Ransomware in the Wild

atlantic.net

Secure Cloud Services
Managed & Compliant Infrastructure

888-618-DATA (3282)
sales@atlantic.net
www.atlantic.net

Table of Contents

Ransomware in the Wild	3
Ransomware Lifecycle	5
Industries Under Attack	6
State and Local Government Targets	6
No Ransomware Authority	8
To Pay or Not to Pay; That Is the Question.	8
Why Is Ransomware Proliferating Across the United States?	9
Should You Be Worried About Ransomware?	10
Ransomware Prevention	11
Conclusion	12
Need Help with Securing Your Business Against Ransomware Threats?	12

Ransomware is an increasingly common type of malware that infects vulnerable computers, potentially infiltrating any computer operating systems and encrypting the user's files. A financial demand is declared to regain access to data. Some of iterations of malware are incredibly malicious, bypassing antivirus and potentially locking users out of the computer system.

The impact of ransomware varies depending on the victim; it appears that bad actors and hackers are increasingly using malware to target businesses, organizations and local authorities. However, despite the increase in higher-profile targets, it is important to remember that individual users can still be victims of ransomware. Because of this, it is very difficult to accurately report on how many individuals are affected and how many victims pay the ransom.

Undoubtedly, ransomware has entered the common vernacular as awareness of ransomware has dramatically increased over the past 5 years. Rarely a month passes without a security incident triggered by a ransomware attack being reported in a newspaper or on TV. Ransomware has been honed to serve in targeted, often coordinated attacks on established organizations, governments and institutions located around the globe.

The motivation behind the attacks is nearly always financial; the antagonists aim to extort cryptocurrency from the target after encrypting critical or sensitive files on the compromised computing infrastructure. Hacking groups prefer Bitcoin as it is relatively easy to clean this cryptocurrency and move it around the blockchain network.

While it is not impossible to trace Bitcoin transactions, there is still relative anonymity in transferring Bitcoin into cash. There have been some successful occurrences of tracing paid ransoms; recently, a ransomware named "SamSam" was successfully traced to two men operating inside Iran. The FBI traced and located the addresses associated with the Bitcoin wallets used in the extortion by tracking the movement of the Bitcoins over blockchain.

Hackers have counteracted this by adapting their collection methods, using clustered Bitcoin wallet addresses to mask currency. Although Bitcoin is the preferred payment method, there has been research conducted into the types of payments made for ransomware. Cash, revenue generating premium telephone numbers and prepaid payment cards such as Paysafecard, Ukash and MoneyPak are among the popular alternatives.

A Brief History of Ransomware

Ransomware is not a new phenomenon; in fact, it only earned the name "ransomware" in recent years. Previously, the attacks were simply known as viruses or Trojan horses. The first documented evidence of a ransomware attack, one that encrypted files with the intention of blackmailing the victim for financial gains, was reported as early as 1989.

This ransomware, called "the AIDS Trojan," pre-dates email and the internet as we know it today. It was distributed on floppy disk by a hacking group posing as a fake company called "PC Cyborg Corporation." Once the user loaded the fake application onto their computer, the user files were encrypted at a specific trigger point written into the malware.

After the user had rebooted their computer a set number of times, victims were prompted with a demand for a licence fee payment in return for their locked out files. The user was ordered to send money offshore to a Panama PO box in return for the unlock key.

"The AIDS Trojan" was a very crude malware which was easily fixed as it used symmetric encryption (both public and private key were stored on the infected computer), and fix-it tools were quickly released to fix the problem.

Fast-forward to 2013, when a huge spike in ransomware attacks fuelled by the release of the notorious CryptoLocker malware. CryptoLocke was a highly sophisticated new malware using asymmetric encryption (only the attacker has the private unlock key). The success of CryptoLocker spawned a vast number of cloned ransomware programs, all using asymmetric encryption to deny a user access to their files.

