April 2021

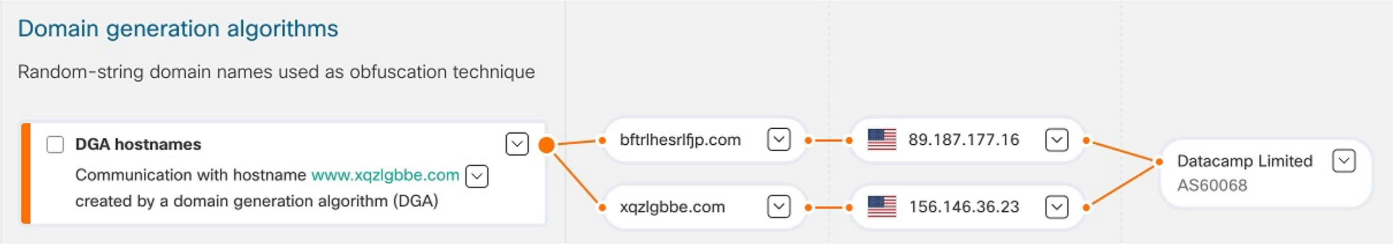
Updates released in April of 2021 to Cisco cloud-based machine learning global threat alerts:

- 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



Domain generation algorithms

Random-string domain names used as obfuscation technique

□ **DGA hostnames**

Communication with hostname www.xqzlgbbe.com created by a domain generation algorithm (DGA)

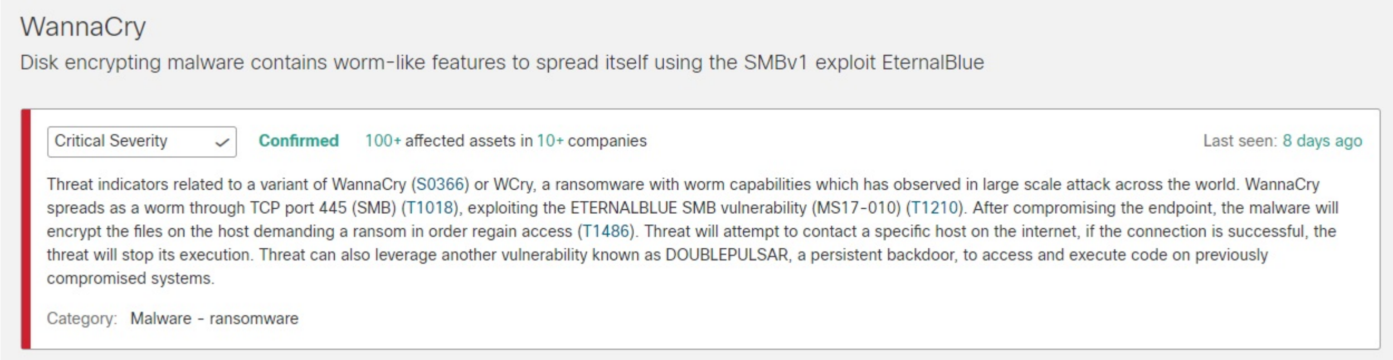
While global threat alerts has supported the detection of DGA domains since 2015, the DGA 2.0 classifier is a new model built on top of a neural network (state-of-the-art solution for text processing) instead of the older random forests. This architectural refresh and a newly crafted training set result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



WannaCry

Disk encrypting malware contains worm-like features to spread itself using the SMBv1 exploit EternalBlue

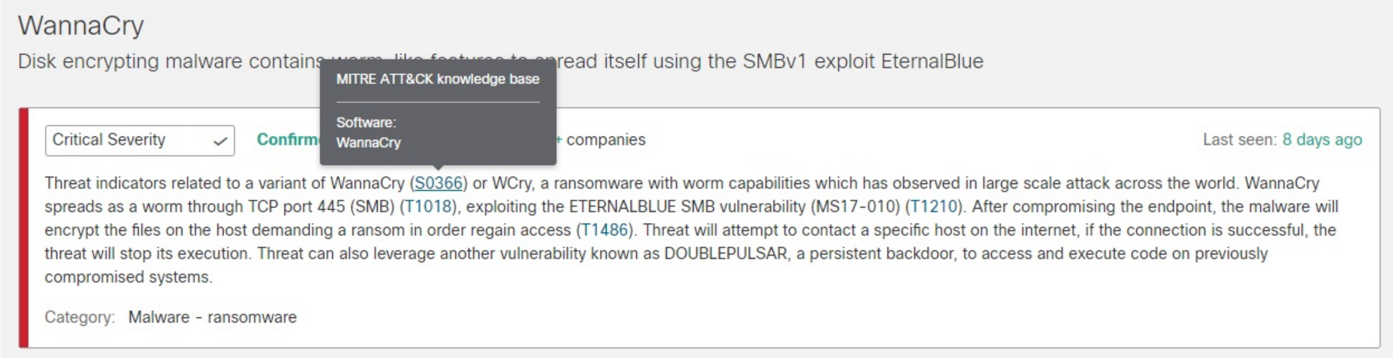
Critical Severity Confirmed 100+ affected assets in 10+ companies Last seen: 8 days ago

Threat indicators related to a variant of WannaCry (S0366) or WCry, a ransomware with worm capabilities which has observed in large scale attack across the world. WannaCry spreads as a worm through TCP port 445 (SMB) (T1018), exploiting the ETERNALBLUE SMB vulnerability (MS17-010) (T1210). After compromising the endpoint, the malware will encrypt the files on the host demanding a ransom in order regain access (T1486). Threat will attempt to contact a specific host on the internet, if the connection is successful, the threat will stop its execution. Threat can also leverage another vulnerability known as DOUBLEPULSAR, a persistent backdoor, to access and execute code on previously compromised systems.

