사이버 위협 보고서

2024년 6월

전문가, 센서, 텔레메트리 및 인텔리전스의 글로벌 네트워크로부터 얻은 인사이트

보고서 내용:

APT 환경의 빠르고 중대한 변화

랜섬웨어 에코시스템을 뒤흔드는 LockBit

확장하는 공격자 도구 상자

제공:

Trellix ADVANCED RESEARCH CENTER

방금 업계 내 다른 조직에서 EDR 회피 도구를 사용하여 엔드포인트 탐지 및 대응 기능을 차단하는 데 성공했습니다.

공격자에 앞서서 그들이 합법적인 보안 도구를 악의적으로 이용하는 것을 차단하기 위한 사이버 보안 경쟁이 점점 더 복잡해지고 있습니다.

CISO는 민첩성, 속도, 자신감, 통제력을 가지고 움직여야 합니다. CEO와 이사회는 로깅 및 경고 도구에 대해 자세히 알고 싶어 합니다. 팀에게 부족한 부분을 파악하도록 작업을 지시하고, 이를 해결하기 위한 계획을 수립합니다.

사이버 보안 경쟁은 철인 3종 경기와 같습니다. 보안 운영, 기술, 인텔리전스의 세 부분에서 경쟁합니다. 경쟁은 일단 시작되면 인내의 게임입니다.

> 방어 메커니즘이 더욱 정교해짐에 따라 국가 및 사이버 범죄자들이 사용하는 공격 도구 및 전술도 더욱 정교해졌습니다.

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 주로 2023년 10월 1일부터 2024년 3월 31일 사이에 수집된 데이터 및 인사이트에 중점을 둡니다.

1. APT 환경의 빠르고 중대한 변화
2. 랜섬웨어 에코시스템을 뒤흔드는 LockBit
3. EDR 킬러 등장
4. 미국 대통령 선거 테마 사기
5. GenAI 및 사이버 범죄 지하 조직

머리말

운영 위협 인텔리전스와 글로벌 위협에 운영 환경에 대한 상황별 맥락을 추가할 수 있는 능력이 CISO의 역할에서 그 어느 때보다 중요해졌습니다.

더 적은 리소스로 더 많은 작업을 수행해야 하는 상황에서 CISO와 보안 운영 팀은 위협을 예측하고, 조직을 대상으로 하는 가장 관련 있는 위협을 식별하고 대비하며, 가장 가능성이 높은 위협 및 행위자에 맞춰서 프로그램과 예산을 준비하고, 사후 대응에서 사전 예방적 태세로 전환하기 위해 위협 인텔리전스가 필요합니다.

Trellix의 "고객 제로(Customer Zero)" 프로그램에서 인텔리전스가 응답자를 움직이고 전략화하는 길을 터줄 가능성이 이보다 더 컸던 것을 본 적이 없습니다.

이 콘텐츠를 요약하고 완벽히 이해하여 전략적 계획 수립, 예산 합리화, 이사회 교육 및 운영 지원에 활용하시기 바랍니다. 이 인사이트가 교육적이고 유익한 정보로 활용되고, APT에 대해 계획하고, 준비하고, 지속하는 방법을 더 잘 안내하고 영향을 미치는 데 디딤돌 역할을 하기를 바랍니다.

Harold Rivas
CISO, TRELLIX

목차

서문

이 보고서를 비롯한 모든 보고서에서는 우리가 관찰하고 있는 내용에 대한 구체적인 인텔리전스와 맥락을 제공하는 데 목표를 두고 있습니다.

환경

지난 6개월 동안은 전례 없는 복합 위기 상황이 지속되고 전 세계적으로 사이버 범죄 및 위협 행위자의 활동이 가속화되었습니다. 우리는 다음과 같은 급격한 행동 변화를 목격하고 있습니다.

- 랜섬웨어 에코시스템은 전형적인 후속 법 집행 조치입니다,
- 자치 단체들이 침투 테스트 및 대체 공격 방법 관련 제품을 랜섬웨어 범죄 조직에 판매하고 있습니다,
- 이스라엘의 전쟁은 국가가 후원하는 직접 공격과 핵티비즘을 촉발시켰습니다.
- 위협 행위자들은 더욱 정교해지기를 원하고 있으며, 하룻밤 사이에 전문가가 될 수 있도록 해주는 저렴하거나 무료 GenAI 기반 도구에 액세스할 수 있습니다.
- EDR 회피 및 종료 도구는 위협 행위자에게 더욱 중요해졌습니다.

쫓고 쫓기는 게임

엔드포인트 탐지 및 대응(EDR) 솔루션을 대규모로 구현하면서 쫓고 쫓기는 사이버 보안 게임이 더욱 복잡해지는 것을 목격하고 있습니다. 범죄 도구를 사용하여 EDR을 무력화하는 위협 행위자가 증가함에 따라 우리의 관심이 증가하고 기존 맬웨어 기반 도구 사용에서 급격하게 변화하고 있습니다.

방어자도 역시 방향을 바꿔야 합니다. EDR은 맬웨어, 랜섬웨어 및 APT 그룹 활동을 탐지하는 데 효과적인 것으로 입증되었지만, EDR이 오프라인으로 전환될 경우 조직과 CISO는 어떻게 해야 합니까? 시스템에서 비정상적인 행동을 놓치지 않으려면 로깅, 경고, 운영 위협 인텔리전스가 필요합니다. 새로운 게임 플레이의 장이 마련됩니다.

우리는 악의적 사용자에 앞서기 위한 핵심 가치인 위협 인텔리전스를 커뮤니티와 공유하고 캠페인 및 위협 그룹을 대규모로 추적하기 위해 성실하게 노력하고 있습니다.

환경이 그 어느 때보다 많이 변화하고 있습니다. 저희는 방어를 강화하고, 대책을 수립하고, 부족한 부분을 파악하는 데 필요한 인텔리전스를 통해 고객과 산업 전반을 지원하는 데 목표를 두고 있습니다.

이 쫓고 쫓기는 게임에서 우리는 이기는 게임을 해야 합니다.

John Fokker
위협 인텔리전스 책임자, TRELLIX

목차

소개: 사이버 위협 보고서: 2024년 6월

사이버 도메인에 영향을 주는 지정학적 사건

Trellix Advanced Research Center에서 2023년 10월 1일부터 2024년 3월 31일 사이의 활동을 조사한 결과 지정학적 동기에 따른 사이버 위협 활동이 눈에 띄게 증가하는 등 위협 활동의 변화가 확인되었습니다. 군사 훈련, 정치 또는 경제 정상 회담, 정치 대회, 선거 등과 같은 지역과 전 세계의 주요 사건들이 사이버 위협 활동을 주도했습니다.

Trellix 분석가들은 위협 행위자가 이러한 이벤트를 중심으로 상대에 대한 관련 인텔리전스를 수집하거나, 네트워크를 선제적으로 조사하여 상황 인식을 위한 정보를 얻거나, 향후 공격을 위해 IT 네트워크를 전략적으로 전개하고 있다고 중간 신뢰 수준에서 평가합니다.

- **바이든 대통령과 시진핑 주석의 샌프란시스코 회동:** 2023년 11월 Trellix 텔레메트리 탐지 데이터에 따르면 APEC(아시아태평양경제협력체) 회의의 일환으로 바이든 미국 대통령과 시진핑 중국 주석의 회동을 불과 며칠 앞두고 중국 관련 APT 행위자 그룹의 악성 활동이 약간 증가한 것으로 나타났습니다. 바이든 시진핑 회동 이후 APEC 정상 회담 기간 동안 위협 활동 수가 크게 감소했습니다.

  APEC 정상 회담이 종료되면서 위협 활동 수준이 2023년 11월 한 달 동안 최저 수준으로 감소했습니다. 중국 관련 위협 행위자 그룹의 이러한 위협 활동 패턴은 중국의 국가 후원 위협 행위자 그룹이 APEC과 같은 지정학적 사건의 영향을 많이 받았다는 것을 의미합니다. 또한 중국의 APT 그룹이 자국의 대외 이미지와 국제적 평판을 유지하기 위해 주요 정치 행사 기간 중에 해킹 활동을 의도적으로 중단했을 가능성이 있다는 것을 나타냅니다.
- **이스라엘-하마스 전쟁:** 이란과 연계된 APT 위협 행위자 그룹의 위협도 이스라엘-하마스 전쟁을 둘러싼 정치적 상황에 따라 주도되었습니다. 미국에서 Trellix 글로벌 텔레메트리 데이터에 따르면 지난 6개월 동안 (2023년 11월 및 12월 제외) 이란과 연계된 APT 위협 행위자 그룹의 악성 활동이 주기적으로 급증했음을 보여줍니다. 특히, 글로벌 텔레메트리에 따르면 이란이 하마스를 공개적으로 지지하는 상황에서 미국이 가자 지구에서 인도주의적 휴전을 추진했던 2023년 11월 말과 2023년 12월 이스라엘 인질 교환 및 정전 합의 기간 동안 미국 조직을 대상으로 하는 이란과 연계된 APT 그룹의 위협 활동이 감소한 것으로 나타났습니다. 또한 Trellix 글로벌 텔레메트리에 따르면 이란과 연계된 APT 위협 행위자 그룹은 이 보고 기간 동안 이스라엘 조직을 대상으로 피싱, 정보 탈취, 백도어, 다운로더, 악성 웹 셸, 일반적으로 악용되는 취약점 등 다양한 TTP를 사용했습니다.

목차

- **군사 훈련:** 또한 전투 준비를 강화하기 위한 다국적 군사 훈련이 악성 활동을 증가시킬 수 있습니다. 가장 최근에 발표된 2024년 3월 Trellix 글로벌 텔레메트리 데이터에 따르면 2024년 3월 4일부터 3월 14일까지 진행된 대규모 한미 합동 군사 훈련인 자유의 방패(Freedom Shield) 기간 동안 한국 내 위협 활동이 반복적으로 급증한 것으로 나타났습니다. 이 군사 훈련은 "한국형 작전 구역"을 운영하고 북한의 진화하는 핵 위협에 대응하기 위해 고안되었습니다. 특히, 한국 내 위협 탐지 횟수가 2024년 3월 7일과 3월 13일에 각각 150,000건을 초과했으며, 이는 평소 한국의 일일 탐지 건수인 20,000회의 약 7배에 해당하는 수치입니다.
- **러시아-우크라이나 전쟁:** 이 지역에서 지속되는 역동적인 전투에서는 크고 작은 사이버 이니셔티브가 수반되었습니다. 특히 러시아와 연계된 행위자들이 새롭고 진화한 와이퍼 맬웨어를 통해 우크라이나 통신사 Kyivstar를 공격하여 수천 대의 가상 서버와 PC를 파괴한 것으로 확인되었습니다. Kyivstar 공격은 2022년에 러시아가 우크라이나를 침공한 이후 우크라이나에서 자행된 가장 영향력이 컸던 사이버 공격 중 하나입니다.

한눈에 보는 요약

이 보고서는 비즈니스 전반의 연구를 위한 리포지토리 역할을 하지만 주요 주제는 변하지 않습니다.

1. **APT 환경의 빠르고 중대한 변화**
    a. **러시아와 연계된 Sandworm 증가:** 지정학적 긴장이 고조됨에 따라 전체 에코시스템에서 APT 활동도 증가합니다. APT 위협이 전반적으로 증가하는 동안, 이 보고서에서 관찰된 기간 동안 러시아와 연계된 Sandworm 팀이 40% 더 많이 탐지되었습니다.
    b. **여전히 위협 활동이 빈번한 중국:** Trellix는 중국과 연계된 위협 행위자 그룹으로부터 2,100만 건 이상의 위협 활동을 탐지하여 중국과 연계된 위협 그룹은 여전히 가장 왕성하게 활동하는 APT 활동 행위자입니다. 탐지된 악성 활동의 23% 이상이 전 세계 정부 부문을 대상으로 합니다.
    c. **Volt Typhoon 활동 급증:** 상대적으로 새로운 중국의 국가 후원 APT 그룹인 Volt Typhoon은 독특한 행동 패턴과 대상 지정 관행으로 인해 눈에 띕니다. 2024년 1월 중순 이후, Trellix 텔레메트리를 통해 Volt Typhoon과 관련한 7,100건 이상의 악성 활동을 탐지했으며, 2024년 1월부터 3월까지 주기적으로 급증했습니다.

목차

2. **랜섬웨어 에코시스템을 뒤흔드는 LockBit**
    a. **범죄 조직의 평판에 영향을 주는 사기꾼들:** 글로벌 법 집행 조치인 Operation Cronos에 이어 Trellix는 LockBit를 사칭하는 사기꾼들을 관찰했으며 이들 집단은 체면을 세우고 수익성이 좋은 작전을 복원하려고 필사적으로 노력했습니다.
    b. **여전히 가장 많은 표적이 되는 미국:** 미국은 랜섬웨어 그룹의 가장 많은 표적이 되고 있으며, 튀르키예, 홍콩, 인도, 브라질이 그 뒤를 이었습니다.
    c. **가장 표적이 되는 운송 및 해운:** 랜섬웨어 행위자들은 2023년 4분기와 2024년 1분기에 운송 및 해운 부문을 가장 많이 위협했습니다. 이 부문은 글로벌 랜섬웨어 탐지 건수의 53% 및 45%를 차지했으며 금융 산업이 그 뒤를 이었습니다.
    d. **선고로 이어지는 법 집행 조치:** 이 보고서를 마무리하기 전에 글로벌 법 집행 기관에서는 LockBit 주모자의 실제 정체를 공개했습니다. 랜섬웨어 범죄자에 대한 추가 조치가 5월 1일에 이루어졌습니다. Kaseya와 다른 여러 조직을 공격한 REvil 계열사는 13년 징역형과 미화 1,600달러 배상금을 선고받았습니다.
3. **EDR 킬러 등장**
    a. **D0nut 랜섬웨어 범죄 조직 등장:** D0nut 랜섬웨어 범죄 조직의 등장은 EDR 킬러 도구를 혁신적으로 활용하여 엔드포인트 탐지를 우회하고 공격 효율을 개선하는 진화한 전술을 보여주었다는 점에서 특히 주목할 만했습니다.
    b. **통신사를 공격하는 데 사용되는 Spyboy의 EDR 회피 도구:** Spyboy가 개발한 "Terminator"라는 EDR "킬러" 도구가 2024년 1월에 새로운 캠페인에 사용되었습니다. 이 도구는 EDR 솔루션을 우회하는 데 사용되며, 탐지 건수의 80%가 통신 부문을 대상으로 했습니다.
4. **미국 대통령 선거 테마 사기**
    a. **아직 기승을 부리는 피싱:** 전 세계가 11월에 있을 미국 대선 결과를 주시하고 있는 가운데, 선거 이미지를 활용하고 기부금을 확보하기 위해 선별된 사기가 관찰되었습니다.

목차

5. **GenAI 및 사이버 범죄 지하 조직**

   a. **무료 AI 기반 도구:** Trellix는 사이버 범죄 지하 조직에서 사용할 수 있는 무료 ChatGPT 4.0 Jabber 도구를 목격했으며, 이 도구를 통해 개발자는 위협 행위자가 불법 행위에 GenAI를 채택하고 다른 사이버 범죄자로부터 배우거나 그들의 아이디어와 도구를 훔치는 GenAI 기술 자료를 만들도록 지원합니다.

   b. **정보 탈취 프로그램 채택 증가:** GenAI 기반 기능을 갖춘 두 개의 정보 탈취 프로그램이 사이버 범죄자들에 의해 사용되는 것이 관찰되었습니다. MetaStealer와 LummaStealer는 GenAI를 탑재하여 각각 탐지를 우회하고 로그 목록에서 봇을 탐지합니다. GenAI 기능은 이러한 범죄 전략을 찾아서 차단하는 것을 더 어렵게 만듭니다.

