December 2021

Updates released in December of 2021 to Cisco cloud-based machine learning global threat alerts:

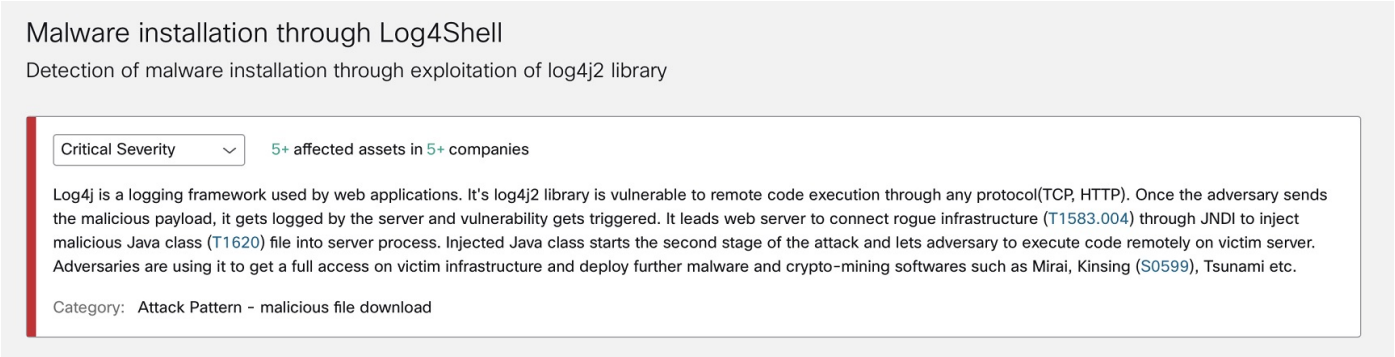
New Log4Shell Detections

We've added new threat detections to our portfolio, including these two types of detection related to the recently discovered Log4j vulnerability:

Malware Installation Through Log4Shell

This is a detection of the already successful Log4j exploitation. Log4j is a logging framework used by web applications. Its log4j2 library is vulnerable to remote code execution (RCE) through any protocol (TCP, HTTP). Once the attacker sends the malicious payload, it gets logged by the server and the vulnerability gets triggered. It leads the web server to connect to rogue infrastructure (T1583.004) through JNDI and inject a malicious Java class (T1620) file into a server process. The injected Java class starts the second stage of the attack and lets the attacker remotely execute code on the victim's server. Attackers use it to get full access to the victim's infrastructure and deploy additional malware and crypto-mining software, such as Mirai, Kinsing (S0599), and Tsunami.

Figure 1:

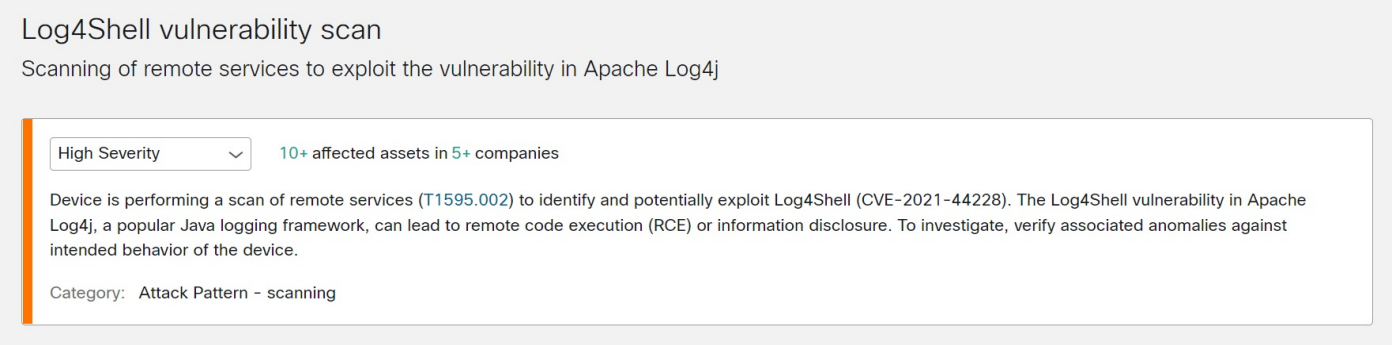


To see if **Malware installation through Log4Shell** has been detected in your environment, click **Malware installation through Log4Shell** to view its details in global threat alerts.

Log4Shell Vulnerability Scan

This is a detection of a device performing a scan of remote services (T1595.002) to identify and potentially exploit Log4Shell (CVE-2021-44228). The Log4Shell vulnerability in Apache Log4j, a popular Java logging framework, can lead to remote code execution (RCE) or disclosure of information. A triggered alert can indicate the presence of an unwanted application or malware performing the scan, as well as testing activities intended on penetration. To investigate, verify the associated anomalies against the intended behavior of the device.

Figure 2:



To see if **Log4Shell vulnerability scan** has been detected in your environment, click **Log4Shell vulnerability scan** to view its details in global threat alerts.

New SNI Spoofing Detector

Attackers use various techniques to avoid network-protection mechanisms. Server Name Identification (SNI) spoofing is a popular technique used to avoid domain-based network-protection mechanisms. This technique involves using a well-known domain name in the SNI field and a server IP address different from the IP address where the well-known domain is hosted. The combination of a well-known SNI and the different server IP address allows one to pass domain-based security checks to reach an unallowed server.

Figure 3:

The new SNI spoofing detector identifies an inconsistency when there's an SNI and IP address mismatch. The detector extracts the domain from the SNI field using encrypted traffic analysis (ETA) and compares the observed server IP address with our global statistical model of IP addresses where the domain is usually hosted. If the observed server IP address does not match the model, then the domain in the SNI field may have been spoofed, and the network traffic is being routed to an unwanted server. The mismatch indicates that there's a low probability that the popular hostname in the SNI extension is actually hosted on the IP address being contacted.

This can be seen in **Alert > Alert detail > Security events**.

Additional Threat Detections

We've added more new threat detections to our portfolio, including:

- FluBot
- LokiBot
- Phorpiex
- Raccoon
- TrickBot

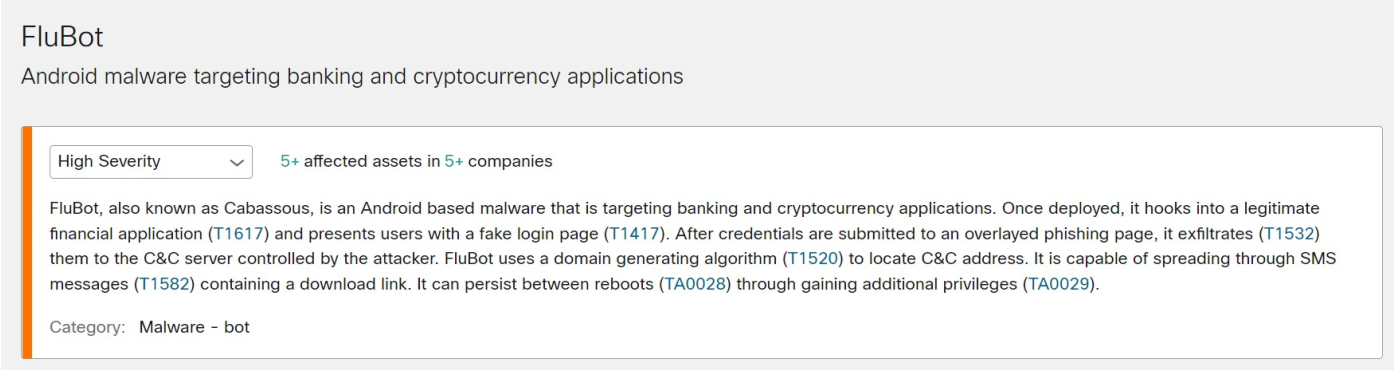
Numerous lower-risk threat detections have also been enriched, including ad injectors, cryptocurrency miners, malicious advertising, malware distribution, and spam tracking.

