사이버 위협 보고서

2023년 6월

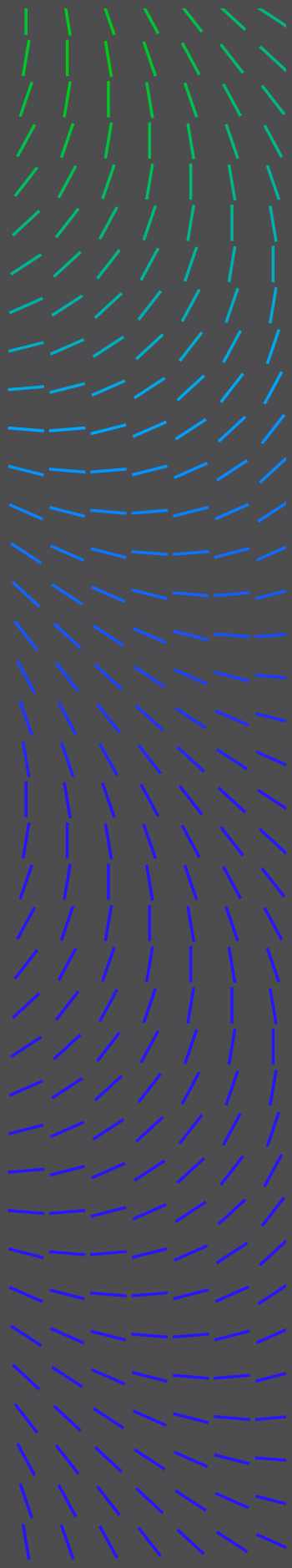
전문가, 센서, 원격 측정 및 인텔리전스의
글로벌 네트워크로부터 얻은 인사이트

제공:

Trellix ADVANCED RESEARCH CENTER

사이버 위협 보고서

Trellix의 Advanced Research Center에서 작성한 이 보고서는 (1) 사이버 보안 위협에 대한 여러 중요 데이터 소스에서 수집한 인사이트, 인텔리전스 및 지침을 강조하고, (2) 사이버 방어의 모범 사례를 알리고 활성화하기 위해 이 데이터에 대한 전문적이고 합리적이며 타당한 해석을 개발합니다. 본 호에서는 2023년 1월 1일부터 2023년 3월 31일 사이에 수집된 데이터 및 인사이트에 중점을 둡니다.



사이버 위협은 속도와 규모에 있어 계속해서 진화하고 증가합니다.

보안 운영 팀이 정보, 자산 및 운영을 방어하기 위해 경쟁하고 있지만, 어느 누구도 위협 환경을 완전하게 파악하지 못합니다.

이유가 무엇입니까? 관점을 얻기 위해서는 넓은 시야가 필요합니다. 여러 개의 소스와 데이터 스트림, 가공하지 않은 인텔리전스, 방대한 양의 원격을 분석합니다.

진정한 인사이트를 얻으려면 많은 조직과 산업 전반에 걸친 전략적 관점이 필요합니다. 그리고 지역과 공격 영역도 마찬가지입니다.

사이버 위협 보고서 2023년 6월 호에 오신 것을 환영합니다.

공격자가 표적으로 삼는 위험, 위협 및 취약성을 이해하고 적극적으로 대응하기

저는 이사회 구성원, CEO, CISO, CIO, CTO 및 국가, 정부 기관, 업계 전반에서 민간 부문 조직의 사이버 방어를 담당하는 기타 리더들과 대화하는 데 많은 시간을 할애합니다.

Trellix는 글로벌 연구, 혁신 및 인텔리전스에서 보안 운영 팀의 최신 사이버 방어 관행에 이르기까지 다양한 주제를 다룹니다. Trellix가 최근 The Mind of the CISO 리더십에서 언급한 바와 같이 다양한 과제에 대해 이야기합니다. 너무 많은 정보 출처(35%), 규제 의무 및 법적 요구 사항 변경(35%), 공격 영역 증가(34%), 숙련된 직원 부족(34%), 구매 부족 및 회사의 다른 부품 사용(31%)[1] 등이 그 예입니다.

거의 모든 이러한 상호작용은 직접적으로 또는 암시적으로 위협 환경의 특성을 다룹니다. 어떤 종류의 공격이 전개되고 있습니까? 가장 영향력 있는 랜섬웨어 그룹은 무엇입니까? 표적이 되는 취약성은 무엇입니까? 어떤 국가가 가장 활동적인 것으로 보입니까? 이메일 및 네트워크 보안에서 어떤 위협 동향을 추적하고 있습니까?

"이사회 구성원, CEO, CISO, CIO, CTO 또는 보안 운영 팀 구성원으로서 이 보고서와 Trellix의 다양한 지침, 정보 및 관점 라이브러리에서 공유되는 이 지식은 귀하의 사명에 매우 중요합니다."

Trellix는 매일 최전선에 있기 때문에 공유할 것이 많습니다. Trellix는 전 세계적으로 10억 개 이상의 센서에서 수집한 방대한 양의 보안 인텔리전스, 인사이트 및 데이터를 활용하고 있습니다. 이사회 구성원, CEO, CISO, CIO, CTO 또는 보안 운영 팀 구성원으로서 이 보고서와 Trellix의 다양한 지침, 정보 및 관점 라이브러리에서 공유되는 이 지식은 임무에 매우 중요합니다.

Trellix의 엘리트 Advanced Research Center 팀 내에서 위협 인텔리전스 관행을 이끌고 있는 제 동료 John Fokker가 여기에 훌륭한 보고서를 작성했습니다. 이러한 인사이트를 통해 팀에 집중하고 프로세스를 강화하며 올바른 XDR 기술을 적용할 수 있습니다. 그리고 귀하의 조직의 안전, 보안, 번영을 보장하기 위해 향후 버전에서 집중해야 할 부분에 대해 알려주십시오.

Joseph (Yossi) Tal
SVP, TRELLIX ADVANCED RESEARCH CENTER 소장

사이버 보안의 최전선 영웅들을 위한 지원

저는 영웅들과 함께 일합니다. 비록 저희 팀이 다양한 공공 및 민간 부문 경력에서 초능력을 가진 것으로 간주되어 왔지만 저희 팀을 말하는 것이 아닙니다.

바로 여러분을 말하는 것입니다. 사이버 공격으로부터 조직을 보호하기 위해 Trellix의 지능형 연구 기능(시스템, 인사이트 및 인텔리전스)에 의존하는 전 세계 사람들과 팀에 대해 이야기하고 있습니다. CISO, CTO 및 CIO는 물론 Europol, FBI 및 NSA, CISA(사이버 보안 및 인프라 보안국), ACSC(호주 사이버 보안 센터), 영국 NCSC-UK(국립 사이버 안보 센터)와 같은 기관의 동료들도 마찬가지입니다. 마찬가지로 중요한, 아마도 훨씬 더 중요한 사람은 바로 보안 운영 팀의 모든 구성원일 것입니다.

"매일 수행하는 업무를 통해 잘 알고 계시듯이 사이버 보안은 놀라울 정도로 빠르게 발전하고 있습니다. 기술의 혁신과 XDR로의 강력한 전환이 이루어지고 있습니다."

보안 운영 임무의 판도를 바꾸는 것은 무엇이라고 생각하십니까? 제 동료 Yossi가 언급한 Trellix 보고서에 따르면 전 세계 사이버 보안 리더들은 이에 대한 자신들의 견해를 공유했습니다. 여기에는 가시성 향상(44%), 중요 사항에 대한 우선순위 강화(42%), 다중 벡터 공격을 해결하기 위한 더 광범위한 협업(40%) 및 정확도 향상(37%)이 포함되었습니다.[2]

이러한 모든 요소는 기본적으로 이 보고서의 내용과 같은 정확한 인사이트, 정보 및 데이터에 의존합니다.

매일 수행하는 업무를 통해 잘 알고 계시듯이 사이버 보안은 기술의 혁신과 XDR로의 강력한 전환, 법에서 책임으로의 규정 변화, 위협 환경의 변화와 같이 놀라울 정도로 빠르게 발전하고 있습니다. 운영 보안 팀이 사이버 공격에서 다음 세대보다 "한발 앞서" 있을 수 있는 방법에 대한 혁신이 진행 중입니다. 승리는 항상 현재 상태에 대한 이해와 함께 인사이트에서 시작됩니다.

Trellix와 함께 하십시오. Trellix가 도와드립니다. 이 보고서는 귀하를 위한 것입니다.

John Fokker
위협 인텔리전스 책임자 및 수석 엔지니어
TRELLIX ADVANCED RESEARCH CENTER

[1] Trellix, "2023 보고서: The Mind of the CISO," 2023.
[2] Trellix, "2023 보고서: The Mind of the CISO," 2023.

전략적 맥락: 불안정한 세상

이 보고서의 데이터를 해석하려면 글로벌 규모의 "더 큰 그림"을 이해해야 합니다. 전 세계 조직에 대한 사이버 위협이 기술적 공백 상태에서 발생하지 않기 때문입니다. 사이버 위험의 주요 동인에는 전쟁 및 기타 불가항력, 경제 주기의 대규모 변화, 팀이 비즈니스 모델, 주요 파트너, 핵심 프로세스, 기술 채택 및 컴플라이언스 규제정책과 같은 요인에 변화를 도입할 때마다 나타날 수 있는 새로운 취약성 등이 있습니다. 2023년 1분기 위협 데이터에 영향을 미치는 요인의 샘플링은 다음과 같습니다.

러시아의 우크라이나 침공 및 서방과의 비대칭 전쟁: 주요 국가의 정치적, 경제적, 영토적 야망을 위한 스파이 활동, 전쟁 및 허위 정보를 목적으로 하는 사이버 활동이 계속해서 증가하고 있습니다. 해커들은 서구 기업, 정부 및 인프라에 점점 더 정교한 사이버 공격을 가하고 있습니다.

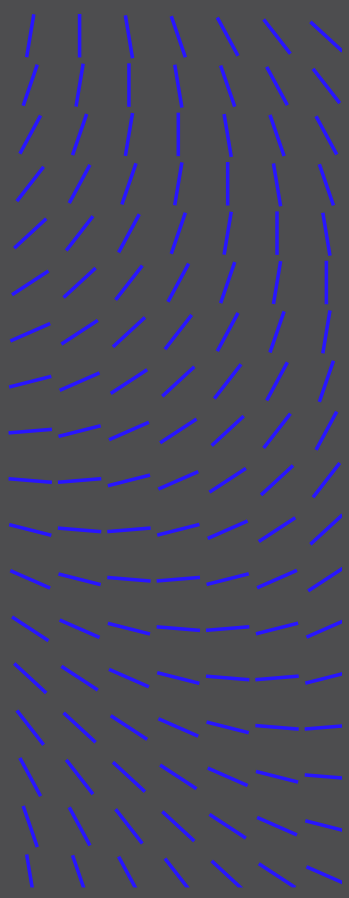
중국에 대한 시진핑의 통합된 통제와 지정학적 열망: 중국과 연계된 APT(지능형 지속 공격) 그룹이 전 세계를 장악함에 따라 중국의 민족주의적 목표, 독단적인 외교 정책 및 기업 스파이 행위는 계속해서 사이버 위험을 주도하고 있습니다.

개발 도상국 및 급속한 인프라 확장: 많은 개발도상국이 경제 성장에 따라 인프라와 기술을 확장하면서 사이버 보안을 최우선 순위로 삼지 않는 경우가 많습니다. 이로 인해 중요한 인프라에서 많은 사이버 관련 취약성이 많이 발생합니다.

글로벌 인플레이션과 경제 및 정치적 영향: 이번 분기에는 시장 변동성, 금융 및 정치적 위기, 지출 우선순위 및 사이버 보안 예산에 대한 압박이 포함되었습니다.

코로나19 이후 지속되는 공급망 중단: 여러 지역에 걸친 새로운 시장 진출 경로를 구축하기 위해 파트너, 운송 네트워크, 정보 공유, 그리고 더 나아가 사이버 위험의 변화가 필요했습니다. 사이버 위협이 매일 공급망에 영향을 미치기 때문에 제로 트러스트 기능에 대한 필요성은 업계 전반에 걸쳐 여전히 매우 높습니다.

Apple의 우수한 보안 환경에 대한 믿음: 위협 행위자가 Golang 기반 맬웨어를 대규모로 활용하고 공격 벡터를 확장하여 수많은 운영 체제를 포괄하기 시작함에 따라 macOS 환경이 더 이상 안전한 것으로 간주될 수 없다는 사실에도 불구하고 Apple의 우수한 보안 환경에 대한 믿음은 지속되고 있습니다.



혼란을 초래하며 세계 무대에 등장한 인공 지능: 사이버 방어는 향상된 머신 러닝, 자연어 처리 및 기타 발전으로 도움을 받기도 하고 피해를 입기도 합니다. 글로벌 사이버 위협이 인간 팀이 관리할 수 있는 것보다 훨씬 빠른 속도로 진화하고 발생함에 따라 인공 지능 솔루션은 엔터프라이즈 사이버 방어에 필수가 되었습니다.

사이버 보안: CISO의 과제와 보안 운영 혁신

사이버 보안 실무자 및 보안 운영 팀에게 가장 중요한 과제는 무엇입니까?
위협 인텔리전스를 대규모로 신속하게 소화하고 조직 전반에 걸쳐 실행 가능한 인사이트를 위협 대응 팀과 태스크포스팀에 즉시 전달하는 것입니다.

Trellix의 목표는 무엇입니까? 이러한 여정을 단순화하는 것입니다.

방법 XDR, 호스트 보호, 네트워크 및 메일 제품에 내장된 우수한 위협 인텔리전스, 위협 대응 및 보안 운영 기능을 사용하여 조직이 집중해야 하는 대응에 필요한 수준의 자동화를 제공합니다.

올해 1분기 위협 환경은 또한 사내 요인의 영향을 받았는데, 그중 상당수는 사이버 보안 리더와 최전선 팀이 직면하고 있는 지속적인 역풍을 반영합니다.

오래된 기술: 많은 조직이 SOAR 및 SIEM과 같은 레거시 기술에 계속 의존하고 있습니다. 실제로 CISO의 96%는 사이버 위협으로부터 회사를 보호하기 위해 더 나은 솔루션이 필요하다고 말합니다.[3]

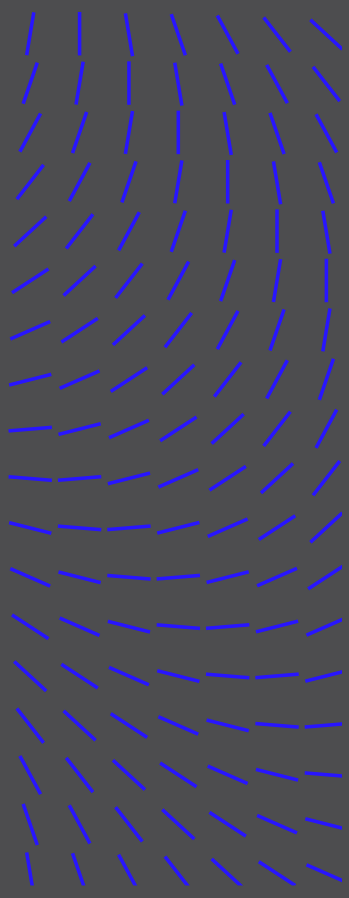
보안 도구의 바다: 보안 운영 팀은 경고가 넘쳐나고 시간에 대한 우선순위를 지정하는 데 필요한 것이 부족합니다. 평균적으로 조직은 25개의 보안 솔루션 및 도구를 사용합니다.[4]

경고 피로: 경고가 넘쳐나는 보안 운영 팀은 우선순위 지정, 오탐, 경고 누락으로 인해 어려움을 겪고 있습니다. IDC에 따르면 35%는 경고를 무시합니다. 이는 부분적으로 45%가 오탐이기 때문입니다.[5]

리소스 부족: 제한된 보안 운영 리소스와 전문 지식으로는 위협에 효과적으로 대응하기 어렵습니다. SOC 분석가의 평균 재직 기간은 얼마입니까? 약 2년입니다.[6]

방법론: 데이터 수집 및 분석 방법

Trellix Advanced Research Center의 세계적 수준의 전문가들은 광범위한 전속 및 공개 글로벌 소스에서 이 보고서를 구성하는 통계, 동향 및 인사이트를 수집합니다. 집계된 데이터는 Insights 및 ATLAS 플랫폼에 제공됩니다. 팀은 머신 러닝, 자동화 및 인간의 민첩성을 활용하여 데이터를 정규화하고, 정보를 분석하고, 전 세계 사이버 보안의 최전선에 있는 사이버 보안 리더 및 보안 운영 팀에 의미 있는 인사이트를 개발하는 등 집중적이고 통합적이며 반복적인 일련의 프로세스를 순환합니다. 방법론에 대한 자세한 설명은 이 보고서의 마지막 부분을 참조하십시오.



응용프로그램: 이 정보를 사용하는 방법

업계를 선도하는 모든 평가 팀은 누구나 사실과 그 의미를 수용, 거부 또는 조작하려는 자연적, 내재적 또는 보이지 않는 성향인 편향의 영향을 이해하고 인정하며 가능한 한 완화해야 합니다. 콘텐츠 소비자에게도 동일한 원칙이 적용됩니다.

고도로 구조화된 통제 기반 수학 테스트 또는 실험과는 달리 이 보고서는 본질적으로 편리성의 표본입니다. 즉, 사용 가능하고 접근 가능한 데이터를 이용하는 의료, 건강 관리, 심리학 및 사회학 테스트에서 자주 쓰이는 비확률 유형의 연구입니다.

간단히 말해 여기에서의 발견은 관찰할 수 있는 내용을 기반으로 하며 탐지, 보고 및 데이터 캡처를 우회하는 위협, 공격 또는 전술의 증거를 포함하지 않습니다.

"완전한" 정보나 "완벽한" 가시성이 없는 상태에서 이는 사이버 보안 위협에 대한 중요한 데이터의 알려진 출처를 식별하고, 사이버 방어에서 모범 사례를 알리고 이를 가능하게 하는 데이터에 대한 합리적이고 전문적이며 윤리적인 해석을 개발하고자 하는 본 보고서의 목적에 가장 적합한 유형의 연구입니다.

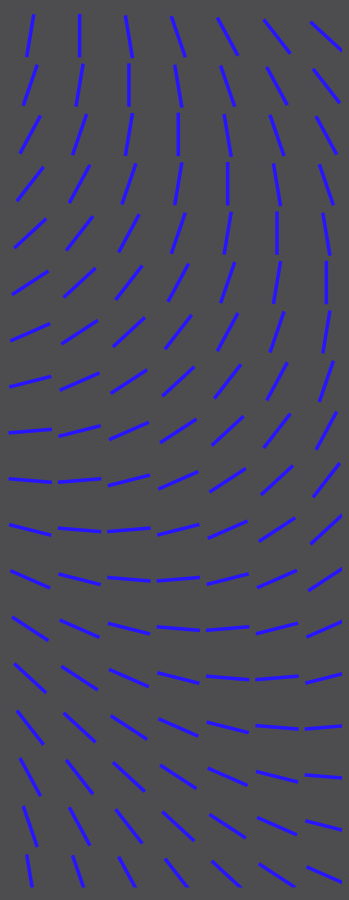
이러한 조사 윤리의 핵심은 다음과 같습니다.