방법론: 데이터 수집 및 분석 방법

Trellix Advanced Research Center의 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.

목차

보고서 분석, 인사이트 및 데이터

국가 및 APT(지능형 지속 공격)

2023년 10월부터 2024년 3월까지 Trellix는 APT 기반 탐지가 이전 6개월에 비해 17% 증가한 것을 목격했습니다. 놀랍게도 이전 보고서에서는 이러한 탐지 건수가 무려 50% 증가한 것으로 확인되었습니다. APT 에코시스템은 1년 전과 근본적으로 달라져서 더 공격적이고, 교묘하며, 능동적입니다.

빠르게 진화하는 사이버 위협 환경에서 APT(지능형 지속 공격) 그룹은 전 세계 사이버 보안에 중요하고 정교한 과제를 계속해서 제기하고 있습니다.

저희의 목표는 2023년 4분기부터 2024년 1분기까지 탐지된 APT(지능형 지속 공격) 관련 활동을 철저히 분석하는 것입니다. 이 분석은 이러한 위협의 기원, 주요 대상, 운영에 사용되는 도구에 초점을 맞춥니다. 이 결과를 두 핵심 메트릭인 백분율 편차와 비례 기여 편차를 사용하여 2023년 상반기(2분기~3분기) 데이터와 비교합니다.

- 백분율 편차: 이 메트릭은 특정 APT 그룹의 활동, 특정 국가의 대상 지정 또는 특정 도구 사용이 시간에 따라 증가 또는 감소했는지 동일하게 유지되었는지를 확인하는 데 도움이 됩니다. 이 메트릭을 이해하면 이 위협 행위자의 행동이 어떻게 변화되고 전체 사이버 위협 환경이 어떻게 진화하고 있는지를 추적하는 데 도움이 됩니다.
- 비례 기여 편차: 이 메트릭은 활동의 원시적인 변화를 보여주는 동시에 이러한 변화가 전체 사이버 보안 위협 환경을 배경으로 어떻게 대응하는지를 보여줌으로써 맥락을 더해 줍니다. 예를 들어 특정 행위자에 대한 탐지가 크게 증가했더라도 전체 위협 환경이 훨씬 더 바쁘게 움직인다면 이는 전체 사이버 위협의 일부에 불과합니다. 반대로 탐지는 줄었지만 나머지 위협 환경이 더 느려졌다면 이 행위자가 상대적으로 더 중요해졌을 수 있습니다.

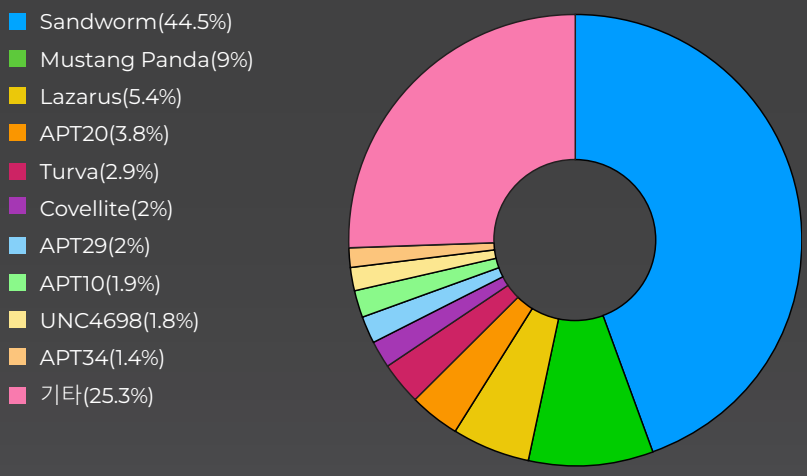
이러한 메트릭을 채택하여 APT 활동 변화의 미묘한 느낌을 이해하고, 전략적 목표, 선호하는 방법론, 제기되는 사이버 보안 과제에 대한 인사이트를 도출하는 데 목표를 두고 있습니다. 다음 섹션에서는 이러한 결과를 살펴보고, 복잡한 APT 환경과 정교한 위협으로부터 보호하기 위해 필요한 지속적인 노력을 조명합니다.

목차

활동적인 국가 및 APT 그룹

또한 2023년 10월부터 2024년 3월까지 다양한 APT 그룹의 활동에 상당한 변화가 목격되었습니다. 이러한 변화는 사이버 위협의 동적 특성뿐만 아니라 정교한 행위자가 사용하는 운영 초점 및 기술의 변화도 강조합니다.

2023년 4분기와 2024년 1분기 사이의 탐지 건수별 상위 10개 APT



사이버 위협 그룹 활동 변경: 편차 및 비례 기여

지능형 지속 공격	백분율 편차	비례 기여 편차
Sandworm	1669.43%	40.34%
Mustang Panda	-2.19%	-6.14%
Lazarus	66.87%	0.07%
APT28	18.67%	-1.49%
Turla	2.95%	-1.74%
Covellite	85.30%	0.23%
APT29	123.98%	0.53%
APT10	80.46%	0.17%
UNC4698	368.75%	1.14%
APT34	96.73%	0.23%
기타	-28.99%	-33.33%

목차

- **전술의 변화:** 역사적으로 파괴적인 사이버 운영으로 유명한 Sandworm 팀은 탐지 건수가 1669% 증가했으며, 비례 기여 편차는 40%입니다. 이 기념비적인 증가는 러시아가 연계된 그룹에서 이들의 활동이 전례 없이 증가한 것을 시사합니다.
- **공격적인 운영 확장:** 광범위한 사이버 간첩 행위 전력이 있는 APT29 그룹은 탐지 건수가 124% 증가하여 활동이 크게 증가한 것을 보여줍니다. 마찬가지로 APT34 및 Covellite 그룹도 탐지 건수가 각각 97% 및 85% 증가하여 운영 속도가 빨라졌거나 새로운 캠페인이 시작되었음을 나타냅니다.
- **항상성:** 이에 반해 Mustang Panda, Turla, APT28과 같은 그룹은 활동 수준에 최소한의 변화가 목격되었으며, 탐지 건수가 Mustang Panda는 -2%로 소폭 감소하고 Turla는 3%로 약간 증가했습니다.
- **새로운 행위자의 등장:** 주목할 만한 것은 탐지 건수가 363% 증가한 UNC4698의 등장으로 APT 환경에서 잠재적으로 중요한 새로운 그룹이 부상한 것을 알 수 있습니다.

UNC4698에 대해 무엇을 알고 있나요?

이 그룹에 대해 알려진 것은 많지 않지만 연구자들은 그들의 행동을 그룹 활동으로 인식할 수 있었으며 아직 어떻게 귀속시켜야 할지 모릅니다.

하지만 UNC4698에 대해 알려진 바에 따르면, 공격의 성격과 지역적 초점으로 보아 중국과 연관된 것으로 추정되는 후원 국가의 경제 또는 국가 안보 목표를 지원하는 데 사용될 수 있는 민감한 운영 데이터를 수집하는 산업 스파이 활동에 초점을 맞추고 있습니다.

주로 아시아의 석유 및 가스 기관을 표적으로 합니다

또한 'SNOWYDRIVE'라는 이름의 특정 맬웨어를 사용하는 것으로 알려져 있습니다.

UNC4698은 USB 플래시 드라이브를 통해 전달되는 맬웨어 사용을 중심으로 다양한 전술, 기술, 절차(TTP)를 사용합니다. 다음은 이 위협 행위자와 관련된 몇 가지 주요 TTP입니다.

- **감염된 USB 장치를 통한 초기 액세스:** 주요 감염 방법에는 호스트 시스템에 백도어를 생성하도록 설계된 악성 소프트웨어가 포함된 USB 드라이브가 있습니다.

목차

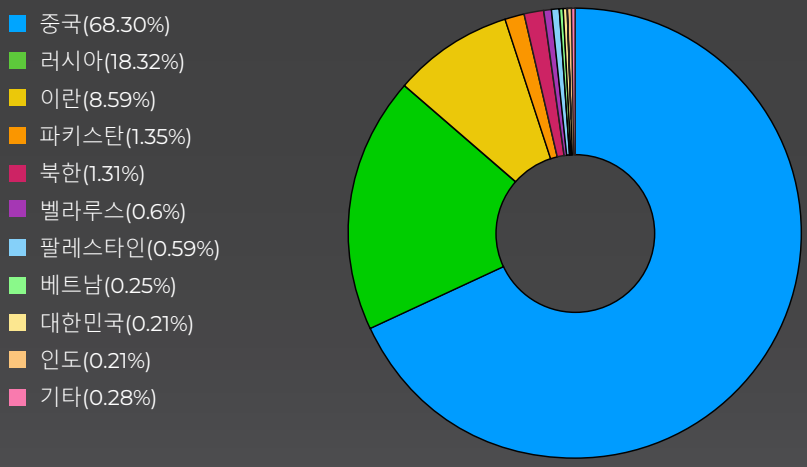
UNC4698에 대해 무엇을 알고 있나요?

- **악성 파일을 통한 실행:** 맬웨어에는 일반적으로 디스크에 악성 실행 파일 및 DLL을 기록하는 드롭퍼가 있습니다. 이러한 파일은 탐지를 피하기 위해 합법적인 소프트웨어로 위장하는 경우가 많으며, 추가적인 제어를 위해 실행됩니다.
- **지속성 및 레지스트리 수정:** UNC4698은 Windows 레지스트리를 수정하여 감염된 시스템에서 지속성을 보장합니다. 그러면 시스템이 부팅될 때마다 맬웨어가 자동으로 시작될 수 있습니다.
- **명령 및 제어(C2) 통신:** 맬웨어는 원격 통신을 위한 방법을 설정하여 공격자가 멀리서 명령을 내리고 손상된 시스템을 제어할 수 있도록 합니다.
- **이동식 미디어를 통한 내부 확산:** 이 맬웨어는 감염된 컴퓨터에 연결된 다른 USB 장치에 스스로 복사하여 다른 시스템으로 감염을 확산시킬 수 있습니다

잘 알려지지 않았거나 확인되지 않은 그룹의 탐지 건수가 62% 증가했는데, 이는 잘 알려진 APT 그룹 외에도 다양하고 증가하는 위협이 있음을 나타냅니다. 총 탐지 건수에서 차지하는 비례 기여율이 8% 증가한 것은 사이버 위협이 끊임없이 진화하고 다양화되고 있다는 것을 강조합니다.

출신 APT 그룹 및 국가

2023년 4분기와 2024년 1분기 사이의 캠페인 관련 탐지 건수별 상위 10개 APT 관련 국가



목차

출신 국가를 살펴보면 2023년 10월부터 2024년 3월까지 Trellix의 텔레메트리에서 국가가 후원하는 사이버 활동 환경에서도 눈에 띄는 변화가 관찰되었습니다.

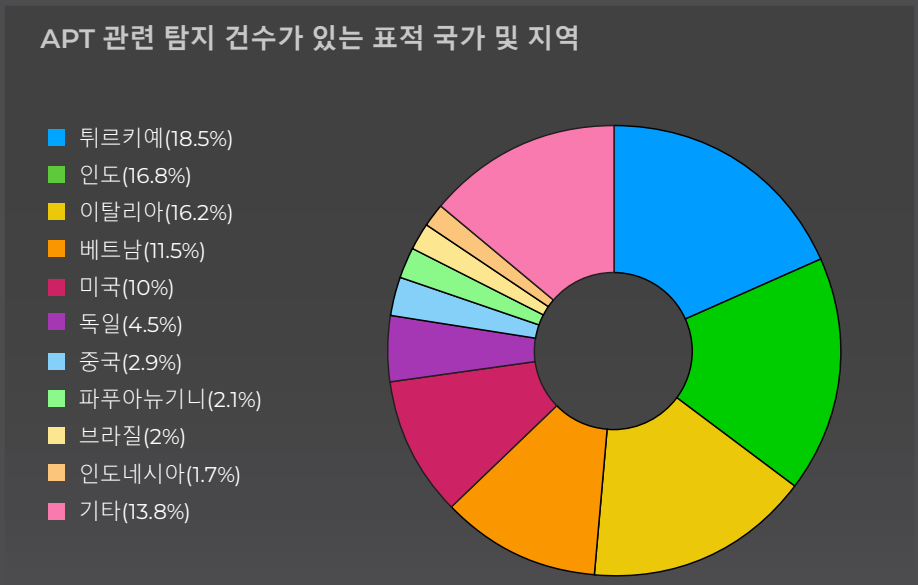
중국과 연계된 위협 그룹은 여전히 가장 왕성하게 활동하는 APT 활동 행위자입니다.

- **실질적인 운영 확대:** 지정학적 동기와 사이버 보안 역량이 여러 국가에 걸쳐 진화하고 있습니다. Trellix 텔레메트리에서 다음이 관찰되었습니다.
  a. 러시아와 연계된 위협 그룹의 APT 탐지 건수가 31%까지 크게 증가하고 비례 기여도가 4% 높아졌습니다. 이는 사이버 운영이 크게 확대된 것을 시사하며, 이는 글로벌 사이버 보안 역학에 대한 보다 광범위한 전략적 목표 또는 대응을 반영할 수 있습니다.
  b. 이란과 연계된 위협 그룹도 탐지 건수가 8% 증가하고 비례 기여도가 3.89% 증가하는 등 사이버 활동이 눈에 띄게 증가했습니다. 이는 이란의 지정학적 목적과 이스라엘-하마스 전쟁에 대한 관여에 따라 이란의 사이버 운영이 크게 확대된 것을 강조합니다.
- **폭넓은 다각화:** 중국은 APT 활동의 가장 왕성한 발원지로 남아 있으며, 탐지 건수는 1% 소폭 증가했습니다. 하지만 전체 탐지에 대한 비례 기여도는 -1% 소폭 감소했으며, 이는 이 기간 동안 APT 출처의 광범위한 다양화를 나타낼 수 있습니다. 올해 2월에는 중국이 지원하는 APT Volt Typhoon이 미국의 중요 인프라를 대상으로 상당한 노력을 했다는 보고도 있었습니다. 자세한 내용은 다음 섹션을 참조하십시오.
- **전략의 변화:** 반대로 북한, 베트남, 인도와 연계된 그룹은 APT 활동이 급격히 감소했으며, 북한과 연계된 탐지 건수는 -82%, 베트남은 -80%, 인도는 -82% 감소했습니다. 특히 북한의 비례 기여도(-6%)가 크게 감소한 것이 눈에 띄는데, 이는 북한의 초점, 전략 또는 역량에 변화가 있다는 것을 나타냅니다.
- **더 많은 국가 등장:** 파키스탄 및 벨라루스와 연계된 그룹의 탐지 건수가 각각 55%, 2019% 증가하는 등 관련 APT 활동이 크게 증가했습니다. 이러한 증가, 특히 벨라루스와 관련된 기하급수적인 증가는 APT 무대에서 새롭거나 이전에는 잘 알려지지 않았던 행위자들의 등장을 강조합니다.

  "기타" 범주의 탐지 건수가 121% 증가하여 APT 활동이 가장 많이 인용되는 국가에 국한되지 않음을 보여줍니다. 이러한 다양성은 사이버 위협의 글로벌 특성과 광범위하고 적응력 있는 사이버 보안 태세의 필요성을 강조합니다.

Trellix는 향후 수개월에 걸쳐 이와 같은 새로운 패턴을 면밀히 추적해 나갈 예정입니다.

목차



표적이 되는 국가 및 지역

이 섹션에서는 2023년 4분기부터 2024년 1분기까지 Trellix가 APT 그룹의 APT 관련 활동을 탐지한 국가 지역을 중심으로, 이러한 정교한 사이버 행위자들의 초점과 전략에 상당한 변화가 있었음을 보여줍니다.

> 이 데이터는 사이버 위협의 글로벌 특성과 국가별로 APT 그룹으로부터 받는 다양한 관심 수준을 강조합니다.

