ZCorum™

Cyber Siege: A Look into Targeted Ransomware Campaigns

Contents

Introduction

Ransomware is a cyberattack that hijacks sensitive information, followed by a ransom demand in exchange for either restoring the data, or not publishing the data where everyone can have access to it. Ransomware has been a particular thorn in the side of internet security efforts for over three decades. They can affect anyone, from a single individual at home, to an entire corporation or even a government entity.

The vector of the attack can vary by method, such as through a phishing email or through brute force hacking, but the result is usually the same—a threat that the damage done will remain until a demand is met. The term ransomware covers a litany of sins and methods in hacking, and thus its history is long, going as far back as the end of the 1980's.

The concept of ransomware emerged in 1989 when a Harvard educated biologist named Joseph L. Popp created the first known ransomware program called the "AIDS Trojan" or "PC Cyborg." The virus was spread via physical floppy disks, which were mailed out to twenty thousand subscribers on a mailing list for attendees of a World Health Organization (WHO) conference in Stockholm, Sweden. When victims ran the disk's program, it encrypted files on their system and demanded a ransom of $189 to be sent to a post office box in Panama. While the ransomware didn't spread widely, it laid the foundation for future attacks.

Evolution of Encryption: During the 1990s, ransomware started utilizing more robust encryption methods, making it harder for victims to recover their files without the decryption key.

Police Themed Ransomware: In the mid-2000s, a new type of ransomware emerged, known as police-themed ransomware. This malware displayed a fake message claiming to be from law enforcement, accusing victims of illegal activities and demanding a fine to unlock their computers. The malware often used scare tactics to intimidate victims.

Ransomware-as-a-Service (RaaS): Around 2012, ransomware attacks became more widespread due to the development of Ransomware-as-a-Service platforms. These allowed less technically skilled criminals to participate in ransomware attacks by purchasing or renting ready-made ransomware kits from more skilled developers. This development led to an explosion of ransomware variants and campaigns.

Proliferation and Sophistication: From 2013 to 2017, ransomware attacks saw exponential growth in both frequency and sophistication. High-profile attacks like CryptoLocker, WannaCry, and NotPetya, garnered widespread attention and caused significant damage to individuals, organizations, and even governments.

Targeted Attacks: As ransomware continued to evolve, cyber criminals began using more targeted approaches. They identified and attacked high-value targets, such as large corporations, healthcare organizations, and critical infrastructure. The Locky and SamSam ransomware families were among those involved in such targeted campaigns.

Expansion of Ransomware Tactics: Beyond encrypting files, ransomware tactics expanded to include data theft and double extortion. Some ransomware groups started stealing sensitive data before encrypting files and threatening to release the data if the ransom was not paid, increasing the pressure on victims to comply.

Ransomware remains a significant threat in the cybersecurity landscape, and attackers continue to adapt their tactics to maximize profit and inflict damage. As security measures improve, ransomware attacks may evolve further, making it essential for individuals and organizations to remain vigilant and implement robust cybersecurity practices. In the remainder of this ebook you can read about some of the more notable ransomware attacks and how they have evolved over time.

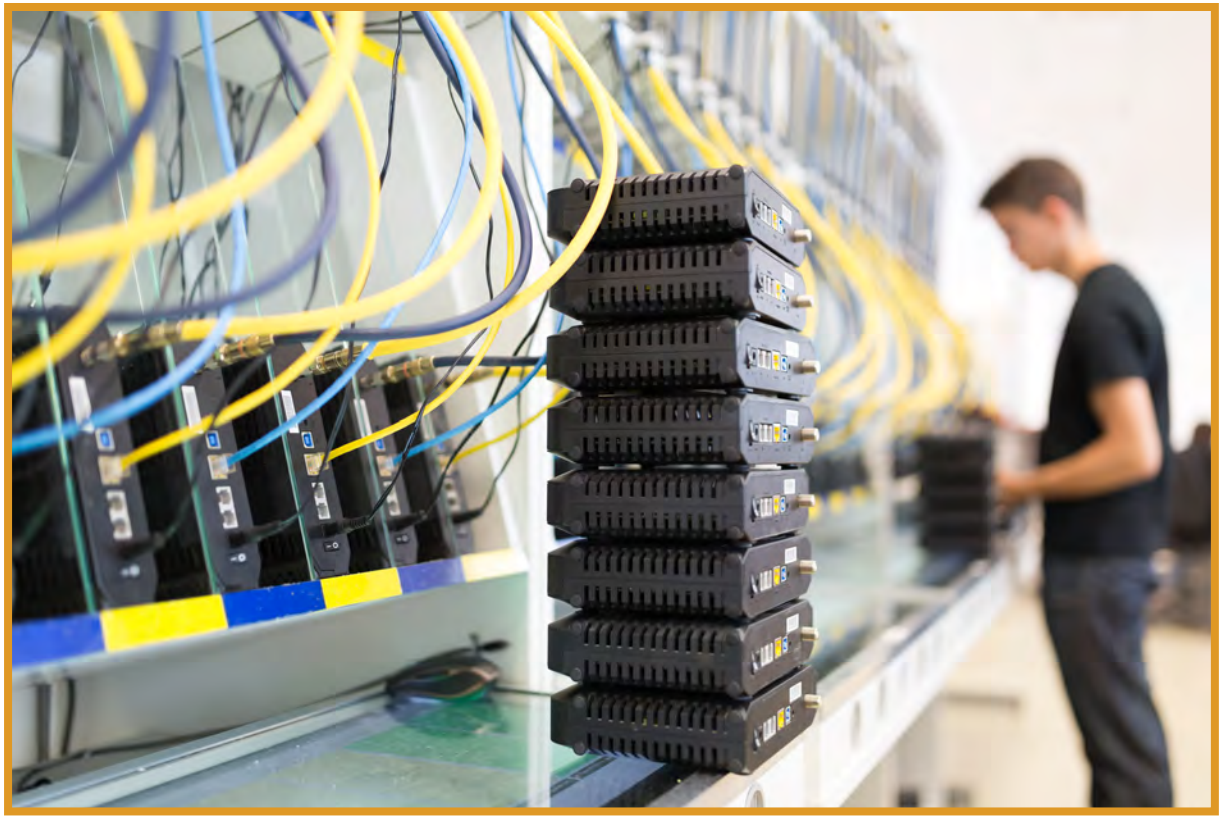
Aids Info Disk Attack

The first recorded instance of a ransomware attack occurred in 1989. This attack is known by several names, most notably the AIDS Trojan (Aids Info Disk) and PC Cyborg. The attack was unique in a historical sense with how it was spread. The virus was spread via physical floppy disks, which were mailed out to twenty thousand subscribers on a mailing list for attendees of a World Health Organization (WHO) AIDS conference in Stockholm, Sweden.

The floppy would be inserted into the victim's computer and proceed to install a trojan horse virus onto the computer. It would then silently wait, counting each instance of the computer booting up. Once ninety boot ups were reached, all directories and files would vanish. The user would be directed to a "message" from the "PC Cyborg Corporation", instructing the unfortunate victim to mail $189 to a PO box in Panama. The perpetrator of this now infamous attack was found to be a biologist, and while his motive is still considered a mystery, the damage done turned out to be relatively easy to undo. This would be the first in a long history of ransomware attacks.

Reveton

Jumping forward to 2012, a ransomware program known as Reveton appeared. Also working as a “Trojan”, Reveton hid inside of another program downloaded by the user, then released its attack on the victim. Reveton’s attack worked by pushing warnings onto the user’s computer screen and locking the system while claiming to be a law enforcement agency. It then extorted money by offering to unlock the victim’s computer once they paid a “fine”. The Reveton ransomware propagated for years and has had long-lasting effects.



EternalBlue

In 2017 one of the largest ransomware attacks in the world occurred, targeting computers running the Microsoft Windows operating system and spreading by means of using an NSA hacking exploit called “EternalBlue”. This attack, known as WannaCry, is estimated to have hit over three hundred thousand computers across one hundred and fifty countries, causing billions of dollars in damages. Investigations led to the belief that the country of North Korea was behind the attack, but they denied the allegation.