시간의 스냅숏: 그 누구도 인터넷에 연결된 모든 시스템의 모든 로그에 액세스할 수 없으며 모든 보안 사고가 보고되는 것도 아니며 모든 피해자가 탈취당하고 유출 사이트에 포함되는 것도 아닙니다. 그러나 우리가 추적할 수 있는 것을 추적하면 분석 및 조사 사각지대를 줄이면서 다양한 위협을 더 잘 이해할 수 있습니다.

오탐 및 미탐: 데이터를 수집하기 위한 Trellix의 특수 추적 및 원격 측정 시스템의 고성능 기술 특성 중에는 오탐 및 미탐 결과에 대응하거나 이를 제거하는 데 도움이 되는 메커니즘, 필터 및 전술이 있습니다. 이를 통해 분석 수준과 연구 결과의 품질을 향상시킬 수 있습니다.

감염이 아닌 탐지: 원격 측정에 대해 이야기할 때 Trellix는 감염이 아닌 탐지에 대해 이야기합니다. 파일, URL, IP 주소 또는 기타 지표가 Trellix의 제품 중 하나에 의해 탐지되고 다시 Trellix에 보고되면 탐지가 기록됩니다.

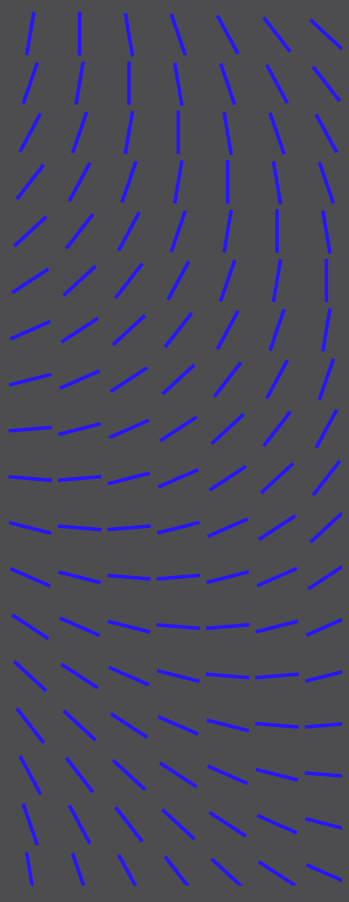
고르지 않은 데이터 캡처: 일부 데이터세트에는 신중한 해석이 필요합니다. 예를 들어 통신 데이터에는 다른 많은 산업 및 섹터에서 운영되는 ISP 클라이언트의 원격 측정이 포함됩니다.



국가 속성: 마찬가지로 국가 해커와 사이버 범죄자가 서로를 속이거나 악의적인 활동을 신뢰할 수 있는 소스에서 오는 것으로 위장하는 등의 일반적인 관행을 고려할 때 다양한 사이버 공격 및 위협에 대한 국가의 책임을 결정하는 것은 매우 어려울 수 있습니다.

앞으로의 길: 지침 및 리소스

이 보고서에 포함된 정보는 최전선의 사이버 보안 영웅들에게 어떤 의미가 있습니까? 사이버 보안 인사이트와 데이터는 행동으로 전환되는 경우에만 유용하며 위험 감소, 의사 결정 개선 또는 더욱 효율적이고 비용 효과가 좋은 보안 운영 활동으로 이어집니다. 추가 지침 및 리소스를 확인하려면 www.trellix.com을 방문하십시오.



[3] Trellix, "2023 보고서: The Mind of the CISO," 2023
[4] Trellix, "2023 보고서: The Mind of the CISO," 2023
[5] IDC Voice of the Analysts, 2021
[6] Ponemon Institute, 2020

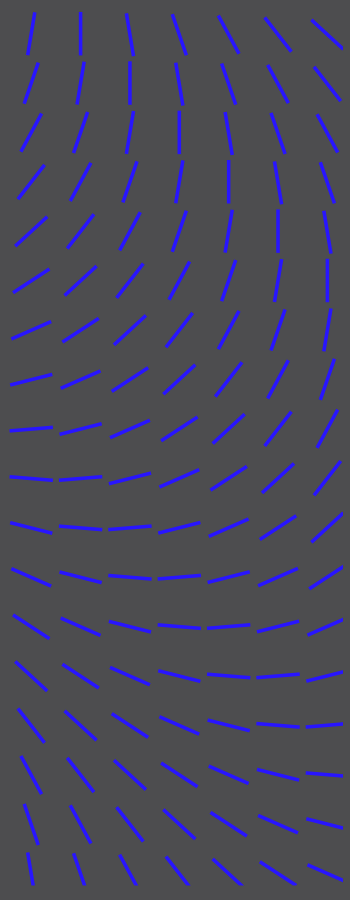
한눈에 보는 2023년 1분기 요약

랜섬웨어 환경

- **랜섬웨어의 물결:** 랜섬웨어는 전 세계적인 사이버 공격의 주요 유형으로 계속해서 왕좌를 차지하고 있습니다. 피싱과 같이 개인을 속이고 조작하여 기밀이나 개인 정보를 누설하는 소셜 엔지니어링 술책은 더욱 정교해지면서 그 어느 때보다 널리 퍼져 있습니다.
- **Cuba와 Play의 우세:** 연초에 몸값 관련 사이버 범죄 활동이 감소된 것이 관찰되었지만 1분기에 가장 널리 퍼진 랜섬웨어 계열은 Cuba(9%)와 Play(7%)였습니다.
- **LockBit의 잔류:** 2분기 연속 활동 감소에도 불구하고 LockBit은 여전히 가장 공격적인 랜섬웨어로, 피해자들이 몸값 요구를 따르도록 압력을 가하고 있습니다.
- **Magecart Group의 잠재적 부상?** 공개 보고에 따르면 이 신용 카드 절도 및 전자상거래 스캘핑 그룹의 2023년 1분기 활동이 크게 증가했습니다. 이러한 위협은 국가와 관련된 다른 주요 APT와 동일한 규모의 활동으로 작동하는 경우가 거의 없으며, 전 세계적으로 Magecart Group이 다시 등장하고 있음을 잠재적으로 나타냅니다.

진화하는 랜섬웨어 전술

- **금전적 목표:** 랜섬웨어의 동기가 주로 재정적이라는 것은 놀라운 일이 아닙니다. 보험(20%) 및 금융 서비스(17%) 섹터는 잠재적인 공격을 가장 많이 탐지했습니다.
- **가장 큰 영향을 받는 중견 기업:** 유출 사이트 데이터를 평가한 결과 이러한 공격의 가장 일반적인 피해자는 직원 수가 51~200명(32%)에 불과하고 수익이 1,000만~5,000만 달러(38%)인 중견 기업인 것으로 나타났습니다.
- **주요 표적으로서의 미국:** 랜섬웨어 그룹의 영향을 가장 많이 받은 국가는 미국(15%)이었습니다. 또한 공격자로부터 "데이터를 다시 구입"하기로 결정한 기업 피해자의 비율이 가장 높은 국가(48%)이기도 합니다. 이는 2위 국가인 영국보다 6배 더 높은 비율입니다.
- **선택된 무기로서의 Cobalt Strike:** Trellix 원격 측정에 따르면 이 도구는 랜섬웨어 행위자들이 매우 선호하는 것으로 나타났습니다(인시던트의 28%). 2022년 4분기 후반, 공급업체 Fortra는 위협 행위자들이 이를 사용하기 어렵게 만들려고 했으나 이러한 행위자 그룹들 사이에서 Cobalt Strike의 인기와 사용은 증가하고 있는 것으로 보입니다.



국가 위험 신호

- **주요 행위자:** 지난 6개월 동안 Mustang Panda 및 UNC4191을 포함하여 중국과 연계된 APT 행위자들은 1분기에 국가를 표적으로 삼는 데 가장 적극적이었습니다. 중국과 연계된 위협 행위자들이 전체 국가 활동의 79.3%를 차지하여 전 세계 무대를 지배했으며 북한, 러시아 및 이란과 관련된 행위자들이 그 뒤를 이었습니다.
- **가장 활발한 APT 그룹:** Mustang Panda는 3분기 연속으로 전 세계에서 가장 활발한 APT 그룹(72%)의 자리를 유지했습니다. 이는 중국이 스파이 활동과 교란을 목적으로 한 악의적인 사이버 활동을 지속하고 있으며 계속해서 증가하고 있음을 나타냅니다.

취약성 인텔리전스

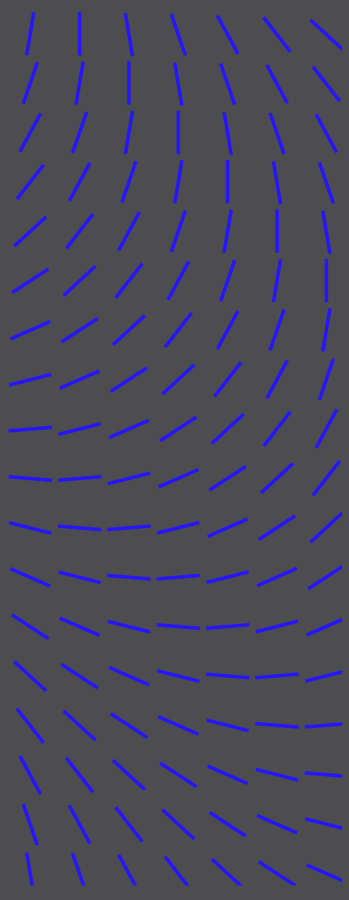
- **알려진 취약성 해결 실패:** 이번 분기의 가장 치명적인 취약성은 알려진 취약성이 대부분이나 아직 해결되지 않았습니다.
- **어제의 뉴스:** 올해 2월에 공개된 Apple 취약성의 경우, 버그는 2021년에 공개된 Pegasus 스파이웨어의 일부로 NSO Group에서 사용된 FORCEDENTRY 익스플로잇까지 거슬러 올라갑니다.

이메일 보안

- **새로운 공격 수단:** Microsoft가 Office 플랫폼에 대한 매크로 첨부 파일을 차단하기 시작했지만 위협 행위자들은 SEO 포이즈닝, OneNote 및 Zip 첨부 파일과 같은 다른 감염 수단을 신속하게 채택하여 Windows 장치를 계속해서 표적으로 삼았습니다.
- **신뢰할 수 없는 브랜드:** 일반적인 피싱 이메일 외에도 점점 더 많은 악의적인 행위자들이 PayPal, Google, DWeb 및 IPFS와 같은 합법적인 브랜드 이름과 서비스를 활용하여 피해자를 속이고 온라인 자격 증명을 도용하고 있습니다.

클라우드에 대한 비인가 액세스

- **전술의 변화:** 점점 더 많은 기업이 온프레미스 인프라에서 Amazon, Microsoft, Google 등의 좀 더 경제적이고 확장 가능한 옵션으로 전환함에 따라 클라우드 인프라 공격이 계속 증가하고 있습니다.
- **유효한 계정:** 다단계 인증, 프록시 및 API 실행을 통한 더욱 정교한 공격이 우세하지만, 지배적인 공격 기술은 계속해서 유효한 계정을 통해 이루어지며 두 번째로 많이 사용되는 공격 벡터 빈도의 두 배 이상입니다. 이는 비인가 액세스의 위험이 현실임을 강조합니다. 사이버 범죄자들이 합법적인 계정이나 웹 사이트 로그인에 액세스하고 이를 판매하여 침투하고 공격을 감행하기 때문입니다.



보고서 분석, 인사이트 및 데이터

보안 인시던트

이 섹션에서 설명하는 보안 인시던트는 공개 보고서를 기반으로 합니다. 2023년 1분기에는 위협 행위자들이 저항이 가장 적은 경로를 악용함에 따라 Windows 바이너리, 타사 도구, 사용자 지정 맬웨어 및 침투 테스트 도구가 계속해서 운영에 영향을 미쳤습니다. PowerShell 및 Windows Command Shell은 지속성, 배포 및 추출로 이어지는 작업을 생성하는 데 계속해서 남용되었습니다.

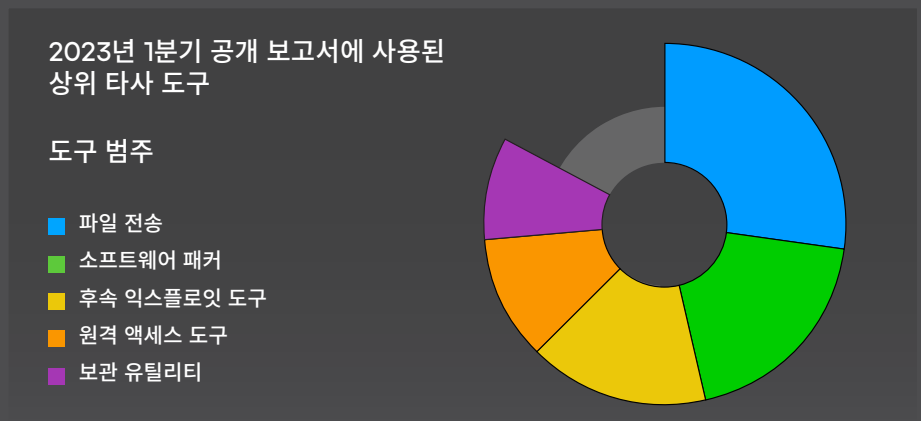
2023년 1분기 이벤트에 사용된 상위 WINDOWS 바이너리

1. PowerShell
2. Windows CMD
3. 예약된 작업
4. RunDLL32
5. WMIC

작업 예약, 악성 DLL 파일 삽입 및 WMI(Windows Management Instrumentation)를 통해 실행되는 명령은 상위 5개를 차지했습니다. 스크립트로 실행하든 수동 키보드 입력으로 실행하든 위협 행위자는 이미 보호되지 않고 모니터링되지 않는 바이너리를 계속해서 마음대로 사용했습니다.

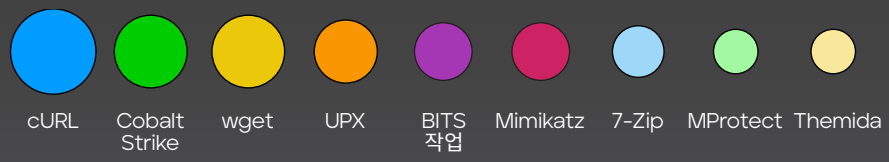
많은 경우 타사 도구, 프리웨어 및 침투 테스트 도구는 지속성 설정, 스크립트 실행, 표적 정보 검색 및 수집, 다른 방법으로는 제한된 계정에 액세스할 수 없는 자산 또는 데이터에 대한 액세스 권한 상승에서 위협 행위자를 지원하는 공격 라이프사이클의 역할을 합니다. 또한 권한 상승에 사용되는 경우 공격자는 다른 방법으로는 제한된 계정에 액세스할 수 없는 높은 권한 및 액세스 영역, 자산 또는 데이터로 설치 프로세스를 실행할 수 있습니다.

2023년 1분기 공개 보고서에 사용된 상위 타사 도구



2023년 1분기 공개 보고서에 사용된 타사 도구

특정 도구



Cobalt Strike, Mimikatz 및 Sharphound와 같은 비도덕적인 타사 도구는 위협 행위자가 암호를 수집하거나 비콘을 설정하거나 권한을 높이는 데 합법적으로 사용됩니다. 공격자가 환경을 손상시키면 cURL과 같은 파일 전송 도구를 사용하여 원격 페이로드에 액세스하거나 Rclone을 사용하여 데이터를 클라우드 스토리지로 반출할 수 있습니다.

2023년 1분기에 Magecart Group, APT29 및 APT41은 금전적 가치를 수집하거나 정부의 기밀을 밝히거나 인프라 사용을 억제하기 위한 방법으로 지리적 위치 및 섹터별로 사용자를 표적으로 삼은 가장 활발한 세 가지 위협 그룹 및 APT였습니다. Magecart Group이 다른 주요 국가 관련 APT의 규모로 작동하지 않기 때문에 1위를 차지했다는 사실은 놀랍습니다. Trellix는 앞으로 몇 달 동안 그룹의 활동을 모니터링하여 현재의 데이터가 글로벌 무대에서 그룹의 재부상을 알리는 신호인지를 파악할 것입니다.

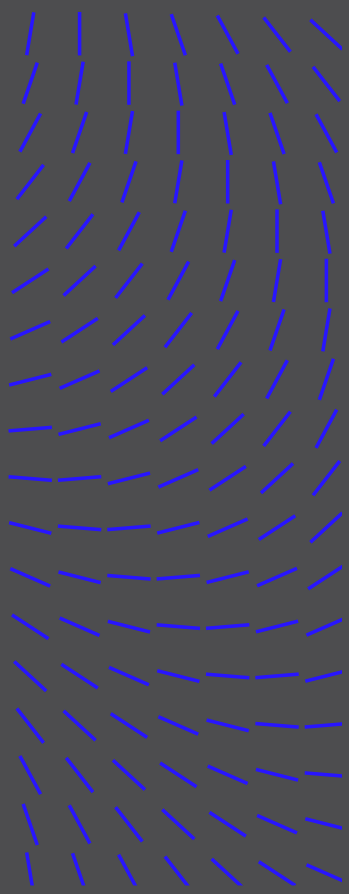
2023년 1분기 공개 보고서의 활발한 상위 위협 행위자

1.	Magecart Group	5%
2.	APT29	4%
3.	APT41	4%
4.	Blind Eagle	4%
5.	Gamaredon Group	4%
6.	Lazarus	4%
7.	Mustang Panda	4%
8.	Sandworm Team	4%

과거 글로벌 캠페인의 경우 문제가 된 섹터를 클릭하거나 다운로드하는 사람을 고르기 위해 비교적 단순한 뿌려놓고 기도하기(spray-and-pray) 기술을 사용했습니다. 표적 공격은 정교하게 발전하여 제조, 금융 및 의료 섹터에 대한 지속성이 증가했습니다. 나머지 두 섹터인 통신과 에너지는 글로벌 이벤트에서 표적이 되었던 빈도가 적었던 것으로 보이지만 두 섹터 모두 똑같이 중요하며 그 안에 있는 조직은 침해를 보고하지 않았거나 인시던트를 인식하지 못했을 수 있습니다.

