전반적인 위협 환경

여기에서 전체 영어 보고서를 다운로드하십시오

Talos는 2022년의 위협 환경에 대한 몇 가지 주요 동향을 관찰했습니다. Cisco Talos Incident Response 인게이지먼트의 텔레메트리 및 고객 사례를 통해 우리는 공격자들이 유명한 레드팀 툴들의 크랙/유출 버전을 이용하고 PowerShell이나 Microsoft PS Exec과 같은 LOTL 바이너리(LoLBins)를 악용하는 것을 확인했습니다. 또한, USB 공격도 크게 늘었습니다.

이중 용도 툴

공격자 입장에서는 악성 툴을 개발하는 과정에서 자원이 많이 소모될 뿐만 아니라, 추적 당할 위험까지 있습니다. 이러한 부담을 피하고 익명성을 높이기 위해 많은 공격자들이 공격 라이프사이클 전반의 다양한 활동을 지원하는 레드팀 프레임워크로 눈길을 돌리고 있습니다.

Cobalt Strike는 공격자들 사이에서 지금까지도 큰 인기를 끌고 있습니다(그림 1). 이 합법적인 네트워크 보안 툴 겸 위협 에뮬레이션 소프트웨어는 정찰, 후속 공격 활동 및 다양한 공격 시뮬레이션을 포함한 폭넓은 기능을 지원하기 때문에 공격자 입장에서도 매우 유용합니다.

Talos와 보안 커뮤니티는 보다 효과적이고 강력한 탐지 기술을 개발하면서 오랫동안 Cobalt Strike를 다뤄 왔습니다. 올해 우리는 위협 행위자들이 Sliver나 Brute Ratel(그림2)과 같은 공격 프레임워크로 선회하는 모습도 볼 수 있었습니다.

또한 Talos는 위협 행위자들이 자체적으로 개발한 Manjusaka와 Alchimist라는 공격 프레임워크도 발견했습니다. Alchemist는 실환경에서 이미 사용되고 있습니다. 아직 널리 사용되고 있지는 않지만 Manjusaka 역시 공격자들 입장에서는 매력적인 옵션입니다.

LOTL 바이너리

LOTL 바이너리(LoLBins)는 한 운영체제에 사전 설치되는 합법적인 유틸리티 및 툴로서 공격자들 사이에서 널리 이용되고 있습니다. LOTL 바이너리는 일상적으로 이용되는 신뢰할 수 있는 툴인 만큼 네트워크 보안 담당자들이 악의적 행동을 모니터링할 때 이를 활용한 공격을 간과할 수 있습니다. 공격의 모든 단계에서 이처럼 합법적인 툴과 유틸리티를 활용하는 공격자들이 계속 관찰되고 있습니다.

Talos의 텔레메트리에 따르면 가장 많이 발생한 Cisco Secure Endpoint Behavioral Protection

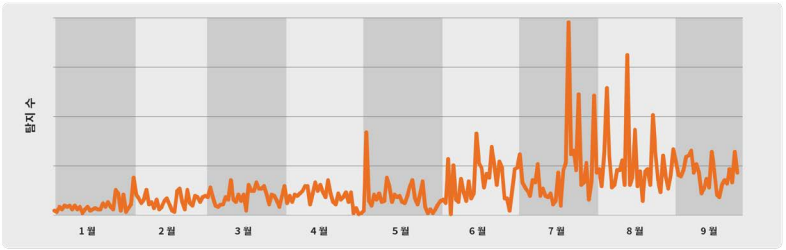

그림 1. Cisco Secure Endpoint의 Cobalt Strike 파이프 사용 탐지 수.

Cobalt Strike

- 이 합법적인 네트워크 보안 툴 겸 위협 에뮬레이션 소프트웨어는 정찰, 후속 공격 활동 및 다양한 공격 패키지를 포함한 폭넓은 기능을 지원하기 때문에 공격자 입장에서도 매우 유용합니다.
- 비컨(beacon)은 공격을 생성하고 HTTP, HTTPS 또는 DNS를 통한 아웃바운드 트래픽을 생성하기 위한 Cobalt Strike의 페이로드입니다. Cobalt Strike 비컨은 Metasploit 프레임워크의 일부인 미터프리터(meterpreter)와 비교할 만한 것으로, 침투 시험자나 공격 보안 연구자들의 업무에 사용될 수 있습니다.

Brute Ratel

- 2020년에 공격 시뮬레이션 툴로 출시된 합법적인 고급 레드팀 툴입니다. 출시 이후 위협 행위자들이 공격 라이프사이클의 여러 단계를 지원하기 위해 사용해 왔습니다.
- Brute Ratel은 엔드포인트 탐지 및 대응(EDR) 및 안티바이러스(AV) 솔루션에 의한 탐지를 회피하도록 설계되었습니다.

Sliver

- 보안 테스트에 사용할 수 있는 오픈 소스 레드팀 프레임워크 및 공격 시뮬레이션 툴입니다. Silver의 임플란트는 바이너리별 비대칭 암호화 키와 동적으로 컴파일링되며 일부 프로토콜(mTLS, HTTP, DNS)에서 C2를 지원합니다.
- Silver 임플란트는 MacOS, Windows 및 Linux에서 지원됩니다. Silver는 Staged 및 Stageless 페이로드, 동적 코드 생성, 명명된 파이프 피벗, 인메모리 .NET 어셈블리 실행 등 다양한 기능을 지원합니다.

그림 2.주요 이중 용도 툴 비교.