Figure 1- An example of the Aids Trojan demand

The use of asymmetric encryption in ransomware has continued from 2013 to the present day and includes some of the most widely known ransomware attacks, such as WannaCry, Emotet, Zeus, Petya and Kovter. Many of the early malware releases targeted any individual's computer with operating system vulnerabilities, but today, much of the evidence suggests that the aggressors are increasingly targeting US state and local government institutions as the rewards are potentially more lucrative.

Top 10 Malware - Breakdown

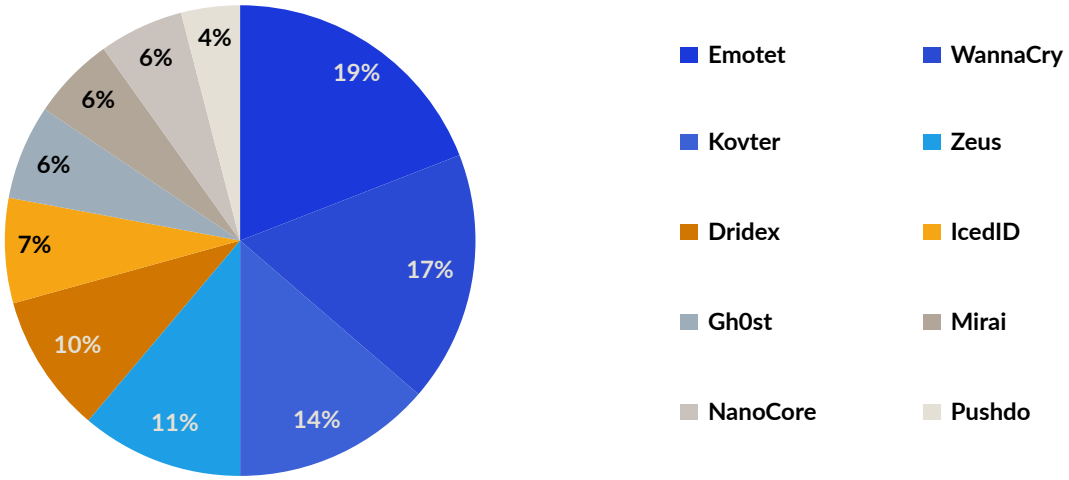

Figure 2 - Break down of the Top 10 Malware Attacks

Source: https://www.cisecurity.org/resources/?type=post

Ransomware Lifecycle

In an in-depth study completed by the International Journal of Computer Science and Network Security, researchers found that the ransomware lifecycle is composed of seven unique stages. When ransomware is created and distributed, there is close collaboration between the creator(s) and the antagonist(s). The creator is the writer of the malware, and a campaigner's job is to distribute the ransomware.

The study discovered the following seven stages of the ransomware lifecycle:

1. Creation – the creation team will write the malware and embed as much sophistication into the program as possible to ensure the victims pay for the release of their files

2. Campaign – the creators and/or campaigners decide whom to target with the ransomware. If individuals are targeted, the hacking group (campaigner) will target as many victims as possible, and if an institution is targeted, research may be conducted about the type of institution to hit and the likelihood of receiving the ransom

3. Infection – the ransomware malware payload has infected the target, and its victims are commonly using computer infrastructure that is not patched or updated with the latest security updates

4. Command and Control – at this stage, the ransomware is activated over the internet. Some ransomware will catalog the contents of the computer such as IP address, domain name, operating system, installed browsers, and anti-malware products

5. Search – the malware will scan the host computer looking for valuable files such as documents, spreadsheets, presentations, images, network drives and databases

6. Encryption – the search results will generate a list of files to encrypt; then, the encryption software will start

7. Extortion – at this stage the files are encrypted, and a ransom is displayed on the victim's computer. It will contain a message stating that the user's files have been encrypted and instructions of how to pay the ransom

Source: https://expert.taylors.edu.my/-file/rems/publication/105055_5256_1.pdf

Industries Under Attack

The healthcare industry is a globally attractive target for ransomware creators, despite healthcare data's protection under HIPAA legislation; the rewards a successful malware breach of healthcare infrastructure could be lucrative for the hackers. Compromising medical records, hospital computer systems, or healthcare databases could cause chaos at a healthcare institution.

PheonixNAP have suggested "almost half of the ransomware incidents reported in 2018 involved healthcare companies" and ransomware infection rates at healthcare institutions increased 90% between 2017 and 2018. Cybercriminals will always target lucrative victims and they have learned that healthcare providers are more likely to pay the ransom if healthcare professionals are locked out of critical IT systems.

Financial institutions are another prime target for ransomware; these businesses store highly valuable data ranging from bank account information to Social Security numbers. If this data were to become compromised, it is unlikely a financial services company will be able to function, which may naturally increase the likelihood of ransom payments being made by these companies.

State and Local Government Targets

Researchers have put significant work into determining who exactly is targeted for ransomware extortion. Recorded Future investigated the recent trend of ransomware attacks that specifically targeted state and local government institutions in the United States. The researchers' aim was to study

how ransomware attacks have changed since 2013 and whether the number of incidents has increased in recent years.

Unsurprisingly, they found that "ransomware attacks on state and local governments are on the rise" with a steady increase between 2016 and 2019. Interestingly, the research suggests that state and local government institutions may not have necessarily been intentionally targeted, but instead that "these attacks tend to be more targets of opportunity."

The study found several important trends regarding the rise of ransomware:

- In 2017, 38 state and local government attacks were reported
- In 2018, 53 state and local government attacks were reported, a 39.47% increase on the previous year
- So far in 2019, 21 state and local government attacks were reported up to April, with more than 63 projected for the entire year.

Another very important finding from the research was that state and local governments were "less likely than other sectors to pay the ransom." although we suspect this trend will change throughout the rest of 2019. This theory is supported by reports that suggest 45% of ransoms have been paid for attacks so far in 2019.

It is estimated that over 170 county, city, or state government systems have been attacked since 2013, and we believe that this figure will continue to increase over the coming years. The attacks so far in 2019 illustrate the shift of ransomware attack targeting to public facilities.

In May and June of 2019, the City of Baltimore was targeted by a sophisticated ransomware attack that affected the majority of the city's services. The ransom was set at 13 Bitcoins (approx. $76,000 at the time). Multiple departments lost their email, phone systems and payment systems used for generating bills and processing property sales.

The attack had a major impact on the city's day-to-day functions; manual processes were reintroduced and thousands of local residents were impacted. The incident made global news especially when the city announced "they would never pay the ransom." It is estimated that the seizure of city IT systems cost up to $18 million to repair, not to mention the significant trauma placed upon the employees and the residents of Baltimore at the time.

One of the very latest ransomware incidents started as recently as August 20th 2019, which affected 22 municipalities in Texas and resulted in swaths of local government organizations being unable to process everyday transactions. The assailants set the

bounty at $2.5 million; the demand was immediately rejected by the state of Texas.

Systems that controlled birth and death certificates and some utility payments were taken offline by the breach. These systems were outsourced to a software provider that managed the IT systems. The attack happened at the IT provider's data centers and affected multiple regional institutions, all of whom outsourced to the same provider. This highlights the criticality of choosing an outsourcing partner which has significant experience in cyber security and systems management.

No Ransomware Authority

One of the biggest challenges of understanding the scale of ransomware attacks is that we can never truly ascertain how accurately the number of incidents is reported. We can question the preciseness of the statistics because there is no centralized reporting authority that enforces notification of a ransomware outbreak.

Businesses, governments and local municipalities currently have no legal obligation to report that ransomware has affected them. Unlike HIPAA legislation, which has clear guidelines and rules about reporting data breaches, this kind of compliance is not enforced for ransomware, and we rely on victims coming clean and accurately reporting the incident.

This likely means that the number of incidents reported is lower than the actual number of occurrences. Failure to report by affected institutions might be to protect reputations, maintain trust, or retain customer loyalty.

Whatever the reason, we should ask why there is less transparency in reporting ransomware incidents. We often have to rely on local news investigations or whistle-blowers to uncover ransomware victims. Accurate ransomware reporting is even more difficult when you consider individual users: John or Jane Doe who was scammed by an overseas fake software reseller.

Despite the harm that ransomware can inflict, relatively little is known about the prevalence and characteristics of such attacks in the general population. What proportion of users pay up? How do users perceive the risks? How do individual users respond to ransomware attacks? These are all questions that would require detailed research and investigation, but our current lack of insight is worth considering as it affects our understanding of the global scale of ransomware.

To Pay or Not to Pay; That Is the Question

The decision to pay a ransom depends on many circumstances, including the type of data that has been encrypted and who has

been affected by the ransomware. There is evidence to suggest that state and local governments choose not to pay ransoms as frequently as other victims, a fact that is often reported in the media during the news reporting on ransomware incidents.

When considering the attacks like those in Texas and Baltimore, choosing not to pay could leave local residents very angry, as they are unable to use the services they pay for and they would be directly affected by the enormous bill to clean up the mess through service cuts and cost savings in the future.

However, it is estimated that one in five ransomware attacks on government institutions are paid and about 4% of domestic cases are settled. In many of the ransomware incidents discussed here, it turned out to be significantly more expensive to NOT pay the ransom, with many organizations having to pay for expensive third party security consultants, IT server hardening, and additional insurance premiums.

For the institutions who chose to pay the ransom, the cost is also very high; Lake City in Florida recently paid $500K in ransom and Riviera City, also in Florida, paid $600K. However, it can be argued that paying the hackers prevented days, weeks, and months of critical system outages. Those figures also pale in comparison to potential costs to rebuild affected infrastructure, considering

If we examine the Lake City incident in more detail, it is suggested that they were advised by their insurance underwriters to pay the ransom; Lake City was covered for ransomware under its cyber-insurance policy, and their deductible payment was only $10,000! The senior leadership team believed that paying the ransomware would, in the long term, save time and money.

There is no doubt that deciding whether you should pay a ransom is an incredibly difficult choice. Conventional wisdom might suggest that you should never pay the ransom; however, when considering the recent Florida examples, you could argue that by paying the ransom, both Lake City and Riviera City saved themselves a small fortune that would have gone to pay expensive security consultants to fix their problems.

Paying up does, however, play into the hands of the hackers, and demands for payment may skyrocket if hackers are sure their victims will pay. Paying up is also only fixing half the problem. Yes you may get your systems back, but the infrastructure will need an expensive overview, fixing, and redeployment to prevent it happening again.

Why Is Ransomware Proliferating Across the United States?

There are numerous examples of computer systems used by corporations, schools,

police and city governments being targeted by ransomware and suffering extensive system outages.

It could be suggested that paying ransoms is feeding this growth; the number of institutions that are covered by cyber insurance has grown, building an estimated $7 billion to $8 billion-a-year cyber insurance market in the U.S. alone.

ProPublica has conducted extensive research suggesting that insurance companies are fueling the rise of ransomware attacks by paying hackers. They also suggest that hacking groups are deliberately targeting American companies that they know have cyber insurance. In response to the attacks on Baltimore, Atlanta and Lake City at the 2019 United States Conference of Mayors, an official statement was released "opposing the payment to ransomware attack perpetrators".

This resolution is significant, as it is one of the first official statements identifying that ransomware is proliferating in the United States, and that ransomware is specifically targeting local US government entities. The resolution warned against paying ransomware attackers, as the practice encourages continued attacks on other government systems. They also strongly recommended "standing united against paying ransoms in the event of an IT security breach."

Should You Be Worried About Ransomware?

No matter what protections organizations employ to prevent ransomware, they should still be concerned about their potential exposure to risk. Hacking communities are actively developing new strains of malware, not to mention sharing and trading the source code on the dark web. Without a doubt, the sophistication of ransomware attacks is growing.

