2022년 3월

2022년 3월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

추가 위협 탐지

다음과 같은 새로운 위협 탐지가 포트폴리오에 추가되었습니다.

- Cyclops Blink
- FormBook
- Gamaredon
- MuddyWater

또한 다양한 저위험 위협 탐지가 강화되었습니다.

Cyclops Blink

Cyclops Blink는 소규모 사무실/홈 오피스 네트워크 디바이스를 노리는 악성 Linux ELF 실행 파일입니다. 4가지 내장 모듈이 있어 파일을 업로드 및 다운로드하고, 시스템 정보를 검색하고(T1082), 악성 코드 버전을 업데이트할 수 있습니다. C2 명령을 사용하여 추가 모듈을 설치할 수 있습니다. 펌웨어 업데이트 프로세스(T1542.001)를 통해 지속성을 유지하고, 다운로드한 파일을 Linux API 호출(T1059.004)을 통해 실행합니다. 각 샘플에는 IP 주소 및 포트 번호 목록이 포함되어 있습니다(T1571). 실행하면 이러한 IP 주소 및 포트를 통해 C2 통신을 활성화하도록 시스템 방화벽(T1562.004)을 수정합니다.

사용자 환경에서 Cyclops Blink가 탐지되었는지 확인하려면 Cyclops Blink Threat Detail(Cyclops Blink 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

