# February 2023

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



# Additional Threat Detections

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

- Agent Tesla
- BlackHat Ad
- LNKR
- Remcos

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

### Agent Tesla

Agent Tesla is a .NET-based Remote Access Trojan, often used to establish a foothold (TA0001) in a victim's network and deploy a second-stage payload (T1105) for further infections. Besides being used as a dropper, it is also capable of stealing information (T1005) from the infected device. Later, it exfiltrates the stolen data through an already established C2 channel (T1041). It is often distributed through phishing emails (T1566) with various themes.

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

### BlackHat Ad

BlackHat Ad campaign infects websites to use them for traffic redirection and leads users to websites that have been compromised (T1204.001). There are several layers of redirection which can lead the user to potentially unwanted services and applications. It can also lead to the installation of more severe malware (T1105) such as information stealers. Two different types of JavaScript injections (T1059.007) have been observed on the compromised websites: simple-script injections and obfuscated-script injections.

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

### LNKR

LNKR (Linker) is a type of adware that is designed to display ads on a user's computer. It typically hijacks the user's web browser (T1185) and injects advertisements into pages while they are being loaded. It can also redirect search engine results to affiliated sites and collect and transmit data to third parties. LNKR is capable of exfiltration (T1041) and is distributed by malicious browser extensions (T1204.002).

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

### Remcos

Remcos was originally developed as a lightweight, fast, and highly customizable Remote Administration Tool by Breaking Security. Later, it was adapted by attackers and used as a Remote Access Trojan. It has both free and professional versions, with varying capabilities such as screen capture (T1113), file transfer (T1105), keylogger (T1056.001), and control of the camera/microphone (T1125). It can inject itself into different processes (T1055) and enable attackers to maintain access to the victim's environment.

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

# Documentation Update

Since the STIX/TAXII API is no longer supported in favor of the new REST API (introduced in June 2021), the STIX/TAXII Service chapter has been removed from this user guide.

- To access the new REST API, see https://api.cta.eu.amp.cisco.com.
- For more information, see global threat alerts REST API is now released!
- If you need assistance, please contact us at cognitive-api-support@cisco.com.