CLM National Conference
March 16, 2018
Houston, Texas

Medical Device Ransomware: The New Reality

I. Ransomware attacks are growing in frequency

Ransomware is malicious software designed to prevent or limit a user from accessing their system until a sum of money is paid. Most ransomware attacks target computer systems, blocking use of emails or files. However, ransomware can affect any type of device that is connected to the internet, making electronic medical devices a target for attacks.

Ransomware attacks on individuals v. organizations

While the majority of ransomware attacks still target consumers, the number of attacks directed at organizations is growing at a more rapid pace. Attacks on businesses increased 3x in 2016, compared to a 2x rate of increase in attacks on individuals. A company is hit with ransomware every 40 seconds.

The reasons for the shift are almost always profit-driven. Successful ransomware attacks against individuals typically net the attacks around $500 in Bitcoin. Infecting a business, on the other hand, represents a much bigger potential payday, especially if the attack can disrupt critical services and/or sensitive information.

Ransomware attacks are becoming easier and more profitable

Experts estimate ransomware attacks generated $1 billion last year. New ransomware as a service platforms are in part key to the growing number of attacks. It is easy for criminals with even the most basic technical knowledge to create their own ransomware through a ransomware platform, which provides everything needed to launch a ransomware campaign (including a management portal) in exchange for agreeing to pay the developers a cut of the ransom profits.

The average ransom demand now tops $1,000, which is more than 3x the average demand in 2015. That jump corresponds with an increase in attacks specifically targeting businesses, and it is further indication that attackers are setting their sights on higher-value victims in search for larger paydays.

While the majority of ransomware attacks (and payments) go unreported, some notable examples of "big-ticket" attacks in the past 12 months include successful scores of $28,000 from Los Angeles Valley College and $21,000 from Madison County in Indiana, as well as a demand of $70,000 from San Francisco's Municipal Transportation Agency, which wasn't paid.

Paying doesn't always work

Of ransomware victims who paid ransom demands, 20% of the victims never retrieved their files. Instead, the attackers walked away with the money and the hijacked information. In some cases the attackers turn around and demand a second ransom. This happened to a Rhode Island law firm. For three months the law firm's computers were held hostage by ransomware. Malware invaded the computer network after a lawyer clicked on an email attachment. It locked down all of the firm's documents and information. The firm claimed to have lost about $700,000 in billable fees before the hackers freed the computer system. The firm first hired computer experts who were unsuccessful in unlocking the network. The firm then paid a ransom in bitcoin to obtain decryption tools from the perpetrators, but the tools did not work. After paying an additional ransom, for a total amount of $25,000 in paid ransom, the lawyers received new encryption tools and recovered most of their information.

Coverage issues for malware attacks

The Rhode Island law firm case is also notable as it involved a coverage dispute. The firm sued to recover the lost business in the amount of $700,000. The insurer has taken the position that it has paid the law firm the policy maximum of $20,000 for losses caused by computer viruses, which are covered under a computers and media endorsement. The insurer says it has no legal obligation to cover other ransomware losses, including lost income. The policy coverage for lost business income applies only when there is physical loss or damage to property at the business premises.

Virtually all standalone cyber insurance policies offer specific coverage for ransomware and other forms of cyber extortion, in addition to other standard coverages.

Covered loss should include reasonable and necessary expenses incurred as a result of a covered threat, including the costs of investigating and assessing a threat, even if no ransom is paid; payment of cryptocurrencies, including bitcoin; any other consideration

or action that may be demanded by the extortionists; and reasonable expenses incurred to mitigate or reduce other covered expenses.

Insurance policies typically contain notification provisions stating that the insured must provide notice "as soon as practicable" after it becomes aware of an incident

Cyber extortion coverage may contain a "consent" provision, which will require the insured organization first obtain the insurer's approval to pay or incur costs, including the payment of ransom.

