THE RISE OF RANSOMWARE IN HEALTHCARE: NEW THREATS, OLD SOLUTIONS

22ND NCHICA ANNUAL CONFERENCE
AUGUST 2016

CHUCK KESLER – CISO, DUKE HEALTH
JON STERNSTEIN – STERN SECURITY
INTRODUCTIONS

Chuck Kesler

• Chief Information Security Officer, Duke Health
• Prior to Duke, led Symantec’s Security Advisory Services team in the US
• NCHICA Board Member
• 30 years of IT technical and management experience
INTRODUCTIONS

Jon Sternstein

• Founder & Principal Consultant at Stern Security
• Former Healthcare Security Officer
• Co-chair of NCHICA Security Workgroup
• SANS Institute – Mentor
  – SANS 560: Network Penetration Testing and Ethical Hacking
AGENDA

- Overview of the ransomware threat in healthcare
- Anatomy of an attack
- Applying old solutions to this new problem
- Is it a breach?
WHAT IS RANSOMWARE?

- Malware that extorts a user or organization by encrypting files until a ransom is paid
- Variants have been observed for several years, but are becoming increasingly sophisticated
- The ransoms demanded may range from a few hundred to thousands of dollars, and often must be paid in Bitcoin
- Access is usually restored after the ransom is paid
RANSOMWARE ISN’T NEW

• In 2012, a Symantec report estimated that a single ransomware command & control server could yield $33,600 per day in ransoms
• In 2014, the Town of Greenland, New Hampshire had a ransomware attack that resulted in the loss of 8 years worth of electronic records
• In 2015, the FBI received more than 2,400 ransomware complaints, which totaled $25M in damages
• Individuals are also being targeted
HOW DO THESE INFECTIONS OCCUR?

• Phishing (link clicks and attachments)
• Drive-by-downloads (e.g. from malicious advertisements)
• Web server vulnerabilities

Common denominators: missing patches, poor access controls
WHY IS RANSOMWARE SO EFFECTIVE?

Organizations that aren’t prepared to respond are intimidated into taking quick and possibly rash action

• Inability to contain a spreading attack forces systems to be taken offline
• Lack of good backups and contingency plans forces organizations to consider paying ransoms
• Sometimes, even the backups have been compromised
HEALTHCARE IN THE CROSSHAIRS

• Hollywood Presbyterian
• MedStar
• Kentucky Methodist Hospital
• Chino Valley Medical Center
• Desert Valley Hospital
• Alvarado Hospital Medical Center
• King’s Daughters’ Health

HealthcareIT News Survey of Hospitals: How many ransomware attacks have targeted your organization in the last 12 months? 75% have had at least one.
EVOLVING RANSOMWARE THREATS

• Spreading via server vulnerabilities (MedStar)
• Attackers using 0-day vulnerabilities
• Potential for a coordinated, time-delayed attack
• Potential for data breach
So, is it a breach?
IS IT A BREACH?

HHS recently released guidance that provides guidelines for ransomware breach analysis and reporting:

http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

“Part of a deeper analysis should involve assessing whether or not there was a breach of PHI as a result of the security incident. The presence of ransomware (or any malware) is a security incident under HIPAA that may also result in an impermissible disclosure of PHI in violation of the Privacy Rule and a breach, depending on the facts and circumstances of the attack.”
"When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a “disclosure” not permitted under the HIPAA Privacy Rule.

Unless the covered entity or business associate can demonstrate that there is a “...low probability that the PHI has been compromised,” based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred. The entity must then comply with the applicable breach notification provisions..."
IS IT A BREACH?

Some considerations for a Ransomware breach analysis:

• What ransomware variant was involved?

• Does that variant have a history of data exfiltration?

• If a new variant, work with security researchers to determine its behavior

• Look at network logs and file access audit trails to determine if there is evidence of data exfiltration

• Also consider the impact to data integrity and availability

• Thoroughly document your findings
ANATOMY OF AN ATTACK
STERN SECURITY LAB PRESENTS
Methodist Hospital (Kentucky)
• Declared State of Emergency
• Shut down all workstations
• Attackers demanded $1600 (4 bitcoins)
• Back to paper for 5 days
Hollywood Presbyterian Medical Center

• Paid $17,000 (40 bitcoins) to regain access
• **Systems were down for 10 days**
• Back to paper records
• Some patients redirected to other hospitals
TECHNICAL ANALYSIS

