ISSN 2277-3061
Volume 17 Number 1
International journal of Computers and Technology

Impact of Ransomware on Cybersecurity

Yaya Itai Phd

Non-Executive Director at ITAIN Bell School Ikeja Lagos Nigeria

Emmanuel Onwubiko

Ojo LGA of Lagos State Nigeria

Abstract

This paper attempts to discover ransomware exposing the lack of cyber-security. It intends to elicit attention with regards to ransomware, a newly emerged cyber threat and to help organizations; IT practitioners understand the need for cyber security knowledge and awareness plus types of tools used. The paper also discusses methodologies trends and research recommendation on cyber-security threats and provides probative strategic strategy.

Keywords: Cyber Security, Ransomware, Malware, Vulnerabilities, hacker and Port Control

1.0 INTRODUCTION

Ransomware is a type of malicious software that attempts to obtain money from a computer user or organization by infecting systems and blocking access. This is typically done through encryption of the files and documents on the victim's machine, then demanding a sum of money to provide the keys to decrypt the files.

There are a number of ways a hacker can initiate an attack, with the most common being a phishing email. This is where the victim is tricked into clicking on a link, or opening an attachment in what appears to be a legitimate email message. The malicious software is then covertly installed on a computer, without knowledge or intention of the user. It can then either stay dormant or spread without user interaction, depending on the type of attack, until it receives a command from the hackers systems to encrypt the files or lock the computer. As soon as the data is encrypted, the user receives the ransom notification and the clock starts ticking (Karl Simpson, July 31, 2017)

Skill and resources are the two elements that make up an attacker's arsenal. An attacker, however, cannot set out to break security or even perform sophisticated attacks without finding weak points in a system first. Massive malware attacks, email-borne heists, hacked devices, and disrupted services these require vulnerability in the network, whether in the form of technology or people, in order to be pulled off. Unfortunately, ransomware attack exposes the lack of cyber security; poor implementation of technologies adds to the likelihood of threats being realized.

The characteristic of today's malware that distinguishes it from previous generations of malware is its degree of customization. Broadly speaking, ransomware is malicious software designed to either lock a victim's screen (locker ransomware) or encrypt their files (crypto-ransomware). In today's bustling world one would be hard pressed to walk into a business without some type of technology present. Industries of all types small and large also must maintain and secure many types of different hardware, software, networks, and web technology depending on their individual mission and infrastructure.

2.0 BACKGROUND

Practicing cyber security is not as easy as patching a server or counting on the IT department and third party software vendors to ensure all vulnerabilities have been mitigated. During cyber security assessments performed by the National Security Test Bed from 2004 to 2006, the most common and easily attackable vulnerabilities were clear text communications over networks, use of default user accounts and weak or documented passwords, poor authentication practices, unpatched components, and misconfigured firewalls (Fink, Spencer, & Wells, 2006). All of these vulnerabilities have one commonality – they require user or administrator action to resolve. Education of IT professionals in this realm is lacking. In 2005, the President's Information Technology Advisory committee estimated that "there are less than 250 active cyber security or cyber assurance specialists in the United States, many of whom lack formal training or extensive field experience (President's Information Technology Advisory Committee, 2005)." What about user education and responsibility? The IT department cannot ensure the user does not document their password, leave their screen unlocked, lose a company laptop or take proprietary company information outside of the building. In order to successfully secure information, every employee must be afforded cyber security training and guidance and understand company policies as well as non-compliance consequences for violations. The single most important cyber security vulnerability today is the lack of employee training, guidance and policies regarding information assurance protection.

3.0 METHODOLOGY

Cyber criminals are constantly innovating and every cyber-attack is constructed using well-defined phases, which are completed sequentially. Unfortunately, there is no silver bullet. There's no single technology methodology that can protect against ransomware, and for effective defense a combination of technologies along with right processes and skilled security professionals is a must to have. Rendering a cyber-attack unsuccessful is all about blocking one or more of these stages (Ravi Mishra 2017). Establishing a 24/7 security operations center (SOC) is a must to have for single point visibility of the entire cyber security exposure.

