# 우크라이나

여기에서 전체 영어 보고서를 다운로드하십시오

올해 Talos의 주요 운영 목표 중 하나는 우크라이나에 대한 지속적 지원이었습니다. Talos는 우크라이나 국민과 인프라의 보호라는 핵심 미션을 수행하기 위해 역내 Talos 고객과 파트너 보호를 전담하는 40명 이상 규모의 태스크포스를 출범했습니다. 이 전문가 팀은 중요한 인프라 고객들을 모니터링하여 위협을 식별하고 공격으로 발생한 문제를 해결하고 정보를 수집합니다.

## 주요 공격자 및 위협

다음은 2022년에 Talos가 관찰한 우크라이나의 단체들과 협력 단체들을 겨냥한 주요 공격자와 위협의 목록입니다.

- 우크라이나 침공 전후로 Talos는 WhisperGate, HermeticWiper, CaddyWiper, DoubleZero, CyclopsBlink를 포함하여 우크라이나의 타깃을 겨냥한 치명적 와이퍼 공격과 기타 멀웨어를 확인했습니다.
- 한편, 공격자들은 러시아 단체를 겨냥한 멀웨어를 사이버 툴이라고 광고하고, 해당 사태와 관련된 주제로 이메일을 발송하여 금융 사기를 치거나 원격 액세스 트로이목마 바이러스를 배포했습니다.
- 러시아 국가 주도 그룹인 Gamaredon은 정보 탈취 멀웨어를 배포했고, 국가의 지원을 받는 것으로 의심되는 한 개인 행위자는 GoMet이라는 공격망 공격을 시도했습니다.
- 중국의 위협 행위자인 Mustang Panda는 가짜 "공식" 문서를 미끼로 유럽과 러시아의 단체들을 겨냥한 피싱 활동을 했습니다.
- 러시아 국가 주도 핵티비스트 단체인 Killnet은 친우크라이나 국가들의 웹사이트를 대상으로 DoS 공격을 감행했습니다.

## 행동 동향

2022년부터 수집한 데이터를 통해 우리는 다음과 같은 우크라이나 내 공격 동향을 확인할 수 있었습니다.

- PowerShell이나 WMI와 같은 일반 유틸리티 프로그램은 아직도 "LOTL(live-off-the-land)" 공격과 탐지 회피를 모색하는 공격자들의 주요 타깃입니다.
- Google Chrome 실행파일이나 Windows Policies Keys를 이용하는 식으로 지속 공격을 수행하는 기법이 증가했습니다.
- 정보 탈취자 및 가상자산 채굴자 탐지도 늘었습니다. 그러나 우리는 주로 파괴적 공격 활동을 펼치는 다양한 수준의 행위자들을 관찰합니다.
- 우리는 “Signed binary proxy execution using rundll32”에 대한 경보 건수가 우크라이나뿐만 아니라 전 세계적으로도 크게 증가한 것을 관찰했습니다. 이것은 동적 링크 라이브러리(DLL)를 이용해 악성 코드를 실행하는 기법입니다.

