February 2024

Updates released in February of 2024 to Cisco cloud-based machine learning global threat alerts:

Additional Threat Detections

We've added new threat detections to our portfolio:

- Coyote
- Donut Loader
- RisePro

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

Coyote

Coyote is a banking Trojan that mainly targets Latin American users, leveraging phishing techniques (T1566.001) with emails that are themed with a payment bill. The malware uses Squirrel installer for distribution. Coyote is crafted using programming languages such as NodeJS and Nim, showcasing the malware's adaptability and evasiveness. To evade detection, the Trojan employs string-obfuscation techniques (T1027) combined with AES encryption. Once installed on a victim's system, Coyote establishes communication with its command-and-control (C2) server (TA0011) to request screen shots, perform keylogging, and so on.

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

Donut Loader

Donut Loader is an advanced toolkit for in-memory execution of scripts and assemblies, which is also used for malicious purposes (T1055.009). It generates encrypted ShellCode (T1027) for stealthy Windows process injection (T1055). The malware can operate stageless, embedding encrypted payloads within the ShellCode using the Chaskey cipher, or staged by downloading from a URL (T1105). Once executed, it avoids detection by erasing memory traces (T1070) and isolating the payload in a new Application Domain.

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

RisePro

RisePro is an information stealing malware sold in telegram and is distributed by Private Loader malware. RisePro can gather data from the infected device (TA0009) and capture screenshots (T1113). RisePro can read and steal credentials from browsers, crypto wallets (addresses and private keys), and credit card information. The data gathered by RisePro is compressed in a zip file and exfiltrated in an HTTP message (T1071.001). The stealer is also capable of using command-and-control (C2) (T1041) to get configuration and load other malware.

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