WANNACRY RANSOMWARE UPDATE

May 14, 2017

WHAT WE KNOW SO FAR

A major ransomware attack broke on Friday May 12, affecting many organizations the world over, reportedly including major telcos, hospital systems and transportation providers. The attack has purportedly spread to some 150 countries around the world. This is the first ransomware worm to ever be seen in the wild. The malware responsible for this attack is a ransomware variant known as 'WannaCry'.

WannaCry gets installed through a vulnerability in the Microsoft SMB protocol, not phishing or malvertising. SMB is a network protocol used to share files between computers. The reason WannaCry is particularly effective is that it can spread laterally on the same network, automatically installing itself on other systems in the network without any end user involvement. The malware is particularly effective in environments with Windows XP machines, as it can scan heavily over TCP port 445 (Server Message Block/SMB), compromising hosts, encrypting files stored on them, and then demanding a ransom payment in the form of Bitcoin.

On March 14, Microsoft released a security update to patch this vulnerability. While this protected newer Windows computers that had Windows Update enabled, many computers remained unpatched globally. This is particularly true of Win XP computers which are no longer supported by Microsoft, as well as the millions of computers globally running pirated software, which are (obviously) not automatically upgraded.

Please read the Cisco TALOS blog for the most up-to-date information on WannaCry: http://blog.talosintelligence.com/2017/05/wannacry.html.

HOW WE PROTECTS OUR CUSTOMERS

A defense-in-depth strategy is always the best approach to information security.

Remember, this is a vulnerability of Microsoft Windows and as such the following best practices are recommended to combat attacks based on Microsoft SMB :

1. Ensure that devices running Windows are fully patched. In particular, apply the following: Microsoft Security Bulletin MS17-010
2. Strongly consider blocking legacy protocols like SMBv1 inside the network. Additionally, consider blocking all SMB connections (TCP ports 139, 445) from externally accessible hosts

To be clear, if the vulnerabilities arenβ€™t patched, an organization will continue to be at risk for infection by this ransomware. However, the following Cisco Security products can limit the installation, spread, and execution of WannaCry:

1. Cisco Network Security (NGFW, NGIPS, Meraki MX) products have had up-to-date rules (since the vulnerability was known in mid-April) to detect and block this malicious activity on SMB connections.
2. Cisco Malware Protection technology (AMP on endpoints, network, and email/web gateways) have up-to-date information on this ransomware and in fact quickly detected and prevented the execution of this ransomware.
3. Cisco Cloud Security (Umbrella) can block connections from malware to command-and-control servers on the internet which results in improper execution of the malware. In this situation, this block automatically triggered a β€□kill switchβ€□ in the malware.

Cisco Umbrella (OpenDNS) first observed requests for WannaCry's kill switch/anti-sandbox domain (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com) starting at 07:24 UTC on Friday, and it was added to the newly seen domain (NSD) category. By blocking this domain, it would prevent the ransomware from running on the machine. If Umbrella customers were blocking the NSD category, then they were protected at the earliest possible point. That domain was then categorized as malware and blocked for everyone.

There is likely to be variants of WannaCry in the coming days and weeks. While the current variant will be added to anti-virus signatures, the new variants have the best chance of being detected by the modern behavioral techniques in Cisco AMP.

CISCO RANSOMWARE SOLUTIONS

Cisco has a defense-in-depth architecture for protecting against ransomware. Take a look at the Ransomware Threat Defense solution

Read more at :

http://blog.talosintelligence.com/2017/05/wannacry.html#more