Emerging Threat – Global Outbreak of WannaCry Ransomware (ETR-2017-C020)

EXECUTIVE SUMMARY:

Reports of malware attacks in Spain began around 8:00am EDT on 12 May 2017. The attacks were ransomware with file extensions of the encrypted files ending in .WNCRY. Shortly thereafter, samples became available of the malware and it was confirmed to be WannaCry using an SMB exploit and worm techniques. This is a new version of the WannaCry malware being called WannaCry 2.0 by threat researchers.

By 1:00pm EDT the attacks were being reported in the UK against the NHS with some hospitals having lost the use of telephones and computers. The full scale of the attack and the initial infection vector remains unknown at this time.

THREAT TECHNICAL DETAILS:

Some samples show the WannaCry malware with no AV detection and others have detection by a majority of the AV vendors. There is a Visual Basic Script file (VBS) packaged with some binaries hinting at possible initial infection vectors being emails with linked or attached Microsoft Office documents.

Once the malware is installed, it encrypts files using AES and RSA encryption. More details on the delivery and infection mechanisms will be provided as details become available.

The malware is using at least one SMB vulnerability in its attack. SMB had a number of known issues going back as far as MS08-068. A named attack called Badlock was reported in 2016 also targeting SMB and recently Microsoft released an additional Vulnerability Note in February 2018, VU#867968, about the possibility of a denial of service attack also using SMB. It has been confirmed that MS17-010 vulnerability for SMB is being used.

The bitcoin addresses for payment of the ransom have been hard-coded into the malware samples.

IMPACT:

There is an active attack in the wild of the WannaCry/WCry ransomware currently. It appears to be global in scope affecting customers in the United States, United Kingdom, Taiwan, Russia, Turkey, Kazakhstan, Indonesia, Vietnam, Japan, Spain, Germany, Ukraine, and the Philippines. The full scope of the attack is currently unknown. It has been seen targeting communications and healthcare organizations but the full list of targets remains unknown.

AFFECTED SOFTWARE:

Microsoft Windows systems using Samba (SMB) file sharing are at risk. Unpatched Microsoft Windows systems are at higher risk.

SYMANTEC MSS SOC DETECTION CAPABILITIES:

For customers with our IDS/IPS Security Management services, vendor signatures will be deployed automatically, but enabled only where it is recommended by the vendor. Customers who would like to adjust their IDS/IPS policy outside the standard vendor policy should contact MSS to discuss their requirements. MSS can be reached by requesting help via phone, e-mail, chat, or by visiting the MSS portal at https://mss.symantec.com.

For customers with monitor-only IDS/IPS devices, Symantec MSS stands ready to provide security monitoring once your IDS/IPS vendor releases signatures and those signatures are enabled on your monitored devices.

Detection

MSS Detection

Detection is provided through SMB threshold detection and DGA domain detection

SEP Detection

For those customers that have Symantec Endpoint Detection, we will add new signatures to our existing detection for this threat as more information emerges.

MSS is evaluating additional intelligence and detection options that may be available for this threat. If reliable and conclusive detection opportunities are identified, they will be added globally to ensure all customers are protected. MSS may directly contact potentially affected customers to discuss any exposure to this threat that is not included in a security incident.

This list represents a snapshot of current detection. Symantec MSS stands ready to provide security monitoring once additional vendors or additional detection is identified and enabled on your monitored devices. As threats evolve, detection for those threats can and will evolve as well.

MITIGATION STRATEGIES AND RECOMMENDATIONS:

This section is used to discuss how the threat can be prevented, contained, and removed. This section can vary depending on the nature of the threat.

Threat Specific Mitigating Guidelines

- SMB should be disabled if not required for business use.
- MS17-010 use has been confirmed and that vulnerability should be patched immediately.
- All SMB-related patches should be applied to servers as soon as practical.
- Any Microsoft updates that haven't been applied to servers should be applied as soon as possible.
- A notice to all users should be sent regarding this attack and a reminder about clicking links or opening files in emails from suspicious or unknown sources should be sent.
- Review current backup policies and procedures and be prepared to perform a restore in case of infection – it is never a good idea to pay the ransom in a ransomware attack if at all avoidable.

Recommended Best Practices

Symantec recommends that all customers follow IT security best practices. These will help mitigate the initial infection vectors used by most malware, as well as prevent or slow the spread of secondary infections.

Minimum Recommended Best Practices Include:

- Disable default user accounts
- Educate users to void following links to untrusted sites.
- Always execute browsing software with least privileges possible
- Turn on Data Execution Prevention (DEP) for systems that support it
- Maintain a regular patch and update cycle for OS and installed software
- For additional details please reference: http://technet.microsoft.com/en-us/library/dd277328.aspx

REFERENCES:

This section is for aggregating available information links from in previous sections of the document, as well as from vendors.

For additional information related to this threat/vulnerability please reference the following links:

- **ETR-Microsoft Windows SMB Zero-Day Vulnerability (ETR-2017-V001)**

- **CERT Vulnerability Note VU#867968: Microsoft Windows SMB Tree Connect Response Denial of Service Vulnerability**
  http://www.kb.cert.org/vuls/id/867968

- **Microsoft Windows VU#867968 Memory Corruption Vulnerability**
  http://www.securityfocus.com/bid/95969/info

- **NHS cyber-attack: hospital computer systems held to ransom across England**
  https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack?CMP=Share_iOSApp_Other

- **Telefonica tells Employees to Shut Down Computers Amid Massive Ransomware Outbreak**
  https://www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/

Thank you for choosing Symantec as your Managed Security Services Provider. Should you have any questions or feedback, please contact your Services Manager, or the Analysis Team can be reached by requesting help via phone, email, chat, or by visiting the MSS portal at https://mss.symantec.com.

Global Client Services Team
Symantec Managed Security Services
MSS Portal: https://mss.symantec.com
MSS Blog: http://www.symantec.com/connect/symantec-blogs/cyber-security-services

Need Help Responding to a Security Incident?
Contact Symantec's Cyber Security Services – Incident Response Team
Email: incidentresponse@symantec.com
US Incident Response Hotline: (855) 378-0073
UK Incident Response Hotline: +44 (0) 800 917 2793
Australia Incident Response Hotline: +61 1800 481 774
Singapore Incident Response Hotline: +65 800 1206718
Japan Incident Response Hotline: +81 0066 33 813303
For Information: http://go.symantec.com/incidentresponse