



April 2022

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

- [Alignment with MITRE ATT&CK[®], on page 1](#)

Alignment with MITRE ATT&CK[®]

The threat intelligence records in global threat alerts have been adjusted with respect to the MITRE ATT&CK[®] framework:

- Where appropriate, naming from the ATT&CK framework is used directly.
- Global threat alerts threat intelligence provides references to relevant ATT&CK Tactics, Techniques, and Software entries.

Figure 1:

Critical Risk ETA

When: February 5th - May 3rd
Modified: yesterday

Threats: WannaCry (S0366), Emotet (S0367), SMB service discovery (T1018), Excessive communication (T1498)

Asset Groups: Catch All
Affected Assets: 2 assets
Usernames: demo_keturah.gaunt, dusti.hilton
IP Addresses: 10.102.77.196 , 10.201.3.51

Figure 2:

SMB service discovery

Discovery of external SMB servers, e.g. to exploit the ETERNALBLUE vulnerability

High Severity 1,000+ affected assets in 100+ companies Last seen: 2 days ago

Device is performing a scan of SMB services on TCP port 445 (SMB) (T1018), potentially to exploit the ETERNALBLUE SMB (MS17-010) or other vulnerabilities (T1210). Behavior is typical for variants of WannaCry (S0366) or WCry ransomware and unlikely to be legitimate, unless initiated by a user. To investigate, verify associated anomalies against intended behavior of the device.

Category: Attack Pattern - scanning

These improvements provide easier process integration with existing standard operating procedures for incident response and shorten the learning curve for new analysts.