야 할 수도 있습니다.

일관성의 필요성

대부분의 경우 지역, 부문, 기술, 운영적 위험 관리 영역 간의 활동 범위가 동시에 추구되고 있기 때문에 지침을 활용하거나 규정 준수를 입증하려는 조직의 범위, 요구 사항, 복잡성이 중복되거나 불일치할 수 있습니다. IoT에 대해 보편적으로 인정되는 정의가 없으면 IoT 및 OT 디바이스 규정에서 범위를 정하기란 특히 어렵습니다. 앞서 언급된 사례는 '커넥티드 제품 및 보조 서비스', '소비자와 연결 가능한 제품', '무선 디바이스'에 적용될 수 있습니다. 이와 동시에 수많은 정부 기관은 조직과 제품이 현재 요구 사항, 새롭게 떠오르는 요구 사항, 진화하는 요구 사항을 충족하는지 여부와 방법에 대한 이해도를 높이기 위해 보다 강력한 평가 체제를 구현하는 것을 목표로 합니다. 이러한 추세가 합쳐짐에 따라 더욱 복잡해집니다. 고무적으로 EU 사이버 회복탄력성법 협의 도중 제기된 질문은 새로운 규정이 기존 사이버 보안 규정과 잠재적으로 상호 작용할 수 있는 방법을 탐구하여 충돌하는 사이버 보안 요구 사항을 피하려는 의도를 나타냅니다.

위험 기반 및 결과 또는 프로세스 지향적(구현별 대비) 반복되는 접근 방식은 사이버 보안을 강화하고 지속적인 개선을 촉진할 수 있습니다. 이와 마찬가지로 부문, 지역, 정책 영역 간의 상호 운용성을 지원하는 데 중점을 두면 상호 연결된 글로벌 공급망 전반에 걸쳐 사이버 보안을 지속적으로 높일 수 있습니다.

주요 인프라 보안 및 회복탄력성을 개선하기 위해 행동에 나서는 정부 기관

계속

지역, 부문, 주제 영역에 걸쳐 개발 중인 주요 인프라 사이버 보안 정책이 점점 더 복잡해지고 있습니다. 이로 인해 큰 기회와 중요한 해결 과제가 발생됩니다. 정부 기관의 진행 방식은 디지털 트랜스포메이션과 생태계 전반적인 보안의 미래에 매우 중요합니다.

소프트웨어 공급망 보안 및 제로 트러스트 아키텍처에 대한 생태계 전반의 투자 가속화

사이버 보안 개선에 관한 미국 EO(Executive Order, 행정 명령) 14028은 자체 및 생태계 전반의 공급망 보안에 투자하고 고객이 제로 트러스트 목표를 달성할 수 있도록 지원하기 위한 Microsoft의 지속적인 이니셔티브를 신속하게 처리하는 촉매제 역할을 했습니다.

Microsoft는 소프트웨어 공급망을 개선하려면 약 15년 전 공개적으로 릴리스했던 Microsoft의 보안 개발 수명 주기를 시작으로 학습 내용 및 모범 사례를 공유해야 한다고 오랫동안 믿어왔습니다.

또한 미국의 국립 사이버 보안 혁신 센터와 긴밀히 협력하여 온-프레미스 및 클라우드 기술 모두에 적용되는 제로 트러스트 아키텍처에 대한 접근 방식을 시연하고 하이브리드 및 멀티클라우드 환경에 피싱 방지 인증을 적용하는 기능을 비롯하여 새로운 제품 기능을 구축하고 있습니다.

오늘날 Microsoft는 EO의 요구 사항을 넘어 소프트웨어 공급망 보안 요구 사항을 준수함을 입증하고 두 가지 방법으로 SBOM(소프트웨어 제품 명세서) 정보를 제공하고 있습니다.

1. 첫째, Windows, Linux, Mac, iOS, Android 플랫폼에서의 구축을 지원하는 CI/CD 파이프라인과 쉽게 통합되도록 구축한 SBOM 생성기 도구의 오픈 소스 버전을 공유하고 있습니다.[13]
2. 둘째, SCITT(Supply Chain Integrity, Transparency, and Trust, 공급망 무결성, 투명성, 신뢰성)에 대한 산업 표준 개발에 기여하고 있습니다. 이를 통해 EO의 소프트웨어 공급망 지침에서 비롯된 요구 사항을 준수함을 입증하는 아티팩트를 포함하여 검증 가능한 공급망 정보를 자동으로 교환할 수 있습니다.

실행 가능한 인사이트

1. 다자간 기관은 국가 차원의 사이버 공격에 대한 긴급한 문제를 해결하기 위해 재구상되어야 합니다.
2. 지역, 부문, 주제 영역 간에 일관적이고 상호 운용 가능한 사이버 보안 정책을 개발합니다.

추가 정보에 대한 링크

- 사이버 보안을 지원하는 공급망 보안에 대한 지속적인 투자 행정 명령 | Microsoft 기술 커뮤니티
- 제로 트러스트 아키텍처 전략 및 요구 사항을 제시하는 미국 정부 기관 | Microsoft Security 블로그
- 사이버 EO | Microsoft Federal
- 공급망 무결성, 투명성, 신뢰성 | github.com
- 제로 트러스트 아키텍처 구현 | NCCoE(nist.gov)

IoT 및 OT 노출: 동향 및 공격

점점 더 연결되는 디지털 세계는 디바이스가 빠르게 온라인으로 연결되고, 대형 시스템과 커뮤니케이션하며, 데이터를 수집하고, 이전에는 모호했던 공간에서 가시성을 창출한다는 것을 의미합니다. 이는 조직과 위협 행위자 모두에게 기회를 제공하며, 사이버 범죄 비즈니스는 미화 수십억 달러 규모의 산업이자 위험이 됩니다.

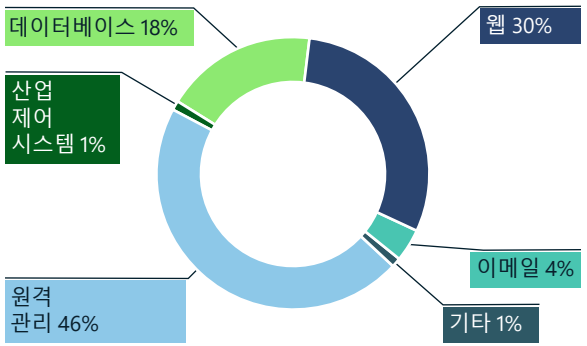
프린터에서 웹 카메라, 실내 온도 조절 디바이스 및 건물 액세스 제어에 이르기까지 모든 것을 포함하는 IoT 디바이스는 개인, 조직, 네트워크에 고유한 보안 위험을 초래합니다. 수많은 조직 운영 시, 중요한 역할을 하지만 빠르게 법적 책임 및 보안상 위험이 될 수 있습니다. 거의 모든 산업에서 IoT 솔루션이 빠르게 채택되면서 공격 벡터의 수와 조직의 노출 위험이 증가했습니다.

서비스로서의 맬웨어는 기업 네트워크뿐만 아니라 민간 인프라 및 유틸리티(병원, 석유 및 가스, 전력망, 운송 서비스, 기타 주요 인프라 포함)를 표적으로 하는 대규모 작전으로 이동했습니다. 위협 행위자들은 운영 환경과 임베디드 IoT 및 OT 디바이스의 환경 설정을 발견하고 악용하려면 상당한 연구 노력이 필요합니다.

IoT 디바이스는 네트워크의 진입점 및 피벗 지점으로서 고유한 보안 위험을 내포합니다. 수백만 개의 IoT 디바이스가 패치되지 않거나 노출됩니다.

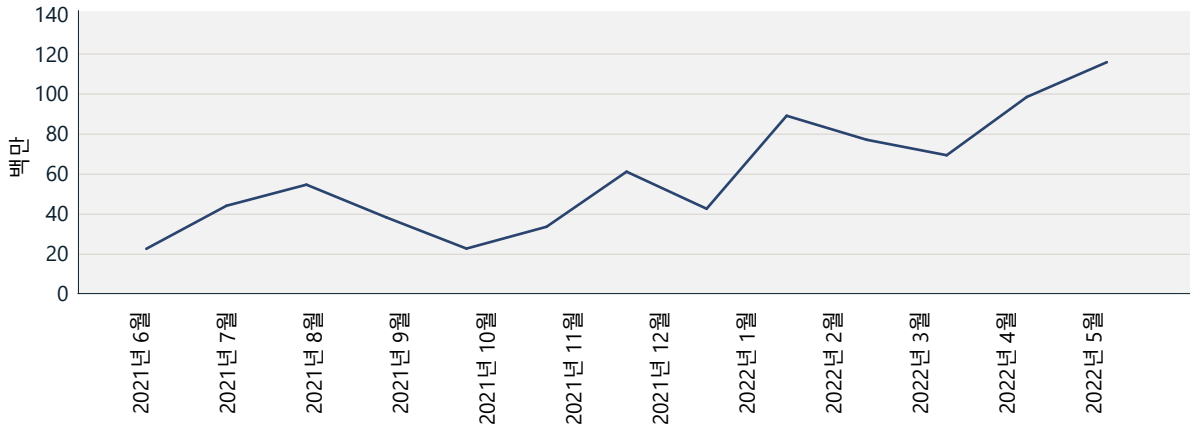
노출된 디바이스는 개방형 네트워크 포트에서 수신 대기하는 서비스를 식별하여 인터넷 검색 도구를 통해 검색할 수 있습니다. 이러한 포트는 일반적으로 디바이스의 원격 관리에 사용됩니다. 올바르게 보호되지 않으면 권한이 없는 사용자가 포트에 원격으로 액세스할 수 있으므로 노출된 IoT 디바이스를 기업 네트워크의 다른 계층으로 전환하는 피벗 포인트로 사용할 수 있습니다. Microsoft는 카메라에서 라우터, 온도 조절기에 이르기까지 인터넷에 노출된 디바이스의 취약점을 악용하려는 다양한 위협 행위자들을 발견했습니다. 그러나 위험이 존재함에도 불구하고 수백만 개의 디바이스가 패치되지 않았거나 노출된 상태로 남아 있습니다.

IoT/OT의 공격 유형 요약



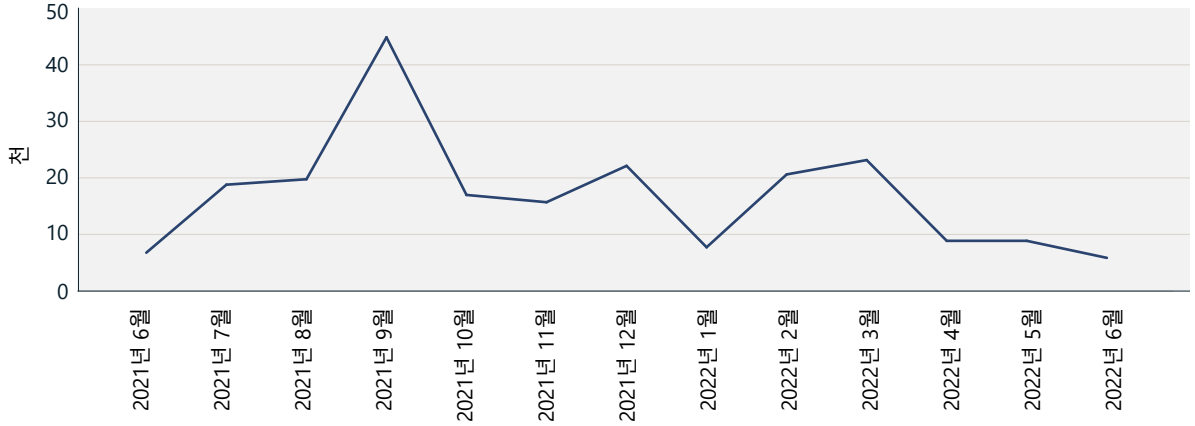
MSTIC 센서 네트워크를 통해 관찰된 공격 유형입니다. 가장 만연한 공격 유형은 원격 관리 디바이스를 표적으로 삼은 공격, 웹을 통한 공격, 데이터베이스를 표적으로 삼은 공격(무차별 암호 대입 또는 악용)이었습니다.

원격 관리 디바이스를 표적으로 삼은 공격



MSTIC 센서 네트워크를 통해 볼 수 있듯이 시간이 지남에 따라 원격 관리 포트에 대한 공격이 증가합니다.

IoT 및 OT를 표적으로 삼은 웹 공격



MSTIC 센서 네트워크를 통해 볼 수 있는, 시간 경과에 따른 웹 공격의 양입니다. 웹에 직접 연결된 디바이스의 수가 계속 감소함에 따라 공격자들은 결국 이를 조사할 가능성이 낮아질 수 있습니다.

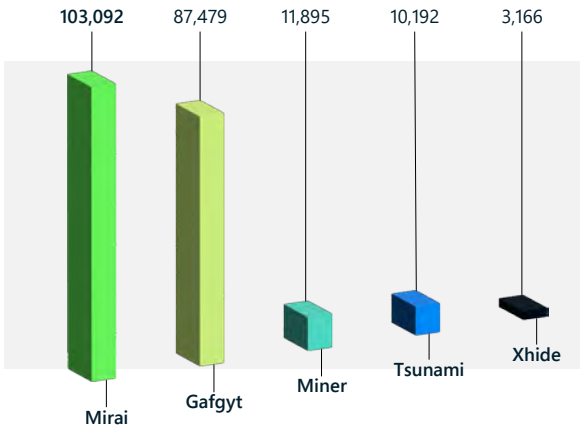
IoT 및 OT 노출: 동향 및 공격

계속

개선된 맬웨어 유틸리티

사이버 범죄 그룹이 진화함에 따라 맬웨어 배포 및 표적 선택지 역시 발전했습니다. 작년에 Telnet과 같은 일반적인 IoT 프로토콜을 표적으로 삼은 공격이 크게 감소했는데, 경우에 따라 60%까지 감소했습니다. 이와 동시에, 봇넷은 사이버 범죄 그룹과 국가 차원의 공격자들에 의해 용도가 변경되었습니다. Mirai와 같은 맬웨어의 지속성은 이러한 공격의 모듈성과 기존 위협의 적응성을 강조합니다.

실제 환경에서 탐지된 최고 IoT 맬웨어



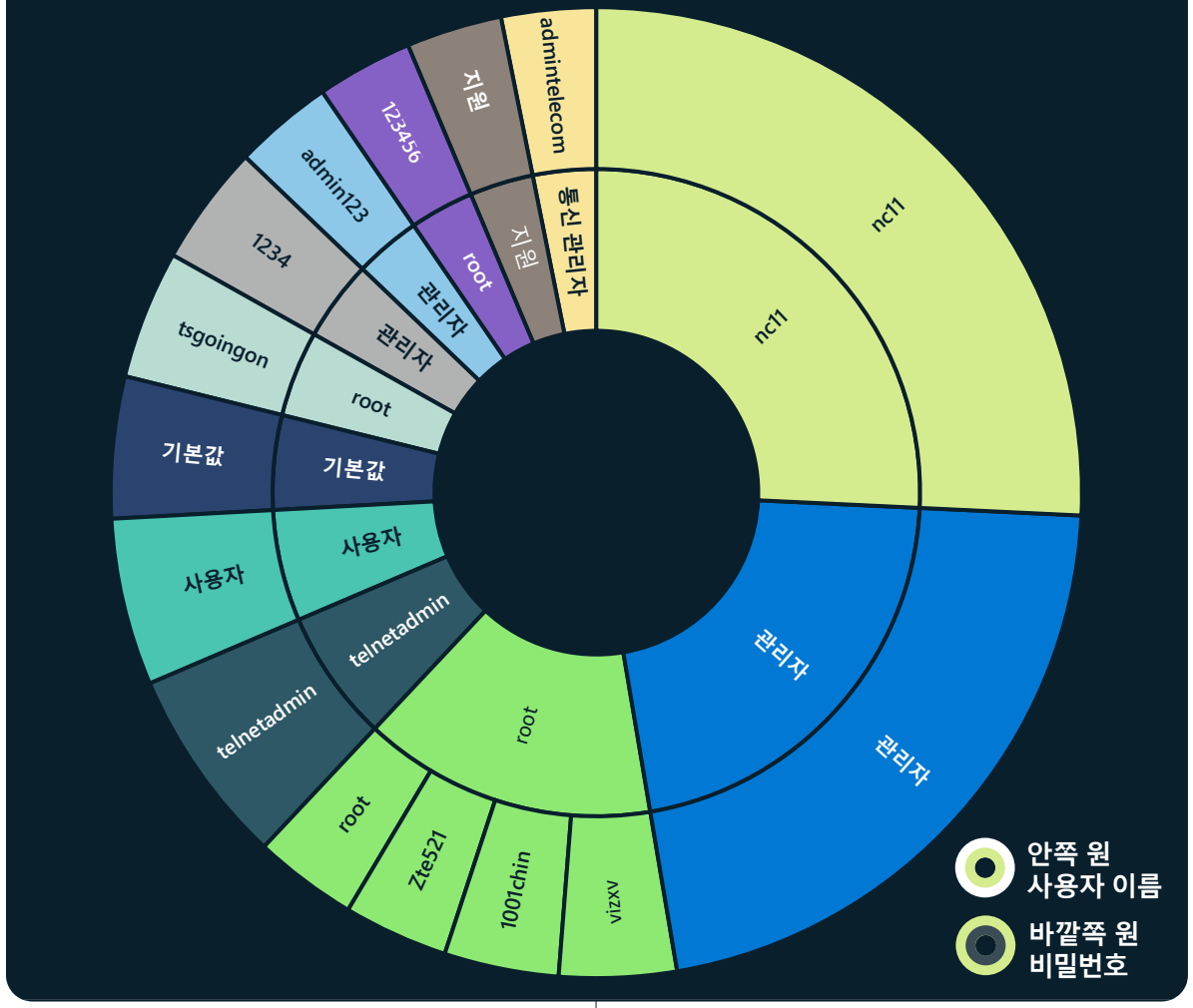
Mirai는 인터넷 프로토콜 카메라, 보안 카메라 디지털 비디오 레코더, 라우터를 비롯하여 광범위한 IoT 디바이스를 감염시키기 위해 진화했습니다. 보안 제어를 우회한 공격 벡터는 추가 취약점을 악용하고 측면으로 이동하여 네트워크 내 엔드포인트를 제어하고 위험을 초래합니다. Mirai는 다양한 아키텍처에 적응하고 알려진 취약점과 제로 데이 취약점을 모두 악용하여 새로운 공격 벡터를 손상시키는 변종을 통해 여러 번 재설계되었습니다.

Mirai의 사용은 지난 한 해 동안 32비트 및 64비트 x86 CPU 아키텍처에서 모두 증가했으며 맬웨어에는 국가 및 범죄 집단에서 빠르게 채택한 새로운 기능을 부여받았습니다. 국가 차원의 공격자들은 현재 외국 적을 표적으로 삼은 DDoS(서비스 분산 거부) 공격 시, 기존 봇넷의 새로운 변종을 활용합니다.

2022년 IoT 디바이스를 표적으로 삼은 공격 수익이 감소함에 따라 Microsoft에서는 Log4j 및 Spring4Shell과 같은 취약점을 악용하여 서버 등의 디바이스에 악성 페이로드를 전달하고 DDoS 공격을 수행하는 대형 봇넷으로 감염 및 모집하는 여러 위협 행위자 그룹을 발견했습니다. 취약한 IoT 디바이스를 대상으로 설계된 맬웨어의 개선된 유틸리티는 측면 이동이 네트워크의 추가 페이로드 및 기타 디바이스에 백도어를 노출시킬 수 있기 때문에 조직과 국가 모두에 심각한 영향을 미칩니다.

다양한 산업 제어 시스템 프로토콜은 모니터링되지 않으므로 OT 관련 공격에 취약합니다. 이는 주요 인프라에 대한 위험이 증가한다는 것을 의미할 수 있습니다.

45일간의 센서 신호를 통해 IoT/OT 디바이스에서 확인된 사용자 이름 및 암호 쌍의 상대적 보급률



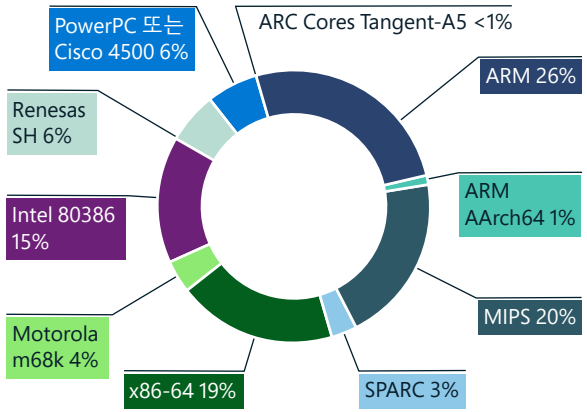
일반적인 사용자 이름 및 비밀번호 페어링을 사용하면 침해 위험이 높아집니다. 3,900만 개 이상의 IoT 및 OT 디바이스의 샘플 크기를 기준으로 동일한 사용자 이름과 비밀번호를 사용하는 디바이스는 약 20%를 차지했습니다.

IoT 및 OT 노출: 동향 및 공격

계속

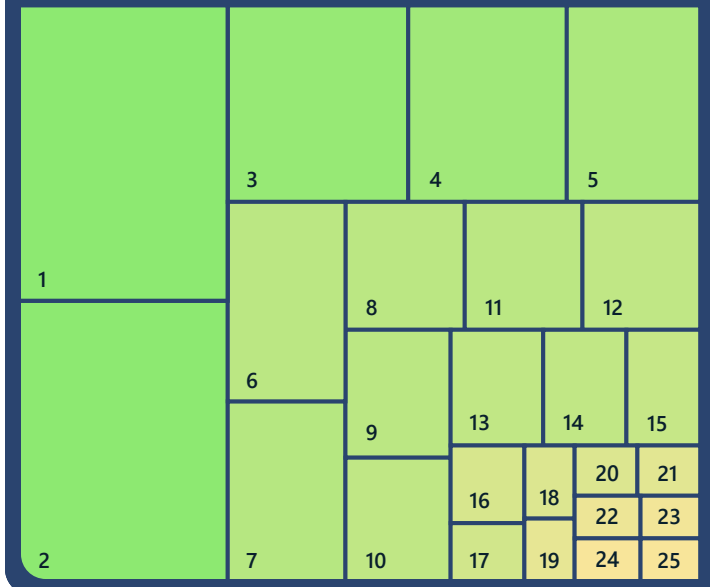
취약한 환경 설정 및 기본 개인 인증 정보는 여전히 네트워크에 위험을 초래하지만 Microsoft는 HTTP를 활용하는 많은 웹 기반 악용을 관찰했습니다. 레거시 봇넷을 활용하는 웹 기반 서비스에 대한 공격이 증가하는 것을 발견했습니다. 한편, 인터넷에서 개방형 텔넷 포트의 수가 감소했는데, 이는 역사적으로 디바이스에 위험을 초래한 봇넷이 관련성을 잃고 있기 때문에 네트워크 보안에 긍정적인 신호입니다. 이처럼 개방형 텔넷 포트의 감소에도 불구하고 여전히 센서 네트워크에서 지속적인 봇넷을 발견했습니다.

CPU 아키텍처에 의한 IoT 악성코드 배포



Microsoft에서 관찰한 바에 따르면, 맬웨어는 ARM에서 실행되는 IoT 디바이스를 표적으로 삼는 경우가 가장 많으며 그다음으로 MIPS, X86-64, Intel 80386 CPU가 그 뒤를 이었습니다.

산업 제어 시스템 프로토콜 보급



1. EtherNet/IP
2. MODBUS
3. BACNet
4. Siemens S7
5. Profinet Real-Time
6. Profinet DCP
7. Siemens S7 Plus
8. CodeSys
9. Siemens WinCC Agent
10. EtherNet/IP O/O
11. Honeywell Control Data Access
12. MMS
13. IEC-60870
14. Honeywell FDA Diagnostics
15. Suitelink
16. DeltaV
17. GSM
18. DNP3
19. AMS
20. SRTP
21. TwinCat
22. Emerson Roc
23. Bently Nevada
24. Mitsubishi MELSEC
25. TriStation Tricon

산업 제어 시스템 프로토콜 취약점

Microsoft는 자체 클라우드 연결 센서의 OT 데이터를 조사하여 가장 일반적인 ICS(산업 제어 시스템) 프로토콜을 확인했습니다. 이러한 프로토콜은 이러한 디바이스의 특성과 공격 표면에 대한 인사이트를 제공합니다. 이는 특히 주요 인프라의 보안과 관련이 있습니다. 일부 주요 학습 사항은 다음과 같습니다.

1. 표시된 대부분의 프로토콜은 독점적이므로 표준 IT 모니터링 도구는 이러한 디바이스 및 프로토콜에 대한 적절한 보안 가시성을 갖지 못합니다. 그 결과, 네트워크가 모니터링되지 않으므로 OT 관련 공격에 더 취약합니다.
2. 다양한 공급업체별 프로토콜이 있습니다. 이는 공급업체별 보안 솔루션이 전체 네트워크를 적절하게 커버할 수 없음을 의미합니다. Microsoft는 다양한 디바이스에 대한 보안 범위를 제공하기 위해 공급업체에 구애받지 않는 접근 방식을 우선시합니다.
3. 조직은 이러한 프로토콜이 네트워크에서 인터넷에 직접 노출되지 않도록 해야 합니다. 이러한 노출은 취약점과 해당 프로토콜의 안전하지 않은 특성으로 인해 주요 보안 위험을 초래할 수 있습니다.

Mirai와 같은 맬웨어는 새로운 기능을 개발하여 지속되며 사이버 범죄 그룹 및 국가 차원의 공격자들이 채택하여 외국 적에 대한 DDoS 공격 시, 기존 봇넷의 새로운 변종을 활용합니다.

실행 가능한 인사이트

1. 패치를 적용하고, 기본 암호를 변경하며, 기본 SSH 포트를 변경하여 디바이스가 강력한지 확인합니다.
2. 불필요한 인터넷 연결 및 개방형 포트를 없애고, 포트 차단, 원격 액세스 거부, VPN 서비스 활용을 통해 공격 표면을 줄입니다.
3. IoT/OT 인식 NDR(네트워크 탐지 및 대응) 솔루션과 SIEM(보안 정보 및 이벤트 관리)/SOAR(보안 오케스트레이션 및 대응) 솔루션을 사용하여 친숙하지 않은 호스트와의 커뮤니케이션 등의 비정상적이거나 권한 없는 동작이 있는지 디바이스를 모니터링합니다.
4. 네트워크를 분할하여 공격자가 측면으로 이동하고 초기 침해 후 자산을 손상시키는 역량을 제한합니다. IoT 디바이스와 OT 네트워크는 방화벽을 통해 회사 IT 네트워크로부터 격리해야 합니다.
5. ICS 프로토콜이 인터넷에 직접 노출되지 않도록 합니다.

공급망 및 펌웨어 해킹

인터넷에 연결된 거의 모든 디바이스에는 디바이스의 하드웨어 또는 회로 기판에 내장된 소프트웨어인 펌웨어가 있습니다. 지난 몇 년 동안 파괴적인 공격을 시작하기 위해 펌웨어를 표적으로 삼는 경우가 많아졌습니다. 펌웨어는 위협 행위자들의 가치가 큰 표적이 될 가능성이 높기 때문에 조직은 펌웨어 해킹으로부터 보호해야 합니다.

펌웨어는 네트워크 연결 또는 데이터 저장과 같은 주요 디바이스 기능을 담당합니다. 펌웨어는 주요 인프라에서 사용되는 산업 제어 장비(OT)와 함께 기업에서 사용되는 라우터, 카메라, 텔레비전, 기타 디바이스(IoT)에서 찾을 수 있습니다. 역사적으로 펌웨어는 안전하지 않은 코드로 작성되어 디바이스를 장악하거나 펌웨어에 악성 코드를 주입하는 데 악용될 수 있는 심각한 취약점을 생성했습니다.

이러한 위험은 공급망과 관련되면 더욱 복잡해집니다. 대부분의 디바이스는 수많은 제조업체의 소프트웨어 및 하드웨어 구성 요소와 오픈 소스 라이브러리를 활용하여 구축됩니다. 대부분의 경우, 디바이스 운영자는 네트워크 내 디바이스의 공급망 위험을 평가할 수 있는 H/SBOM(하드웨어 및 소프트웨어 재료 명세서)에 대한 가시성이 없습니다. 2020년 6월, 소비자 및 산업 장비 공간에서 수억 개의 IoT 디바이스에 영향을 미치는 다양한 제조업체에서 사용하는 네트워킹 스택에서 취약점이 발견되었습니다.[14] 경우에 따라 네트워크 스택은 다른 공급업체에 의해 브랜드가 변경되었으며 디바이스가 취약하다는 표시가 없었습니다. IoT/OT 디바이스의 해당 소프트웨어 및 하드웨어 공급망을 표적으로 삼아 조직을 침해하는 악의적인 행위자의 위협이 증가하고 있습니다.

펌웨어 업데이트 프로세스는 디바이스마다 크게 다르며 이를 수행하는 복잡성과 물류 관련 어려움은 업데이트 빈도에 영향을 미칩니다. 디바이스가 최신 펌웨어를 실행 중인지 항상 확인할 수 있지 않기 때문에 보안 전문가들이 IoT 및 OT 디바이스의 보안 상태를 모니터링하고 확인하기가 어렵습니다. 뿐만 아니라, 일부 디바이스에는 암호로 서명되지 않은 펌웨어가 있어 사용자의 확인 없이도 업데이트할 수 있습니다. 이러한 취약점은 생산 및 유통 체인 전반에 걸쳐 디바이스를 공급망 공격에 더욱 노출시킵니다.

