7/28/2021

CASE STUDY

RANSOMWARE

Alpa Meherkar
STUDENT

Executive Summary

Ransomware is a type of cyberattack or crime, which jeopardizes, and freezes the system of a user. The attacker demands a ransom in return to free that system from the attack. Users may pay the ransom and get back hold of their systems or may consider a legal procedure to get a hold of their attacker.

Introduction

Ransomware is a growing form of computer crime that is hitting all types of organizations, including law enforcement. Ransomware is malicious software that once loaded on a victim system encrypts the hard drive and issues a warning that unless a ransom is paid within 24–48 hours, all the data will become unrecoverable.[1] Ransomware is malware that locks your keyboard or computer to prevent you from accessing your data until you pay a ransom, usually demanded in Bitcoin.[2] Once installed, the malware may prevent you from using the keyboard, stop certain apps from running, and block the desktop so you can't access the taskbar or run additional programs. It may even hijack the camera to display a photo or video of you using the computer, making the presentation more intimidating. Worse yet, some forms may encrypt files on your hard disk, which may be difficult or impossible to decrypt without the encryption key.[3]

The digital extortion racket is not new—it's been around since about 2005, but attackers have greatly improved on the scheme with the development of ransom crypto ware, which encrypts your files using a private key that only the attacker possesses, instead of simply locking your keyboard or computer.[2] The software then tells the victim to typically send between $250 and $1,000 to the criminal within the allotted period. When the ransom is paid, the criminal will send the victim an alphanumeric sequence to unlock the malware.[1]

The victims typically infect themselves by clicking on a phishing message or downloading the ransomware from an infected or malicious website.[1] It is not the case that ransomware just affects desktop machines or laptops; it also targets mobile phones and if it became more lucrative, the IoT would be next (think: control of your Nest thermostat during very cold weather).[2]

The relatively short period allowed to pay the ransom is to discourage the victims from finding alternative methods of decrypting the system. Many victims find that they need more time to figure out how to use bitcoin. In some cases, victims have negotiated with the criminals for lower fees.[1]

Analysis

Ransomware attack isn't a single event. It is a series of events designed to disrupt and disable systems and to force organizations to pay large sums to recover data and get back online. We can better understand the scope of the ransomware threat and why having the right recovery plan in place is critical.

The seven stages of ransomware attack-

The beginning three stages of a ransomware attack are like calm before storm. They can happen without one ever seeing it coming. Prevention is important to intercede where possible, but these attacks are designed to target systems where they are most vulnerable, often starting with users.

Stage 1 – Initiation of the Attack

This first stage is where the attacker sets up the ransomware to infiltrate the system. This can be done in several ways such as sending out phishing email attacks, setting up malicious websites, exploiting weaknesses in RDP connections, or attacking software vulnerabilities directly. The more users one's organization has, the more vulnerable they are to a user targeted attack like phishing, malicious websites, or combinations of these. It only takes one user to make a mistake and execute the ransomware code, infiltrating the system.

Stage 2 – Instantiation

The second stage occurs once the ransomware has infiltrated your system. The malicious code will set up a communication line back to the attacker. The ransomware attacker may download additional malware using this communication line. At this point, the ransomware may lay hidden and dormant for days, weeks, or months before the attacker chooses to initiate the attack. The ransomware may try to move laterally across other systems in the organization to access as much data as possible. Many ransomware variants now also target backup systems to eliminate the chance for the victim to restore data. One could be completely unaware that their systems are compromised, and the attacker can wait for the optimal time to unleash the attack.

Stage 3 – Activation

The third stage is when the attacker activates, or executes, the ransomware attack remotely. This can happen at any time the attacker chooses and catch any organization completely off guard. Once the attack has begun, it can be a race against time for that organization to even identify that the attack is occurring so that mitigation and recovery efforts may go into action.

Once an attack has been activated, the system and data are in jeopardy. Without a plan in place to mitigate the attack and recover, downtime can stretch from hours to days or even weeks. The results are costly both to the financial bottom line and potentially to the brand reputation.

Stage 4 – Encryption

Ransomware holds data hostage through encryption (or in some cases a lock screen but encryption is most likely in a corporate attack.) Different ransomware variants use different encryption methods which range from encrypting the master boot record of a file system to encrypting individual files or entire virtual machines. Ransomware that also targets backup systems may delete or encrypt the backups to prevent recovery. Decrypting the data is highly unlikely, so the organization will have three choices: lose the data, recover from a replica or backup, or pay the ransom.

Stage 5 – Ransom Request

In this stage, the organization or a user whose system is compromised is officially the victim and the ransomware has encrypted data. They are presented with information on how to pay a ransom via a cryptocurrency transaction. Depending on what data the ransomware was able to encrypt, not only will data be inaccessible, but applications and entire systems can be disabled by the encryption. Operations can be severely impacted without access to data or services.

Stage 6 – Recovery or Ransom

This is the stage where many of the organizations we've seen in the news experienced impacts of significant downtime or disruption and many have chosen to pay a ransom as a result. Without an effective recovery method, even if the data can be recovered, at least partially, the cost of doing so may exceed the cost of paying the ransom. However, if one's organization has an effective recovery plan in place, they may be able to recover the data quickly with minimal disruption and no need to pay a ransom, eliminating the negative publicity of downtime and paying an exorbitant ransom.

Stage 7 – Clean Up

Paying a ransom or even recovering data from a backup or replica does not necessarily eliminate the ransomware on the system. The malicious files and code may still be present and need to be removed. The attack itself will likely reveal the type of ransomware and make it easier to locate and purge from the system. If necessary, systems can be recovered in an isolated network to clean up the malware without risking re-activation. Once the malware has been cleaned up, the system can be returned to normal operation.

