Healthcare Held Hostage: Ransomware Attack Prevention and Response

June 2017
# Table of Contents

Overview ................................................................................................................................. 3  
Ransomware Trends and Impacts in Healthcare ................................................................. 5  
  The Evolution of Ransomware ......................................................................................... 5  
  Ransomware Attack Techniques ...................................................................................... 6  
  To Pay or Not to Pay? ....................................................................................................... 7  
Case Study: The WannaCry Attack ..................................................................................... 8  
  What is WannaCry? ......................................................................................................... 8  
  What is Unique about this Attack? .................................................................................. 9  
Ransomware Prevention and Response ............................................................................ 11  
  Ransomware Prevention and Response Checklist ............................................................ 12  
Conclusion ............................................................................................................................. 14
Overview

Ransomware attacks are rippling through the healthcare industry and have been creating significant challenges for organizations that have fallen victim. These attacks involve holding critical healthcare systems hostage until payment has been received to unlock or decrypt the hijacked data. Malware trends show that the criminals behind ransomware attacks are beginning to favor healthcare organizations and the onslaught is likely to continue in 2017 and beyond. According to cybersecurity insurance firm Beazley, ransomware attacks more than quadrupled in 2016, with nearly half happening in the healthcare sector¹.

The *WannaCry* ransomware attack in May 2017 demonstrated the susceptibility of the healthcare industry to attack and exposed potential damaging impacts to patient care, treatment, and critical systems and information. The attack also demonstrated weaknesses that are common to the industry as organizations struggle to prevent and respond to large-scale ransomware incidents.

Ransomware attacks can cause substantial damage in terms of lost productivity, patient care impact due to unplanned downtime, and financial costs associated with response and recovery activities. Some organizations have had to resort to paying cybercriminals to release critical systems. Maintaining disaster recovery plans, effective vulnerability and malware defenses, employee awareness training, and incident response processes can go a long way in handling ransomware attacks and limiting losses.

Meditology advises healthcare entities on information security and privacy protections including building and sustaining programs to prevent, detect, and respond to ransomware attacks. This report provides an update on recent ransomware attacks and provides recommendations for preventing and responding the ransomware incidents.

*Figure 1– WannaCry ransomware notes*²

---


Preventing and Responding to Attacks

Effective ransomware prevention and response hinges upon the development and execution of a formal information security strategy and program.

The figure below provides a summary of specific activities that healthcare entities should perform to fortify networks and systems and respond effectively to a ransomware attack. Further details including a detailed ransomware prevention and response checklist can be found later in this report.

---

Stay Informed of Latest Variants and Attacks
Formalize and Test Incident Management Program
Document and Test Disaster Recovery Processes
Conduct Awareness Training for Phishing
Patch Vulnerabilities & Address Outdated Systems
Update Anti-virus and Conduct Routine Scans
Monitor Network for Anomalous Activity
Remove Local Administrative Rights for Users
Scan for Phishing Attempts and Enhance Spam Filters
Conduct Routine Penetration and Tabletop Tests

Figure 2– Ransomware prevention and response checklist
Ransomware Trends and Impacts in Healthcare

The Evolution of Ransomware

Ransomware is not a new phenomenon. Attacks have been around since as early as 1989, with the introduction of the PC Cyborg malware\(^3\). The sophistication and frequency of attacks, however, has seen a sharp increase in recent years. The specific targeting of the healthcare industry is also a more recent development along with the ability to obfuscate payments using bitcoin technology.

![PC Cyborg ransomware note](image)

**Figure 3– PC Cyborg ransomware note\(^4\)**

The fundamental approaches to defending against ransomware attacks have not changed a great deal since the introduction of ransomware attacks, although the specific technical attacks and defense methods have continued to evolve. Ransomware has also become far more lucrative, with some reports estimating ransomware as a billion-dollar industry in 2016\(^5\).