이러한 위협을 해결하기 위해 Microsoft는 펌웨어가 공급망의 여러 단계를 통과할 때 펌웨어의 보안성 및 무결성을 보장하고 수집 또는 그 과정 중에 변조되지 않았다는 사실을 언제든지 증명하기 위해 상당한 투자를 하고 있습니다. 이를 통해 각 파이프라인 세그먼트 간의 신뢰를 검증하고 고객에게 배송하는 모든 구성 요소에 대해 인증되고 입증 가능한 엔드 투 엔드 관리 체인을 제공할 수 있습니다. Microsoft는 파트너와 협력하여 이 칩-클라우드 보안을 기업 및 OT 네트워크의 모든 디바이스에 제공하고 있습니다.

"ICT 인프라 공급업체는 단일 공격을 광범위하게 복제할 수 있기 때문에 점점 더 표적이 되고 있습니다. 이와 동시에, 공급망 보안 및 회복탄력성에 대한 국제 법률, 규정, 고객 요구가 증가하고 있으며, 이러한 요구 사항은 다양한 경우가 많습니다.

해결책은 파트너십입니다. Microsoft는 공급업체 및 전 세계 정부 기관과 함께 공급망 생태계 전반에서 고객 및 규제 기관의 요구 사항을 능가하는 보안 문제를 해결하기 위해 최선을 다하고 있습니다. 이를 위해, Microsoft는 공급망 전체에 유연하게 배포되는 보안 및 운영 회복탄력성에 대한 포괄적인 접근 방식을 추진하고 있습니다.

설계에서 디바이스 운영에 이르기까지 펌웨어 무결성을 높이는 것이 Microsoft의 집단적 접근 방식의 핵심입니다. 공급업체의 SDL 프로세스를 보장하고 하드웨어 신뢰점 혁신을 배포하는 것은 공급망 무결성을 '구축'할 수 있는 방법의 예입니다.

Microsoft 커뮤니티는 지속적인 모니터링 및 이상 탐지와 새로운 변조 방지 기술 및 암호화 메커니즘을 결합한 공동 연구 개발을 활용하고 있습니다. 다 함께 공격 표면으로서 공급망의 매력을 최소화하기 위해 노력하고 있습니다."

Edna Conway,
클라우드 인프라 부문 부사장 겸 보안 및 위험 책임자

펌웨어 취약점에 대한 집중 조명

공격자들은 IoT 디바이스 펌웨어의 취약점을 점점 더 활용하여 기업 네트워크에 침투하고 있습니다. XDR 에이전트를 사용하여 약점을 식별하는 전통적인 IT 엔드포인트와 달리 IoT/OT 디바이스 내 취약점 식별은 훨씬 더 어렵습니다.

Microsoft 및 Ponemon Institute에서 최근 진행한 한 설문 조사는 기업에서의 IoT/OT 디바이스의 기회와 해결 과제를 모두 강조합니다.[15] 응답자 중 68%는 IoT/OT의 채택이 전략적 디지털 트랜스포메이션에 중요하다고 생각하는 반면, 60%는 IoT/OT 보안이 IT/OT 인프라에서 가장 안전하지 않은 측면 중 하나라고 인식하고 있습니다.

IoT 디바이스 펌웨어의 취약점을 활용하여 네트워크에 침투하는 공격자의 한 예로는 Mikrotik 라우터[16]의 기본 비밀번호와 취약점을 활용하여 기업 방어 시스템을 우회하는 Trickbot 트로이 목마가 있습니다. IoT 디바이스 펌웨어의 근본적인 과제는 디바이스의 보안 상태 및 취약점에 대한 가시성이 부족하다는 것입니다.

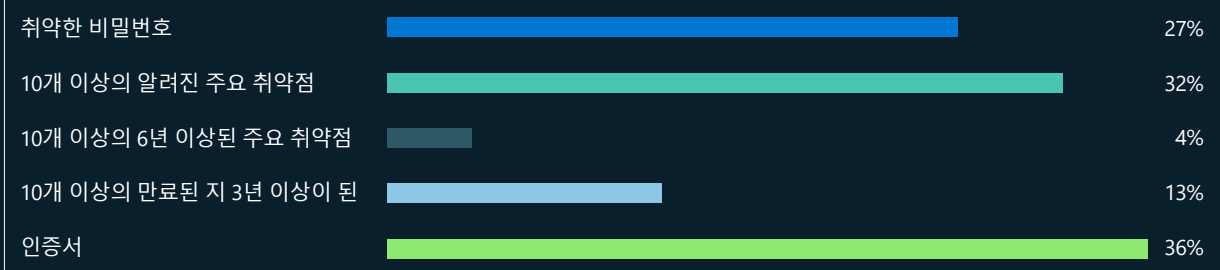
안전한 디바이스를 구축하는 데 사용할 수 있는 솔루션이 있지만 이미 수십억 개의 디바이스가 시장에 출시되고 기업에 배포되었습니다. 이를 브라운필드 디바이스라고 합니다. 2021년 Microsoft는 ReFirm Labs를 인수하여 브라운필드 디바이스 보안을 조명하고 디바이스 빌더가 제품의 보안을 개선할 수 있도록 지원했습니다. ReFirm Labs는 디바이스의 바이너리 펌웨어 이미지를 분석하고 잠재적인 보안 취약점에 대한 자세한 보고서를 생성합니다.[17] 이 기술은 Microsoft Defender for IoT의 향후 릴리스에 통합될 예정입니다.

지난 한 해 동안 Microsoft에서는 고객이 스캔한 고유한 펌웨어의 집계 결과를 조사했습니다. 발견된 모든 약점이 악용될 수 있는 것은 아니지만 이러한 조사 결과는 디바이스 펌웨어 보안의 근본적인 문제를 강조합니다.

IoT/OT 디바이스에 존재하는 약점 유형은 전통적인 Windows 또는 Linux 엔드포인트에서 절대 허용되지 않습니다.

- 취약한 암호: 스캔된 펌웨어 이미지 중 27%에는 취약한 알고리즘(MD5/DES)을 사용하여 인코딩된 암호가 포함된 계정이 포함되어 있는데, 이는 공격자가 쉽게 침해할 수 있습니다.

분석된 펌웨어 이미지의 보안 취약점



- 알려진 취약점: 다른 시스템과 마찬가지로 IoT/OT 디바이스 펌웨어는 오픈 소스 라이브러리를 광범위하게 활용했습니다. 하지만, 디바이스는 이러한 구성 요소의 오래된 버전으로 제공되는 경우가 많습니다. Microsoft의 분석에 따르면 이미지 중 32%에는 중요(9.0 이상)로 평가된 알려진 취약점(CVE)이 10개 이상 포함되어 있습니다. 4%는 6년 이상 된 치명적인 취약점을 10개 이상 포함하고 있었습니다.
- 만료된 인증서: 인증서는 연결과 ID를 인증할 뿐만 아니라, 중요한 데이터를 보호하는 데 사용되지만 분석된 이미지 중 13%에는 3년 이상 전에 만료된 인증서가 10개 이상 포함되어 있습니다.
- 소프트웨어 구성 요소: 이미지 중 36%에는 패킷 캡처 도구(tcpdump, libpcap)와 같이 Microsoft에서 IoT 디바이스 내에서 제외할 것으로 권장하는 소프트웨어 구성 요소가 포함되어 있습니다. 이러한 도구는 공격 체인의 일환으로 네트워크 정찰을 활용할 수 있습니다.

실제 환경에서의 펌웨어 공격

Viasat: 위성 통신을 표적으로 삼기 위해 펌웨어 취약점 사용

2022년 2월, 위성 네트워크 사고가 발생하여 전략적 통신 네트워크의 연결이 끊어짐에 따라 유럽 전역에 영향을 미쳤습니다. Viasat의 KA-SAT 시스템은 많은 양의 트래픽을 수신하여 수많은 모뎀의 연결을 끊었고 네트워크에 대한 서비스 거부 공격이 시작되었습니다. 고정 광대역이 중단됨에 따라 운영자는 수천 개의 풍력 발전용 터빈에 원격으로 액세스할 수 없게 되었고 악성 와이퍼 맬웨어가 영향을 받는 모뎀에 배포되었습니다. 이러한 중단은 통신을 위해 기업과 조직에서 사용하는 30,000개 이상의 위성 단말기에 영향을 미쳤습니다.

Cyclops Blink: 방화벽 게이트웨이를 표적으로 삼기 위해 펌웨어 공급망 공격 사용

위협 행위자들에게 C2(지휘 및 통제)와 공격 인프라의 개발 및 확장은 성공의 중요한 구성 요소입니다. 안정적인 C2 인프라에 대한 필요성이 커짐에 따라 라우터는 패치가 자주 발생하지 않고 포괄적인 보안 솔루션이 없기 때문에 매력적인 공격 벡터가 되었습니다.

Microsoft는 펌웨어 분석 기술과 관련하여 정부 기관 및 업계와 협력하여 디바이스 보안에 대한 심층적인 가시성을 제공하고 디바이스 빌더 및 운영자에게 전체 수명 주기 보안을 제공하고 있습니다.

2019년 6월부터 국가와 연계된 APT(Advanced Persistent Threat, 지능형 지속공격) 그룹은 모듈식 맬웨어 Cyclops Blink를 사용하여 악성 펌웨어 업데이트를 실행하고 대형 봇넷에 모집하여 취약한 WatchGuard 방화벽 디바이스와 ASUS 라우터를 표적으로 삼았습니다. 맬웨어는 권한 상승을 허용하는, 알려진 취약성을 악용하여 디바이스를 성공적으로 감염시켜 위협 행위자들이 디바이스를 관리할 수 있도록 합니다. 일단 감염되면 맬웨어는 추가 모듈을 설치할 수 있도록 허용하고 펌웨어 업데이트를 회피합니다. 다른 WatchGuard 디바이스에서 호스팅되는 C2 서버에 연결하는, 침해된 디바이스가 발견되었습니다. 다양한 TCP 포트에서 C2에 수많은 SSL 인증서를 발급하는 Cyclops Blink 운영자는 악성 펌웨어 업데이트를 실행하고 스캔과 같은 전통적인 보안 방법을 회피하여 네트워크에 대한 원격 액세스 권한을 얻었습니다.

Microsoft가 공급망 보안을 개선하는 방법

Microsoft는 이러한 IoT 및 OT 디바이스 보안 문제를 해결하기 위해 정부 기관 및 업계와 협력하고 있습니다(66페이지의 토론 참조). 이러한 기여로는 펌웨어 분석 기술을 활용하여 디바이스 운영자에게 네트워크에 있는 디바이스의 보안 상태에 대한 가시성을 제공하는 것이 있습니다. 이를 통해 고객은 추가 보호, 업그레이드 또는 교체가 필요한 디바이스를 식별하고 우선순위를 지정할 수 있으며 디바이스 빌더가 디바이스 보안에 투자하도록 수요를 촉진할 수 있습니다. 이와 동시에, 보안 디바이스를 설계하고 보안 개발 수명 주기를 채택할 수 있는 포괄적인 솔루션으로 빌더를 지원하고 있습니다.

또 다른 핵심 구성 요소는 빌더와 운영자에게 보안 문제가 발견되고 해결될 때 디바이스 펌웨어를 업데이트할 수 있는 강력한 인프라를 제공하는 것입니다. Microsoft는 펌웨어 분석 및 Defender for IoT를 IoT Hub용 디바이스 업데이트와 결합하여 IoT 및 OT 디바이스 보안의 전체 수명 주기를 해결하는 솔루션을 제공합니다. 이는 고객이 고객의 IoT 및 OT 솔루션에 대한 제로 트러스트 접근 방식을 지원하는 디바이스를 채택하여 인프라를 보호한다는 비전을 실현하는 데 중요한 단계입니다.[18]

공격자들은 IoT 디바이스 펌웨어의 취약점을 점점 더 표적으로 삼아 기업 네트워크에 침투하고 있습니다.

실행 가능한 인사이트

1. 네트워크에서 IoT/OT 디바이스에 대한 심층적인 가시성을 확보하고 침해된 경우 기업에 대한 위험별로 우선순위를 지정합니다.
2. 펌웨어 스캔 도구를 사용하여 잠재적인 보안 취약점을 이해하고 공급업체와 협력하여 위험도가 높은 디바이스의 위험을 완화하는 방법을 식별합니다.
3. 공급업체에서 안전한 개발 수명 주기 모범 사례를 채택하도록 요구하여 IoT/OT 디바이스의 보안에 긍정적인 영향을 미칩니다.

추가 정보에 대한 링크

- 미국 정보 통신 기술 산업을 지원하는 중요한 공급망 평가

정찰 기반 OT 공격

복잡성 높은 공급망은 특정 설계 정보를 사용하여 실제 시스템을 계획합니다. 이 설계 정보를 구성하는 수많은 자산 중에서 가장 민감한 자산은 환경과 해당 자산을 정의하는 프로젝트 파일입니다. 이 파일은 액세스 권한을 얻고 환경에 완전히 맞춤화된 성공적인 공격을 배포하려는 위협 행위자들에게 중요한 전략적 표적입니다.

운영 프로세스를 중단하기 위해 산업 시스템을 표적으로 삼는 것은 두 단계로 구성됩니다.

1. 먼저 공격자는 OT 네트워크에 액세스해야 합니다. 이는 기업 측 네트워크(Purdue 모델 레벨 4)에 있는 IoT 디바이스를 통해 입력하고 전통적으로 방화벽 및 네트워킹 장비로 분리된 IT-OT 경계를 넘어 운영 및 제어 수준으로 이동하여 수행할 수 있습니다.
2. 둘째, 네트워크 디바이스를 식별해야 합니다. 산업 시스템은 환경에 맞춰 특별히 설계된 사용자 맞춤형 아키텍처의 표준 디바이스 및 구성 요소를 사용합니다. 이러한 표준 디바이스 중 하나는 PLC(프로그래밍 가능한 로직 컨트롤러)입니다. 모든 제조업체는 산업 시스템의 중요한 구성 요소인 PLC를 위한 고유한 인터페이스 및 기능을 개발하며, 이러한 디바이스는 고객의 환경에 맞춰 특별히 설계된 사용자 맞춤형 스키마로 추가 환경 설정됩니다.

각 PLC의 고유한 환경 설정은 환경 및 해당 자산의 정의와 래더 로직 등을 포함하는 프로젝트 파일에 설명되어 있습니다.

분석에 따르면 공격의 증거를 보여 주는 대부분의 환경에서 공격 이전의 타임라인이 공격 자체의 길이를 훨씬 초과합니다. 위협 행위자들은 환경과 해당 자산을 원격으로 시뮬레이션하는 데 수개월을 투자하여 모델을 구성하고 표적 공격을 준비하기 위해 다양한 시도를 하는 경우가 많습니다. 환경이 지속적으로 변화하고 새로운 디바이스를 통합함에 따라 특히 프로젝트 및 환경 설정 파일의 데이터와 관련된 취약점이 발생합니다. 프로젝트 파일을 도난당하면 공격이 몇 주 또는 몇 달이나 앞당겨지고 공격자들은 표적으로 삼은 환경을 빠르고 정확하게 모델링할 수 있기 때문에 악의적인 활동을 탐지하기가 더 어려워집니다.

Industroyer 및 Incontroller

모듈식 맬웨어 및 공격 프레임워크를 활용하여 국가에서 후원하는 공격자들에 의한 조직, 주요 인프라, 정부 기관을 표적으로 삼은 공격은 증가했습니다. 우크라이나에서 주요 작전을 방해하려는 새로운 시도는 표적으로 삼은 환경에 고도로 맞춤화된 정찰 기반 OT 공격에 대한 위협이 증가하고 있다는 사실을 강조합니다. 국가 차원의 사이버 공격자들이 수행하는 확장된 정찰 및 연구 단계는 사이버 전쟁을 활용하여 인프라를 원격으로 무력화하여 혼합 사이버 운동 작전과 정치적 전략에서 특정 전략 또는 운영 목표를 달성하는 전략을 암시합니다.

표적 환경에 고도로 맞춤화된 정찰 기반 OT 공격의 위협이 증가했습니다.

정찰 기반 OT 공격

계속

2022년 초, 두 가지 적응 가능한 치명적인 OT 공격이 확인되었습니다. 우크라이나의 변전소 및 보호 계전기를 표적으로 삼은 사이버 물리적 공격은 2016년 배포 후 우크라이나에서 정전을 일으킨 것으로 알려진 맬웨어인 Industroyer의 변종을 비롯한 맞춤형 맬웨어에서 수행했습니다.

Industroyer2는 새로운 표적에 대해 처음으로 알려진 악성 OT 공격 맬웨어의 첫 번째 재배포입니다. Industroyer용으로 개발된 IEC104 프로토콜(전력 시스템 모니터링 및 제어를 위한 표준 프로토콜) 플러그인을 활용했으며 모델 번호 ABB RTU540/560의 PLC와 유사한 원격 단말기 디바이스를 표적으로 삼았습니다. 이 맬웨어의 작성자는 피해자 환경에 대한 지식을 사용하여 미리 결정된 출력에 반복적으로 명령을 실행하여 수동으로 켤 수 없도록 했습니다. 이로 인해 정전이 더 오래 지속되고 더 큰 피해를 입었습니다.

같은 기간 동안 식별된 모듈식 공격 프레임워크인 Incontroller는 레거시 보안 솔루션을 우회하여 OT 디바이스에 침투하고 공격하는 리드 타임을 크게 줄이는 모듈식 툴킷입니다. 이 범용 툴킷에는 다양한 환경에 맞춰 고도로 사용자 맞춤화할 수 있는 데이터 수집, 정찰, 공격 기능이 있으며 OT 공격에 대한 연구 단계에 큰 영향을 미칠 수 있기 때문에 정찰을 수행하는 데 필요한 시간을 줄이고 디바이스 및 해당 환경 설정에 대한 정보를 추출하여 환경 시뮬레이션을 지원합니다.

Incontroller 프레임워크는 Schneider Electric 및 Omron PLC에 대한 프로토콜을 지원하고 펌웨어 버전, 모델 유형, 커넥티드 디바이스와 같은 정보를 수집합니다. 이 툴킷은 환경 설정을 변경하고 출력을 켜고 끄는 명령을 실행할 수 있습니다. 환경에 액세스하면 프레임워크는 더 많은 페이로드를 전달하기 위해 디바이스에 백도어를 이식하고, 액세스 포인트를 늘리기 위한 취약점을 발행하고, 래더 로직을 업로드하고, DoS 공격을 시작하는 기능을 지원합니다. 툴킷의 일반적인 특성을 통해 위협 행위자는 모든 PLC 또는 위치에 대해 새로운 공격을 작성할 필요 없이 환경을 신속하게 공격할 수 있습니다. 이를 통해 위협 행위자는 잠재적으로 여러 산업에 걸쳐 다양한 유형의 컴퓨터와 쉽게 상호 작용할 수 있습니다.

실행 가능한 인사이트

1. 시스템 정의가 포함된 파일을 안전하지 않은 채널을 통해 전송하거나 필수 인력이 아닌 사람에게 전송하지 않습니다.
2. 이러한 파일을 어쩔 수 없이 전송해야 한다면 네트워크 활동을 모니터링하고 자산이 안전한지 확인합니다.
3. EDR 솔루션을 통해 모니터링하여 엔지니어링 스테이션을 보호합니다.
4. OT 네트워크에 대한 인시던트 대응을 사전에 수행합니다.
5. Defender for IoT와 같이 지속적으로 모니터링을 배포합니다.

미주

1. 참조 예시: NIS2(Network and Information Systems, 네트워크 및 정보 시스템)의 보안에 대한 개정 지침 | 유럽의 디지털 미래 형성(europa.eu), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1, 보안법 개정 (주요 인프라 보호) 법 2022(homeaffairs.gov.au), 칠레: 상원에 도입된 사이버 보안 및 주요 정보 인프라에 대한 법안 | 뉴스 게시물 | DataGuidance, 중요한 기술을 보호하기 위해 경제 안보 법안을 통과시킨 일본 | 재팬타임스, 사이버 보안법 검토 및 CII의 사이버 보안 강령 개정(csa.gov.sg), 영국의 사이버 회복탄력성을 개선하기 위한 법률 제안—GOV.UK(www.gov.uk), 통신 (보안) 법 2021(legislation.gov.uk), NIST 사이버 보안 프레임워크 업데이트—CSF 2.0을 향한 여정 | NIST
2. 인증서—홈 페이지
3. 사이버 공격 신고 의무 도입에 관한 협의 개시(admin.ch)
4. 참조 예시: 제목 없음(house.gov)
5. 사이버 회복탄력성법 | 유럽의 디지털 미래 형성(europa.eu)
6. 참조 예시: Microsoft 보안 개발 수명 주기
7. 참조 예시: Microsoft에서 SPDX로 SBOM(소프트웨어 재료 명세서) 생성—Engineering@Microsoft, SBOM(소프트웨어 재료 명세서)의 최소 요소 | 미국통신정보관리청(ntia.gov)
8. 참조 예시: https://www.microsoft.com/en-us/msrc/cvd
9. PSTI(제품 보안 및 통신 인프라) 법안—제품 보안 팩트시트—GOV.UK(www.gov.uk)
10. 무선 디바이스 및 제품의 사이버 보안을 강화하는 위원회(europa.eu)
11. 클라우드 인증 제도: 유럽 전역에서 신뢰할 수 있는 클라우드 서비스 구축 — ENISA (europa.eu)
12. 인증 — ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool" GitHub - Microsoft/sbom-tool: SBOM 도구는 다양한 아티팩트에 대해 SPDX 2.2 호환 가능한 SBOM을 생성할 수 있는 확장성이 뛰어난 엔터프라이즈급 도구입니다.
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come
15. IoT/OT 혁신은 중요하지만 상당한 위험이 따른다(2021년 12월): 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. C2 인프라에서 Trickbot의 IoT 디바이스 사용에 대해 알아보기(2022년 3월): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. IoT 펌웨어 스캔에 대한 채널 9 에피소드에 대한 IoT 쇼(2022년 5월): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. IoT 솔루션에 제로 트러스트 접근 방식을 적용하는 방법(2021년 5월): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

사이버 영향력 작전

오늘날 외국의 영향력 작전은 새로운 방법과 기술을 활용하여 신뢰를 떨어뜨리도록 설계된 캠페인을 보다 효율적이고 효과적으로 만듭니다.

사이버 영향력 작전

개요

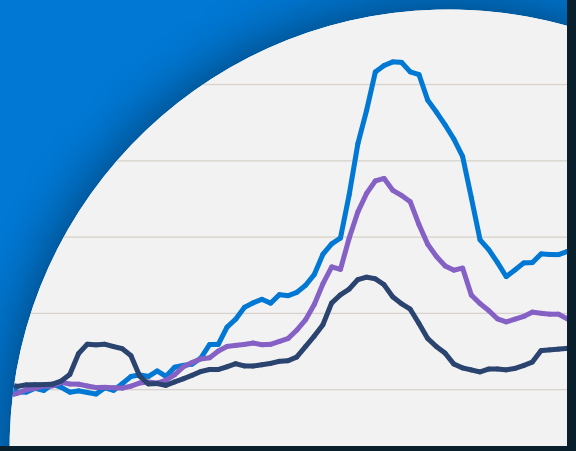
오늘날 외국의 영향력 작전은 새로운 방법과 기술을 활용하여 신뢰를 떨어뜨리도록 설계된 캠페인을 보다 효율적이고 효과적으로 만듭니다.

국가 차원의 공격자들은 선전을 배포하고 국내외 여론에 영향을 미치기 위해 점점 더 정교한 영향력 작전을 많이 사용하고 있습니다. 이러한 캠페인은 신뢰를 침식하고 양극화를 심화하며 민주적 절차를 위협합니다. 숙련된 첨단 지속적 조작 (Advanced Persistent Manipulator) 공격자는 인터넷 및 소셜 미디어와 함께 전통 미디어를 활용하여 캠페인의 범위, 규모, 효율성을 크게 높이고 글로벌 정보 생태계에 미치는 막대한 영향을 크게 높이고 있습니다. 지난 한 해 동안 이러한 작전은 우크라이나에 대한 러시아의 하이브리드 전쟁의 일환으로 사용되는 경우가 많았지만, 러시아와 중국, 이란을 포함한 다른 국가들이 글로벌 영향력으로 확대하기 위해 소셜 미디어로 구동되는 선전 작전을 점점 더 많이 펼쳤습니다.

사이버 영향력 작전은 점점 더 많은 정부 기관과 국가가 이러한 작전을 통해 의견을 형성하고, 적의 신뢰를 떨어뜨리며, 불화를 조장함에 따라 점점 더 정교해지고 있습니다.

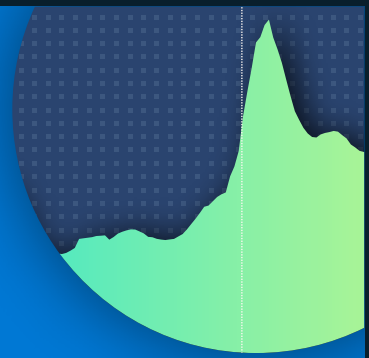
74페이지에서 자세히 알아보기

러시아의 우크라이나 침공은 영향력을 극대화하기 위해 보다 전통적인 사이버 공격 및 동적인 군사 작전과 통합된 사이버 영향력 작전을 보여줍니다.



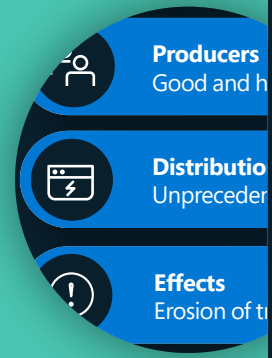
76페이지에서 자세히 알아보기

러시아, 이란, 중국은 코로나19 팬데믹 기간 동안 선전과 영향력 캠페인을 더 광범위한 정치적 목표를 달성하기 위한 전략적 디바이스로 사용하는 경우가 많았습니다.



76페이지에서 자세히 알아보기

합성 미디어는 매우 현실적인 인위적 이미지, 비디오, 오디오를 쉽게 만들고 배포하는 도구가 확산됨에 따라 더욱 일반화되고 있습니다. 미디어 자산의 출처를 인증하는 디지털 출처 기술은 오용을 방지하고자 합니다.



80페이지에서 자세히 알아보기

사이버 영향력 작전으로부터 보호하기 위한 총체적인 접근 방식

Microsoft는 사이버 영향력 작전에 대처하기 위해 이미 완성도가 높은 사이버 위협 인텔리전스 인프라를 구축하고 있습니다. Microsoft의 전략은 외국 공격자들의 선전 캠페인을 탐지, 방해, 방어, 억제하는 것입니다.

83페이지에서 자세히 알아보기

서문

민주주의가 번성하려면 신뢰할 수 있는 정보가 필요합니다. Microsoft가 주로 중점을 두는 영역은 국가에서 개발하고 영구화시키는 영향력 작전입니다. 이러한 캠페인은 신뢰를 침식하고 양극화를 심화하며 민주적 절차를 위협합니다.

외국 영향력 작전은 정보 생태계에 항상 위협이 되어 왔습니다. 그러나 인터넷과 소셜 미디어 시대와의 차이점은 캠페인의 범위, 규모, 효율성이 크게 증가하고 글로벌 정보 생태계의 상태에 미칠 수 있는 막대한 영향입니다.

예로부터 전해 내려오는 '거짓말은 진실이 신발을 신기도 전에 지구 반대편에 도달한다'라는 말은 현재 데이터로 입증되고 있습니다. MIT(매사추세츠공과대학교)의 연구[1]에 따르면 거짓은 진실보다 리트윗될 가능성이 70% 더 높으며 6배 더 빠르게 첫 1,500명에게 도달합니다. 인터넷과 소셜 미디어에서 선전 캠페인이 번성하고 전통적인 뉴스에 대한 신뢰를 훼손함에 따라 정보 생태계는 점점 더 흐려지고 있습니다. 2021년 한 연구[2]에서 미국 성인 중 7%만이 신문, 텔레비전, 라디오 뉴스 보도에 대해 '상당한' 신뢰와 확신을 가지고 있다고 답한 반면, 34%는 '전혀 없다'고 답했습니다.

Microsoft는 외국 사이버 영향력 공간의 주요 공격자, 위협, 전술을 식별하고 학습한 교훈을 공유하기 위해 노력해 왔습니다. 올해 6월, Microsoft에서 우크라이나에서 얻은 교훈에 대한 포괄적인 보고서를 발표했는데, 이 보고서는 러시아의 사이버 영향력 작전에 대한 자세한 내용을 담고 있습니다.[3]

또한 딥페이크와 같은 첨단 기술이 어떻게 무기화되고 언론인들의 신뢰성을 훼손할 수 있는지에 대해 연구하고 있습니다. 뿐만 아니라, 업계, 정부 기관, 학계와 협력하여 가짜 뉴스를 식별할 수 있는 AI(인공 지능) 시스템과 같은 합성 미디어를 탐지하고 신뢰를 회복하는 더 나은 방법을 개발하고 있습니다.

전통적인 사이버 공격과 영향력 작전의 결합 및 민주주의적 선거의 방해를 비롯하여 빠르게 변화하는 정보 생태계와 국가 온라인 선전의 특성으로 인해 민주주의에 대한 온라인 및 오프라인 위협을 완화할 수 있는 사회 전체에 대한 접근 방식이 필요합니다.

