elastic security labs

2022년 글로벌 위협 보고서

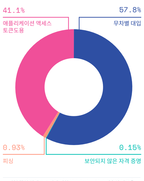
인포그래픽

위협은 어디에서 오는 걸까요?

Elastic Security Labs의 2022년 글로벌 위협 보고서는 솔루션 원격 분석을 기반으로 위협 현상, 동향 및 조직이 미래를 준비하는 데 도움이 되는 권장 사항을 보여줍니다. 조사 결과는 다음과 같습니다...

실제 클라우드는 관리자가 기본적으로 설정된 항목에 대한 추가 보안 제어를 수동으로 구현할 때 안전해집니다

자격 증명 액세스 경보의 거의 41%가 다양한 자격 증명 항목 중 애플리케이션 액세스 토큰을 도용하려는 시도에서 발생했습니다.



자격 증명 액세스 수법에 대한 MITRE ATT&CK 기술의 백분율

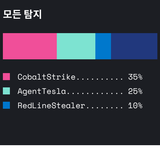
일단 공격자가 내부에 들어오면 자격 증명 액세스가 우선 순위입니다

클라우드 기반 탐지 경보에 대한 MITRE ATT&CK 수법 이름의 백분율

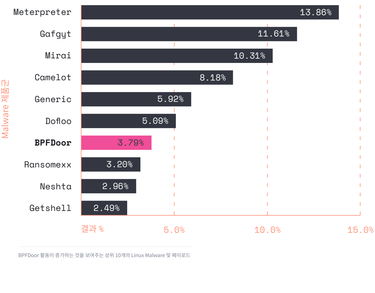
상용 소프트웨어가 무기화되고 있습니다

레드 팀을 위해 설계된 Malware가 조직을 상대로 사용되고 있습니다.

CobaltStrike는 Windows 엔드포인트에서 가장 인기 있는 악성 바이너리 또는 페이로드였고, AgentTesla와 RedLineStealer가 그 뒤를 이었습니다.

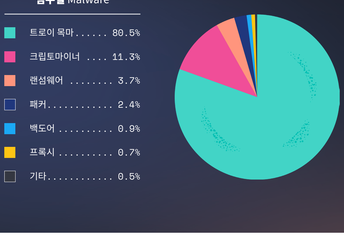


개방형 소프트웨어는 생각보다 안전하지 않습니다



BPFDoor 활동이 증가하는 것을 보여주는 상위 10개의 Linux Malware 및 페이로드

트로이 목마는 계속해서 결과물을 무기화하는 데 선호되는 방법입니다



좋은 소식 – 엔드포인트 보안이 작동 중입니다

엔드포인트 공격은 방어를 우회하려는 노력에서 점점 다양해지고 있습니다. 올해 우리는 효과가 없었던 50개의 다른 엔드포인트 침투 기술을 관찰했습니다.

기술	신호 퍼센트
가장	44.29%
시스템 바이너리 프록시 실행	30.00%
액세스 토큰 조작	12.32%
프로세스 인젝션	7.62%
BITS 작업	4.74%
신뢰할 수 있는 개발자 유틸리티 프록시 실행	0.90%
XSL 스크립트 프로세싱	0.66%
방어력 약화	0.65%
방어 회피 공격	0.64%
시스템 스크립트 프록시 실행	0.13%
레지스트리 수정	0.03%
호스트상의 지표 제거	0.01%

2022년 글로벌 위협 보고서에서 Elastic Security Labs 연구원들의 연구 결과를 모두 확인해 보세요