



April 2021

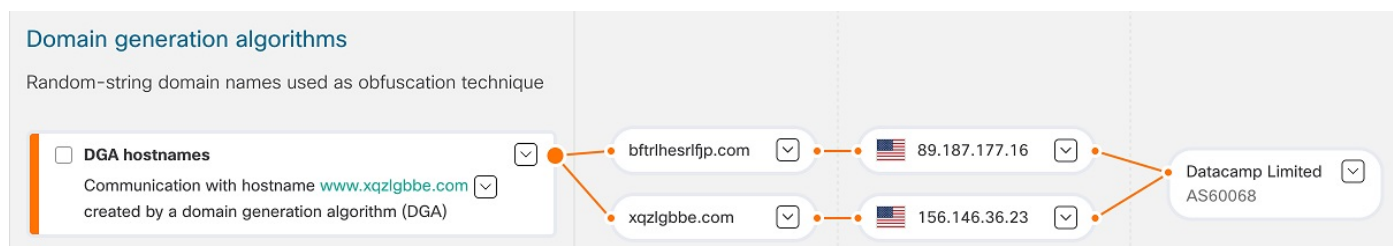
Updates released in April of 2021 to Cisco cloud-based machine learning global threat alerts:

- [New DGA 2.0 Classifier, on page 1](#)
- [New MITRE References in Alert Descriptions, on page 1](#)

New DGA 2.0 Classifier

Domain generation algorithms (DGAs) are used by attackers to randomly generate host names to bypass security products with blocking capabilities. These algorithms are commonly used for communication in botnets and adware. Since they're dynamically generated, they can successfully bypass security products that rely on static, signature-based watchlists, that would otherwise block them.

Figure 1: Example: random-string domain generated by DGA to obfuscate blocker



While global threat alerts has supported the detection of DGA domains since 2015, the DGA 2.0 classifier is a new model built on top of a neural network (state-of-the-art solution for text processing) instead of the older random forests. This architectural refresh and a newly crafted training set result in doubling the recall (number of true positives) while producing fewer false positives.

This can be seen in **Alert > Alert detail > Security events**.

New MITRE References in Alert Descriptions

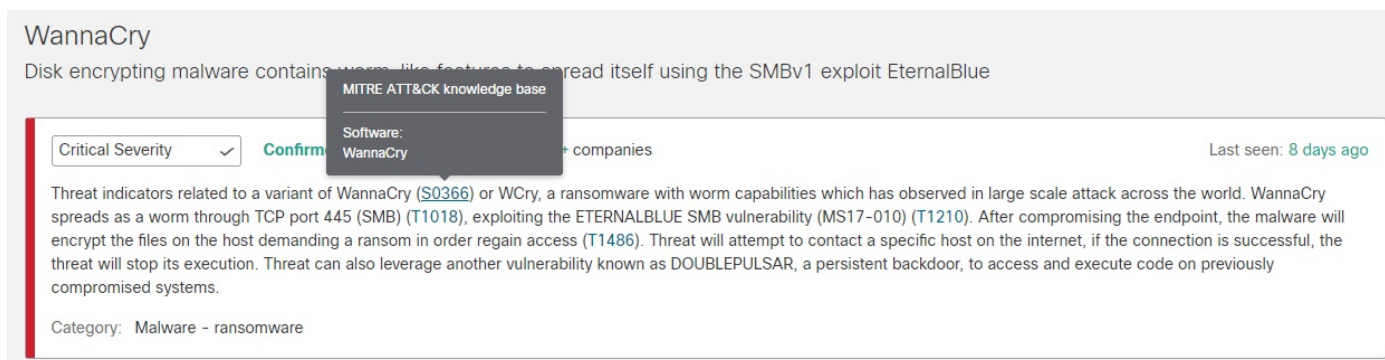
Now we've added MITRE references directly in the description of the alert (where available), so that you can conveniently access supplemental information.

Figure 2: Example: four MITRE references (S0366, T1018, T1210, T1486) in the description of WannaCry



Looking for additional details about the alert and its description? Click on an ID number...

Figure 3: Example: embedded link to the MITRE ATT&CK knowledge base for S0366



...to open a new browser page showing you the MITRE ATT&CK knowledge base with more information and details about the specific threat.

Figure 4: MITRE ATT&CK page with more information and details on S0366

attack.mitre.org/software/S0366/

MITRE | ATT&CK®

Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute

Search

Home > Software > WannaCry

WannaCry

WannaCry is ransomware that was first seen in a global attack during May 2017, which affected more than 150 countries. It contains worm-like features to spread itself across a computer network using the SMBv1 exploit EternalBlue.^{[1][2][3][4]}

ID: S0366

- ① Associated Software: WanaCry, WanaCrypt, WanaCrypt0r, WCry
- ① Type: MALWARE
- ① Platforms: Windows

Contributors: Jan Miller, CrowdStrike

Version: 1.1

Created: 25 March 2019

Last Modified: 13 May 2020

