Ransomware in Cities Across the United States

Clifton Paul Robinson
Northeastern University
robinson.c@husky.neu.edu

Abstract - **Ransomware is the attack that continues to grow and has become a nightmare on state and local governments. The malware that will infest a system and encrypts all the files can completely cripple an entire local government or organization has been on the rise over the past several years thanks to anonymous criminals who run sites that send our ransomware and collect the money that is demanded. In this paper, we look at more recent examples of ransomware attacks on cities and governing bodies that paid the price in one way or another, though these examples we can draw conclusions on how to prevent these attacks and how to deal with them if you are, in fact, hit with one.**

I. Introduction

Over the past decade, we have seen the amazing growth and development of the Internet. From the increased reliance on social media to everything starting to be on the cloud, we have entered an even stronger age of technology. However, where there is further advancement comes stronger adversaries attempting to destroy what everyone relies on now. Today we see strong attacks that can end up crippling certain services like what we see in Distributed Denial-of-Service (DDoS) attacks, stealing sensitive data like in man-in-the-middle and eavesdropping attacks, and see adversaries prey on human error to infect certain systems with malware as we see in phishing attacks, as well as many others.

As technology advances, so do these attacks, but how do we combat them? How do we handle them once we have already been attacked? What happens if these attacks hold cities or towns hostage? In this paper, we take a look at ransomware attacks on local and city governments. These attacks encrypt entire systems and put them on lockdown while demanding a ransom, once the ransom is paid the attackers send the encryption key. Recently, ransomware has come to the forefront of cyberattacks, especially on smaller governments within the United States. In this paper, we will look at data and recent events such as Baltimore, ME, Georgia, and several other cases to look at the growing threat of ransomware and how we can start to combat it.

II. Ransomware Attacks

As stated quickly prior, ransomware is a type of malicious software that is designed to deny all access to a computer system or data until a ransom is paid [Homeland]. As stated by Norton, the concept behind this attack is quite simple: “Lock and encrypt a victim’s computer data, then demand a ransom to restore access.” These attacks can end up being detrimental to individuals as well as organizations because usually, the adversary gives a set amount of time to pay the ransom before they get locked out for good, losing all of their data forever.

There are several ways that ransomware can spread, the most common way this happens is through phishing emails. These are fake emails that are intended to trick the target into either handing over personal data or download malware. In this case, a phishing email would be sent containing either a file or a download link to the ransomware software, once it is downloaded onto the system and starts running the software is able to encrypt and lock all of the data until it receives the encryption key.

Ransomware isn't black and white though, there are actually five different types of ransomware, and some are more harmful than others, but they all share a common goal: getting a ransom. The five types are [Norton]:

1. **Crypto Malware:** This one is more well-known and causes a lot of damage. This type of malware encrypts files and can only be unencrypted after the ransom is paid.
2. **Lockers:** This one is known for infecting an operating system to completely lock out the owner of the computer, making it impossible to access any files or applications.
3. **Scareware:** This is a type of fake software that disguises itself as an antivirus. This malware says it found an issue and then demands money to fix the issue. Some instances will lock you out, while others will just flood your screen with alerts and pop-up messages.
4. **Doxware:** This form is more commonly referred to as leakware. This is really the blackmail version of ransomware, where the attackers threaten to publish the victims' stolen information online unless a ransom is paid.
5. **RaaS:** This is also known as "Ransomware as a Service." This acts as the middle-man for ransomware attacks. Here the malware is hosted by a hacker anonymously and they handle distributing the ransomware and collecting the payments, where they receive a part of the ransom.

When you see all of these attacks it can be overwhelming for sure, but it really does boil down to the fact that it deals with someone paying a ransom to get their information back. Now, we start to ask, what if this happens to me? How can I prevent this? Why do people do this? Throughout this paper, we will look at different ransomware attacks and see how it was handled and why it happened.