Trellix Advanced Research Center에서는 다음과 같은 요인이 특정 국가 및 지역에서 탐지된 활동에 영향을 미쳤다고 중간 신뢰 수준에서 평가합니다.

튀르키예에서는 APT 관련 탐지 건수가 전례없이 급증했습니다.

운영 목표:
튀르키예를 대상으로 하는 위협의 탐지 건수는 무려 1458% 증가했으며, 이는 전체 탐지 건수에 대한 비례 기여도가 16% 증가한 것으로 해석됩니다. 이러한 현저한 증가는 사이버 위협의 초점이 튀르키예로 빠르게 이동하고 있음을 나타내며, 이는 지정학적 긴장이나 APT 그룹의 특정 운영 목표를 반영하는 것일 수 있습니다.

- **전략적 중요성:** 인도와 이탈리아도 탐지 건수가 각각 614%, 308%까지 크게 증가했습니다. 공격 대상 목록에서 이러한 국가의 부상은 경제적, 정치적, 기술적 요인으로 인해 사이버 도메인에서 이들 국가의 전략적 중요성이 커지고 있음을 시사하는 것일 수 있습니다.

목차

- **확장되는 환경:** 흥미롭게도 베트남과 미국의 경우 APT 탐지 건수는 여전히 높지만 다른 동향을 보여주었습니다. 베트남의 탐지 건수는 9% 증가했지만, 비례 기여도는 -9% 감소하여 표적 환경이 확대된 것을 나타냅니다. 미국은 탐지 건수가 15%로 약간 증가했지만 비례 기여도는 -7% 하락하여 APT 그룹의 대상 전략이 다양화되고 있음을 시사합니다.
- **지정학적 전개:** 독일, 중국, 파푸아뉴기니, 브라질은 모두 탐지 건수가 증가했으며, 독일과 중국은 비례 기여도에 큰 변화가 나타나고 있습니다. 이러한 대상 국가의 다양화는 APT 그룹이 글로벌 사이버 보안 태세와 지정학적 전개에 대응하여 전략적이고 기회주의적으로 조정하고 있다는 것을 반영합니다.
- **국가 안보 강화:** 반대로 인도네시아는 탐지 건수가 -48%로 크게 감소하고 비례 기여도도 -4%로 하락했습니다. 이러한 감소는 일시적인 우선순위 하락이나 국가 사이버 보안 조치의 성공적인 강화를 나타낼 수 있습니다.
- **초점 통합:** Trellix가 APT 관련 활동을 탐지한 다양한 기타 국가를 나타내는 "기타" 범주는 탐지 건수가 -23% 감소하고 비례 기여도는 -21% 감소했습니다. 이러한 감소는 APT 그룹이 이 기간 동안 이익이 큰 특정 표적에 집중할 수 있다는 것을 나타냅니다.

지정학적 동향으로 인해 환경이 계속해서 빠르게 변화할 수 있다고 봅니다.

악성 도구

목차

2023년 4분기부터 2024년 1분기까지 APT 캠페인에 사용된 악성 도구를 분석한 결과 사이버 위협 행위자의 선호도와 운영 전술에 주목할 만한 동향이 나타났습니다. 탐지율과 비례 기여도의 차이는 진화하는 사이버 위협 환경과 이러한 정교한 그룹 간의 도구 사용 역학 변화에 대한 인사이트를 제공합니다.

다음과 같은 동향이 관찰되었습니다.

- **더욱 강력해지는 공격 도구:** Cobalt Strike는 탐지 건수가 17% 감소했음에도 불구하고 여전히 많은 위협 그룹에서 선택하는 도구입니다. 비례 기여 편차의 상대적으로 작은 감소(-1%)는 사이버 운영에서 여전히 인기와 효과를 유지하고 있음을 시사하며, 다양하고 널리 사용되는 공격 도구를 방어하는 데 어려움이 있음을 강조합니다.
- **웹 셸, PowerShell 및 원격 액세스 공격 의존성:** China Chopper, PowerSploit 및 Gh0st RAT도 탐지 건수가 각각 23%, 24%, 24%로 크게 감소했습니다. 이러한 감소에도 불구하고 비례 기여 편차의 소폭 변화는 이들이 여전히 위협 행위자의 도구 키트에 필수적이라는 것을 나타냅니다. 웹 셸 공격, PowerShell exploit, 원격 액세스 기능으로 잘 알려진 이러한 도구는 사이버 운영에 대해 입증된 다목적 도구에 대한 지속적인 의존성을 시사합니다.
- **탐지 가능성이 낮은 도구:** Empire, Derusbi, BADFLICK, JJdoor/Transporter, JumpKick, MURKYTOP은 모두 비슷한 탐지 건수 하락 추세를 보이며 25% 이상 감소하였습니다. 이러한 획일적인 감소는 위협 그룹이 선호하는 도구의 광범위한 변화 또는 대응 및 탐지 기술에 대한 적응을 반영할 수 있으며, 탐지 가능성이 낮은 새로운 도구로의 이동을 촉진합니다.
- **끊임없는 혁신:** "기타" 악성 도구 범주는 탐지 건수가 30%까지 큰 폭으로 증가하고, 비례 기여 편차도 6% 눈에 띄게 증가했습니다. 이러한 증가는 위협 행위자들이 탐지를 회피하고 목표를 달성하기 위해 새로운 도구와 기술을 모색하면서 끊임없이 혁신하고 적응하고 있음을 보여줍니다.

악성 도구 사용에 대한 선호도가 변화하는 것은 사이버 보안 발전에 대응하는 사이버 위협 행위자들의 적응적 특성을 의미합니다.

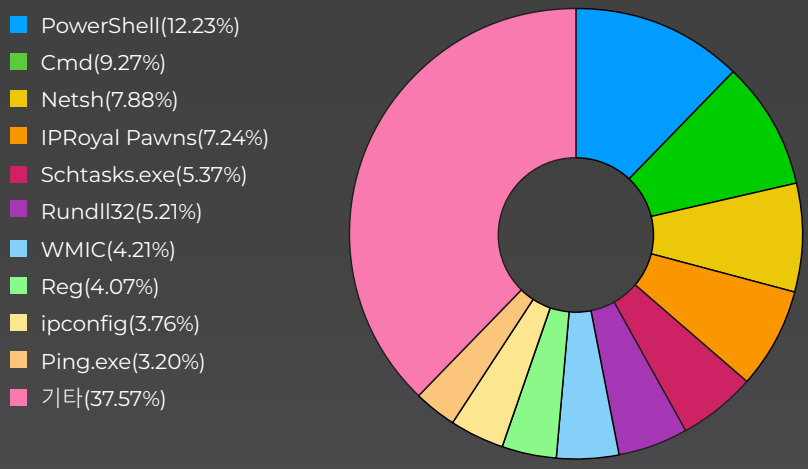
> 방어 메커니즘이 더욱 정교해짐에 따라 APT 그룹의 공격 도구 및 전술도 더욱 정교해졌습니다.

"기타" 범주의 탐지 건수 증가에서 알 수 있듯이 더 광범위한 도구로의 전환은 진화하는 사이버 위협으로 인해 제기되는 위험을 완화하기 위한 지속적인 연구, 위협 인텔리전스, 적응형 방어 전략의 필요성을 강조합니다.

목차

무해한 도구

2023년 4분기와 2024년 1분기 사이에 탐지된 상위 10개 무해한 도구



> "LotL(Living off the Land)"로 알려진 이러한 관행은 탐지 노력을 복잡하게 만들고 위협 행위자의 정교함을 강조합니다.

2023년 4분기부터 2024년 1분기까지 APT 그룹이 사이버 운영에서 무해한 도구를 사용한 것은 악의적인 목적에 합법적인 시스템 도구를 활용하는 최신 사이버 위협의 중요한 측면을 강조합니다. "LotL(Living off the Land)"로 알려진 이러한 관행은 탐지 노력을 복잡하게 만들고 위협 행위자의 정교함을 강조합니다. 통계에 따르면 이러한 도구의 사용량에는 큰 차이가 있으며, 이는 사이버 운영에서 이러한 도구의 전략적 중요성을 반영합니다.

- **다용성:** PowerShell은 비례 기여 편차 1%에서 탐지 건수가 105%로 크게 증가했습니다. 이러한 급증은 정찰부터 페이로드 전달까지 광범위한 악성 활동을 자동화하는 데 있어 그 다재다능함과 강력함을 강조합니다.
- **네트워크 조작에 집중:** Netsh 및 IPRoyal Pawns는 탐지 건수가 각각 99% 및 102%까지 크게 증가했습니다. 이러한 도구는 네트워크 구성 및 프록시 트래픽에 자주 사용되며, 이는 네트워크 조작 및 회피 기술에 전략적 초점을 맞추고 있음을 나타냅니다.
- **자동 확장/축소:** Schtasks.exe는 138%로 열거된 도구 중에서 가장 큰 백분율 편차를 경험했습니다. 이는 사용자의 직접적인 개입 없이 악성 페이로드의 지속 및 실행을 위해 예약된 작업에 대한 의존도가 증가하고 있음을 반영합니다.

목차

- **전술적 변화:** 반대로 Rundll32와 WMIC는 사용량이 증가했지만 비례 기여 편차가 감소하여 이러한 도구의 지속적인 유용성에도 불구하고 APT 그룹의 전술적 선호도가 변화했음을 나타냅니다.
- **도구 다각화:** Windows 시스템의 오래된 명령줄 인터프리터인 Cmd 도 탐지 건수가 65% 증가하는 등 사용량이 크게 증가했습니다. 사용량의 증가에도 불구하고 비례 기여 편차는 -2.5% 감소하여 APT 그룹 간에 도구 사용이 더욱 다양해지고 있음을 보여줍니다.

  일반적으로 덜 사용되거나 더 전문화되고 다양한 도구를 나타내는 "기타" 범주는 탐지 건수가 42% 증가했습니다. 하지만 비례 기여 편차가 크게 감소(-21%)하여 사이버 위협 행위자들이 처분할 수 있는 도구가 확대되고 있음을 강조합니다.

APT 그룹의 무해한 도구 사용 환경이 진화하는 것은 정교한 사이버 위협을 탐지하고 방어하는 것이 얼마나 복잡한지를 보여줍니다. 이러한 도구의 전략적 선택과 적용은 대상 환경에 대한 깊은 이해와 탐지되지 않은 상태로 유지하려는 노력을 보여줍니다.

> **CISO 팁:** 따라서 사이버 보안 방어는 기존의 맬웨어 탐지를 넘어 사이버 운영에서 합법적인 도구의 오용에 대응하기 위한 행동 분석 및 이상 탐지를 포함하도록 진화해야 합니다.

Trellix Advanced Research Center에서 제공하는 Trellix ATLAS 글로벌 센서를 통해 수집되는 데이터와 업계에서 검증된 보고서의 전략적 인사이트를 결합함으로써, 고객은 각 부문을 대상으로 하는 위협 행위자를 파악하고 행동 분석을 통해 환경 내에서 비정상적인 행동을 탐지할 수 있습니다.

목차

결론

2023년 4분기부터 2024년 1분기까지 APT(지능형 지속 공격) 활동을 분석한 결과 사이버 위협 환경의 역동적이고 점점 더 복잡해지는 특성이 밝혀졌습니다. APT 그룹의 발원지, 표적 국가, 악성 및 무해한 도구 사용과 관련된 통계를 살펴보면 사이버 위협 행위자들의 진화하는 전략을 강조하는 몇 가지 주요 동향을 확인할 수 있습니다.

APT 그룹은 다음에 대해 지속적으로 입증합니다.

1. 높은 수준의 적응성 및 정교함
2. 높은 수준의 악성 도구 활용
3. 높은 수준으로 합법적인 시스템 유틸리티를 악용하여 스파이 행위, 운영 중단, 민감한 정보 절도

이러한 그룹의 표적 및 운영 전술에서 관찰되는 큰 차이는 전략적 목표뿐만 아니라 글로벌 사이버 보안 개발 및 방어 조치에 대한 대응도 반영합니다.

특정 국가에서 APT 관련 활동이 획기적으로 증가하는 등 표적 관행의 극적인 변화는 이러한 사이버 운영을 주도하는 지정학적 동기를 강조합니다. 마찬가지로, "LotL(Living off the Land)" 전략의 현저한 증가를 포함한 도구 사용 변화는 합법적인 활동과 악성 활동이 점점 더 얽혀 있는 환경에서 APT 위협을 탐지하고 대처해야 하는 지속적인 과제를 강조합니다.

또한 APT 발원지의 다양화와 표적 전략의 확대는 사이버 기능의 전 세계적인 확산과 사이버 보안에 대해 통일되고 협력적인 접근 방식이 필요하다는 것을 나타냅니다.

> 이러한 정교한 위협 행위자에게 벗어날 수 있는 국가나 조직은 없습니다.

목차

Volt Typhoon: 중국을 중심으로 하는 국가 기반 APT 위협

국가 위협 행위자 그룹은 2023년 4분기와 2024년 1분기 동안 전 세계 상업 및 공공 부문 조직에 지속적이고 심각한 위협이 되고 있습니다. 정교한 사이버 위협에 잘 준비되고 능숙한 공격자들은 사이버 범죄자나 핵티비스트에 비해 우수한 인재와 자원을 바탕으로 장기간에 걸쳐 끊임없이 네트워크를 표적으로 삼습니다.

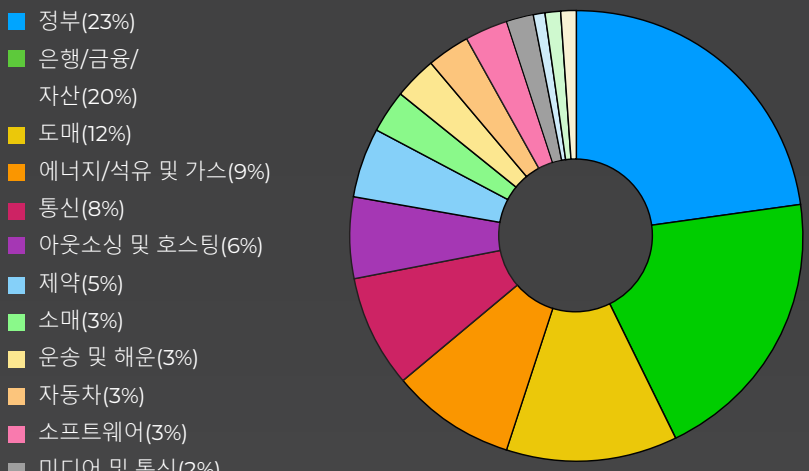
특히 Trellix 텔레메트리 탐지를 기반으로 중국 관련 국가 후원 위협 행위자 그룹은 전 세계적으로 정부 부문에 점점 더 많은 위협을 가하고 있습니다. 저희 데이터에 따르면 2023년 10월부터 2024년 3월까지 중국과 연계된 위협 행위자 그룹의 위협 활동이 2,100만 건 이상 탐지된 것으로 나타났습니다.

23%

탐지된 악성 활동의 23% 이상이 전 세계 정부 부문을 대상으로 합니다.

중국과 연계된 위협 행위자 그룹의 위협 활동이 2,100만 건 이상 탐지되었습니다.

