January 2024

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

Additional Threat Detections

We've added a new threat detection to our portfolio:

- Balada Injector

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

Balada Injector

Balada Injector is a malware that infects WordPress-based websites. It injects a backdoor to redirect visitors to compromised sites such as fake support pages, lottery winning sites, and push-notification scams. The latest Balada Injector campaign was launched after WPScan reported about CVE-2023-6000, a cross-site scripting (XSS) flaw in Popup Builder versions 4.2.3 and older (T1189). Those compromised websites are used in phishing emails to distribute malware (T1566.001) and can deploy a variety of malware families.

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