2025

elastic security labs

글로벌 위협 연구 보고

개요

인내심을 갖고 은밀하게 공격하던 시대에서 이제 새로운 고속 위협의 시대로 옮겨가고 있습니다.

연도별 분석을 통해 뚜렷한 전략 변화가 확인되었습니다. 공격자들은 속도를 높이기 위해 전술을 재정비하고, AI를 무기화해 새로운 위협을 대규모로 생성하며, 장기적인 잠복보다는 즉각적인 실행을 택하고 있습니다. 공격 주기가 몇 달에서 몇 분으로 단축되면서, 이제는 실시간 및 과거 데이터를 활용해 신속하게 컨텍스트 중심적인 결정을 내릴 수 있어야 성공적으로 방어할 수 있게 되었습니다.

Elastic Security Labs의 2025년 Elastic 글로벌 위협 보고서에서는 이 새로운 환경을 분석합니다.

글로벌 위협 원격 분석에 대한 분석을 바탕으로 가장 중요한 공격자의 행동과 방어 혁신을 파악했습니다. 학습할 내용을 미리 살펴보면 다음과 같습니다.

#01

Windows에서 적의 우선순위가 바뀌었습니다.

전술 범주의 하나인 **실행**이 이제 악성 행위의 **32.1%**를 차지하며, 이전의 약 16%에서 두 배로 증가하여 **방어 회피**를 앞서는 최고 전술로 부상했습니다. 이는 지난 3년 간의 흐름을 뒤집는 변화로, 공격자가 초기 은폐보다 즉각적인 페이로드 실행을 우선시하는 전략으로 전환하고 있음을 보여줍니다.

2025 **32.1%**

2024 ~16%

이것이 고객에게 의미하는 바

→ 공격자들은 더 이상 숨으려 하지 않고, 침입하자마자 악성 코드를 실행하는 데 집중하고 있습니다. 이는 런타임 메모리 보호와 초기 액세스 방지가 중요해지고 있음을 보여줍니다.

#02

클라우드 공격 표면은 매우 집중되어 있습니다

모든 클라우드 보안 이벤트의 60% 이상이 단 세 가지 적대적 목표로 귀결됩니다.

공격자의 목표

/초기 침투
/지속성 유지
/자격 증명 액세스

이것이 고객에게 의미하는 바

→ 모든 주요 클라우드 플랫폼에서 **ID 기반 공격**에 집중하고 있는 것은 인증 흐름을 강화하고 비정상적인 권한 액세스를 모니터링하는 것이 클라우드 워크로드를 방어하는 가장 효과적인 방법이라는 분명한 신호입니다.

#03

AI 무기화의 증가

+15.5%

'일반' 위협은 15.5% 증가했습니다. 이는 공격자들이 대규모 언어 모델(LLM)을 이용해 단순하지만 효과적인 악성 로더와 도구를 신속히 만들어내고 있기 때문으로 보입니다.

이것이 고객에게 의미하는 바

→ AI로 생성된 위협이 확산하면서, 악성 코드의 양과 다양성이 폭발적으로 증가하고 있습니다. 이제는 정적 시그니처보다 **행동 기반 분석과 AI 탐지 기술**을 활용해 새로운 위협을 대규모로 자동 식별하고 차단해야 할 때입니다.

#04

심각한 문제인 브라우저 인증 정보 도용

> 8명 중 1명

브라우저 데이터를 훔치도록 설계

150,000개 이상의 악성 코드 샘플 분석 결과, **전체의 8분의 1 이상이 브라우저 데이터를 탈취하도록 설계**된 것으로 확인되었습니다. 이러한 자격 증명은 단순히 한 번의 공격에 사용되는 것이 아니라, **액세스 브로커 경제**를 탈바꿈하는 주요 자산으로 활용되어 다른 공격자들에게 기업 클라우드 계정을 침투할 수 있는 열쇠를 꾸준히 공급하고 있습니다.

이것이 고객에게 의미하는 바

→ 브라우저는 조직의 가장 민감한 데이터가 노출될 수 있는 주요 공간입니다. 정보 탈취형 악성 코드가 브라우저의 내장 보안 기능을 우회하도록 진화하면서, 기존의 ID 보호만으로는 이를 막기 어려운 실정입니다.

이러한 추세는 서로 깊이 연결되어 있습니다.

공격자는 AI로 생성된 악성 코드를 사용하여 브라우저 자격 증명을 탈취한 후, 이를 사용해 클라우드 계정에 대한 액세스 권한을 얻을 수 있습니다. 일단 침투하면 즉시 랜섬웨어를 배포하거나 데이터를 탈취하기 위해 실행에 집중합니다. 이 보고서는 이러한 TTP가 어떻게 최신 공격 체인을 형성하는지, 그리고 더 중요한 것은 여러 지점에서 공격 체인을 어떻게 차단할 수 있는지 보여줍니다.

위협 환경은 복잡하지만, 악성 코드와 위협 행동을 이해하고 고급 방어 체계를 활용하면 복원력을 크게 개선할 수 있습니다.

1단계
실행에 집중

2단계
클라우드 계정에 대한 초기 액세스 권한 확보

3단계
AI로 생성된 악성 코드 활용

4단계
브라우저 자격 증명 탈취

Elastic Security는 오늘날의 위협을 탐색하고 보다 안전한 미래를 구축하기 위한 공유 인텔리전스, 고급 기능 및 인사이트를 제공합니다.