Microsoft는 신뢰할 수 있는 뉴스와 정보가 번성하는 건강한 정보 생태계를 지원하기 위해 최선을 다하고 있습니다. 국가가 주도하는 영향력 작전의 진화하고 확장되는 위험에 대처하기 위해 도구와 위협 탐지 기능을 개발하고 있습니다. 이 작업을 가능하게 하기 위해 Microsoft는 최근 Miburo Solutions를 인수했고, Global Disinformation Index 및 NewsGuard와 같은 제삼자 검증업체와 파트너 관계를 맺고 있으며, C2PA(Coalition for Content Provenance and Authenticity, 콘텐츠 출처 및 진위 확인을 위한 연합)를 비롯한 다중 이해관계자 파트너십에 참여하고 때로는 이를 주도합니다. 함께 협업해야지만 민주적 절차와 제도를 훼손하려는 사람들을 성공적으로 상대할 수 있습니다.

Teresa Hutson
기술 및 기업의 사회적 책임 부문 부사장

사이버 영향력 작전의 동향

사이버 영향력 작전은 기술이 빠르게 발전함에 따라 점점 더 정교해지고 있습니다. 전통적인 사이버 공격에 사용되는 도구가 사이버 영향력 작전에 중복 적용되어 확장되고 있습니다. 또한 국가 간의 조정과 증폭이 증가하고 있습니다.

Microsoft는 올해 외국 영향력 작전 분석 전문 회사인 Miburo Solutions를 인수하여 외국 영향력 작전 퇴치에 투자했습니다. Microsoft는 Miburo Solutions의 분석가와 Microsoft의 위협 컨텍스트 분석가가 함께하는 DTAC(Digital Threat Analysis Center, 디지털 위협 분석 센터)를 구성했습니다. DTAC는 사이버 공격 및 영향력 작전을 비롯하여 국가 차원의 위협을 분석 및 보고하고 정보 및 위협 인텔리전스를 지정학적 분석과 결합하여 인사이트를 제공하고 효과적인 대응 및 보호를 제공합니다.

전 세계 인구의 4분의 3 이상이 정보의 무기화에 대해 우려한다고 답했으며,[4] Microsoft 데이터는 이러한 우려를 뒷받침합니다. Microsoft와 파트너는 국가 차원의 공격자들이 전략적 목표와 정치적 목표를 달성하기 위해 영향력 작전을 활용하는 방법을 추적해 왔습니다. 파괴적인 사이버 공격과 사이버 스파이 활동 외에도 권위주의적인 정권은 사이버 영향력 작전을 점점 더 많이 활용하여 여론을 형성하고, 적의 신뢰를 떨어뜨리고, 공포와 불화를 조장하고, 현실을 왜곡하고 있습니다.

이러한 외국 사이버 영향력 작전으로는 일반적으로 세 단계가 있습니다.

사전 배치

조직의 컴퓨터 네트워크 내 맬웨어를 사전에 배치하는 것과 마찬가지로 외국 사이버 영향력 작전은 인터넷의 공개 도메인에 가짜 내러티브를 사전 배치합니다. 사전 배치 전술은 특히 IT 관리자가 가장 최근의 네트워크 활동을 스캔하는 경우 더 많은 전통적인 사이버 활동에 오랫동안 도움이 되었습니다. 네트워크에서 장기간 휴면 상태로 유지되는 맬웨어는 후속 사용을 더욱 효과적으로 만들 수 있습니다. 인터넷에서 눈에 띄지 않는 가짜 내러티브는 후속 참조를 더 신뢰할 수 있게 만들 수 있습니다.

시작

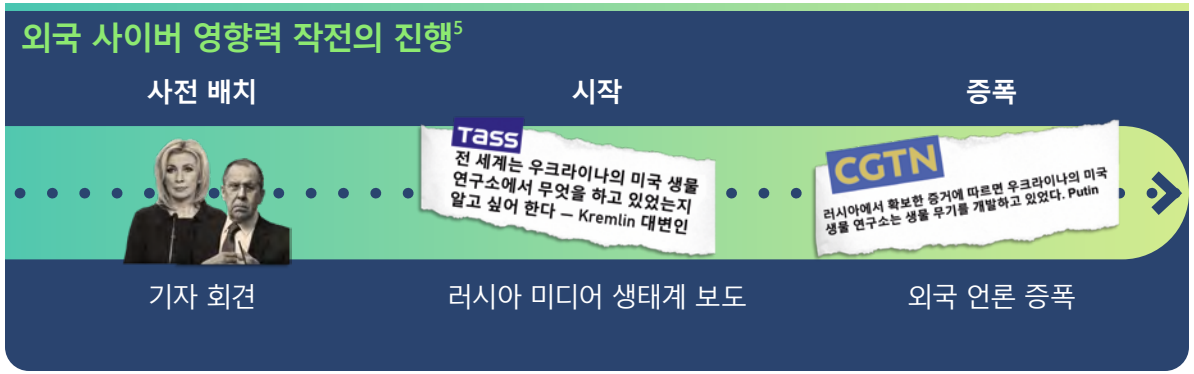
공격자의 목표를 달성하는 데 가장 도움이 되는 시간에 정부 기관에서 지원하고 영향을 받는 언론 매체와 소셜 미디어 채널을 통해 내러티브를 전파하기 위해 조정된 캠페인이 시작되는 경우가 많습니다.

증폭

마지막으로, 국가에서 통제하는 미디어와 대리인은 표적으로 삼은 청중 내부의 내러티브를 증폭시킵니다. 기술 조력자가 무의식적으로 내러티브의 범위를 확장하는 경우가 많습니다. 예를 들어, 온라인 광고는 금융 활동에 도움이 될 수 있으며 조정된 콘텐츠 게시 시스템은 검색 엔진을 범람시킬 수 있습니다.

이 3단계 접근 방식은 우크라이나의 생물무기 및 생물연구소에 대한 러시아의 가짜 내러티브를 뒷받침하기 위해 2021년 말에 사용되었습니다. 이 내러티브는 2021년 11월 29일 미국에서 자금을 댄 우크라이나의 생물 연구소가 생물 무기와 연결되어 있다고 주장한 모스크바 거주 미국인이 정규적으로 올리는 영어 콘텐츠의 일환으로 YouTube에 처음 업로드되었습니다. 이 이야기는 몇 달 동안 크게 주목받지 못했습니다. 2022년 2월 24일, 러시아 탱크가 국경을 넘었을 때 내러티브는 주목받았습니다. Microsoft의 데이터 분석 팀은 2월 24일에 러시아가 통제하거나 러시아의 영향을 받는 10개의 뉴스 사이트에서 '작년 보고서'에 대해 이야기하며 신뢰성을 부여하려는 보고서를 동시에 게시한 사실을 확인했습니다. 또한 러시아 외교부 관계자들은 기자 회견을 열어 정보 환경에서 미국 생물 연구소에 대한 거짓 주장을 더욱 강화했습니다. 그런 다음 러시아에서 후원하는 팀은 소셜 미디어와 인터넷 사이트에서 내러티브를 더 광범위하게 확대하기 위해 노력했습니다.

전 세계의 권위주의적인 정권이 협력하여 정보 생태계를 상호 수익을 위해 오염시키기 위해 협력하고 있습니다. 예를 들어, 코로나19 팬데믹 기간 동안 러시아, 이란, 중국은 민주주의와 추가 지정학적 목표를 대상으로 하는 여러 배포 방식(공공연한 방식, 약간 은밀한 방식, 은밀한 방식)을 혼합하여 선전 및 영향력 작전을 사용했습니다(76페이지에서 자세히 논의). 세 정권은 선호하는 내러티브를 홍보하기 위해 서로의 메시지 및 정보 생태계를 이용했습니다. 이 보도의 대부분은 공식 성명에서 정부 기관 인사들이 행하는 미국과 동맹국에 대한 비판이나 음모론으로 구성되었으며, 자국 백신과 코로나19에 대한 자국의 대응을 미국 및 기타 민주주의 국가보다 우월하다고 홍보했습니다. 국영 매체는 서로를 증폭시킴으로써 한 국영 매체가 생산하는 민주주의에 대한 부정적인 보도 또는 러시아, 이란, 중국에 대한 긍정적인 보도가 다른 언론 매체에 의해 강화되는 생태계를 만들었습니다.



미국 생물학 실험실과 생물학 무기에 대한 내러티브가 다양한 외국 영향력 작전(사전 배치, 시작, 증폭)의 세 가지 광범위한 단계를 통해 어떻게 확산되었는지 보여 주는 그림

사이버 영향력 작전의 동향

계속

이러한 어려움에 더해 민간 부문의 기술 기관은 무의식적으로 이러한 캠페인을 지원할 수 있습니다. 조력자로는 인터넷 도메인을 등록하고, 웹 사이트를 호스팅하고, 소셜 미디어 및 검색 사이트에서 자료를 홍보하고, 트래픽을 채널링하고, 디지털 광고를 통해 이러한 연습 비용을 지불하는 회사가 포함될 수 있습니다. 조직은 권위주의적인 정권이 사이버 영향력 작전에 사용하는 도구와 방법을 알고 있어야 캠페인의 확산을 탐지하고 방지할 수 있습니다. 또한 소비자가 외국 영향력 작전을 식별하고 내러티브나 콘텐츠에 대한 참여를 제한할 수 있는 보다 정교한 능력을 개발하도록 지원해야 할 필요성이 커지고 있습니다.

권위주의적인 선전을 포함한 사이버 영향력 작전은 신뢰를 무너뜨리고, 양극화를 심화시키며, 민주적 절차를 위협하기 때문에 전 세계 민주주의 국가에 위협이 되고 있다.

투명성을 높이고 이러한 영향력 캠페인을 폭로하고 방해하기 위해서는 정부 기관, 민간 부문, 시민 사회 전반에 걸친 조정 및 정보 공유가 필요합니다.

전 세계적으로 4분의 3 이상의 사람들이 정보가 무기화되는 방식에 대해 걱정하고 있습니다.

코로나19와 러시아의 우크라이나 침공 기간 동안의 영향력 작전에 대한 스포트라이트

팬데믹 기간과 러시아의 우크라이나 침공 기간 동안 정보 환경을 통제하고자 하는 국가는 권위주의적인 정권이 사이버 작전과 정보 작전을 어떻게 혼합하는지에 대한 명확한 예시를 보여줍니다.

코로나19 선전

러시아, 이란, 중국은 코로나19 팬데믹 기간 동안 선전과 영향력 캠페인을 사용했습니다. 코로나19는 다음과 같이 두 가지 중점적인 방식으로 이러한 캠페인에서 두드러지게 등장했습니다.

1. 팬데믹 자체에 대한 표현
2. 더 넓은 정치적 목표를 달성하기 위한 전략적 디바이스로 코로나19를 사용한 캠페인

이러한 캠페인 유형의 광범위한 목표는 두 가지로, 첫째, 민주주의, 민주주의 제도, 세계 무대에서 미국과 동맹국의 이미지를 훼손하는 것 그리고 둘째, 국내외적으로 자국의 입지를 강화하는 것입니다.

이에 대한 예시는 영어를 사용하는 독자들을 대상으로 하는 것으로 알려진 러시아 계정 및 미디어 조직의 메시지와 러시아 정부 기관이 코로나19의 백신 및 중증도에 대해 자국민과 소통한 방식에서 볼 수 있습니다.

RT.com에서 가장 많이 본 코로나바이러스 관련 기사 상위 10개(2021년 10월~2022년 4월)

비 러시아 독자를 대상으로 하는 백신 반대 선전

러시아어(아래에서 영어로 번역)	**영어**
"봉쇄와 부스터샷은 전염을 방지한다"	"백신 접종은 전염을 억제하지 못하고 새로운 변이에 효과가 없다"
"러시아의 유명 인사들이 양성 반응을 보이고 있다"	"화이자 백신은 위험한 부작용이 있다"
"러시아에서 확진 사례와 사망자가 증가하고 있다"	"대량 백신 접종은 정치적 동기가 있다"
"Sputnik V 백신은 매우 효과적이다"	"화이자와 모더나에서 규제되지 않은 시험을 실시한다"
"대중교통 탑승 시, 백신 증명서가 필요하다"	

러시아의 코로나19 메시지는 언어별로 다양합니다.

코로나19 바이러스의 기원을 모호하게 하려는 캠페인이 또 다른 예시입니다. 팬데믹이 시작된 이래로 러시아, 이란, 중국의 코로나19 선전은 이러한 중심 주제를 증폭시키기 위해 다른 보도를 강화했습니다. 이 보도의 대부분은 미국에 대한 비판이나 음모론을 조장하는 것으로 구성되었습니다. 국영 매체는 주기적으로 서로를 증폭시킴으로써 한 국영 매체가 생산하는 민주주의에 대한 부정적인 보도 또는 러시아, 이란, 중국에 대한 긍정적인 보도가 다른 언론 매체에 의해 계속해서 강화되는 생태계를 개발했습니다.

이에 대한 한 예시는 러시아와 이란 국영 매체가 코로나19는 미국이 만든 생물 무기일 수도 있다는 초기 주장입니다. 이러한 주장은 팬데믹 초기에 코로나19는 무기로 만들어졌다고 믿는다고 주장한 한 법학 교수와의 인터뷰 후 비주류 음모 웹 사이트에서 유포되었습니다.[6] 도달 범위가 제한된 일부 웹 사이트에 인터뷰가 게시된 이후, 국영 매체에서 이 이야기를 다뤘습니다. 이란 정부에서 후원하는 이란 언론 매체(영어 및 프랑스어)인 PressTV[7]는 2020년 2월 '코로나바이러스는 Francis Boyle이 믿는 것처럼 미국의 생물학적 무기인가?'라는 제목의 영어 기사를 게재했습니다. 이 기사는 '미국의 모든 전쟁에서 방사능, 화학, 생물학, 기타 금지된 무기가 사용되어 표적으로 삼은 지역의 사람들에게 치명적인 피해를 입히고 있다'라고 쓴 것처럼 미국이 코로나19의 배후에 있다고 암시했습니다.[8] 러시아 국영 매체와 중국 정부 기관 계정은 이러한 정서를 반영했습니다. 크렘린 선전을 유포하는 역할로 유명한 국영 매체 Russia Today(RT)[9]는 코로나19가 "이란과 중국을 겨냥한 미국의 '생물학적 공격'의 산물일 수 있다"[10]라고 주장하는 이란 정부 관계자들의 성명을 홍보하는 기사를 한 개 이상 작성하고 이러한 내용을 암시하는 소셜 미디어 게시물을 최대한 많이 게재했습니다. 예를 들어, 2020년 2월 27일 '코로나19가 생물학적 무기라는 사실이 밝혀지면 놀라지 않을 사람은 #coronaviru손 들어보세요.'[11]라는 트윗이 리트윗됐습니다.

우크라이나 전쟁—전쟁 무기로서의 선전

러시아의 우크라이나 침공은 사이버 영향력 작전이 보다 전통적인 사이버 공격 및 지상 군사 작전과 어떻게 융합되어 영향력을 극대화할 수 있는지 보여 주는 뚜렷한 예입니다.

우크라이나 침공을 앞두고 Microsoft 위협 인텔리전스 분석가들은 최소 6명의 개별 러시아 동맹 공격자들이 우크라이나를 대상으로 237건 이상의 사이버 공격을 시작하는 것을 보았습니다. 이러한 캠페인은 서비스와 기관의 역량을 저하시키고, 우크라이나 사람들이 신뢰할 수 있는 정보에 접근하지 못하도록 저지하며, 우크라이나 대통령에 대한 의구심을 품게 했습니다.

코로나19와 러시아의 우크라이나 침공 기간 동안의 영향력 작전에 대한 스포트라이트

계속

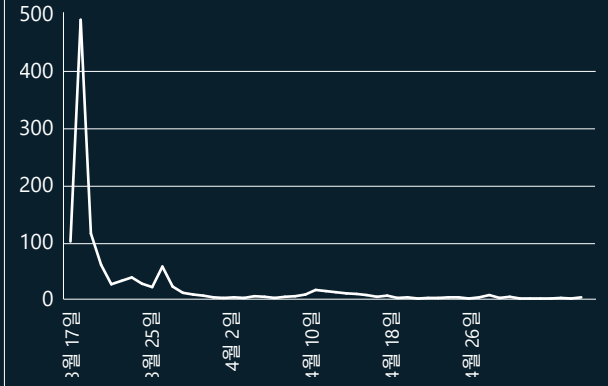
2022년 4월에 발표된 Microsoft 보고서에서 키이우의 정보 환경을 통제하려는 명백한 시도에서 어떻게 러시아가 주요 우크라이나 언론사에 대한 파괴적인 맬웨어를 시작한 날 키이우의 TV 타워에 미사일 공격을 시작했는지 볼 수 있습니다.[12]

사이버 공격과 영향력 작전이 어떻게 수렴되는지에 대한 또 다른 예에서 러시아 위협 행위자는 우크라이나 시민들에게 마리우폴 거주자라고 사칭하는 이메일을 보내 전쟁 확대와 관련하여 우크라이나 정부를 비난하고 동포들에게 정부에 대항할 것을 촉구했습니다. 이 이메일은 이메일을 수신하는 사람들의 이름을 구체적으로 명시하며 전송되어 이전 스파이 관련 사이버 공격에서 이들의 정보가 도난당했다는 사실을 시사합니다. 악성 링크는 포함되지 않았는데, 이는 의도가 순수한 영향력 작업임을 시사합니다.

해킹, 유출, 기타 민감한 자료를 특징으로 하는 것은 영향력 작전에서 러시아 공격자들이 사용하는 일반적인 전술입니다. 우크라이나 전쟁 내내 친러시아 소셜 미디어 채널은 우크라이나 정보원으로부터 유출되거나 민감한 자료라고 주장하는 내용을 홍보했습니다. 유출되거나 민감한 자료는 친러시아 소셜 미디어 채널과 매체에서 기관에 대한 신뢰를 떨어뜨리고 주류 내러티브에 의문을 제기하기 위한 광범위한 영향력 전략의 일환으로 사용됩니다. 이러한 정보는 우크라이나와 서방 국가를 겨냥한 선전을 만들고, 디지털 보안에 대한 신뢰를 떨어뜨리며, 우크라이나에 대한 서방 국가의 원조를 약화시키기 위해 조작될 수 있습니다.

러시아는 사실을 모호하게 하거나 훼손하기 위해 지상에서 사건이 발생한 후 여론을 형성하기 위해 다른 정보 공격을 사용했습니다. 예를 들어, 3월 7일 러시아는 유엔에 제출한 서류를 통해 우크라이나 마리우폴에 있는 한 산부인과 병원이 군사 장소로 사용되고 있다는 이야기를 사전 배치했습니다. 3월 9일 러시아는 병원을 폭격했습니다. 폭탄 테러 소식이 전해진 후 러시아 유엔 대표 Dmitry Polyanskiy는 폭탄 테러에 대한 보도가 '가짜 뉴스'라고 트윗하고 군사 기지로 사용되었다는 러시아의 이전 주장을 인용했습니다. 그런 다음 러시아는 병원 공격 이후 2주 동안 러시아가 통제하는 웹 사이트에 이 내러티브를 광범위하게 퍼뜨렸습니다.

트래픽이 있는 도메인
(2022년 3월 9일~2022년 4월 30일)



선전 웹 사이트에서는 2022년 4월 1일에 간단한 회복을 시작으로 약 2주 동안 산부인과 병원에 대한 이야기를 게시했습니다(출처: Microsoft AI for Good Lab).

2022년 2월과 3월 마리우폴에 있는 주산기 병원의 위성 이미지

Microsoft의 자체 위성 이미지 분석에 따르면 주산기 병원이 폭격을 당했습니다. 첫 번째 사진은 2022년 2월 24일에 두 번째 사진은 2022년 3월 24일에 촬영되었습니다(사진 출처: Planet Labs).

전쟁이 진행됨에 따라 러시아의 잔학 행위에 대한 눈속임은 계속되었습니다. 예를 들어, 2022년 6월 말, 러시아 언론 매체와 인플루언서는 쇼핑몰 폭격을 정당하고 필요한 공격으로 묘사하여 쇼핑몰이 아닌 우크라이나 영토 국방군의 무기고로 사용 중이라고 거짓 주장했습니다.[13] 텔레그램에서 활동하는 여러 친크렘린 블로거들은 '가짜 깃발' 내러티브를 강화하는 콘텐츠를 게시하고 증폭했으며, 블로거들은 현장 영상에서 군복을 입을 사람들의 존재[14]와 여성의 부재를 포함하여 조작 혐의를 보이는 지표에 대해 지적했습니다.[15] 러시아는 구축되어 있는 선전 메신저와 매체 시스템에 의존하여 캠페인을 시작했습니다. 온라인에서 이러한 이야기가 증폭하면 러시아가 국제무대에서 책임을 회피하고 책임을 피할 수 있도록 합니다.

러시아와 같은 국가는 폐쇄된 정보원으로부터 파생된 정보를 활용하여 대중의 인식에 영향을 미치고 '해킹 및 유출' 캠페인을 활용하여 반대 내러티브를 전파하고 불신을 심는 것의 가치를 이해합니다.

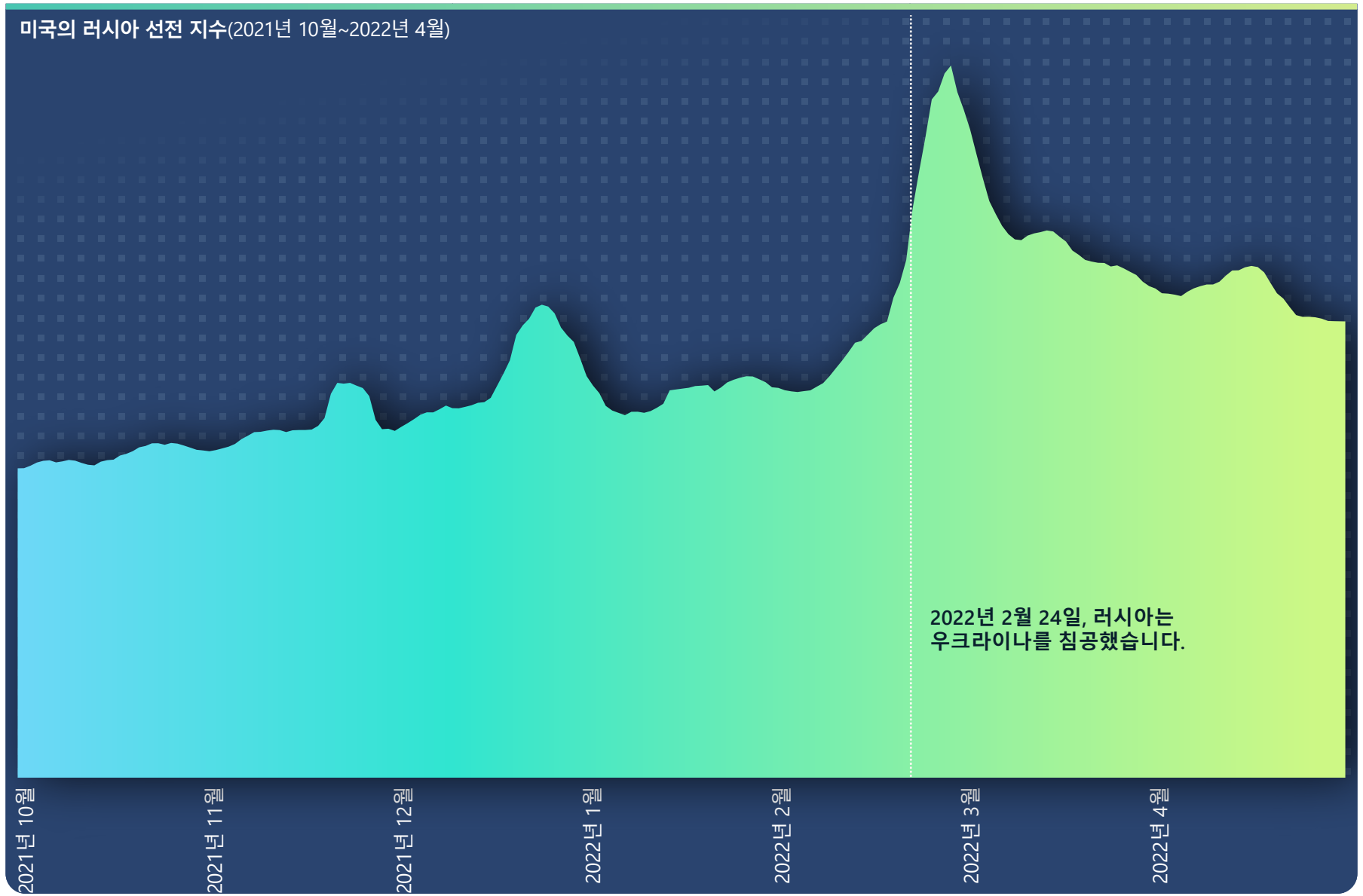
추가 정보에 대한 링크

- 우크라이나 방어: 사이버 전쟁 초기의 교훈 | 문제에 대응하는 Microsoft
- 우크라이나에서 러시아의 사이버 공격 활동 개요 | Microsoft 특별 보고서
- 우크라이나를 겨냥한 사이버 공격 중단 | 문제에 대응하는 Microsoft

러시아 선전 지수 추적

2022년 1월, 거의 1,000개의 미국 웹 사이트가 러시아 선전 웹 사이트로 트래픽을 참조했습니다. 미국 시민들을 대상으로 하는 러시아 선전 웹 사이트의 가장 일반적인 주제는 우크라이나 전쟁, 미국 국내 정치(친트럼프 또는 친바이든), 코로나19, 백신 관련 내러티브였습니다.

RPI(Russian Propaganda Index, 러시아 선전 지수)는 인터넷 전체 뉴스 트래픽에서 러시아에서 제어하는 매체, 후원하는 매체, 증폭기의 뉴스 흐름을 모니터링합니다. RPI를 사용하여 정확한 타임라인에 따라 인터넷과 다른 지역에서 러시아 선전의 소비를 차트로 표시할 수 있습니다. 하지만 Microsoft에서는 이전에 확인된 웹 사이트에 게시된 러시아 선전만 관찰할 수 있다고 지적합니다. Microsoft에는 권위 있는 뉴스 웹 사이트, 미확인 웹 사이트, 소셜 네트워크 그룹을 포함한 다른 유형의 웹 사이트 내 선전에 대한 인사이트는 없습니다.



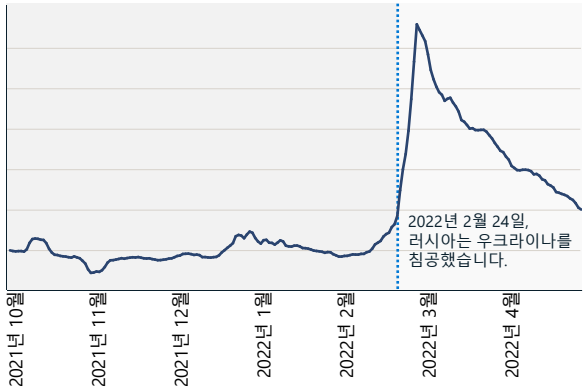
러시아 선전 지수 추적

계속

러시아 선전 지수: 우크라이나

우크라이나 전쟁이 시작되었을 때 러시아 선전은 216% 증가하여 3월 2일에 정점을 찍었습니다. 아래 차트는 이처럼 갑작스러운 증가가 어떻게 침공과 일치했는지 보여줍니다. 두 그래프는 침공이 시작된 직후 러시아 선전이 어떻게 급증했는지 보여줍니다.

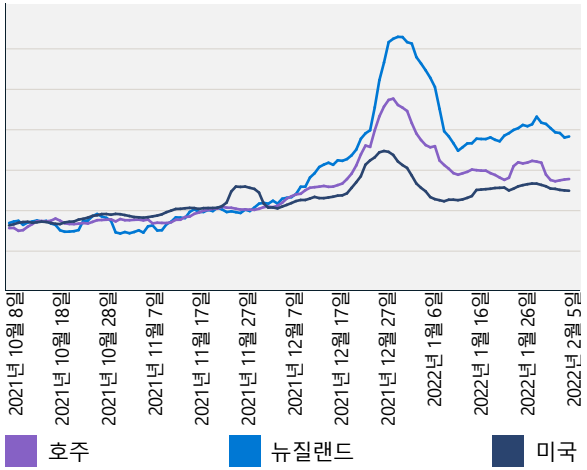
RPI, 우크라이나
(2021년 10월 7일~2022년 4월 30일)



러시아 선전 지수: 뉴질랜드, 호주, 미국 비교

뉴질랜드의 RPI에 대한 평가는 코로나19 선전과 관련하여 2021년 말에 급증한 것으로 나타났습니다. 뉴질랜드에서의 이러한 러시아 선전 소비의 급증은 2022년 초 웰링턴에서 대중들의 시위가 많아지기 전에 발생했습니다. 두 번째 급증은 분명히 러시아의 우크라이나 침공과 관련이 있었으며, 호주와 미국의 RPI를 초과했습니다.

RPI, 뉴질랜드, 호주, 미국 비교



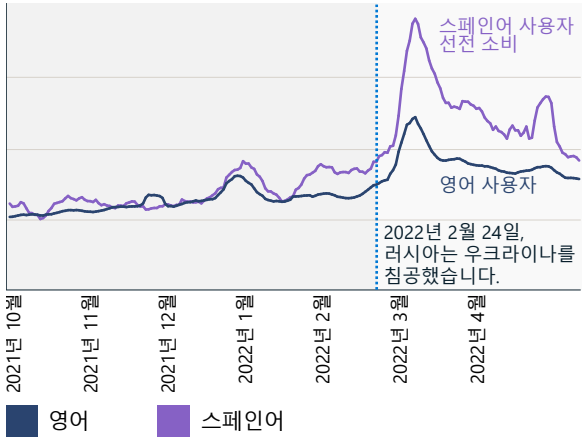
뉴질랜드에서의 러시아 선전 소비는 2021년 12월 첫째 주까지 호주와 유사합니다. 12월 이후 뉴질랜드에서의 러시아 선전 소비는 호주와 미국의 소비에 비해 30% 이상 증가했습니다.