Category: Malware - ransomware

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



WannaCry

Disk encrypting malware contains ... read itself using the SMBv1 exploit EternalBlue

MITRE ATT&CK knowledge base

Software:
WannaCry

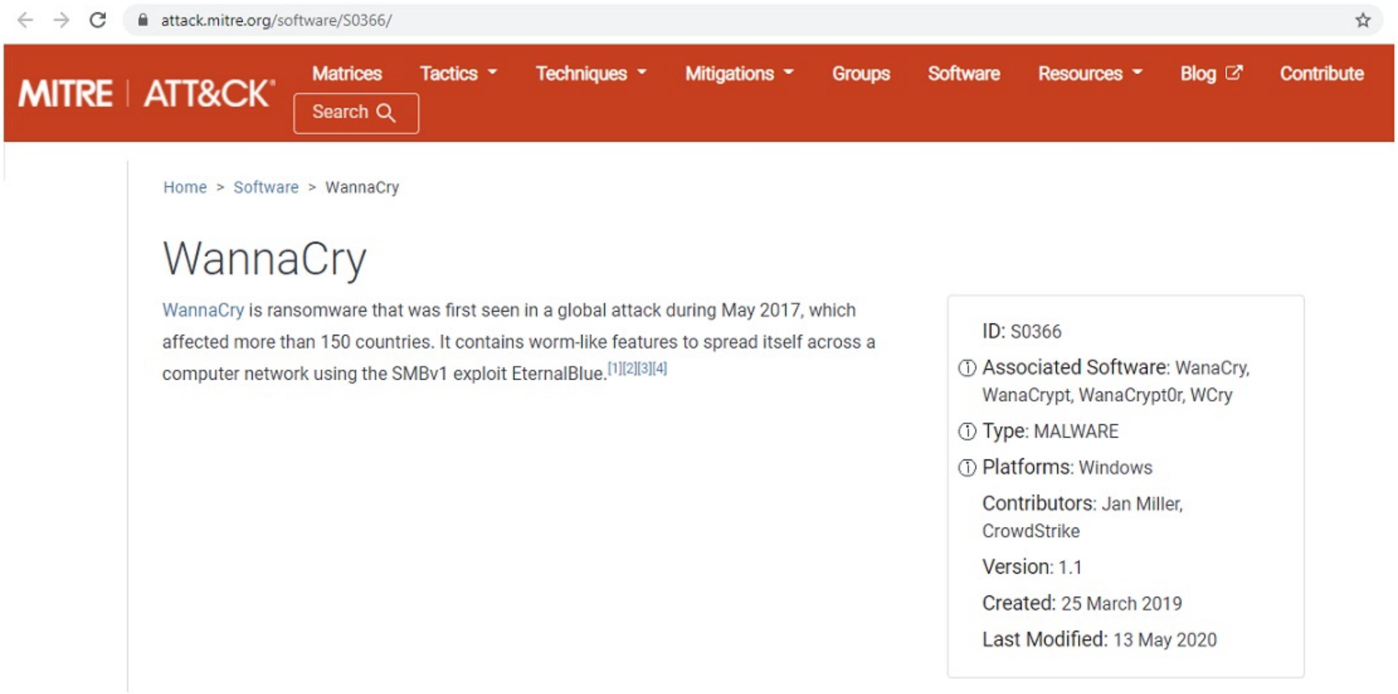
Critical Severity Confirm ... companies Last seen: 8 days ago

Threat indicators related to a variant of WannaCry (S0366) or WCry, a ransomware with worm capabilities which has observed in large scale attack across the world. WannaCry spreads as a worm through TCP port 445 (SMB) (T1018), exploiting the ETERNALBLUE SMB vulnerability (MS17-010) (T1210). After compromising the endpoint, the malware will encrypt the files on the host demanding a ransom in order regain access (T1486). Threat will attempt to contact a specific host on the internet, if the connection is successful, the threat will stop its execution. Threat can also leverage another vulnerability known as DOUBLEPULSAR, a persistent backdoor, to access and execute code on previously compromised systems.

Category: Malware - ransomware

...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



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

ⓘ Associated Software: WanaCry, WanaCrypt, WanaCrypt0r, WCry

ⓘ Type: MALWARE

ⓘ Platforms: Windows

Contributors: Jan Miller, CrowdStrike

Version: 1.1

Created: 25 March 2019

Last Modified: 13 May 2020