지능형 지속 공격(APT)

여기에서 전체 영어 보고서를 다운로드하십시오

2022년에는 지정학적 환경이 크게 변화함에 따라 국가 주도 지능형 지속 공격(APT)의 양상도 달라졌습니다. Cisco Talos는 러시아, 이란, 중국, 북한 및 인도 아대륙 국가의 몇몇 단체와 관련된 사이버 공격을 확인했습니다. 이 단체들은 스파이 활동, 지적재산 탈취, 치명적 멀웨어 배포 등 다양한 악의적 활동을 펼쳤습니다. 그중에서도 특히 다음과 같은 주요 동향이 관찰되었습니다.

- 신종 커스텀 멀웨어 및 기존 멀웨어의 변종
- Log4j 유틸리티와 같은 공개된 취약점 악용
- 탐지 회피를 위한 툴링 및 행동 패턴의 업데이트
- 이란 정부 주도 MuddyWater 그룹과 중국 정부와 연관된 조직의 APT 등 CTIR(Cisco Talos Incident Response) 인게이지먼트에서 APT 활동 증가

러시아

2022년에 Talos가 확인한 정부 주도 단체들로서, 2월 우크라이나 침공 전까지 두드러진 활동을 보인 단체들은 다음과 같습니다.

Fancy Bear

러시아군 정보 기관인 GRU(Directorate of the General Staff) 소속으로 의심되는 단체입니다.

- 침공 몇 주 전 발생한 와이퍼 공격인 WhisperGate에서 관찰된 것과 유사한 TTP(tactics, techniques, and procedures)를 사용했습니다.

Gamaredon

크림 반도에서 러시아 정부의 지원을 받아 활동하는 것으로 의심됩니다.

- 정보 탈취 멀웨어로 우크라이나 정부 사용자들을 감염시켜 민감한 데이터를 유출하기 위한 대규모 스피어피싱 공격을 감행했습니다.

Turla

러시아 연방보안국(FSB)과도 일부 연계된 러시아 단체입니다.

- 워터링 홀, 스피어피싱, 소셜 엔지니어링 기법, 알려진 취약점 악용 및 Crutch나 Gazer와 같은 커스텀 백도어 등을 이용해 나토 회원국과 구소련 국가의 공공 및 민간 단체를 겨냥한 고도로 표적화된 활동을 진행하고 있습니다.

이란

이 단체들은 지적 재산 탈취와 정보 수집을 주 목적으로 전 세계에서 사이버 공격을 감행합니다. 이들은 랜섬웨어나 기타 치명적 멀웨어를 배포하기 위한 기술적 수단을 보유하고 있을 가능성이 큽니다.

MuddyWater

종합적으로 검토를 해본 결과, MuddyWater는 특정 국가나 지역을 겨냥하는 다수의 하위단체들로 구성된 것으로 판단됩니다.

- MuddyWater의 하위단체들은 각자의 TTP를 이용해 지정된 타깃을 공격하고, 다른 지역의 공격에서 효과를 본 멀웨어, 툴 또는 절차를 서로 공유합니다.
- 올해 MuddyWater는 터키 정부 기관들을 겨냥한 공격을 시도했고, 중동에서는 SloughRAT라는 신종 임플란트를 배포했습니다.
- CTIR 인게이지먼트를 통해 우리는 다수의 백도어 및 후속 공격 툴이 사용되는 것을 확인했습니다. 심지어 복구 후에도 서버 인프라에 추가 백도어가 존재했고, 원격 서비스 실행 및 공격 툴의 실행을 위한 임패킷도 확인되었습니다.

지능형 지속 공격(APT)

중국

중국과 연계된 APT 행위자들은 다양한 산업 부문의 단체들을 겨냥하면서 중국의 전략적 목표에 부합하는 영역의 지적 재산과 민감한 데이터를 탈취했습니다.

Mustang Panda

시사 사건을 이용해 미국과 아시아에서 공격을 일삼는 것으로 알려져 있습니다.

- 러시아-우크라이나 전쟁을 이용해 러시아 단체를 비롯한 유럽의 기관들을 공격했습니다.

Deep Panda

정부, 군, 공익사업체, 금융 기관 등을 타깃으로 삼는 개별적인 정부 주도 사이버 스파이 단체.

- Log4j 취약점을 이용해 의료 기관을 공격했고, 이후 공격 지속을 위한 커스텀 백도어를 배포하였습니다.

북한

Talos는 북한 정부와 연계되어 스파이, 데이터 탈취 및 와해성 공격으로 정치 안보 목표를 지원하는 Lazarus Group 등의 위협 활동을 확인했습니다.

Lazarus Group

커스텀 멀웨어를 활용하고 폭넓은 금전 탈취 행위를 벌이는 것으로 알려져 있습니다.

- 공개된 VMware Horizon 서버의 Log4j 취약점을 이용해 미국, 캐나다, 일본의 에너지 기업을 공격했습니다.
- Talos는 이른바 MagicRAT라고 하는 신종 원격 액세스 트로이 목마 바이러스와 기타 커스텀 임플란트의 국제 정찰 및 데이터 탈취 활동을 확인했습니다.

남아시아

Talos는 주로 인도의 단체들을 겨냥한 수많은 공격들을 추적했습니다. 이 중 대다수는 오랜 적대국인 파키스탄 정부와 관련된 자들이 벌인 것으로 보입니다.

Transparent Tribe

- 주로 아프가니스탄과 인도의 정부/군 기관 및 관련 단체를 겨냥합니다. 최근에는 인도 내 학생들과 교육 기관까지 공격하기 시작한 만큼 공격 범위를 확대한 것으로 보입니다.

Bitter APT

- 이 단체의 주요 목표는 스파이 활동인 것으로 보입니다. 남아시아와 동아시아의 정부 및 에너지/엔지니어링 관련 단체들을 겨냥한 공격을 장기간 진행했습니다.

기타 APTs

- 올해 초 Talos는 남아시아에서 활동하는 일부 APT 공격자들이 의도치 않게 다른 위협 단체들의 VBA 코드를 재사용했을지도 모른다는 내용의 연구를 발표했습니다.