미국에서의 러시아 선전 지수: 영어 및 스페인어

RPI는 또한 언어 전반에 걸친 선전을 추적합니다. RT 및 Sputnik News를 포함한 여러 매체는 20개 이상의 언어로 제공됩니다. 해당되는 언어로는 영어, 스페인어, 독일어, 프랑스어, 그리스어, 이탈리아어, 체코어, 폴란드어, 세르비아어, 라트비아어, 리투아니아어, 몰도바어, 벨로루스어, 아르메니아어, 오세트어, 조지아어, 아제르바이잔어, 아랍어, 터키어, 페르시아어, 다리어가 포함됩니다.

다음 그래프는 미국의 스페인어 뉴스에 대한 RPI가 영어 뉴스보다 훨씬 높다는 것을 보여줍니다.

러시아 선전 소비는 스페인어 사용자들 사이에서 2배 더 높습니다.



미국에서의 러시아 선전 소비는 스페인어 사용자들 사이에서 2배 더 높습니다.

러시아 선전은 라틴 아메리카에서 높습니다.

스페인어로 된 RT는 페이지 뷰와 Facebook 팔로워가 가장 많은 국제 뉴스 매체입니다.

출처: Microsoft AI for Good Research Lab

합성 미디어

우리는 AI 지원 미디어 제작 및 조작의 황금시대에 접어들고 있습니다. Microsoft 분석가들은 이러한 사실은 매우 사실적인 합성 이미지, 비디오, 오디오, 텍스트를 인위적으로 생성하기 위해 사용하기 쉬운 도구 및 서비스의 확산과 특정 대상에 최적화된 콘텐츠를 빠르게 배포하는 기능이라는 두 가지 주요 추세에 의해 주도된다는 점에 주목합니다.

이러한 추세의 발전 중 그 어느 것도 자체로는 본질적인 문제가 되지 않습니다. AI 기반 기술은 순수 합성 콘텐츠를 만들거나 기존 자료를 개선하는 등 재미있고 흥미진진한 디지털 콘텐츠를 만드는 데 사용할 수 있습니다. 이러한 도구는 광고 및 커뮤니케이션을 위해 기업에서 널리 사용되고 있으며 팔로워를 위한 매력적인 콘텐츠를 만들기 위해 개인들 사이에서 널리 사용되고 있습니다. 그러나 합성 미디어는 해를 끼칠 의도로 생성되고 배포된다면 개인, 회사, 기관, 사회에 심각한 피해를 줄 가능성이 있습니다. Microsoft는 이러한 피해를 제한하기 위해 내부 및 광범위한 미디어 생태계 전반에 걸쳐 기술과 관행을 개발하는 원동력이 되었습니다.

이 섹션에서는 유해한 합성 콘텐츠를 생성하는 최신 기술, 해당 콘텐츠가 널리 보급될 경우 발생할 수 있는 피해, 합성 미디어 기반 사이버 위협으로부터 방어할 수 있는 기술적 완화에 대한 Microsoft 분석 인사이트에 대해 살펴보겠습니다.

합성 미디어 생성

합성 텍스트 및 미디어 분야는 한때 대형 영화 스튜디오의 방대한 컴퓨팅 리소스로만 가능했던 기술이 현재 전화 앱에 통합됨에 따라 엄청나게 빠르게 발전하고 있습니다. 이와 동시에, 도구는 점점 더 사용하기가 쉬워지고 있으며 법의학 미디어 전문가도 속일 수 있는 수준의 사실감으로 콘텐츠를 생성할 수 있습니다. 누구든지 말하거나 행동하는 사람의 합성 비디오를 만들 수 있는 시점에 아주 가깝게 도달했다고 할 수 있습니다. 우리가 온라인에서 보는 콘텐츠의 상당량이 AI 기술을 사용하여 완전히 또는 부분적으로 합성되는 시대에 접어들고 있다고 믿는 것은 무리가 아닙니다.

> 보다 정교하고 사용하기 쉬우며 널리 사용할 수 있는 도구를 사용할 수 있게 됨에 따라 합성 콘텐츠 제작이 증가하고 있으며 곧 현실과 구별할 수 없을 정도로 발전할 것입니다.

고품질의 무료 및 상업용 이미지, 비디오, 오디오 편집 도구가 많이 있습니다. 이러한 도구는 오해의 소지가 있는 텍스트 추가, 얼굴 교체, 컨텍스트 제거 또는 변경과 같이 간단하지만 잠재적으로 피해를 입힐 수 있는 디지털 콘텐츠를 변경하는 데 사용할 수 있습니다. 이러한 '칩페이크(cheap fakes)'는 비도덕적인 콘텐츠를 퍼뜨리고 정치적 이념을 홍보하며 평판을 깎아내리는 데 널리 사용됩니다. 잘 알려진 예로는 미국 하원의장인 Nancy Pelosi가 연설할 때 불분명하게 발음하고 술에 취한 것처럼 보이는 2019년도 비디오[16]입니다. 효과를 내기 위해 비디오가 느려졌다는 사실이 빠르게 확인되었지만 원본 비디오와 문맥이 드러나기 전전 '칩페이크'는 널리 퍼졌습니다.

미디어 콘텐츠를 변경하는 보다 정교한 접근 방식으로는 고급 AI 기술을 적용하여 (a) 순수 합성 미디어를 만들고 (b) 기존 미디어를 보다 정교하게 편집하는 것 등이 있습니다. 딥페이크라는 용어(이 이름은 가끔 사용되는 심층 신경망에서 유래됨)는 최첨단 AI 기술을 활용하여 생성된 합성 미디어에서 자주 사용됩니다. 해당 기술은 독립 실행형 앱, 도구, 서비스로 개발되고 있으며 기존의 상용 및 오픈 소스 편집 도구에 통합되고 있습니다.

이러한 기술은 개인과 기관에 피해를 입히려는 악의적인 공격자들에 의해 무기화됩니다. 딥페이크 기술의 예는 다음과 같습니다.

- **페이스 스왑(비디오, 이미지)**—비디오의 얼굴을 다른 얼굴로 바꿉니다. 이 기술은 개인, 회사 또는 기관을 협박하거나 개인을 난처한 장소 또는 상황에 놓는 데 사용될 수 있습니다.
- **퍼피티어링(비디오, 이미지)**—비디오를 활용하여 스틸 이미지 또는 두 번째 비디오를 움직이게 합니다. 개인이 난처한 말을 하거나 오해의 소지가 있는 말을 한 것처럼 보이게 할 수 있습니다.
- **생성적 적대 신경망(비디오, 이미지)**—사실적인 이미지를 생성하기 위한 기술 제품군입니다.
- **트랜스포머 모델(비디오, 이미지, 텍스트)**—텍스트 설명에서 풍부한 이미지를 생성합니다.

이러한 고급 AI 기반 기술은 오늘날 사이버 영향력 캠페인에서 아직 널리 사용되지 않지만 도구가 더 쉽고 널리 사용됨에 따라 문제는 더욱 커질 것으로 예상합니다.

합성 미디어 조작의 영향

정보 작전을 사용하여 해를 입히거나 영향력을 확대하는 것은 새롭지 않습니다. 그러나 정보가 확산되는 속도와 허구 속에서 사실을 신속하게 구분할 수 없는 우리의 무능은 Pelosi의 예에서 알 수 있듯이 가짜 및 기타 합성된 악성 미디어로 인한 영향과 피해가 훨씬 더 클 수 있다는 사실을 의미합니다.

우려하는 피해로는 시장 조작, 지불 사기, 비싱, 사칭, 브랜드 손상, 평판 손상, 봇넷 등의 여러 범주의 피해가 있습니다. 이러한 범주 중 상당수는 허구 속에서 사실을 구분하는 우리의 능력을 약화시킬 수 있는 실제 사례에 대해 널리 보고했습니다.

더 장기적이고 더 교활한 위협은 우리가 보고 듣는 것을 더 이상 신뢰할 수 없는 경우 무엇이 진실인지에 대한 우리의 이해를 대상으로 합니다. 이로 인해 공적 또는 사적 인물의 손상된 이미지, 오디오 또는 비디오는 가짜로 치부될 수 있는데, 이를 거짓말쟁이의 배당금(Liar's Dividend)이라고 합니다.[17] 최근 연구[18]에 따르면 다른 많은 남용 시나리오가 그럴듯하지만 이러한 기술 남용은 이미 금융 시스템을 공격하는 데 사용되고 있음을 보여줍니다.

합성 미디어

계속

합성 미디어 탐지

업계, 정부 기관, 학계 전반에 걸쳐 합성 미디어를 탐지 및 완화하고 신뢰를 회복하는 더 나은 방법을 개발하기 위한 노력이 진행 중입니다. 고려해야 할 장벽뿐만 아니라 향후 유망한 몇 가지 경로가 있습니다.

한 가지 접근 방식은 가짜를 식별할 수 있는 AI 기반 시스템, 즉 공격적인 AI 시스템에 대응하기 위해 본질적으로 '방어적인' AI 시스템을 구축하는 것입니다. 이 분야는 합성 오디오 및 비디오를 생성하는 현재 시스템이 훈련된 미디어 포렌식 분석가와 자동화된 도구로 발견할 수 있는 명백한 아티팩트를 남기는 활발한 연구 분야입니다.

안타깝게도 현재 가짜 미디어에는 결함이 드러나지만 정확한 아티팩트는 특정 도구 또는 알고리즘에만 국한되는 경향이 있습니다. 즉, 알려진 가짜 미디어에 대한 훈련은 2020년 딥페이크 이미지 탐지기 구축을 위한 공개적인 경쟁에서 입증된 것처럼 일반적으로 다른 알고리즘으로 일반화되지 않습니다.[19] 고급 탐지기 개발에 대한 투자는 매우 흥미롭지만, Microsoft는 다음과 같은 두 가지 이유로 이러한 투자가 의미 있는 개선을 가져올지에 대해 매우 회의적입니다.

첫째, 우리에게는 실제 세계를 반영하는 우수한 물리적 모델이 있습니다. 현재의 가짜 미디어 제작자들은 절차를 무시하여 탐지 가능한 아티팩트를 생성하지만 최신 모델은 더욱 현실적일 것입니다. 컴퓨터로 모델링할 수 없는 카메라로 포착한 실제 장면에는 본질적으로 특별한 것이 없습니다.

둘째, 고급 가짜 생성 알고리즘은 생성 프로세스의 일환으로 GAN(생성적 적대 신경망)이라는 기술을 사용합니다. GAN은 생성기를 활용하여 가짜 이미지를 생성하고 판별기를 활용하여 가짜 이미지를 탐지하고 생성기를 훈련시키는 두 AI 시스템을 서로 대립시킵니다. 더 나은 탐지기 개발에 대한 투자는 생성기를 통해 가짜 미디어의 품질을 향상시킬 뿐입니다.

합성 미디어

계속

디지털 자산의 출처

가짜 미디어 탐지를 신뢰할 수 없다면 합성 미디어의 유해한 사용으로부터 보호하려면 무엇을 할 수 있을까요? 새롭게 부상하는 중요한 기술 중 한 가지 기술은 디지털 미디어 제작자가 자산을 인증할 수 있도록 지원하고 소비자가 디지털 자산이 변조되었는지 여부를 식별하는 데 도움이 되는 메커니즘인 디지털 출처입니다. 디지털 출처는 콘텐츠가 인터넷을 이동할 수 있는 속도와 악의적인 공격자들이 콘텐츠를 쉽게 조작할 수 있는 기회를 고려하면 오늘날 소셜 미디어 네트워크의 맥락에서 특히 중요합니다.

디지털 출처 기술은 최신 버전의 암호화 문서 서명으로, 오늘날 웹을 통해 이동하는 개체의 출처, 편집 기록, 메타데이터를 포착하도록 설계되었습니다. 이러한 유형의 엔드 투 엔드 변조 방지 미디어 인증을 지원하는 비전과 기술 방식은 Microsoft 연구원 및 과학자로 구성된 교차 팀에서 개발했습니다. Microsoft는 프로젝트 오리진(Microsoft, BBC, CBC/Radio-Canada, New York Times에서 설립)에서 미디어 출처 기술을 실현하기 위한 업계 간 파트너십을 공동으로 이끌고 CAI(Content Authenticity Initiative, 콘텐츠 진위 이니셔티브, Adobe에서 설립)에 참여하고 있습니다. 또한 Microsoft는 기술 및 미디어 서비스 파트너와 협력하여 C2PA(콘텐츠 출처 및 진위 확인을 위한 연합)를 설립했습니다. C2PA는 표준 조직으로서, 최근 이미지, 비디오, 오디오, 텍스트를 포함한 미디어 자산과 함께 활용할 수 있는 가장 진보된 디지털 출처 사양에 대해 발표했습니다.

C2PA에서 지원하는 개체는 개체와 메타데이터가 변조되지 않도록 보호하는 매니페스트를 전달하며 함께 제공되는 인증서는 게시자를 식별합니다.

합성 미디어는 원래 해를 입히도록 설계되지 않았지만 개인과 기관에 대한 신뢰를 훼손하기 위해 악의적인 공격자들에 의해 무기화되고 있습니다.

디지털 출처는 미디어 자산의 출처를 인증하여 온라인 미디어 콘텐츠에 대한 사람들의 신뢰를 회복하는 데 도움이 될 가능성이 있는 유망한 신기술입니다.

C2PA 사양을 기반으로 공개적으로 사용 가능한 이 솔루션은 기존 제품의 새로운 기능 또는 새로운 독립 실행형 앱과 서비스로 부상하고 있습니다. 몇 년 안에는 일반적으로 사용되는 대부분의 캡처, 편집, 저작 도구에서 C2PA를 사용할 수 있을 것으로 예상합니다. 이는 기업이 오늘날 디지털 출처에 대한 요구와 용도를 결정하고 기존 워크플로에서 사용하는 도구에 이러한 추가 보호 계층을 요구할 수 있는 기회를 제공합니다.

900%

2019년 이후 매년 딥페이크의 확산 비율[20]

실행 가능한 인사이트

1. PR 및 커뮤니케이션 대응을 사전에 고려하여 잘못된 정보 위협으로부터 조직을 보호하기 위한 사전 조치를 취합니다.
2. 출처 관련 기술을 사용하여 공식적인 커뮤니케이션을 보호합니다.

추가 정보에 대한 링크

- 허위 정보에 대한 유망한 단계 | 문제에 대응하는 Microsoft
- 이정표 달성, 2022년 1월 31일
- 프로젝트 오리진 | Microsoft ALT Innovation
- C2PA(Coalition for Content Provenance and Authenticity, 콘텐츠 출처 및 진위 확인을 위한 연합)
- 미디어 인증에 사용되는 프로젝트 오리진 시스템에 대한 기술 세부 정보 살펴보기 | Microsoft ALT Innovation

사이버 영향력 작전으로부터 보호하기 위한 총체적인 접근 방식

Microsoft는 이미 완성도 높은 사이버 위협 인텔리전스 인프라를 기반으로 사이버 영향력 작전에 대한 보다 광범위하고 포괄적인 관점을 개발하고 있습니다.

우리는 작전으로 인한 위협에 대처하기 위해 제안된 대응 및 완화 전략에 대한 프레임워크를 사용하며, 이는 탐지, 중단, 방어, 억제의 네 가지 핵심 요소로 나눌 수 있습니다.

또한 Microsoft는 이 공간에서 기반을 단단히 하기 위해 네 가지 원칙을 채택했습니다. 첫째, 표현의 자유를 존중하고 플랫폼, 제품, 서비스를 통해 정보를 생성, 게시, 검색할 수 있는 고객의 역량을 유지하겠다고 약속합니다. 둘째, 플랫폼과 제품이 외국 사이버 영향력 사이트 및 콘텐츠를 증폭시키는 데 사용되는 것을 방지하기 위해 적극적으로 노력합니다. 셋째, 외국 사이버 영향력 콘텐츠나 공격자로부터 고의적으로 수익을 취하지 않습니다. 마지막으로, 제품에 대한 내부 및 신뢰할 수 있는 제삼자 데이터를 활용하여 외국의 사이버 영향력 작전에 대응하기 위해 콘텐츠 표면의 우선순위를 지정합니다.

탐지

사이버 방어와 마찬가지로 외국 사이버 영향력 작전에 대응하는 첫 번째 단계는 이를 탐지할 수 있는 역량을 개발하는 것입니다. 어떤 단일 회사나 조직도 개별적으로 필요한 진전을 이룰 수 없습니다. 기술 부문 전반에 걸친 새롭고 광범위한 협력이 중요하게 작용할 것이며, 사이버 영향력 작전을 분석하고 보고하는 데 있어 진전은 학술 기관 및 비영리 조직을 포함하여 시민 사회의 역할에 크게 의존하고 있습니다.

프린스턴대학교의 Jake Shapiro 연구원과 카네기 국제평화재단의 Alicia Wanless 연구원은 이 역할을 인식하여 새로운 'IRIE(Institute for Research on the Information Environment, 정보 환경 연구소)'를 출범할 계획을 세웠습니다. IRIE는 Microsoft, Knight Foundation, Craig Newmark Philanthropies의 지원을 받아 CERN(European Organization for Nuclear Research, 유럽 핵 연구 기구)를 모델로 한 포괄적인 다중 이해관계자 연구 기관을 설립할 것입니다. 데이터 처리 및 분석에 대한 전문 지식을 결합하여 이 분야에서의 새로운 발견을 가속화하고 확장할 것입니다. 연구 결과는 정책 입안자, 기술 회사, 소비자에게 공유되어 보다 광범위하게 알려질 것입니다.

방어

두 번째 전략적인 요소는 투자와 혁신이 필요한, 오랜 우선순위인 민주적 방어를 강화하는 것입니다. 기술이 민주주의에 야기한 도전과 기술이 민주주의 사회를 보다 효과적으로 방어할 수 있는 기회에 대해 고려해야 합니다.

Microsoft의 전략 프레임워크는 여러 부문 이해관계자가 선전, 특히 외국 공격자들의 캠페인을 탐지, 중단, 방어, 억제할 수 있도록 지원하는 것을 목표로 합니다.

우리 시대의 가장 큰 기술적 과제 중 하나인 인터넷과 디지털 광고가 전통적인 저널리즘에 미치는 영향부터 시작하는 것이 적절합니다. 1700년대 이래로 자유 독립 언론은 부패를 폭로하고, 전쟁을 기록하며, 이 시대와 다른 시대의 가장 큰 사회적 도전을 조명하는 등 지구상의 모든 민주주의를 지원하는 데 특별한 역할을 했습니다. 그러나 인터넷은 광고 수익을 삼키고 유료 가입자를 유인하여 지역 뉴스를 장악했습니다. 수많은 지역 신문이 무너졌습니다. Microsoft에서 진행한 최근 연구 결과를 통해 여러 인사이트 중 하나는 신문이 없는 마을은 무의식적 및 필연적으로 평균 이상의 외국 선전에 노출된다는 것입니다. 그렇기 때문에 민주주의의 비판적 방어 갈래 중 하나로 특히 지역 수준에서 전통 저널리즘과 자유 언론을 강화해야 합니다. 이를 위해서는 다양한 국가 및 대륙의 현지 요구 사항을 반영해야 하는 지속적인 투자와 혁신이 필요합니다. 이러한 문제는 쉽지 않으며 Microsoft 및 기타 기술 회사가 점점 더 많이 더 지원하고 있는 다중 이해관계자 접근 방식이 필요합니다.

또한 새로운 공공 정책 혁신이 필요한데, 이는 공적인 우선순위가 되어야 합니다. 여기에는 게시자가 기술 회사와 공동으로 광고 수익을 협상할 수 있도록 하는 법과 고용한 언론인에 대한 급여세의 일부를 지역 보도국에서 완화하기 위해 세금 공제를 제공하는 법이 포함될 수 있습니다. 저널리스트는 합법적인 출처와 가짜 출처에서 콘텐츠를 구분하는 기능을 포함하여 자신의 기술을 지원할 다양한 도구가 많이 필요합니다.

또한 소비자가 국가 주도의 정보 작전을 식별할 수 있는 보다 정교한 역량을 개발할 수 있도록 지원해야 할 필요성이 빠르게 커지고 있습니다. 이는 어려워 보일 수 있지만 다른 사이버 위협에 대처하기 위해 기술 부문에서 오랫동안 추구해 온 작업과 유사합니다. 스팸 또는 기타 사기를 치는 커뮤니케이션을 식별하는 데 도움이 되도록 이메일 주소를 보다 주의 깊게 살펴보는 소비자 교육을 고려하세요. News Literacy Project(뉴스 문해력 프로젝트)와 Trusted Journalism(신뢰할 수 있는 저널리즘)과 같은 미국의 이니셔티브가 그 예입니다.

더 장기적이고 더 교활한 위협은 우리가 보고 듣는 것을 더 이상 신뢰할 수 없는 경우 무엇이 진실인지에 대한 우리의 이해를 대상으로 합니다.

사이버 영향력 작전으로부터 보호하기 위한 총체적인 접근 방식

계속

프로그램은 뉴스와 정보에 대해 잘 알고 있는 소비자를 발전시키는 데 도움이 됩니다. 전 세계적으로 NewsGuard의 브라우저 플러그인과 같은 새로운 기술은 이러한 노력을 훨씬 빠르게 진행하는 데 도움이 될 수 있습니다.

또한 민주주의 기초의 일부는 시민 교육이라는 사실을 상기시켜야 합니다. 항상 그렇듯이 이러한 노력은 학교에서 시작되어야 합니다. 그러나 우리는 평생 지속적인 시민 교육을 받아야 하는 세상에 살고 있습니다. 국제전략문제연구소(Center for Strategic and International Studies)가 주도하고 Microsoft의 첫 취임 서명자이자 파트너였던 새로운 Civics at Work 서약은 기업 커뮤니티 내에서 시민 문해력을 활성화하기 위해 노력합니다. 이는 민주적 방어를 강화할 수 있는 폭넓은 기회를 보여 주는 좋은 예입니다.

중단

최근 몇 년 동안 Microsoft의 DCU(디지털 범죄 부서)는 랜섬웨어에서 봇넷 및 국가 차원의 공격에 이르기까지 사이버 위협을 방해하는 전술을 개선하고 도구를 개발했습니다. Microsoft는 광범위한 사이버 공격에 대응하기 위한 적극적인 중단의 역할부터 시작하여 중요한 교훈을 많이 얻었습니다.

사이버 영향력 작전에 대응하는 경우, 중단이 훨씬 더 중요한 역할을 할 수 있으며 중단에 대한 최선의 접근 방식은 더욱 명확해지고 있습니다. 광범위한 속임수에 대한 가장 효과적인 해독제는 투명성입니다. 그렇기 때문에 Microsoft에서는 외국 사이버 영향력 작전 탐지 및 대응을 전문으로 하는 선도적인 사이버 위협 분석 및 연구 회사인 Miburo Solutions를 인수하여 국가 차원의 영향력 작전을 탐지하고 중단할 수 있는 역량을 강화했습니다.

Microsoft의 경험에 따르면 정부 기관, 기술 회사, NGO는 사이버 공격을 신중하게 다루고 충분한 증거로 간주해야 합니다. 이러한 중단의 영향을 이해하는 것은 매우 중요하며 사이버 영향력을 중단하는 데 훨씬 큰 도움이 될 수 있습니다. 러시아의 우크라이나 침공을 앞두고 가짜 그래픽 비디오를 사용하려는 음모와 같은 특정 캠페인을 포함한 러시아 계획을 폭로하는 등 효과적으로 투명성 관련 조치를 취하는 미국 정부 기관의 정보 공유에 대해 확인하세요.

지난여름 제네바의 CyberPeace Institute(사이버피스 인스티튜트)가 우크라이나 안팎에서 진행 중인 사이버 공격에 대해 발표한 바와 같이, 광범위한 시민 사회 및 민간 부문 조직이 사이버 영향력 작전과 관련하여 투명성을 향상시킬 수 있는 기회가 있습니다. 새롭게 발견되고 제대로 문서화된 작업에 대한 신뢰할 수 있는 보고서는 대중이 특히 인터넷에서 읽고, 보고, 듣는 내용을 더 잘 평가하는 데 도움이 될 수 있습니다. 이를 위해 Microsoft는 기존 사이버 보고서를 기반으로 확장하고 적절한 경우, 속성에 대한 설명을 포함하여 사이버 영향력 작업에 대해 발견한 내용과 관련된 새로운 보고서, 데이터, 업데이트를 발표할 것입니다. 또한 데이터 기반 접근 방식을 사용하여 회사 전체에서 외국 정보 작전의 보급과 점진적인 개선을 보장하는 다음 단계를 살펴보는 내용의 연례 보고서를 발행할 것입니다.

뿐만 아니라, 이러한 유형의 투명성을 기반으로 하는 추가 단계를 고려할 것입니다.

예를 들어, 디지털 광고의 역할은 광고가 외국 작전의 자금을 지원하는 동시에 외국에서 후원하는 선전 사이트에 대한 합법성을 창출하는 데 도움이 될 수 있기 때문에 특히 중요합니다. 이러한 재정적 흐름을 중단하기 위해서는 새로운 노력이 필요할 것입니다.

억제

마지막으로, 국제 규칙 위반에 대한 책임이 없다면 국가가 행동을 바꿀 것이라고 기대할 수 없습니다. 그러한 책임을 묻는 것은 정부의 책임입니다. 그러나 점점 더 많은 이해관계자들의 행동이 국제 규범을 강화하고 확장하는 데 중요한 역할을 하고 있습니다. Microsoft를 포함한 30개 이상의 온라인 플랫폼, 광고주, 게시자가 최근 업데이트된 유럽 위원회의 허위 정보에 대한 실천 강령(Code of Practice on Disinformation)에 서명하여 증가하는 문제를 해결할 수 있는 약속 강화에 동의했습니다. 최근의 파리 요청(Paris Call), 크라이스트처치 콜(Christchurch Call), Declaration on the Future of the Internet(인터넷의 미래에 관한 선언)과 마찬가지로 다자 및 다중 이해관계자들의 행동은 민주주의 국가의 정부 기관과 대중을 하나로 모을 수 있습니다. 그런 다음 정부 기관은 이러한 규범과 법률을 기반으로 세계 민주주의 국가에서 필요하고 마땅히 받아야 할 책임을 증진할 수 있습니다.

신속하며 급진적인 투명성을 통해 민주주의적인 정부 기관과 사회는 국가 차원의 공격 원인을 밝혀 대중에게 알리고 기관에 대한 신뢰를 구축함으로써 영향력 캠페인의 힘을 효과적으로 무디게 할 수 있습니다.

Microsoft는 외국 영향력 작전을 탐지하고 중단할 수 있는 기술적 역량을 강화했으며 사이버 공격에 대한 보고와 같이 이러한 작전에 대해 투명하게 보고하기 위해 최선을 다하고 있습니다.

실행 가능한 인사이트

1. 조직 전체에 강력한 디지털 방역 관행을 구현합니다.
2. 직원이나 비즈니스 관행에 의한 의도하지 않은 사이버 영향력 캠페인 활성화를 줄이는 방법을 고려합니다. 여기에는 알려진 외국 선전 사이트에 대한 공급 감소가 포함됩니다.
3. 정보 문해력 및 시민 참여 캠페인을 사회에서 선전 및 외국의 영향력으로부터 방어하는 데 도움이 되는 핵심 구성 요소로 지원합니다.
4. 영향력 작전을 해결하기 위해 노력하는 업계 내 관련 그룹과 직접 교류합니다.

미주

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. 우크라이나 방어: 사이버 전쟁 초기의 교훈(microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. 러시아 외교부 대변인 Maria Zakharova: https://tass.com/politics/1401777, Lavrov: 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. 러시아 크레멘추크의 주장과 증거 비교—bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. 사실 확인: '술에 취한' Nancy Pelosi 동영상은 조작되었다 | 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. 딥페이크 탐지 챌린지 결과: AI 발전을 위한 개방형 이니셔티브(facebook.com)
20. 딥페이크 2020: 티핑 포인트, Johannes Tammekänd, John Thomas, Kristjan Peterson, 2020년 10월

사이버 회복탄력성

현대화의 위험과 보상을 이해하는 것은 회복탄력성에 대한 총체적인 접근 방식에 매우 중요합니다.

사이버 회복탄력성

개요

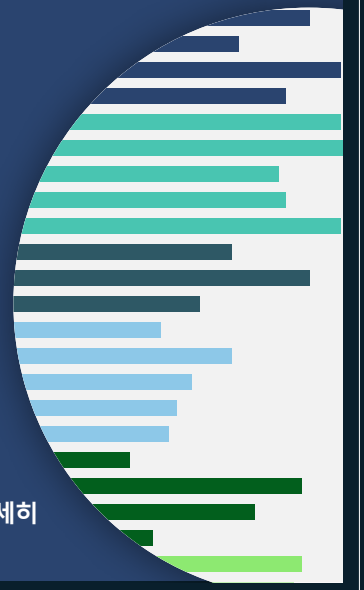
사이버 보안은 기술 성공의 핵심 요소입니다. 혁신과 생산성 강화는 조직이 최신 공격에 최대한 탄력적으로 대처할 수 있도록 하는 보안 조치를 도입해야만 달성할 수 있습니다.

Microsoft는 팬데믹으로 인해 Microsoft의 직원이 어디에서 일하든 보호하기 위해 보안 관행과 기술을 전환해야 했습니다. 지난 한 해 동안 위협 행위자들은 팬데믹과 하이브리드 업무 환경으로의 전환 도중 노출된 취약점을 계속 활용했습니다. 그 이후로 Microsoft의 주요 과제는 다양한 공격 방법의 보급과 복잡성을 관리하고 국가 차원의 활동을 증가시키는 것이었습니다.

