Ransomware in Municipalities:

An Investigation into ransomware and its specific use in targeting US cities

Nick Williams

Tufts University

December 6, 2019

Abstract

Every 14 seconds an organization falls victim to a ransomware attack, on average. This is expected to rise to every 11 seconds by 2021[6]. With ransomware attacks increasing 97% in the last two years combined with the fact that ransomware is generating 25 million dollars a year in revenue for hackers, it is not going anywhere soon [6]. All the predictions say that it will only increase and 81% of surveyed security analysts said their organizations are not prepared to handle a ransomware attack [6]. This paper will dive specifically into the ransomware attacks on municipality. These have been on the increase in America hitting the small and technologically outdated cities. Most notably, and to be discussed in detail, was the attack on Atlanta in March of 2018 which crippled their systems for weeks. The demand was for $51,000 and they denied paying it. The repairs and delays in business were estimated to cost the city 17 million dollars [7]. I will be looking into why these cities are targeted, what ransomware is and what are the tools being used in attacks, and how these cities can try and prevent them or handle the aftermath. I will specifically be looking at SamSam, Sodinokibi, the social engineering behind phishing and the psychology of recovery.

Introduction

I. *Ransomware, Broadly Speaking*

Ransomware in its simplest form is a piece of malware that attacks and compromises a machine and demands the user pay a ransom or bad things will happen. These so-called bad things can be a very broad range of things and most commonly the malware will encrypt data or lock out a user therefore restricting access and demand the ransom be paid in order to regain access. However other types of ransomware include those which provide a fake scare saying there is malicious activity on the computer and a fee must be paid to remove it. There is also ransomware that will compromise a computer and threaten to leak stolen sensitive information if the user does not pay a ransom [1]. All these types of ransomwares demand money and there is no guarantee that the attacker will keep their word after the user has paid the ransom. For this paper I will be focusing on mainly ransomware that restricts user access. This alone is a broad field and is being narrowed to municipal attacks in the United States. These are attacks that are centered at cities and usually restricting access to city networks and hardware as well as digital resources that the city maintains.

II. *To The Community*

Ransomware in municipal cities has been on the rise lately as well as all cases of ransomware attacks. Ransomware differs from many other malwares in that it does not need to lie dormant for very long to encrypt data for a simple ransomware attack. Therefore, it can be a small file that acts quickly and less subtly once it finds a compromised machine. This, partnered with the possibility for a high-profit, has made ransomware an extremely appealing field to many black-hat hackers. A survey of cyber security professionals revealed that half do not feel their business is prepared for an attack and with the average attack on a business costing 133,000 dollars it bodes for an alarming issue [6]. Beyond the cost of simply paying the ransom or repairing your systems there are large costs associated with downtime and reputation hits. Municipalities in specific are usually much lower on budgeting and security professionals leaving them particularly exposed to attacks. Moreover, there is very little legislation helping fight back against ransomware where only five states have laws specifically regarding ransomware attacks. All these frightening statistics combine show the absolute need to take steps in the right direction to fighting ransomware and this paper hopes to take some of those steps.

Ransomware in Municipality

I. *Which Cities are Targeted and Why? Who Reports It?*

Ransomware is on the rise and municipal governments are particularly at risk for a plethora of reasons. Hackers, just like any business scheme, want to maximize profit at

the lowest cost possible. Therefore, it makes good sense to attack municipalities. The chief concern for local governments is money for multiple reasons. Firstly, the lack of funding means that they cannot hire as many cyber security professionals as this is a highly demanded field with competitive salaries that local governments cannot afford. This leaves them more vulnerable and less prepared. The lack of funding is also a problem when it comes to system updates. Even simple things that do not require a professional can lead to serious vulnerabilities. For example, Atlanta, who suffered a large ransomware attack, had many machines that were outdated and no longer supported as of 2015. While the lack of cyber professionals is an issue because no one can adequately prepare for an attack or recover, it also is an issue because there is less training of users. With low end user accountability, the systems are more susceptible to breaches from user ignorance. All these combined make systems highly vulnerable and a promising target as far as gaining access.

There has also been a drastic increase in targeting organizations over individuals since they can see to a larger payout. Despite America's "We do not negotiate with terrorists" policy, multiple cities have paid out the ransom. Many small ransoms have been paid and even larger ones, notably Jackson County, Georgia who paid 400,000 dollars, Lake City, Florida who paid 460,000, and Riviera Beach, Florida who paid 600,000 dollars [4]. It is more common for a local government to pay out since it has services that it needs immediate access to, like 911 or 311 services which can be affected by municipal ransomware.