Like any other insurance policy, a cyber policy may contain exclusions that may significantly curtail and undermine the purpose of the coverage. For example, some insurers insert exclusions based on purported shortcomings in the insured's cyber security.

II. Ransomware attacks in the medical field

Hospitals have been targets of ransomware attacks

Hospitals have been targets of ransomware attacks before - in February 2016, a Los Angeles hospital paid approximately $17,000 ransom in bitcoin to a hacker who seized control of the hospitals' computers systems and would give back access only when the money was paid.

The stakes are raised when a cyberattack goes beyond affecting the computer systems and affects medical devices. In May 2017, the WannaCry ransomware attack hit worldwide, targeting computers running the Microsoft Windows operating system, encrypting data and demanding ransom payments in bitcoin. The WannaCry attack affected over 65 hospitals in the UK, with up to 70,000 devices including computers and MRI machines affected, causing some hospitals to run on an emergency-only basis during the attack. The very next month a Pittsburg Hospital was hit in a major cyberattack of another ransomware.

Medical devices are also susceptible to ransomware attacks

Whereas WannaCry's author's motivation appears primarily financial in nature many types of cyberattack are less obvious. Destruction of data, theft of medical records, doxxing (malicious publication of private or identifying information about an individual), BotNets, etc. are all potential motivations for attackers. Insecure medical devices as well as non-medical devices (i.e. industrial control systems, security cameras, appliances, etc.) that connect to a hospital's network either temporarily or permanently are all potential vectors of attack and expose the Hospital's staff and patients. Essentially any

device that connects directly or wirelessly to a network is at risk for a ransomware attack.

III. Response to ransomware attacks in the medical field

FDA Guidelines

The growing threat of cyber attacks has led the FDA to regulate medical devices. The first FDA guidance for designing new products came out in 2014 and, late last year, it released guidelines for products that are already in the market. The principles are that devices should be designed to be secure, to be able to be updated if flaws are found, and to be safeguard in case of an attack.

Digital Millennium Copyright Act

On October 28, 2016 the Library of Congress updated the Digital Millennium Copyright Act (DMCA) to provide an exemption for security researchers acting in good faith to conduct research on consumer devices. The Library of Congress approves exemptions on a temporary basis and exemptions must be renewed. If an exemption however were revoked third party research on medical device security vulnerabilities would be illegal under the DMCA

IV. Defending against ransomware attacks should be a priority for healthcare providers

The issue for many hospitals remains that they rely on old, unsupported systems. A medical device is expected to live in the field for 30 years while the underlying software components have a much shorter lifespan. Hospitals also tend to not invest in qualified security personnel, and therefore are not following technological threats and advances. This combination makes hospitals an easy target for ransomware attacks. Hospital policies need to be evaluated and updated with technology, upgrades on medical devices should be performed as recommended, and knowledgeable IT personnel should be on staff to monitor potential threats. Having IT personnel is crucial as, if an attack happens, they will be in the best position to mitigate the damage of the attack.

Perpetrators of ransomware attacks have cleverly set the price to decrypt victim's data relatively low when compared to the high cost of a target losing all their data and the high cost of liability in the aftermath. It's the victim's willingness to pay combined with the widespread use of network connected devices that makes it unlikely we'll see these types of attack go away anytime soon.

Of the companies that have experienced ransomware attacks, 7 out of 10 have fallen victim to at least one that got past their security and successfully encrypted their files.

Traditional security solutions are simply struggling to keep up with the incredible pace at which new ransomware variants are being produced.

As a result, some organizations are looking to new solutions that utilize machine learning and behavioral analytics to block ransomware during runtime, while others are simply assuming they'll be infected and are prioritizing response and recovery, instead (some even going as far as to stockpile Bitcoin in anticipation of paying off attackers).

For large breaches it can be nine to 12 months before an insured delivers their view of the loss to their carrier. Involving the forensic accountant earlier in the process can help mitigate some surprises later and gives the insurer better control of the claim and its expenses.