Enterprise Network Protection Against Cyberattacks Primer: Ransomware Attacks the Healthcare Industry

A TrendLabs℠ Primer

Ransomware, which renders files inaccessible for a ransom, is real. It has been heavily banking on an individual's or an organization's valuable data for profit. Due to its lucrative nature, more and more cybercriminals are now using ransomware to embezzle money from individuals and enterprises around the world. In fact, recent media coverage and the spike of ransomware attacks against various industries – particularly the healthcare industry – echo the **2016 Trend Micro Predictions** that this year will be the Year of Online Extortion.

In this primer, we will dissect how ransomware can manifest across different layers of an enterprise's infrastructure and how it uses information from previous incidents as leverage to impact targeted businesses more. We will also discuss how ransomware can be detected and prevented at each layer, and how individuals or enterprises can effectively protect their data without paying any ransom.

Indiscriminate Extortion Schemes

Like any other online extortion scheme, a **ransomware** attack can mean significant monetary loss to a victim– may it be through a ransom payment or lost business transactions. The loss of personal files with sentimental values may be difficult, but the consequence of losing valued corporate and business files proves to be more troublesome, more expensive, and perhaps even more damaging in terms of its cost to business.. During our research, we've observed that the lack of appropriate defenses and backups can easily make users vulnerable to a ransomware attack. And in the event of a successful ransomware attack, a hacker may set a ransom (with an **average price range of 0.5-5 BTC**) based on the specific value of the data that they've accessed.. In addition, a successful ransomware attack can also tarnish an organization's reputation as issues on legal and/or compliance may be raised.

Without a robust and secure environment, hospitals (or any other organization) will be viewed as soft targets that can be targeted frequently. Once a ransomware successfully encrypts all critical and sensitive information – along with other high-valued assets – an organization's privacy and operational security is immediately put at risk, thus leading organizations to pay the ransom just to retrieve the files taken hostage. Knowing that an entire organization's privacy and security is at risk pushes attackers to maximize the leverage they have based on the content they are holding hostage.

Ransomware Attack in Healthcare Facility

The **healthcare industry** is facing serious threats like data breaches, information theft, and recently ransomware. Hospital systems operate over public networks and even on the internet, which makes them vulnerable to hacking and other forms of cyberattacks. Apart from being heavily reliant on data, a hospital's focus on prioritizing patients' health rather than cybersecurity makes them even more susceptible targets.

As illustrated in the recent spate of healthcare-focused ransomware attacks, losing access to up-to-date patient information when providing critical care is enough reason for any organization to worry. Without quick access to patient records, urgent surgeries and medical procedures can be delayed or canceled, and it may also drive hospital personnel to revert to paper documentation—, which is a large impact to operations. Then there is always the worst-case scenario of jeopardizing human life—a real-life impact of ransomware attacks in the industry.

Early in 2016, **Locky**—the encryption-based ransomware strain that deletes original versions of the files—hit the **Methodist Hospital** in Henderson, Kentucky. The attack left the hospital in an "internal state of emergency" as personnel were unable to access patient files. The attack came in via phishing emails, particularly in the form of MS Word® documents laced with malware. The perpetrators demanded four bitcoins (approximately USD $1,600) for the decryption key. In order to prevent the attack from spreading and compromising other systems, the hospital shut down all of its desktop computers and transferred to its backup system while the main system was incapacitated by the ransomware. No ransom was paid, nor was a single patient information compromised.

However, the **Hollywood Presbyterian Medical Center** wasn't as fortunate. Prior to the Methodist Hospital attack, the Los Angeles hospital experienced a similar crippling extortion scenario, which significantly impacted the hospital's systems. It appears the hackers specifically targeted this hospital perhaps knowing about their vulnerabilities since the institution coughed up a considerable ransom—40 untraceable bitcoins which is approximately US $17,000—to the hackers. We are likely to see more targeted ransomware attacks against organizations that can pay higher amounts of ransom based on their risk profiles.

Ransomware as a Growing Threat to all Enterprises

Ransomware is particularly noteworthy among hospitals and other organizations because it denies users access to the system instead of stealing data. Victims can only regain access to their affected files in two ways: either restoring data from a backup (without it, business operations can be disrupted) or paying the ransom (which is no guarantee of successful decryption and it also inadvertently funds the activities of the cybercriminals for future attacks).

As previously seen in the Locky ransomware hospital attack where a weaponized Microsoft® Office email attachment was sent, the common attack vector is a phishing or spam email where the target is tricked into clicking a link or attachment in what appears to be a legitimate email (may include the user's name and mailing address). With several ransomware variants now out in the market, cybercrooks—even those without advanced knowledge—are capable of launching costly and devastating attacks that take advantage of a user's predisposition to trust links and attachments in emails.

