#### **Business Email** Compromise

Employee clicks on what appears to be a legitimate email message with logo from the EMR software company requesting review of document.

The document contains a hidden payload which opens a back door for the hacker.

With data captured on a compromised staff computer, the hacker is able to determine the firm's public IP address. Scanning this address, a **Remote Desktop Service** is discovered on the practice EMR server, so that the doctor could use a laptop at home. No proper security safeguards allow infiltration.



Cadence Cyber is contacted to respond. Cadence works with Homeland Security, FBI, ransom negotiators and attorneys. Negotiators contact RaaS to obtain sample decrypted files, ensuring no more subterfuge. Forensics are performed on remaining practice logs to ascertain the how, why and when of infiltration.



## **Owner Discovers Cadence**

Practice is questioned by Homeland Security. Doctors try to see patients in between disruptive meetings and questions. Practice was found not to be in compliance with HIPAA "security rule". Alaris goes into reactive mode to remediate. Negotiation partner is able to reduce the ransom demand and the decrytion keys were obtained.



HHS, Homeland Security, FBI

# The Anatomy of a Ransom

# Based on a True Story of Medical Practice - Four Week Business Interruption and More Than \$300,000 Impact

# Infiltration



Hackers team up with a customer service provider known as "Ransomware as a Service." The RaaS team encrypts and disables all systems for the doctor's practice. RaaS prepares and sends a broken English email to inform the doctor that his practice is shut down. RaaS and hackers split any monetary gains.

Within hours, Russian-based threat actors move laterally through the network, identifying equipment, treatment room workstations, EMR files with 30 years worth of patient information, insurance, and tax files. Threat actors erase system logs to cover their tracks.



#### **Ransomware as a Service (RaaS)**

## **Disruptive Month**



The Google-advertised firm in Australia claims to be able to decrypt files within 48 hours. **Six hours** is spent transferring records to see if files can be restored (potential HIPAA violation). Meanwhile a scramble begins to figure out how to contact patients and reschedule procedures requiring office equipment.

After several days, the Australian company admits they cannot decrypt the files; although now they have critical practice information. All systems are down! Employees reschedule with paper calendars, no payments are processed, and no medical equipment is utilized. Patient records were the only source of information. **This goes on** for three weeks.

**Fortifying the Gates...** 



**Contacting Australia** 

- Month Revenue Loss Attorney Fees Credit Monitoring Negotiation Fees Ransom Updated Equipment **HIPAA** Violation
- \$168,000 \$ 5,800 \$ 23,000 \$ 12,000 \$ 75,000 \$ 25,000 TBD

Through employee training, detection and automated response systems and new barriers to entry such as zero-trust and two factor authentication, the practice is in a much better position to thwart off other potential ransomware attacks. Once an organization has been hit, they are more likely to be hit again.



**Costly Lesson** 

# **Interesting Brunch**



Doctor receives an alarming and confusing email from the RaaS "customer service department" demanding \$500,000 in crypto-currency to their wallet for the key to decrypt files.

### The Oh Sh\*t Moment



The owner visits the practice confirming phones, network and medical devices are inoperable. 80,000 patient files were encrypted with an ".eking" extension. Before responding to the ransom email, the doctor Googles "what is .eking" and an ad pops up for a company to assist in decryption.

**Final Costs** 

\$308,800



**CADENCE CYBER** INFO@CADENCE-CYBER.COM 813-546-4646