2021년 12월

2021년 12월에 릴리스된, Cisco 클라우드 기반 머신 러닝 전역 위협 알림에 대한 업데이트:

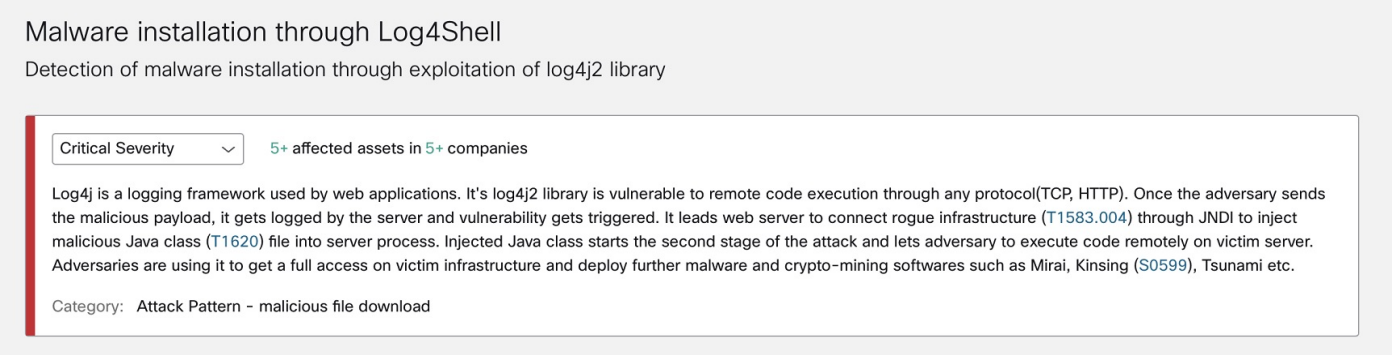
새 Log4Shell 탐지

최근에 발견된 Log4j 취약성과 관련된 두 가지 유형의 탐지를 포함한 새로운 위협 탐지가 포트폴리오에 추가되었습니다.

Log4Shell을 통한 악성코드 설치

이미 성공을 거둔 Log4j 익스플로잇을 탐지했습니다. Log4j는 웹 애플리케이션에서 사용하는 로깅 프레임워크입니다. Log4j의 log4j2 라이브러리는 아무 프로토콜(TCP, HTTP)을 통한 RCE(Remote Code Execution)에 취약합니다. 공격자가 악성 페이로드를 전송하면 서버에 로깅되고 취약성이 트리거됩니다. 웹 서버가 JNDI를 통해 비인가 인프라(T1583.004)에 연결하고 악성 Java 클래스(T1620) 파일을 서버 프로세스에 삽입하게 합니다. 삽입된 Java 클래스는 공격의 두 번째 단계를 시작하여, 공격자가 피해자의 서버에서 원격으로 코드를 실행할 수 있게 합니다. 공격자는 이를 이용하여 피해자의 인프라에 대한 전체 액세스 권한을 얻고 추가 악성코드 및 암호화폐 채굴 소프트웨어(예: Mirai, Kinsing(S0599), Tsunami)를 구축합니다.

그림 *1:*

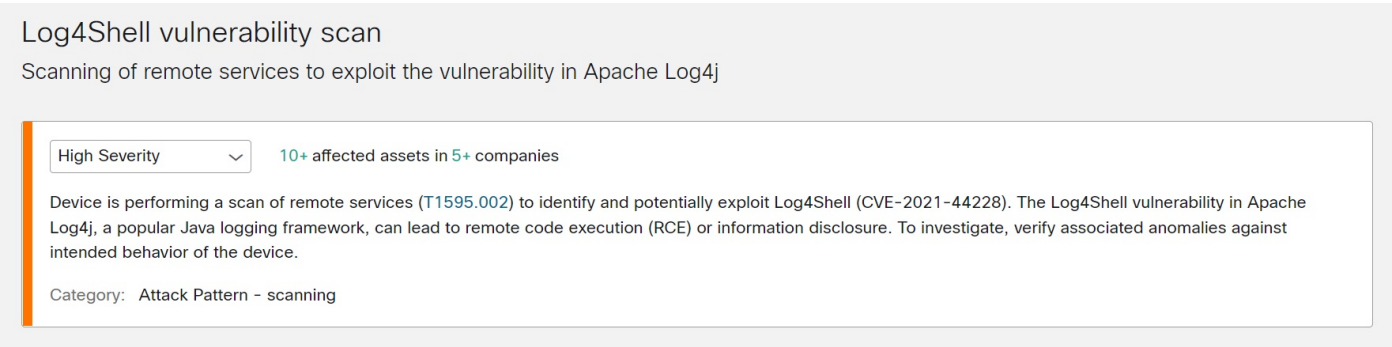


자신의 환경에서 **Log4Shell**을 통한 악성코드 설치가 탐지되었는지 확인하려면 **Malware installation through Log4Shell(Log4Shell**을 통한 악성코드 설치)를 클릭하여 전역 위협 알림에서 세부 정보를 확인하십시오.

Log4Shell 취약성 스캔

Log4Shell(CVE-2021-44228)을 식별하고 잠재적으로 익스플로잇하기 위해 원격 서비스(T1595.002) 스캔을 수행하는 디바이스가 탐지되었습니다. 인기 있는 Java 로깅 프레임워크인 Apache Log4j의 Log4Shell 취약성 때문에 RCE(Remote Code Execution) 또는 정보 노출이 발생할 수 있습니다. 트리거된 알림은 스캔을 수행 중인 원치 않는 애플리케이션 또는 악성코드가 있으며, 침투에 대한 테스트 활동이 진행 중임을 의미할 수 있습니다. 조사하려면 디바이스의 의도된 동작을 상대로 관련 변칙을 확인해야 합니다.

그림 *2:*



사용자 환경에서 **Log4Shell** 취약성 스캔이 탐지되었는지 확인하려면 **Log4Shell vulnerability scan(Log4Shell** 취약성 스캔**)**을 클릭하여 전역 위협 알림에서 관련 세부 정보를 확인하십시오.

새 **SNI** 스푸핑 탐지기

공격자는 다양한 기법을 사용하여 네트워크 보호 메커니즘을 방지합니다. SNI(Server Name Identification) 스푸핑은 도메인 기반 네트워크 보호 메커니즘을 방지하는 데 자주 사용하는 기술입니다. 이 기법은 SNI 필드에 잘 알려진 도메인 이름을 사용하고, 잘 알려진 도메인이 호스팅되는 IP 주

소가 아닌 서버 IP 주소를 사용합니다. 잘 알려진 SNI와 다른 서버 IP 주소를 조합하여 도메인 기반 보안 검사를 통과하고 허용되지 않는 서버에 도달합니다.

그림 *3:*

새로운 SNI 스푸핑 탐지기는 SNI와 IP 주소가 일치하지 않는 불일치를 식별합니다. 탐지기는 ETA(encrypted traffic analysis)를 사용하여 SNI 필드에서 도메인을 추출하고, 관찰된 서버 IP 주소를 도메인이 일반적으로 호스팅되는 IP 주소의 전역 통계 모델과 비교합니다. 관찰된 서버 IP 주소가 모델과 일치하지 않으면 SNI 필드의 도메인이 스푸핑 중일 수 있으며, 네트워크 트래픽이 원치 않는 서버로 라우팅되고 있다는 뜻입니다. 불일치는 SNI 확장의 인기 있는 호스트 이름이 실제로 연결되는 IP 주소에서 호스팅될 가능성이 낮음을 의미합니다.

Alert(알림**) > Alert detail(**알림 세부 정보**) > Security events(**보안 이벤트**)**에서 확인할 수 있습니다.

추가 위협 탐지

다음과 같은 새로운 위협 탐지가 포트폴리오에 추가되었습니다.

- FluBot
- LokiBot
- Phorpiex
- Raccoon
- TrickBot

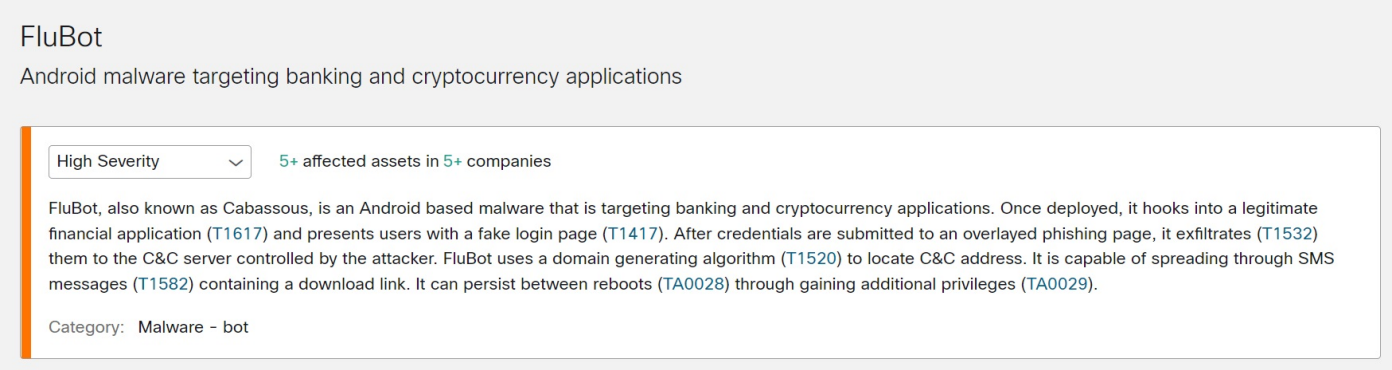
또한 애드 인젝터, 암호화폐 채굴기, 악성 광고, 악성코드 배포, 스팸 추적 같은 다양한 저위험 위협 탐지 기능이 강화되었습니다.

