



HHS ASPR/CIP HPH Cyber Notice: International Ransomware Campaign UPDATE #1

June 28, 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. You may forward this message widely with no restrictions.

Dear HPH Sector Colleagues,

The U.S. government is aware of an international ransomware campaign that has affected critical infrastructure sectors including Transportation, Healthcare and Public Health (HPH) Sector assets in addition to other Sectors overseas. Note that impacts external to your facility may affect your ability to provide services. For example, the current cyber attack’s compromise of a Danish shipping company has temporarily limited or stopped container shipping into and out of the Port Authority of New York and New Jersey as well as the Port of Los Angeles which could disrupt supply chains for many sectors, including the HPH sector. Additionally, at least one support company that provides health records services is impacted which may impact the ability to enter information into patient charts and access clinical test results.

Cybercriminals are known to leverage mentions of current events in unrelated phishing schemes. If cybercriminals have not already started to send phishing email messages out with subject lines or texts mentioning NotPetya, it is highly likely these campaigns will occur.

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/maillinglist.aspx>

Thank you-

HHS/ASPR Critical Infrastructure Protection Program

Quick Links in the Document:

- [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*

- ***NEW*** Our partners at NH-ISAC have tested a "vaccine" that has been reported as potentially helpful for systems that have not been impacted. While the use of this "vaccine" should not preclude proper patching, consider the business impact of creating a file C:/Windows/perfc.exe or editing the existing file to make them 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.