---


Ransomware Attack Techniques

Ransomware is typically delivered through a combination of channels ranging from phishing attacks, spam emails with malicious attachments, drive-by downloads where users visit a malicious website, and USB flash drive infection. Common ransomware attack vectors and techniques are outlined in the following table:

<table>
<thead>
<tr>
<th>Ransomware Attack Techniques</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Phishing**                | • Phishing is the primary entry point for many of the most recent ransomware attacks.  
                              • Phishing attacks attempts deliver ransomware by tricking users into clicking links in emails that appear legitimate. |
| **Spam**                    | • Attachments are included in spam emails that once clicked will deliver the malicious ransomware payload.  
                              • Microsoft Office macros are a common malicious attachment type in ransomware spam emails. |

---

### Ransomware Attack Techniques

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Drive-by Downloads</strong></td>
</tr>
<tr>
<td>• Ransomware is often delivered to users that visit websites that have been infected with malicious code.</td>
</tr>
<tr>
<td>• Legitimate websites may have components or advertisements that can be an infection source.</td>
</tr>
<tr>
<td><strong>Infected USB Flash Drives</strong></td>
</tr>
<tr>
<td>• USB storage devices are a common entry point for ransomware and other malicious programs that can execute when plugged into a new device.</td>
</tr>
<tr>
<td><strong>Outdated Operating Systems &amp; Missing Patches</strong></td>
</tr>
<tr>
<td>• Ransomware campaigns often use known vulnerabilities such as those found in web browsers, Operating Systems, and other applications to infect systems.</td>
</tr>
<tr>
<td>• Outdated systems such as Windows XP or unpatched computers are prime targets for the introduction of ransomware.</td>
</tr>
<tr>
<td><strong>Exploits</strong></td>
</tr>
<tr>
<td>• Exploits for ransomware strains vary widely, which makes it more difficult for organizations to effectively prevent attacks.</td>
</tr>
<tr>
<td>• Black/darknet market tools and exploit kits are often leveraged.</td>
</tr>
<tr>
<td>• Client-side vulnerabilities are targeted (e.g. unpatched browsers and systems, Flash Player weaknesses, Adobe Reader vulnerabilities).</td>
</tr>
<tr>
<td><strong>File Shares</strong></td>
</tr>
<tr>
<td>• Several strains of ransomware are built to target file shares and encrypt related files.</td>
</tr>
<tr>
<td>• Attackers know that healthcare organizations and users tend to have excessive access rights to multiple business-critical file shares.</td>
</tr>
<tr>
<td><strong>Self-Propagation</strong></td>
</tr>
<tr>
<td>• Some strains of ransomware including the <em>WannaCry</em> attack are computer worms, which means that they are designed to self-propagate across systems.</td>
</tr>
</tbody>
</table>

### To Pay or Not to Pay?

The most effective way to respond to a ransomware attack is to rely upon the restoration of backup data to a known, uninfected state. In other circumstances, organizations may choose to accept a certain degree of data loss if backups are not sufficient or available.

Ransomware payments to malicious actors are a last resort and not recommended by federal agencies as they perpetuate the business model for attackers. There is also no guarantee that ransomware payments will result in decryption of data or action on the part of the attackers. Some organizations have paid substantial ransoms due to inadequate backup and recovery capabilities. Payments can range from thousands to multi-millions.

---


Case Study: The *WannaCry* Attack

What is *WannaCry*?

*WannaCry* is a specific strain of ransomware that infected the National Health Society and healthcare other organizations across the globe in May 2017, including government institutions in China, Russia, the United States, and much of Europe. The attack infected and disrupted health systems, causing delays in patient care, infections of medical devices, and other adverse impacts to patient care delivery.

![Figure 5– WannaCry ransomware note](image)

*WannaCry* leverages a vulnerability in Server Message Block (CVE-2017-0144) to infect systems. The attack targets systems running Windows Server 2012, Windows 8, and older Windows operating systems including Windows XP.

*WannaCry* targets and encrypts 176 file types including databases, multimedia files, archive files, and Microsoft Office documents. The attack was notable for its speed and effectiveness of proliferation in a relatively short time period.

---

What is Unique about this Attack?

The attackers behind the *WannaCry* ransomware campaign leveraged a recently-leaked National Security Agency (NSA) hacking tool and exploit. The NSA discovered a vulnerability in Microsoft's software that was codenamed *EternalBlue*. This exploit was leaked by a hacker group called the Shadow Brokers earlier this year and leveraged in the deployment of the *WannaCry* malware campaign.

