June 27, 2017

To: Trend Micro™ TippingPoint Customers

Subject: WCRY Ransomware Attack (update)

The following is an update related to the WannaCry/WCry ransomware outbreak that has affected several organizations around the world. Trend Micro TippingPoint is continuing to actively review the contents of this disclosure in order to recommend coverage leveraging the TippingPoint solution. At this point, we have identified the following filters that should help you protect against the exploits listed in the table below:

CVE Number	Filter(s)	Source	Released	Category	Comments
CVE-1999-0519 CVE-1999-0520	2176		Prior to 2006	Security Policy	SMB: Null Session SetUp
	5614	DV7378	9/24/2007	Exploit	SMB: Malicious SMB Probe/Attack
	*11403	DV8265	11/01/2011	Security Policy	SMB: Suspicious SMB Fragmentation
CVE-2017-0145	27711	DV8936	4/11/2017	Exploit	SMB: Server SMBv1 Buffer Overflow Vulnerability
CVE-2017-0144	27928	DV8938	4/18/2017	Vulnerabilities	SMB: Remote Code Execution Vulnerability (EternalBlue)
CVE-2017-0146	27928 27929	DV8938	4/18/2017	Vulnerabilities	SMB: Remote Code Execution Vulnerabilities (EternalChampion) SMB: Remote Code Execution Vulnerability (EternalBlue)
CVE-2017-0147	27929 27937	DV8938	4/18/2017	Vulnerabilities	SMB: Remote Code Execution Vulnerability (EternalBlue) SMB: NT_TRANSACT_RENAME Information Disclosure Vulnerability (EternalSynergy)
	27935	DV8938	4/18/2017	Exploit	SMB: DoublePulsar Backdoor
	28304	MW1370	5/15/2017	Virus (ThreatDV)	Ransom_WCRY.I Download Attempt (Specific)
	28305	MW1370	5/15/2017	Virus (ThreatDV)	Ransom_WCRY.I Download Attempt (Generic)
	30623	MW1251	8/16/2016	Virus (ThreatDV)	TLS: Suspicious SSL Certificate (DGA)
*Prone to false positives or performance issues					

Additionally, here are some of the solutions and best practices that organizations can adopt and implement to safeguard their systems from threats like WannaCry:

- Customers should not use any security product to block the malwares attempt to reach the killswitch domain. During the early stages of infection, the malware reaches out to a hardcoded killswitch domain (for example: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com). If the malware cannot resolve that address, it proceeds with delivering the ransomware component. If the malware receives a valid response from the killswitch domain, it does not deploy the ransomware. Right now, researchers and organizations are buying these killswitch domains to slow down the number of infections. It's important that these domains are NOT blocked.

- The ransomware exploits a vulnerability in SMB server. Patching is critical for defending against attacks that exploit security flaws. A patch for this issue is available for Windows systems, including those no longer supported by Microsoft. When organizations can't patch directly, using a virtual patch can help mitigate the threat.
- Deploying firewalls and intrusion prevention systems can help reduce the spread of this threat. A security system that can proactively monitor attacks in the network also helps stops these threats.
- Aside from using an exploit to spread, WannaCry reportedly also uses spam as entry point. Identifying red flags on socially engineered spam emails that contain system exploits helps. IT and system administrators should deploy security mechanisms that can protect endpoints from email-based malware.
- WannaCry drops several malicious components in the system to conduct its encryption routine. Application control based on a whitelist can prevent unwanted and unknown applications from executing. Behavior monitoring can block unusual modifications to the system. Ransomware uses a number of techniques to infect a system; defenders should do the same to protect their systems.
- WannaCry encrypts files stored on local systems and network shares. Implementing data categorization helps mitigate any damage incurred from a breach or attack by protecting critical data in case they are exposed.
- Network segmentation can also help prevent the spread of this threat internally. Good network design can help contain the spread of this infection and reduce its impact on organizations.
- Disable SMB by enabling a traffic management rule to block port 445 over TCP/IP on systems that do not require SMB to be enabled. Running unneeded services gives more ways for an attacker to find an exploitable vulnerability.

For additional information, visit the following blogs:

- Updates on the latest WCRY (WannaCry) Ransomware Attack and Trend Micro Protection
- WannaCry/WCry Ransomware: How to Defend against It

For questions or technical assistance, on any TippingPoint product, contact the TippingPoint Technical Assistance Center (TAC).

Thank you,
Trend Micro™ TippingPoint

For contact information, please visit us at https://tmc.tippingpoint.com