중국과 연계된 APT 그룹의 글로벌 탐지 건수



(출처: ATLAS)

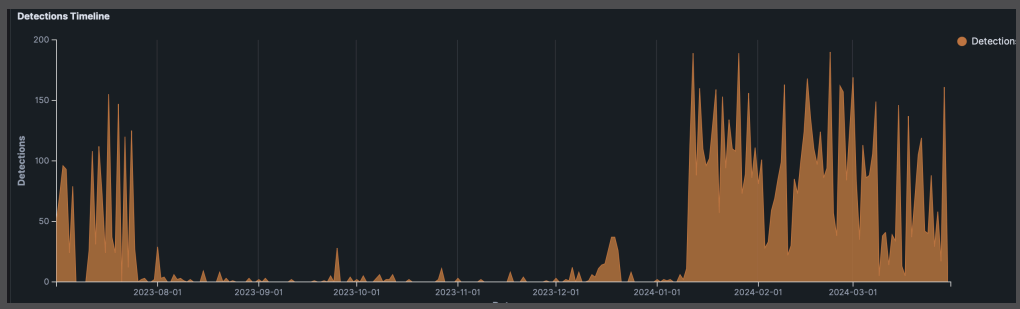
목차

개요

상대적으로 새로운 중국 국가 후원 APT 그룹인 Volt Typhoon은 기존의 다른 중국 관련 APT 그룹의 사이버 스파이 및 인텔리전스 수집에서 벗어난 독특한 행동 패턴과 표적 프로필로 인해 눈에 띕니다. 이전의 오픈 소스 보고에 따르면 이 중국 APT 그룹은 지정학적 위기나 전쟁이 발생했을 때 내부 확산을 용이하게 하여 운영 기술(OT) 자산과 기능을 방해하기 위해 산업 제어 IT 네트워크에 사전 배치되었습니다. Trellix 텔레메트리 데이터에 따르면 Volt Typhoon은 2024년 1월에 운영을 재개한 이후 미국을 포함한 글로벌 정부 부문을 반복적으로 공격하는 동시에 LotL(Living off the Land) 기술을 채택하고 있습니다.

운영 일정표

Trellix 글로벌 텔레메트리 데이터에 따르면 Volt Typhoon은 2021년 중반에 처음 탐지되었지만 2023년 8월부터 2024년 1월까지 활동이 거의 없거나 전혀 없이 대부분 휴면 상태로 전환되었습니다. 이러한 중단 기간은 2023년 5월에 발표된 Volt Typhoon에 대한 첫 번째 공급업체 보고서가 전 세계적인 관심을 끌었던 이후 몇 달 동안 위협 조사가 정점에 달했기 때문일 수 있습니다. 또한 Volt Typhoon이 이 기간 동안 대중 노출로 인해 공격 인프라를 변경할 가능성이 있어 위협 활동이 거의 탐지되지 않았기 때문일 수 있습니다.



2023년 7월부터 2024년 3월 사이의 Volt Typhoon 탐지 일정표(출처: Trellix ATLAS)

Volt Typhoon은 Trellix 텔레메트리 데이터를 기반으로 2024년 1월 중순경 운영을 재개했습니다. 2024년 1월 중순 이후, Trellix 텔레메트리를 통해 Volt Typhoon과 관련한 7,100건 이상의 악성 활동을 탐지했으며, 2024년 1월부터 3월까지 주기적으로 급증했습니다.

2024년 1월부터 3월 사이의 Volt Typhoon 탐지 세부 정보

목차

전술, 기술, 절차(TTP)

저희의 탐지 데이터에 따르면 Volt Typhoon은 2024년 1월 중순에 운영을 재개한 이후 여러 네이티브 Windows 도구와 기능을 지속적으로 활용하여 악의적인 이유로 명령을 실행했습니다. 합법적인 소프트웨어와 기능을 시스템에서 사용할 수 있는 이중 사용 도구인 LOTL(Living-off-the-land) 도구로 알려진 이러한 도구는 Volt Typhoon을 비롯한 중국에 기반을 둔 국가 행위자 그룹 사이에서 점점 더 인기를 얻고 있습니다. Netsh.exe는 방화벽 설정을 사용하지 않도록 설정하거나 감염된 호스트에 대한 원격 호스트 액세스를 허용하도록 프록시 터널을 설정하는 등 다양하고 악의적인 용도로 사용할 수 있는 도구 중 하나입니다. Ldifde는 Volt Typhoon 위협 행위자들이 정보 수집을 위해 활용하는 다른 도구입니다.

도메인 컨트롤러에 액세스한 후 공격자는 Ldifde.exe를 사용하여 민감한 데이터를 내보내거나 디렉터리에 대한 승인된 변경을 수행할 수 있습니다. 마찬가지로 Volt Typhoon 위협 행위자도 악의적인 시도에 Ntdsutil을 사용합니다. Ntdsutil은 관리자가 데이터베이스 유지 관리를 수행하도록 허용하는 합법적인 도구이지만 Active Directory 덤프를 생성하여 자격 증명을 수집하고 민감한 데이터를 반출하는 데에도 사용할 수 있습니다.

Volt Typhoon 위협 행위자는 위협 운영에서 FRP, Impacket, Mimikatz와 같은 오픈 소스 도구를 계속 사용했습니다. 또한 Trellix 텔레메트리에서는 2023년 2월과 3월 사이에 다음 LOTL 도구와 명령을 사용하여 Volt Typhoon을 탐지했습니다.

- Comsvcs
- Dnscmd
- Ldifde
- MiniDump
- Net
- Netsh
- Ntdsutil
- reg
- Ping
- PowerShell
- PsExec

목차

저희 텔레메트리에서 관찰된 Volt Typhoon에서 활용하는 주요 MITRE ATT&CK 도구는 다음과 같습니다.

- 초기 액세스 – T1190: 공용 응용프로그램 Exploit
- 실행 – T1106: 기본 API
- 지속 – T1546: 이벤트 트리거 실행
- 권한 상승 - T1546: 이벤트 트리거 실행
- 방어 회피 – T1070.001: Windows 이벤트 로그 지우기
- 방어 회피 – T1070: 파일 삭제
- 방어 회피 – T1027: 파일 또는 정보 난독화
- 자격 증명 액세스 – T1003.003: NTDS
- 자격 증명 액세스 – T1003: OS 자격 증명 덤핑
- 자격 증명 액세스 – T1110: 무차별 대입
- 자격 증명 액세스 – T1555: 암호 저장소의 자격 증명
- 검색 – T1069.002: 도메인 그룹
- 검색 – T1069.001: 로컬 그룹
- 검색 – T1083: 파일 및 디렉터리 검색
- 검색 – T1057: 프로세스 검색
- 검색 – T1010: 응용프로그램 창 검색
- 수집 – T1560: 수집 데이터 보관
- 수집 – T1560.001: 유틸리티를 통한 보관
- 명령 및 제어 – T1090.002: 외부 프록시
- 명령 및 제어 – T1105: 인그레스 도구 전송
- 명령 및 제어 – T1132: 데이터 인코딩

랜섬웨어 환경의 진화

2023년 4분기 사이버 위협 환경에서는 랜섬웨어 공격이 증가했으며, 그해 새롭게 등장한 랜섬웨어 계열이 점점 더 큰 영향을 미치고 있습니다.

- **EDR 킬러 도구:** 이 중에서 D0nut 랜섬웨어 범죄 조직의 등장은 EDR 킬러 도구를 혁신적으로 활용하여 엔드포인트 탐지를 우회하고 공격 효율을 개선하는 진화한 전술을 보여주었다는 점에서 특히 주목할 만했습니다. 자세한 내용은 다음 섹션을 참조하십시오.
- **취약성 공격:** 이 기간에도 랜섬웨어 배포를 용이하게 하기 위해 중요한 취약점을 악용하는 추세가 계속되었습니다. 특히, CVE-2023-4966(Citrix Bleed라고도 함)은 LockBit 3.0 계열사에 의해 악용되어 정교한 사이버 공격에 대한 중요 인프라의 지속적인 취약성을 강조합니다. 또한 Confluence Data Center 및 Confluence Server에서 CVE-2023-22518을 악용하여 공격자들은 널리 사용되는 비즈니스 플랫폼에 침투하여 랜섬웨어를 배포하는 데 집중했습니다. 새로 발견된 취약점을 악용하여 Qlik Sense 설치를 표적으로 한 Cactus 랜섬웨어 캠페인은 보안 환경에 적응하고 새로운 취약점을 악용하는 공격자의 민첩성을 더욱 잘 보여주었습니다. 2023년 4분기는 랜섬웨어 그룹이 활발하게 활동한 분기입니다.

목차

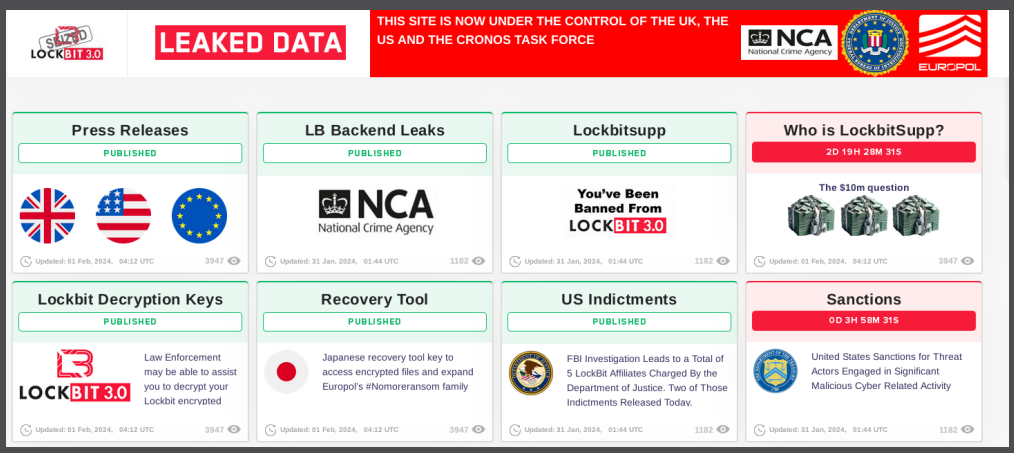
하지만 2024년 1분기에 주목할 만한 법 집행 조치로 인해 현상 유지가 흔들렸습니다.

Operation Cronos: LockBit 근절을 위한 법 집행 조치

2024년 2월 19일부터 국제 법 집행 조치인 Operation Cronos가 전개되었습니다. 악명 높은 LockBit 범죄 조직을 완전히 소탕하여 오랜 범죄 단체에 당한 만큼 되갚아 주었습니다. 사법당국은 잘 알려진 게시 중단 공지를 표시하는 데 그치지 않고 범죄 그룹의 유출 사이트를 완전히 통제하고 범죄 단체를 세상에 노출시킴으로써 자신을 일부 드러냈습니다. 저희가 제기한 일부 기소장과 활동 중인 계열사가 LockBit 백엔드에 로그인하면 친숙한 환영 메시지를 표시하여 정체가 밝혀졌음을 명시적으로 알려주었습니다.

이러한 조치는 LockBit의 운영을 방해하고 그들의 평판을 훼손하고 범죄 조직 내에서 신뢰를 무너뜨리기 위한 것이었습니다.

이 보고서를 마무리하는 시기에 Operation Cronos는 또 다른 반전이 있었습니다. 글로벌 법 집행 기관에서는 LockBit 주모자의 실제 정체를 공개하여 2라운드를 시작했습니다. 이것이 법 집행의 유일한 승리는 아니었습니다. 5월 1일 Kaseya와 다른 많은 조직을 공격한 REvil 계열사는 징역 13년을 선고받고, 미화 1,600만 달러의 손해배상금을 갚아야 했습니다. Trellix Advanced Research Center의 REvil 사례 지원에 관한 자세한 내용은 여기를 참조하십시오.



목차

작년 2월 보고서에 따르면 LockBit이 몸값 요구에 가장 적극적인 것으로 나타났습니다. 이러한 사이버 범죄자들은 2018년까지 발견된 취약점을 이용하는 등 다양한 기술을 사용하여 캠페인을 실행합니다. LockBit은 2023년까지 신상 공개(name-and-shame) 사이트에 가장 많은 피해자가 게시되어 가장 널리 퍼진 랜섬웨어 그룹으로 남아 있습니다. 주로 다양한 부문의 북미 및 유럽 조직을 표적으로 삼았으며, 산업재 및 서비스 부문에 가장 큰 영향을 미쳤습니다. 2023년에 LockBit은 지속적으로 진화하여 랜섬웨어 프로그램에 새로운 도구와 방법을 도입했습니다. 주목할 만한 사건으로는 유출된 Conti 랜섬웨어의 코드를 기반으로 LockBit Green 암호기 개발을 진행 중인 LockBit과 macOS를 대상으로 하는 LockBit 변종이 있습니다. 또한 2023년에는 LockBit RaaS가 ALPHV, NoEscape 등 운영이 중단된 다른 RaaS 프로그램의 계열사에 새로운 홈을 제공하는 것을 목격했습니다.

파괴적인 조치의 여파로 LockBit이 체면을 세우고 수익성이 좋은 작전을 복원하려고 필사적으로 노력하는 것을 목격했습니다. 이는 LockBit의 범죄 활동이 널리 알려졌기 때문에 예상된 일이었지만, 사이버 범죄 지하 조직에서는 수년간의 신뢰보다 서버를 복원하는 것이 더 쉽습니다. 사법 당국이 LockBit의 운영, 인물 및 계열사에 대해 얼마나 많은 정보를 확보했는지는 아직 밝혀지지 않았습니다.

> 이러한 불확실성은 LockBit 및 (이전) 팀과 기꺼이 관계를 맺는 모든 사이버 범죄자에게 큰 위험을 초래합니다.

법 집행 조치 후 범죄자들의 세계는 냉혹한 경쟁의 세계라는 것이 명확해졌습니다. Trellix Advanced Research Center는 유출된 LockBit Black 버전을 사용하여 재정적 이익을 위해 유명 브랜드를 사칭하는 다른 행위자들을 관찰했습니다.

사기꾼이든 아니든, 그들이 만든 피해자는 실제로 존재했고, 이 모든 사건으로 인해 지난 두 분기는 영화 각본에나 어울릴 법한 상황이었습니다.

랜섬웨어의 글로벌 현황

2024년 1분기의 랜섬웨어 활동을 조사하는 동안 유출 사이트, 텔레메트리, 공개 보고 등 다양한 출처를 조사했습니다. 각 범주에 대해 몇 마디 말씀드리겠습니다.

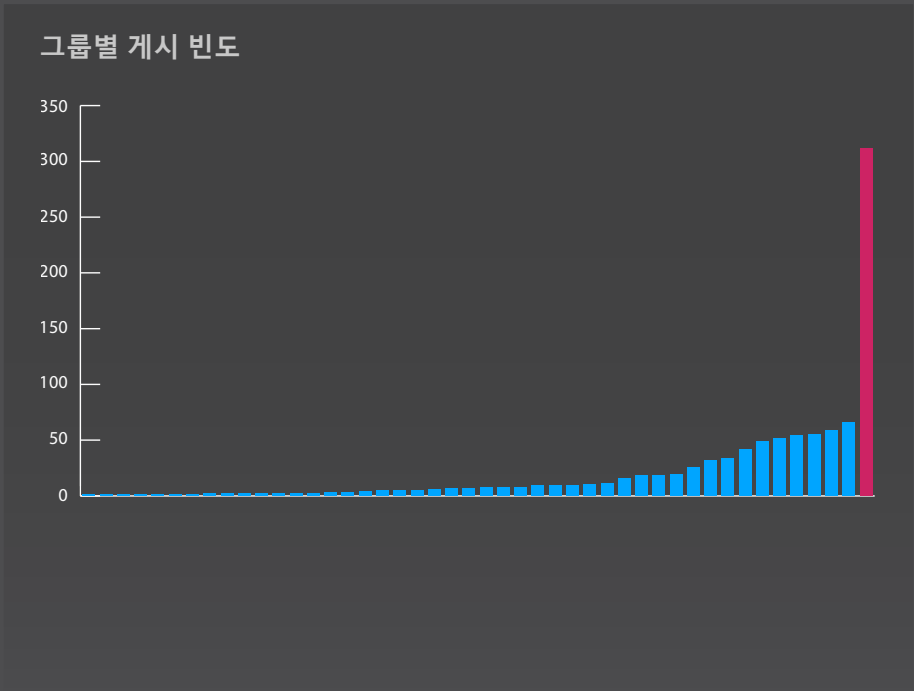
- **유출 사이트:** 이 사이트는 요구된 몸값을 지불하지 않은 피해자가 갈취당한 증거를 보여줌으로써 범죄 조직의 활동을 살펴볼 수 있도록 고안되었습니다. 또한 유출 사이트가 반드시 지형을 정확하게 반영하는 것은 아니라는 점에 유의해야 합니다. 범죄자에 의해 운영된다는 점에서 모든 진술이 진실하지도 않고 정확하지도 않습니다. 또한 범죄 조직이 약속을 지키면 몸값을 지불한 피해자가 목록에 등재되지 않아 완전한 정보가 제공되지도 않습니다. 이 보고서에 사용된 데이터는 유출 사이트의 전반적인 동향을 나타내며 의미 있는 그림을 그려줍니다.

목차

- **텔레메트리:** 텔레메트리란 Trellix 센서 에코시스템에서 파생되었으며 탐지란 파일, URL, IP 주소 또는 기타 표시기가 당사 제품 중 하나에서 탐지되어 당사에 다시 보고되는 경우를 의미합니다. 고객이 내부 규칙을 미세 조정하기 위해 특정 파일에 대한 탐지를 테스트하고 집계된 로깅에도 표시되므로 모든 탐지가 감염이라고 말할 수는 없습니다. 따라서 이 데이터는 여전히 동향에 드러나는 것처럼 큰 그림을 모색할 때 유용합니다.
- **공개 보고서:** 공급업체와 개인이 제출한 보고서를 Advanced Research Center에서 처리하여 기능을 분석하고 동향을 도출했습니다. 각 보고서에는 고유한 편향성이 있으며, 예를 들어 다른 공급업체에 비해 특정 공급업체의 지리적 입지가 우세할 수 있습니다. 이러한 차이로 인해 보고 주체에 따라 사안이 다르게 보고될 수 있습니다. 포함된 보고서의 편향성이 다양하기 때문에 특정 필터를 적용하지 않습니다.

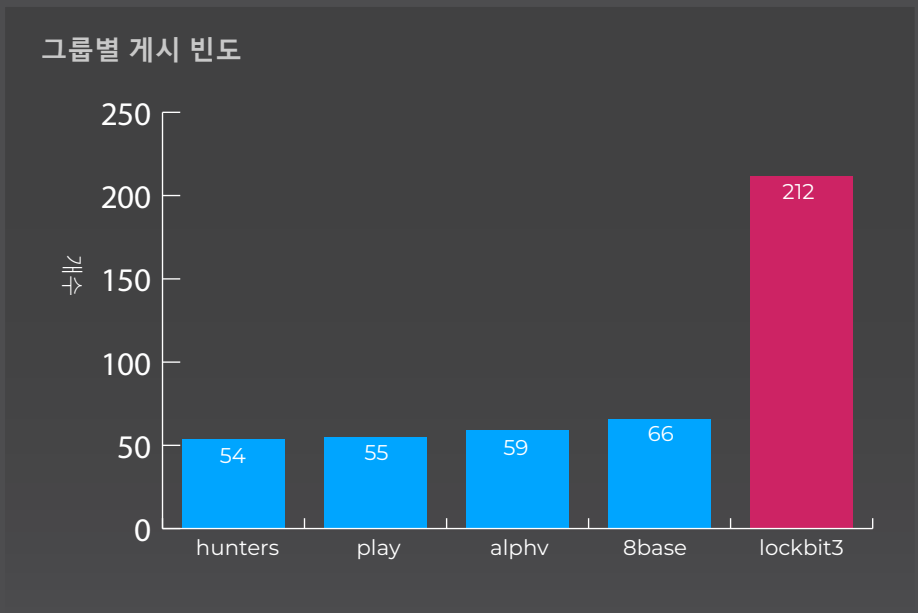
활성 랜섬웨어 그룹

2024년 1분기의 집계된 유출 사이트 게시물을 살펴보면 많은 곳에서 활동의 흔적이 보입니다. 유출 사이트에 일반 공지가 게시되는 경우도 있지만, 대부분은 피해자 데이터의 갈취 또는 유출에 대한 "증거"입니다. 또한 한 명의 피해자를 여러 번 게시하는 경우가 많아 데이터에 피해자가 두 번 이상 집계되어 부풀려질 수 있습니다.



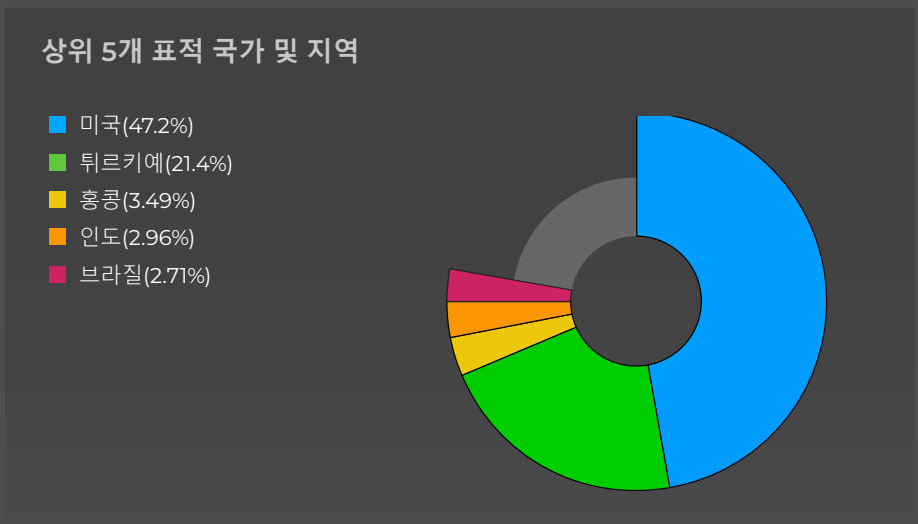
목차

가장 활발하게 활동하는 랜섬 범죄 조직 유출 사이트 5곳의 빈도를 보면, 그래프가 LockBit의 활동으로 인해 왜소해 보입니다. LockBit을 제외한 다른 범죄 조직의 활동에서는 분기당 평균 50개 이상의 게시물을 올렸는데, 이는 두 명의 피해자가 게시물을 올리는 데 걸리는 평균 시간이 2일 미만이라는 것을 의미합니다. 위에서 살펴본 바와 같이 이 수치는 몸값을 지불하지 않은 피해자를 반영한 것이므로 실제 피해자 수는 더 많을 가능성이 높지만 그 수를 정확히 파악할 수 있는 방법은 없습니다.



표적이 되는 국가 및 지역

랜섬웨어 조직의 지속적인 활동을 기반으로 Trellix 텔레메트리에서 랜섬웨어 탐지를 확인할 수 있습니다. 미국이 탐지 건수가 가장 많고 튀르키예, 홍콩, 인도, 브라질이 그 뒤를 이었습니다.



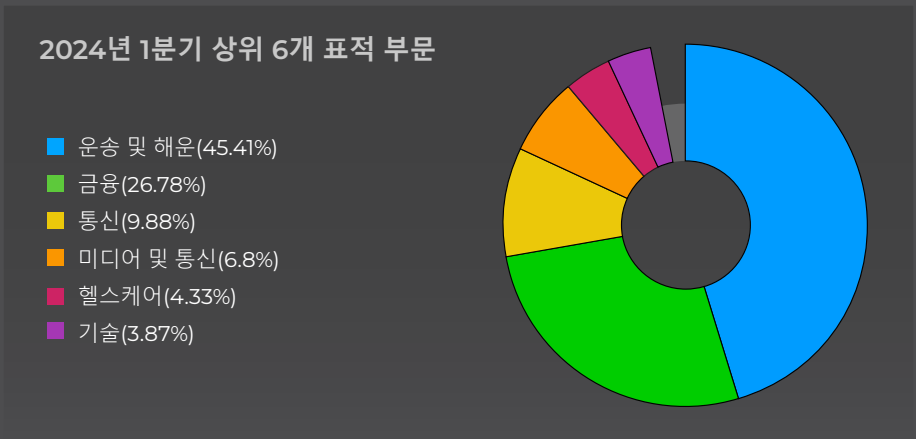
목차

랜섬웨어가 거의 모든 지역의 모든 부문에 위협이 된다는 점을 고려할 때, 탐지 메트릭은 고객 인구와 관련하여 의미가 있습니다.

이전 분기의 텔레메트리는 인도와 중국에서 탐지 건수가 증가한 것을 제외하면 다소 비슷한 양상을 보였습니다. 해당 지역에 대한 특정 캠페인이 있었다는 증거는 없으며, 맬웨어 테스트가 수행되어 해당 지역에서 더 많은 탐지 건수가 발생한 것으로 의심됩니다.

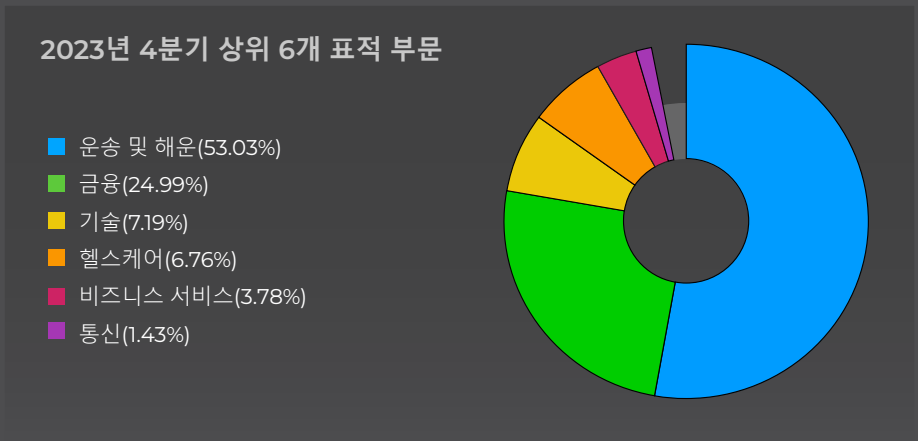
표적 부문

분야별 글로벌 텔레메트리 집계에 따르면 탐지 건수의 절반이 운송 및 해운 업계에서 발생하고, 4분의 1 이상이 금융 서비스에서 발생했습니다. 이 두 부문은 전체 탐지 건수의 72% 이상을 차지하며, 서비스의 가용성이 가장 중요하다는 것은 당연합니다. 운송 회사가 랜섬웨어 공격으로 인해 물품을 이동하지 못하면 운영 프로세스를 계속 진행할 수 없어 막대한 재정적 부담을 안게 됩니다. 마찬가지로 금융 산업은 신뢰를 기반으로 하며, 랜섬웨어 공격으로 인해 민감한 데이터가 유출되거나 기업이 가동 중지될 경우 금융 회사의 근간에 큰 타격을 줍니다.



2023년 마지막 분기에 상위 2개 부문에서는 차이가 없었지만 상위 표적 부문은 약간 달랐습니다. 이 두 부문은 해당 기간 동안 합산하여 전체 탐지 건수의 78%에 달하는 큰 비중을 차지했습니다. 2024년 1분기 기술 및 의료 부문은 전 분기 대비 감소했지만, 그 차이가 자체적으로 하나 이상의 특정 사건에 기인한다고 볼 수는 없습니다.

목차



도구 및 기술

언급된 세 가지 출처 중 마지막은 공개 보고서입니다. 수집된 보고서를 기반으로 MITRE 기술, 관련 도구 및 명령줄을 추출할 수 있습니다.

> **CISO 팁:** 이러한 기술은 탐지 관점에서 조직 블루 팀에서 사용할 수 있습니다. 가장 많이 사용되는 기술과 도구에 집중함으로써 가장 효과적인 것부터 시작하여 다양한 행위자의 다양한 유형의 공격을 완화할 수 있습니다. 또한 레드 및 퍼플 팀 연습을 통해 이러한 기술에 집중하여 어떤 탐지 조치가 마련되어 있는지 테스트할 수 있습니다.

아래 표에서는 가장 빈번한 기술을 내림차순으로 보여줍니다.

MITRE ATT&CK 기술	고유한 캠페인
강력한 데이터 암호화	31
파일 및 디렉터리 검색	23
PowerShell	23
인그레스 도구 전송	21
시스템 정보 검색	21
파일 또는 정보 난독화	19
레지스트리 수정	18
Windows Command Shell	17
파일 또는 정보 정체 밝히기/디코드	16
서비스 중지	16

랜섬웨어의 목적을 고려할 때, 데이터 암호화와 파일 및 디렉터리 검색 기술은 당연히 가장 높은 순위를 차지합니다. 이러한 기술을 2023년 4분기에 가장 많이 사용된 기술과 비교해 보면, 구체적인 순위는 다를 수 있지만 목록의 상위 기술 대부분이 비슷하다는 것을 알 수 있습니다.

목차

MITRE ATT&CK 기술	고유한 캠페인
강력한 데이터 암호화	45
PowerShell	29
파일 또는 정보 난독화	25
파일 및 디렉터리 검색	24
Windows Command Shell	24
시스템 복구 금지	23
공용 응용프로그램 Exploit	21
인그레스 도구 전송	21
프로세스 검색	21
서비스 중지	21

위의 APT 섹션과 마찬가지로 공격자들은 계속해서 합법적인 도구를 범죄에 활용하고 있습니다. 도구는 목적(이 경우 기술)을 위한 수단이므로 사용된 도구는 관찰된 기술에 영향을 미칩니다. 예를 들어 PowerShell과 Windows Command Shell은 "시스템 복구 금지" 기술에 주된 기여를 하는 섀도 복사본 제거 등의 추가 명령을 시스템에서 실행하는 데 자주 사용됩니다. 아래 이미지에서 볼 수 있듯이 가장 많이 사용되는 도구인 이유이기도 합니다.

CLI 도구 이름(attr)	고유한 캠페인
Cmd	7
PowerShell	6
VSSAdmin	5
wevtutil	4
curl	4
Rundll32	4
reg	4
Schtasks.exe	3
BCDEdit	3
wget	2

목차

VSSAdmin, BCDEdit 및 wevtutil을 사용하는 것은 랜섬웨어가 피해자의 시스템을 공격 이전처럼 정상적인 상태로 복구할 수 없도록 한다는 징후입니다. reg 사용은 다양한 이유로 수행될 수 있는 레지스트리 변경을 나타냅니다. 맬웨어는 지속성을 위해 레지스트리를 사용하는 경우가 많지만, 랜섬웨어는 암호화가 완료되면 아무런 목적이 없기 때문에 지속성을 중요하게 생각하지 않습니다. 대신 다른 설정을 변경하여 평소에는 불가능했던 특정 작업을 허용할 수 있습니다. Rundll32는 동적 링크 라이브러리를 로드하거나 실행하는 데 자주 사용되지만 종종 프로세스 주입의 대상이 되기도 합니다.

이전 분기와 마찬가지로 PowerShell과 명령 프롬프트는 똑같은 이유로 목록에서 1위를 차지했습니다. VSSAdmin 및 BCDEdit도 있지만 Windows Event Log Utility(wevtutil)은 상위 도구 목록에 없습니다. 언급된 모든 도구의 발생 빈도가 낮고 두 분기 중 어느 한 분기에 13건으로 가장 높았다는 점을 감안하면, 모든 캠페인에서 동일한 도구를 사용하지 않는 것은 놀라운 일이 아닙니다. 작은 편차로 인해 이러한 도구가 제외될 수 있습니다.