2023년 1분기 공개 보고서의 표적이 된 상위 섹터

1.	제조	8%
2.	금융	7%
3.	건강	6%
4.	통신	5%
5.	에너지	5%



Trellix 연구팀이 분석하고 조사한 이벤트에는 개별 위협 행위자, 위협 그룹 또는 더욱 정교한 APT에 대한 풍부한 정보, 상관관계 또는 속성이 포함되어 있습니다. 맬웨어 계열과 함께 도구, 기술 및 절차에는 로더 및 다운로더 맬웨어, RAT, 정보 도용자 및 랜섬웨어가 포함됩니다. Insights를 통해 분석되고 제공되는 2023년 1분기 이벤트에서 Trellix는 우크라이나가 가장 빈번하게 표적이 되었고 미국이 그 뒤를 바짝 쫓고 있다고 판단했습니다.

Royal Ransom, Trigona 및 Maui 랜섬웨어 계열은 2023년 1분기에 큰 타격을 입혔습니다. Trellix는 최근 Royal Ransom과 Windows 및 Linux 실행 파일의 내부 작업에 대한 자세한 분석을 발표했습니다. 표시된 통계는 특히 Insights 플랫폼에서 나온 것이지만 전 세계적으로 연결된 인프라에서 많은 추가 이벤트가 발생했습니다. 여기에는 보고되거나 비공개로 유지되는 알려진 이벤트와 아직 식별 및 해결되지 않은 이벤트가 포함됩니다.

2023년 1분기 공개 보고서의 표적이 된 상위 국가

7%

분석에 사용될 수 있는 공개 이벤트에서 Trellix는 우크라이나가 위협 행위자들에 의해 가장 많이 표적이 된 국가였으며 미국이 그 뒤를 바짝 쫓고 있다고 판단했습니다.

1.	우크라이나	7%
2.	미국	7%
3.	독일	4%
4.	대한민국	3%
5.	인도	3%

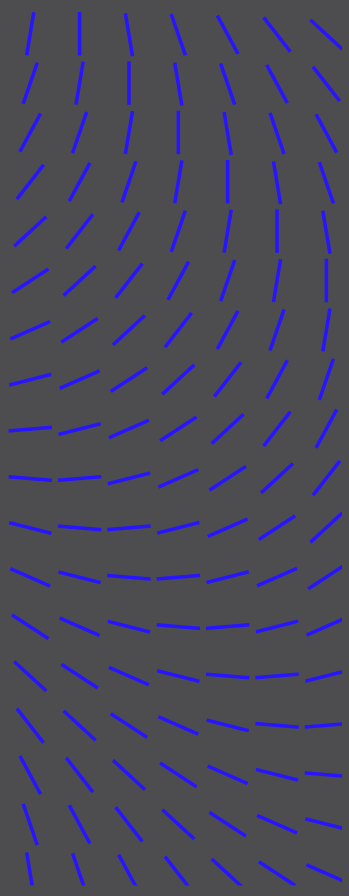
2023년 1분기 공개 보고서에 사용된 상위 랜섬웨어

1.	Royal Ransom	7%
2.	Trigona	4%
3.	Maui	4%
4.	Magniber	3%
5.	LockBit	3%

랜섬웨어

아래에 표시된 통계는 탐지 자체가 아닌 캠페인의 통계입니다. Trellix의 글로벌 원격 측정 결과 다양한 랜섬웨어 그룹의 여러 캠페인에 속하는 침해 지표(IoC)가 드러났습니다.

연초, 특히 1월에 사이버 범죄 활동이 감소하는 것은 상당히 흔한 일입니다. 이러한 동향은 Hive와 Cuba의 활동이 현저하게 감소한 것을 설명할 수 있습니다. 게다가 FBI와 Europol이 1월 말에 Hive의 활동을 중단시킨 것은 이들의 운영에 상당한 방해가 되었을 것입니다. LockBit은 여전히 랜섬웨어 분야의 주요 계열이고 특히 공격적이며 피해자가 몸값을 지불하도록 유도하는 데 성공적인 것으로 보입니다.



2023년 1분기 이벤트에 사용된 상위 랜섬웨어

8%

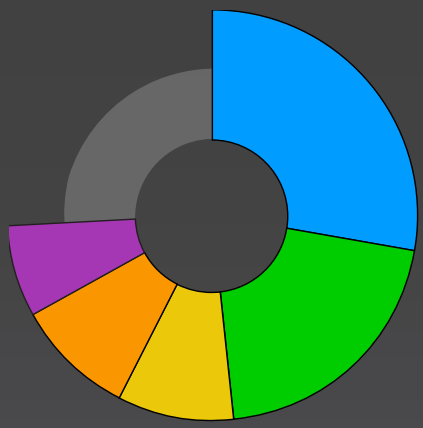
Cuba는 가장 활동적인 랜섬웨어 그룹이었고 Play와 LockBit이 그 뒤를 이었습니다.

- Cuba
- Play
- LockBit 3.0
- Clop
- Hive

2023년 1분기에 사용된 랜섬웨어 도구

28%

CobaltStrike는 이번 분기 전체 랜섬웨어 인시던트의 거의 3분의 1에 사용되었으며 위협 행위자가 도구를 남용하는 것을 더 어렵게 만든 최근 업데이트에도 불구하고 사용량이 증가했습니다.



- Cobalt Strike
- Mimikatz
- Empire
- BloodHound
- SystemBC

2023년 1분기 랜섬웨어 그룹의 영향을 가장 많이 받은 국가

15%

미국은 계속해서 랜섬웨어 활동의 가장 큰 영향을 받는 국가이며, 이번 분기에는 튀르키예가 그 뒤를 바짝 쫓고 있습니다.

1.	미국	15%
2.	튀르키예	14%
3.	포르투갈	10%
4.	인도	9%
5.	캐나다	9%

2023년 1분기 랜섬웨어 그룹의 영향을 가장 많이 받은 섹터

1.	보험	20%
2.	금융 서비스	17%
3.	제약	7%
4.	통신	4%
5.	아웃소싱 및 호스팅	4%

랜섬웨어 그룹은 "유출 사이트"라고 하는 웹 사이트에 정보를 게시하고 피해자와의 교착 상태에 빠진 협상을 시작하거나 몸값 지불이 거부될 때 피해자를 갈취합니다. Trellix 전문가들은 오픈 소스 도구인 RansomLook을 사용하여 게시물에서 데이터를 수집한 다음 결과를 정규화하고 풍부하게 하여 피해자에 대한 익명 분석을 제공합니다.

여기서 중요한 점은 모든 랜섬웨어 피해자가 각 유출 사이트에 보고되는 것이 아니라는 사실입니다. 많은 피해자가 몸값을 지불하고 보고되지 않은 상태로 남아 있습니다. 아래 메트릭은 갈취 또는 보복의 표적이 된 피해자 랜섬웨어 그룹의 지표이며 전체 피해자 수와 혼동해서는 안 됩니다.

2023년 1분기 유출 사이트별 가장 많은 피해자가 보고된 랜섬웨어 그룹

1.	LockBit	30%
2.	Hive	22%
3.	Clop	12%
4.	Royal Ransom	7%
5.	ALPHV	5%

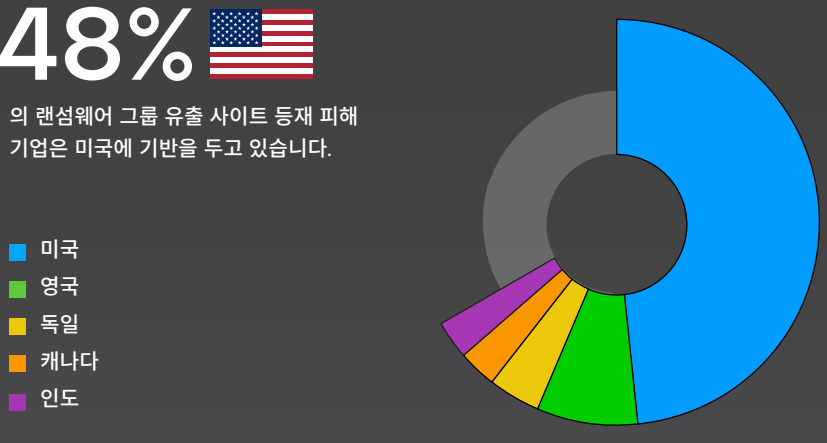
2023년 1분기 유출 사이트별 랜섬웨어 그룹의 영향을 가장 많이 받은 섹터

1.	공산품 및 서비스	25%
2.	소매	14%
3.	기술	11%
4.	건강	8%
5.	금융 서비스	6%

2023년 1분기 랜섬웨어 유출 사이트에 등재된 상위 기업의 국가

48%

의 랜섬웨어 그룹 유출 사이트 등재 피해 기업은 미국에 기반을 두고 있습니다.



2023년 1분기 랜섬웨어 유출 사이트에 등재된 기업의 규모

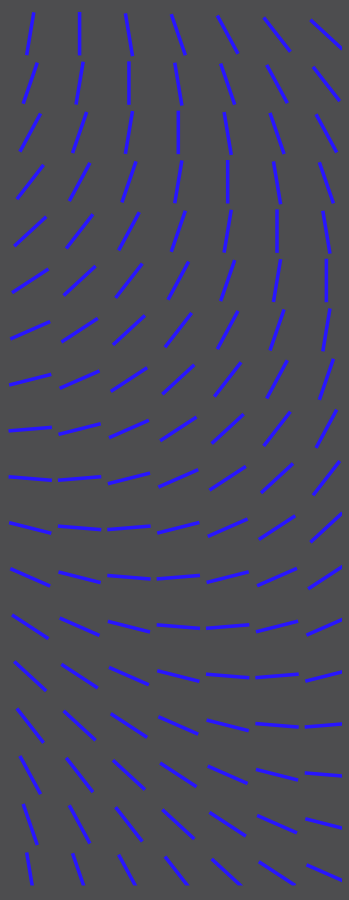
직원 범위		연간 수익	
1. 51~200	32%	1. 1,000만 ~ 5,000만 달러	38%
2. 1,001~5,000	22%	2. 10억~100억 달러	23%
3. 11~50	15%	3. 100만~1,000만 달러	21%
4. 201~500	15%	4. 1억~2억 5천만 달러	11%
5. 501~1,000	15%	5. 5억~10억 달러	7%

국가 활동

여러 소스에서 수집한 국가 그룹 활동에 대한 인사이트는 위협 환경을 보다 잘 파악하고 관찰 편향을 줄이는 데 도움이 됩니다. 먼저, 국가 그룹 IoC와 Trellix 고객 원격 측정의 상관관계에서 추출한 통계를 나타냅니다. 두 번째로 보안 업계에서 발행한 다양한 보고서에 대해 위협 인텔리전스 그룹에서 조사, 분석 및 검토한 내용에 대한 인사이트를 제공합니다.

