Potential imminent cyber threat to hospitals and healthcare providers

James J. Giszczak, Dominic A. Paluzzi, Christine N. Czuprynski, Emily A. Johnson, Colin M. Battersby | Thursday, October 29, 2020

The FBI and DHS-CISA have issued a warning about an imminent threat to hospitals and healthcare providers. They have credible information to suggest that there will be a widespread Ryuk ransomware attack this weekend, and the FBI, DHS and the NSA's Cybersecurity Threat Operations Center are currently investigating the threat. Based on recent news and court filings, it is clear that the Trickbot malware infrastructure was recently targeted for disruption by Microsoft and the US Cyber Command.

There is a fear that the targeted healthcare entities likely already have the encryption malware on their systems, the threat actors just have not commanded it to activate.

The government has recommended that hospitals and healthcare providers implement the following measures *as soon as possible*:

- Establish and practice out of band, non VoIP, communications.
- Rehearse IT lockdown protocol and process, including practicing backups.
- Ensure backup of medical records, including electronic records and have a 321-backup strategy – have hard copy or remote backup or both.
- Expedite patching response plan (IRP) within 24 hours.
- Prepare to maintain continuity of operations if attacked.
- Review plans within the next 24 hours should you be hit.

- Power down IT where not used.
- Ensure proper staffing for continuity.
- 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.
- Be prepared to re-route patients if patient care is disrupted due to IT outage.
- Ensure sufficient staffing to maintain continuity of operations with disrupted IT networks.
- Report all potentially related cyber incidents to the **FBI 24/7 CyberWatch Command Center at 855-292-3937**

If no attacks materialize over Halloween weekend, do not take that to mean that the threat has passed. All entities, not just hospital and healthcare providers, should use this opportunity to assess their security vulnerabilities and incident response and crisis management plans.

The McDonald Hopkins incident response team is on stand-by to assist organizations through responding to cybersecurity events. Contact the team's 24/7 hotline at 855-MH-DATA1 (855-643-2821) or connect via email at incidentresponse@mcdonaldhopkins.com.

James J. Giszczak

Dominic A. Paluzzi

Christine N. Czuprynski

Emily A. Johnson

Colin M. Battersby