Ransomware

AN OVERVIEW

RYAN PATRICK — VP, Fortified Health Security

Fortified HEALTH SECURITY

fortifiedhealthsecurity.com | 615-600-4002 | 2555 Meridian Blvd Suite 250, Franklin, TN 37067

Ransomware

Ransomware! The word alone strikes fear in the hearts of CIOs, CISOs and hospital administrators alike. Since the Anthem breach, there have been several hospitals across the U.S. and many more globally that have been affected. One hospital, reportedly, was turning away patients.

WHAT IS RANSOMWARE?

Ransomware is malicious software which blocks access to a computer system or data in some way until a sum of money is paid. Some forms of ransomware systematically encrypt files on the system's hard drive, which then become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying.

There are a few different attack vectors or methods:

- Ransomware typically propagates as a trojan, whose payload is disguised as a seemingly legitimate file.
- Ransomware can be downloaded by unwitting users by visiting malicious or compromised websites.
- It can also arrive as a payload, either dropped or downloaded by other malware.
- Some ransomware is delivered as attachments to spammed email.
- The most significant threat can often be ransomware which connects to file shares, encrypting centrally stored data which is critical to operations.

WHAT IS THE HISTORY?

The first known ransomware was the 1989 "AIDS" trojan (also known as "PC Cyborg") written by Joseph Popp. Basically, victims would receive a floppy disk (remember those?) labeled "AIDS Information Introductory Diskette" and booting the malicious software would hide directories and encrypt the files on the C drive. It then prompted the victim to renew a license and contact PC Cyborg Corporation to admit payment ($189) which was sent to a P.O. Box in Panama. It had limited success because the method of delivery was "snail mail" and the age of home computing was still in its infancy.

There was a pretty significant lull in activity until 2005 when a new type of ransomware was utilized: Misleading Apps. This malware exaggerated the impact of issues on the computer and required payment to "fix" the issues with the infected system.

The evolution continued in 2008 when “Fake Anti-virus” software was introduced. This software fakes scans claiming to find large numbers of threats and security issues on the computer. The user would then be prompted to make a payment for software that would remediate all the issues found.

In 2011, we began to see “Locker” ransomware which would disable access and control of the computer, effectively locking up the computer from use.

Today, we are seeing what most people recognize as ransomware: Crypto-Ransomware. This is what we’ve seen in the news where the malware encrypts local and network file shares and databases.

WHAT CAN YOU DO TO PROTECT YOUR ORGANIZATION?

Bottom line: Defense in depth. The best prevention is proactive security measures around people, process and technology.

Of all the risks to an organization, regardless of industry, it is the employees that pose the greatest concern. Organizations must be diligent in effectively training and educating their employees on acceptable use and what to look for. At minimum, security and awareness training at minimum must:

- Be continuous and engaging
- Create awareness of the threat
- Promote safe web browsing practices
- Warn against clicking embedded links in unverified emails
- Encourage employees to scrutinize emails before opening them
- Underscore backing up important files offline
- Be tested via solutions like phishing

Furthermore, at the organizational level, end-user least privilege must be implemented. All users should be operating WITHOUT administrative rights. This seems so obvious and simple yet we come across organizations that haven’t enforced this.

Organizational processes need to reflect industry best practices in addressing known attack vectors and vulnerabilities. These are often loosely followed and not well-documented, but prove to be extremely effective at preventing breaches, aiding in incident response and creating operational efficiencies. The first thing I would recommend is backups, backups, backups! This is best method of reacting to a ransomware incident. If you’re able to recover data from backups then there is no reason to pay the ransom. It’s important to note that the backups should be done offline/physically disconnected from your computing environment.

> “The best prevention is proactive security measures around people, process and technology.”

An organization must have approved and continuously tested organizational policies and procedures. With regards to ransomware, the following should be in an approved policy and tested at least annually:

- Disaster Recovery
- Business Continuity
- Incident Response
- Breach Notification

Additional organizational processes around vulnerability management, penetration testing (client-side attacks), annual risk assessments and application blacklisting should be fully vetted and mature in order to prevent a successful ransomware attack.

In order to complete your defense and maintain a strong security posture, the following technologies should be considered:

- Security Information & Event Monitoring (SIEM)
- Intrusion Prevention System/Intrusion Detection System
- SPAM/Email Filters
- Web Content Filters
- Anti-Virus/Anti-Malware
- NextGen Firewalls
- Data Loss Prevention (DLP)
- USB Lockdown
- Vulnerability Scanning

WHAT WILL THE FUTURE HOLD?

Knowing that, if I was any good at predicting the future, I would already be independently wealthy after hitting the lotto several times, I will attempt to give a high-level prediction of what we could see in the next 12 months:

- **High-profile spear/targeted attacks** – much like phishing; targeted attacks to increase effectiveness are all but inevitable. Attackers will eventually learn from past successes and start to exploit this method.
- **Exfiltration of data** – Attackers will not only get organizations to pay them for access to their own data but they will siphon it off the network and sell it on the black market…making money twice.
- **Network devices** – Attackers would completely crush an organization by denying network access at the core.

Ransomware is a real threat and it works – unfortunately. Organizations need to employ a defensive, in-depth approach around people, process and technology in order to prevent attacks. My best and final recommendation is to find a partner to help…

CONTACT US TO START ON THE PATH FROM COMPLIANCE TO CONFIDENCE.

For more information, visit our website at:

fortifiedhealthsecurity.com

INQUIRIES

1 (615) 600-4002

sales@fortifiedhealthsecurity.com

OFFICE

2555 Meridian, Suite 250
Franklin, TN 37067

ABOUT THE AUTHOR

Ryan Patrick is a Vice President of Fortified Health Security where he focuses on increasing client security posture through driving collaboration between sales and operations teams. Prior to joining Fortified, he served as the Deputy Chief Information Officer for the New York State Division of Military and Naval Affairs and as a Director of a Security & Privacy healthcare IT consulting practice, in addition to working in the information security office for organizations such as MetLife and Memorial Sloan-Kettering Cancer Center. He currently holds an M.B.A. from Norwich University, the Certified Information Systems Security Professional (CISSP) certification and is a HITRUST Common Security Framework (CSF) certified practitioner.

ABOUT FORTIFIED HEALTH SECURITY

Fortified Health Security is a leader in information security, compliance and managed services, focused exclusively on helping healthcare professionals overcome operational and regulatory challenges everyday in regards to HIPAA, HITECH, and Meaningful Use. Founded in 2009, Fortified has established a heritage of excellence, compliance and innovation. Today, Fortified partners with healthcare organizations across the continuum, serving health systems, single hospital entities, physician practices, post acute providers, payors and business associates. *www.fortifiedhealthsecurity.com*.