HHS ASPR/CIP HPH Cyber Notice: International Ransomware Campaign UPDATE #2

June 29, 2017

Dear HPH Sector Colleagues,

HHS continues to monitor on-going impacts to the HPH Sector from Petya/notPetya ransomware. At this time there is no new information to share about the threat vector. We are tracking the resolution of port closures, medical data software availability, and impacts to pharmaceutical companies and will report to you if we become aware of any long-term impacts to the HPH Sector.

HHS/ASPR CIP will continue to monitor the situation but will no longer provide daily updates unless the situation warrants. We encourage you to connect with relevant trade associations, ISAO/ISACs, and government partners to discuss any long-term concerns related to this ransomware event.

Please review the information below. You may share this message freely with no restrictions. We will update you as more information becomes available.

To join our mailing list please visit:
https://www.phe.gov/Preparedness/planning/cip/Pages/mailinglist.aspx

Thank you-

HHS/ASPR Critical Infrastructure Protection Program

cip@hhs.gov

- If you are the victim of a ransomware attack
- Mitigating against this threat *updated*

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. 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 *updated*

- ***updated*** Our partners at NH-ISAC have tested a "vaccine" that has been reported as potentially helpful for systems that have not been impacted. The "vaccine" may also help spread of infection. Use of this "vaccine" should not preclude proper patching as it only prevents harm from one specific strain of malware. When using this vaccine, consider any potential business impact. The "vaccine" is the creation of a file **C:\Windows\perfc** and setting the permissions to READ ONLY. As with any patch/update, this modification should be evaluated before implementation by appropriate system security personnel. For further information on this "vaccine" please visit https://nhisac.org/nhisac-alerts/petya-ransomware-updates/
- 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
- Utilize HPH Sector ISAC and ISAO resources.