Although the *EternalBlue* vulnerability was patched by Microsoft shortly after it was discovered in March 2017, there was still relatively little time for healthcare entities to apply a patch before the brunt of the attack hit the industry in May of the same year. Microsoft also took the rare step of issuing a patch for outdated and unsupported Operating Systems including Windows XP.

The *WannaCry* malware strain is a computer worm, which is a special kind of malware that is designed to self-propagate across systems. The speed and effectiveness of the attack raised alarm for organizations that were infected as well as healthcare entities whose defenses were not up to par to tackle a prospective *WannaCry* infiltration.

The United States was for the most part left unscathed by the *WannaCry* attack, as the early spread of the malware in Russia, Ukraine, Taiwan, and Europe. For US-based healthcare entities, the next attacks and variants of the *WannaCry* ransomware could very well have a greater impact. The *WannaCry* incident serves as a warning shot for many healthcare entities to continue to build defensive and preventative measures to address future ransomware attacks.

![Image](image.png)

*Figure 6–Countries targeted by WannaCry Ransomware*¹⁰

---

The *WannaCry* attack was stifled by a fortunate discovery by a malware analysis engineer who detected “kill switch” that allowed the attack to be shut down by redirecting the domain associated with malware\(^\text{11}\). Other ransomware attacks and versions of *WannaCry* are unlikely to provide such convenient shutdown mechanisms.

Source of the *WannaCry* attack has not been confirmed, but early indicators in investigative reports point to tools found from the Lazarus group, a well-organized and sophisticated hacking group. However, this attack appears less careful in its execution than typical Lazarus operations\(^\text{12}\). Profits for this specific attack were relatively low given the scale of infection; the initial profits were estimated at about $70,000.


Ransomware Prevention and Response

Effective ransomware prevention and response depends upon the development and execution of a formal information security strategy and program. Specific measures can be taken by healthcare entities to prevent, detect, and reduce the impact of ransomware events.

The following section includes prescriptive guidance and checklist activities for battling ransomware in healthcare settings.

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stay Informed of Latest Variants and Attacks</td>
</tr>
<tr>
<td>Formalize and Test Incident Management Program</td>
</tr>
<tr>
<td>Document and Test Disaster Recovery Processes</td>
</tr>
<tr>
<td>Conduct Awareness Training for Phishing</td>
</tr>
<tr>
<td>Patch Vulnerabilities &amp; Address Outdated Systems</td>
</tr>
<tr>
<td>Update Anti-virus and Conduct Routine Scans</td>
</tr>
<tr>
<td>Monitor Network for Anamalous Activity</td>
</tr>
<tr>
<td>Remove Local Administrative Rights for Users</td>
</tr>
<tr>
<td>Scan for Phishing Attempts and Enhance Spam Filters</td>
</tr>
<tr>
<td>Conduct Routine Penetration and Tabletop Tests</td>
</tr>
</tbody>
</table>

*Figure 7– Ransomware Prevention Checklist*
Ransomware Prevention and Response Checklist

1. **Stay Informed**: Ransomware variants and attacks are evolving and applying a variety of techniques to gain unauthorized access to systems. Keep abreast of the latest attacks including *WannaCry* and implement specific countermeasures to prevent these attacks.

☐ Address the following *WannaCry*-specific prevention steps:
   - Install the MS17-010 patch issued by Microsoft
   - Disable the SMB v1 protocol
   - Filter and monitor port 445 traffic
   - Disable Microsoft Office macros

☐ Get involved with one or more cyber threat information sharing organizations and obtain routine updates on common and emerging cyber threats to the healthcare sector including the FBI and HITRUST CyberThreatExchange (CTX).

2. **Incident Management**: Incident management plans and exercises are crucial to an organization’s survival after a ransomware attack has been initiated. An incident management plan is especially important with ransomware due to quick proliferation and large-scale spread of ransomware threats.

☐ Develop and document a formal security incident response plan.

☐ Conduct routine (e.g. annual) security incident response tabletop exercises and run through simulated ransomware attacks.