This is not to say that all is hopeless though! Since 2011 60% of counties have increased cyber security spending and funding, according to a study conducted by the International City/County Management Association in 2017 [18]. However, this study also revealed that only 43% of attacked cities/counties perform forensic analysis after the attack which is crucial for learning from their mistakes to properly rebuild and protect themselves in the future [18]. It also showed that 67% of municipalities lack a written response plan for a ransomware attack [18]. It is near impossible to secure a system and having a detailed plan up front could save hundreds of thousands of dollars in recovery. While there are some options to partner with bigger agencies like in the case of the Colorado ransomware attacks on public transportation in 2018. Stemming from this attack the state of Colorado declared a state-wide emergency, the first move of its kind [9]. This allowed the Colorado National Guard Cyber Security team to be deployed. While collaboration opens new resources, many cities are hesitant due to intense bureaucracy. This leads to many cases of ransomware going un-reported and handled with hiring private teams or slow IT team recoveries. The real issue is that while municipalities try to fight back, they can only do it so fast with limited resources. The people who intend to attack are evolving at a much faster pace.

II. *Case Study of Large City: Atlanta*

The city of Atlanta was hit with one of the largest ransomware attacks recorded for a municipal system. While it is common for attackers to target small cities for their relative unpreparedness some large cities are equally unprepared, as was the case with Atlanta. The attack occurred two months after a new mayor, Keisha Bottoms, had entered office and she admitted that she had put little thought into cyber security prior to the ransomware attacks. One of Atlanta's chief issues was the lack of updated hardware that lead to gaping vulnerabilities in software. Scans run after the attacks showed over 2,000 serious security vulnerabilities that had been known for months prior to the attacks [9]. Being prepared and on top of these could have helped mitigate the problems early on. The attack on Atlanta was executed by a program called SamSam which is to be explained in detail later. Atlanta is a specifically interesting example when it comes to the decision to pay the ransom or not. It is highly advised to not pay the ransom because this encourages the craft of ransomware as well as showing the city as willing to pay and weak to attacks. There also is the complication that the attackers might not unlock the network after the ransom is paid. With all these negative sides to paying, Atlanta decided not to pay. The ransom that was asked of Atlanta was about 51,000 dollars. Atlanta has yet to recover entirely from the attack now, over a year later. It was most recently estimated that it could cost Atlanta a total of 17 million in loss of revenue and recovery costs to restore itself to its previous state [7]. This massive difference between ransom and costs of recovery is an important consideration.

III. *Case Study of Small Cities: Texas Attacks*

Cases like that of the simultaneous attack of 22 cities in Texas in August of 2019 by a ransomware called Sodinokibi are much more common than larger attacks like that of Atlanta. The reason being that these smaller towns usually have less protected data and it is easier to gain access. For example, the Texas attacks used vulnerabilities in the server and some access through phishing and exploit kits. However, once the malware was in it used the data inside to get credentials and spread like wildfire to any connected computer it could. Therefore, it was so effective, reaching 22 cities. The ransomware is an extremely evasive and sophisticated ransomware that can be seriously problematic for organizations. The attackers demanded collectively 2.5 million dollars from the Texan cities showing the bolder moves made by attackers [5]. None of the cities paid the ransom and have since been in recovery. Luckily Texas nearly immediately enter a state-wide emergency and deployed many teams to fight back. Still this was a huge hit to Texas as a whole. It left many government employees without access to computers and forced them to make calls on their personal cellphones as phone lines were down. There was a potential loss of legal documents and automated processes such as issuing tickets, issuing utility bills, and even checking out library books were either put to a halt or done with old fashioned paper and pen. Overall, small or large city, if there is a ransomware attack it

will leave the city in a bad place having to spend tens of thousands or millions of dollars to recover.

Specifics of Ransomware

I. *Social Engineering*

The social engineering behind ransomware is highly important and extremely interesting. One highly used method of distribution for ransomware is through phishing which involves social engineering. While phishing is on the decline thanks to increased security lessons in organizations, it is still a highly relevant form in ransomware. The ransomwares that are moving away from phishing are exploiting vulnerabilities to gain access more like a traditional malware. However, phishing is used to gain access usually though an email that either tricks a user into opening a file with malicious code in it that runs or through tricking the user into revealing credentials that then allow the attacker to gain access. This is an important field to understand as the attackers get more sophisticated, they can make phishing scams that look identical to official content. Without the proper education it is likely that many more people will fall victim to phishing. This returns to one of the main takeaways of this paper in that education is one of the most important steps we can take to help mitigate the damages done by ransomware.

II. *Crafting and Use of Ransomware*

Crafting and use of homemade malware are frighteningly easy to do. There are many guides online to walk a user step by step though creating their own malware. Anyone with some coding experience will not struggle to spin up their own custom ransomware. Even more disturbing possibly is the rise of ransomware as a service or RaaS. To start with the ransomwares that can be built from scratch, they are far less sophisticated, but still a dangerous thing to know that anyone who wants to attack an individual has easy access to do so. For example, there is the Hidden Tear ransomware that is fully built and only requires the user to set up a server before it is deployable to targets. A much more sophisticated option is ransomware as a service (RaaS). There are people who will build much more highly sophisticated ransomwares and distribute them to affiliates to attack targets. For building and distributing the ransomware they usually take 30-40% of the ransom once it is paid [16]. This is rising in popularity and those developers are putting some of their profits back into development after seeing how profitable it can be. It will most likely be the case that RaaS is the future of ransomware.

III. *Notable Ransomwares*

The two ransomwares we will investigate are the two used in the Atlanta and the Texas attacks. These are SamSam for Atlanta and Sodinokibi for Texas. SamSam is a targeted malware that differs from others in that it is not randomly distributed through

bulk spam emails and is instead targeted at a specific organization. It has been around since 2015 and the FBI has indicated that two Iranian men are behind it, but with little jurisdiction nothing has been done about criminal charges against them [22]. SamSam is extremely popular with 67 reported attacks in 2018 and the creators of SamSam are thought to have made 6 million in revenue since 2015 [19]. SamSam's main point of attack is brute force where it attempts to get weak passwords to gain access to remote desktop protocols. It also has been linked to heavy usage of JBoss sever vulnerabilities. Once the attackers are into one computer, they attempt to work their way through many computers on the same network to have a more devastating effect. This is done through giving advanced privileges to one computer and exploring the network for business-critical documents to encrypt as well as other credentials to gain access to new machines. Unlike many other ransomwares, SamSam requires no user interaction like accidentally opening a malicious file. It is an entirely remote attack with stolen credentials, sometimes purchased from the dark web. Some of the best ways to protect from SamSam is to have strong passwords, remove open remote desktop protocol ports if you can, regular security checks on the network and having good current backups in case of an attack.

Sodinokibi on the other hand is a RaaS. This is an interesting category of ransomware as the developers do not do the actual attacks. It is a much newer ransomware with a large surge of attacks in 2019. Despite it being a RaaS it is not any less profitable for the developers and it has been seen to generate 287,000 dollars in three days for the developers with potentially 4.5 million dollars or more total according to an article from mid-October 2019 [17]. Through bitcoin and other concealing tactics, it is extremely hard to trace the transactions and the perpetrators remain unknown as of now. However, there is some connection to the authors of GandCrab, a now retired ransomware that was responsible for 40% of all reported ransomware incidents globally [20]. While Sodinokibi is like SamSam in that once it is in it tries to spread it is different in how it gains access and spreads. Sodinokibi commonly gains access through an Oracle WebLogic vulnerability (CVE-2019-2725) and then spreads through spam and exploit toolkits. However, it has also been known to enter through an initial phishing email. Once it is in the system there are malicious JavaScript files that are usually obfuscated so that they go undetected by anti-virus software. An August version of Sodinokibi was only flagged by one vendor on VirusTotal in August. Once into the machine it de-obfuscates itself and begins its nasty work. This starts with a Windows PowerShell script which helps it bypass permissions. Next it goes about removing any security defenses it can and then encrypting all the data and displaying a ransom note. Interestingly, there is a step that checks the language of the files before encryption and if it finds files that are in the language of a prior Soviet Union State it does not encrypt and attempts to wipe all trace of ever being there. It is suspected this is because the attackers have nationality within the prior Soviet Union States and are attempting to avoid persecution if caught. Many of the

ways in which to protect yourself from Sodinokibi are common to protecting yourself from SamSam like strong passwords and good backups.

Direction of Ransomware and Municipalities in the Future

I. *The "American" Mentality and Global Incidents*

When it comes to recovery from ransomware attacks there are a couple of options, but the real question is to pay the ransom or not to pay. While the focus of this paper has been on ransomware attacks in the United States this is a global issue. The connectivity of the web today allows for an attacker from anywhere in world to reach almost anywhere else in world. This means that ransomware is plaguing the whole world. However, America differs from everyone else in that America is driven by a lower government intervention and a strong feeling about not negotiating with terrorists. The United States is recorded paying 3% of ransomware ransoms while Canada is seen to pay 77% and European countries like the UK and Germany paid 42% and 22% of the time [6]. Of course, these are only reported cases and many times ransomware attacks go unreported, especially in private organizations. It is always a hard decision to make when paying as people's lives or critical societal functions might be on the line or it could cost way more to repair than to pay the ransom. All of this is important for attackers to consider as they try to set a price low enough that it will be paid, but high enough that it is profitable. This mentality to not negotiate and not pay ransoms is great though because if very few people are paying the ransom then the attackers will be less attracted to attack.