위에서 언급한 바와 같이 이러한 통계는 탐지 자체가 아닌 캠페인의 통계입니다. 다양한 로그 집계, 고객의 위협 시뮬레이션 프레임워크 사용, 위협 인텔리전스 기술 자료와의 높은 수준의 상관관계로 인해 데이터가 분석 목표를 충족하도록 수동 필터링됩니다.

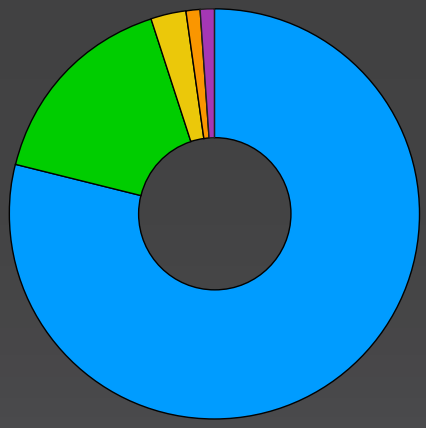
특히 Mustang Panda가 2023년 1분기에 탐지의 상당 부분을 주도하면서 중국 관련 위협 행위자가 전 세계 환경을 지배하는 것을 계속해서 보고 있습니다. 중국 관련 APT 그룹은 사이드로딩 및 기타 스텔스 기술에 크게 의존하기 때문에 다른 위협 행위자에 비해 맬웨어 도구 교체 빈도가 낮을 수 있습니다. 만약 그렇다면 이 관행은 "예상치 편향" 또는 중국 관련 해시 탐지의 부풀려진 추정치로 이어질 수 있습니다.



2023년 1분기 국가 활동 배후에 가장 널리 퍼져 있는 위협 행위자 국가

79%

중국은 2023년 1분기 국가 관련 활동의 대다수를 차지했습니다.



2023년 1분기 가장 널리 퍼져 있는 위협 행위자 그룹

1.	Mustang Panda	72%
2.	Lazarus	17%
3.	UNC4191	1%
4.	Common Raven	1%
5.	APT34	1%

2023년 1분기 국가 활동에서 가장 널리 사용된 MITRE ATT&CK 기술

1.	LDLL 사이드 로딩	14%
2.	정보용 파일 난독화/디코드	11%
3.	인그레스 도구 전송	10%
4.	로컬 시스템 데이터	10%
5.	파일 및 디렉터리 검색	10%

2023년 1분기 국가 활동에서 가장 널리 사용된 악성 도구

38%

PlugX는 2023년 1분기 악성 국가 활동의 38%를 차지했습니다.

1.	PlugX	38%
2.	Cobalt Strike	35%
3.	Raspberry Robin	14%
4.	BLUEHAZE/DARKDEW MISTCLOAK	3%
5.	Mimikatz	3%

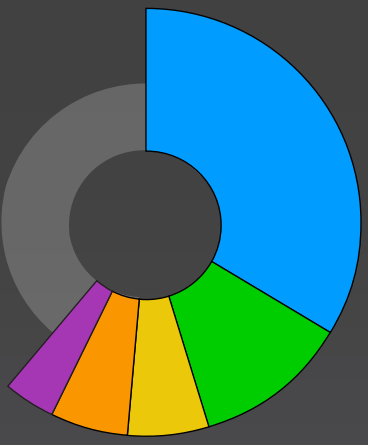
인도는 유능한 사이버 프로그램을 보유한 아시아 및 인접 지역의 주요 국가 중 하나입니다. 주로 중국과 연계된 위협 행위자로 구성된 일부 그룹은 인도의 기술, 군사 및 정치 발전에 큰 관심을 보였습니다. 인도에서 주목할 만한 수의 탐지는 Mustang Panda 때문일 수 있습니다.

2023년 1분기 국가 활동이 가장 많이 탐지된 국가

34%

필리핀은 2023년 1분기에 국가 활동이 가장 많이 탐지된 국가 1위를 차지했습니다.

- 필리핀
- 인도
- 미얀마
- 카메룬
- 미국



2023년 1분기 국가 활동이 가장 많이 감지된 섹터

취약성 인텔리전스

Trellix Advanced Research Center의 리버스 엔지니어링 및 취약성 분석 전문가는 최신 취약성을 지속적으로 모니터링하여 위협 행위자가 이를 활용하는 방법과 이러한 공격의 가능성 및 영향을 완화하는 방법에 대한 지침을 고객에게 제공합니다.

2023년 1분기의 가장 중요하지만 놀랍지 않은 발견 중 하나는 이 기간의 가장 중요한 취약성 중 다수가 이전 CVE용 패치에 대한 바이패스, 오래된 라이브러리의 사용으로 인해 발생하는 공급망 버그, 또는 예상 명성 5분이 훨씬 지난 후에도 지속되는 장기 패치 취약성 등으로 구성되었다는 것입니다.

예를 들어 올해 1월에 등장한 Zoho의 ManageEngine 제품의 치명적인(9.8) 취약성인 CVE-2022-47966을 생각해 보십시오. ManageEngine은 전 세계 수천 개의 회사에서 사용되고 있으므로 이 취약성의 악용이 실제로 탐지되었을 때 우리는 놀라지 않았습니다. 우리를 놀라게 한 것은 근본적인 원인, 바로 오래된 버전인 Apache Santuario 1.4.1의 활용이었습니다. 이 버전에는 알려진 문제가 포함되어

있어 XML 주입을 허용하고 있었습니다. Zoho는 10월에 제품군 전반에 걸쳐 취약성을 패치했고, 거의 3개월 후인 1분기에 CISA는 실제 악용에 대한 주의 경고를 발표하고 공급업체에 패치를 촉구했습니다.

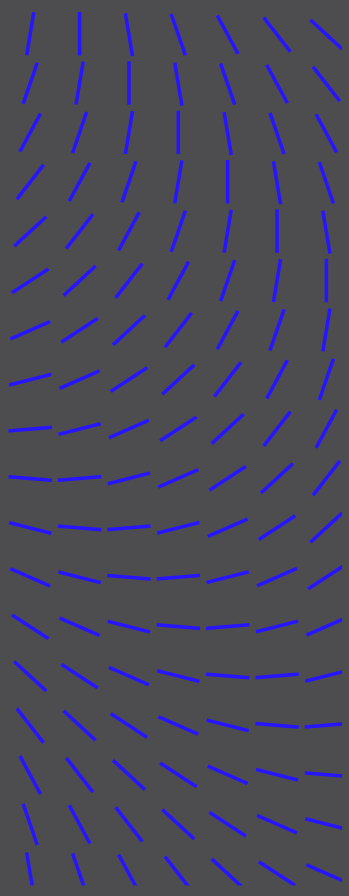
또 다른 예는 CWP(제어 웹 패널)의 치명적인 취약성인 CVE-2022-44877입니다. 이 취약성은 직접적으로 관련되지는 않았지만 이전 예시와 동일한 특성을 많이 가지고 있습니다. 이는 10월에 다시 패치되었음에도 불구하고 1월에 활발하게 악용된 또 다른 9.8 RCE입니다. 근본 원인은 URL 매개변수에서 표준 셸 변수 확장을 사용하는 명령 주입으로 Black Hat에서 논의할 주제는 아니었습니다.

세 번째 예는 2021년 2월에 해결된 VMware ESXi의 OpenSLP 서비스 취약성인 CVE-2021-21974로, 거의 정확히 2년 후에 실제 악용으로 인해 갑작스럽게 다시 등장했습니다. Shodan에 따르면 우리가 2월 버그 보고서에서 이 취약성에 대해 보고했을 때 약 48,000개의 인터넷 연결 가능 서버가 여전히 취약한 버전의 ESXi를 실행하고 있었습니다. 오늘날 그 수치는 여전히 38,000개 이상으로 22% 미만의 변화를 나타냅니다.

날짜	Shodan에 따른 취약한 ESXi 서버 수
2023년 2월 말	48,471
2023년 4월 말	38,047

올해 초 Apple 장치를 조사했을 때 다음과 같은 몇 가지 예를 발견했습니다. CVE-2023-23530 및 CVE-2023-23531의 두 가지 취약성은 이들의 영향이 RCE가 아닌 로컬 권한 상승으로 제한된다는 점에서 이전 예와는 다릅니다. 그러나 2021년 NSO Group이 Pegasus 스파이웨어를 배포하는 데 사용한 FORCEDENTRY 익스플로잇에 의해 매우 유사한 취약성이 악용되었기 때문에 그 중요성을 간과할 이유는 없습니다. 사실 우리가 발견한 두 CVE는 FORCEDENTRY 익스플로잇의 기반이 되는 것과 동일한 프리미티브인 NSPredicate라는 무해한 클래스를 사용합니다. 안타깝게도 FORCEDENTRY를 완화하기 위한 Apple의 접근 방식에는 광범위한 거부 목록을 사용하는 것이 포함되었으며 이는 NSPredicate가 남용되는 방식을 강화했습니다. 이러한 완화는 우리로 하여금 근본적인 문제를 해결하지 못하고 겉돌게 했습니다.