Technical overview
1. Delivery
2. Execution
3. Encryption
4. Payment
5. Decryption
MALICIOUS DOCUMENT

Infection
- Enabling Macros = Infection
- Runs in memory
- Grabs complete malware from Internet
- Deletes traces of itself
MALICIOUS COMMUNICATION

Communication

• Connects to Command & Control using a Domain Generation Algorithm
  – Example: On August 29th, 2016 use YYISIEJAOOO.COM

• Gets Encryption Keys
• Determines Cost
• Gets Ransom Note
MALICIOUS ACTIVITY

Execution

• Deletes Volume Shadow Copies
• Adds itself to Startup
• Encrypts files
• Encrypts network shares
• Delivers Ransom Note
Bitcoins
- Anonymous Payment
- Buy Bitcoin @ Coinbase
- Receive decryption software
- Must purchase for each infected machine
- Will you get your files back?
RANSOMWARE IN HEALTHCARE

Kansas Heart Hospital

- May 2016
- **Paid ransom, but didn’t get decryption keys**
- Malware authors demanded second payment
- Hospital refused to pay second ransom
RANSOMWARE BREACHES

Encrypts and Steals Data
- Chimera Ransomware - 2015
- Crysis Ransomware - 2016
- Reportable Breach
It’s not just Windows anymore!

- Official “Transmission” BitTorrent client for Macs was infected
- Signed with valid certificate
- Apple revoked certificate
RANSOMWARE MALVERTISING

- March 2016
- Affected sites: MSN, BBC.com, the New York Times, AOL, Newsweek and more.
- Malicious advertisements
- Criminal acquired ad domains after they expired
OLD SOLUTIONS FOR NEW PROBLEMS
SOLUTIONS

Implement Security Best Practices

• Nothing new here – same practices apply to ransomware

• Basic concepts: protect, detect, respond, and recover

• SANS 20 Critical Security Controls
  https://www.sans.org/critical-security-controls
Application Whitelisting

- Can completely prevent ransomware
- Only allow known good applications
- Caveat: you have to know what apps you want to allow, which can be difficult in a dynamic environment
**PROTECT**

- Patching – operating systems, Office, Adobe, browsers, etc.
- Remove unnecessary software
- Web filtering
- Block suspicious attachments
- Block/whitelist Office macros
- Network share access controls – minimize write permissions!
- Much more…
PROTECT

Backup Important Files

- Must test data recovery
- HIPAA requirement
  - Data backup plan (R) § 164.308(a)(7)(ii)(A)
  - Data backup and storage (A) § 164.310(d)(2)(iv)
DETECT & RESPOND

Intrusion detection & prevention

• Identify potential "command & control" communications
• Automatically drop traffic to known bad actors
• Need 24x7x365 coverage for monitoring and response, which can be a huge challenge for smaller organizations
DETECT & RESPOND

Awareness – don’t forget about Layer 8!

• Make sure users and IT personnel can recognize the signs of a ransomware attack and know what to do if one occurs

• Successfully containing a ransomware attack hinges on quick recognition and reporting of the issue
RESPOND & RECOVER

Be prepared!

• Assume the worst may happen
• Have cybersecurity insurance in place
• Identify those who need to be involved in managing a significant incident
• Practice with tabletop exercises
• Decide and document how decisions will be made about paying ransoms
• Have a Bitcoin account ready
• Know your local FBI and law enforcement contacts
  – Report ransomware attacks to the FBI via www.ic3.gov
RESPOND & RECOVER

Basic steps for incident response still apply for ransomware:

• Contain the spread of the ransomware
• Eradicate the ransomware from affected systems
• Restore affected systems and data to return to normal operations
• Perform a post-incident review, including breach analysis
• Document lessons learned and implement improvements
HELP! WE HAVE RANSOMWARE... NOW WHAT?!
Part II: Solution
RANSOMWARE HELP

Home Solutions

• PC
  – CryptoPrevent software

• Mac
  - Application Whitelisting: Google’s Santa Project
  - Firewall: Little Snitch
# RANSOMWARE HELP