CLI 도구 이름(attr)	고유한 캠페인
PowerShell	13
Cmd	9
WMIC	6
Net	6
echo	5
VSSAdmin	4
msiexec	3
Schtasks.exe	3
Rundll32	3
BCDEdit	3

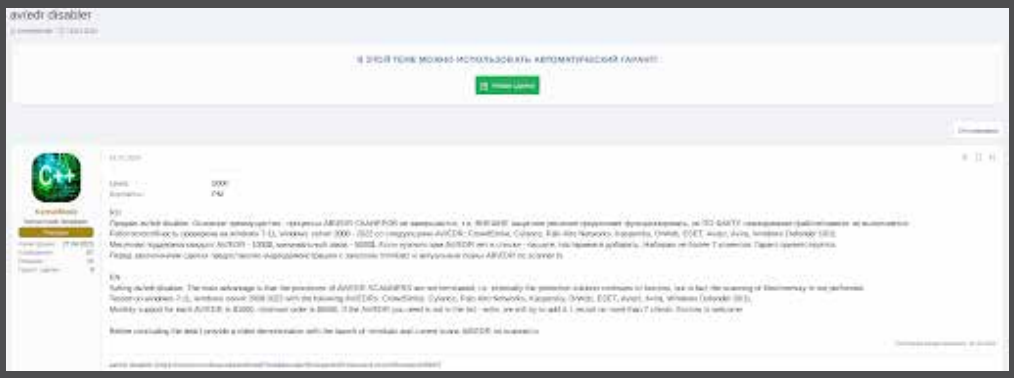
랜섬웨어의 위협은 여전합니다.

목차

EDR 킬러 및 회피 도구의 등장

전 세계적으로 많은 조직에서 EDR 솔루션을 채택하면서 더욱 정교한 공격을 더 잘 탐지하고, 이해하고, 대응할 수 있는 것으로 입증되었습니다. 오늘날 위협 행위자들은 종종 LOLBins(living-off-the-land binaries)와 더 복잡한 공격 방법에 의존하지만, EDR 기술이 등장하면서 공격자가 탐지되지 않는 것이 더 어려워졌습니다.

그러나 보안은 여전히 쫓고 쫓기는 게임이며 공격자들은 EDR 솔루션을 회피하거나 무력화할 방법을 찾고 있습니다. 이러한 움직임은 EDR 킬러 및 회피 도구/기술을 낳았으며, 그 중 일부는 사이버 범죄 지하 조직 포럼에서 제공되고 있습니다. 예를 들어, 앞서 D0nut 랜섬웨어 조직이 자체 EDR 킬러 덕분에 유명해진 것을 보았습니다.



XSS 지하 조직 포럼의 EDR 무력화 광고

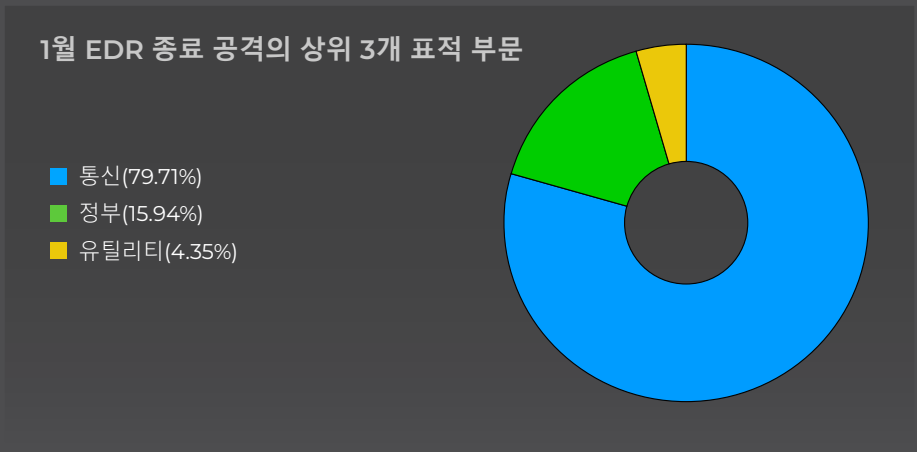
Spyboy의 EDR Terminator 도구를 사용하는 1월 캠페인

취약한 드라이버를 악용하여 권한 있는 코드를 실행하는 일반적인 기술 중 하나를 BYOVD(Bring Your Own Vulnerable Driver) 공격이라고 합니다.

이 방법의 예로는 Spyboy라는 위협 행위자가 제공한 EDR "Terminator" 도구가 있습니다. Terminator 도구는 Zemana 맬웨어 방지 도구에 속하는 합법적이지만 취약한 Windows 드라이버를 활용하여 CVE-2021-31728을 악용할 가능성이 있는 Windows 커널 내에서 임의의 코드를 실행합니다. Terminator는 2023년 중반에 온라인에 등장했으며, Trellix는 제품 적용 범위에 관한 자세한 기술 자료 문서를 발행했습니다(여기에서 확인 가능).

2024년 1월 11일부터 17일까지 Trellix Advanced Research Center에서는 새로운 캠페인인 Trellix 텔레메트리에서 Spyboy의 Terminator가 비정상적으로 탐지되는 것을 확인했습니다. 이 Terminator 캠페인은 6일 중 3일 동안 급증했으며 단일 정부 기관, 국가 유틸리티 회사, 위성 통신 회사에서 여러 번 탐지되었습니다. 구체적인 표적을 고려할 때, Trellix는 이 공격이 러시아-우크라이나 충돌과 관련이 있다고 높은 신뢰 수준에서 평가하고 있습니다.

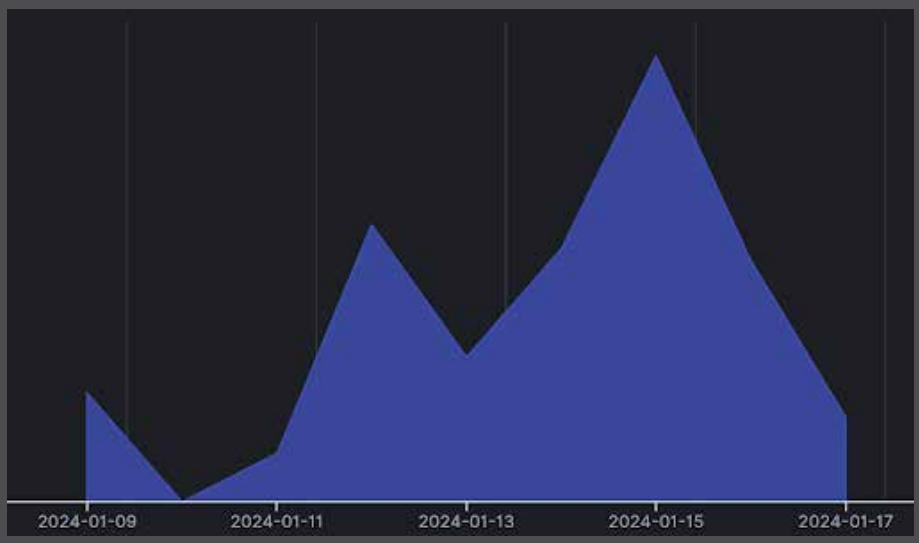
목차



Trellix ATLAS 탐지, 1월 EDR Terminator 캠페인에서 우크라이나를 표적으로 지정

더 많은 EDR 킬러가 관찰됨

2023년 초에 비슷한 목적을 가진 도구인 AuKill이 Sophos에 의해 설명되었습니다. 또한 이 도구는 BYOVD(vulnerable driver it brought)를 사용했습니다. EDR Terminator 및 AuKill 사례에서 사용된 드라이브는 서로 다르지만 둘 다 무해한 드라이버입니다. 반면에 2022년 일부 캠페인에서는 유사한 도구에서 로드된 맞춤형 악성 드라이버를 사용하는 것을 확인했습니다.



목차

이러한 목적으로 무해한 드라이버를 남용하면 이러한 공격을 탐지하기가 더 어려워지며, 앞서 언급한 LOLB 사용과 일치합니다. 이진 파일과 드라이버는 기술적으로 다르지만, 동일하지는 않더라도 의도와 동기는 비슷합니다. 2022년의 HermeticWiper에서도 무해한 드라이버를 사용했습니다. 이 경우 바이러스 백신을 비활성화하는 대신 드라이버를 사용하여 컴퓨터를 지웠습니다. 위에서 언급한 EDR Terminator의 사용과 HermeticWiper의 속성이 겹치는 또 다른 점은 친러시아 행위자가 사용한다는 점입니다.

LATAM 고객 중 한 곳에서 맬웨어 배포에 Discord 콘텐츠 전달 네트워크가 사용된 사례도 확인했습니다. 저희 팀은 이러한 방식으로 Discord가 맬웨어 공격에 계속 사용되는 것을 관찰했습니다.

> **CISO 팁:** 모든 SOC는 EDR을 면밀히 모니터링하는 것이 절대적으로 중요합니다. EDR 도구가 꺼져 있는 경우 SOC에 즉시 알림을 보내고 적절한 조치를 취할 수 있도록 경고 및 로깅을 설정해야 합니다. EDR 도구를 종료하면 변조를 나타내는 지표가 될 수 있으며, 공격자의 네트워크 액세스를 제한하려면 신속하게 대응해야 합니다. 또한 심층 방어 전략을 사용하여 네트워크 탐지 및 대응(NDR) 플랫폼과 같은 다른 도구에서 잠재적인 사고를 탐지하고, 공격자가 네트워크에 액세스하는 것을 제한하기 위해 신속하게 대응해야 합니다.

목차

공격자의 주요 표적이 되는 이메일

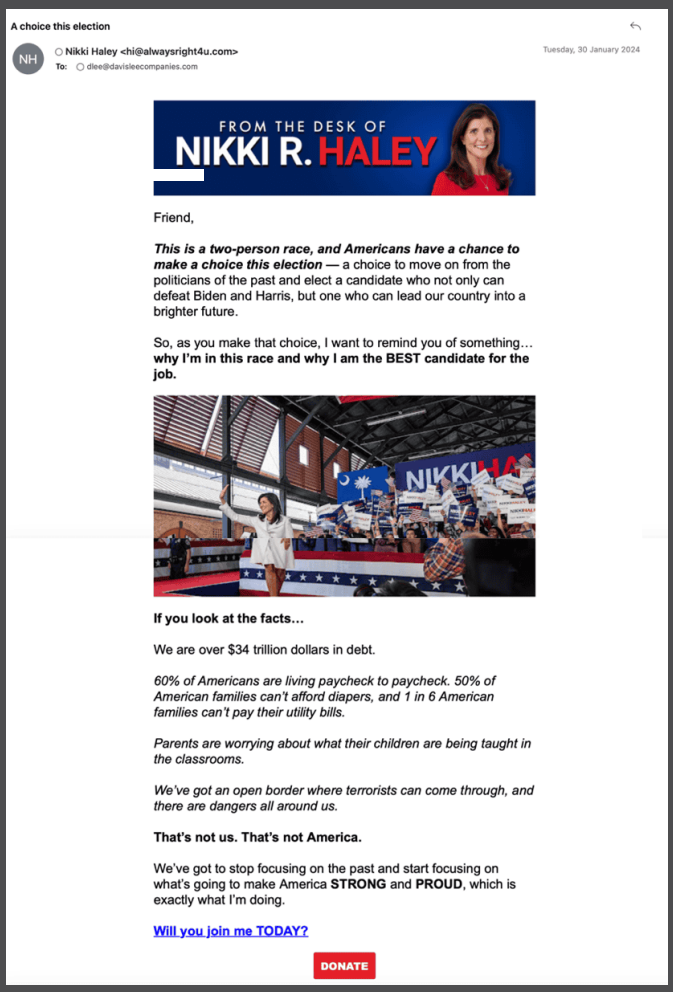
Trellix는 하루에 20억 개의 이메일 샘플과 9300만 개의 이메일 첨부 파일을 처리합니다. 이에 따라 공격자가 이메일을 통해 피해자를 노리는 새로운 기법을 관찰할 수 있는 엄청난 양의 데이터와 기회가 제공됩니다.

선거 기부금 사기

선거 기부금 피싱 사기에서는 애국심을 악용하고 유명 정치 후보자의 이름을 사용하여 개인의 선의와 정치 후보자에 대한 지지를 악용합니다. 2024년 1분기에 저희 연구원들은 사이버 범죄자들이 합법적인 마케팅 서비스를 악용하여 성조기와 함께 후보자 이미지로 장식된 그럴듯한 기부 페이지를 만들어 수신자에게 기부를 독려하는 것을 발견했습니다.

이러한 사기에서는 수신자를 속이기 위해 정식 마케팅 서비스 URL을 사용하여 이메일이 합법적인 것으로 믿게 합니다. 하지만 이메일은 사람들의 관대함을 활용하기 위해 발송됩니다. 이메일 내의 링크를 클릭하면 기부 페이지로 연결되며, 여기서 금융 정보를 입력하거나 발신자의 계정 또는 지갑 주소로 기부금을 보내라는 메시지를 받게 됩니다.

이메일 연구원들은 선거 기부를 활용하는 다음과 같은 악성 이메일을 목격했습니다.



A choice this election

NH ○ Nikki Haley <hi@alwaysright4u.com>
To: ○ dlee@davisleecompanies.com
Tuesday, 30 January 2024

FROM THE DESK OF
NIKKI R. HALEY

Friend,

This is a two-person race, and Americans have a chance to make a choice this election — a choice to move on from the politicians of the past and elect a candidate who not only can defeat Biden and Harris, but one who can lead our country into a brighter future.

So, as you make that choice, I want to remind you of something… **why I'm in this race and why I am the BEST candidate for the job.**

If you look at the facts…

We are over $34 trillion dollars in debt.

60% of Americans are living paycheck to paycheck. 50% of American families can't afford diapers, and 1 in 6 American families can't pay their utility bills.

Parents are worrying about what their children are being taught in the classrooms.

We've got an open border where terrorists can come through, and there are dangers all around us.

That's not us. That's not America.

We've got to stop focusing on the past and start focusing on what's going to make America **STRONG** and **PROUD**, which is exactly what I'm doing.

Will you join me TODAY?

DONATE

목차

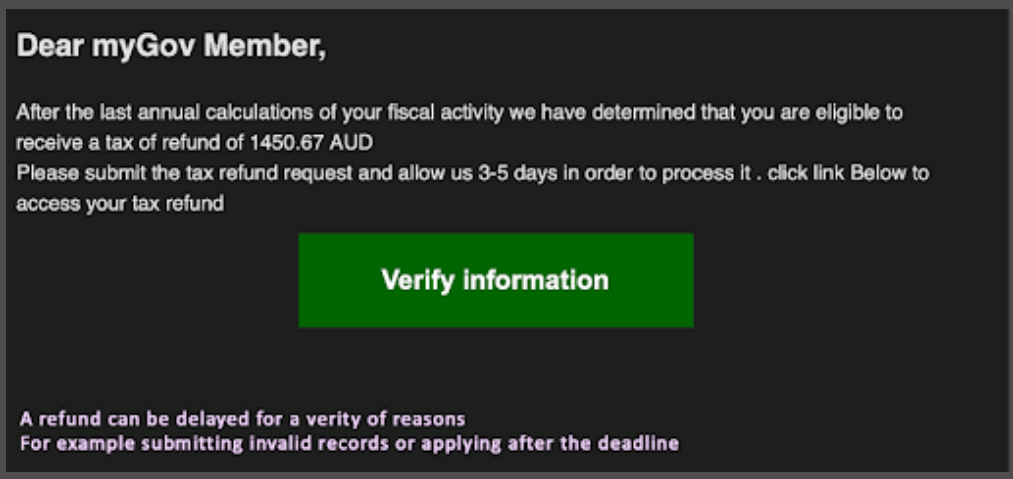
세금 피싱

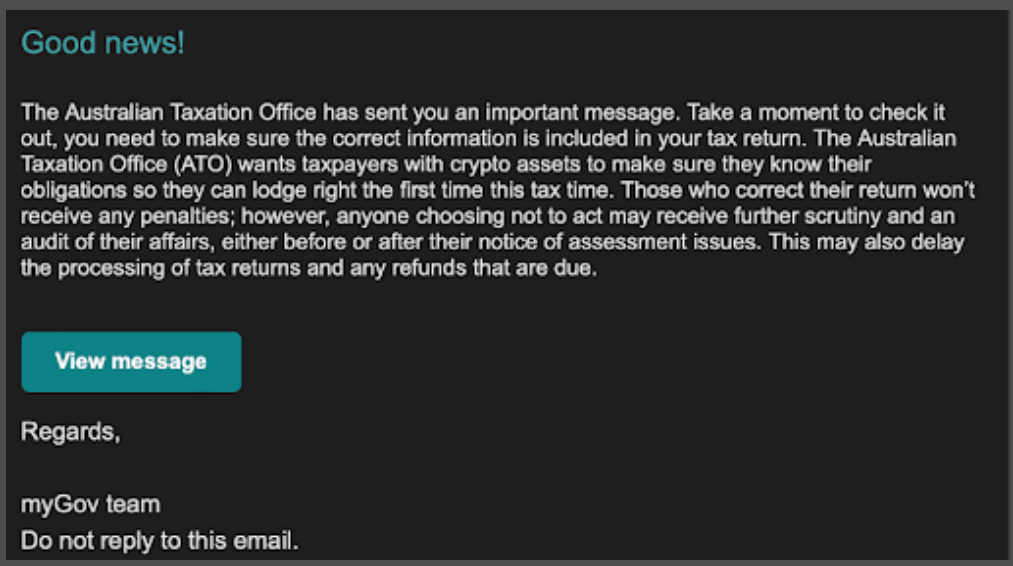
세금의 맥락에서 피싱 공격은 특히 우려됩니다. 사기꾼은 정부 기관, 세무 당국 또는 평판이 좋은 세금 신고 대행 서비스를 사칭하여 개인 정보를 유출하도록 속입니다. 미납 세금이 있거나 미신고된 신고서가 있거나 세금 환급을 받을 자격이 있다고 주장할 수 있습니다. 이들의 궁극적인 목표는 주민등록번호, 은행 계좌 정보 또는 기타 중요한 데이터를 확보하는 것입니다. 이 이메일에는 공식 정부 또는 세무 서비스 웹사이트로 연결되는 것처럼 보이지만 실제로는 데이터를 도용하도록 설계된 사기 사이트로 리디렉션되는 링크가 포함되어 있습니다.

