HHS ASPR/CIP HPH Cyber Notice: Current International Ransomware Campaign

June 27, 2017

Dear HPH Sector Colleagues,

The U.S. government is aware of an international ransomware campaign that may be affecting Healthcare and Public Health Sector assets in addition to other Sectors. Please review the information below and share with colleagues. We will update you as more information becomes available.

You may forward this message broadly with no restrictions.

You may send additional questions to cip@hhs.gov

Thank you-

HHS/ASPR Critical Infrastructure Protection Program

Quick links in the document:

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@hhs.gov

Mitigating against this threat

- Educate users on common Phishing tactics to entice users to open malicious attachments or to click links to malicious sites.
- Patch vulnerable systems with the latest Microsoft security patches: https://technet.microsoft.com/en-us/security/bulletins.aspx
- Verify perimeter tools are blocking Tor .Onion sites
- 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.
- Monitor US-CERT for the latest updates from the U.S. government. See below for current reporting.
- Utilize HPH Sector ISAC and ISAO resources. See below for further information.

US-CERT Resources

Multiple Petya Ransomware Infections Reported

06/27/2017 12:56 PM EDT

Original release date: June 27, 2017

US-CERT has received multiple reports of Petya ransomware infections occurring in networks in many countries around the world. Ransomware is a type of malicious software that infects a computer and restricts users' access to the infected machine until a ransom is paid to unlock it. Individuals and organizations are discouraged from paying the ransom, as this does not guarantee that access will be restored. Using unpatched and unsupported software may increase the risk of proliferation of cybersecurity threats, such as ransomware.

Petya ransomware encrypts the master boot records of infected Windows computers, making affected machines unusable. Open-source reports indicate that the ransomware exploits vulnerabilities in Server Message Block (SMB). US-CERT encourages users and administrators to review the US-CERT article on the Microsoft SMBv1 Vulnerability and the Microsoft Security Bulletin MS17-010. For general advice on how to best protect against ransomware infections, review US-CERT Alert TA16-091A. Please report any ransomware incidents to the Internet Crime Complaint Center (IC3).

Sector ISAO and ISAC resources

National Health Information-Sharing and Analysis Center has shared the following TLP-White Message and will continue to share information at nhisac.org.

HITRUST has shared the following Threat Bulletin for distribution.