HHS ASPR/CIP HPH Cyber Notice: On-Going Impacts to HPH Sector from WannaCry

June 2, 2017

DISCLAIMER: This product is provided "as is" for informational purposes only. The Department of Health and Human Services (HHS) does not provide warranties of any kind regarding any information contained within. HHS does not endorse any commercial product or service referenced in this product or otherwise.

Dear HPH Sector Colleagues,

HHS is aware of two, large, multi-state hospitals systems that are continuing to face significant challenges to operations because of the WannaCry malware. Note: this is not a new WannaCry attack.

The behaviors that have been reported are typical for environments where the WannaCry scanning virus persists, even though the encryption stage has been blocked by anti-virus, or is not executing. The virus can persist even on a machine that has been patched. The virus will not spread to a patched machine, but the attempt to scan can disrupt Windows operating systems when it executes. The particular effect varies according the version of Windows on the device. For those devices or systems, we are providing additional guidance below.

We are also sharing FDA's emergency phone line for those with questions or reports of malware affecting devices as part of the recommended reporting process below.

You may send additional questions to cip@hhs.gov

Mitigating risks of WannaCry

WannaCry ransomware is a fast-propagating worm which exploits Windows' Server Message Block version 1 (SMBv1) protocol to move through a network or infect other systems on the Internet. However, SMBv1 might not be the only vector of infection for WannaCry, so even patched systems could still be infected if the malware is introduced to the system in a different manner.

Furthermore, a newly patched system could have been previously infected, and if so, would still scan for other vulnerable systems and/or encrypt files. Patching a system is similar to how in physical

medicine, a quarantine will prevent an infection from spreading however will not cure the patient who has been quarantined. Reimaging removes the infection in the operating system no matter where the virus is residing.

Mitigate the risk of WannaCry infection by:

- Patch vulnerable systems with the update from Microsoft which fixes the SMBv1 vulnerability: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- Disable SMBv1 on all devices, across the network and disable it at the firewall if possible. If it is not possible to disable SMBv1, consider the business-impact for quarantining those devices off the network until another solution can be found.
- See the Tech Support page from Microsoft below for instructions on disabling SMBv1: https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows-server
- Block port 445 on all firewalls
- If possible, reimage potentially affected devices to mitigate risk that malware is on the system in the background.
- Use a reputable anti-virus (AV) product whose definitions are up-to-date to scan all devices in your environment in order to determine if any of them have malware on them that has not yet been identified. Many AV products will automatically clean up infections or potential infections when they are identified.
- Work with vendors to make sure both the distribution stage and the encryption stage of WannaCry are detected and blocked.
- Work with vendors or IT support staff to investigate and remediate systems exhibiting network-scanning activity consistent with WannaCry, which could reimaging per the previous bullet point.

If you are the victim of a ransomware attack

If your organization is the victim of a ransomware attack, HHS recommends the following steps:

1. Please contact your FBI Field Office Cyber Task Force (www.fbi.gov/contact-us/field/field-offices) or US Secret Service Electronic Crimes Task Force (www.secretservice.gov/investigation/#field) immediately to report a ransomware event and request assistance. These professionals work with state and local law enforcement and other federal and international partners to pursue cyber criminals globally and to assist victims of cyber-crime.
2. Please report cyber incidents to the US-CERT (www.us-cert.gov/ncas) and FBI's Internet Crime Complaint Center (www.ic3.gov).
3. ****NEW**** If your facility experiences a suspected cyberattack affecting medical devices, you may contact FDA's 24/7 emergency line at 1-866-300-4374. Reports of impact on multiple devices should be aggregated on a system/facility level.

4. For further analysis and healthcare-specific indicator sharing, please also share these indicators with HHS' Healthcare Cybersecurity and Communications Integration Center (HCCIC) at HCCIC_RM@hhs.gov

Additional Resources

- ICS-CERT: vendor-specific security bulletins and FDA, Center for Devices and Radiological documents: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-135-01H
- Microsoft Security Bulletin MS17-010 – Critical: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- Microsoft Windows Advisory: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- Additional Microsoft Information: https://support.microsoft.com/en-us/help/204279/direct-hosting-of-smb-over-tcp-ip
- US-CERT SMB Advisory and Best Practices: https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices