akerman

Blog Post

Ransomware Targeting Hospitals and Healthcare Providers

October 29, 2020
By Elizabeth F. Hodge

While fighting a surge of new coronavirus infections in many parts of the country, healthcare providers must also be prepared to defend against ransomware. On October 28, 2020, the FBI, the U.S. Department of Health and Human Services (HHS), and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint alert warning of "credible information of an increased and imminent" cybercrime threat to U.S. hospitals and healthcare providers. Cybercriminals are using Trickbot malware to infect the IT systems of health systems and providers with Ryuk ransomware.

The alert notes that responding to this threat will be particularly challenging for healthcare organizations during the COVID-19 pandemic, particularly those organizations currently experiencing surges in coronavirus cases. Further, the alert acknowledges the reality that organizations will have to balance the risk posed by the pandemic against this new cyber threat when determining cybersecurity investments.

According to reports, healthcare systems across the country have already been affected by this threat. In addition, there are likely organizations whose IT systems are infected with the Trickbot malware who do not yet realize it. The alert warns those organizations that have indicators of a Trickbot network compromise to immediately back up and secure sensitive or proprietary data, as the infection

Related People

Elizabeth F. Hodge

Related Work

Data Privacy and Security
Healthcare
Hospitals and Health Systems

Related Offices

West Palm Beach

Health Law Rx

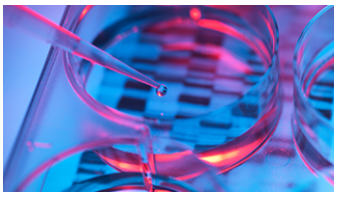
Akerman Perspectives on the Latest Developments in Healthcare Law

Visit this Akerman blog

Coronavirus Resource Center

Visit the Resource Center

may be an indicator of imminent ransomware attack. To assist hospitals and providers with addressing this new threat, the alert lists ransomware prevention steps that organizations should take, including:



- Have a business continuity plan in place and review it to make sure it is still appropriate during the pandemic.
- Test incident response plans immediately. Assess whether changes need to be made to address any changes to the organization as a result of COVID-19.
- Make sure critical patching is current.
- Educate (or re-educate) workforce members about phishing emails.
- Maintain offline, encrypted backups of data and regularly test the backups.
- Regularly backup data, air gap, and password protect backup copies offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, secure location.
- Power down non-essential systems and equipment.
- Do not just focus on Trickbot malware and Ryuk ransomware, as the bad actors have many tools at their disposal and can adapt their methods for deploying ransomware.

Hospitals and providers should also review these patient safety action items:

- Review patient transfer protocols in case critically ill patients need to be moved to another facility. Many transfer agreements and protocols were implemented before the pandemic. Assess whether these plans need to be updated.

- Additionally, consider what happens if multiple facilities in the region are attacked – where can/will the provider safely transfer patients? According to media reports, a recent ransomware attack on a hospital in Germany resulted in a critically ill patient having to be transferred to another facility, and the patient died as a result of the delay in treatment.
- Assess whether the organization will need to increase staffing to deal with a possible influx of patients from other facilities or to assist with the entity's own patients if its systems go down.
- Monitor medical devices for unusual activity and report any such aberrant activity to the FDA. Currently, it does not appear that the FDA is aware of any issues with medical devices as a result of this ransomware threat, but the agency is alert to the possibility.

Finally, healthcare organizations should:

- Report suspicious activity related to the alert to their local FBI field office at 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.
- Report suspected potential medical device impacts related to a cyber attack to the FDA at CyberMed@fda.hhs.gov.
- Continue to monitor alerts from the FBI, CISA, and HHS because this is an evolving situation.
