Timeline of ‘WannaCry’ Ransomware Defense

Microsoft Security Bulletin
March 14th, 2017
On March 14th, Microsoft released a patch (MS17-010) for a new SMB vulnerability.

Cisco NGFW | Meraki MX
March 14th, 2017
On the same day, Cisco Talos released Snort™ signature #41978 to detect vulnerabilities identified in MS17-010.

Shadow Brokers
April 14th, 2017
A group known as “The Shadow Brokers” released a set of vulnerabilities allegedly stolen from the National Security Agency (NSA) that go by the names of Eternal Blue and Double Pulsar.

Cisco NGFW | Meraki MX
April 25th, 2017
Talos releases Snort™ signatures #42329, #42332, #42340 for Double Pulsar and Anonymous SMB shares.

Cisco Talos
With more than 250 world class researchers around the globe and a global network of intelligence and data sources, Cisco continues to monitor, research, and protect customers against ‘WannaCry’ and other emerging threats.

Cisco Umbrella
May 12th, 2017 | 10:12 UTC
Cisco Umbrella adds attribution of the attack type to ransomware and moves the kill switch domain to the malware category.

Cisco AMP
May 12th, 2017 | 9:33 UTC
Approximately 60 minutes after the first seen samples, AMP detected the ransomware. Threat was detected via automatic analysis rules and low prevalence methods. AMP successfully detected and blocked on endpoints, email and web gateways, and network security.

Cisco Umbrella
May 12th, 2017 | 7:43 UTC
Cisco Umbrella pushes kill switch domain globally into ‘Newly Seen Domains’ categories which resulted in protection against the ransomware and spreading of the worm.

Cisco Investigate
May 12th, 2017 | 7:30 UTC
MalwareTechBlog releases information about a new attack dubbed “WannaCry” on Twitter and his blog.
Cisco Investigate screenshot was included in the blog as it was used as a part of the intelligence collection and discovery.

For more information, please visit cisco.com and talosintelligence.com