III. Background

Over the past several years we have started to see ransomware attacks come into the forefront of the media with constant attacks being carried out against many local governments. This starts to become an issue because it is hard to determine when ransomware is downloaded, so usually, we don’t know how it infects a computer or system. As we start to look deeper into how this spreads we can see that it usually comes from one of three sources: Emails, Browsers, or Malicious Downloads [How Does Ransomware Get on your Computer]. Now the better question is why is this becoming such a common attack? When you begin to think about what they are attacking it starts to make sense, when adversaries successfully attack governments with ransomware they place a full lockdown on important documents and cripple the city from the inside making even the simplest tasks impossible. In the next part, we will take a look at several recent examples of ransomware attacks and see how they responded and took action against the malware.

IV. Recent Examples

Recently, there have been so many ransomware attacks that if we covered all of them this paper would go on forever, so we will take a look at three of the more recent examples and see how each one was handled, how it impacted everything, and what the outcome was. The three ransomware attacks we will look at are the cities of Baltimore, Maryland and Riviera Beach Florida, and the Georgia Court Agency.

Baltimore, Maryland:

More recently, this attack seems to be one of the biggest ones, this is probably because the attack was carried out on the 30th biggest city in the United States and with Baltimore having a population of over 600,000 people, an attack like this can put an entire city on standstill.

On May 7, 2019, the city had discovered that they were a victim of a ransomware attack. They immediately took their systems offline to keep the ransomware from spreading, but a lot of damage had already been done, the attack took down the city's voicemail, email, parking fines database, as well as a system that is used to pay water bills, property taxes, and vehicle citations. As soon as they knew what happened they immediately notified the F.B.I. about the attack. Another big issue the city faced was that 1,500 pending home sales were also delayed. After the took everything offline they put into place an offline fix that allowed transactions to continue [Chokshi].

Then the city was sent a digital ransom note that said they would get the decryption key if they paid the hackers 13 Bitcoins, which is about $75,000 when the attack happened. Right off the bat, the city stated that they would not pay this ransom, following the common recommendation of the FBI. Going into July 2019, Baltimore said they were very close to being back to completely normal operation, but now the city has also put in more than $18 million to fix what was broken from this ransomware attack [Eiten].

Riviera Beach, Florida:

In June 2019, Riviera Beach was hit with a ransomware attack because a police department employee opened a phishing email. This city is much smaller than Baltimore, Riviera Beach has 10 people in their I.T. Department while Baltimore has about 50. The demanded ransom for them was for $600,000 to regain access to all of their cities data. This price was even higher than Baltimore, but Riviera Beach went against the advice of the FBI and voted to pay the ransom, luckily, $300,000 of it was covered by their insurance policy [Gallagher].

For a city that has an operating budget of only $2.5 million per year they decided that if they didn't pay the ransom they would have paid two to three times more, and that would have been without insurance. However, even though the city got their data back they are far from being in the clear. Now, the small I.T. department needs to work to patch all the issues that led to this attack and they are also on the radar now because they are known as a city that paid a ransomware attack.

Georgia Court Agency:

Out of the three examples, this is the most recent and has the most interesting responses. Hackers were able to infect computers at a Georgia Courts Agency while demanding a ransom of an undisclosed amount last month. They were able to bring down the administrative office of the courts where they maintain court documents, offer online applications, and publish information on court operation. All of their websites were down and *still* are down [Niesse].

Luckily, no personal information was compromised from this attack because this agency doesn't keep that information. The agency does see this as an inconvenience, but people can go to their offices to fill out their forms in person. It is interesting seeing an agency truly just not care about a ransomware attack, overall they are acting like all business is normal, just no website to tie everything together.

V. Discussion

When you look at all three of these examples it is really hard to determine one true response to ransomware attacks. You see Baltimore refuse to pay the ransom, Riviera Beach pays because they have no other options, and the Georgia Court Agency pretty much just ignore it. The real issue is a common one in the field of computer science, ethics. We see tons of ethical dilemmas whether it's about data collection, hidden agreements in terms and conditions, web scrapers, the list can go on because we are still in uncharted waters. However, ransomware is a true ethical dilemma.

