September 2022

Updates released in September of 2022 to Cisco cloud-based machine learning global threat alerts:

- New Web Interface, on page 1
- Additional Threat Detections, on page 1

New Web Interface

During the Early Access phase, we refined our new web interface to bring it to you now as the main web interface of global threat alerts.

The new interface brings you:

- Improved alert workflows
- Alignment with MITRE ATT&CK®
- Enhanced view of alert details

Read more about it in a walk-through of the dashboard.

Additional Threat Detections

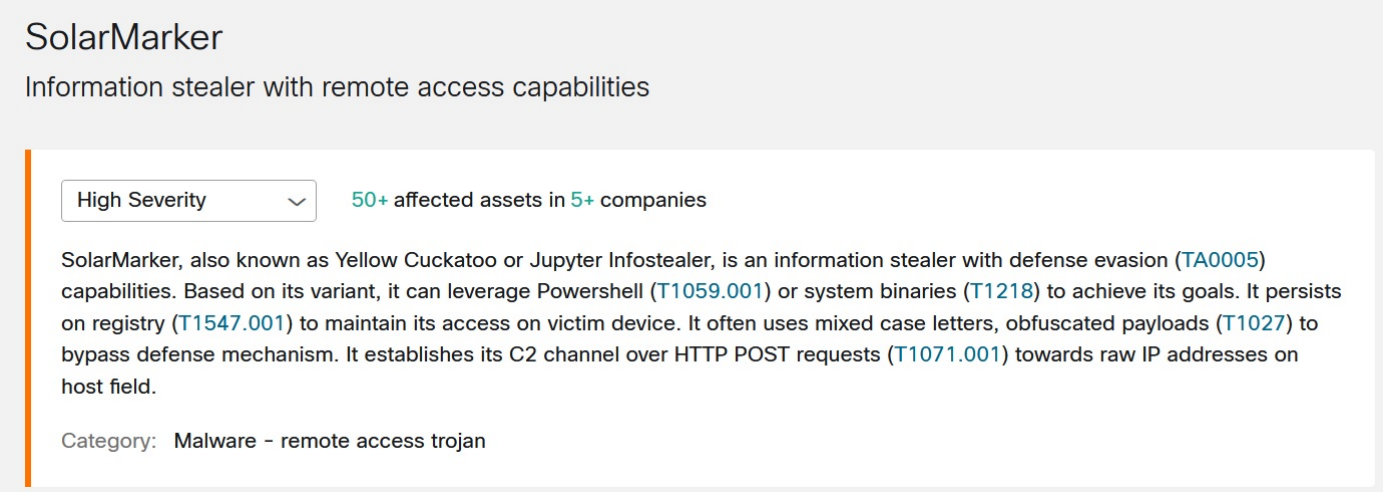
We've added a new threat detection, SolarMarker, to our portfolio. And we've updated indicators for our existing threat detections.

SolarMarker

SolarMarker, also known as Yellow Cuckatoo or Jupyter Infostealer, is an information stealer capable of evading defenses (TA0005). Based on its variant, it can leverage Powershell (T1059.001) or system binaries (T1218) to achieve its goals. It persists in the registry (T1547.001) to maintain access to the victim's device. It often uses mixed-case letters and obfuscated payloads (T1027) to bypass defense mechanisms. It establishes its C2 channel over HTTP POST requests (T1071.001) towards raw IP addresses in the host field.

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

Figure 1:


SolarMarker
Information stealer with remote access capabilities
High Severity
50+ affected assets in 5+ companies
SolarMarker, also known as Yellow Cuckatoo or Jupyter Infostealer, is an information stealer with defense evasion (TA0005) capabilities. Based on its variant, it can leverage Powershell (T1059.001) or system binaries (T1218) to achieve its goals. It persists on registry (T1547.001) to maintain its access on victim device. It often uses mixed case letters, obfuscated payloads (T1027) to bypass defense mechanism. It establishes its C2 channel over HTTP POST requests (T1071.001) towards raw IP addresses on host field.
Category: Malware - remote access trojan