September 2023

Updates released in September 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:

- Andariel
- PurpleFox

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

Andariel

Andariel is a threat actor targeting South Korean institutions and corporations. It is known to have relations to Lazarus (G0032), which is a North Korea-based advanced persistent threat. Andariel is known to use its own arsenal including (T1105) remote access trojans, loaders, and reverse shells. They leverage Go, Rust, and .NET framework, while developing their tooling (T1587.001). It spreads through spearphishing (T1566.001), drive-by downloads (T1189), and exploitation of public-facing applications (T1190).

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

PurpleFox

PurpleFox is a dropper malware with self-spreading capabilities. After infecting its victim, PurpleFox uses it to scan the internet for vulnerable servers (T1595.001) that are publicly exposed. Compromised devices (T1584.004) are used to host (T1105) initial payloads of the kill chain. It is observed to leverage MSI files (T1204.002) containing DLLs and a hidden rootkit (T1014). It renames its DLLs to legitimate system resources to get them executed through the Network Service group of the svchost (T1543.003). It modifies the local firewall policies (T1562.004) of the host to prevent reinfection of the same device.

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