효과적인 사이버 회복탄력성을 위해서는 핵심 서비스 및 인프라에 대해 진화하는 위협을 견딜 수 있는 총체적이고 적응력 있는 접근 방식이 필요합니다.

89페이지에서 자세히 알아보기

현대화된 시스템과 아키텍처는 초연결 세상에서 위협을 관리하는 데 중요합니다.

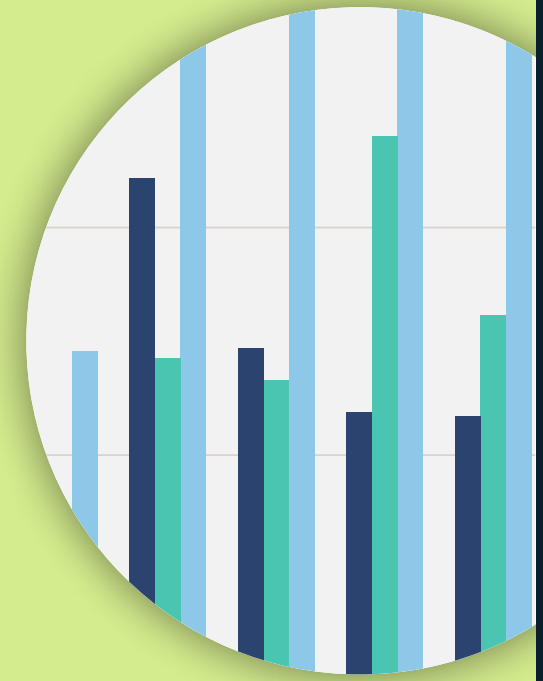


90페이지에서 자세히 알아보기

기본 보안 태세는 고급 솔루션 효율성의 결정적인 요소

92페이지에서 자세히 알아보기

비밀번호 기반 공격이 ID 손상의 주요 원인으로 남아 있지만 다른 유형의 공격이 새롭게 등장하고 있습니다.



93페이지에서 자세히 알아보기

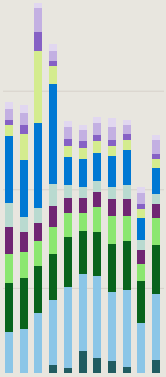
사이버 영향력 작업에 대한 회복탄력성의 인간적 차원은 협업 및 협력 가능한 역량입니다.

102페이지에서 자세히 알아보기

성공적인 사이버 공격의 대부분은 기본적인 보안 방역을 활용하여 예방할 수 있습니다.

08페이지에서 자세히 알아보기

지난 한 해 동안 전 세계는 양, 복잡성, 빈도 면에서 전례 없는 DDoS 활동을 경험했습니다.



98페이지에서 자세히 알아보기

서문

Microsoft는 팬데믹으로 인해 Microsoft의 직원이 어디에서 일하든 보호하기 위해 보안 관행과 기술을 전환해야 했습니다. 지난 한 해 동안 위협 행위자들은 팬데믹과 하이브리드 업무 환경으로의 전환 도중 노출된 취약점을 계속 활용했습니다. 그 이후로 Microsoft의 주요 과제는 다양한 공격 방법의 보급과 복잡성을 관리하고 국가 차원의 활동을 증가시키는 것이었습니다.

디지털 위협 활동과 사이버 공격 수준의 정교함은 매일 증가하고 있습니다. 오늘날 복잡성 높은 공격 중 상당수는 ID 아키텍처, 공급망, 다양한 수준의 보안 제어를 사용하는 서드파티를 손상시키는 데 중점을 둡니다. 특히 ID 피싱 공격이 명백하고 현존하는 위협임을 확인했습니다. 그러나 이러한 공격 유형은 일반적으로 우수한 ID 관리, 피싱 제어, 엔드포인트 관리 관행에서는 성공하지 못합니다. 그렇기 때문에 기본적인 방역 조치를 취하면 공격의 98%를 막을 수 있다는 기본적인 사항을 기억해야 합니다. Microsoft에서는 제로 트러스트 접근 방식의 일환으로 ID 및 디바이스를 관리하며, 관리 방식으로는 위협 행위자를 효과적으로 차단하고 데이터를 보호하기 위한 최소 권한 액세스 및 피싱 방지 개인 인증 정보 등이 있습니다.

오늘날 정교한 기술이 부족한 위협 행위자조차 사이버 범죄 경제에서 고급 전술, 기술, 절차에 대한 액세스가 광범위하게 제공됨에 따라 굉장히 파괴적인 공격을 시작할 수 있습니다. 우크라이나 전쟁은 국가 차원의 공격자들이 랜섬웨어 사용 증가를 통해 공격적인 사이버 작전을 어떻게 확대했는지 보여 주었습니다. 랜섬웨어는 이제 위협 행위자가 이중 또는 삼중 갈취 전술을 활용하여 몸값을 갈취하고 개발자가 RaaS(Ransomware as a Service)를 제공하는 정교한 산업입니다. RaaS를 통해 위협 행위자들은 제휴 네트워크를 활용하여 공격을 수행함으로써 덜 숙련된 사이버 범죄자들의 진입 장벽을 낮춰 궁극적으로 공격자 풀을 확장합니다.

이로 인해 Microsoft는 랜섬웨어 제거 프로그램을 설계했습니다. 이 프로그램의 목표는 제어 및 적용 범위의 격차를 수정하고, 서비스 기능 향상에 기여하며, 랜섬웨어 공격 시 보안 운영 센터 및 엔지니어링 팀을 위한 복구 플레이북을 개발하는 것입니다.

최근 공급망 및 서드파티 공급업체를 대상으로 한 공격은 업계의 주요 변곡점을 나타냅니다. 이러한 공격으로 인해 고객, 파트너, 정부 기관, Microsoft에서 발생하는 중단이 계속해서 증가함에 따라 보안 이해관계자 간의 사이버 회복탄력성 및 협업에 집중하는 것이 중요하다는 사실을 보여줍니다. 또한 악의적 공격자들은 온-프레미스 시스템을 대상으로 하여 조직이 인프라를 현대화하고 보안이 더 강력한 클라우드로 마이그레이션하여 레거시 시스템에서 발생하는 취약성을 관리해야 할 필요성을 높이고 있습니다.

우리는 보안이 기술 성공의 핵심 요소인 시대에 살고 있습니다. 혁신과 생산성 강화는 조직이 최신 공격에 최대한 탄력적으로 대처할 수 있도록 하는 보안 조치를 도입해야만 달성할 수 있습니다. 디지털 위협이 증가하고 진화함에 따라 모든 조직 구조에 사이버 회복탄력성을 구축하는 것이 중요합니다.

Bret Arsenault
최고 정보 보호 책임자

사이버 회복탄력성: 연결된 사회의 중요한 기반

디지털 기술의 혁명으로 조직은 운영 방식과 제공하는 서비스 모두에서 더욱 연결되도록 변화했습니다. 사이버 환경의 위협이 증가함에 따라 조직 구조에 사이버 회복탄력성을 구축하는 것은 재무 및 운영 회복탄력성만큼 중요합니다.

디지털 트랜스포메이션은 조직이 고객, 파트너, 직원, 기타 이해관계자와 상호 작용하는 방식을 영원히 바꿔 놓았습니다. 새로운 기술은 사람들과 소통하고, 제품을 혁신하고, 운영을 최적화할 수 있는 엄청난 기회를 제공합니다. 팬데믹은 사람들이 새로운 방식으로 어디서나 협업할 수 있도록 하는 혁신적인 기술을 주도하여 디지털 트랜스포메이션을 가속화했습니다.

사이버 위협이 엔데믹이 됨에 따라 '항상 연결된' 세상에서 조직을 침해하지 못하도록 방지하는 것은 더욱 어려워지고 있습니다. 사이버 회복탄력성은 빗발치는 공격에도 불구하고 운영을 지속해나가고 성장 가속화를 유지할 수 있는 조직의 역량을 나타냅니다. 예방은 생존 및 복구 역량과 균형을 이루어야 하며 정부 기관과 기업은 사이버 회복탄력성의 일환으로 자산, 데이터, 기타 리소스를 보호하기 위해 보안 및 개인 정보 보호를 넘어 확장되는 포괄적인 모델을 개발하고 있습니다.

사이버 회복탄력성에 대한 총체적인 접근 방식 개발

사이버 회복탄력성을 위해서는 다음과 같이 핵심 서비스 및 인프라에 대해 진화하는 위협을 견딜 수 있는 총체적이고 적응력 있는 글로벌한 접근 방식이 필요합니다.

- Microsoft의 사이버 회복탄력성 벨 곡선에서 설명된 기본 사이버 방역
- 디지털 트랜스포메이션의 위험/보상 트레이드오프에 대한 이해 및 관리
- 위협 및 취약성을 사전에 탐지할 수 있는 실시간 대응 역량
- 자동으로 수정하는 기능을 비롯하여 알려진 공격에 대한 보호 및 새롭고 예상되는 공격 벡터에 대한 예방 활동
- 장애 격리 및 세분화를 통해 공격 및 재해의 영향 감소
- 중단 시, 자동화된 복구 및 중복
- 운영 테스트의 우선순위를 지정하여 격차를 찾고 클라우드 기반 보안 솔루션과 같은 외부 리소스에 대한 공유 책임과 종속성에 대해 이해

효과적인 사이버 회복탄력성 프로그램은 사용 가능한 서비스를 이해하고 중단 시 호출이 가능한 신뢰할 수 있는 리소스 카탈로그를 보유하는 것과 같은 리소스 기본 사항에서 시작됩니다. 이를 기반으로 한 프로그램은 자체 효율성을 평가하고, 주요 서비스 및 종속성의 성능을 측정하고, 온-프레미스 및 클라우드 서비스에서 기능을 테스트 및 검증하고, 조직의 디지털 수명 주기 전반에 걸쳐 지속적인 개선을 제공할 수 있어야 합니다.

총체적인 접근 방식을 제공하기 위해 Microsoft는 조직과 협력하여 가장 중요한 온-프레미스 및 온라인 서비스, 비즈니스 프로세스, 종속성, 직원, 벤더, 공급업체를 식별하고 있습니다. 또한 고객 및 시장 기대치, 규제 및 계약 의무, 내부 운영과 관련된 자산 및 리소스를 식별하고자 합니다. 이러한 주요 리소스가 식별되면 병렬 작업을 통해 위협, 중단, 잠재적 공격 벡터, 시스템, 프로세스 취약점을 탐지하고 모니터링해야 합니다. 지금과 같이 기술이 부족한 상황에서 이를 수행하려면 조직에 제기된 전반적인 위험에 따라 엄격한 우선순위를 지정해야 합니다.

이러한 총체적인 접근 방식 유형은 측정 가능한 성능 강화, 탐지, 대응, 복구 시간 단축, 중단 시 영향 반경 감소를 목표로 하여 지속적으로 진화하는 위협 환경을 배경으로 적응해야 합니다. 이 접근 방식은 증가하는 위협의 연결성 역시 인식해야 합니다. 예를 들어, 보안 인시던트로 인해 개인 정보 보호에 영향을 미치는 데이터 침해가 발생할 수 있기 때문에 다양한 내외부 팀이 신속하게 대응하고 영향을 최소화하기 위해 협력해야 합니다.

사이버 회복탄력성은 기업이 사이버 공격을 포함한 중단에도 불구하고 운영을 계속하고 성장 가속화를 유지할 수 있는 역량입니다.

실행 가능한 인사이트

1. 침해의 영향을 제한하고 침해가 성공하더라도 안전하고 효과적으로 계속 운영할 수 있도록 하는 기술 시스템을 구축하고 관리합니다. 일반적으로 중요한 자산, 민첩성 지원, 적응성 설계(예: 하이브리드, 멀티클라우드, 다중 플랫폼)에 집중하고, 공격 표면을 줄이고(예: 사용하지 않는 애플리케이션 및 과도하게 프로비저닝된 액세스 권한 제거), 침해된 리소스를 가정하고, 악의적 공격자가 진화할 것이라고 예상합니다.
2. 디지털 프로젝트 계획 시, 기회와 함께 잠재적 위협을 고려하고 클라우드 기반 보안 솔루션을 포함한 디지털 기술 공급망 전반의 회복탄력성에 대한 책임을 공유합니다.
3. 설계에 따라 보안을 내장하는 시스템을 구축하고 미래의 진화하는 위협을 예측, 탐지, 저항, 적응, 대응하기 위한 조치를 취합니다.
4. 비즈니스 리더가 새로운 개발과 관련된 위험을 이해할 수 있도록 필요시 보안 팀과 상의하도록 합니다. 마찬가지로 보안 팀은 비즈니스 목표를 고려하고 리더에게 이를 안전하게 추구하는 방법에 대해 조언해야 합니다.
5. 사이버 인시던트에 대한 조직의 회복탄력성을 위해 명확한 운영 관행과 절차가 마련되어 있는지 확인합니다.

시스템 및 아키텍처 현대화의 중요성

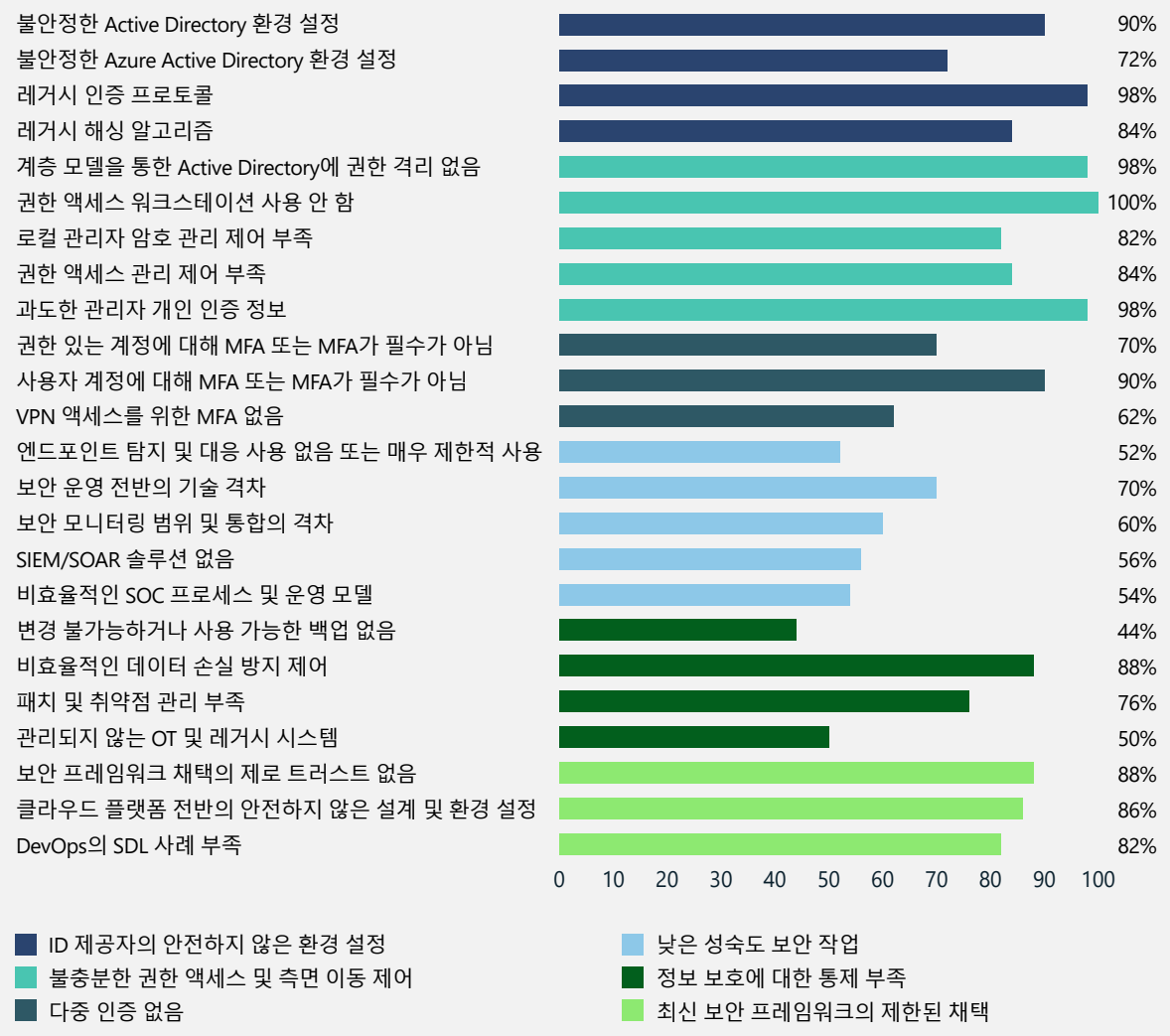
초연결 세상을 위한 새로운 기능을 개발함에 따라 레거시 시스템과 소프트웨어로 인한 위협을 관리해야 합니다.

스마트폰, 태블릿, 클라우드 서비스와 같은 최신 연결 도구가 표준이 되기 전에 개발된 레거시 시스템은 이를 여전히 사용하는 조직에 평균적인 위험이 되었습니다. 이러한 위험 노출은 고객이 공격에 대응하고 공격으로부터 복구하는 데 도움이 되는 보안 전문가 그룹인 Microsoft 보안 서비스 인시던트 대응 팀의 조사 결과로 강화됩니다.

지난 한 해 동안 공격에서 복구하는 고객에게서 발견된 문제는 이 페이지의 차트에 표시된 대로 6가지 범주와 관련이 있었습니다. 다음 페이지에서는 회복탄력성 향상을 위해 수행할 실행 가능한 단계에 대해 간략히 설명합니다.

보안 인시던트 중 80% 이상은 최신 보안 접근 방식을 통해 해결할 수 있는 몇 가지 누락된 요소로 추적될 수 있습니다.

사이버 회복탄력성에 영향을 미치는 주요 문제



이 차트는 조직의 사이버 회복탄력성을 높이는 데 중요한 기본 보안 제어를 놓치는 데 영향을 받는 고객의 비율을 보여줍니다. 조사 결과는 지난 한 해 동안의 Microsoft 계약을 기반으로 합니다.

"리더들은 사이버 회복탄력성을 비즈니스 회복탄력성의 중요한 측면으로 생각해야 합니다. 이들은 자연재해 또는 기타 예상치 못한 이벤트와 같은 방식으로 사이버 중단에 대비하고 운영, 커뮤니케이션, 법률 등과 같은 내부 이해관계자를 한데 모아 전략을 수립해야 합니다. 이렇게 하면 조직이 중요한 비즈니스 시스템을 가능한 한 빨리 온라인 상태로 되돌려 정상적인 비즈니스 운영을 재개할 수 있습니다.

하지만 거기서 끝나지 않습니다. 수많은 조직이 서드파티 공급업체 및 서비스 제공자에 의존하고 있기 때문에 리더들은 사이버 회복탄력성 계획을 엔드 투 엔드 가치 사슬로 확장하여 비즈니스 연속성과 회복탄력성을 더욱 보장해야 합니다."

Ann Johnson,
보안, 규정 준수, ID, 관리 비즈니스 개발 부문
기업 부사장

시스템 및 아키텍처 현대화의 중요성

계속

조직이 접근 방식을 현대화하고 위협으로부터 보호하기 위해 해결할 수 있는 명확한 영역이 있습니다.

문제점	실행 가능한 단계
ID 제공자의 안전하지 않은 환경 설정 ID 플랫폼과 해당 구성 요소의 잘못된 환경 설정 및 노출은 권한 없는 높은 권한 액세스를 얻기 위한 일반적인 벡터입니다.	AD 및 Azure AD 인프라와 같은 ID 시스템을 배포하고 유지 관리할 때 보안에 대한 환경 설정 기준 및 모범 사례를 따릅니다. 권한 분리 및 최소 권한 액세스를 적용하고 ID 시스템 관리를 위해 PAW(권한 있는 액세스 워크스테이션)를 활용하여 액세스 제한을 구현합니다.
불충분한 권한 액세스 및 측면 이동 제어 관리자는 디지털 환경에서 과도한 권한을 가지며 인터넷 및 생산성 위험에 노출되는 워크스테이션에서 관리에 대한 개인 인증 정보를 노출하는 경우가 많습니다.	관리 액세스를 보호하고 제한하여 환경의 회복탄력성을 높이고 공격 범위를 제한합니다. 권한 액세스 관리 제어(예: 적시 액세스 및 충분한 관리)를 사용합니다.
MFA(다중 인증) 없음 오늘날의 공격자는 침입하지 않고 로그온합니다.	MFA는 모든 조직에서 활성화해야 하는 중요하면서 기본적인 사용자 액세스 제어입니다. 조건부 액세스와 함께 MFA는 사이버 위협에 대처하는 데 매우 유용할 수 있습니다.
낮은 성숙도 보안 작업 영향을 받는 대부분의 조직은 기존 위협 탐지 도구를 사용했으며 시기적절한 대응 및 수정을 위한 관련 인사이트가 없었습니다.	포괄적인 위협 탐지 전략에는 XDR(확장 탐지 및 대응)과 머신 러닝을 사용하여 신호에서 노이즈를 분리하는 최신 클라우드 네이티브 도구에 대한 투자가 필요합니다. 디지털 환경 전반에 걸쳐 심층적인 보안 인사이트를 제공할 수 있는 XDR을 통합하여 보안 운영 도구를 현대화합니다.
정보 보호에 대한 통제 부족 조직은 데이터 위치 전반에 걸쳐 전체 범위를 포괄하고 정보 수명 주기 전반에 걸쳐 효율성을 유지하며 데이터의 비즈니스 중요도에 부합하는 총체적인 정보 보호 제어를 통합하기 위해 계속해서 고군분투하고 있습니다.	중요한 비즈니스 데이터가 무엇이고 어디에 있는지 식별합니다. 정보 수명 주기 프로세스를 검토하고 데이터 보호를 적용하는 동시에 비즈니스 연속성을 보장합니다.
최신 보안 프레임워크의 제한된 채택 ID는 서로 다른 디지털 서비스 및 컴퓨팅 환경에 대한 액세스를 지원하는 새로운 보안 경계입니다. 제로 트러스트 원칙, 애플리케이션 보안, 기타 최신 사이버 프레임워크를 통합하면 조직이 상상하기 어려울 수 있는 위험을 사전에 관리할 수 있습니다.	제로 트러스트 프레임워크는 최소 권한 및 모든 액세스에 대한 명시적인 확인의 개념을 적용하고 항상 손상을 가정합니다. 또한 조직은 비즈니스 시스템에서 더 높은 수준의 보증을 위해 DevOps 및 애플리케이션 수명 주기 프로세스에서 보안 제어 및 관행을 구현해야 합니다.

기본 보안 태세는 고급 솔루션 효율성의 결정적인 요소

분석을 통해 Microsoft는 고급 보안 솔루션이 있는 경우에도 공격자들이 초기 액세스 권한을 얻고, 발판을 구축하며, 공격을 구현할 수 있도록 하는 조직 방어의 일반적인 사각지대가 만연하다는 사실을 발견했습니다.

대부분의 경우, 사이버 공격의 결과는 공격이 시작되기 훨씬 전에 결정됩니다. 공격자들은 취약한 환경을 활용하여 초기 액세스 권한을 얻고, 감시를 수행하며, 횡적 이동과 암호화 또는 유출을 통해 혼란을 야기합니다. 조기에 공격자를 차단하면 전반적인 영향을 줄일 수 있는 기회가 크게 증가합니다.

Microsoft는 이러한 환경에서 실제 사례의 가장 일반적인 단점을 식별하기 위해 보안 태세의 특정 환경 설정을 연구했습니다. 이를 통해 위협 행위자가 탐지되지 않은 네트워크에 대한 액세스 권한을 확보하고 이를 통해 이동할 수 있도록 하는, 사람이 운영하는 랜섬웨어 공격 중에 가장 일반적으로 악용되는 취약점을 확인할 수 있었습니다.

기본 보안에 대한 환경 설정이 켜져 있어야 함

온보딩되지 않았거나 오래된 조직의 디바이스(취약점 및 보안 에이전트 상태 관련)는 공격자의 잠재적인 진입점 및 액세스 설정 경로 역할을 합니다. 업데이트된 EDR(엔드포인트 탐지 및 대응)[1] 및 EPP(엔드포인트 보호 플랫폼)[2] 솔루션을 통해 조직의 디바이스를 온보딩하는 것이 중요한 단계이지만 랜섬웨어를 중지한다는 보장은 없습니다.

EDR 및 EPP와 같은 고급 솔루션은 초기 공격 흐름에 공격자를 탐지하고 자동 수정 및 보호를 지원하는 데 중요합니다. 그러나 이러한 고급 솔루션은 공격을 탐지하는 기본적인 기능에 의존하기 때문에 기본 보안에 대한 환경 설정을 켜야 합니다. 실제로 기본 보안에 대한 환경 설정의 부재로 인해 훼손된 고급 솔루션이 있는 시나리오가 만연했습니다.

보안에 대한 환경 설정 모범 사례는 SOC(보안 운영 센터) 분석가 대응 시간보다 회복탄력성을 나타내는 더 큰 지표입니다.

SOC 분석가가 고객 및 파트너 모집단에서 6개월이 넘는 기간 동안 관련 경고를 보고 조치를 취하는 데 걸리는 시간이 70% 단축되는 것을 확인했습니다. 이러한 인식의 증대는 좋은 징조입니다. 그러나 보안에 대한 환경 설정 가시성은 SOC 분석가의 성능을 향상시켰지만 조직의 디바이스를 온보딩하고 업데이트하여 제품 가시성을 활성화하는 것이 성공적인 예방을 더 잘 예측하는 요소였습니다.

알 수 없는 디바이스로 인한 위험

고객이 어떤 자산이 어떤 운영 체제에서 실행되고 있는지 알고 있는 클라우드 네트워크와 달리 온-프레미스 네트워크에는 조직에서 모니터링하거나 관리하지 않는 IoT, 데스크톱, 서버, 네트워크 디바이스와 같은 다양한 디바이스가 포함될 수 있습니다.

엔터프라이즈급 네트워크에는 평균적으로 EDR 에이전트로 보호되지 않고 기업 리소스 또는 고부가가치 자산에 액세스할 수 있는 3,500개 이상의 연결된 디바이스가 있습니다. MDE(Microsoft Defender for Endpoint)는 네트워크 검사를 사용하여 디바이스를 발견하고 디바이스 이름, 운영 체제 배포, 디바이스 유형과 같이 네트워크에 연결된 사용자의 디바이스 분류에 대한 정보를 제공합니다.

3,500개

평균적으로 엔드포인트 탐지 및 대응 에이전트로 보호되지 않는 기업의 연결된 디바이스 수

EDR 에이전트에서 지원하지 않는 디바이스의 경우 최소한 디바이스의 존재를 인식하고 취약점을 평가하고 네트워크 액세스를 제한하여 디바이스를 보호해야 합니다.

실행 가능한 인사이트

1. 고급 솔루션조차 보안 관련 기본 환경 설정이 없기 때문에 훼손될 수 있습니다.
2. 보안 태세 환경 설정의 모범 사례에 투자하여 향후 공격으로부터 보호합니다. 이러한 기본 설정은 공격으로부터 방어하는 조직의 능력 측면에서 막대한 투자 수익을 창출합니다.
3. 적용 가능한 모든 디바이스를 EDR 솔루션에 온보딩합니다.
4. 보안 에이전트를 업데이트하고 변조로부터 보호하여 제품의 가시성을 높이고 더 완전한 보안 이점을 얻을 수 있도록 합니다.

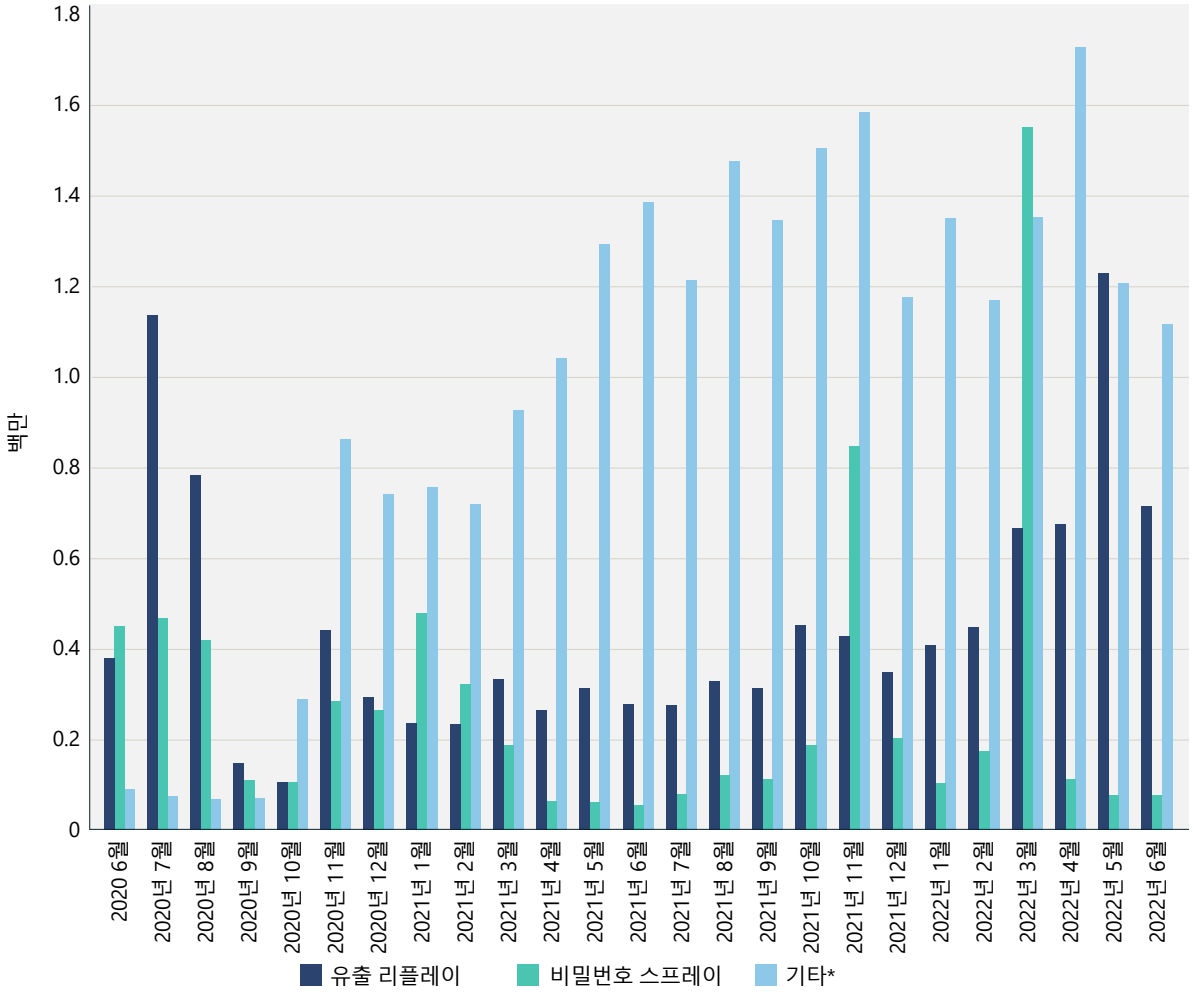
ID의 건전한 상태를 유지하는 것은 조직 웰빙의 기본

ID 보호는 그 어느 때보다 중요합니다. 비밀번호 기반 공격이 ID 손상의 주요 원인으로 남아 있지만 다른 유형의 공격이 새롭게 등장하고 있습니다. 정교한 공격의 양은 비밀번호 스프레이 및 위반 재생의 이전 표준에 비해 계속 증가하고 있습니다.

