June 2023

Updates released in June of 2023 to Cisco cloud-based machine learning global threat alerts:

- Additional Threat Detections, on page 1

Additional Threat Detections

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

- AMOS
- JackalControl
- RMS
- Satacom
- UNC4841

We've also updated indicators for our existing threat detections.

AMOS

AMOS, also known as Atomic macOS Stealer, is an information stealer that targets Apple MacOS. It focuses on capturing various types of information, such as Keychain passwords (T1555.001), crypto wallets, system data, local files, and even OS credential dumping (T1003). Once it collects the data (T1560), it exfiltrates it via a command-and-control channel (T1041).

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

JackalControl

JackalControl is a Trojan used by GoldenJackal APT that allows attackers to control the victim's device. JackalControl is distributed via fake Skype installers or MS Word documents distributed as attachments. JackalControl can gain persistence by creating scheduled tasks (T1053.005), a registry key (T1547.001), or a Windows service (T1543.003). JackalControl gathers information about the infected device (T1082) to generate a bot id that is used to communicate to the command-and-control server using an HTTP POST request (T1071.001).

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

RMS

RMS (Remote Manipulator System), also known as RuRat and Gussdoor, is a legitimate tool developed by TektonIT for the remote administration of Microsoft Windows and Android devices. The tool has been observed in campaigns conducted by TA505 and other threat actors, who have employed phishing emails as a means of payload distribution (T1566.001). Once RMS is installed, the threat actors gain unauthorized remote access and control over the compromised device for malicious activities, such as exfiltrating sensitive data via command-and-control (T1071.001) and deploying additional malware.

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

Satacom

Satacom, also known as LegionLoader, is a malware that distributes browser extensions (T1176) designed to steal mainly cryptocurrency. The malware spreads through third-party websites that distribute pirated software and subsequently redirects victims to websites hosting zip files that contain the Satacom installer. The victim accesses the redirection link (T1204.001), which downloads and executes the malicious file (T1204.002) that collects data related to Bitcoin wallets and exfiltrates it via the command-and-control channel (T1041). The malicious browser extension delivered by Satacom has been observed to target Coinbase, Bybit, KuCoin, Huobi, and Binance users. It can bypass 2FA to steal the victim's Bitcoin addresses and currency.

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

UNC4841

UNC4841 is a threat actor suspected of carrying out campaigns for reasons of espionage. This group aims at different organizations in the public and private sectors of the Americas, Europe, and Asia Pacific regions. UNC4841 has been observed to exploit zero-day vulnerabilities. One of the vulnerabilities exploited by UNC4841 is CVE-2023-2868, in the Barracuda Email Security Gateway (ESG). This group uses attachments in phishing emails to distribute malware (T1566.001) and can deploy a variety of malware families, including a backdoor such as Saltwater, Seaside, SeaSpy, and SkipJack. Some of the malware has been specifically designed to exploit Barracuda ESG.

To see if UNC4841 activity has been detected in your environment, click UNC4841 Activity Threat Detail to view its details in global threat alerts.