HHS Update #2: International Cyber Threat to Healthcare Organizations

May 13, 2017

Executive Summary from today's Sector call

ASPR CIP held our sector call today with over 1800 participants. The information below is responsive to several requests for information noted on the call. In addition, we would like to flag for the community that a partner noted an exploitative social engineering activity whereby an individual called a hospital claiming to be from Microsoft and offering support if given access to their servers. It is likely that malicious actors will try and take advantage of the current situation in similar ways.

Additionally, we received anecdotal notices of medical device ransomware infection. Please note the directions below for reporting ransomware attacks to FBI.

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

- For overall Cyber Situational Awareness visit the US-CERT National Cyber Awareness System webpage at: https://www.us-cert.gov/ncas
- NCCIC portal for those who have access: hsin.dhs.gov
- FBI FLASH: Indicators Associated With WannaCry Ransomware

Where can I find the latest Microsoft Security Information?

Visit the Microsoft Update Catalog for the latest security updates.

ASPR TRACIE: Healthcare Cybersecurity Best Practices

Our message from May 12, 2017 including information on how to protect from email-based and open RDP ransomware attacks can be found on the TRACIE portal here.

ASPR TRACIE also 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.

Next Sector Call, Monday May 15 1100 ET

Our next call for the Healthcare and Public Health Sector will be Monday, May 15 to include a situational awareness brief from HHS and discussion. This will be an operator-moderated call-- to speak on this call, you will need to press *1. You may share this call information with healthcare cyber professionals across the sector. Additional calls will be scheduled as needed.

Date: Monday, May 15

Time: 1100 ET

Telephone number: 888-576-3153

Participant Passcode: 6989004

How to request an unauthenticated scan of your public IP addresses from DHS

The US-CERT's National Cybersecurity Assessment & Technical Services (NCATS) provides integrated threat intelligence and provides an objective third-party perspective on the current cybersecurity posture of the stakeholder's unclassified operational/business networks.

- NCATS focuses on increasing the general health and wellness of the cyber perimeter by broadly assessing for all known external vulnerabilities and configuration errors on a persistent basis, enabling proactive mitigation prior to exploitation by malicious third parties to reduce risk.
- Attributable data is not shared or disseminated outside of DHS or beyond the stakeholder; non-attributable data is used to enhance situational awareness.
- NCATS security services are available at no-cost to stakeholders. For more information please contact NCATS_INFO@hq.dhs.gov

If you are the victim of ransomware or have cyber threat indicators to share

If your organization is the victim of a ransomware attack, please contact law enforcement immediately.

1. Contact your 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.
2. Report cyber incidents to the US-CERT and FBI's Internet Crime Complaint Center.
3. 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.