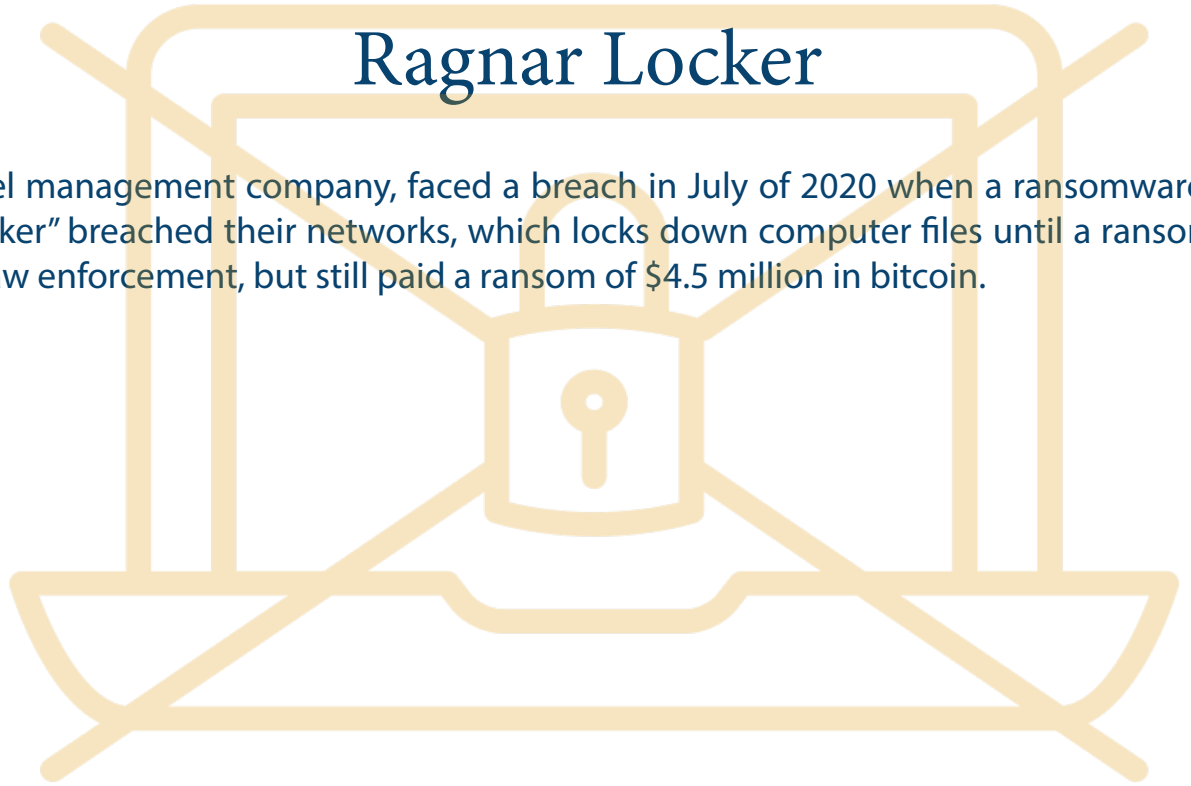
SamSam

In March of 2018, the city of Atlanta, Georgia suffered a devastating ransomware attack it wasn't prepared for. After facing criticism for not properly upgrading the city's IT infrastructure, Atlanta became the victim of what's known as a SamSam Ransomware attack. While typical ransomware attacks rely on the victim to open a malicious link or file through phishing, SamSam employed a brute force password cracking. Once it was inside the IT infrastructure, city digital services such as bill payments for utilities and payments for outstanding tickets were taken down. Forms had to be filled out on paper until the services were recovered, which ended up costing the city $2.7 million.

UCSF

In June 2020, at the University of California at San Francisco's School of Medicine, the IT system was compromised by hackers. University IT staff worked to minimize the damage once the malware was discovered, and while sensitive information at the time was not affected, including their work on the COVID 19 virus, servers were encrypted and held for ransom for $3 million dollars. After days of negotiations between the hacker group and a representative for UCSF, a payment of just over $1.1 million was accepted by the hackers.

Ragnar Locker



CWT, a travel management company, faced a breach in July of 2020 when a ransomware attack named "Ragnar Locker" breached their networks, which locks down computer files until a ransom is paid. CWT contacted law enforcement, but still paid a ransom of $4.5 million in bitcoin.

CNA

CNA Financial, a prominent US commercial insurance company, fell victim to a ransomware attack in March of 2021 when their network was breached and disrupted. The ransomware in this case was able to trick a CNA employee into downloading it by disguising itself as a browser update. Once it was downloaded, company and customer information was stolen, and employees were blocked from logging in. 75,000 members were affected, and CNA reportedly paid $40 million to the hackers.

Colonial Pipeline

Colonial Pipeline, a critical oil pipeline system that runs from Texas and up the East United States, became the victim of a ransomware attack in May of 2021. Like the Atlanta SamSam attack, the attack on Colonial Pipeline involved only their billing services, but the pipeline was shut down as a precautionary measure. The halt in the movement of oil caused a fuel shortage, particularly in the Southeastern United States, which resulted in rising fuel prices. It was also discovered that the perpetrators had stolen a hundred gigabytes worth of data before the attack occurred, and they demanded a ransom in return for the data. The ransom was paid in bitcoin, but most of the payment was recovered in the aftermath.

Kaseya

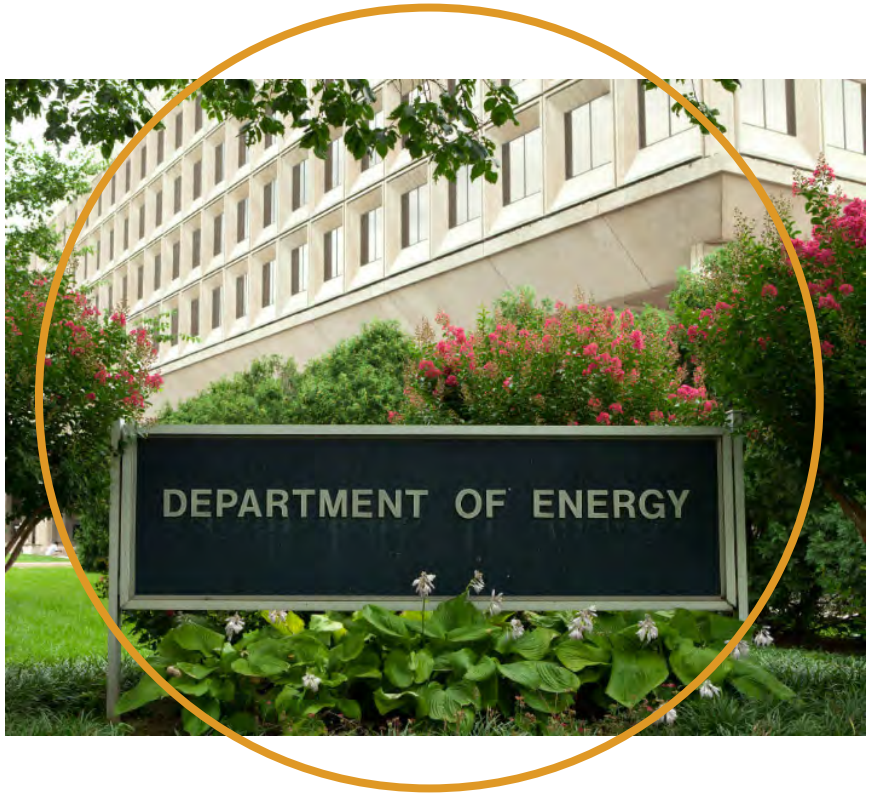
Kaseya, a provider of remote IT management software, suffered a ransomware attack in July of 2021 when hackers hijacked one of their popular management software tools by exploiting a zero-day vulnerability that had yet to be patched. This allowed the hackers to release the ransomware through Kaseya's application to the company's clients, numbering around 1,500 businesses. The hackers demanded seventy million dollars in bitcoin. The ransom was not paid, and law enforcement was brought in to assist with recovery efforts. This attack highlights how important it is for a business to vet the cybersecurity efforts of companies in their supply chain, especially those that provide network and computing services that can be compromised and used as a vector for distributing malware.