Hackers are continuously looking for vulnerabilities in operating systems and popular applications, discovering backdoors and security flaws they can exploit with cleverly-designed software. System administrators and security teams are firefighting detected threats, and the process of protecting computer infrastructure can be time consuming and painstakingly difficult.

Organizations can implement the best industry standard security practices, threat detection systems, and hardware layer protections, but a business' IT security is only as strong as its weakest link. Unfortunately, the majority of ransomware is still propagated by user-initiated actions. Careless, accidental, or reckless actions by employees can leave the door wide open to a ransomware attack.

This is where the expertise and professionalism of a managed security service provider

can bolster the security of your business. Whether you choose to implement security recommendations or outsource your entire IT department, the experts at Atlantic.Net put your business first, securing your IT platforms from the very latest and future threats.

Ransomware Prevention

To protect yourself from ransomware infection, it is important to follow several security best practices to ensure that you are safeguarded. It is essential to be certain that your infrastructure and network are in a healthy state to give the best possible protection from ransomware.ess.

- **System Inventory** – One of the first steps to follow, particularly if you are a business, is to complete an inventory of all your business assets. This will include all digital assets such as servers, desktops, laptops, network equipment, and digital infrastructure. Cataloguing what assets you own will allow you to create a baseline to work from
- **Risk Analysis** – Conduct a cybersecurity risk analysis using the baseline created with the system inventory. This process will allow you to identify security weaknesses and create a priority list of what to fix first
- **Run a Supported Operating System** – It is important to be running a modern, manufacturer-supported operating system. OS licencing can be expensive, but it is critical to have supported operating systems, as you are then entitled to security updates and patching. Windows 7 and Windows Server 2008 are phasing out of support in January 2020, and all previous iterations are already no longer supported
- **Patching** – Arguably, one of the best methods to protect against malware is to ensure that your infrastructure is patched to the very latest levels. This includes server patching, Windows updates, firmware, and microcode updates
- **Application Updates** – software applications need to be updated too; this will help to reduce vulnerabilities. Ensure that antivirus is installed and updated daily to guarantee the very latest threat prevention databases are invoked
- **Training** – Another key protection against ransomware is to train all employees about the risks of ransomware. This should help them to understand what cybersecurity is and what to look out for in avoiding risks. Common examples including being on the lookout for phishing, scams, and fake websites
- **Backups** – If the worst does happen and you are impacted by ransomware, often the quickest resolution is to restore from backup. Regular offsite backups should be completed on a daily, weekly, and monthly rotation to reduce the likelihood of the backups also being infected
- **Disaster Recovery** – Create and test a disaster recovery plan, including a scenario where a total outage is caused by ransomware. This might be a high availability DR

setup in a secondary site or with a cloud provider

- **Penetration Testing** – This is a technique of testing external and internal computer infrastructure against all known vulnerabilities. Pen testing and vulnerability scanning will generate a list of recommended fixes needed to harden the infrastructure

Conclusion

The research we have undertaken is unanimous in the opinion that ransomware is an increasing threat. We have seen increases in the number of ransomware attacks in the last few consecutive years. It would appear that hackers are changing their methodology to focus on ransomware (instead of other types of malware), as it is the most likely attack method to succeed.

We have found evidence that suggests there is a shift away from targeting individual users in blanket ransomware attacks, instead choosing to target wealthy businesses, healthcare, education, and local and regional government institutions. Hackers choose to target these institutions because it is likely to have the biggest impact if the breach is successful.

As there is no reporting authority, reports of factual numbers of ransomware victims are very difficult to produce, and it is possible that only a fraction of the incidents are actually being reported. We have also found evidence that suggests the hackers are shifting their focus towards creating ransomware specifically targeted at institutions who are more likely to pay. Hackers may "know" which institutions are covered by cybersecurity insurance, and victims with insurance may be more likely to pay out.

Many technical, process and training safeguards can be introduced to help create a robust cyber security policy that should be implemented throughout the entire organization. Each of these safeguards should be reviewed and renewed annually, but it is also important to have a tried-and-tested business continuity and disaster recovery process should the worst happen.