또한 Trellix는 2024년 1분기 호주 세무당국을 가장하는 이메일이 급증하는 것을 관찰하고 이를 성공적으로 탐지했습니다.

목차

아래는 공격자가 세금 환급 관련 링크를 클릭하도록 유도하기 위해 급조한 캠페인의 한 예입니다.





GenAI 기술 발전 경쟁: 사이버 범죄 지하 조직으로부터 얻은 결과

AI와 머신 러닝은 더 이상 주머니 사정이 넉넉한 조직만 이용할 수 있는 것이 아닙니다. ChatGPT 등은 범죄자를 포함하여 누구나 이용할 수 있으므로, AI는 선한 행위자와 악한 행위자 사이의 군비 경쟁이 되었습니다. AI는 강력하고 추가 비즈니스 목표를 위해 책임감 있게 활용되어야 하지만, 공격자가 이점을 실현하지 못하도록 해야 합니다. 사이버 범죄자들의 전술이 점점 더 정교해지고 무기가 더 위험해짐에 따라 우리는 새로운 역량을 활용하여 사이버 범죄자들을 능가해야 합니다.

목차

CISO 팁: CISO의 역할은 이러한 진화하는 환경을 탐색하는 데 있어서 더욱 중요해졌습니다. 사이버 공격이 증가하고, AI에 대한 압박이 증가하고, 책임이 커지는 상황에서 CISO의 90%가 압박감을 느끼는 것은 당연한 일입니다. AI와 GenAI에 보조를 맞추는 것은 매우 중요하며, 거의 모든 CISO는 조직이 더 많은 일을 할 수 있다는 데 동의합니다. 자세한 내용은 Trellix의 최신 보고서인 CISO의 마음: GenAI 영향력 파악을 참조하십시오.

위협 행위자들은 가속화된 기능과 경제성 때문에 GenAI에 매력을 느낍니다. 가장 중요한 것은 전문성을 제공한다는 점입니다. 악의적인 행위자는 완벽한 문법, 로고, 로그인 정보를 사용하여 모든 언어로 스피어 피싱 이메일을 제작할 수 있습니다. 전문적인 기술이 없이도 exploit을 10배 더 빠르게 찾아서, 작성하고, 테스트할 수 있습니다.

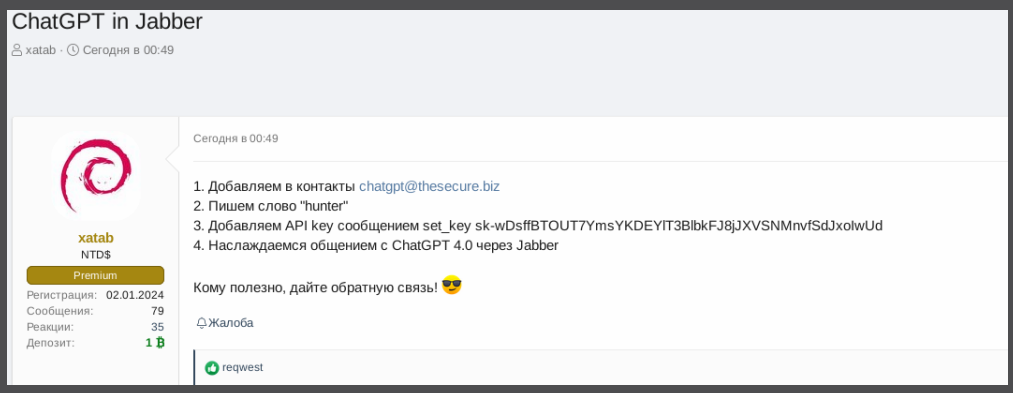
Advanced Research Center 팀은 정기적으로 사이버 범죄 지하 조직을 샅샅이 뒤져서 동향을 추적합니다. GenAI는 사이버 범죄자들 사이에서 가속화되고 있으며, 성공을 공유하고 도구를 판매하고 있습니다. 지난 보고서 이후 2024년 초부터 다음과 같은 내용을 관찰했습니다.

러시아 범죄 APT 그룹에 의해 사용되었을 가능성이 있는 'Jabber의 ChatGPT' 프로젝트

1월에 XSS 지하 조직 포럼의 프리미엄 행위자 **xatab**이 API 및 사용 방법에 대한 지침과 함께 "ChatGPT 4.0 in Jabber"를 만들 개발자를 찾는 것을 목격했습니다.

사이버 범죄자들이 LLM 통합을 수용하는 이외에 "ChatGPT in Jabber" 프로젝트의 배후에 있는 **xatab**의 의도/동기는 위협 행위자의 서신을 가로채서 수집하고, 그들의 요청을 도청하여 사이버 범죄자들이 무엇에 관심이 있는지, GenAI가 지원하는 불법 활동의 주요 주제와 범위는 무엇인지에 관한 인텔리전스와 지식을 얻기 위한 것일 수도 있습니다.

관찰된 내용은 다음과 같습니다.



XSS 포럼 지침 및 "ChatGPT in Jabber"에 대한 API 키에 공유된 **xatab**

목차

```
Python
1. Add to your contacts chatgpt@thesecure.biz
2. Write a keyword "hunter"
3. Add API key in the message: set_key <OPENAI_API_KEY>
4. Enjoy the conversation with  ChatGPT 4.0 via Jabber

If useful share your feedback!
```

2024년 1월 31일에 **xatab**은 XSS 포럼에서 "ChatGPT in Jabber" 프로젝트에 미화 2,000달러를 제공했습니다. 최근 요청받은 봇을 제작한 후 처음에 **xatab**에서 무시당한 **germans** 행위자가 제기한 XSS 불만을 바탕으로 **germans**가 Jabber용 ChatGPT 봇을 미화 1500달러에 개발하는 데 합의한 것으로 보입니다. 이 봇은 Exploit 포럼(@exploit[.]im)과 XSS(@thesecure[.]biz) Jabber 서버용으로 만들어졌으며, **xatab**은 이를 테스트하고 포럼 회원들로부터 피드백을 받기 위해 Exploit과 XSS 다크넷 포럼에 모두 게시했습니다. 이 봇은 xmppgpt 프로젝트를 기반으로 할 수 있습니다.

xatab 행위자는 Exploit/XSS 포럼에 자신들이 미국/영국/캐나다/호주 조직의 기업 액세스 브로커를 고용하여 유익한 협업을 하고자 하는 APT 팀(일부 업계에서는 숙련된 침투 테스터로 알려져 있음)임을 알리는 여러 게시물을 남겼습니다. 그들은 모든 액세스에 대해 수익 지분의 20%를 제공했으며 제안의 의도/진위를 보여주기 위해 Exploit 및 XSS 포럼에 하나의 BTC를 예치했습니다.

사이버 범죄 커뮤니티 **xatab**에 무료 ChatGPT 4.0을 제공하여 다음 두 가지를 실현합니다.

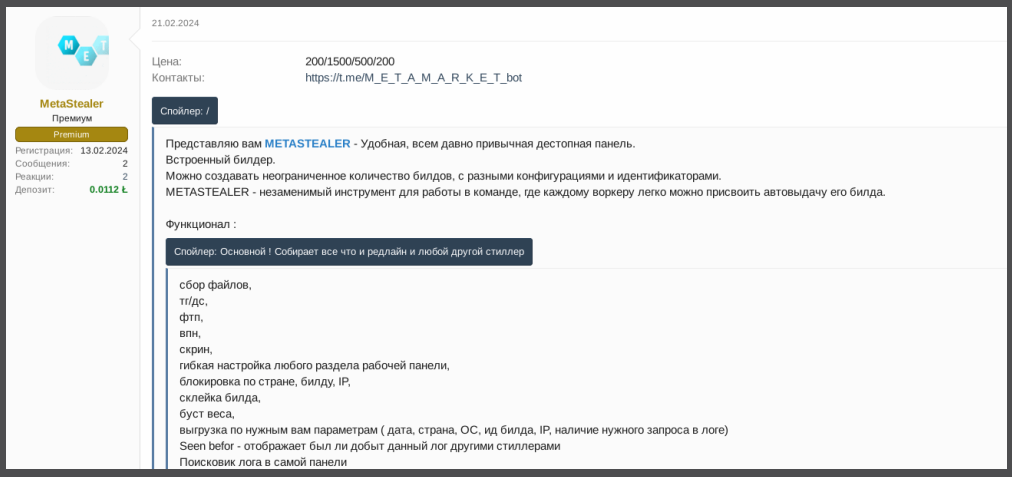
1. 위협 행위자가 혁신하고 GenAI를 운영에 도입할 수 있도록 지원하려는 조력자 및 지원자 지원
2. 다른 사이버 범죄자로부터 배우거나 혁신적인 아이디어와 도구를 도용하기 위해 GenAI 지식 기반/풀을 구축하려고 시도

Trellix는 주어진 지침에 따라 "ChatGPT in Jabber" 프로젝트를 테스트했으며 위협 행위자의 조언에 따라 작동하는 것으로 보입니다.

정보 탈취 프로그램에서 GenAI 채택

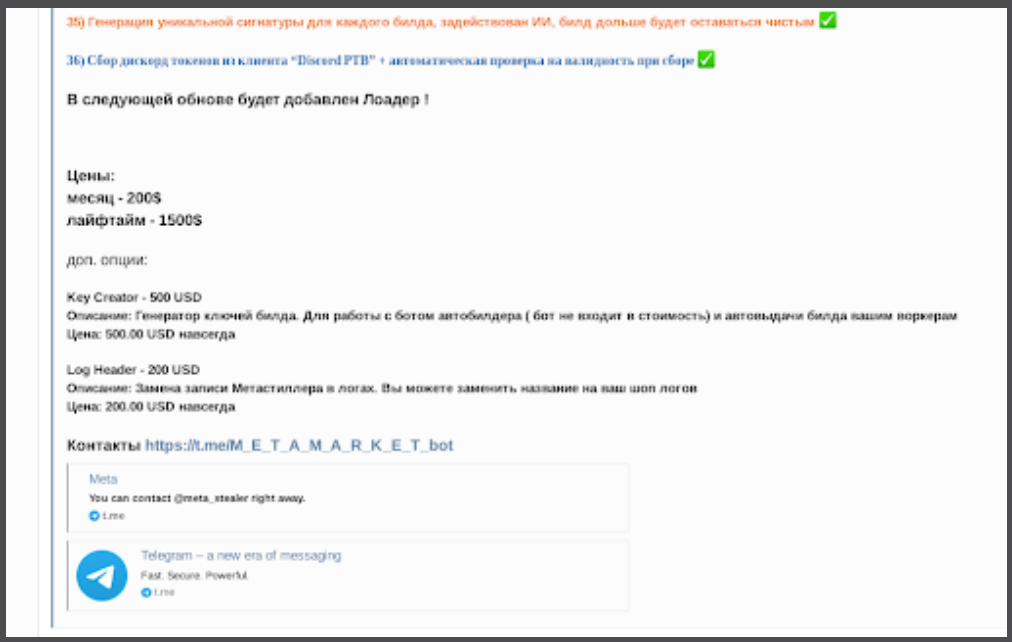
2024년 2월 21일, 저희 연구진은 위협 행위자인 MetaStealer가 XSS 포럼에서 새롭고 수정된 버전의 **MetaStealer**를 광고하는 것을 관찰했습니다. MetaStealer는 2021년에 처음 등장한 정보 탈취 프로그램으로 유명한 Redline의 분할 기업으로 여겨집니다. **MetaStealer**는 여러 버전이 활동하고 있지만, Trellix가 발견한 최근 버전에는 GenAI 기반 기능이 있어 탐지를 회피할 수 있습니다.

목차



XSS 포럼의 수정된 MetaStealer 버전에 공유된 **MetaStealer**

아래 스크린샷에서 35) 미만의 주황색 텍스트는 "모든 빌드에 대해 고유한 서명 생성, AI 사용, 장시간 선명하게(또는 탐지되지 않음) 유지되는 빌드"로 해석되며, MetaStealer 개발자들이 탐지를 회피하고 AV/EDR 시스템의 레이더 아래에 이전보다 긴 시간 동안 머물 수 있도록 MetaStealer의 고유한 빌드를 만들 수 있는 새로운 GenAI 기반 기능을 스틸러에 내장했음을 시사합니다.

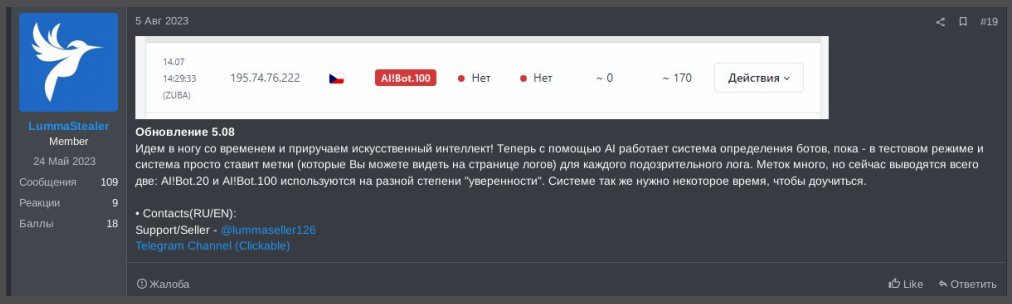


수정된 MetaStealer에는 방어 회피를 위한 GenAI 기반 기능이 내장되어 있습니다.