The ransomware family **CryptXXX**, for instance, works by getting users to click links to, or visit, compromised websites. To avoid early detection, CryptXXX can also check if the target system is running on a virtual environment. Then there is the **ZCRYPT** ransomware family that targets Windows® 7 (and later versions) which can be spread through a USB flash drive—meaning it can embed itself onto external or removable drives and infect any machine that it can connect to via a USB port. Similarly, ZCRYPT can infect every connected machine in an organization if the ransomware is downloaded over a shared network drive.

And as if malicious URLs and spam emails aren't enough, the **SAMSAM** crypto-ransomware is particularly notable because the ransomware infects systems through unpatched server vulnerabilities—servers that have not been kept up-to-date or are out of support like Windows® Server 2003 systems. SAMSAM also encrypts files across networks and is even known to manually locate and delete network backups to coerce companies to pay the ransom. Once the security flaws are exploited, SAMSAM infects the unpatched servers with backdoors and webshells.

Solutions and Recommendations

The threat ransomware poses is more significant than ever, as it broadly targets end users, small and medium-sized businesses, and even large organizations. It's high time that enterprises should start thinking of a layered solution and begin implementing holistic and consistent security practices. As countless successful attacks have demonstrated, ransomware is not going away anytime soon. And the best mitigation for the perils of this type of malware is to have operational practices and security controls in place that can minimize the risk and the damage of ransomware to individuals and businesses.

To stay clear from ransomware, it is important to keep security software updated and avoid suspicious attachments and sites. Additionally, besides employee education, back-up strategies should be evaluated regularly (including **copies stored off site**), risk assessment exercises should be performed, and limitation of access to critical data and shared drives should be practiced.

With ransomware attacks, paying the ransom may be the simple way to go, but Trend Micro and law enforcement agencies like the **FBI** recommend that individuals and organizations should never pay the ransom. . A better strategy is to add additional layers of security that can help thwart ransomware attacks.. To help, Trend Micro offers **free tools** such as the **Trend Micro™ Crypto-Ransomware File Decryptor Tool** that can recover encrypted files locked by certain variants of crypto-ransomware without the use of a decryption key. Meanwhile, the **Trend Micro™ Lock Screen Ransomware Tool** is designed to detect and resolve locked screens caused by ransomware.

In building your ransomware strategy, Trend Micro's broad portfolio of security solutions can be used to deploy a multi-layered approach to protecting users and organization from this formidable threat. Since email is the number one threat vector for ransomware, this large attack surface is one where organizations need to start. Most ransomware can be prevented through effective monitoring of email traffic and filtering out emails with potentially unsafe attachments, links, and other malicious payloads. For organizations using Microsoft Office® 365, Trend Micro™ **Cloud App Security** was able to block over two million threats that weren't detected by the built-in Office 365 security. The Trend Micro™ Cloud App Security blocks threats through malware scanning and file risk assessment, sandboxing, document exploit detection, and web reputation. For non-cloud enterprise email deployments, Trend Micro™ **Deep Discovery Email Inspector** can identify and block spear phishing threats in ways that a traditional email gateway cannot– making it an effective overlay to existing security practices.

While email may be the number one attack vector, endpoints are still found to be a common target for ransomware like CryptXXX, and other newer variants appearing regularly. Trend Micro's™ **Smart Protection Suites** have endpoint security that can minimize the risk of ransomware through behavior monitoring and proactive detection of ransomware files, whitelisting of all trusted applications, and vulnerability shielding. For other network protocols and attack methods that can leave you vulnerable to ransomware such as ZCRYPT, a reliable network defense offering like Trend Micro™ **Deep**

Discovery Inspector is a recommended addition. It can detect malicious traffic, command and control (C&C) communications, attacker behavior, zero-day exploits, and other ransomware-related threats that can spread within your network. Deep Discovery also integrates with Trend Micro email and web gateways, endpoint, server protection, and third party solutions to provide a connected threat defense where threat intelligence is communicated across multiple layers.

Attacks on servers, including corporate file shares that house many important documents, can be particularly disruptive to an organization. As underscored in the case of the SAMSAM ransomware, **patch management** is crucial to minimize exploitation of vulnerabilities. **Deep Security** can protect servers across the hybrid cloud (physical, virtual, and cloud) from the threat of ransomware with suspicious activity detection, software vulnerability shielding, and lateral movement detection.

Find out more: **http://www.trendmicro.com/us/security-intelligence/enterprise-ransomware/index.html**

Created by:

TrendLabs

The Global Technical Support and R&D Center of Trend Micro

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**

Securing Your Journey to the Cloud

www.trendmicro.com