FluBot

FluBot(Cabassous라고도 함)은 스페인 시장 내 뱅킹 및 암호화폐 애플리케이션을 노리는 안드로이드 기반 악성코드입니다. 이 악성코드는 합법적인 금융 애플리케이션(T1617)을 가로채고 사용자에게 가짜 로그인 페이지를 제공합니다(T1417). 오버레이된 피싱 페이지에 자격 증명이 제출되면 이 악성코드는 자격 증명을(T1532) 공격자가 제어하는 명령 및 제어 서버로 추출합니다. FluBot은 도메인 생성 알고리즘(T1520)을 사용하여 명령 및 제어 주소를 찾습니다. 다운로드 링크가 포함된 SMS 메시지(T1582)를 통해 확산될 수 있으며, 추가 권한(TA0029)을 얻은 후 리부팅(TA0028)을 통해 영구적으로 유지됩니다.

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

그림 *4:*

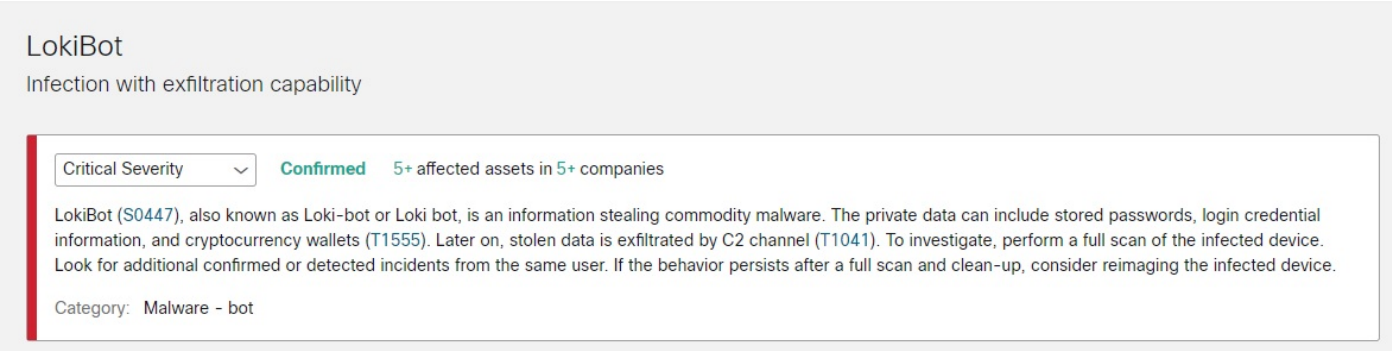


LokiBot

Loki-봇 또는 Loki 봇이라고도 하는 LokiBot(S0447)은 정보를 훔치는 상용 악성코드입니다. 이 악성코드는 저장된 비밀번호, 로그인 자격 증명 및 암호화폐 지갑(T1555) 등의 비공개 데이터도 훔칠 수 있습니다. 도난당한 데이터는 나중에 C2 채널(T1041)을 통해 추출됩니다. 조사하려면 감염된 디바이스의 전체 스캔을 수행해야 합니다. 동일한 사용자의 추가로 확인되거나 탐지된 인시던트를 찾아 보십시오. 전체 스캔 및 정리 후에도 문제가 해결되지 않는다면 감염된 디바이스 이미지 재설치를 고려해야 합니다.