비밀번호 기반 공격은 여전히 일반적이며 이러한 방법을 통해 침해된 계정 중 90% 이상이 강력한 인증으로 보호되지 않습니다. 강력한 인증은 둘 이상의 인증 요소(예: 암호 + SMS 및 FIDO2 보안 키)를 사용합니다.

표적 비밀번호 스프레이 공격이 증가했으며 수천 개의 IP 주소에 분산된 공격자 트래픽의 양이 매우 급증했습니다.

공격 범주별로 침해된 사용자



매달 공격 범주별로 침해된 사용자입니다. 비밀번호 스프레이 공격량은 2021년 11월과 2022년 3월의 급증에서 볼 수 있듯이 변동성이 매우 컸습니다. 이러한 급증은 수천 명의 사용자와 수천 개의 IP 주소가 영향을 받았다는 사실을 나타냅니다. *'기타'는 피싱, 맬웨어, 중간자 공격(man-in-the-middle), 온-프레미스 토큰 발급자 손상 등을 포함하여 비밀번호 스프레이 및 위반 재생과 다른 공격을 나타냅니다. 출처: Azure AD ID 보호.

4,500건

이 설명을 읽는 데 걸리는 시간 동안 Microsoft는 4,500건의 비밀번호 공격을 방어했습니다.

ID의 건전한 상태를 유지하는 것은 조직 웰빙의 기본

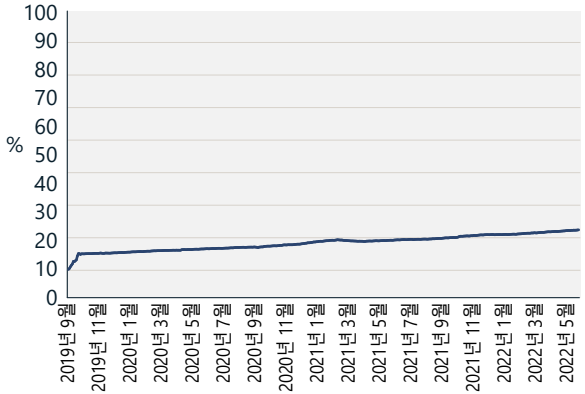
계속

강력한 인증 채택

긍정적인 점은 Azure AD(Azure Active Directory) 엔터프라이즈급 고객 기반 사이에서 강력한 인증 채택이 꾸준히 증가하고 있다는 점입니다. Azure AD의 경우 강력한 인증 MAU(월간 활성 사용자)는 작년 19%에서 26%로 증가한 반면, 관리 계정에 대한 강력한 인증 MAU는 30%에서 약 33%로 증가했습니다.

이러한 추세는 긍정적이지만 대다수의 강력한 인증에 도달하려면 여전히 상당한 성장이 필요합니다. 해당 환경에서 아직 강력한 인증을 사용하지 않는 고객은 사용자를 보호하기 위해 강력한 인증의 계획 및 배포를 시작해야 합니다.[3] 강력한 인증 배포를 설계하는 동안 비밀번호없는 인증은 가장 안전한 사용 환경을 제공하여 비밀번호 공격의 위험을 제거하므로 고려되어야 합니다.

강력한 인증 사용
(2019년 9월~2022년 5월)

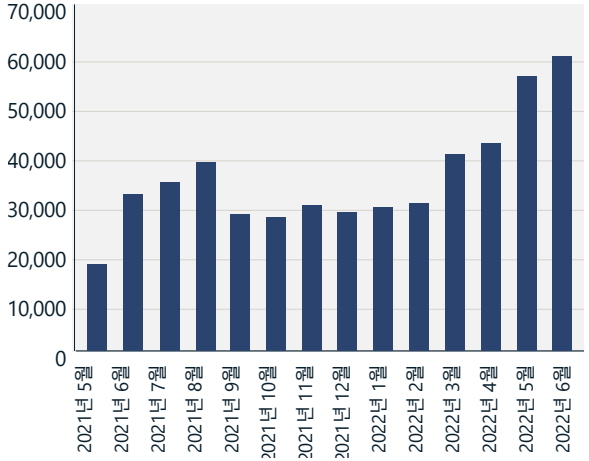


강력한 인증 사용량은 2019년 이후 두 배로 증가했지만 사용자 중 26%와 관리자 중 33%만이 강력한 인증을 사용하고 있습니다. 출처: Azure Active Directory.

토큰 재생 공격의 꾸준한 증가

다른 공격 형태의 비중은 2022년에 증가했습니다. 탐지 가능성을 줄이기 위해 암호 기반 인증을 피하는 표적 공격이 증가했습니다. 이러한 공격은 브라우저 SSO(싱글 사인온) 쿠키 또는 맬웨어, 피싱, 기타 방법을 통해 얻은 새로 고침 토큰을 활용합니다. 경우에 따라 공격자들은 탐지 가능성을 더욱 줄이기 위해 대상으로 한 사용자의 지리적 위치 근처에 있는 인프라를 선택합니다. 토큰 재생 공격이 꾸준히 증가하여 Azure AD ID 보호에서 매월 40,000건 이상이 탐지되었습니다. 토큰 재생은 해당 토큰을 소유한 공격자가 합법적인 사용자에게 발급한 토큰을 사용하는 것입니다. 토큰은 일반적으로 사용자의 브라우저에서 쿠키를 추출하거나 고급 피싱 방법으로 맬웨어를 통해 얻습니다.

탐지된 토큰 재생 공격의 양



매월 탐지된 토큰 재생 공격. 출처: Azure AD ID 보호, 비정상적인 토큰 검색으로 플래그가 지정된 고유한 세션.

ID의 건전한 상태를 유지하는 것은 조직 웰빙의 기본

계속

토큰 추출

공격자는 맬웨어보다 더 많은 개인 인증 정보가 있어야 목표를 달성할 수 있습니다. 실제로 사람이 운영하는 모든 랜섬웨어 공격에는 100% 도난당한 개인 인증 정보가 포함됩니다. 수많은 정교한 침입에는 다크 웹에서 구매한 개인 인증 정보가 포함되는데, 이는 처음에 정교하지 않고 광범위하게 배포된 개인 인증 정보 도난 맬웨어에서 도난당한 개인 인증 정보입니다. 이러한 맬웨어 형식은 세션 정보 및 MFA 클레임을 포함한 토큰을 훔치도록 발전했습니다. 즉, 사용자가 회사 자산에 로그인하는 홈 시스템의 감염은 회사 네트워크에 대한 심각한 인시던트로 이어질 수 있습니다.

공격자들은 또한 피해자가 피싱 이메일 또는 인스턴트 메시지의 악성 링크를 클릭하고 ID 제공자의 합법적인 로그인 페이지처럼 보이는 웹 사이트로 연결되는 중간자(man-in-the-middle) 공격을 통해 피해자의 디바이스에서 토큰을 추출할 수 있습니다. 실제로 이는 사용자와 ID 제공자 간의 모든 트래픽을 릴레이하고 가로채는 공격자가 만든 웹 서비스입니다. 공격자는 사용자 이름과 암호를 가로채고 MFA 챌린지를 릴레이할 수도 있습니다. 이로 인해 ID 제공자가 발급하고 공격자가 가로채 토큰에 공격자가 MFA 요구 사항을 충족하는 데 사용할 수 있는 MFA 클레임이 포함될 수 있습니다.

Microsoft Defender for Cloud Apps는 2022년 초부터 매월 평균 895건의 해당 공격을 탐지했습니다. 이러한 공격 형태는 인증서 기반 인증, Windows Hello for Business 또는 FIDO2 보안 키와 같은 MFA의 피싱 방지 요소를 활용하여 방지할 수 있습니다.

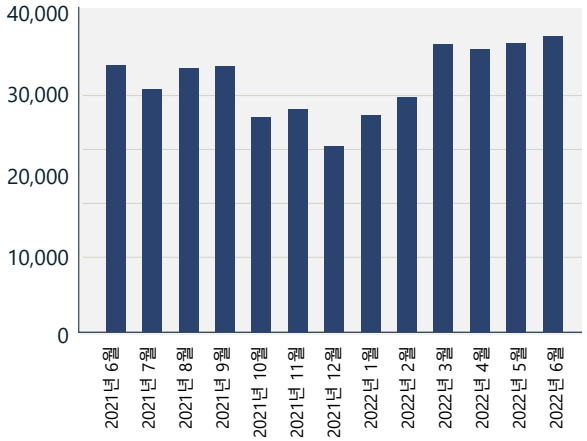
암호 기반 공격은 계정이 손상되는 주요 방법입니다.

MFA 피로

공격자는 'MFA 피로'라는 개념을 활용하여 피해자가 실수 또는 피로의 결과로 요청을 수락하기를 바라며 피해자의 디바이스에 여러 MFA 요청을 생성합니다. 이러한 공격은 Microsoft Authenticator와 같은 최신 인증자 앱을 숫자 일치[4] 및 추가 컨텍스트 지원[5]과 같은 기능과 결합하여 방지할 수 있습니다. Azure AD ID 보호는 매월 30,000건의 MFA 피로 공격이 있는 것으로 추정됩니다.

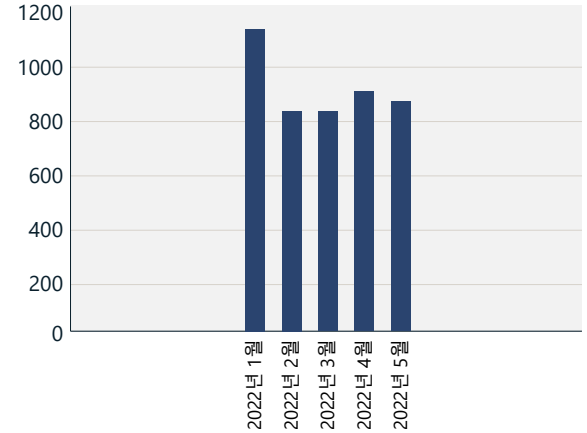
정교한 공격의 비중이 계속 증가하고 있는데, 이는 다중 인증의 피싱 방지 요소에 대한 필요성을 강조합니다.

MFA 피로 공격의 예상 인스턴스



출처: Azure AD ID 보호.

중간자(man-in-the-middle) 공격 이후 탐지된 피싱 인스턴스



출처: Microsoft Defender for Cloud Apps.

실행 가능한 인사이트

1. 조직 전체의 모든 계정이 강력한 인증 방법으로 보호되는지 확인합니다.
2. 비밀번호 없는 인증은 가장 안전하고 사용자 친화적인 환경을 제공하여 비밀번호 공격의 위험을 제거합니다.
3. 전체 조직에서 레거시 인증을 사용하지 않도록 합니다.
4. 피싱 방지 형태의 강력한 인증으로 고부가가치 및 관리 계정을 보호합니다.
5. 온-프레미스 ID 제공자에서 클라우드 ID 제공자까지 현대화하고 모든 앱을 클라우드 기반 ID 제공자에 연결하여 일관된 사용자 환경과 보안을 제공합니다.

추가 정보에 대한 링크

› 이번 세계 비밀번호의 날 (World Password Day)에서는 비밀번호를 완전히 버리는 것을 고려하고 있습니다. | Microsoft Security

운영 체제 기본 보안 설정

보안 위협 환경이 지속적으로 진화함에 따라 사이버 회복탄력성을 개선하기 위해 기본적으로 환경 설정된 컴퓨터 보안에 대한 필요성이 증가하고 있습니다. 운영 체제 보안은 그 어느 때보다 시급하고 복잡하며 비즈니스에 중요하지만, 올바르게 관리하는 것은 어려울 수 있습니다.

과거에는 컴퓨터 및 디바이스 보안에 고객 또는 IT 전문가가 원하는 수준으로 환경 설정해야 하는 내장형 보안 기능이 포함되었습니다. 공격자가 목표를 달성하기 위해 자동화, 클라우드 인프라, 원격 액세스 기술에서 더욱 고급화된 도구를 활용하고 있기 때문에 이러한 접근 방식은 더 이상 적절하지 않습니다. 칩에서 클라우드에 이르기까지 모든 보안 계층이 기본적으로 환경 설정되는 것이 중요해졌습니다. Microsoft는 기본적으로 Windows 운영 체제 보안을 환경 설정하도록 발전했습니다.[6]

계층화된 보안 태세, 새로운 보안 기능, 정기적이고 일관적인 패치 및 업데이트, 피싱 및 기타 사기를 신고하기 위한 보안 교육 및 인식 등 심층적인 방어를 수용하는 고객은 맬웨어를 줄일 수 있습니다.

심층 방어를 단순화하기 위해 Windows 11에는 메모리 무결성, 보안 부팅, 신뢰할 수 있는 플랫폼 모듈 2.0을 포함하여 기본적으로 긴밀하게 통합된 하드웨어 및 소프트웨어 보호가 켜져 있습니다. 지원되는 하드웨어를 사용하는 Windows 10 사용자는 Windows 설정 앱 또는 BIOS 메뉴에서 이러한 기능을 켤 수도 있습니다.

일반적으로 구형 디바이스는 하드웨어 보안과 소프트웨어 보안 기술 간에 강력한 조정이 없는 경우가 많습니다. 기본적으로 보안이 활성화되지 않은 디바이스는 가능한 경우 설정에서 수동으로 환경 설정합니다.[7]

기본적으로 보안이 활성화되지 않은 디바이스는 가능한 경우 설정에서 수동으로 환경 설정하는 것이 좋습니다.

하드웨어 및 소프트웨어 수명 주기 전반에 걸쳐 보호를 제공하는 데 도움이 되는 지속적인 운영 체제 업데이트 및 보안 패치를 사전에 적용하세요.

실행 가능한 인사이트

1. 신뢰할 수 있는 플랫폼 모듈에서 로그온 개인 인증 정보를 바인딩하는 암호 없는 솔루션을 사용하고, 특히 FIDO(Faster Identity Online, 더 빠른 ID 온라인) 얼라이언스[8] 업계 표준을 충족하는 비밀번호 없는 솔루션을 찾습니다.
2. 조직 디바이스에서 사용되지 않고 오래된 실행 파일을 모두 적시에 정리합니다.
3. 메모리 무결성, 보안 부팅, 신뢰할 수 있는 플랫폼 모듈 2.0(기본적으로 사용하도록 설정되지 않은 경우)을 활성화하여 고급 펌웨어 공격으로부터 보호함으로써 최신 CPU에 내장된 기능을 활용하여 부팅을 강화합니다.
4. 데이터 암호화 및 개인 인증 정보를 켭니다.
5. 애플리케이션 및 브라우저 컨트롤을 활성화하여 신뢰할 수 없는 애플리케이션 및 기타 내장된 악용 방지 기능으로부터 강화된 보호를 제공합니다.
6. 메모리 액세스 보호를 활성화하여 누군가 외부에서 액세스할 수 있는 포트에 악성 디바이스를 연결하는 것과 같은 일상적인 물리적 공격으로부터 보호합니다.

추가 정보에 대한 링크

- Windows 보안 가이드북 | 상업용
- Windows 11의 새로운 보안 기능은 하이브리드 업무를 보호하는 데 도움이 됩니다 | Microsoft Security 블로그

소프트웨어 공급망 중심성

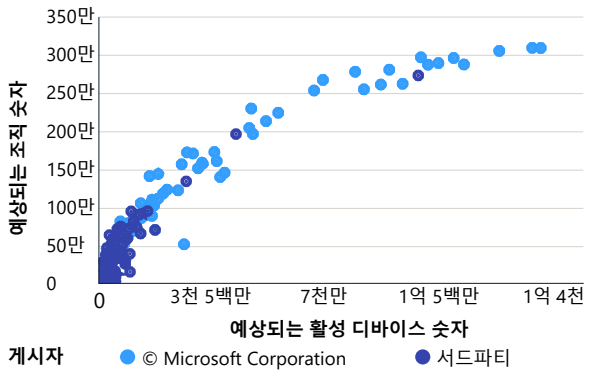
서드파티 앱, 플러그인, 확장에 대한 공격은 공급 생태계에서 중심적인 역할을 하는 공급업체에 대한 고객의 신뢰를 약화시킬 수 있습니다. 네트워크 이론을 활용하여 소프트웨어 중심성을 살펴보면 특히 중앙 앱에 대한 패치의 중요성을 조명하는 데 도움이 됩니다.

1,800만 개의 애플리케이션 실행 파일로 구성된 Windows App Network가 500만 개의 조직에 설치 및 사용되어 소프트웨어 생태계의 최상의 뷰를 제공합니다. 가장 많이 사용되는 10만 개의 애플리케이션 중 97%는 업데이트 및 보안 패치를 유지 관리하는 서드파티 조직에서 생성됩니다. 이는 상업용 애플리케이션 생태계의 두 가지 중요한 특성을 보여줍니다.

첫째, Windows 상업용 애플리케이션 생태계에는 중심성이 있습니다. (1,800만 개 중) 상위 10만 개의 애플리케이션만 1,000개 이상의 디바이스에서 사용됩니다. 즉, 이러한 애플리케이션의 1% 중 절반 이상이 디바이스 생태계에서 이러한 광범위한 영향을 미칩니다.

둘째, 상위 1만 개 애플리케이션 공급업체가 가장 많이 사용되는 상업용 애플리케이션의 업데이트 및 보안 패치를 관리하는 이러한 애플리케이션 관리 효율성에는 다양성이 있습니다. 이는 회사가 다양한 소프트웨어 공급업체의 보안, 규정 준수, 관리 제어에 대한 상호 의존성을 보여줍니다.

가장 많이 사용되는 애플리케이션의 상업용 보급



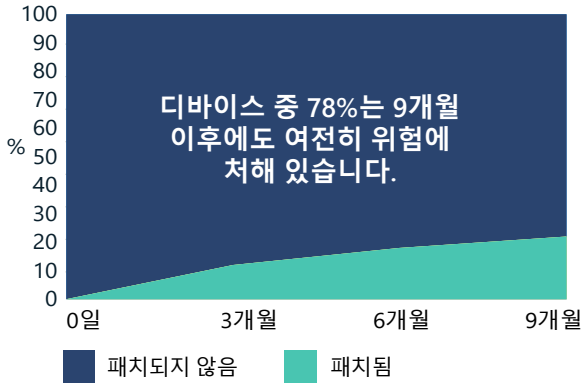
상위 애플리케이션은 수백만 개의 조직과 수천만 개의 디바이스에서 사용됩니다. 애플리케이션은 거의 유비쿼터스에 가까운 특징을 갖고 있기 때문에 악의적 공격자들은 사용자를 기반으로 한 수백만 개의 디바이스에 영향을 미칠 수 있는 이러한 상위 애플리케이션의 취약점을 악용하기 위해 지속적으로 주시하고 있습니다.

수백만 개의 상업용 디바이스가 패치 릴리스 후 몇 달 또는 제품 지원이 종료된 후에도 여전히 취약한 애플리케이션 버전을 사용합니다. 예를 들어, 2017년 이후로 지원되지 않는 PDF 판독기 버전을 실행하는 활성 Windows 상업용 디바이스가 백만 개 이상 있습니다.

지원되지 않는 이전 버전의 애플리케이션은 수백만 개의 상업용 디바이스에서 계속 사용되고 있습니다. 그 결과, 조직은 패치되지 않는 취약점을 보유할 위험이 있습니다.

지원 중인 애플리케이션 버전의 경우, 회복탄력성을 높이는 추세와 정반대로 중요한 패치 채택 속도가 정체되고 있습니다. 대신, 곡선에서 필요한 회복탄력성을 달성하기 위해 매월 패치의 기하급수적으로 상향 채택하는 모습을 보여줘야 합니다.

중요한 패치 배포 비율



브라우저 세트의 134개 버전에 영향을 미치는 치명적인 취약점을 조사한 결과, 패치가 릴리스된 지 9개월이 지난 후에도 78%인 수백만 대의 디바이스가 영향을 받는 버전 중 하나를 아직도 사용하고 있었습니다.

Microsoft에서는 InterpretML[9] 툴킷을 사용하여 이전 앱 버전의 디바이스를 보유할 가능성이 더 높은 조직과 상관관계가 있는 특성을 식별했습니다. 이러한 예측 변수 중 가장 중요한 변수는 낮은 디바이스 참여 시간, 아시아 태평양 및 라틴 아메리카와 같은 지리적 영역, 자동차, 화학, 통신, 운송 및 물류, 건강 의료기관(청구 처리자), 보험과 같은 산업이었습니다.

소프트웨어 회복탄력성 유지 관리에는 사용하지 않는 애플리케이션을 정기적으로 사용하지 않도록 설정하거나 제거하는 작업이 포함되어야 합니다.

조직의 보안 및 규정 준수는 조직의 노력과 소프트웨어 공급업체의 노력에 달려 있습니다.

실행 가능한 인사이트

1. 조직을 통해 모든 애플리케이션과 엔드포인트에 대해 시기적절한 업데이트를 수행합니다.
2. 조직 디바이스에서 사용되지 않고 오래된 실행 파일을 모두 적시에 정리합니다.

추가 정보에 대한 링크

- Microsoft Intune 설명서 | Microsoft Docs
- 앱 관리 | Microsoft Docs
- Microsoft Defender for Endpoint | Microsoft Security
- OSS 보안 공급망 프레임워크 | Microsoft Security Engineering
- Microsoft 오픈 소스 소프트웨어 보안 공급망 프레임워크 | GitHub

새롭게 떠오르는 DDoS, 웹 애플리케이션, 네트워크 공격에 대한 회복탄력성 구축

가속화된 디지털 트랜스포메이션은 기존 네트워크 및 보안 경계 모델에 종지부를 찍었습니다. 클라우드로 마이그레이션한다는 것은 기업이 디지털 자산을 보호하기 위해 클라우드 네이티브 네트워크 보안을 채택해야 함을 의미합니다.

공격 복잡성, 빈도, 양은 계속해서 증가하고 있으며 더 이상 휴가철에만 국한되지 않아 연중 내내 진행되는 공격으로의 전환을 나타냅니다. 이는 전통적으로 트래픽 사용량이 가장 높은 시즌을 넘어 지속적인 보호의 중요성을 강조합니다.

DDoS(분산형 서비스 거부) 공격

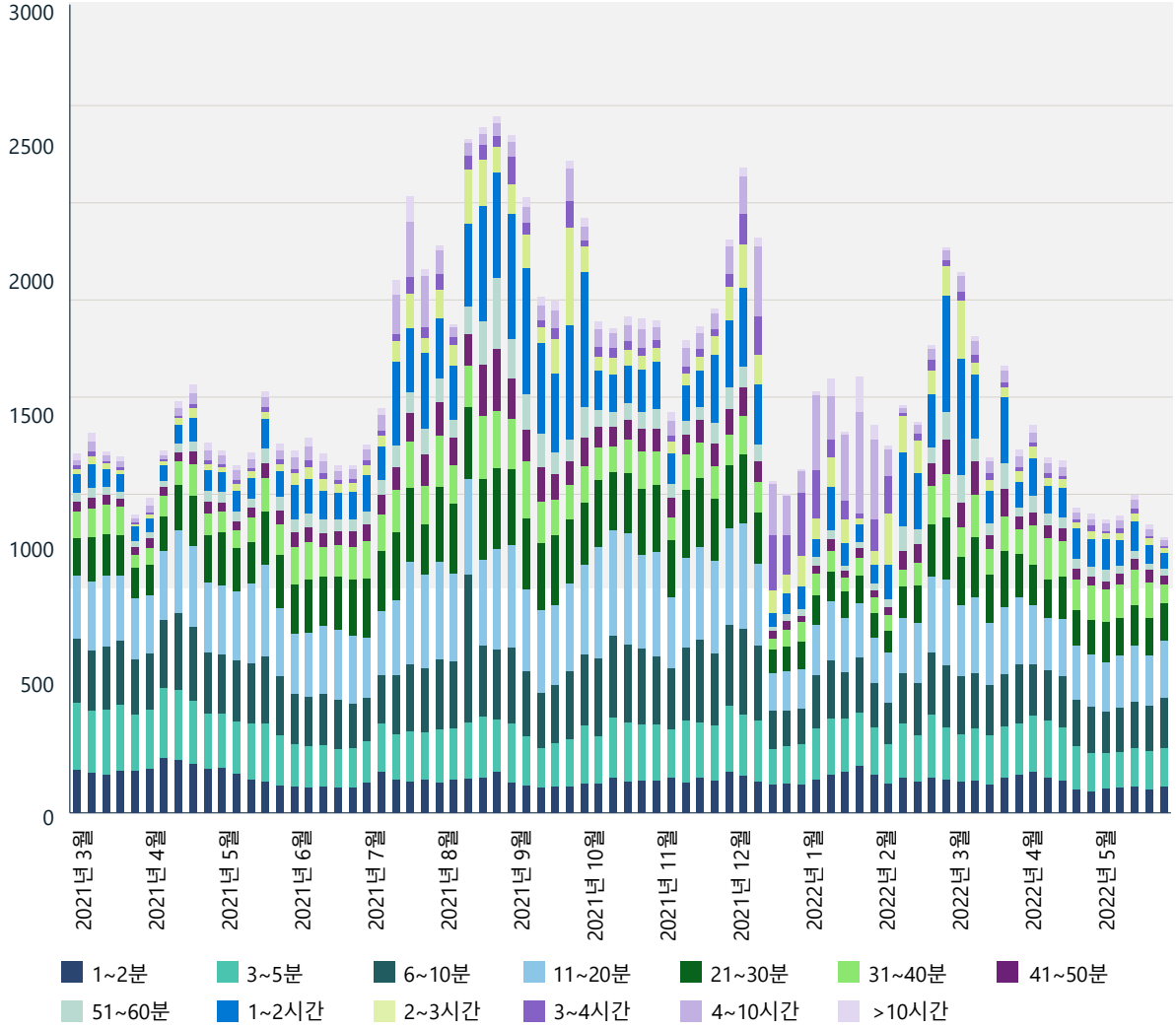
지난 한 해 동안 전 세계는 양, 복잡성, 빈도 면에서 전례 없는 DDoS 활동을 경험했습니다. 이 폭발적인 DDoS는 국가 차원의 공격의 상당한 증가와 저비용 DDoS 공격 대행 서비스의 지속적인 확산에 의해 주도되었습니다. Microsoft는 하루 평균 1,955건의 공격을 완화했는데, 이는 전년 대비 40% 증가한 수치입니다. 이전에는 일반적으로 연말연시에 공격이 가장 많이 발생했습니다. 그러나 올해 하루 동안 가장 많은 공격이 기록된 날은 2021년 8월 10일이었습니다. 이는 연중 내내 계속되는 공격으로의 전환을 나타낼 수 있으며 전통적으로 트래픽 사용량이 가장 높은 시즌을 넘어 지속적인 보호의 중요성을 강조합니다.

2021년 11월, Microsoft는 여러 국가에 걸쳐 있는 약 1만 개의 소스에서 3.4Tbps(초당 테라비트)의 처리량으로 볼류메트릭 DDoS 공격을 차단했습니다. 2+Tbps 이상의 유사한 대용량 볼류메트릭 공격이 2022년에 완화된 것은 공격의 복잡성과 빈도뿐만 아니라 공격의 양(대역폭)도 증가하고 있음을 강조합니다.

공격 기간

지난 한 해 동안 관찰된 대부분의 공격은 수명이 짧았습니다. 공격의 약 28%는 10분 미만, 26%는 10~30분, 14%는 31~60분 동안 지속되었습니다. 공격의 32%는 한 시간 이상 지속되었습니다.

DDoS 공격 횟수 및 기간 분포
(2021년 3월~2022년 5월)



작년에 진행된 대부분의 공격은 수명이 짧았습니다. 공격의 약 28%는 10분 미만으로 지속되었습니다.

