HHS Update #3: International Cyber Threat to Healthcare Organizations

May 15, 2017

Important note to those who have requested to join this mailing list

We had an overwhelming response to join our mailing list today. We have not yet completed the addition of all new partners to our mailing list. We will continue to add members and once that is complete, we will re-send this message to all. You may see a re-sending of this message after a further update. We apologize for any confusion.

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

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 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 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.

HHS HCCIC Slack Channel

- HCCIC Slack Channel: Please provide the email addresses of personnel that would like to part of the HHS HCCIC Channel. Send the information to HHSHCCIC@hhs.gov

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
- SMB Vulnerability: SMB version1 is affected as per US-CERT guidance:
- http://www.malwaretech.com
- https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis
- http://www.ransomwarehotline.com
- Second Sink Hole Domain: ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

Open Source Links for Information and Indicators:

- https://www.us-cert.gov/ncas/current-activity/2017/03/16/Microsoft-SMBv1-Vulnerability
- https://www.us-cert.gov/security-publications/Ransomware

Healthcare and Public Health-directed Resources:

- ASPR TRACIE: Healthcare Cybersecurity Best Practices: https://asprtracie.hhs.gov/documents/newsfiles/NEWS_05_13_2017_08_17_11.pdf
- Fact Sheet on the FDA's Role in Medical Device Security: https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf

Receive healthcare intelligence through InfraGard participation

Cyber Health Working Group is a component of Healthcare Intelligence, a national special interest group of InfraGard, the only public-private, non-profit organization affiliated with the FBI. The CHWG is a force multiplier, leveraging its distinct model to connect and collaborate with other organizations and the USG. Partnerships with HITRUST, NHISAC, HHS, and others only make us stronger in the fight to protect the healthcare sector. The three benefits to the group are:

- Peer-To-Peer
- Trusted Forum
- Threat Exchange

The requirements to join:

- Current InfraGard membership or a pending application;
- IT position in a healthcare-related company or organization;
- Access, and ability to share, tactical cyber threat information.

For more information and to register, go to www.intelligence.healthcare.

DHS support for private sector cyber incident table top exercises

Contact the National Cyber Exercise and Planning Program for information about planning your own Cyber Table Top Exercise @ 703-235-5641 or email: cep@hq.dhs.gov.

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

EMS partner activities

EMS partners reported that the NEMSIS TAC has taken precautions to protect against network and computer infection from the latest variants of ransomware. They also recommended their software partners take appropriate actions and report safeguards to clients.