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

그림 *5:*

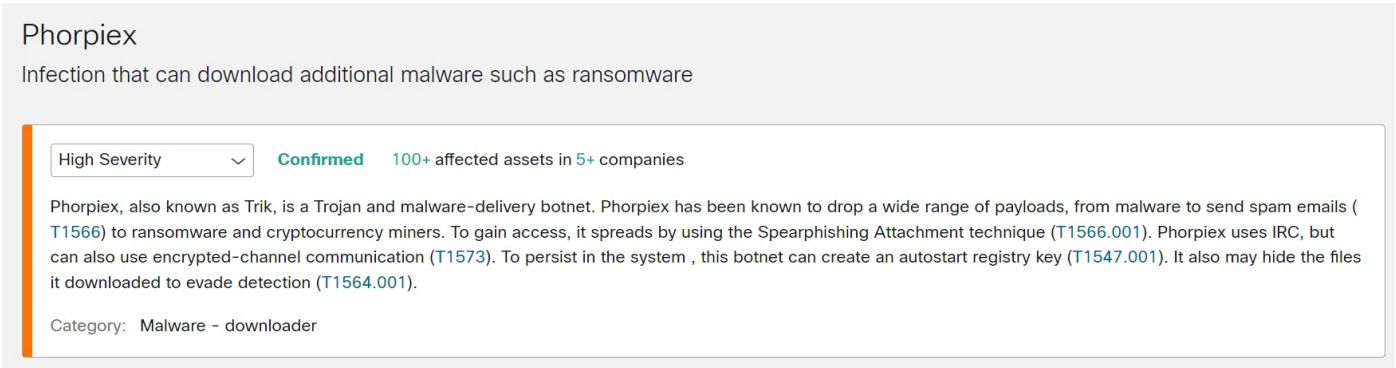


Phorpiex

Phorpiex는 운영 체제를 감염시켜 추가 악성코드를 전달하는 트로이 목마 및 웜입니다. Phorpiex는 랜섬웨어, 암호화폐 채굴기, 스팸 이메일을 전송하는 악성코드 같은 다양한 페이로드를 드롭한다고 합니다(T1566). 액세스 권한을 얻기 위해 스피어피싱 첨부 기술(T1566.001)을 사용하여 확산됩니다. Phorpiex는 IRC를 사용하지만 암호화된 채널 통신(T1573)을 사용할 수도 있습니다. 시스템에서 유지되기 위해 이 봇넷은 자동 시작 레지스트리 키(T1547.001)를 생성합니다. 탐지를 회피하기 위해 다운로드한 파일을 숨기기도 합니다(T1564.001).

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

그림 *6:*



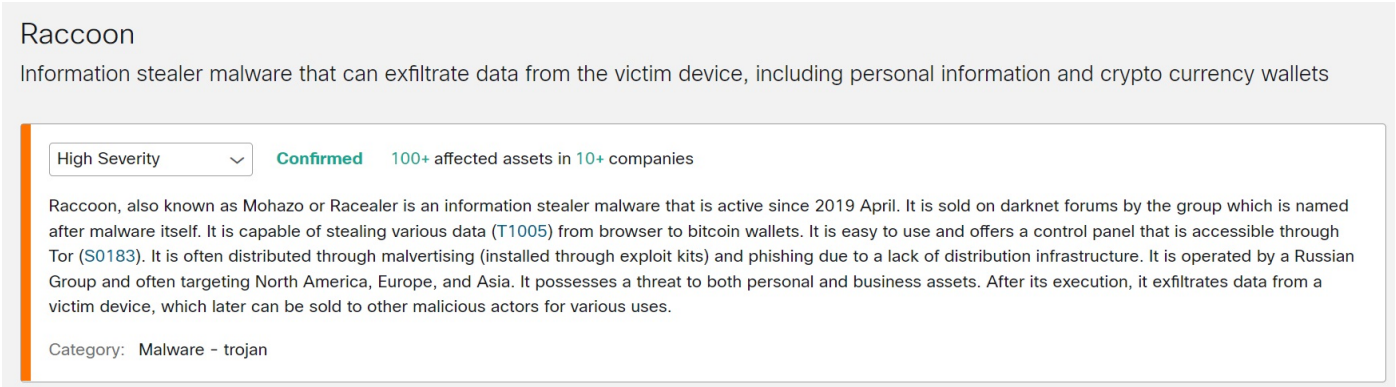
Raccoon

Raccoon(Mohazo 또는 Racealer라고도 함)은 2019년 4월 이후 활성화된, 정보를 훔치는 악성코드입니다. 브라우저의 데이터를 훔쳐(T1005) 비트코인 지갑으로 보낼 수 있으며, 개인 및 비즈니스 자산 모두에 위협이 됩니다. Raccoon은 피해자의 디바이스에서 데이터를 추출하여, 이러한 데이터는 나중에 다양한 용도로 다른 악의적인 공격자에게 판매됩니다.

Raccoon은 악성코드 자체의 이름을 딴 그룹에 의해 다크넷 포럼에서 판매되며, 북미와 유럽 및 아시아를 주로 노리는 러시아 그룹에서 운영합니다. Tor를 통해 액세스할 수 있는 제어 패널로 쉽게 사용할 수 있습니다(S0183). Raccoon은 배포 인프라 부족 때문에 주로 (익스플로잇 킷을 통해 설치되는) 멀버타이징과 피싱을 통해 배포됩니다.

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

그림 *7:*



TrickBot

Trickster라고도 하는 TrickBot(S0266)은 일부 금융 기관의 민감한 정보를 노리는 뱅킹 트로이 목마입니다. 이 악성코드는 주로 악성 스팸 캠페인을 통해 배포됩니다. 이러한 캠페인 대부분은 VB 스크립트 같은 다운로더를 사용하여 배포됩니다.

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

그림 ***8:***