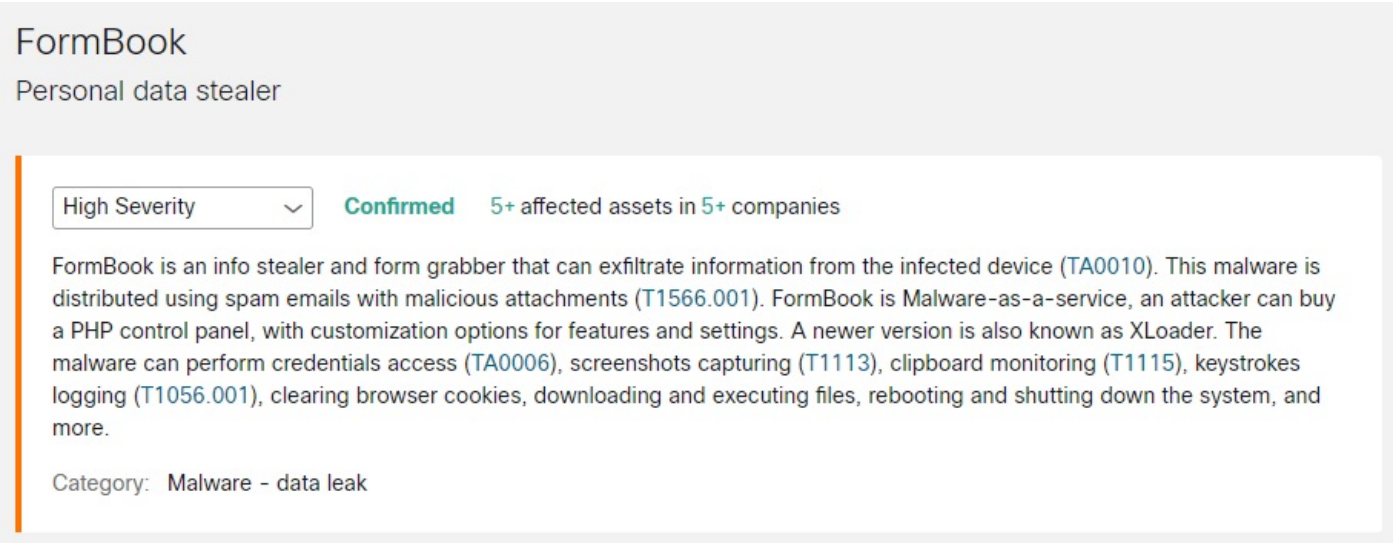
그림 *1:*

FormBook

FormBook은 감염된 디바이스(TA0010)에서 정보를 추출할 수 있는, 정보를 훔치고 폼을 강탈하는 악성코드입니다. 이 악성코드는 악성 첨부 파일이 포함된 스팸 이메일을 사용하여 배포됩니다(T1566.001). FormBook은 MaaS(malware-as-a-service)이며, 공격자는 기능 및 설정에 대한 맞춤 설정 옵션을 제공하는 PHP 제어판을 구매할 수 있습니다. 최신 버전은 XLoader라고도 합니다. 이 악성코드는 자격 증명에 액세스하고(TA0006), 스크린샷을 캡처하고(T1113), 클립보드를 모니터링하고(T1115), 키 입력을 로깅하고(T1056.001), 브라우저 쿠키를 지우고, 파일을 다운로드 및 실행하고, 시스템을 재부팅 및 종료하는 등의 작업을 수행할 수 있습니다.

사용자 환경에서 FormBook이 탐지되었는지 확인하려면 FormBook Threat Detail(FormBook 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 *2:*

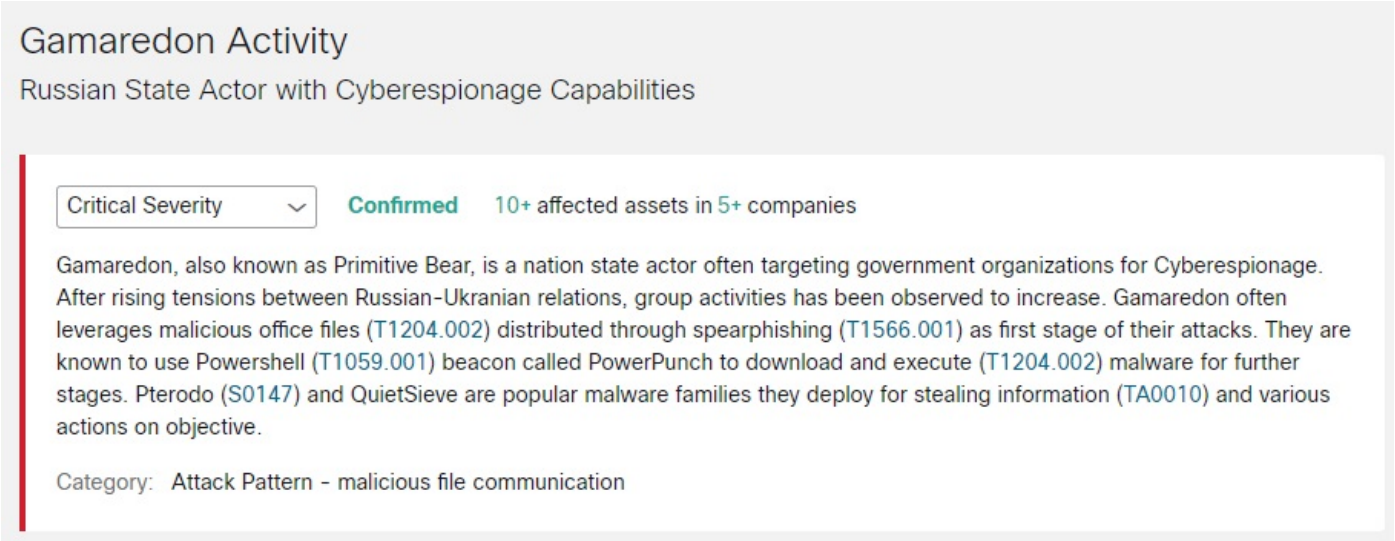


Gamaredon

Primitive Bear라고도 하는 Gamaredon은 사이버 스파이 활동을 위해 주로 정부 조직을 노리는 국가 주도형 공격자입니다. 러시아와 우크라이나 간의 긴장이 고조된 후 그룹 활동이 증가했습니다. Gamaredon은 공격의 첫 번째 단계인 스피어피싱(T1566.001)을 통해 배포되는 악의적인 Office 파일(T1204.002)을 주로 활용합니다. PowerPunch라고 하는 Powershell(T1059.001) 비컨을 사용하여 후속 단계에서 악성코드를 다운로드하고 실행합니다(T1204.002). Pterodo(S0147)와 QuietSieve는 이 악성코드가 정보 도용(TA0010) 및 기타 다양한 작업을 위해 자주 구축하는 악성코드 제품군입니다.

사용자 환경에서 Gamaredon 활동이 탐지되었는지 확인하려면 Gamaredon Activity Threat Detail(Gamaredon 활동 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 *3:*

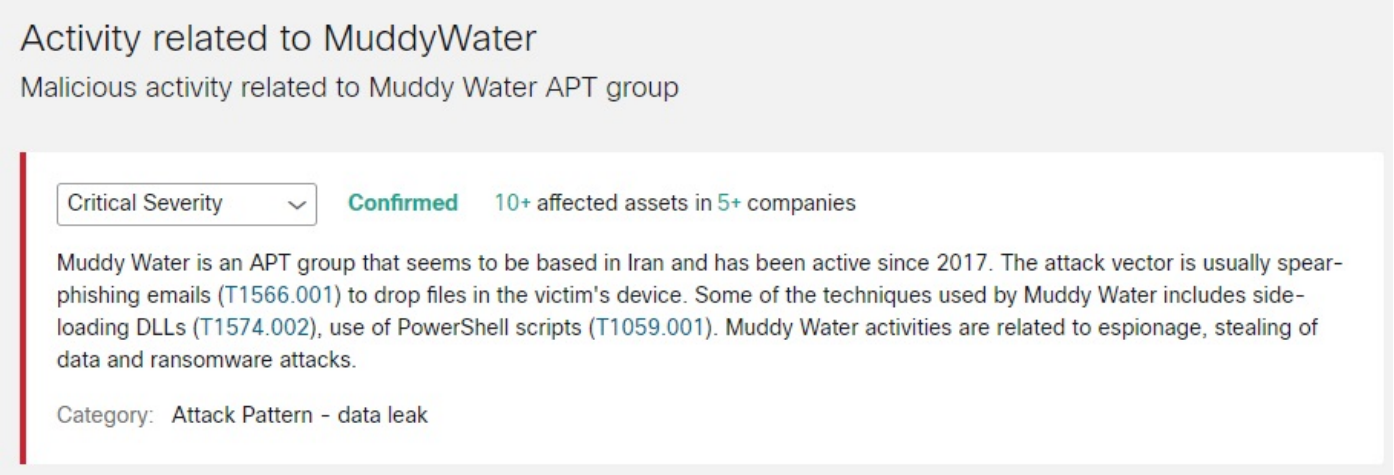


MuddyWater

Muddywater는 이란에서 활동하는 것으로 추정되는 APT(Advanced Persistent Threat) 그룹으로, 2017년부터 활발하게 활동하고 있습니다. 일반적인 공격 벡터는 피해자의 디바이스에 파일을 드롭하는 스피어 피싱 이메일(T1566.001)입니다. Muddywater에서 사용하는 대표적인 기술은 사이드 로딩 DLL(T1574.002)과 PowerShell 스크립트 사용(T1059.001)입니다. Muddywater 활동은 스파이 활동, 데이터 도용 및 랜섬웨어 공격과 관련이 있습니다.

사용자 환경에서 Muddywater 활동이 탐지되었는지 확인하려면 Muddywater Activity Threat Detail(Muddywater 활동 위협 세부 정보)을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

그림 *4:*


Activity related to MuddyWater
Malicious activity related to Muddy Water APT group
Critical Severity
Confirmed
10+ affected assets in 5+ companies
Muddy Water is an APT group that seems to be based in Iran and has been active since 2017. The attack vector is usually spear-phishing emails (T1566.001) to drop files in the victim's device. Some of the techniques used by Muddy Water includes side-loading DLLs (T1574.002), use of PowerShell scripts (T1059.001). Muddy Water activities are related to espionage, stealing of data and ransomware attacks.
Category: Attack Pattern - data leak