A Review of Ransomware Attacks and its Impact on the Bank Sector

Merikh Ahadi[1], Eronimus A[2]

[1]PhD Scholar, Central University of Punjab
[2]Assistant Professor, Central University of Punjab

Abstract

Ransomware is an online attack perpetrated by cybercriminals who demand ransomto release hold on encrypted or stolen data. In the past few years, ransomware attackshave evolved to complex malware with advanced encryption capabilities that now primarily target public and private sector organizations such as banks.

This paper covers ransomware basics including how this malware works and its known attack vectors, type of damages caused by ransomware attacks to banks, andexplanation of bank's strategies in order to prevent, detect and eradicate ransomwareinfections.

Keywords: Ransomware, cyber threats, financial sector

Introduction

Ransomware is a type of malware that prevents or limits users from accessing their system, often encrypting data in an unrecoverable fashion. Ransomware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Ransomware is one of cybercrime'sstrongest business models today and it has crippled organizations like Banks acrossthe globe.

In a ransomware attack cyber criminals use malware with encryption to hold victim'scritical data ransom preventing them from being able to access their systems until the victim pays. Cyber criminals will often start a ransomware attack through email tricking users into clicking a malicious link or opening a weaponized attachment thatspreads malware on an organization's network. It's becoming much easier for cybercriminals to execute ransomware attacks through ransomware as a service and cryptocurrency is enabling the smooth money transaction.

The best strategy is one that prevents banks from ever having to decide whether to pay the ransom or not the first place to start is email which continues to be the top Attack vector. Organizations must block malicious emails with a secure email gateway that provides advanced inbound outbound and internal scanning that use machine learning to continuously improve the detection of sophisticated attacks caneven further enhance protection. Banks should take a look at their data protections in the worst-case scenario of a successful ransomware attack the ability to recover important data can give banks greater control to protect and preserve corporate datawhile reducing exposure to risk.

In the following sections, I have reviewed ransomware basics and I have provided suggestions to help banks to better prepare for ransomware attack and I have highlighted important steps that should be taken before and after a ransomware attack.

Research Methodology

For this paper, I have performed my research based on specific criteria related to ransomware. First, my research is based on recent studies, from year 2015 onwards.Additionally, my sources include only scientific journals and conference papers; this is to ensure that the collected information is authentic. Finally, I only focus on my topic of interest: the threats caused by ransomware to Banking Sector.

Reference number	Purpose/Motivation	Methodology
[1]	Explore research endeavors in ransomware Highlight issues and potential	Literature review
[2]	Ransomware attacks in organization (Mainly IOT devices).	Literature review
[3]	Evaluate the evolution of ransomware and its behavior	Literature review
[4]	Ransomware can be avoided through Prevention techniques.	Literature review
[5]	Intensive review of ransomware and previous research	Literature review

Research Gap

In the reviewed papers, there is not enough information about ransomware attack vectors. In the reviewed papers, there is no effective suggestion that can help Banksto prepare for ransomware attacks.

Research Contribution

In the following sections, I have tried to review ransomware basics and provide suggestions to help banks to better prepare for ransomware attack and I have highlighted important steps that should be taken before and after a ransomware attack.

Common ransomware attack vectors

Ransomware attacks involved a variety of infection vectors. Even so, ransomware actors prefer some methods over others. Below are some of the most important andpopular attack vectors [7].

Unsecured remote desktop protocol connections: Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which provides a user witha graphical interface to connect to another computer over a network connection.

Email Phishing: Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

Exploitation of software vulnerabilities: Software vulnerabilities are weaknessesor flaws present in software codes.

Unsafe web browsing: Unsafe browsing involves overlooking important actions that are intended to secure our online sessions. The most persistent unsafe browsinghabits by users, however, are visiting sites that are not securely encrypted.

Social engineering: Social engineering is the act of exploiting human weaknesses to gain access to personal information and protected systems. Social engineering relies on manipulating individuals rather than hacking computer systems to penetratea target's account.

How does ransomware work and what type of damage it can do tobanks?

Ransomware can originate from a malicious website that exploits a known vulnerability, phishing email campaigns, social engineering, or web-based drive bymalware injections. When the exploit is executed a downloader is placed on the system. The downloader silently communicates with control servers to download and install ransomware and secure an encryption key. The contacted C&C server responds by sending back the requested Encryption Key and provide payment methods then the ransomware starts to encrypt the entire hard disk content, personalfiles and sensitive information. A warning is displayed on the screen with instructions on how to pay for the decryption key.

Most ransomware attacks appear to have a financial motive. In some cases, what initially appears to be a ransomware attack can be a destructive attack that's designedto destroy digital assets and data rather than release them unharmed to their rightful owners. A destructive attack uses malware to wipe system components, corrupt dataand render enterprise devices inoperable.