이와 같은 동향을 지적하고 공급업체가 보안을 심각하게 생각하지 않는다고 결론을 내리거나 위협 행위자 및 연구원에 의한 오래된 익스플로잇의 반복을 한탄하고 싶지만 이는 올바른 교훈이 아닙니다. 취약성 연구원은 변종 분석에 참여합니다. 실질적인 취약성 연구원은 실제 위협 행위자의 우선순위를 에뮬레이션하고, 거의 패치되지 않은 제품에서 완화 바이패스 또는 이전 CVE를 찾는 것이 쓸데없이 시간을 낭비하는 것보다 지속적으로 더 나은 ROI를 생성하기 때문입니다. 이러한 동향을 올바르게 인식하는 조직의 경우 다음과 같은 교훈을 얻어야 합니다. 최신 위협 탐지 기술은 현대 위협 환경에서 대체할 수 없지만 패치 프로세스 및 공급망 조사와 같은 기본 요소에서 많은 승리를 거둘 수 있습니다.



이메일 보안

이메일 보안 통계는 전 세계 고객 네트워크에 배포된 여러 이메일 보안 어플라이언스에서 생성된 원격 측정을 기반으로 합니다.

합법적인 브랜드를 활용하여 사용자를 속이고 자격 증명을 도용하는 피싱 공격이 증가하고 있으며 DWeb, IPFS 및 Google 번역이 이메일 공격에 많이 사용되고 있습니다. 공격자들은 또한 무료 메일과 두 가지 애플리케이션(PayPal Invoicing 및 Google Forms)과 같은 유사한 서비스를 남용하여 보이스피싱 공격을 수행하고 탐지를 피했습니다. 이 기간 동안 비슷하게 표적이 된 것은 Scribd, Les Mills 및 Google Play 기프트 카드와 같은 새로운 브랜드였습니다.

또한 이러한 공격에 사용된 특정 맬웨어에 있어 Formbook과 Agent Tesla는 작년 말에 비해 2023년 1분기에 눈에 띄게 증가했습니다. 이는 Remcos, Emotet 및 Qakbot에 비해 두 맬웨어가 더 쉽게 획득 및 배포할 수 있기 때문일 수 있습니다.

2023년 1분기 가장 널리 퍼진 이메일 맬웨어 전술

44%

Formbook은 1분기 이메일 맬웨어의 거의 절반을 차지했으며 Agent Tesla가 그 뒤를 바짝 뒤따랐습니다.

2023년 1분기 이메일 피싱의 가장 많은 표적이 된 국가

30%

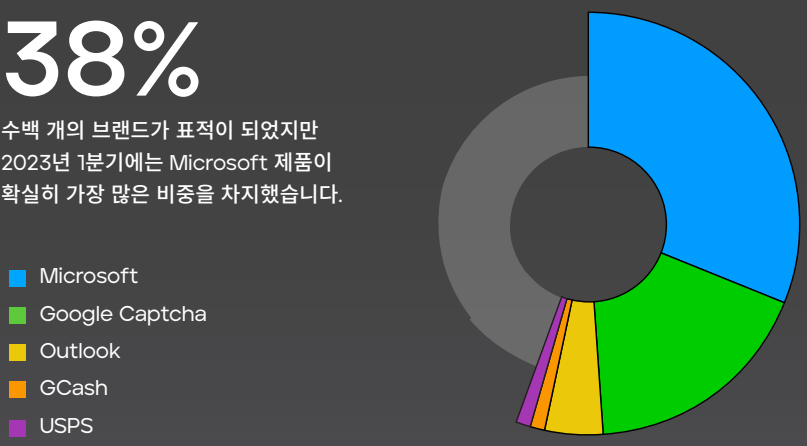
미국과 대한민국은 1분기 이메일 피싱 시도의 주요 피해자였으며 전 세계 전체 피싱 시도의 거의 3분의 2가 집중되었습니다.

1.	미국	30%
2.	대한민국	29%
3.	대만	10%
4.	브라질	8%
5.	일본	7%

2023년 1분기 이메일 피싱의 가장 많은 표적이 된 제품 및 브랜드

38%

수백 개의 브랜드가 표적이 되었지만 2023년 1분기에는 Microsoft 제품이 확실히 가장 많은 비중을 차지했습니다.



2023년 1분기 악성 이메일의 영향을 가장 많이 받은 섹터

1.	정부	11%
2.	금융 서비스	8%
3.	제조	6%
4.	기술	6%
5.	엔터테인먼트	5%

2023년 1분기 가장 많이 남용된 웹 호스팅 제공업체

1.	IPFS	41%
2.	Google Translate	33%
3.	Dweb	16%
4.	AmazonAWS Appforest	3%
5.	Firebase OWA	3%

2023년 1분기 피싱 공격에 가장 많이 사용된 우회 공격 기술

79%

302 리디렉션 기반 우회는 2023년 1분기 피싱 공격에 사용된 가장 일반적인 우회 기술이었습니다.

46%

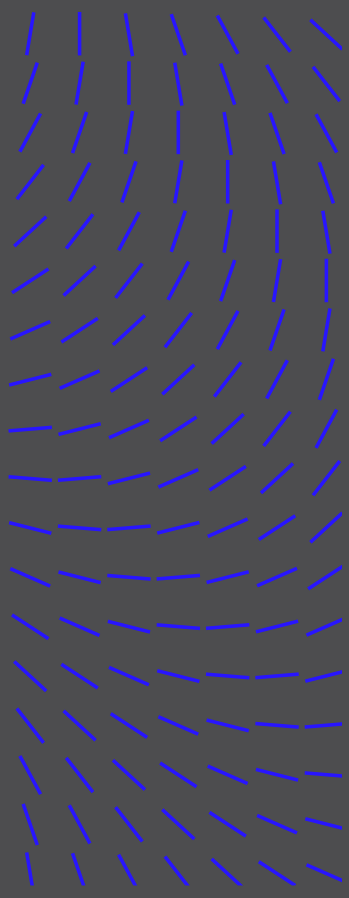
Captcha 기반 공격은 2022년 4분기에 비해 1분기에 크게 증가했습니다.

네트워크 보안

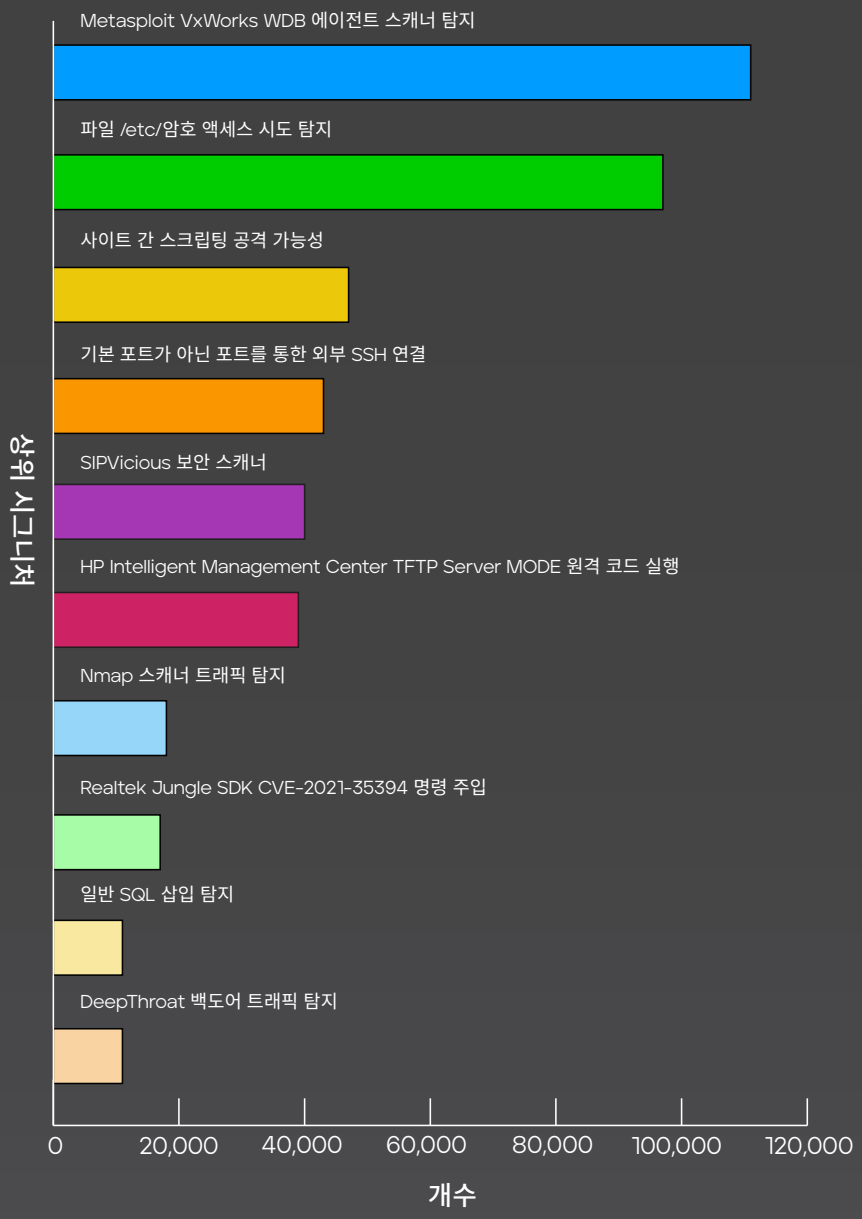
고객을 위협하는 네트워크 기반 공격을 탐지하고 차단하는 과정에서 Trellix Advanced Research Center의 네트워크 연구팀은 정찰 및 초기 침해에서 C2 통신 및 내부 확산 TTP에 이르기까지 킬 체인의 다양한 영역을 검사합니다.

