NOW & NEXT

Data Privacy & Healthcare Alert

FEBRUARY 14, 2022

FBI issues stark warning to hospitals regarding ransomware attacks

By Sarah Swank, Tina Sciocchetti, and Meredith LaMaster

Hospitals should act swiftly to protect vulnerable systems against LockBit 2.0 ransomware.

What's the Impact?

- An increasing number of hospitals have experienced significant operational and financial burdens due to ransomware attacks
- Hospitals should prepare by developing robust cybersecurity protocols and training key personnel to interface with law enforcement in the event of an attack

On February 4, 2022, the FBI released a cautionary report to hospitals warning of potential system compromises due to Lockbit 2.0 ransomware. In the midst of practitioner fatigue, labor shortages, and financial hardships caused by the COVID-19 pandemic, hospitals face the potential threat of losing control of internal operations, exposing patient data, and demands for significant ransoms to regain possession of their network. Ransomware is a form of malicious software, better known as malware, that denies users access to internal computer files, networks,

and systems and, in some cases, results in exfiltration of data.[1] To regain network control and/or prevent data exfiltration, perpetrators demand victims pay ransoms within an allotted amount of time.

"Indicators of compromise associated with Lockbit 2.0 ransomware"

LockBit 2.0 utilizes numerous tactics, techniques, and procedures through its Ransomware-as-a-Service (RaaS) operations to create substantial defense and mitigation barriers. The ransomware infiltrates susceptible networks through insider and purchased access and unpatched vulnerabilities, among other mechanisms. After network access is gained, LockBit's actors increase administrative privileges through publicly available tools. From there, the actors further utilize tools to steal data that is then encrypted. A ransom note with instructions on how to access the decryption software is left in all affected areas of the victim's system. LockBit escalates threats by threatening to leak stolen data, which poses an additional, significant risk to hospitals due to HIPAA. The FBI's warning comes despite LockBit's assertions that it does not hack healthcare organizations.

The impact of prior ransomware attacks

A 2021 study conducted by Ipsos, a multinational market research and consulting firm, indicated healthcare systems are a common target for ransomware attacks, with hospitals accounting for 30% of all large data breaches.[2] It is estimated that these breaches alone cost hospitals $21 billion in 2020.[3] 48% of the 130 hospital executives surveyed by Ipsos experienced a shutdown of some sort in the prior six months due to an external attack.[4] Midsize hospitals faced more significant downtime and financial burdens, with shutdown times averaging almost ten hours, at a cost of $45,700/hour.[5] Larger hospitals experienced a somewhat smaller burden, with shutdown times averaging 6.2 hours and $21,500/hour.[6] Even with the uptick in ransomware attacks and staggering numbers associated with regaining control of their systems, more than 60% of hospital IT teams stated higher priority concerns, with less than 11% citing cybersecurity as a high priority.[7]

---

[1] *See* Ransomware, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware; *See* Preparing for a Cyber Incident, https://www.secretservice.gov/sites/default/files/reports/2021-11/Preparing%20for%20a%20Cyber%20Incident%20-%20A%20Guide%20to%20Ransomware%20v%201.1.pdf.

[2] *See* Perspectives in Healthcare Security, Sept. 9, 2021, https://info.cybermdx.com/hubfs/Downloadable%20Assets/CyberMDX%20Philips_Perspectives%20in%20Healthcare%20Security%20Report.pdf.

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

Preparation and response tips

Cybersecurity[8]

To help guard against ransomware attacks, hospitals should consider implementing the following preventative measures:

- Frequently update operating systems, software, and applications
- Utilize patch systems
- Set anti-virus and anti-malware software to automatically update and conduct regular scans
- Regularly back up data and create an encrypted, offline version of the back-up data not tied to the hospital's computers or networks
- Utilize multi-factor authentication (where appropriate)
- Draft and implement a continuity plan in case the hospital falls prey to ransomware, and ensure that staff is properly trained on how to operate during an attack
- Scan ingoing and outgoing emails
- Adjust firewalls to prevent access to known malicious IP addresses
- If not in use, consider disabling Remote Desktop Protocol (RDP) vulnerabilities
- Restrict personnel privileges for installing and running applications

Reporting to and Working with Law Enforcement

The FBI encourages anyone who believes they may be the victim of a ransomware attack to report information to their local field office. Hospitals may take a number of protective measures if they find themselves in the midst of an attack. The U.S. Secret Service recommends the following steps:

- Keep all systems affected by ransomware powered
- Isolate infected devices and compromised network components
- Collect available information on the ransomware
- Utilize different methods of communication
- Restore the system with the oldest secure backup

In addition, hospital personnel should be prepared to provide details to law enforcement regarding:

- Firewall, event, and active directory logs

---

[8] *See* Ransomware, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware; *See* Preparing for a Cyber Incident, https://www.secretservice.gov/sites/default/files/reports/2021-11/Preparing%20for%20a%20Cyber%20Incident%20-%20A%20Guide%20to%20Ransomware%20v%201.1.pdf.

- DNS (domain name system), web proxy, remote access authorization, DHCP (Dynamic Host Configuration Protocol) lease, router, IDS/IPS (intrusion detection systems/intrusion prevention systems) alerts, anti-virus and anti-malware, VPN (virtual private network), two-factor authentication, SNMP (Simple Network Management Protocol), and SIEM (security information and event management) logs
- Timeline of attack
- Live imaging of breached servers
- Copies of suspected links, emails, or malware

HIPAA Guidance

The HIPAA Security Rule requires covered entities and business associates to adopt policies and procedures to respond to and recover from ransomware infiltrations. This includes conducting frequent offline data backups and implementing a contingency plan with disaster recovery and emergency operations planning. Once an entity is aware, the Office for Civil Rights (sub-agency of the U.S. Department of Education) recommends implementing a security incident response plan to determine the scope of the incident, the origination, the duration, and how it occurred. Covered entities may have HIPAA breach notification requirements, which must be managed in response to a ransomware attack. Unless the covered entity or business associate can demonstrate that there is a "... low probability that the PHI (protected health information) has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred.

Ransom Payments

The FBI does not encourage paying ransoms but acknowledges the significant burdens entities like healthcare systems may face if unable to operate as a result of a cyberattack. Whether a hospital decides to pay a ransom demand or not, the local FBI office should be notified and/or a complaint filed online.

What's next

Some say it is not "if," but "when," hospitals may be hit with a cyberattack. For some, it is happening more than once. These attacks are disruptive to operations, costly, and can impact patient care. As ransomware attacks continue to increase, it is imperative that hospitals invest in the necessary technology and infrastructure to prevent such potentially debilitating threats. Proper protocols and training will enhance preparedness and response. If attacks occur, hospitals should act fast to restore data and operations and comply with reporting obligations.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Sarah Swank
202.585.8500
sswank@nixonpeabody.com

Tina Sciocchetti
518.427.2677
tsciocchetti@nixonpeabody.com

Meredith LaMaster
312.977.9257
mlamaster@nixonpeabody.com