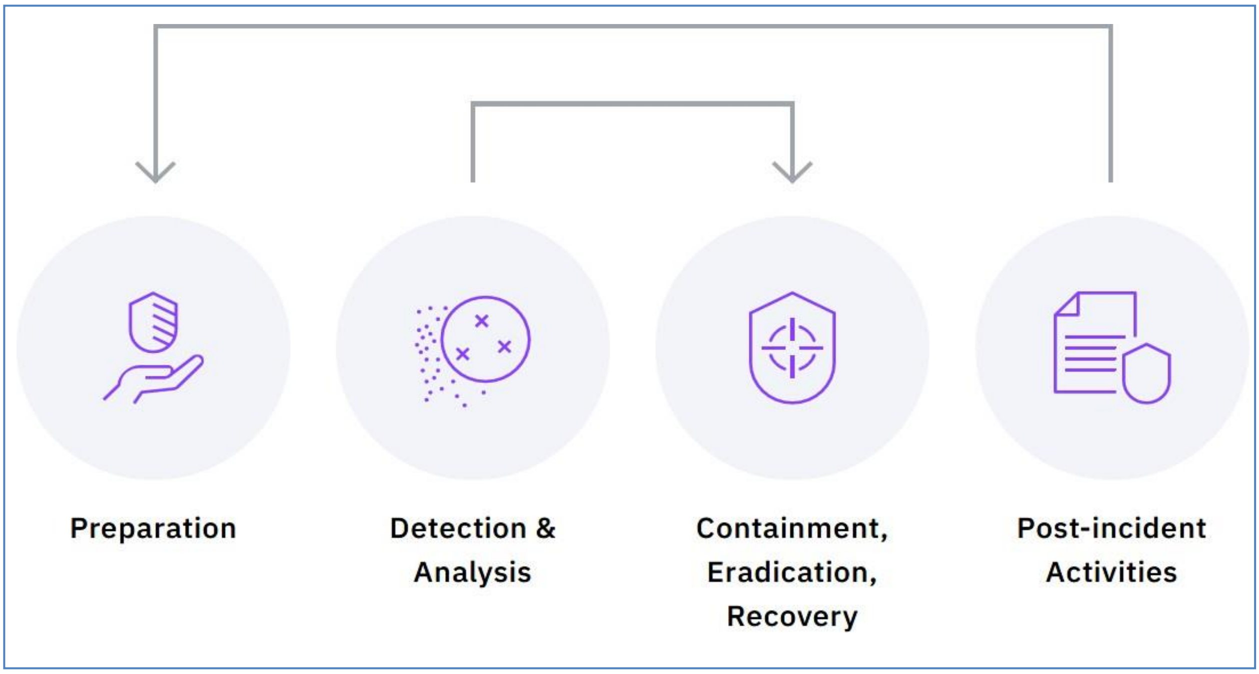
Data Breach is another ransomware attack model that has emerged in the past five years is the blended attack mode. It begins as a classic ransomware attack, demanding payment for encrypted files but behind the scenes, attackers have alreadyexfiltrated data from the Bank. If payment of the ransom is resisted, attackers threaten to expose or auction it online. These blended attacks can circumvent backupstrategies because they essentially extort the victim into payment even if backups are in place. Blended attacks can put immense pressure on organizations to pay extortion fees. Some damages caused by a ransomware attack is listed below [6]:

- Loss of Data and Information
- Employee Downtime and Loss of Production
- Ransom Costs
- IT Consultant Time and Labor
- Forensic Investigation Cost
- Data Leak and Compliance Issues
- Regulatory FINES (HIPPA, etc.)
- Impact on Reputation and Loss of Business Relationships
- IT Infrastructure Upgrades/Overhaul

How should banks prepare for ransomware attacks

When a ransomware attack is discovered, every second counts. Uninterrupted, timeis the ally of the attacker. As time passes, more data and files are encrypted, more devices are infected, ultimately driving up both cost and damage. Immediate—yet methodical and informed—action must be taken. Alerting IT security teams and allowing them to launch the incident response process that they have prepared to combat ransomware should be a first step.

If bank has an insurance contract with a 3rd party, it is advisable to engage them aswell. Other parties to consider contacting are federal law enforcement and regulators, depending on the local requirements for the geographies in which Bank operates. The following image1 illustrates the main phases of bank's ransomware preparation strategy [6]



Preparation

The preparation phase of the attack lifecycle involves preparing an organization forthe types of events and incidents they are most likely to encounter given the sector

[1] Image depicted from IBM white paper: The definitive guide to ransomware: Readiness, response, and remediation (Authors: Limor Kessem, Mitch Mayne)

In which they operate, the systems they use, and applicable key risk indicators (KRI)as they evolve over time.

