April 2022

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

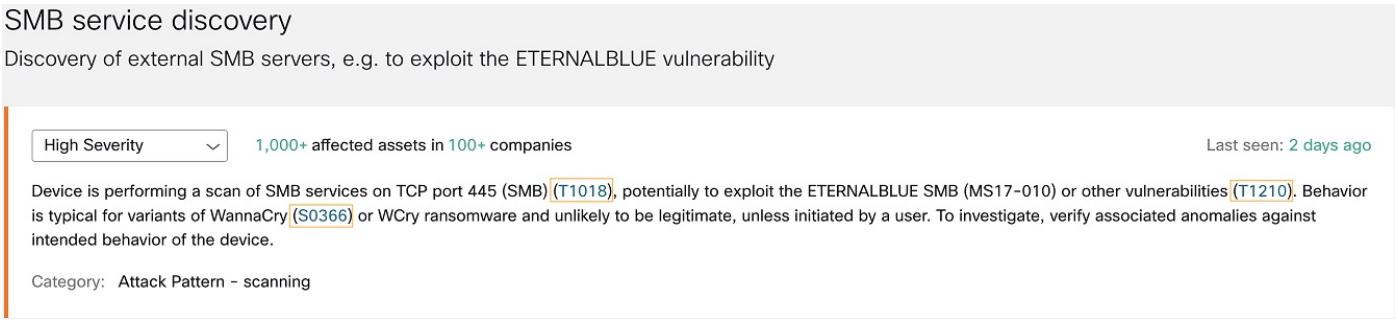
Alignment with MITRE ATT&CK®

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:

Figure 2:



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