U.S. Department of Health and Human Services

Public Health Emergency

HHS Update: International Cyber Threat to Healthcare Organizations

May 2017

This urgent incident-related message is being sent to the ASPR TRACIE listserv on behalf of the ASPR Critical Infrastructure Program.

Ransomware can infect computers multiple ways and may or may not require user interaction.

This message outlines several vectors of attack and what users can do to help protect themselves.

All inquiries regarding this incident should be directed to cip@hhs.gov.

Where can I find the most up-to-date information from the U.S. government?

www.us-cert.gov

https://hsin.dhs.gov (NCCIC portal for those who have access. We are not posting anything to the HPH portal at this time.)

How can I help protect myself from email-based ransomware attacks?

Ransomware can be delivered via email by attachments or links within the email. Attachments in emails can include documents, zip files, and executable applications. Malicious links in emails can link directly to a malicious website the attacker uses to place malware on a system. To help protect yourself, be aware of the following:

- Only open up emails from people you know and that you are expecting. The attacker can impersonate the sender, or the computer belonging to someone you know may be infected without his or her knowledge.

- Don't click on links in emails if you weren't expecting them – the attacker could camouflage a malicious link to make it look like it is for your bank, for example.
- Keep your computer and antivirus up to date – this adds another layer of defense that could stop the malware.

What is HHS doing to secure our systems?

- HHS Office of the Chief Information Officer implemented an enterprise block across all OpDivs and StaffDivs and is ensuring all patching is up to date.
- HHS is working with the Department of Homeland Security to scan HHS' CIDR IP addresses through the DHS NCATS program to identify RDP and SMB.
- HHS notified VA and DHA and shared cyber threat information.
- HHS is coordinating with National Health Service (England) and UK-CERT.
- HHS through its law enforcement and intelligence resources with the Office of Inspector General and Office of Security and Strategic Information, have ongoing communications and are sharing and exchanging information with other key partners including the US Department of Homeland Security and the Federal Bureau of Investigation.

Requests for information, impacts, and indicators

Please notify us at cip@hhs.gov if:

- You identify a new attack vector identified for this ransomware other than email, or the following ports: SMB share and RDP; or
- There are any impacts to patient care or supply chain distribution because of ransomware.

Please share any indicators or cyber threat information with the HHS Healthcare Cybersecurity and Communications Integration Center at HCCIC-mgmt@hhs.gov.

If you are the victim of ransomware

If your organization is the victim of a ransomware attack, please contact law enforcement immediately. We recommend organizations contact their FBI Field Office Cyber Task Force 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. Victims are also encouraged to report cyber incidents to the US-CERT and FBI's Internet Crime Complaint Center.

ASPR TRACIE Resources

ASPR TRACIE has the best and promising healthcare cybersecurity practices available in our Technical Resources domain. Issue 2 of *The Exchange* (released in 2016) highlights lessons learned from a recent attack on a U.S. healthcare system and features articles that demonstrate how collaboration at all levels is helping healthcare facilities implement practical, tangible steps to prevent, respond to, and recover from cyberattacks. The video "Cybersecurity and Healthcare Facilities" features subject matter experts describing last year's attack on MedStar, steps we can take to prevent and mitigate attacks, and what the federal government is doing to address cybersecurity. The Cybersecurity and Information Sharing Topic Collections include annotated resources reviewed and approved by a variety of subject matter experts.

Office of the Assistant Secretary for Preparedness & Response
U.S. Department of Health & Human Services
200 Independence Avenue, S.W. Washington, D.C. 20201