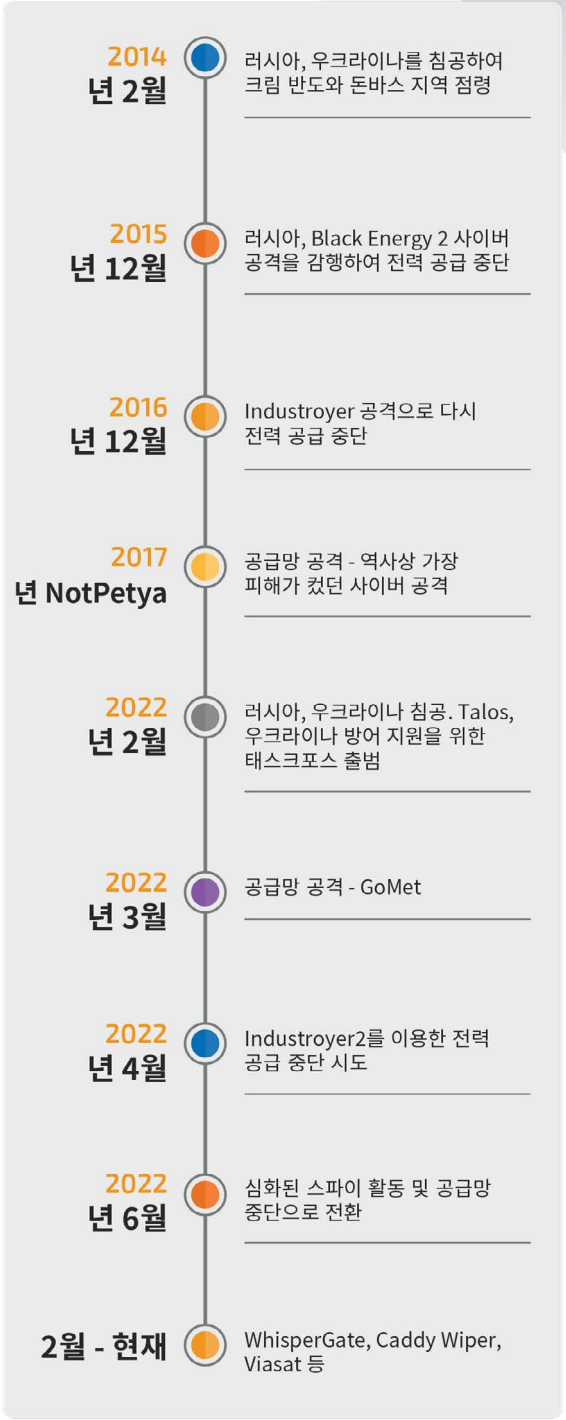


**그림 1.**우크라이나를 겨냥한 주요 사이버 공격.

# 우크라이나

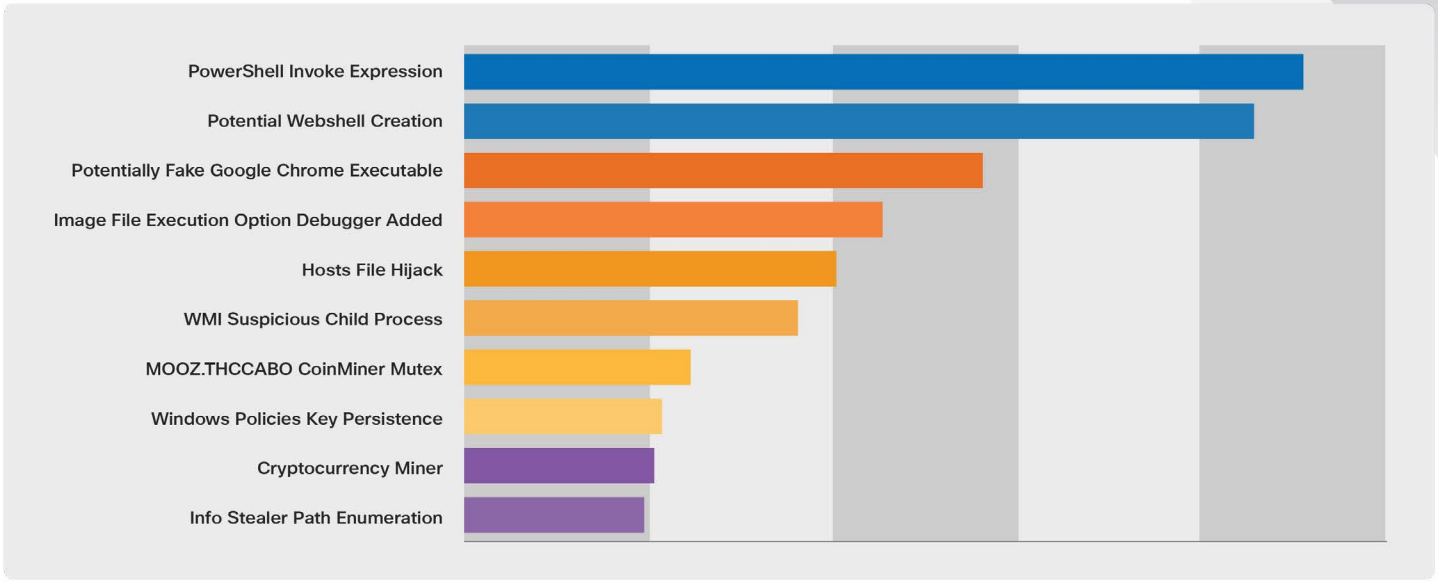


**그림 2.** 우크라이나의 Cisco Secure Endpoint 이용 고객들이 가장 많이 사용한 Cisco Secure Endpoint의 Behavioral Protections 규칙.

**우크라이나 내 타깃에 대한 공격 활동은 증가했지만, 2022년 상반기 중 시스코 고객을 겨냥한 위협은 전반적으로감소했습니다. 이는 원래 다른 지역에서 공격 활동을 했을 위협 행위자들이 우크라이나 사태로 인해 해당 지역으로 몰리게 된 결과일 수 있습니다.**

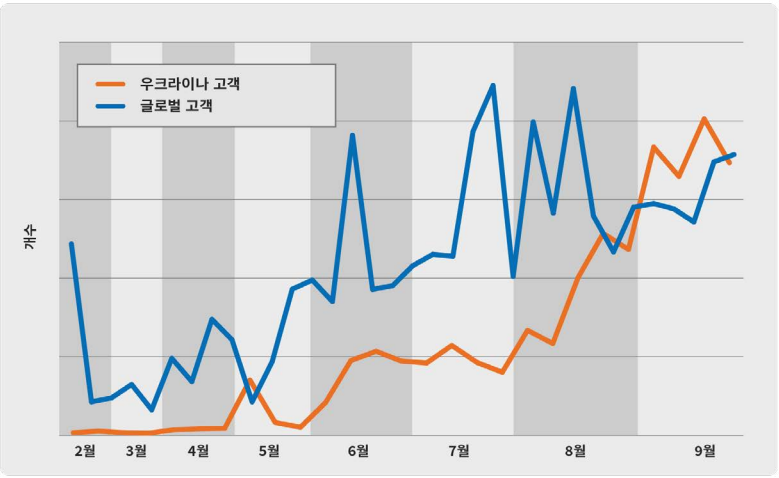


**그림 3.** 2022년 2월부터 9월까지 우크라이나 고객 및 글로벌 고객 대상 “Signed binary proxy execution using rundll32”에 대한 Exploit Prevention 탐지 건수.

## 결론

우크라이나를 겨냥한 사이버 공격이 둔화되고 있다거나 교전이 중단되면 반드시 이러한 사이버 전쟁도 종식될 것이라는 조짐은 어디에도 없습니다. 역내 긴장감과 이번 사태에 뛰어든 위협 행위자들의 다양성을 고려하면 우크라이나를 겨냥한 공격은 아마도 계속될 것으로 보입니다. 나아가 우리는 러시아의 사이버 위협 행위자들이 이번 전쟁의 결과에 영향을 주기 위해 필요한 파괴적 공격들을 감행할 가능성이 높다고 봅니다.

 