Emerging Ransomware Threats

CYSE 280 – Professor Gladden

Brandon Creech

Old Dominion University

Abstract

Technology continues to develop with the human generation to meet their daily needs. However, with new technology comes more opportunities for online hackers to extort personal information and money from innocent companies and citizens. Ransomware, a malicious method of attack used by hackers, has seen a significant rise in the past decade with a notoriety for imploring major losses to victims. This paper will cover the statistical effects of ransomware and why hackers target specific people. It will also detail the types of ransomwares that circulate on the internet, the ways companies and citizens can protect themselves against it, and how they are favoring in this battle for now and the future.

Emerging Ransomware Threats

Hackers use methods to exploit their victims for their own personal gain. Whether this is through infiltrating or impersonating, they often times do it with malicious intent. Often times the news we see on televisions regarding hackers and cybersecurity are about data breaches and bank account details being stolen, but not often enough do we hear about ransom becoming a hacker's weapon. Victims, especially civilians who have no governmental authority, are thrown into an unexpected, twisted game where they are the puppet in the hacker's master scheme. The civilian has no matter of choice as their assets and in extreme cases, theirs, or someone else's life, are in danger of being confiscated. In this paper, the dangers of ransomware will be highlighted and how numerous cybersecurity companies have taken steps to fight and prevent these threats through frameworks and tools at their disposal.

Ransomware Statistics

Ransomware has continued to become an upwards crisis in the world. Behind anything you browse online can be something malicious that is hidden. Based on 2021 alone, the rate of ransomware attacks has skyrocketed to 148% (SearchLogistics). The activity is becoming less of a phenomenon, but rather more of a reality we must all take fear of. People who are less tech-savvy or have little IT experience are more vulnerable as they can be more carefree about what

they are navigating. They must be wary as hackers can manipulate ransomware into several different forms: email phishing, RDP vulnerabilities, and software vulnerabilities.

Email phishing	RDP vulnerabilities	Software vulnerabilities
Definition: Malicious emails that lure victims into clicking onto them, which then can steal their information. One of the most common forms of ransomware.	RDP (also known as Remote Desktop Protocols) are tools that hackers use to gain access to a victim's computer remotely either through a video or snapshots.	Bugs within a software that a hacker targets.
Examples: Emails that promise free money/gift cards, fake news headlines with links, "You've been selected!" emails. Emails with bad grammar/spelling are obvious ones.	Bait links similar to email phishing, but also can require the victim to input their credentials to initiate the remote access to the desktop.	Inadequate coding, unfinished software.

Vulnerable Targets: Less IT experienced/tech-savvy people. Teenagers and senior citizens.	Less IT experienced/tech-savvy people. Teenagers and senior citizens. High-valued companies like bank institutions, tech conglomerates, or the government.	High-valued companies like bank institutions or conglomerates. Cybersecurity companies.

Although these forms of ransomware can be daunting, there are ways people can identify whether what they are accessing online is suspicious. For example, email phishing can be suspected when the promises made by it seem too good to be true or that it has bad grammar/spelling. Software vulnerabilities can consistently make operations ineffective, especially if the software is essential.

Company Frameworks

Over the years, companies have developed frameworks that are specifically designed to combat ransomware from happening to their cybersecurity infrastructure. These were constructed based on team discussions, identifying weak points in their infrastructure, and educating employees on ransomware. Several frameworks are considered effective when ransomware is detected including:

1. Prioritizing critical systems that are vulnerable and isolating them when exposed to ransomware (CISA.gov).

2. Periodically examine organizational logs within the detection/prevention systems. (This can help show early signs of ransomware and other forms of malware that are just starting their attack.)
3. Use this information from the logs to determine what parts of the operations have become susceptible and to eliminate the threat before it causes further damage.

Because ransomware continues to evolve, these frameworks may not always be able manage the risk. As hackers develop new tactics, companies have to be able to develop new tactics as well that counter them.

Tools/Resources for Citizens Against Ransomware

1. Maintain a trusted anti-virus that can quickly detect hidden malware in files and alert the user before downloading them. A trusted anti-virus should also be able to run consistently effective maintenance scans throughout the whole computer system.

2. Have the computer run continuous backups of all personal files. Backups can help the user recover files that may have become corrupted or deleted from any form of malware/ransomware and mitigate losses (Jnguyen).

3. Enforcing user authentication, such as a 2-step, can be effective in preventing hackers from gaining access to user personal information. Having a 2-step authentication on all sensitive logins makes it 10x more difficult for the hacker to even conduct their activity.

4. Your own instincts are the frontline defenses and perhaps the most important tools in preventing ransomware from happening in the first place. Knowing if a file is safe to download and whether you trust it or not is the single most important tool everyone should be able to utilize. Everyone should be able to sense what they are navigating could be malicious or not.

Conclusions – 1. State of the ransomware fight in the cybersecurity infrastructure and 2. In the citizen society

In the current fight against ransomware, elements of the battle are constantly evolving. Ransomware is taking on different forms as if they are offsprings of each other, such as how Petya was a resurrection of GoldenEye in 2017 and that GoldenEye became known as WannaCry's "deadly sibling" (Kaspersky). Although we cannot eliminate ransomware completely, we can find tactics that help minimize the losses dealt by these malicious attackers. Companies, more specifically in the cybersecurity field, continue to discuss and develop from these losses to better their defenses. Not only is minimizing losses against ransomware beneficial for companies, but it also helps the consumers of these companies because they can trust them to be able to deal with these threats swiftly.

Consumers of companies and citizens overall are also learning how to defend themselves in this developmental era of technology. They are presented as prime targets of ransomware which is why they must always better their instincts and protection of their own devices. Through various tools that can be utilized built into a standard computer system and

valuing a trusted antivirus to eliminate threats from within, these people can create a barrier between themselves and hackers that will make their computer and data impenetrable.

References

Ransomware Statistics: How Bad Are Ransomware Attacks in 2023?. SearchLogistics. (2023, May 25). https://www.searchlogistics.com/learn/statistics/ransomware-statistics/

I've Been Hit by Ransomware!: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

Jnguyen. (2023, May 24). *Ransomware Attack - What Is It and How Does It Work?*. Check Point Software. https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/

Kaspersky. (2023, May 18). *Ransomware Attacks and Types – How Encryption Trojans Differ*. www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types