3. **Business Continuity and Disaster Recovery**: The effectiveness of business continuity and disaster recovery plans are critical to quickly recover from a ransomware incident and limit the financial and care delivery impact of such an incident. Organizations with proper backups can recover from ransomware downtime much faster and potentially minimize the impact of the event.

☐ Update formal disaster recovery and business continuity plans, policies, and procedures.

☐ Conduct routine tabletop incident simulation exercises to validate system recovery and restore processes.

☐ Conduct routine backup restoration testing for key systems.

4. **Education Training and Awareness**: Malicious actors often use methods like phishing and scam emails to infect their targets with ransomware. Proper education and training initiatives are vital to teach users about the importance of exercising caution when accessing suspicious or unfamiliar emails.

☐ Conduct ongoing end user awareness training and phishing simulation exercises.
5. **Vulnerability and Patch Management:** Ransomware campaigns use known vulnerabilities such as those found in web browsers and other applications to infect systems. Vulnerability management activities help minimize this risk and if done correctly can limit ransomware infections. Outdated systems such as Windows XP or unpatched computers are prime targets for the introduction of ransomware. Proper patching is also necessary to prevent the spread of ransomware.

- Perform an inventory of outdated operating systems in use including workstations, servers, and medical devices. Identify systems running Windows XP and other unsupported platforms.
- Consider isolating systems on the network running outdated operating systems including medical devices.

6. **Endpoint Protection:** Organizations can mitigate known ransomware, malware, and viruses by making use of endpoint protection software and host based firewalls and anti-malware protection.

- Validate anti-virus and anti-malware solutions are up to date and are configured to conduct regular scans.

7. **Audit Logging and Monitoring:** Proper audit logging and monitoring initiatives are needed to ensure that threats such as ransomware are detected quickly and managed effectively. Logging and monitoring capabilities also support the ability for organizations to eradicate ransomware from the environment and identify activities that may be symptomatic of related malware infection or breach.

- Monitor systems and network activity for potential intrusions or suspicious activities.
- Review available signatures and plugins for your Intrusion Prevention and Detection Systems (IDS/IPS) and enable related alerts.

8. **Configuration Management:** Ransomware incidents can be minimized or contained when the organization places strict configuration controls on computing resources.

- Identify and remove local administrative rights for workstations and systems for end users.
- Disable Microsoft Office macros.

9. **Transmission Protection:** Many ransomware variants can infect website visitors or email attachments. Effective web filtering and other transmission protection mechanisms can prevent the introduction of malware that delivers or spreads ransomware. Such protections can also prevent the ransomware from communicating with the attackers.

- Scan incoming and outgoing emails for possible phishing attempts.
- Enable or enhance strong spam filters to prevent phishing emails from reaching end users.

10. **Ongoing Testing and Due Diligence**

- Conduct routine penetration testing / ethical hacking exercises.
Conclusion

Ransomware attacks in the healthcare sector have increased in both frequency and sophistication over the last several years. The spike in ransomware infections in healthcare in 2017 has demonstrated the relative vulnerability of the industry and potential damaging impacts to patient safety, healthcare delivery, and the financial effectiveness of healthcare entities.

HIPAA and regulatory compliance is no longer the only prominent business driver for information security in healthcare. To limit the impact of ransomware attacks, healthcare organizations must prioritize the development of robust information security and risk management programs and focus efforts on backup and recovery, anti-phishing protections, applying patches, and other recommendations outlined in this report.

About Meditology

Meditology Services LLC is a healthcare-focused advisory services firm with core principles of quality, integrity, loyalty, and value. Our executive team has an average of 15 years of consulting and operational experience in healthcare with provider and payer clients nationally of varying size and complexity. We understand the importance of relationships and derive much of our business from a long list of satisfied clients who value the quality of our work products combined with the professionalism, approach, and innovative solutions we bring to our engagements. Meditology services clients across the U.S. with offices in Atlanta, Philadelphia, San Diego, Denver, and Nashville.

Meditology Services LLC
5256 Peachtree Road, Suite 190
Atlanta, GA 30341
info@MeditologyServices.com
Tel. (404) 382-7591
www.meditologyservices.com