Ransomware Activity Targeting the Healthcare Sector

- The FBI, HHS and the Cybersecurity and Infrastructure Security Agency (CISA) issued a Joint Cybersecurity Advisory about malicious cyber actors targeting the healthcare sector with Trickbot malware, often leading to Ryuk ransomware attacks, data theft, and the disruption of healthcare services. The malware is primarily introduced through phishing scams.
- These issues will be particularly challenging within the COVID-19 pandemic. Administrators will need to consider the potential impact on patient care and ability to maintain operations in the absence of IT systems, and balance this risk when determining their cybersecurity investments;
- Recommended preparedness, mitigation and response activities that hospitals can take are outlined in the advisory and summarized below.

Joint Cybersecurity Advisory (AA20-3020A)

The FBI, HHS, and CISA joint advisory, issued 10/28, details the threat to healthcare providers and precautions to protect their networks. The advisory is available at: https://us-cert.cisa.gov/ncas/alerts/aa20-302a and has been distributed by NYSDOH. The document outlines:

- technical details of the threat the tactics, techniques, and procedures (TTPs);
- indicators of compromise by Trickbot malware and Ryuk ransomware;
- recommended mitigation measures, network best practices, ransomware best practices, and user awareness best practices.

Conference call briefings were conducted on 10/28 and 10/29 to review the advisory and outline preventative steps and mitigation strategies summarized below.

General Preparedness Activities. Below is a list of preparedness activities hospitals should take:

- Rehearse IT lock-down of electronic records, including backup strategies;
- Have a 321 backup strategy for patient information and EMRs (possibly via hard copy);
- Speed any pending patching;
- Prepare to maintain continuity of operations of your essential functions during any outages of IT systems; review and rehearse procedures within the next 24 hours; (see continuity of operations resources developed by IHA at http://www.iroquois.org/emergency-preparedness-continuity);
- Consider powering down IT where not used;
- Prepare limiting use of personal email by staff;
- Prepare for any need to redirect patients during any outages;
- Ensure proper staffing for continuity of operations;
- Know how to contact CISA and FBI for assistance or to report information (see contact information below).

Mitigation Activities. In preparation for potential Ryuk attacks, please consider the following:

- Disable Remote Desktop Services for systems that do not require it;
- Block TCP port 3389 on the firewall, if possible;
- Carefully monitor the indicators associated with this campaign;.
- Monitor e-mail traffic for threats and prevent executable files from reaching end users;
- Refrain from opening attachments or links from unknown sources;
- Implement architectural controls for network segregation;

- Implement allow lists & block lists for specific applications to prevent unauthorized applications;
- Use anti-virus protection and ensure that it is kept updated;
- Use least-privilege to limit administrative access on account;
- Maintain encrypted backups of all critical systems as well as off-site copies;
- Disable macros for documents received via email.

Response Activities. The FBI also recommends that any victims of Ryuk take the following steps in addition to the previous mitigation steps, including, but not limited to:

- Scan system backups for registry persistence;
- Scan system backups for other malware infections, particularly Trickbot and/or Ryuk;
- Execute a network-wide password reset;
- Continue to monitor firewall traffic for known Trickbot and Ryuk communications as well as for known exploit kit traffic.

Resources. Recommended mitigation resources noted in the advisory include:

- Monitor National Cyber Awareness System alerts and advisories are available at https://us-cert.cisa.gov/ncas/alerts.
- Follow ransomware best practices outlined in a ransomware guide recently issued by CISA: https://www.cisa.gov/publication/ransomware-guide.
- Join and engage with cybersecurity and healthcare information sharing organizations to receive critical information and services to better manage ransomware and cyber risk.
    - CISA: cisa.gov, https://us-cert.cisa.gov/mailing-lists-and-feeds | central@cisa.gov
    - FBI: ic3.gov, www.fbi.gov/contact-us/field | CyWatch@fbi.gov
    - HHS/HC3: http://www.hhs.gov/hc3 | HC3@HHS.gov
    - Health Information Sharing and Analysis Center (H-ISAC): https://h-isac.org/membership-account/join-h-isac/
    - Sector-based ISACs: https://www.nationalisacs.org/member-isacs
    - Information Sharing and Analysis Organization (ISAO) Standards Organization: https://www.isao.org/information-sharing-groups/

Reporting Incidents. Below are contacts and recommendations for reporting suspected incidents.

- Report suspicious or criminal activity related to this advisory to your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. Please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
- To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.dhs.gov.
- Report problems with medical devices through the FDA MedWatch Voluntary Reporting Form available at https://www.accessdata.fda.gov/scripts/medwatch. For urgent matters, such as potential medical device impacts related to a cyber-attack affecting your hospital system, please contact CyberMed@fda.hhs.gov.