November 2023

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

Additional Threat Detections

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

• Crisis-Driven Cyber Threat

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

Crisis-Driven Cyber Threat

Crisis-linked cyber activities are carried out by various actors and driven by a global crisis such as pandemics, wars, and natural disasters. When multiple actors engage around a single event, attribution often remains unknown or mixed. These activities typically include phishing campaigns (T1566), impersonation of legitimate organizations (T1656), abuse of trusted relationships (T1199), and scams. Potential outcomes include gaining an advantage over information warfare, gaining initial access, conducting cyber operations (T1583), and financial gain.

To see if crisis-driven cyber threats have been detected in your environment, click Crisis-Driven Cyber Threat Detail to view its details in global threat alerts.