St. Margaret's Health

Also in 2021, St. Margaret's Health in Illinois experienced a cyberattack that caused a major disruption to their systems, impacting their ability to submit claims to insurers, Medicare, and Medicaid for 14 weeks. Although the hospital was eventually able to continue providing services, the effects were long-reaching, and the ransomware was cited as one of the reasons the hospital closed in June of 2023.

PharMerica

One of the most recent high profile Ransomware attacks was reported in May of 2023, when PharMerica, a pharmacy services provider, was reported to be the victim of a massive data breach. Sensitive customer data such as names, addresses, social security numbers, birth dates, and more were all stolen from nearly six million people. The attack itself happened in March, but affected customers were not made aware until two months later. The hacking group that took responsibility for the attack claimed to have taken nearly five terabytes of information, and threatened to release it if a ransom was not paid. When the deadline passed and PharMerica hadn't paid it, the group began to leak the stolen data.



MOVEit

Most recently, in June of 2023 a breach in US government services has potentially put the data of millions at risk. US federal agencies across the country along with hundreds of other companies, experienced breaches through their MOVEit applications. The MOVEit application is a software application used by businesses and agencies to transfer files, and hackers reportedly exposed a flaw in it that had yet to be patched. The effects of the hack are still being determined at this time, but it is known to have compromised major entities like the Department of Energy, the US Office of Personnel Management and the DMVs for the states of Oregon and Louisiana. Colleges in New York and Georgia have also revealed their networks were compromised, as were corporate entities like First National Bankers Bank and Shell.

Conclusion

Ransomware has evolved over the years, from being delivered via compromised floppy disks, to fake browser updates and phishing emails. Hackers are becoming more and more sophisticated in their methods and how they breach systems. While no company wants to pay a ransom, the threat of losing access to mission critical data, or sensitive information being leaked to the public, may make paying the ransom more palatable in the long run compared to the potential loss of business and the possible lawsuits that can result.

Mitigation and prevention of ransomware is challenging due to the constantly evolving nature of these attacks. In the case of an encryption attack, where the information is locked down, maintaining regular backups of the data will minimize the damage done. However, hackers now know that many companies are taking this minimal step, so the threat of releasing sensitive data to the public is becoming more prevalent. A robust cybersecurity plan is critical to protecting your business. This should include ongoing employee training, keeping systems and software up to date with the latest security patches, deploying intrusion detection software on servers and endpoints, and actively monitoring those systems 24 x 7 to address any incidents as they happen so you can prevent the spread of any malware that is discovered.

Resources

ZCorum's managed cybersecurity service, CyberZCurity, offers comprehensive and proactive protection against the growing landscape of cyber threats. Our skilled and experienced cybersecurity staff provide real-time 24/7/365 proactive monitoring, analysis, and response to potential security incidents. We quickly identify and immediately neutralize threats, minimizing the risk of data breaches and unauthorized access.

Every broadband provider has unique security needs, and our services will be tailored to suit your specific operation. Entrusting your cybersecurity to our proactive and always-on approach lets you focus on your core operations knowing that your network is safeguarded around the clock. Give yourself and your company peace of mind by contacting us or visiting our website zcorum.com.

ZCorum™

4501 North Point Parkway,
Suite 125
Alpharetta, GA 30022
Toll Free: 1-800-909-9441
info@ZCorum.com

ZCorum is a partner that has managed networks for nearly three decades. We provide a suite of managed services that will reduce the operational costs, increase the subscribers' satisfaction, and provide additional revenue opportunities for your clients. Let us work with you to enhance your service to your clients. Let us know how we can help.