다른 예로는 LummaStealer라는 체계적으로 확립된 정보 탈취 프로그램이 있습니다. 2023년 8월부터 LummaStealer 팀이 AI 기반 기능을 테스트하여 정보 탈취 프로그램 사용자가 로그 목록에서 봇을 탐지할 수 있는 것을 목격했습니다. LummaStealer에 내장된 AI 기반 시스템은 잠재적으로 의심스러운 사용자 로그가 봇인지 아닌지를 탐지하도록 훈련된 맞춤형 신경망입니다. LummaStealer는 **AI!Bot.<숫자>** 레이블을 사용하여 탐지된

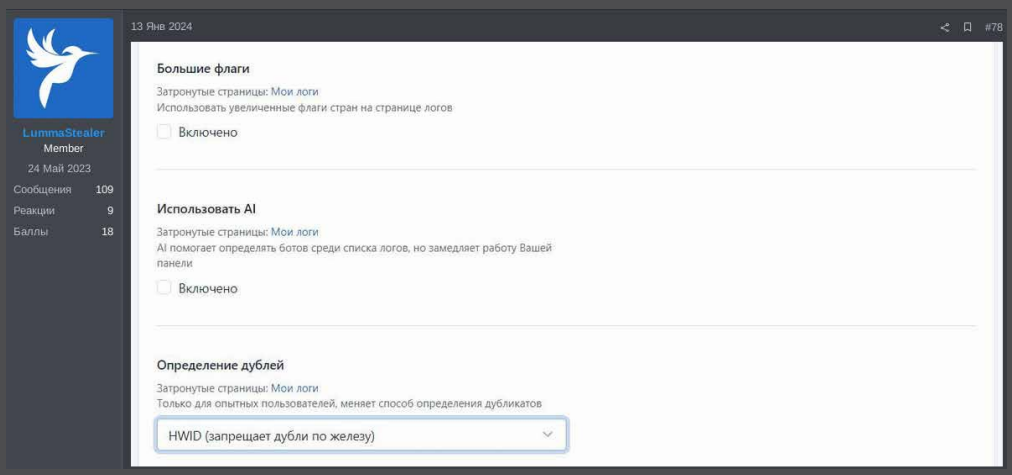
목차

로그를 봇으로 분류합니다. 여기서 <숫자>는 봇 탐지를 나타내는 0-100 범위인 것으로 보입니다.



LummaStealer는 RAMP 포럼에 그들의 정보 탈취 프로그램이 스틸러 로그 목록에서 봇을 탐지하는 AI 기반 기능을 갖추고 있다는 행위자의 조언을 게시합니다.

LummaStealer는 신경망이 여전히 교육 중이며 탐지 정확도를 향상시키는 데 시간이 걸릴 것이라고 사용자에게 조언했습니다. 2024년 1월에 **LummaStealer**는 GenAI 기반 기능이 LummaStealer 패널의 작업 속도를 늦추기 때문에 기본적으로 비활성화되어 있다고 조언했습니다.

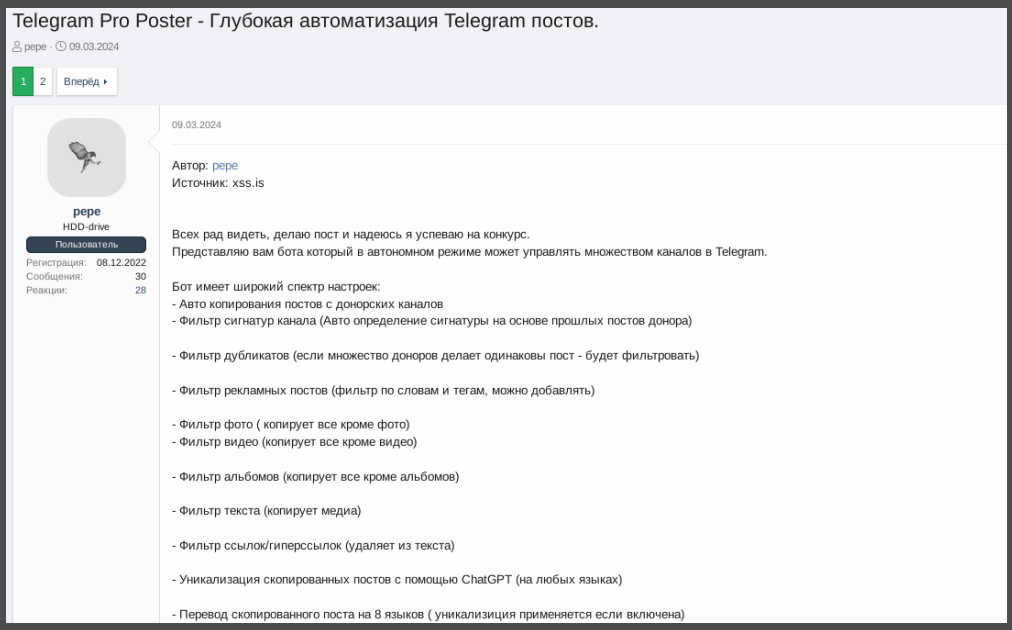


LummaStealer는 RAMP 포럼에 AI 기반 봇 탐지가 기본적으로 비활성화되어 있다는 행위자의 조언을 게시합니다.

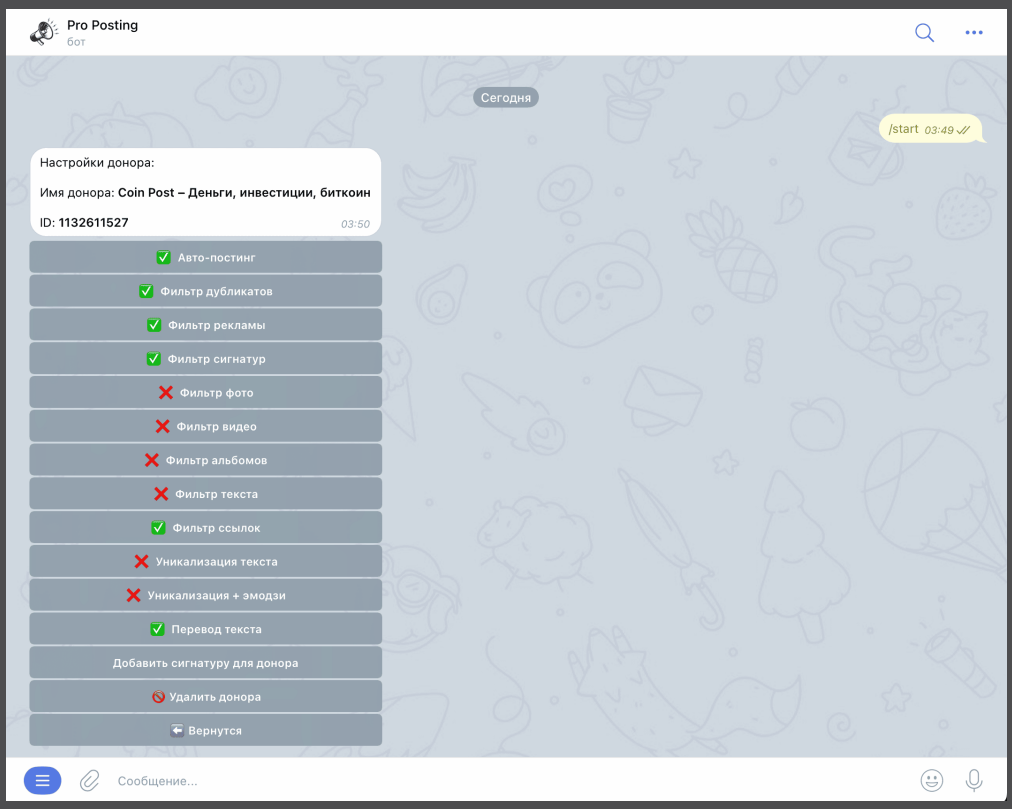
‘Telegram Pro Poster’의 봇 프로젝트

2024년 3월 초에 Trellix는 한 위협 행위자가 악성 도구/소프트웨어의 지하 경쟁의 일환으로 XSS 포럼에 "Telegram Pro Poster" 프로젝트를 게시하는 것을 목격했습니다. Telegram Pro Poster는 “Telegram 게시 심층 자동화”를 위한 봇입니다. 이 Python 기반 봇을 통해 사용자는 "기부자" 텔레그램 채널의 게시물을 대상 채널로 자동 복사하여 여러 개의 (무제한) 텔레그램 채널을 자율적으로 관리할 수 있습니다. 수많은 게시물 필터링 기능 중에서 이 봇은 텔레그램 메시지를 번역하고 ChatGPT를 사용하여 주어진 게시물을 구문 분석하기 위한 두 가지 GenAI 내장 기능을 갖추고 있습니다.

목차



Telegram Pro Poster GenAI 기반 봇에 관한 XSS 포럼 게시물



Telegram Pro Poster의 필터링 기능(기본적으로 비활성화되는 '고유화' 기능 포함)

Trellix는 Telegram Pro Poster의 소스 코드를 입수하여 ChatGPT API를 통해 기증자 채널에서 복사된 게시물을 대상 텔레그램 채널로 전송하기 전에 다음과 같은 8개 언어로 번역하는 다음 코드 조각을 확인했습니다.

목차

```
Unset
API_ID = 99999999 #APP TELEGRAM ID
API_HASH = "HASH" # APP TELEGRAM HASH
BOT_TOKEN = "API" # BOT API
DATABASE_PATH = 'database.db'
OPEN_AI_KEY = 'API KEY' # OPEN AI KEY


language_codes = {
    'Ukranian': 'украинский',
    'Russian': 'русский',
    'English': 'английский',
    'Indian': 'индийский',
    'Italian': 'итальянский',
    'Brasilian': 'бразильский',
    'Germany': 'немецкий',
    'Indonesian': 'индонезийский'
}
...
def gpt_translate(input_text, language):
    print(f'Перевожу этот текст: {input_text}')
    if len(input_text) > 10:
        openai.api_key = OPEN_AI_KEY
        language = language_codes[language]

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": f"Когда ты получаешь текст то ты
должен перевести его на {language}."},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        return unique_text
    else:
        return input_text
```

기본적으로 "고유화"라는 두 번째 기능은 비활성화되어 있지만, 이 기능이 켜지면 OPEN_AI_KEY를 사용하여 ChatGPT에 지정된 텍스트를 원하는 언어로 구문 분석하고 선택적으로 이모티콘을 추가하도록 요청합니다.

```
Python
def unique_text(input_text, is_emoji_need):
    print(f'Уникализирую этот текст: {input_text}')
    if len(input_text) > 5:
        openai.api_key = OPEN_AI_KEY

        if is_emoji_need:
            content_text = "Перефразируй текст и добавь эмодзи: "
        else:
            content_text = "Перефразируй текст:"

        response = openai.ChatCompletion.create(
            model="gpt-3.5-turbo",
            messages=[
                {"role": "system", "content": content_text},
                {"role": "user", "content": input_text}
            ],
        )
        unique_text = response.choices[0].message['content']
        token_count = response['usage']['total_tokens']
        return unique_text

    else:
        return input_text
```

목차

사이버 범죄자들의 XSS 커뮤니티에서는 이미 "Telegram Pro Poster 프로젝트"가 흥미로운 프로젝트이며 이 도구가 분명히 유용할 것이라는 긍정적인 피드백을 공유하고 있습니다. 또 다른 위협 행위자는 XSS 포럼 스레드에서 이 봇이 이미 다양한 텔레그램 채널에서 채택되고 있는 것을 목격했다고 조언했습니다.

후기

경쟁이 진행 중이다

운영 위협 인텔리전스는 특정 사이버 위협의 성격, 의도, 타이밍에 대한 인사이트를 제공합니다. 이는 위협 행위자의 전술, 기술, 절차(TTP) 관련 정보를 포함하여 전술 인텔리전스보다 더 상세하고 맥락적인 정보를 제공합니다.

조직에서는 운영 인텔리전스를 사용하여 사이버 공격의 배후에 있는 동기나 사용된 방법과 같은 광범위한 맥락을 이해할 수 있으므로 보안 팀이 특정 유형의 공격을 예측하고 대비할 수 있도록 도와줍니다.

고객과의 작업에서 모든 CISO의 가장 중요한 목표는 조직에 대한 위험을 제한하는 것입니다. 운영 위협 인텔리전스를 적용하는 것은 CISO와 SecOps 팀이 앞을 내다보고 입지를 다질 수 있도록 하여 이러한 위험을 제한할 수 있는 가시적인 방법입니다. 이를 통해 조직 전반에서 보안 조치의 부족한 부분을 파악하고 상대방의 마음속에 들어가 상대방을 정상 궤도에서 벗어나게 할 수 있습니다.

Trellix는 Trellix만의 위협 인텔리전스를 공유하여 사실 기반의 견고한 플랫폼을 제공함으로써 귀하가 내려야 할 몇 가지 중요한 의사 결정을 지원합니다. Trellix의 목적은 사이버 방어를 획기적으로 개선하고 무엇을 선택하든 다음 단계에서 공격자를 물리치도록 돕는 것입니다.

함께 시작합시다!

Ashok Banerjee,
최고 기술자, TRELLIX

목차

방법론

수집: Trellix와 Trellix Advanced Research Center의 세계적 수준의 전문가들은 광범위한 글로벌 소스로부터 통계, 동향 및 인사이트를 수집하여 이 보고서를 구성합니다.

- **전속 소스:** 경우에 따라 텔레메트리은 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 예리한 특성을 활용하여 데이터를 정규화하고, 결과를 풍부하게 하고, 개인 정보를 제거하며, 공격 방법, 에이전트, 섹터, 지역, 전략 및 결과 간의 상관관계를 파악하는 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.

응용 분야: 이 정보를 사용하는 방법

업계를 선도하는 모든 평가 팀과 프로세스는 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.

목차

- 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 파악하고, 사이버 방어에서 모범 사례를 알리고 이를 가능하게 하는 데이터에 대한 합리적이고 전문적이며 윤리적인 해석을 개발하고자 하는 본 보고서의 목적에 가장 적합한 유형의 연구입니다.

본 보고서의 분석을 이해하는 방법

본 보고서에 나와 있는 인사이트와 데이터를 이해하려면 다음 지침을 간단히 검토해야 합니다.

- **일시적인 현황:** 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(false positive) 및 잘못된 부정:** 데이터를 수집하기 위한 Trellix의 특수 추적 및 텔레메트리 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:** 텔레메트리에 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 텔레메트리가 포함됩니다.
- **국가 책임 규명:** 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.

목차

리소스

위협 보고서 보관

The Mind of the CISO

X에서 TRELLIX ARC를 팔로우하세요.

Trellix ARC

이전의 사이버 위협 보고서 보기

Trellix Advanced Research Center

목차

TRELLIX ADVANCED RESEARCH CENTER 정보

Trellix Advanced Research Center는 글로벌 사이버 위협 환경에서 사이버 위협 행위자가 사용하는 새로운 방법, 동향 및 도구에 대한 연구를 선도하고 있습니다. 저희 연구원으로 구성된 엘리트 팀은 전 세계 CISO, 수석 보안 리더 및 보안 운영 팀의 최고 파트너 역할을 합니다 Trellix Advanced Research Center는 보안 분석가에게 최첨단 콘텐츠를 통해 운영 및 전략적 위협 인텔리전스를 제공하고 업계 최고의 AI 기반 XDR 플랫폼을 구축하며 전 세계 고객에게 인텔리전스 제품 및 서비스를 제공합니다. 자세한 내용은 https://www.trellix.com/ko-kr/advanced-research-center.html을 참조하십시오.

TRELLIX 소개

Trellix는 사이버 보안과 세상을 바꾸는 기술의 미래를 혁신하는 글로벌 기업입니다. 오늘날 최첨단 위협에 직면한 조직은 Trellix가 보유한 개방형 XDR(eXtended detection and response) 플랫폼을 통해 확실히 운영을 보호하고 복원할 수 있습니다. Trellix는 광범위한 파트너 에코시스템과 더불어 인공 지능, 자동화, 분석을 통해 기술 혁신을 가속함으로써 40,000곳 이상의 기업 및 정부 고객에게 실시간 보안을 지원하고 있습니다. 자세한 내용은 https://trellix.com을 참조하십시오.

목차