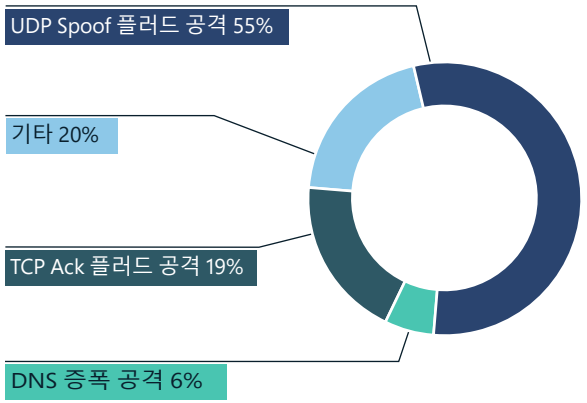
새롭게 부상하는 DDoS에 대한 회복탄력성 구축, 웹 애플리케이션 및 네트워크 공격 계속

DDoS 공격 벡터

작년에 일반적으로 사용된 공격 벡터는 SSDP(Simple Service Discovery Protocol, 심플 서비스 디스커버리 프로토콜), CLDAP(Connectionless Lightweight Directory Access Protocol, 비연결형 경량 디렉터리 접근 프로토콜), DNS(Domain Name System, 도메인 이름 시스템), 단일 피크로 구성된 NTP(Network Time Protocol, 네트워크 타임 프로토콜)를 활용하여 포트 80에 대한 UDP(User Datagram Protocol, 사용자 데이터그램 프로토콜)의 리플렉션이었습니다. 또한 웹 사이트를 대상으로 하는 애플리케이션 계층 DDoS 공격이 1,630만 피크 RPS(초당 요청 수)와 9.89Tbps 피크 트래픽으로 증가했습니다.

2022년에 Microsoft는 매일 거의 2,000건의 DDoS 공격을 완화하고 역사상 보고된 최대 규모의 DDoS 공격을 차단했습니다.

DDoS 공격 벡터



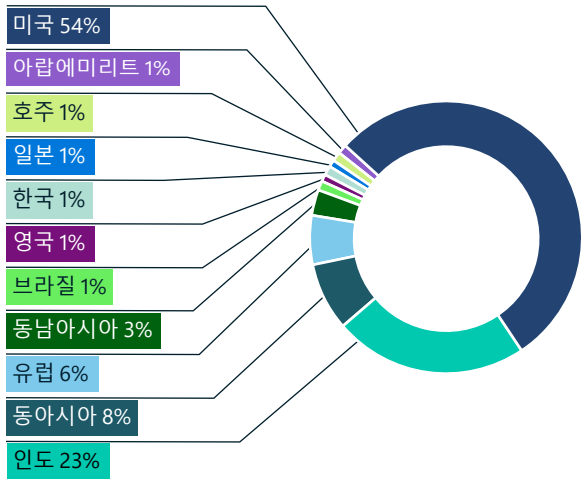
UDP Spoof 플러드 공격은 2022년 상반기에 16%에서 55%로 증가하여 상위 벡터가 되었습니다. TCP Ack 플러드 공격은 54%에서 19%로 감소했습니다.

게임 산업은 주로 Mirai 봇넷의 변종과 소량 UDP 프로토콜 공격으로 인해 DDoS 공격의 주요 표적이 되고 있습니다. UDP는 일반적으로 게임 및 스트리밍 애플리케이션에서 사용되기 때문에 공격 벡터의 압도적인 다수는 UDP Spoof 플러드였으며 일부는 UDP 리플렉션 및 증폭 공격이었습니다.

지리적 대상 지역

지난 한 해 동안 탐지된 DDoS 공격 중 54%는 미국 내 표적을 대상으로 수행되었으며, 이러한 추세는 대부분의 Azure 및 Microsoft 고객이 미국에 있다는 사실로 어느 정도 설명될 수 있습니다. 또한 인도를 대상으로 한 공격은 전체 공격 중 2%(2021년 하반기)에서 23%(2022년 상반기)로 급격히 증가했습니다. 동아시아, 특히 홍콩은 8%로 여전히 인기 있는 대상입니다. 유럽의 경우, 암스테르담, 비엔나, 파리, 프랑크푸르트 지역에 대한 공격이 집중되었습니다.

DDoS 공격 대상

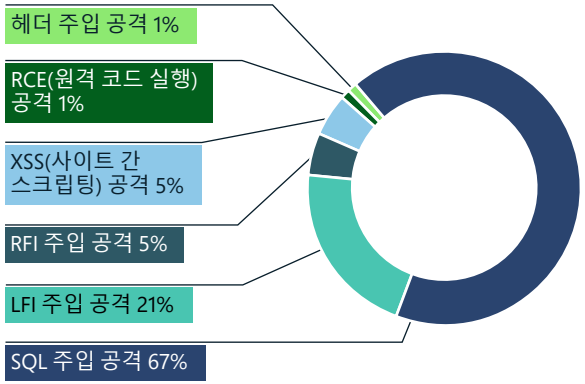


Microsoft는 아시아를 대상으로 한 많은 양의 공격의 원인이 특히 중국, 일본, 한국, 인도 내 지역의 거대한 게임 입지에 있다고 생각합니다. 스마트폰 보급률 증가로 인해 모바일 게임의 인기가 높아짐에 따라 이러한 입지는 계속해서 확장되어 이 지리적 대상이 계속해서 증가할 것임을 시사합니다.

웹 애플리케이션 악용

WAF(웹 애플리케이션 방화벽)는 DDoS 보호와 함께 웹 및 API(애플리케이션 프로그래밍 인터페이스) 자산을 보호하기 위한 심층 방어 전략의 필수적인 부분을 형성합니다. Microsoft에서는 Azure WAF를 통해 매월 3,000억 개 이상의 WAF 규칙이 트리거되는 것을 확인했습니다.

가장 많이 퍼진 공격 배포 유형



Azure WAF는 매일 수십억 건의 OWASP(Open Web Application Security Project, 개방형 웹 애플리케이션 보안 프로젝트) 상위 10개[10] 공격을 탐지합니다. Microsoft에서 확인한 신호에 따르면 공격자들은 대부분 SQL 삽입 공격을 시도한 후 로컬 파일 삽입 및 원격 파일 삽입 공격을 시도했습니다. 이는 주입 공격이 세 번째로 일반적인 웹 공격 유형이라는 사실을 보여 주는 OWASP 상위 10개 목록과 일치합니다.

또한 Azure 웹 애플리케이션을 대상으로 한 봇 공격이 증가하여 월 평균 17억 건의 봇 요청이 있었고 해당 트래픽 중 4.6%는 악성 봇으로 구성되었습니다.

새롭게 떠오르는 DDoS, 웹 애플리케이션, 네트워크 공격에 대한 회복탄력성 구축

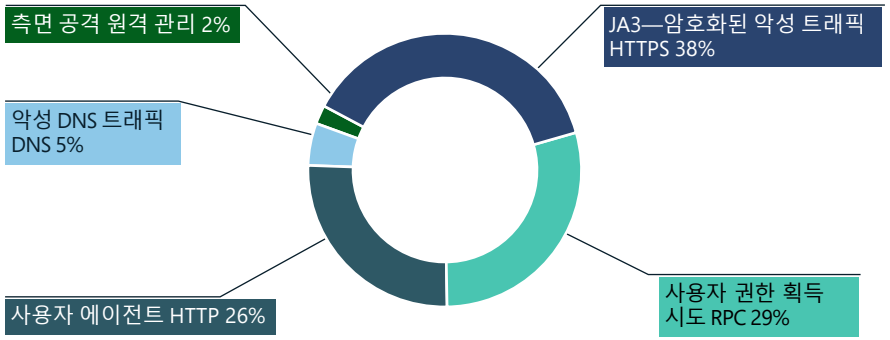
계속

개인 인증 정보 스터핑 공격, 신용 카드 사기, 사이버 영향력 캠페인, 공급망 공격을 수행하는 봇의 수가 증가함에 따라 웹 애플리케이션을 대상으로 한 봇 공격이 꾸준히 증가할 것으로 예상됩니다.

네트워크 침입: 탐지 및 예방

2022년에 네트워크 계층 악용, 특히 맬웨어가 크게 증가한 것으로 나타났습니다. Azure Firewall IDPS(침입 탐지 및 방지 시스템)는 6월 한 달 동안에만 1억 5천만 개 이상의 연결을 차단했습니다.

IDPS 거부 트래픽 이유



IDPS 트래픽 경보 이유

IDPS 경고 및 거부 트래픽을 분석하면 공격자별 다음과 같은 접근 방식이 표시됩니다. 거부 트래픽에서는 공격자가 SSL을 활용하여 활동을 숨기고 원격 실행 공격이 점점 더 보편화되고 있습니다. 경고 트래픽에서 원격 실행 공격을 수행하는 데 사용되는 SMB/SMB2 프로토콜이 표시됩니다.

실행 가능한 인사이트

1. 데이터센터 또는 클라우드 서비스 내의 시스템 간 트래픽과 이러한 트래픽에 액세스하려는 트래픽을 검사합니다.
2. 연중 내내 강력한 네트워크 보안 대응 전략을 개발합니다.
3. 클라우드 네이티브 보안 서비스를 사용하여 강력한 제로 트러스트 네트워크 보안 태세를 구현합니다.

추가 정보에 대한 링크

- Azure Firewall을 통해 랜섬웨어 공격에 대한 보안 방어 개선 | Azure 블로그 및 업데이트 | Microsoft Azure
- DDoS 증폭 공격의 구조 | Microsoft Security 블로그
- Azure Web Application Firewall을 통해 에지부터 클라우드까지 인텔리전트한 애플리케이션 보호 | Azure 블로그 및 업데이트 | Microsoft Azure

데이터 보안 및 사이버 회복탄력성에 대한 균형 잡힌 접근 방식 개발

디지털 트랜스포메이션은 데이터 자산의 방대한 확장과 보안, 규정 준수, 개인 정보 보호 위험의 증가를 촉진했습니다. 사이버 회복탄력성이 뛰어난 조직은 데이터 보호, 규정 준수, 복구 기능에 대한 균형적인 투자를 유지하고 이를 전문 규제 대응 프로세스와 통합하여 고유한 유형의 위반을 해결해야 합니다.

데이터 유출은 발생 가능성의 문제가 아니라 시기의 문제입니다. IBM과 Ponemon Institute의 'Cost of a Data Breach, 2021' 연구에 따르면 전 세계 평균 데이터 유출 비용은 미화 424만 달러(전년 대비 10% 증가)이며 미국에서는 미화 905만 달러를 기록했습니다. 규정 준수 실패가 비용 증폭의 가장 큰 요인으로 밝혀졌습니다. 반대로 침해 비용 절감은 IR(인시던트 대응) 계획, 제로 트러스트 배포 성숙도, 보안 AI 및 자동화, 암호화 사용과 같은 모범 사례와 관련이 있었습니다.

데이터 유출은 불가피합니다. 균형 잡히고 회복 탄력적인 접근 방식을 취하는 조직은 위반의 빈도, 영향, 비용을 줄일 수 있습니다.

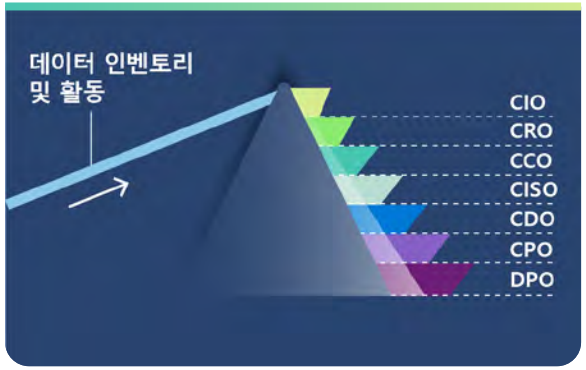
데이터 거버넌스, 보안, 규정 준수, 개인 정보 보호는 상호 의존적입니다.

최근 몇 년 동안 데이터는 조직의 중요한 가치 창출 엔진으로 두각을 나타냈습니다. 이와 동시에, 데이터 거버넌스와 보안을 모두 요구하는 개인 정보 보호 규정의 등장으로 위험 역할 간의 경계가 모호해졌습니다. CDO(최고 데이터 책임자) 또는 CPO(최고 개인 정보 보호 책임자)와 같은 새로운 임원급 역할은 보안 및 규정 준수에 기득권이 있지만, 데이터 보호의 구현 및 운영은 CIO(최고 정보 책임자) 및/또는 CISO(최고 정보 보안 책임자)가 이끄는 팀에 의존하는 경우가 많습니다. CDO가 주도하는 데이터 거버넌스 이니셔티브에도 보안 이점이 있기 때문에 일방적이지 않습니다. 이러한 상호 연결성의 결과로 IT, 데이터 거버넌스, 보안, 규정 준수, 개인 정보 보호 팀은 효율성을 달성하고 위험을 관리하기 위해 그 어느 때보다 더욱 긴밀하게 협력해야 합니다.

전체 조직의 데이터 자산을 위한 통합형 데이터 위험 관리 플랫폼은 미래입니다.

IT, 데이터 거버넌스, 보안, 규정 준수, 개인 정보 관리 프로세스를 조정하는 것은 각 분야에 대한 맞춤형 애플리케이션 환경과 일반적인 조직의 하이브리드 및 멀티클라우드 데이터 스프롤에서 일관적이지 않은 적용 범위로 구성된 환경에서 어렵습니다. Microsoft에서는 조직이 데이터의 위치를 찾아 파악하고, 데이터를 보호하고, 데이터의 액세스, 사용량 및 수명 주기를 제어하고, 데이터 자산 전체에서 데이터 손실을 방지하기 위해 단일 창이 필요하다고 생각합니다.

동일한 데이터 인벤토리 및 활동 정보에서 작업하면 팀 간의 프로세스가 쉬워지고, 보다 포괄적으로 위험을 볼 수 있으며, 조직이 위반에 대한 대응을 더 잘 준비하고 간소화할 수 있습니다.



'단일 유리창 (single pane of glass)'은 프리즘 역할을 해야 합니다. 데이터 보안, 규정 준수, 개인 정보 보호에 대한 이해관계가 있는 팀은 동일한 데이터 인벤토리 및 활동에 대해 다르면서도 일관적인 관점을 조정하고 협업해야 합니다. 데이터 활동에는 데이터 보안 방정식의 중요한 부분인 데이터 액세스, 수정, 이동 이벤트가 포함됩니다.

효과적인 데이터 거버넌스, 보안, 규정 준수, 개인 정보 보호는 상호 의존적이며 팀 간의 협업이 필요합니다.

실행 가능한 인사이트

1. 방어와 복구의 균형을 유지하고 규정 준수, 데이터 보호, 대응 기능에 투자하여 데이터 침해 영향을 최소화합니다.
2. 데이터 위험 사일로를 없애고 전체 데이터 자산을 포괄하는 프로세스와 도구를 개발하고 채택합니다.

추가 정보에 대한 링크

- Microsoft Purview—데이터 보호 솔루션 | Microsoft Security
- 규정 준수와 데이터 거버넌스의 미래: Microsoft Purview 소개 | Microsoft Security 블로그

사이버 영향력 작전에 대한 회복탄력성: 사람 차원

지난 5년 동안 그래픽 및 머신 러닝의 발전으로 몇 초 만에 인터넷을 통해 널리 퍼질 수 있는 고품질의 사실적인 콘텐츠를 빠르게 생성할 수 있는, 사용하기 쉬운 도구가 도입되었습니다.

텍스트, 오디오, 시각적 콘텐츠를 통해 보고된 이벤트를 인간이나 알고리즘이 사실과 허구를 확실하게 구분할 수 없는 지점에 도달했습니다. 이러한 도구와 결과물의 확산은 모든 디지털 미디어의 신뢰성에 의문을 제기하여 지역 및 세계 이벤트에 대한 우리의 이해를 방해하고 있습니다. 기술의 발전으로 가능해진 새로운 형태의 영향력 행사는 민주적 절차에 중대한 영향을 미칩니다.[11]

이러한 사이버 영향력 작전에 맞서 보다 회복탄력적인 미래를 준비하기 위해 무엇을 할 수 있을지 의문이 제기됩니다. 기술은 퍼즐의 한 부분일 뿐입니다. 미디어 문해력, 인식, 경계를 목표로 하는 교육, 현장, 지역, 국가, 국제적으로 신뢰할 수 있는 기자와 함께 양질의 저널리즘에 대한 투자, 영향력 작전에 대한 공유 및 경고 네트워크와 속일 목적으로 디지털 미디어를 생성하거나 조작하는 악의적인 공격자를 처벌하는 새로운 종류의 규정을 포함하여 다양한 노력이 필요할 것입니다.

또한 디지털 콘텐츠에 대한 신뢰를 회복하는 것이 다양한 관점과 참여가 필요한 야심 찬 목표라는 사실을 알고 있습니다. 이러한 위협을 자체적으로 해결할 수 있는 단일 회사, 기관 또는 정부 기관은 없습니다. 인간으로서 우리의 초능력은 협업하고 협력하는 능력입니다. 이는 전 세계의 정부 기관, 산업, 학계, 특히 뉴스, 사회 및 미디어 조직 등 모든 사람이 우리 사회의 개선과 건강을 위해 협력해야 하기 때문에 지금 특히 중요합니다.

추가 정보에 대한 링크

- 국방성 사이버 임무에서의 AI용 애플리케이션 | 문제에 대응하는 Microsoft
- AI 및 사이버 보안: 증가하는 과제와 유망한 방향. 117차 의회, 상원 군사위원회의 사이버 보안 소위원회에서 진행한 사이버 공간 내 작전에 대한 AI 애플리케이션 관련 청문회, 117차 의회(2022년 5월 3일, Eric Horvitz의 증언)

기술 개발을 통한 인적 요소 강화

인적 요소를 해결하는 것은 모든 사이버 보안 기술 전략의 핵심 구성 요소입니다. IT Security의 Kaspersky Human Factor에 따르면[12] 사이버 보안 인시던트 중 46%는 부주의하거나 제복을 입은 직원이 의도치 않게 공격을 조장하는 것과 관련이 있습니다.

디지털 보안 및 회복탄력성 조직의 Microsoft 교육 및 인식 팀은 직원들이 자신과 고객 시스템 및 데이터를 보호할 수 있도록 권한을 부여하여 사이버 보안의 인적 요소를 강화하는 일을 담당합니다. 목표는 다음과 같습니다.

- 직원 전체에 걸쳐 전사적으로 중앙 집중식 핵심 보안 기술을 구축하여 Microsoft 및 고객을 대상으로 한 위험을 줄입니다.
- 원하는 행동 결과를 지원하기 위해 다중 교육 강화 접근 방식을 통해 직원들의 보안 지식을 강화합니다.
- 매년 요구되는 보안 교육 및 이벤트를 통해 보안 사고방식을 Microsoft 문화의 본질적인 부분으로 만들어 문화를 변화시킵니다.
- 사이버 보안과 관련된 모든 것에 대한 모범 사례, 회사 정책 정보, 인시던트 보고를 위한 중앙 집중식 원스톱 웹 리소스를 촉진합니다.

표적화된 중앙 집중식 사이버 보안 기술 프로그램은 매년 한 번 이상 모든 Microsoft 직원들에게 전달됩니다. 교육 서비스는 현재 사이버 보안 이니셔티브를 지원하고 측정 가능한 행동 결과를 제공하도록 최적화되어 있습니다. Microsoft의 IRMC(Information Risk Management Council, 정보 위험 관리 위원회)는 교육을 통해 해결해야 할 중요한 사이버 보안 행동 변경 결과를 식별하는 데 중요한 역할을 합니다.

모든 사이버 보안 기술 프로그램을 통해 솔루션의 효율성, 효과, 가능한 경우 결과를 측정합니다. 예를 들어, Microsoft의 내부자 위협 기술 서비스는 95% 교육을 규정 준수하고 학습자 만족도가 뛰어나며, 그 결과 Microsoft의 Report It Now 도구를 통해 가능한 내부자 위협 사례를 보고하는 관리자가 크게 증가했습니다. 이 프로그램에는 다음 프로그램이 포함됩니다.

보안 기반: 핵심 보안 및 개인 정보 보호 관행을 다루는 전사적인 중앙 집중식 사이버 보안 인식 및 규정 준수 교육입니다. 매우 기대되는 이 교육 시리즈는 에듀테인먼트 모델을 사용하여 사이버 보안에 대한 학습을 매력적이면서 흥미롭게 만듭니다.

스트라이크: LOB(기간 업무) 솔루션을 구축하고 유지 관리하는 엔지니어를 위한 Microsoft의 필수 기술 교육입니다. 초대를 통해서만 제공되는 이 교육은 사이버 보안 방역 모범 사례의 시기적절하고 중요한 영역을 다루고 대상 그룹의 요구에 맞춰 조정된 실시간 하이브리드 제공 모델을 사용합니다.

프로그램별: 대상 교육 프로그램은 Shadow IT, Insider Threat, Microsoft Federal을 포함한 특정 사이버 보안 이니셔티브를 지원합니다. 이러한 서비스는 경영진 후원 및 스코어카드 보고를 통해 해당 사이버 보안 이니셔티브에 대한 전반적인 참여 전략에 긴밀하게 통합되어 '체크 표시'하는 교육 접근 방식을 방지합니다.

MSProtect: 사이버 보안과 관련된 모든 것에 대한 모범 사례, 회사 정책 정보, 인시던트 보고를 제공하는 Microsoft의 중앙 집중식 웹 리소스입니다. 이 주문형 리소스는 공식 교육 서비스 이외의 직원이 사용하는 리소스입니다.

보안 기술은 규정 준수, 체크 표시하는 활동으로 간주되어서는 안 됩니다. 대신, 행동 변화에 집중하여 식별된 대상 행동에서 결과를 모니터링하고 경청 시스템을 구축하여 서비스의 영향력을 결정합니다.

실행 가능한 인사이트

1. 필요할 때 언제 어디서나 직원들에게 보안 교육 및 리소스를 제공합니다.
2. 기업 전체의 이해 관계자가 정보를 제공하는 중앙 집중식 기술 전략을 개발합니다.
3. 교육의 영향력을 추적하고 효율성(수량), 효과(품질), 결과(비즈니스 영향)를 분석하도록 합니다.

추가 정보에 대한 링크

› Microsoft, 3천만 명의 사람들을 지원한 후 다음 단계의 기술 이니셔티브 시작

랜섬웨어 제거 프로그램의 인사이트

Microsoft는 지난 5년 동안 자체적인 제로 트러스트 여정[13]을 통해 ID와 디바이스가 강력하게 관리되고 정상적으로 실행되도록 했습니다. 랜섬웨어의 위험이 증가함에 따라 Microsoft에서는 Microsoft와 고객을 보호하기 위한 접근 방식을 지원하기 위해 심층적인 관점을 개발했습니다.

심층적인 내부 평가에 따라 제어 및 적용 범위의 격차를 수정하고, Defender for Endpoint, Azure, M365와 같은 서비스의 기능 강화에 기여하고, SOC 및 엔지니어링 팀을 위해 랜섬웨어 공격 시 복구하는 방법에 대한 플레이북을 개발하기 위해 랜섬웨어 제거 프로그램을 구축했습니다.

첫 번째 단계는 Microsoft를 대상으로 하는 랜섬웨어 공격에 대한 보호 범위를 이해하는 것이었습니다. Defender for Endpoint를 배포하고 모든 디바이스가 관리되고 제로 트러스트 정책을 준수하는지 확인하기 위한 노력은 이미 진행 중이었지만, 공격으로부터 효과적으로 복구할 수 있는지 여부에 대한 더 큰 질문의 모든 측면을 이해하는 방법을 모색해야 했습니다. 인사이트를 확보하기 위해 알려진 제어 목록에 대한 전반적인 엔터프라이즈급 정책과 일치하는 NIST 8374: 랜섬웨어 위험 관리: CSF(사이버 보안 프레임워크) 프로필[14]을 평가했습니다. 이 분석은 적용 범위의 격차를 빠르게 식별했습니다.

다음으로, CSF의 식별, 탐지, 보호, 대응, 복구 기능 전반에 걸친 격차의 우선순위를 지정했습니다. 제로 트러스트 및 기타 프로그램에 대한 전략적 연계를 찾았고 기존 작업 흐름이 없는 격차도 발견했습니다. 이러한 격차를 해결하는 데 필요한 작업과 노력의 양을 평가한 후 두 가지 주요 요소 분리했습니다.

- **PtE(엔터프라이즈급 보호):** 성공할 경우 공격으로부터 자신을 보호하고 복구할 수 있도록 기업으로서 수행해야 하는 작업 항목을 정의합니다.
- **PtC(고객 보호):** 고객과 비즈니스를 보호하기 위한 기능을 제품에 구축합니다.

결과를 자체 기업에 내장

주요 위험을 해결하고 랜섬웨어 공격으로부터 주요 서비스를 보호하기 위해 향후 6개월에서 12개월 동안 전용 랜섬웨어 프로그램의 일환으로 아래 5가지 시나리오를 달성하는 데 투자를 집중할 계획입니다. 각 시나리오에서 성공하면 프로그램의 범위를 점차 확장하여 기업의 모든 부분에 도달할 것입니다.

시나리오 1: 보안 팀 구성원은 랜섬웨어 공격과 관련된 전반적인 위험을 이해하고 경영진에게 제어 격차 및 위험 상태에 대한 인식을 제공하기 위한 프로세스를 설정합니다.

시나리오 2: 보안 팀 구성원은 자신과 Microsoft 내의 다른 팀이 랜섬웨어 공격에 대응하고 주요 서비스를 복구하는 데 도움이 되도록 설계된 플레이북에 액세스할 수 있습니다.

시나리오 3: 엔터프라이즈급 회복탄력성 팀 구성원은 주요 시스템의 백업에 대해 따라야 할 표준이 있습니다. 플레이북은 랜섬웨어 공격 시 데이터를 복구할 수 있도록 존재하며 정기적인 백업 및 복구 연습이 수행됩니다.

시나리오 4: 서비스 담당자는 Microsoft 주요 서비스로 우선순위가 지정된 서비스에 특히 중점을 두고 랜섬웨어 공격으로부터 서비스, 고객 데이터, 엔드포인트, 네트워크 자산을 보호하는 데 필요한 보안 및 운영 제어와 정책을 이해하고 구현합니다.

시나리오 5: 모든 직원들은 랜섬웨어 공격을 인식하는 방법과 보안 팀에 알리고 대응을 시작하는 방법에 대해 설명하는 교육 및 훈련 리소스에 액세스할 수 있습니다.

실행 가능한 인사이트

1. 중요 서비스를 대상으로 한 랜섬웨어 공격과 관련 엔드 투 엔드 복구 및 수정 활동을 문서화하고 검증합니다.
2. 엔터프라이즈급 위기관리 플레이북을 업데이트하는 데 이해관계자를 참여시켜 랜섬웨어별 활동과 랜섬웨어에 대한 몸값 지불 여부/시기를 결정하기 위한 의사 결정 프로세스 및 지침을 포함합니다.
3. 배포된 보안 제품(예:Defender for Endpoint Attack Surface Reduction 규칙)에서 사용할 수 있는 기능을 활성화하여 탐지 및 보호 범위를 개선합니다.
4. 보안 표준 팀과 협력하여 랜섬웨어 공격으로부터 보호하기 위한 기준을 정의하고 엔지니어링 팀에 랜섬웨어 공격으로부터 보호하는 방법에 대한 교육 및 설명서를 제공합니다.
5. DevOps 팀에서 보안 및 운영 정책을 더 쉽게 배포할 수 있도록 자동화를 시행하고 시스템이 규정 준수에서 벗어나는 경우 신속하게 플래그를 지정하고 수정하도록 합니다.

추가 정보에 대한 링크

- Microsoft가 랜섬웨어로부터 보호하는 방법 공유 | Microsoft Inside Track

양자 보안 영향에 대한 현재 조치

오늘날 암호화와 암호화가 보호하는 모든 것을 대상으로 하는 위협을 관리해야 한다는 압박이 양자 컴퓨팅에 가해지고 있습니다. 최근 발행된 국가 사이버 보안 개선을 위한 각서 'Improving the Cybersecurity of National Security Department of Defense and Intelligence Community Systems'[15](미국 행정명령 10428)[16]는 국가 차원의 공격을 해결하는 데 소프트웨어 공급망 안전의 중요성을 강조합니다.

양자 컴퓨터의 정의

양자 컴퓨터는 양자 물리학의 속성을 활용하여 데이터를 저장하고 계산을 수행하는 컴퓨터입니다. 이것은 최고의 슈퍼컴퓨터를 훨씬 능가할 수 있는 특정 작업에 매우 유리할 수 있습니다. 양자 컴퓨팅은 이미 데이터 암호화 및 처리의 새로운 지평을 열고 있습니다. 연구 결과에 따르면 양자 컴퓨팅은 빠르면 2030년에 미화 수십억 달러 규모의 양자 산업이 될 것으로 예상됩니다.[17] 실제로 양자 컴퓨팅과 양자 통신은 의료 및 에너지에서 금융 및 보안에 이르기까지 다양한 산업 분야에서 혁신적인 효과를 낼 태세입니다.

양자 컴퓨팅은 오늘날 암호화와 암호화가 보호하는 모든 것에 대한 위협입니다.

오늘날 암호화에 대한 위협

Shor의 1994년 알고리즘과 수백만 개 이상의 물리적 큐비트로 구성된 산업 규모의 양자 컴퓨터를 사용하면 현재 널리 배포된 모든 공개 키 암호화 알고리즘을 효율적으로 깨뜨릴 수 있습니다. 적대적인 양자 기반 공격에 대해 효율적이고 민첩하며 '양자 컴퓨터의 공격으로부터 안전한' 암호화 시스템을 고려, 평가, 표준화하는 것이 중요합니다. '포스트 양자 암호', 즉 양자 공격에 강력한 기존 알고리즘 및 프로토콜로의 소프트웨어 마이그레이션을 달성하려면 10년 이상은 아니더라도 몇 년이 걸릴 것입니다.[18]

즉 오늘날 암호화와 암호화가 보호하는 모든 것을 대상으로 하는 위협을 관리해야 한다는 압박이 가해진다는 사실을 의미합니다. 악의적 공격자들은 지금 암호화된 데이터를 기록하고 나중에 양자 컴퓨터를 사용할 수 있게 되면 이를 악용할 수 있습니다. 암호화 문제를 해결하기 전에 양자 컴퓨팅을 사용할 때까지 기다리면 너무 늦을 것입니다.