FluBot

FluBot (also known as Cabassous) is an Android-based malware that targets banking and cryptocurrency applications within the Spanish market. It hooks into legitimate financial applications (T1617) and presents the user with a fake login page (T1417). After credentials are submitted to the overlayed phishing page, it exfiltrates (T1532) them to a command-and-control server controlled by the attacker. FluBot uses a domain generating algorithm (T1520) to locate the command-and-control address. It's capable of spreading through SMS messages (T1582) containing the download link and can persist through reboots (TA0028) by gaining additional privileges (TA0029).

To see if FluBot has been detected in your environment, click FluBot Threat Detail to view its details in global threat alerts.

Figure 4:

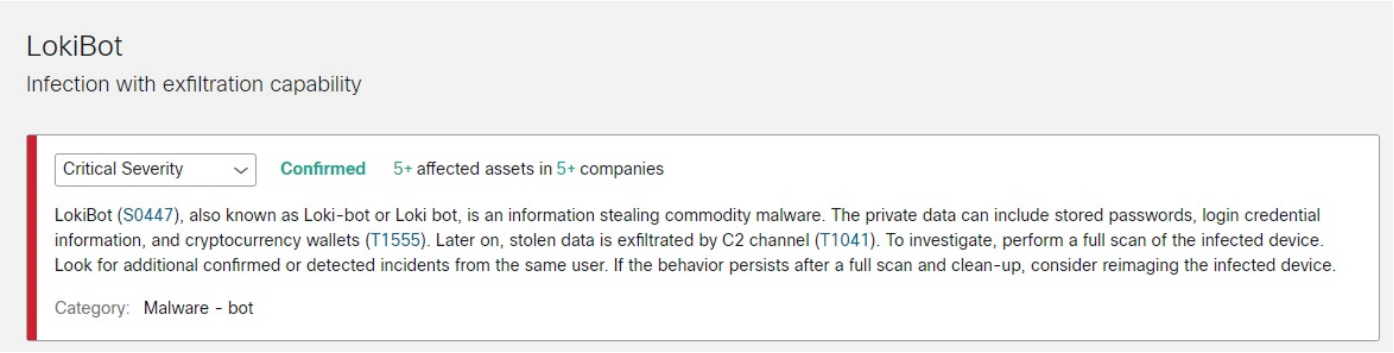


LokiBot

LokiBot (S0447), also known as Loki-bot or Loki bot, is an information-stealing, commodity malware. The private data it steals can include stored passwords, login credentials, and cryptocurrency wallets (T1555). Later, stolen data is exfiltrated by a C2 channel (T1041). To investigate, perform a full scan of the infected device. Look for additional confirmed or detected incidents from the same user. If the behavior persists after a full scan and clean-up, consider reimaging the infected device.

To see if LokiBot has been detected in your environment, click LokiBot Threat Detail to view its details in global threat alerts.

Figure 5:

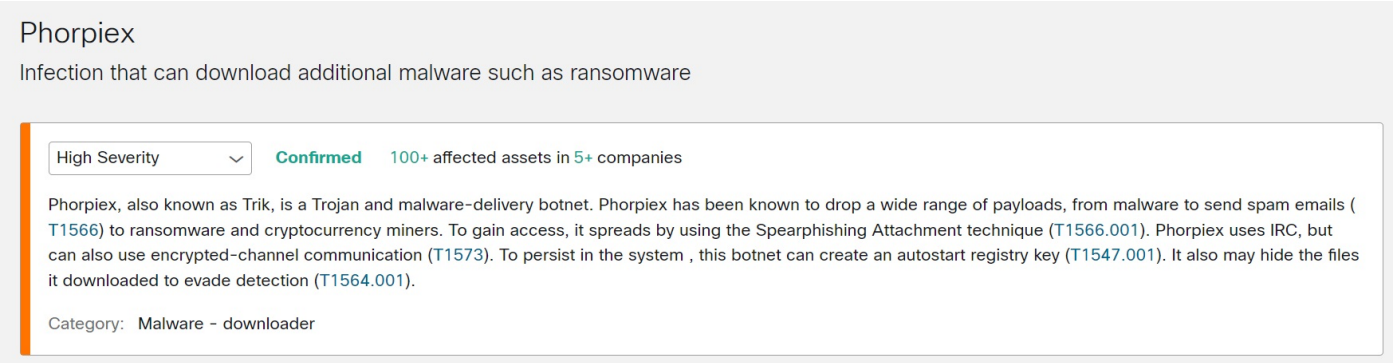


Phorpiex

Phorpiex is a Trojan and worm that infects operating systems to deliver additional malware. Phorpiex has been known to drop a wide range of payloads, including ransomware, cryptocurrency miners, and malware that sends spam emails (T1566). To gain access, it spreads by using the Spearphishing Attachment technique (T1566.001). Phorpiex uses IRC, but can also use encrypted-channel communication (T1573). To persist in the system, this botnet creates an autostart registry key (T1547.001). It may also hide the files it downloaded to evade detection (T1564.001).

To see if Phorpiex has been detected in your environment, click Phorpiex Threat Detail to view its details in global threat alerts.

Figure 6:



Raccoon

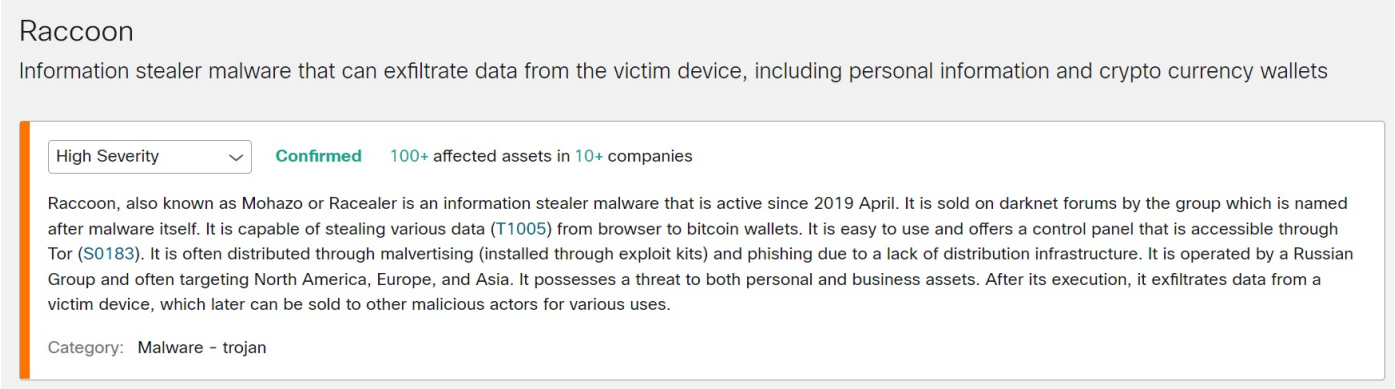
Raccoon (also known as Mohazo or Racealer) is an information-stealer malware that has been active since April of 2019. It's capable of stealing data (T1005) from browsers to bitcoin wallets and is a threat to both personal and business assets. Raccoon exfiltrates data from a victim's device, which later can be sold to other malicious actors for various uses.

Raccoon is sold on darknet forums by the group named after the malware itself and is operated by a Russian group often targeting North America, Europe, and Asia. It can be easily used by a control panel accessible

through Tor (S0183). Raccoon is often distributed through malvertising (installed through exploit kits) and phishing due to a lack of distribution infrastructure.

To see if Raccoon has been detected in your environment, click Raccoon Threat Detail to view its details in global threat alerts.

Figure 7:



TrickBot

TrickBot (S0266), also known as Trickster, is a banking Trojan that targets sensitive information at select financial institutions. This malware is frequently distributed through malicious spam campaigns. Many of these campaigns rely on downloaders for distribution, such as VB Scripts.

To see if TrickBot has been detected in your environment, click TrickBot Threat Detail to view its details in global threat alerts.

Figure 8: