NCCIC

National Cybersecurity and Communications Integration Center

WHAT IS WANNACRY/WANACRYPT0R?

WannaCry is ransomware that contains a worm component. It attempts to exploit vulnerabilities in the Windows SMBv1 server to remotely compromise systems, encrypt files, and spread to other hosts. Systems that have installed the MS17-010 patch are not vulnerable to the exploits used. Patches to address the vulnerabilities identified in Microsoft Security Bulletin MS17-010 are available for all versions of Windows from XP onward.

What if I have been infected?

- Isolate the system to prevent the malware from compromising additional devices.
  - While the system may still be used, WannaCry will continue to encrypt files and attempt to spread.
- Do not connect to or power on unpatched systems on compromised networks.
- The U.S. Government does not encourage paying a ransom to criminal actors. Paying the ransom does not guarantee decryption or removal of the malware. CERT Australia and other open source reporting have stated that a backdoor remains even if payment is made.
- A cyber security incident can be reported to the NCCIC 24/7/365 at NCCICCustomerService@hq.dhs.gov or (888) 282-0870.
- Restore from backups. Encrypted files cannot currently be decrypted without the corresponding private key.
  - If backups are not available, consider storing the encrypted data before wiping the computer in the event that a decryption method is found in the future.

What if a system cannot (currently) be patched?

There are several workarounds that can help protect systems from infection, including the following:

- Disable SMBv1 on every system connected to the network.
  - Information on how to disable SMBv1 is available at the following location: https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012
  - While many modern devices will operate correctly without SMBv1, some older devices may experience communication or file/device access disruptions.
- Block port 445 (Samba).
  - This may cause disruptions on systems that require port 445.
- Review network traffic to confirm that there is no unexpected SMBv1 network traffic. The following links provide information and tools for detecting SMBv1 network traffic and Microsoft's MS17-010 patch:
  - https://blogs.technet.microsoft.com/ralphkyttle/2017/05/13/smb1-audit-active-usage-using-message-analyzer/
  - https://www.wireshark.org/#download
  - https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_010
- Vulnerable embedded systems that cannot be patched should be isolated or protected from potential network exploitation.

NCCIC

National Cybersecurity and Communications Integration Center

How do I decrypt my files?

- There is currently no method of decrypting encrypted files without having the private key.

If I think a device is vulnerable and would like to report it, who do I contact?

- Contact ICS-CERT to report the issue at ics-cert@hq.dhs.gov or (877) 776-7585.

What else can I do going forward to prevent this kind of attack?

- Keep systems up to date and patch as soon as possible.
  - The CVEs for the vulnerabilities associated with WannaCry exploits are as follows: CVE-2017-0143; CVE-2017-0144; CVE-2017-0145; CVE-2017-0146; CVE-2017-0147; and CVE-2017-0148
- Segregate networks based on functionality and the need to access resources.
- Keep offline data backups up to date.
- Additional information about ransomware is available in the following references:
  - https://ics-cert.us-cert.gov/sites/default/files/documents/Destructive_Malware_White_Paper_S508C.pdf
  - https://www.us-cert.gov/security-publications/Ransomware
  - https://www.us-cert.gov/ncas/alerts/TA17-132A
  - https://www.justice.gov/criminal-ccips/file/872766/download
  - https://www.justice.gov/criminal-ccips/file/872771/download

About ICS-CERT

The Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors.

https://ics-cert.us-cert.gov

About NCCIC

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

http://www.dhs.gov/national-cybersecurity-communications-integration-center