Key Issues/Goals

A ransomware attack is perpetuated by threat actors who place malicious software (malware) on computer systems, networks and/or servers. The malware encrypts files and enables the threat actor to display a message demanding a fee to be paid in order for systems, networks and/or servers to return to normal operation. Ransomware attacks are targeting every industry globally, including highly regulated industries such as government and healthcare.

Once a company or person has been infected, the legal considerations and challenges are multipronged. In a scenario where all systems may potentially be encrypted and an organization is no longer operational, victims must take decisive and immediate action.

Response-

The victim of a security incident, ransomware or otherwise, and one may need individuals at their disposal who possess a unique background in cyber incident investigation and response. If you have a cyber insurance policy, it will set forth coverage requirements, and possibly a panel of response companies and/or attorneys you may be required to call in the event of a data breach.

If a user or organization wishes to engage an outside forensics investigation team or ransomware negotiation consultant. They should be engaged by outside counsel acting on behalf of the company to maintain legal privilege. Further, any reports or post-incident review should also be conducted under the advisement of the same counsel to maintain legal privilege. These issues should be discussed further with outside counsel.

Pay the Ransom or not-

OFAC issued an advisory to companies that pay or facilitate a ransom payment, warning them that ransomware attack victims, and third parties who assist these victims, could be in violation of federal law if they pay or facilitate the payment of a ransom to a sanctioned individual or entity, whether intentionally or otherwise. Penalties can be criminal or civil, and violations are strict liability offenses (ie, violations regardless of culpability). The fines for violations can be substantial (ranging up to $20 million and imprisonment).

The advisory notes that civil penalties may be imposed for sanction violations even if the parties who initiate or facilitate the transaction did not know or have reason to know that they were engaging in a prohibited transaction.

The advisory encourages victims to self-report attacks and ransom payments to law enforcement, and states that in determining the “appropriate enforcement outcome” for a ransomware payment made to a sanctioned individual or entity, OFAC will consider the victim’s “self-initiated, timely, and complete report of a ransomware attack to law enforcement” and “full and timely cooperation with law enforcement” as significant mitigating factors.

Payment of Ransom-

Aside from determining whether paying a ransom is permitted in the applicable jurisdiction, the company should also look to whether its insurer will cover the ransomware payment. A company must assess the severity of the threat, whether a restoration from backup is possible, and the overall financial impact of the loss of business per day. The different severity levels that the company uses to measure the impact, and the industry that the company is part of, also influence the legal risks.

Other risk factors include possible ineffectiveness of the ransom payment, as the payment of a ransom does not guarantee the systems can be unlocked; previous incidents show that

some threat actors have a history of not providing the decryption keys following payment. If the threat actor is known for not providing the means to unlock the affected systems, it may not be recommended to pay the ransom even if all other factors would weigh in favor of payment.

Other prosecution risks should be taken into consideration, specifically in a loss-of-life situation, and where the company needs to evaluate potential sanctions in applicable jurisdictions if there is an indication that the company or its employees might be liable for the seriousness of the situation (eg, in relation to inside threat actors or insufficient system design or backup plans).

Additionally, careful consideration is required in relation to the company's security offerings as potentially both a ransom payment being made public and an unmitigated ransom attack can impair a company's sales strategy in the area of security offerings. Finally, the payment of ransom increases the likelihood of further ransomware attacks, as perpetrators have been known to direct targeted attacks against companies who have been prepared to make ransom payments previously.

Breached-

The fact that ransomware malware has infiltrated the network could be considered a breach and further legal analysis should be conducted. Ransomware threat actor groups have developed a new tactic of egressing your data to use the data as leverage and force one into providing payment.

The threat actor validates that they have some of your data, they have most likely implemented their own operational security measures.

In situations like this, it is important to implement out-of-band communications using easily disposable phones, computers procured directly from a supplier and secure email systems.

Notifying Law Enforcement-

The decision of whether to involve law enforcement includes many factors, such as the applicable legal requirements regarding regulatory notice, contractual requirements and the benefits in contacting law enforcement. Similarly, potential drawbacks should also be considered.

Law enforcement may want to act quickly to publicly share decryption keys at their disposal, or they may simply note your victimization and ask that you share information regarding the breach such as indicators of compromise. These factors should be analyzed closely.

Conclusion

Preventing ransomware attacks before they happen should be part of every cyber security plan. Having said that, cyber-attacks and cyber-crimes by their nature are designed to bypass preventative measures and continue to evolve rapidly in order to do so.[5]

Modern ransomware attacks require modern data management and recovery solutions that protect data across multiple platforms including on-premises, cloud, tiered storage, and SaaS applications.

Ransomware attacks infiltrate systems despite the best efforts of prevention and preparation. Understanding how ransomware attacks impact systems is the first step in planning for both prevention and recovery.

References

[1] Advanced Persistent Security, Ira Winkler, Araceli Treu Gomes, 2017.

[2] Rugged Embedded Systems, J. Rosenberg, 2017.

[3] The Basics of Cyber Safety, John Sammons, Michael Cross, 2017.

[4] https://www.sciencedirect.com/topics/computer-science/ransomware

[5] https://www.zerto.com/blog/ransomware/the-7-stages-of-a-ransomware-attack/

[6] https://www.dlapiper.com/en/us/insights/publications/2020/12/understanding-ransomware-stratagems/