PUBLICATION

FBI Warns Hospital and Health Care Providers are Under Attack

Authors: Layna S. Cook Rush, Alexander Frank Koskey, III
October 29, 2020

A public cybersecurity advisory was issued yesterday about a likely ransomware attack against the health care and public health sector. The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) have credible information suggesting an Eastern European threat group plans to launch a widespread *Ryuk ransomware attack*.

CISA, the FBI and HHS have issued a joint cybersecurity advisory describing the methods used by cybercriminals to infect systems with Ryuk ransomware. For the threatened attacks to transpire as predicted, it is likely that the information technology systems for many health care providers are already infected by some form of a precursor malware.

It is recommended that hospitals and health care systems become very familiar with the Advisory and implement the following measures within the next 24 hours *(among others noted in the Advisory):*

- **Report all potentially related cyber incidents to your insurance carrier, outside legal cyber counsel, and the FBI 24/7 CyberWatch Command Center at 855-292-3937.**
- Expedite patching response plan within 24 hours.
- Ensure backup of medical records, including electronic records, and have a 321-backup strategy; have hard copy or remote backup or both.
- Immediately establish and practice out-of-band, non VoIP communications.
- Review IT lockdown protocol and processes, including practicing backups.
- Assess any contractual notification obligations you may have to entities for which your health care entity serves as the business associate or partner – making paper/backup copies of such agreements (where possible).
- Ensure the appropriate logging capabilities are on and not simply in default mode.
- Do not allow evidence to be destroyed in the process of rebuilding systems.
- Do not communicate directly with the threat actor without assistance from cyber counsel.
- Ensure you have the ability to make payroll timely to avoid angry employee chatter.
- Avoid making internal or external communications without experienced cyber counsel guidance.
- Engage forensics and mitigation teams at the direction of legal counsel to help protect privilege.
- Print out a copy of your cyber and other insurance policies and become familiar with the coverage and requirements.
- Prepare to maintain continuity of operations, if attacked.
- Review plans within the next 24 hours should you be hit.
- Check that your anti-virus and endpoint detection and response (EDR) are running; a stopped state may indicate compromise.
- Consider limiting use of personal email.
- Be prepared to reroute patients.
    - Have your medical staff assess now how long your entity can be down for a given service line/patient type before the entity needs to transfer for safety reasons.

    - Make sure health care entities have a paper or backup system for scheduling appointments and procedures to avoid patients coming in for procedures that need to be rescheduled.
- Know how to contact federal authorities when phones are down or email has been wiped.
- Consider limiting/powering down non-essential internet facing IT services.
- Limit personal email services.
- Ensure sufficient staffing to maintain continuity of operations with disrupted IT networks.
- Understand the contractual obligations your third-party IT vendors have to you – making paper/backup copies of such agreements (where possible).

The full Cybersecurity Advisory provides technical details, indicators of compromise (IOCs) for Trickbot, Ryuk attack techniques under the MITRE ATT&CK framework, and significantly more detail about mitigation.

You should download the full Cybersecurity Advisory and discuss it with your IT team or IT services provider as soon as possible. Be proactive and take action now.

Our Incident Response Team is on high alert and is available to assist immediately. For any questions, our team leads can be reached at any time (24/7/365):

- Layna Cook Rush, CIPP/US, 225.936.7069
- Alexander F. Koskey, CIPP/US, CIPP/E, 863.640.1269

Note: Download Joint Agency Advisory Here