2023년 1분기 가장 주목할 만한 맬웨어 콜백 동향

랜섬웨어 Stop 활동 거부됨	94%
Amadey가 배포한 LockBit 랜섬웨어 증가율	25%
Android 맬웨어 활동 증가율	12.5%
Ursnif 활동 증가율	10%
Smoke Loader 활동 증가	7X
Amadey 활동 증가	4X
Cobalt Strike 활동 증가	3X
Emotet 활동 증가	2X



2023년 1분기 외부 서비스에 대한 가장 영향력 있는 공격



클라우드 인시던트

Amazon, Microsoft, Google 등에서 개발하고 제공하는 서비스에 대한 클라우드 인프라 공격이 계속 증가하고 있습니다. 아래 표는 고객 및 클라우드 공급자별 클라우드 기반 공격 텔레메트리 데이터를 설명합니다.

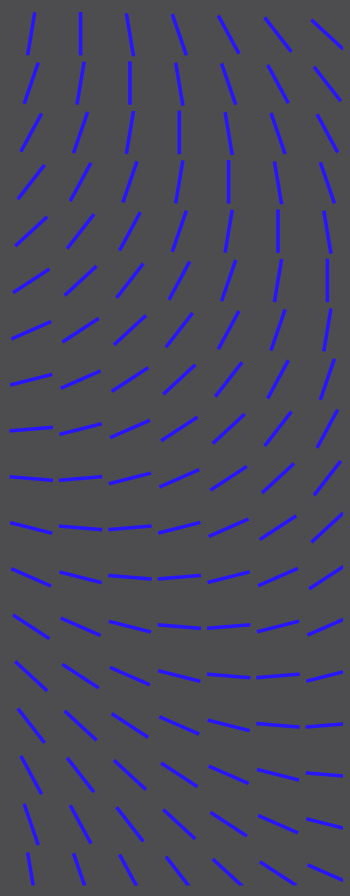
2023년 1분기 MITRE ATT&CK 기술에 의한 탐지

	AWS	Microsoft Azure	GCP
유효한 계정	3,437	4,312	997
클라우드 컴퓨팅 인프라 수정	4,268	0	17
비 표준 포트	115	0	17
다단계 인증	190	1,534	22
네트워크 서비스 검색	141	93	0
무차별 대입	25	1,869	22
프록시	299	2,744	135
계정 검색	264	68	787
이메일 전달 규칙	25	0	22
API를 통한 실행	1,143	0	252

방법론

수집: Trellix와 Advanced Research Center의 노련한 세계적 수준의 전문가들은 광범위한 글로벌 소스에서 이 보고서를 구성하는 통계, 동향 및 인사이트를 수집합니다.

- **전속 소스:** 경우에 따라 원격 측정은 기술, 인프라 또는 데이터 서비스를 제공하는 네트워크를 포함하여 전 세계 공공 및 민간 섹터 네트워크에 배포된 고객 사이버 보안 네트워크 및 방어 프레임워크의 Trellix 보안 솔루션에 의해 생성됩니다. 수백만 개에 달하는 이러한 시스템은 10억 개의 센서로부터 데이터를 생성합니다.
- **오픈 소스:** 다른 경우에 Trellix는 특허받은 독점 오픈 소스 도구의 조합을 활용하여 인터넷에서 사이트, 로그 및 데이터 리포지토리뿐만 아니라 악성 행위자가 랜섬웨어 피해자에 대한 정보나 피해자의 정보를 게시하는 "유출 사이트"와 같은 다크웹을 스크랩합니다.



정규화: 집계된 데이터는 Insights 및 ATLAS 플랫폼에 제공됩니다. 팀은 머신 러닝, 자동화 및 인간의 민첩성을 활용하여 데이터를 정규화하고, 결과를 풍부하게 하고, 개인 정보를 제거하며, 공격 방법, 에이전트, 섹터, 지역, 전략 및 결과 간의 상관관계를 식별하는 집중적이고 통합적이며 반복적인 일련의 프로세스를 순환합니다.

분석: 다음으로 Trellix는 (1) 광범위한 위협 인텔리전스 기술 자료, (2) 높이 평가되고 공인된 출처의 사이버 보안 산업 보고서, (3) Trellix 사이버 보안 분석가, 조사자, 리버스 엔지니어링 전문가, 법의학 연구원 및 취약성 전문가의 경험과 인사이트를 참조하여 이 방대한 정보 저장소를 분석합니다.

해석: 마지막으로 Trellix 팀은 사이버 보안 리더와 보안 운영 팀이 (1) 사이버 위협 환경의 최신 동향을 이해하고 (2) 이 관점을 사용하여 미래의 사이버 공격을 예측, 방지 및 방어하는 능력을 향상시키는 데 도움이 되는 의미 있는 인사이트를 추출, 검토 및 검증합니다.

리소스

위협 보고서 보관

The Mind of the CISO

Trellix Advanced Research Center Discovers a New Privilege Escalation Bug Class on macOS and iOS

A Royal Analysis of Royal Ransom

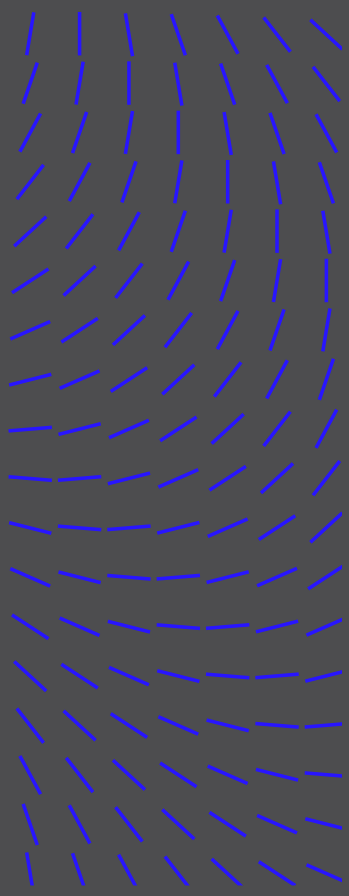
Feeding Gophers to Ghidra

TWITTER

Trellix ARC

이전의 사이버 위협 보고서 보기

Trellix Advance Research Center

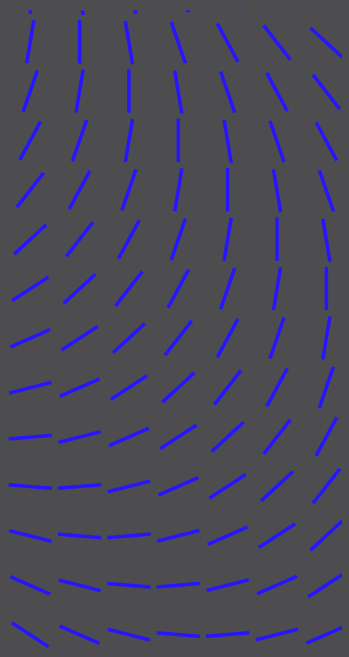


TRELLIX ADVANCED RESEARCH CENTER 정보

사이버 보안 업계의 가장 포괄적인 헌장인 Trellix Advanced Research Center는 글로벌 위협 환경에서 새롭게 부상하는 방법, 동향 및 행위자의 최전선에 있으며 전 세계 보안 운영 팀의 최고의 파트너 역할을 수행하고 있습니다. The Trellix Advanced Research Center는 보안 분석가에게 인텔리전스와 최신 콘텐츠를 제공하는 동시에 최고의 XDR 플랫폼을 지원합니다. 또한 Trellix Advanced Research Center의 위협 인텔리전스 그룹은 전 세계 고객에게 인텔리전스 제품 및 서비스를 제공합니다.

TRELLIX 소개

Trellix는 사이버 보안과 세상을 바꾸는 기술의 미래를 혁신하는 글로벌 기업입니다. 오늘날 최첨단 위협에 직면한 조직은 Trellix가 보유한 개방형 XDR(확장된 탐지 및 대응) 플랫폼을 통해 확실히 운영을 보호하고 복원할 수 있습니다. Trellix는 광범위한 파트너 에코시스템과 함께 머신 러닝 및 자동화를 통한 기술 혁신을 가속하여 40,000개 이상의 기업 및 정부 고객에게 생활 보안을 제공합니다.



자세한 내용을 알아보려면 Trellix.com을 방문하십시오.

Trellix

Trellix 소개

Trellix는 사이버 보안의 미래를 혁신하는 글로벌 기업입니다. 오늘날 최첨단 위협에 직면한 조직은 Trellix가 보유한 개방형 XDR(확장된 탐지 및 대응) 플랫폼을 통해 확실히 운영을 보호하고 복원할 수 있습니다. Trellix의 보안 전문가는 광범위한 파트너 에코시스템과 더불어 머신 러닝 및 자동화를 통해 기술 혁신을 가속함으로써 40,000곳 이상의 기업 및 정부 고객을 지원하고 있습니다.

072022-05-KO