To pay or not to pay? That is the question and there doesn't seem to be a right or wrong answer. You first have to ask yourself if it is good or bad to pay a criminal to receive information back. The second is when a government agency needs to pay a ransom from ransomware it partially comes from their operating budget which is from the taxpayers. How ethical is it to pay a ransom with taxpayer money? Even if the money gets back the taxpayers information? As you can see this these questions get hard to answer. The FBI will always say never to pay but that makes sense, why would the Federal Bureau of Investigation tell people to pay ransoms to people breaking the law.

Ransomware is a weird attack because it seems to have "honest" criminals. One of the reasons the FBI says not to pay is because there is no guarantee that that the criminals will send the decryption after they have been paid. Everything I read never said that once the ransom was paid the decryption was never sent, showing a weird type of criminal that is true to their word. This just really seems like a different type of attack in most ways, especially with how you deal with it after it happened, but that can be prevented.

VI. Countermeasures

I've said it many times, ransomware is interesting, but when it comes to countermeasures it is the most dangerous malware that is the easiest to avoid. As we saw in the Riviera Beach attack, the ransomware was downloaded from an employee opening a phishing email. The first countermeasure for local governments is to make sure that everyone with access is trained for internet threats. This automatically helps lower the chance of employees clicking on infected links and potential phishing emails, especially because humans are the biggest danger to cybersecurity.

The two other main countermeasures that take a lot of human error out of the equation are keeping your security up to date and doing continuous backups on an offline server. With up to date security, you are usually safe from most malware because it catches it before it can be downloaded or spread through a system. With an offline backup, it also renders a malware attack completely useless because all you have to do is reboot the system with the last backup. If you follow these countermeasures, you will be safe from ransomware attacks.

VII. Conclusion

Ransomware has more recently become the goto attack, especially when it comes to local governments. We have seen a rise in this because more times than not the victims end up paying the ransom. As we move into a future that is relying more and more on technology and the internet we have to wonder will ransomware evolve or will it go extinct? In my own opinion, I believe that ransomware will not be around for much longer just due to the fact that it's simple yet effective. We have also been given many different factors to prevent these attacks, once people start listening and implementing these defenses then it won't be worth it for these criminals to continue exploiting these attacks.

We looked at three recent examples that give a strong overview of how ransomware attacks can affect local governments in different ways. Tons of other examples could be used to show the impact this attack can have as well as seeing how other areas outside of governments are affected by ransomware attacks. We see a simple attack that can cause a lot of damage and can be fixed with an untraceable payment, but it starts and ends with an ethical dilemma, to pay or not to pay?

References

CBS News. "Georgia Court System Struck by Ransomware Attack." CBS News, CBS Interactive, 2 July 2019.

Chokshi, Niraj. "Hackers Are Holding Baltimore Hostage: How They Struck and What's Next." The New York Times, The New York Times, 22 May 2019.

Duncan, Ian. "Baltimore Proposes to Use $10 Million in Excess Revenues to Cover Cost of Ransomware Recovery." Baltimoresun.com, Baltimore Sun, 1 July 2019.

Eiten, Kimberly. "Baltimore Ransomware Attack: City Inches Closer To Normal Operation." CBS Baltimore, CBS Baltimore, 12 June 2019.

Gallagher, Sean. "A Tale of Two Cities: Why Ransomware Will Just Get Worse." Ars Technica, 21 June 2019.

"How Does Ransomware Get on Your Computer?: Ransomware Encryption." Comodo Enterprise, 8 June 2018.

Niesse, Mark. "Georgia Court Agency Hacked in Ransom Attack." Ajc, Ajc.com, 5 July 2019.

Norton. "What Is Ransomware? And How to Help Prevent It." Official Site.

Pelly, Scott. "How Cybercriminals Hold Data Hostage... and Why the Best Solution Is Often Paying a Ransom." CBS News, 60 Minutes.

Stewart, Emily. "Hackers Have Been Holding the City of Baltimore's Computers Hostage for 2 Weeks." Vox, Vox, 21 May 2019.