- Security Awareness & Training – One of the most effective ways to secure any organization. Continuous security training & simulations can help reduce the risk significantly.
- Vulnerability Assessment (VA) & Patch Management – Continuous VA & Patch Management is a very effective measure.
- Email Security Gateways (Perimeter Security) – Email being one of the most common channels used to spread malware, requires a strong focus. Organizations can also consider dedicated email ATP technologies from major security vendors.
- Firewalls / Next Generation Firewalls (Perimeter Security) –scan all traffic for malicious activity and block / alert when required.
- Web Security Gateways (Perimeter Security) – Prevent drive by attacks and infections from visiting infected websites
- Anti-Virus (AV) / Endpoint Protection Platforms (Endpoint security): Platforms based on machine learning will serve the purpose better than traditional ones. There are even dedicated Ant-Ransomware solutions out there.
- Application Whitelisting (Endpoint security) – There are dedicated solutions out there for this, as well as AV solutions and OSes with this capability.
- Port Control (Endpoint Security) – Restrict USB access by using solutions like Group Policies
- Backup – A multitude of backup solutions exists, choose the one that suits your need so that you can quickly restore in case of an infection. Make sure that the backup is not infected. If taking cloud / network backup, do not map it as a network drive
- Network Sandboxing – Helps analyze malicious files / payloads if they bypass the perimeter controls or can augment perimeter security controls.
- Network Segmentation / Micro-segmentation – A number of solution exists and infection in one segment will not spread to others if properly implemented
- Ad-Blocker –check out the browser store should in case is not present.
- Browser / Application Virtualization – Will prevent machine infections from malicious websites as the Application (Browser) is running in a virtual instance.

4.0 Business Impact

The impact of ransomware to an organization is independent on the industry in which it operates. For example, a lack of cyber-security may lead to the following;

- **Reputational damage** – Loss of customer and stakeholder trust can be the most harmful impact of ransomware event, since the overwhelming majority of people would not do business with a company that had been breached, especially if it failed to protect its customers' data. This can translate directly into a loss of business, as well as devaluation of the brand you've worked so hard to build. Taking a reputational hit may also affect your ability to attract the best talent, suppliers and investors.
- **Theft** – While ransomware is a big-name, banks may net the attacker a sizeable haul, smaller businesses' defenses are typically less sophisticated and easier to penetrate, making them a softer target. Cyber-enabled fraud leads to monetary losses, but stolen data can be worth far more to hackers, especially when sold on the Dark Web. For example, the 2015 'Hidden Data Economy' report by Kaspersky Labs puts the value of login credentials to hotel loyalty programs or online auction accounts at up to $1,400. Intellectual property theft may be equally damaging, with companies losing years of effort and R&D investment in trade secrets or copyrighted material – and their competitive advantage.
- **Financial losses** – Ransomware costs large business disproportionately more than small businesses when adjusted for organizational size. For a large corporation, the financial impact of a breach may run into the millions, but at their scale, the monetary implications are barely a blip on the radar. Large businesses shell out an average of $38,000 to recover from a single data breach in direct expenses alone (Kaspersky Lab, 'Damage Control: The Cost of Security Breaches', 2015). A casual stance on security could quite easily put you out of business.
- **Fines** – As if direct financial losses weren't punishment enough, there is the prospect of monetary penalties for businesses that fail to comply with data protection legislation. Global authorities are considering tougher regulations; one of the most draconian measures proposed by the European Parliament for a privacy breach, applicable from 25 May 2018, is a fine of 20 million euros, or 4% global annum revenues whichever was the higher– a sum that would threaten many growing businesses with insolvency.
- **Below-the-surface costs** – In addition to the economic costs of incident response, there are several intangible costs that can continue to blight a business long after a ransomware event itself. The impact of lack of cyber security disruption tends to be woefully underestimated – especially among firms that have little in the way of

formal business resilience and continuity strategies – and small organizations that already struggle to manage cash flow may face crippling rises in insurance premiums or see an increased cost to raise debt.