1. NoMoreRansom.org
2. Master List

   A. Lists ways to decrypt files (if available)
   B. [https://goo.gl/VnAjsn](https://goo.gl/VnAjsn)

<table>
<thead>
<tr>
<th>Name</th>
<th>Extensions</th>
<th>Extension Pattern</th>
<th>Comment</th>
<th>Encryption Algorithm</th>
<th>Also known as</th>
<th>Decryptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>.CryptoHasYou.777</td>
<td>.enc</td>
<td>.[timestamp]$<em>{email}$.777 e.g. .14-05-2016-11-59-36$</em>{<a href="mailto:ninja.gaiver@aol.com">ninja.gaiver@aol.com</a>}$</td>
<td></td>
<td>AES(256)</td>
<td>XOR</td>
<td><a href="https://decrypter.emsis">https://decrypter.emsis</a></td>
</tr>
<tr>
<td>7ev3n</td>
<td>.R4A</td>
<td></td>
<td></td>
<td>XOR</td>
<td>7ev3n-HONE$T</td>
<td><a href="https://github.com/has">https://github.com/has</a></td>
</tr>
<tr>
<td>.Block8</td>
<td>.block8</td>
<td></td>
<td>Based on HiddenTear</td>
<td>AES (256)</td>
<td></td>
<td><a href="http://www.bleepingcom">http://www.bleepingcom</a></td>
</tr>
<tr>
<td>Alpha Ransomware</td>
<td>.encrypt</td>
<td></td>
<td></td>
<td>AES(256)</td>
<td>AlphaLocker</td>
<td><a href="http://download.bleeping">http://download.bleeping</a></td>
</tr>
<tr>
<td>AutoLocky</td>
<td>.locky</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="https://decrypter.emsis">https://decrypter.emsis</a></td>
</tr>
<tr>
<td>BedBlock</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REFERENCES AND BACKUP SLIDES
REFERENCES

• Methodist Hospital Declares State of Emergency

• Hollywood Presbyterian Medical Center pays ransom
  – http://www.theregister.co.uk/2016/02/18/la_hospital_bitcoins/
  – http://arstechnica.com/security/2016/02/hospital-pays-17k-for-ransomware-crypto-key/

• Kansas Heart Hospital asked to pay two ransoms

• Malicious Advertisements on major news sites

• Evolution of ransomware

• Brian Krebs – Krebs on Security blog
  – http://krebsonsecurity.com/tag/ransomware/

• Google's Santa Project
  – https://github.com/google/santa
REFERENCES

• Ransomware that encrypts and Steals Data – Crysis

• Ransomware Master List
  – https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml#

• Ransomware Prevention Tips
  – https://sternsecurity.com/blog/ransomware-prevention-tips

• The Complete Ransomware Guide
  – https://blog.varonis.com/the-complete-ransomware-guide

• US CERT advisory
  – https://www.us-cert.gov/ncas/alerts/TA16-091A

• SamSam
  – http://blog.talosintel.com/2016/03/samsam-ransomware.html

• Ransomware exploiting Jboss vulnerabilities

• Locky

• CryptoPrevent
PROTECT

Endpoint Protection
• Starts traditional signature-based anti-virus, but much more
• Also validate files with behavioral and reputational techniques
• Host-based firewalling and intrusion detection/prevention
• Many endpoint protection features may not be enabled by default – enable them!
• Won’t prevent, but can help contain and eradicate a ransomware attack
Patching

• Critical operating system patches (yes, Mac & Linux too!)
• Web servers
• Web browsers
• Office applications
• Flash, Silverlight, Quicktime, and other similar browser plugins
• Extra credit: remove Flash, Silverlight, etc. if not needed, or consider using plugins that selectively block ads and Flash content
Email Filtering

- Spam control
- URL re-writing
- Virus scanning

- Block suspicious attachments: .exe, .jar, .scr, .bat, .aru, .cmd, .vbs, .7z, .ex, .ex_, .ex1, .pif, .application, .gadget, .com, .hta, .cpl, .msc, .vb, .vbe, .js, .jse, .ws, .wsf, .wsc, .wsh, .ps1, .ps1xml, .ps2, .ps2xml, .psc1, .psc2, .scf, .lnk, .inf, .reg, .docm, .dotm, .xlsm, .xltm, .xlam, .pptm, .potm, .ppam, .pps, .sldm, .msi, .msp, .mst
PROTECT

Limit permissions on network shares

• Ensure that only those who need access to shares have access
• Write permissions should be strictly limited
• Discontinue the use of any world-writeable shares!
• Keep in mind that ransomware can affect cloud-based file sharing services too
Network segmentation

- Avoid flat internal networks
- Create zones where systems with similar security profiles are grouped
- Require traffic between zones to flow through firewalls
- Monitor for malicious traffic between zones
- Implement using Virtual Routing and Forwarding (VRF) technology
- Caveat: requires sophisticated network engineering and knowledge of application data flows