암호화가 사이버 생태계 전체에서 사용됨에 따라 암호화 기반 보안 서비스가 손상될 수 있습니다. 예를 들어, 여기에는 통신(TLS, IPSec), 메시징(이메일, 웹 회의), ID 및 액세스 관리, 웹 브라우징, 코드 서명, 결제 거래, 보호를 위해 암호화에 의존하는 기타 서비스가 포함됩니다.

양자 컴퓨터가 현실화됨에 따라 암호화 알고리즘 및 기능의 구현을 포함하는 서드파티 소프트웨어 구성 요소도 추가 조사가 필요합니다. 이를 위해서는 가치 사슬에 있는 모든 조직이 체인의 보안을 유지하기 위해 자신의 역할을 수행해야 합니다. 업계 기관과 정부 기관은 소프트웨어 공급망 보안 요구 사항을 정의하기 위해 더 많은 노력을 기울이고 있으며, 경우에 따라 체인 보안을 위한 새로운 의무를 도입하고 있습니다. 국가 안보 양해 각서 NSM-8[19]은 NSS(National Security Systems, 국가 보안 시스템)에서 포스트 양자 암호를 구현하기 위한 요구 사항과 일정을 설정합니다. 180일 이내에 '현대화 계획, 지원되지 않는 암호화 사용, 승인된 미션 고유 프로토콜, 양자 내성 프로토콜, 필요시 양자 내성 암호화 사용 계획' 시점에 대한 기대치를 제시합니다.

표준화는 양자 컴퓨터의 공격으로부터 안전한 암호화로의 전환에서 긴 리드 타임이 소요되는 작업입니다. 공개 키 암호화를 활용하여 표준을 연구하는 표준 기관은 이제 양자 이후 알고리즘을 실험하고 적응하기 시작해야 합니다.

새로운 PQC(포스트 양자 암호) 알고리즘(양자 공격에 강하다고 생각되는 기존 알고리즘)은 현재 NIST의 Post-Quantum Standardization Project를 통해 검토 중입니다.[20] 이 작업은 표준 기구 내 전 세계적인 노력에 영향을 미칠 것입니다. 미국 정부 기관의 알고리즘에서 선택한 것과 일부 중복되겠지만, 호환 알고리즘에 대한 국가 기관/규제 선택이 다르면 국제적 문제가 발생할 수 있습니다. 이러한 단편화는 제품 및 서비스 엔지니어링을 복잡하게 만듭니다.

새로운 포스트 양자 암호 알고리즘은 NIST의 Post-Quantum Cryptography Standardization 프로그램을 통해 검토 중입니다. 이 작업은 표준 기구 내 전 세계적인 노력에 영향을 미칠 것입니다.

실행 가능한 인사이트

SAFECode 및 파트너 회원과 함께 업계에서는 PQC로의 전환을 준비하기 위해 즉각적으로 단기적인 활동을 취해야 합니다.[21] 여기에는 다음이 포함됩니다.

1. 암호화를 사용하는 제품/코드의 인벤토리를 가져옵니다.
2. 암호화가 변경될 때 필요한 코드 변동을 최소화하는 등 암호화 민첩성 전략을 조직 전체에 구현합니다.
3. 암호화를 사용하는 제품 또는 서비스에서 양자 컴퓨터의 공격으로부터 안전한 알고리즘 후보군의 사용을 파일럿합니다.
4. 암호화, 키 교환, 서명에 대해 다양한 공개 키 알고리즘을 사용할 준비를 합니다.
5. 매우 큰 키 크기, 암호, 서명의 영향력에 대해 애플리케이션을 테스트합니다.

추가 정보에 대한 링크

- Microsoft에서 새로운 큐비트 종류를 생성하는 데 필요한 기본 물리학을 시연했습니다 | Microsoft Research

비즈니스, 보안, IT를 통합하여 회복탄력성 향상

강력한 사이버 회복탄력성은 보안을 구현하기 위해 보안 팀과 협력하는 비즈니스 리더에 달려 있습니다. Microsoft의 경험에 따르면 보안 리더십은 조직을 가장 효과적으로 보호하기 위해 조직 리더의 지원이 필요한 어려운 분야입니다.

보안 리더는 위험, 기술, 경제, 조직 프로세스, 비즈니스 모델, 문화 혁신, 지정학적 이해관계, 스파이 활동, 국제 제재 준수와 관련된 주제에 걸쳐 다양한 동적 과제를 탐색합니다. 이들 각각의 주제는 미묘한 차이가 있어 이해를 하고 면밀히 관리해야 합니다.

보안 리더는 또한 인텔리전트하고 자금이 풍부하며 동기가 높은 인간 공격자들과 숙련도가 낮지만 효과적인 사이버 범죄자들을 저지하는 임무를 맡고 있습니다. 이들의 팀은 보안이 우선순위가 낮았거나 존재하지 않았던 30년이 넘는 시간 동안 점진적으로 구축된 복잡성 높은 기술 자산을 방어해야 합니다. 몇 년 전에 내린 결정은 오늘날 기술적 부채를 상환하고 보안의 격차를 해소할 때까지 위험을 초래할 수 있습니다.

조직의 리더와 정책 입안자는 보안 리더를 적극적으로 지원하고 통합형 보안과 나머지 조직 간의 교량 역할에 도움을 줌으로써 보안에 상당히 높은 긍정적인 영향을 미칠 수 있습니다. Microsoft에서는 이러한 관계를 가진 고객과 협력 시 고객이 보다 회복 탄력적인 조직을 구축하고 적응 및 혁신을 위한 민첩성을 향상시키는 것을 볼 수 있습니다.

조직 리더십은 다음 세 가지 주요 영역에 중점을 두어 보안 리더를 지원할 수 있습니다.

1. 설계에 따른 보안 구축

보안은 때때로 비즈니스 프로세스에서 장애물 또는 사후에 고려할 사항으로 간주되며, 위험을 피하거나 큰 비용을 들이지 않고 쉽게 수정하기에는 너무 늦은 경우에만 의사 결정 시 고려되는 경우가 많습니다.

조직 리더와 정책 입안자는 다음을 확인해야 합니다.

새로운 이니셔티브 진행 시, 초기에 보안을 포함합니다. 새로운 디지털 이니셔티브와 클라우드 채택은 새로운 애플리케이션 또는 디지털 기능마다 조직의 위험이 증가하지 않도록 보안을 우선시해야 합니다. 보안이 안정적으로 포함되면 이러한 프로세스를 사용함으로써 레거시 시스템을 현대화하여 보안과 생산성의 이점을 동시에 얻을 수 있습니다.

보안을 위해 예방 유지 관리를 표준화합니다. 보안 업데이트, 패치 적용, 보안 환경 설정과 같은 기본 보안 유지 관리에 전체 조직의 지원(예산, 예약된 가동 중지 시간, 공급업체 제품 지원을 위한 인수 요구 사항 포함)이 할당되었는지 확인합니다.

안타깝게도 수많은 조직에서는 이러한 일반적인 관행을 부분적으로만 지연, 연기 또는 적용합니다. 이는 공격자가 악용할 수 있는 광범위한 기회를 제공합니다. 보안 정규화의 필요성은 미국 NIST 800-40에 나와 있습니다.[22]

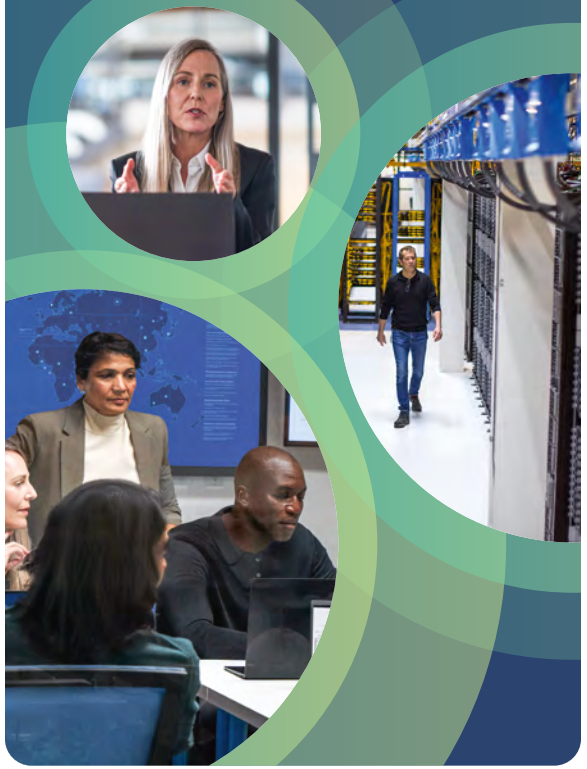
2. 보안을 통한 참여

조직 리더는 리소스의 우선순위를 지정하고 보안 재해에 대비할 수 있도록 주요 보안 프로세스에 적극적으로 참여하고 이를 지원해야 합니다. 여기에는 다음에 대한 참여가 포함됩니다.

주요 비즈니스 자산을 식별합니다. 보안 리더와 팀은 보안 리소스를 가장 중요한 곳에 집중하기 위해 어떤 자산이 비즈니스 크리티컬한지 알아야 합니다. 이는 이전에 다루지 않은 새로운 질문을 하고 대답하는 것을 포함하는 새로운 연습인 경우가 많습니다.

바로 사이버 보안 비즈니스 연속성 및 재해 복구에 대한 연습입니다. 사이버 공격은 대부분 또는 모든 비즈니스 운영을 방해하거나 중단시키는 주요 이벤트가 될 수 있습니다. 조직 전체의 팀이 이러한 상황을 처리할 준비가 되어 있는지 확인하면 비즈니스 운영을 복원하는 시간을 줄이고, 조직의 피해를 제한하며, 고객, 시민, 구성원들의 신뢰와 확신을 유지하는 데 도움이 됩니다. 이는 기존 비즈니스 연속성 및 재해 복구 프로세스에 통합되어야 합니다.

보안 위험 결정은 모든 위험과 기회에 대한 완전한 가시성을 보유한 비즈니스 또는 미션 담당자가 내리는 것이 가장 좋습니다.



비즈니스, 보안, IT를 통합하여 회복탄력성 향상

계속

3. 보안을 올바르게 배치

조직이 보안 위험 책임을 구조화하는 방식은 잘못된 보안 위험 의사 결정을 설정하는 경우가 많습니다. 위험 결정은 모든 위험과 기회에 대한 완전한 가시성을 보유한 비즈니스 또는 미션 담당자가 내리는 것이 가장 좋지만 조직은 보안 팀의 실무 전문가에게 보안 위험 책임을 (암시적 또는 명시적으로) 할당하는 경우가 많습니다. 이는 보안 팀에 건전하지 않은 부담을 주는 동시에 비즈니스 담당자로부터 비즈니스의 주요 위험에 대한 가시성과 통제력을 박탈합니다. 조직은 다음을 통해 이 문제를 해결할 수 있습니다.

비즈니스 담당자 준비: 비즈니스 담당자에게 전반적인 보안 위험과 이러한 위협이 비즈니스에 미칠 수 있는 영향에 대해 교육합니다. 이러한 노력에 보안 팀을 직접 참여시키면 보안 및 전반적인 비즈니스 민첩성과의 협업 관계도 향상됩니다.

비즈니스 담당자에게 보안 위험 할당: 비즈니스 담당자가 보안 위험을 이해하고 받아들일 수 있을 만큼 충분한 정보를 얻으면 조직은 보안 위험에 대한 책임을 명시적으로 이전하는 동시에 해당 위험을 관리하고 정보에 입각한 전문 지식과 지침을 담당자에게 제공할 책임이 있는 보안 팀을 보유해야 합니다.

"사이버 회복탄력성은 우수한 데이터 백업으로 시작하는 고전적인 비즈니스 연속성 및 재해 복구에 따라 차등으로 규모가 정해집니다. 프로세스, 기술 및 종속성(사람 및 서드파티 포함)에 대한 복구 기능으로 진행되고 항상 켜져 있는 자가 치유형 서비스, 중요한 역할에 대한 회복탄력성, 중요한 서드파티를 위한 페일오버로 이동합니다. 가장 회복 탄력적인 조직은 IT, 비즈니스 관리자, 보안 전문가 간의 통합을 촉진합니다. 뛰어난 회복탄력성에는 처음부터 회복탄력성을 위한 설계, 안전한 변경 관리, 세분화된 오류 격리가 포함됩니다. 사이버 회복탄력성은 우수한 모든 위험 계획 프로그램 중 한 시나리오일 뿐입니다. 사이버 위험이 증가하고 사이버 보안과 회복탄력성 간의 공통부분이 더욱 중요해짐에 따라 CISO(최고 정보 보안 책임자)와 엔터프라이즈급 회복탄력성 프로그램의 연결이 더욱 강력해지고 있습니다. 매년 더 많은 CISO가 전사적 회복탄력성을 위한 주인의식을 갖고 있습니다."

Lisa Reshaur
Microsoft의 위험 관리 부문 총괄 관리자

추가 정보에 대한 링크

- 회복탄력성에서 디지털 인내에 이르기까지: 조직이 디지털 기술을 활용하여 전례 없는 시기에 고비를 넘기는 방법 | 공식 Microsoft 블로그
- IT 팀과 보안 팀이 협력하여 엔드포인트 보안을 개선하는 방법 | Microsoft Security

사이버 회복탄력성 벨 곡선

모든 조직이 채택해야 하는 회복탄력성의 성공 요인

이미 본 것처럼 수많은 사이버 공격은 기본적인 보안 방역을 따르지 않았기 때문에 성공합니다. 모든 조직이 채택해야 하는 최소한의 표준은 다음과 같습니다.

- **MFA(다중 인증) 사용:** 침해된 사용자 비밀번호로부터 보호하고 ID에 대한 추가 회복탄력성을 제공하는 데 도움이 됩니다.
- **제로 트러스트 원칙 적용:** 조직에 미치는 영향을 제한하는 회복탄력성 계획의 초석입니다. 이러한 원칙은 다음과 같습니다.

1 – 명시적으로 확인—리소스에 대한 액세스를 허용하기 전에 사용자와 디바이스가 양호한 상태인지 확인합니다.

2 – 최소 권한 액세스 사용—리소스에 액세스하는 데 필요한 권한만 허용하고 그 이상은 허용하지 않습니다.

3 – 위반 가정—시스템 방어가 위반되어 시스템이 손상될 수 있다고 가정해보겠습니다. 즉, 가능한 공격에 대해 환경을 지속적으로 모니터링해야 합니다.

- **확장된 탐지 및 대응 맬웨어 방지 사용:** 소프트웨어를 구현하여 공격을 탐지 및 자동으로 차단하고 보안 작업에 대한 인사이트를 제공합니다. 위협 탐지 시스템에서 인사이트를 모니터링하는 것은 적시에 위협에 대응하는 데 필수적입니다.
- **최신 상태 유지:** 패치가 적용되지 않고 오래된 시스템은 많은 조직이 공격의 희생양이 되는 주요 이유입니다. 펌웨어, 운영 체제, 애플리케이션을 포함한 모든 시스템이 최신 상태로 유지되는지 확인합니다.
- **데이터 보호:** 중요한 데이터, 데이터의 위치, 올바른 시스템이 구현되었는지 여부를 아는 것은 적절한 보호를 구현하는 데 매우 중요합니다.

98%

기본 보안 방역은 여전히 공격의 98% 방지합니다.

요점

- 다중 인증 활성화
- 제로 트러스트 원칙 적용
- 최신 맬웨어 방지 프로그램 사용
- 최신 상태 유지
- 데이터 보호

미주

1. EDR(엔드포인트 탐지 및 대응)은 엔터프라이즈 네트워크가 인텔리전트형 위협을 예방, 감지, 조사 및 대응할 수 있도록 설계된 엔터프라이즈 엔드포인트 보안 플랫폼입니다. 엔드포인트 탐지 및 대응은 실시간에 가깝고 실행 가능한 고급 공격 탐지 기능을 제공합니다. 보안 분석가는 경고의 우선순위를 효과적으로 정하고, 위반의 전체 범위에 대한 가시성을 확보하고, 위협을 해결하기 위한 대응 조치를 취할 수 있습니다.
2. EPP(엔드포인트 보호 플랫폼)는 파일 기반 맬웨어를 방지하고, 신뢰할 수 있는 애플리케이션과 신뢰할 수 없는 애플리케이션의 악의적인 활동을 탐지 및 차단하고, 보안 인시던트 및 경고에 동적으로 대응하는 데 필요한 조사 및 수정 기능을 제공하기 위해 엔드포인트 디바이스에 배포된 솔루션입니다.
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. Windows 보안 가이드북: 상업용
7. Windows 11의 새로운 보안 기능은 하이브리드 업무를 보호하는 데 도움이 됩니다 | Microsoft Security 블로그
8. FIDO 얼라이언스: 비밀번호보다 안전한 개방형 인증 표준
9. https://interpret.ml/
10. OWASP 상위 10위 | 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. 행정명령 14028 국가의 사이버 보안 개선
17. https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth
18. "포스트 양자 암호로의 전환을 위한 긴 여정," 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

기여 팀

기여 팀

본 보고서의 데이터와 인사이트는 다양한 Microsoft 팀에서 작업하는 다양한 보안 중심 전문가 그룹에서 제공되었습니다. 전반적으로 이들의 목표는 사이버 공격의 위협으로부터 Microsoft, Microsoft의 고객, 전 세계를 보호하는 것입니다. Microsoft에서는 세상을 모두에게 더 안전한 곳으로 만들겠다는 공통의 목표를 가지고 투명성을 추구하는 정신으로 이와 같은 인사이트를 공유할 수 있어서 자랑스럽게 생각합니다.

AI for Good Research Lab: 데이터와 AI의 힘을 활용하여 전 세계 다양한 과제를 해결합니다. 이 랩은 Microsoft 외부 조직과의 협력을 통해 AI를 적용하여 생계와 환경을 개선합니다. 중점 영역으로는 온라인 안전(허위 정보, 사이버 보안, 아동 안전), 재난 대응, 지속 가능성, 건강을 위한 AI 등이 있습니다.

Azure 엣지 및 플랫폼, 기업, OS 보안: Windows, Azure, 기타 Microsoft 제품 전반의 핵심 OS 및 플랫폼 보안을 담당합니다. 이 팀은 업계 최고의 보안 및 하드웨어 솔루션을 Microsoft 플랫폼에 구축하여 칩에서 클라우드로의 악용, ID, 맬웨어 손상을 줄입니다. PC, 엣지 및 서버, Microsoft Pluton 보안 프로세서 등을 아우르는 Microsoft의 보안 코어 플랫폼의 크리에이터입니다.

Azure 네트워킹, 코어: Microsoft WAN, 데이터센터 네트워크, DDoS 플랫폼, 네트워크 엣지 플랫폼 및 네트워크 보안 제품(예: Azure WAF, Azure Firewall, Azure DDoS Protection Standard)을 포함한 Azure의 사용자 정의 네트워킹 인프라에 중점을 둔 클라우드 네트워킹 팀입니다.

클라우드 보안 연구 팀: 이 팀은 Microsoft 클라우드를 보호하고, 혁신적인 보안 기능 및 제품을 구축하며, 연구를 수행하여 Microsoft 고객이 조직을 안전하게 혁신할 수 있도록 보호하고 권한을 부여합니다.

CST(Customer Security and Trust, 고객 보안 및 신뢰): Microsoft 제품 및 온라인 서비스에서 고객 보안의 지속적인 개선을 주도하고 있는 팀입니다. 회사 전체의 엔지니어링 및 보안 팀과 협력하는 CST는 고객을 보호하고 Microsoft에 대한 글로벌 신뢰를 증진하기 위해 규정 준수를 보장하고 보안을 강화하며 투명성을 향상시킵니다.

고객 성공: 고객 성공의 보안 팀은 고객과 직접 협력하여 모범 사례, 교훈, 지침을 공유하여 보안 혁신 및 현대화를 가속화합니다. 이 팀은 Microsoft와 고객의 여정에서 배운 모범 사례와 교훈을 참조 전략, 참조 아키텍처, 참조 계획 등으로 수집하고 구성합니다.

CDOC(사이버 방어 운영 센터): Microsoft의 사이버 보안 및 방어 시설은 Microsoft의 기업 인프라와 고객이 액세스할 수 있는 클라우드 인프라를 보호하기 위해 회사 전체에서 보안 전문가를 한데 모은 융합 센터입니다. 인시던트 대응기는 Microsoft의 서비스, 제품, 디바이스 그룹 전체에서 모인 데이터 과학자 및 보안 엔지니어와 함께 항시 위협을 보호, 탐지, 대응합니다.

민주주의 전진 이니셔티브: 건강한 정보 생태계를 촉진하고, 개방적이고 안전한 민주적인 프로세스를 보호하고, 기업의 시민적 책임을 옹호함으로써 민주주의의 기본을 보존, 보호, 발전시키기 위해 노력하는 Microsoft 팀입니다.

DCU(Digital Crimes Unit, 디지털 범죄 부서): 기술, 법의학, 민사 소송, 형사 입건, 공공 및 민간 파트너십을 활용하여 전 세계적으로 사이버 범죄와 싸우는 데 전념하는 변호사, 수사관, 데이터 과학자, 엔지니어, 분석가, 비즈니스 전문가로 구성된 팀입니다.

디지털 외교: 전직 외교관, 정책 입안자, 법률 전문가로 구성된 국제 팀이 국가 차원의 갈등이 고조되는 상황에서 평화롭고 안정적이며 안전한 사이버 공간을 발전시키기 위해 노력하고 있습니다.

DSR(Digital Security & Resilience, 디지털 보안 및 회복탄력성): Microsoft가 가장 신뢰할 수 있는 디바이스 및 서비스를 구축하는 동시에 회사를 안전하게 유지하고 회사 및 고객 데이터를 보호할 수 있도록 지원하는 데 전념하는 조직입니다.

DSU(Digital Security Unit, 디지털 보안부): Microsoft와 Microsoft의 고객을 보호하기 위해 법률, 지정학적, 기술적 전문 지식을 제공하는 사이버 보안 변호사 및 분석가 팀입니다. DSU는 전 세계의 고급 사이버 공격자에 대한 Microsoft의 엔터프라이즈급 보안 방어에 대한 신뢰를 구축합니다.

DTAC(Digital Threat Analysis Center, 디지털 위협 분석 센터): 사이버 공격 및 영향력 작전을 포함한 국가 차원의 위협을 분석하고 보고하는 전문가 팀입니다. 이 팀은 정보 및 사이버 위협 인텔리전스를 지정학적 분석과 결합하여 고객과 Microsoft에 인사이트를 제공하여 효과적인 대응 및 보호를 제공합니다.

엔터프라이즈 및 보안: 인텔리전트한 클라우드 및 인텔리전트 에지를 위한 현대적이고 안전하며 관리 가능한 플랫폼을 제공하는 데 중점을 둔 팀입니다.

엔터프라이즈 모빌리티: 클라우드 및 온-프레미스에서 데이터를 안전하게 유지하기 위해 모던 워크플레이스와 최신 관리 기능을 제공하는 데 도움이 되는 팀입니다. Endpoint Manager에는 Microsoft와 고객이 모바일 디바이스, 데스크톱 컴퓨터, 가상 머신, 내장형 디바이스, 서버를 관리하고 모니터링하는 데 사용하는 서비스와 도구가 포함되어 있습니다.

기여 팀

계속

엔터프라이즈급 위험 관리: Microsoft의 고위 경영진과 위험 논의에 대한 우선순위를 지정하기 위해 여러 사업부에서 협업하는 팀입니다. ERM은 여러 운영 위험 팀을 연결하고, Microsoft의 엔터프라이즈급 위험 프레임워크를 관리하고, NIST 사이버 보안 프레임워크를 활용하여 회사의 내부 보안 평가를 지원합니다.

글로벌 사이버 보안 정책: 정부 기관, NGO, 업계 파트너와 협력하여 고객이 Microsoft 기술을 채택하고 사용할 때 보안과 회복탄력성을 강화할 수 있는 사이버 보안 공공 정책을 홍보하는 팀입니다.

IDNA(Identity and Network Access, ID 및 네트워크 액세스) 보안: 무단 액세스 및 사기로부터 모든 Microsoft 고객을 보호하기 위해 노력하는 팀입니다. IDNA Security는 엔지니어, 제품 관리자, 데이터 과학자, 보안 조사관으로 구성된 학제 간 융합 팀입니다.

M365 보안: 엔터프라이즈급 고객을 보호하기 위해 MDE(엔드포인트용 Microsoft Defender) 및 MDI(Microsoft Defender for Identity) 등을 비롯한 보안 솔루션을 개발하는 조직입니다.

Microsoft AETHER(AI, Ethics and Effects in Engineering and Research, 엔지니어링 및 연구 관련 AI, 윤리 및 효과): 새로운 기술이 책임감 있는 방식으로 개발되고 배치되도록 하는 임무를 지닌 Microsoft의 자문 위원회입니다.

Microsoft Bing 검색 및 배포: 전 세계 사용자가 중요한 주제 및 인기 급상승 스토리를 추적하는 등 신뢰할 수 있는 검색 결과 및 정보를 빠르게 찾을 수 있도록 지원하는 동시에 사용자에게 개인 정보를 제어할 수 있도록 지원하는 세계적 수준의 인터넷 검색 엔진을 제공하는 데 전념하는 팀입니다.

Microsoft 고객 및 파트너 솔루션: 보안 및 기술 영업 전문가와 고문 등 현장 역할을 담당하는 Microsoft 통합형 상업용 출시 관련 조직입니다

Microsoft Defender 전문가: 제품 중심 보안 연구원, 응용 과학자 및 위협 인텔리전스 분석가로 구성된 Microsoft의 가장 큰 규모의 글로벌 조직입니다. Defender 전문가는 Microsoft 365 보안 제품 및 Microsoft Defender Experts 관리 서비스에서 혁신적인 검색 및 대응 기능을 제공합니다.

Microsoft Defender for IoT: IoT/OT 맬웨어, 프로토콜, 펌웨어의 리버스 엔지니어링을 전문으로 하는 도메인 전문가 연구원으로 구성된 팀입니다. 이 팀은 IoT/OT 위협을 헌팅하여 악의적인 추세와 캠페인을 발견합니다.

Microsoft Defender 위협 인텔리전스(RiskIQ): Microsoft의 광범위한 외부 원격 분석 컬렉션 분석을 통해 전술 인텔리전스를 생성하고, 이전에 알려지지 않은 위협 인프라를 발견하도록 진화하는 위협 환경을 차트화하고, 위협 행위자 및 캠페인에 컨텍스트를 추가하는 팀입니다. 이 팀은 방어자들에게 중요한 전술 정보를 제공하기 위해 시기적절하고 독특한 연구를 정기적으로 발표합니다.

Microsoft 보안 비즈니스 개발 팀: Microsoft의 사이버 보안 성장 전략, 파트너십, 전략적 투자를 주도하는 팀입니다.

MSRC(Microsoft Security Response Center, Microsoft 보안 대응 센터): Microsoft의 고객 및 파트너 생태계를 보호하기 위해 노력하는 보안 연구원과 협력하는 팀입니다. Microsoft CDOC(사이버 방어 운영 센터)의 필수적인 부분인 MSRC는보안 대응 전문가를 한데 모아 위협을 실시간으로 보호, 탐지, 대응할 수 있도록 지원합니다.

인시던트 대응을 위한 Microsoft 보안 서비스: 조사에서 성공적인 억제 및 복구 관련 활동에 이르기까지 전체 사이버 공격을 통해 고객을 지원하는 사이버 보안 전문가 팀입니다. 서비스는 복구에 대한 조사 및 기초 작업에 중점을 둔 DART(탐지 및 대응 팀)와 억제 및 복구 측면에 중점을 둔 CRSP(손상 복구 보안 관행)라는 두 개의 고도로 통합된 팀을 통해 제공됩니다.

MSTIC(Microsoft Threat Intelligence Center, Microsoft 위협 인텔리전스 센터): 국가 차원의 위협, 맬웨어, 피싱 등을 포함하여 Microsoft 고객에게 영향을 미치는 가장 정교한 공격자와 관련된 인텔리전스를 식별, 추적, 수집하는 데 집중하는 팀입니다.

1ES(One Engineering System, 단일 엔지니어링 시스템): Microsoft 개발자가 최대한 생산적이고 안전하게 작업할 수 있도록 지원하는 세계적 수준의 도구를 제공한다는 사명을 지닌 팀입니다. 이 팀은 Microsoft의 엔드 투 엔드 소프트웨어 공급망을 보호하기 위한 중앙 전략을 이끌고 있습니다.

OpTIC(Operational Threat Intelligence Center, 운영 위협 인텔리전스 센터): Microsoft와 Microsoft의 고객을 보호하기 위한 Microsoft CDOC(Cyber Defense Operation Center, 사이버 방어 운영 센터)의 임무를 지원하는 사이버 위협 인텔리전스를 관리하고 배포하는 팀입니다.

Microsoft

위협 환경을 조명하고 디지털 방어를 강화합니다.

- 자세히 알아보기: https://microsoft.com/mddr
- 자세히 살펴보기: https://blogs.microsoft.com/on-the-issues/
- 교류하기: @msftissues 및 @msftsecurity