5.0 RECOMMENDATION

- **Map Architecture** – What technologies are present in the business? How are they connected? Do these technologies connect to any outside sources?
- **Conduct a Risk Assessment** – Going through the architecture, what vulnerabilities exist? What is the impact of a breach? What areas are extremely high impacts? Is there a plan in place in case of a data loss?
- **Digital Asset Identification** – Conduct an inventory of the physical locations of digital assets. Are assets physically secured?
- **Profile Model** – List assets in order of priority of protection. Identify critical assets
- **Identify and Remove Vulnerabilities** – Patch vulnerabilities found during previous steps/inventories. Remove unused programs and services.
- **Standardize Policies** – Review or create policies for the protection of all assets and specifically critical assets. Ensure policies are standardized and all employees understand compliance with policies is critical.
- **Incident Response** – Logs/documentation should be kept during installation and recovery of systems. Log files should be reviewed on a regular basis to track possible breaches/security incidents.
- **Training** – On the job training should take place on a recurring basis in accordance with policies. Training should be tailored for users and administrators. Leadership must set the example for strong security practices.

6.0 CONCLUSIONS

In conclusion, ransomware and lack of cyber-security cannot be overemphasized; as the threat landscape has primarily changed into an organized and profitable vehicle for writing viruses, spyware, and other malicious code. As many large businesses have robust IT departments and resources to create more secure use of technology.

The single most important cyber security vulnerability today is the lack of employee training, guidance and policies regarding information assurance and protection. Statics show that cyber-attacks are growing at an alarming rate. With the creation of new technologies at the same speed.

For this reason today's threats are more serious and are increasingly complex to be tackled with a traditional security approach. To make matters more complicated, the IT ecosystem is changing at a fast pace with increased numbers of uniquely different vulnerabilities and a widening variety of networking environments only being the tip of the mobility iceberg.

Employee productivity, remote access, and centralized access control add to the list of challenges. As companies hold important customer information and equally important business intelligence information in which the loss of can have catastrophic consequences. Therefore, I believe that a more user-centric approach to protecting digital assets is paramount. In addition to antivirus and firewalls, properly implemented endpoint security requires additional technologies that also need to be centrally manageable (e.g., antispam, antispyware, and application control) as well as adaptively adjustable to new threats and environments.

7.0 REFERENCES

1. Ravi Mishra, "Technology Stack for Ransomware Protection" 2017
2. Karl Simpson, " Ransomware on the rise" 2017
3. President's Information Technology Advisory Committee. (2005). *Cyber Security: A Crisis of Prioritization.* Arlington: National Coordination Office for Information Technology Research and Development.
4. Lorenzo Franceschi-Bicchierai (2016)"Researchers Found a Hacking Tool that Targets Energy grids on the dark web, motherboard".
5. LizardStresser botnets using webcams, IoT gadgets to launch DDoS attacks', SC Magazine, July 2016 www.scmagazineuk.com/lizardstresser-botnets-using-webcams-iot-gadgets-to-launchddos-attacks/article/506962
6. https://www.linkedin.com/pulse/fallchill-onwubiko-emmanuel/
7. https://www.linkedin.com/pulse/wannacry-ransomware-onwubiko-emmanuel

Dr Yaya Itai Core competences are in Information Technology, Control, Fraud Management, Business Process Improvement, Business Continuity management to Disaster Avoidance, ISO 27001 Standards, Operations Management, Project and Change management, and Information Security. Specialties: Fraud Management-behavioral monitoring, Technology Control, Strategic Information Systems Planning, Change management, Business Transformation, Process improvement, E-business solutions design, Systems integration, Operations/Service management, Systems evaluation & selection, and Information Systems management, Software Engineering, Database Management Systems, Modeling and Simulation, Software Systems Architecture, Computational Intelligence, Algorithm Design and Analysis, Data Structures, Computer Networks and Data Communications, Computer Architecture, Data Mining and Data Warehousing, Distributed Systems, Computer Security and Data Encryption and Translation Systems.