End-user education: Proactive end-user education and training continue to be criticalin helping to prevent compromises of all types

Maintain a good antivirus and endpoint protection: Endpoint antivirus solutions arenot the sole protection mechanism for threat detection, but they are a common initialdetection method that can be deployed to users across the organization

Maintain an aggressive and current patch management policy: Attackers that aim toplant ransomware in IT networks often use system vulnerabilities to gain foothold within a network.

Enforce least privilege principles: With least privilege principles in place, admins can grant minimal permissions necessary for each user, based on requirements for their daily work.

Developing and rehearsing an incident response plan: An incident response plan is put into place to enable companies to act quickly and effectively during a stressful situation of threats, disruption, or disaster that can affect the organization’s operations on all levels, but specifically threatening to digital assets and the access to data.

Detection

The way by which an organization first detects ransomware infection can vary according to the situation, but in most cases, an employee will find it impossible to access files, receive a ransom note, or notice that a certain service is no longer accessible. The most time-sensitive issue at the onset of the attack is to identify anyand all infected systems and those in imminent danger of becoming infected. The first goal is to contain the spread of the infection as soon as possible and help minimize the risk to the organization by isolating the infected systems.

Analysis

The Analysis phase largely focuses on two areas and the first goal is to contain the spread of the infection as soon as possible and help minimize the risk to the organization by isolating the infected systems.

1. Identifying the specific variant of ransomware in action
2. Determining how the malware entered the organization (root cause analysis)

Containment

The Containment phase is a critical part of the response plan. Once a system has been identified as potentially having ransomware, the suspected infected computer should be immediately removed from your networks (including WiFi connections),and either shut down, or ideally hibernated to assist in forensic and sample analysiswhile minimizing the risk of the ransomware continuing the encryption process.

Failure to quickly isolate infected systems from the network may contribute to augmenting the incident by allowing the malware to continue to encrypt more files on the local system or network shares, thereby increasing recovery efforts.

Eradication

The Eradication phase involves removing the ransomware from infected systems across the organization. Depending on the scope of the attack, this operation can belengthy and may involve both user devices and more pivotal machines and services that have been impacted.

System that has been identified as infected with ransomware should be rebuilt from a trusted source, relying on trusted templates and safely-kept settings.

Recovery

Once a Bank has contained the ransomware and identified the root cause of the infection, there are several considerations an organization should examine when beginning the recovery phase.

- Patch vulnerabilities
- Restoring data from backups

Post incident activities

Post-incident activity is an important part of the response plan and should not be skipped. After any incident, large or small, it is recommended to meet with relevantstakeholders and discuss the elements that worked well and examine those that did not work. This kind of “lessons learned” analysis can help Banks improve processes Over time and ensure that future incidents are handled more efficiently and thereby minimize potential impact.

Notify Authorities: Most organizations understand compliance and regulatory requirements that pertain to their company. In general, those requirements apply to all cases of a data breach and the loss of private information belonging to customersand individuals. Banks may have more specialized obligations to report.

Conclusion and recommendations

Ransomware has attracted great attention from cyber security experts in recent yearsbecause of the fast growth of its attacks and the creation of new variants capable ofbypassing antiviruses and anti-malwares. It is a relatively new malware but has generated much interest from cybercriminals because of its successful attack and direct financial interest.

Ransomware objective is to block its victim from accessing their own resources by encrypting important files that seem valuable to the victim, such as images, spreadsheets and presentations.

Banks are one of the main targets of ransomware attacks

Most common attack vectors to deploy a ransomware include phishing emails, infected USB storage, use of bank employee's hacked accounts, visits to malicious websites, etc.

This paper's recommendation is that Banks should employ a good protectionframework (as explained in this paper) to be ready for ransomware attacks and to minimize ransomware damage

References:

1. J. P. Tailor and A. D. Patel, "A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control," Int. J. Res. Sci. Innov., vol. IV, no. November, pp. 2321–2705,2017.
2. B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," Comput. Secur., vol. 74, pp.144–166, 2018.
3. I. Yaqoob et al., "The rise of ransomware and emerging security challenges in the Internet ofThings," Comput. Networks, vol. 129, pp. 444–458, 2017.
4. S. B. Surati and G. I. Prajapati, "A Review on Ransomware Detection & Prevention," vol. IV, no. Ix, pp. 86–91, 2017.
5. H. Shakir and A. N. Jaber, "A Short Review for Ransomware: Pros and Cons A Short Reviewfor Ransomware: Pros and Cons," no. August 2018.
6. IBM white paper: The definitive guide to ransomware: Readiness, response, and remediation (Authors: Limor Kessem, Mitch Mayne)
7. What Are the Most Common Attack Vectors for Ransomware?, Anthony M. Freed, November 2021, https://www.c ybereason.com/ blog/ what-are -the-most-common-attack-vectors-for-ransomware