전반적인 위협 환경

시그니처 25개 중 4개가 PowerShell 관련 시그너처입니다. 이는 위협 행위자들이 악의적 목적으로 이 네이티브 Windows 유틸리티 프로그램을 꾸준히 이용하고 있음을 보여줍니다(그림 3). 공격자들은 PowerShell을 이용하여 ChromeLoader와 같은 애드웨어를 설치하고, 가상자산 채굴 프로그램을 다운로드하고, Elasticsearch와 같은 소프트웨어의 취약점을 악용하는 등 다양한 활동을 펼칩니다.

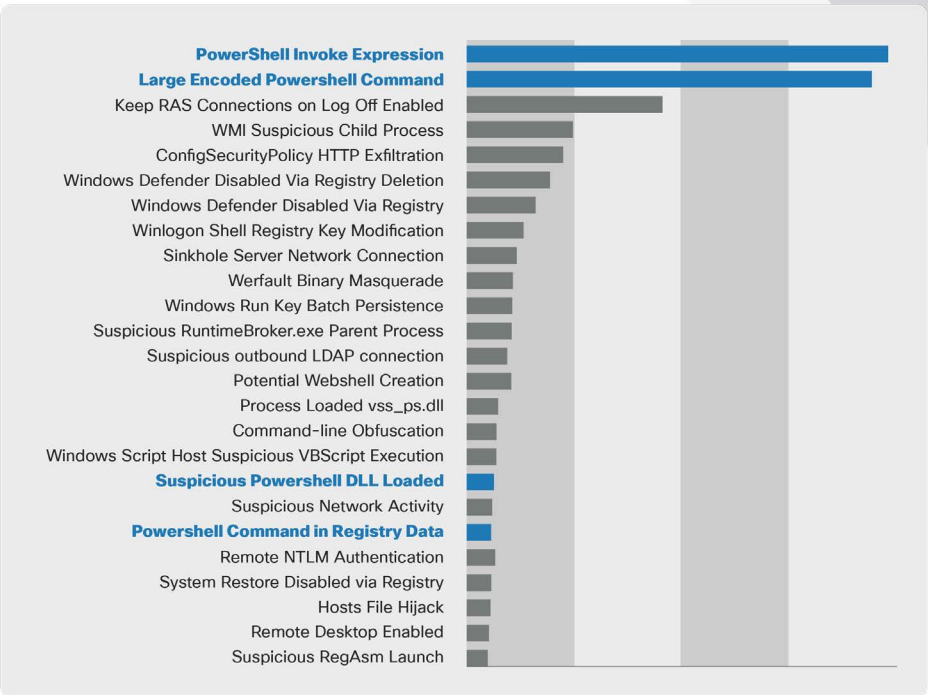

그림 3. 가장 많이 발생한 Cisco Secure Endpoint Behavioral Protection 시그너처 상위 25개.

USB 위협

이동식 저장장치를 이용한 멀웨어 유포는 플로피 디스크 시절부터 이용되던 방식입니다. 2022년에도 Talos는 Cisco Secure Malware Analytics를 통해 USB나 외장 하드를 이용한 공격을 다수 확인했습니다. 아직도 공격자들이 이 오래된 전술을 효과적으로 사용하고 있다는 뜻입니다. USB 드라이브에 실행파일을 저장하는 수법이나 USB 드라이브에 있는 파일이 탐지되지 않도록 숨김 설정을 하는 수법이 대표적입니다(그림 4, 5).

USB 위협이 증가한 원인 중 하나로 꼽히는 것이 Raspberry Robin멀웨어입니다. 이 멀웨어는 USB 드라이브를 통해 다른 디바이스로 확산됩니다. 지능형 지속 공격(APT) 단체들 역시 USB 드라이브를 공격에 이용하는 것으로 확인되었습니다.

2022년에 USB 공격이 다시 증가했습니다. 공격자들은 구형 공격 벡터에 대한 기업들의 관심이 멀어지는 틈을 노릴 것으로 보입니다.

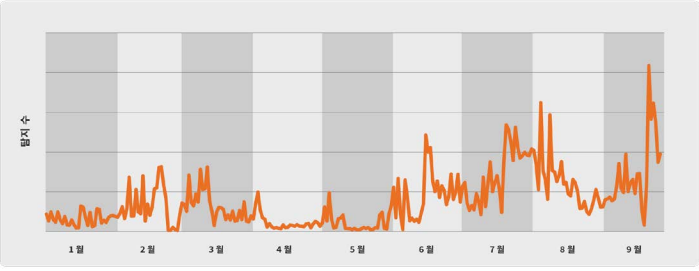

그림 4. Cisco Secure Malware Analytics의 USB 저장 실행파일 탐지.

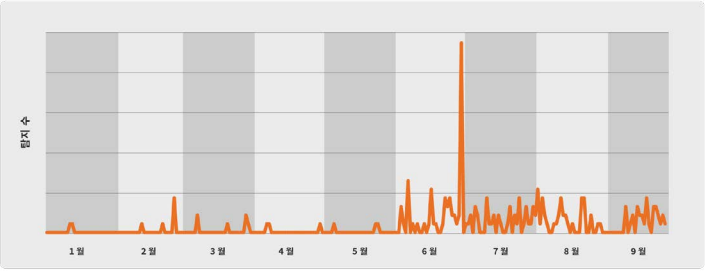

그림 5. Cisco Secure Malware Analytics의 USB 저장 파일의 숨겨진 속성 설정 탐지.