II. *Protection from Ransomware*

Part of the discussion regarding protection is ransomware insurance. This is a service that is offered by some private companies that in the case of a ransomware attack the company will insure some amount of the ransom payment. However, this is a highly flawed system for many reasons. Ransomware insurance is no different than many other insurance companies in that they are just trying to make money. They do not want to pay out ransoms and it can be extremely hard, even when attacked, to get a payout. Beyond this, when they do pay it is an encouraging sign to the attackers. A company that pays out has three flaws. First, they are now seen as a company who will pay out making them a possible future target. Second, they usually do not take the full steps to protect their systems because they just paid out and moved on. Finally, paying money to the ransomware developers and attackers will allow them to fund building better and more sophisticated ransomware as well as buy illegal criminal activity on the dark web, as seen with the Sodinokibi developers [20]. If this continues to be a profitable business, then the attacks will continue to happen.

III. *Recovery from Ransomware*

It has clearly been shown above the consequences of paying the ransom, but also, we have discussed how in some situations the ransom must be paid for critical reasons. We also have seen, like in the case of Atlanta, rebuilding a system can be extremely costly. So, the question remains, is there really a good way to effortlessly recover from ransomware? As of right now it looks like the bleak answer is not really. With over 70 municipalities being hit in 2019 it has become the biggest year for hits to the government. Therefore, one of the most important steps to take is to attempt to prevent an attack. This involves securing systems and training employees to protect from attacks. Prevention measures up front can save millions of dollars in recovery. Another issue is the legislation surrounding ransomware. Cybersecurity is an emerging field and legislation is traditionally a slow-moving field. These do not mix well and only now are states beginning to catch up with legislation. The good news is that as of 2019 37 states have introduced cybersecurity legislation and 24 have enacted these bills [20]. This is not enough though as this is a global issue. Cybersecurity is also a massive field and not able to be covered with one blanket statement. As far as ransomware goes only 5 states have legislation to protect against it. States like California are taking the right steps by passing legislation SB 1137 which makes just placing ransomware on a computer equivalent to extortion and fully punishable by fines and jailtime [13]. Clarifications like this in the law are the right steps to be taken to help ensure that organizations can fight back and hopefully stop some of these attacks. Therefore, attached below, I have included my letter to Massachusetts government to urge for the implementation of similar legislation. It will not be enough to stop at simple cyber security legislation and we must do all we can to stop ransomware before it becomes even worse.

Supporting Material: A Letter to Congress

Dear Governor Charles Baker,

My name is Nick Williams and I am a student at Tufts University in Medford. I am studying computer science and specializing in cybersecurity. I am writing to you with concerns regarding the current legislation surrounding ransomware, especially with attacks on US municipalities. Unfortunately, cybercrime is advancing much faster than protection can keep up with, so it is critical to try to help protect organizations and help them fight back in any way possible.

In 2019 we have seen the largest number of attacks on US cities, counties, and states with over 70 ransomware attacks recorded. There are most likely more attacks that have gone unreported. Ransomware is a dangerous form of malware that can infect an entire computer network in hours. Once infected the attackers locks out the users, encrypting files, and demanding a ransom in order unlock their files. I am sure you are familiar with these cases, but notably we have seen large scale attacks on Atlanta (estimating 12 million dollars in repairs), Baltimore (estimating 17 million in repairs) and even this year 22 cities simultaneously hit in Texas. These attacks are only continuing to grow and are taking out crucial services like local school districts, emergency services, automated government processes and much more. While there are amazing things happening now like the recent passing of bill 315 by the Senate, the DHS Cyber Hunt and Incident Response Team Act of 2019, which will help in response and repair for attacked cities there are more steps that can be taken to help down the road in persecution of criminals that commit these acts.

Five states have taken such action in outlining specific legislation to combat ransomware crime and I urge you to follow suit and consider supporting the creation of a similar bill. It can be modeled off California Senate Bill 1137, Computer Crimes: Ransomware. In summary it "Makes it a crime for a person to knowingly introduce ransomware into any computer, computer system, or computer network." It considers ransomware like extortion and can be punished with up to 4 years in prison. It is extremely beneficial to get ahead of law making so it can be integrated as soon as possible and see actual use in a court of law.

I hope that this is something that can be considered closely by yourself and possibly introduced as a powerful way to combat computer crime. Thank you for your time.

Sincerely,

Nick Williams

Works Cited

1. Barak, I. (2017, May 31). How Does Ransomware Work? Retrieved December 7, 2019, from https://www.cybereason.com/blog/how-does-ransomware-work.
2. BluEnt Software and Product Development. (2017, September 5). You Can Create Your Own Ransomware - Here's How! Retrieved December 7, 2019, from https://www.bluent.net/blog/create-your-own-ransomware.
3. Boyd, C. (2019, November 17). SamSam ransomware: what you need to know. Retrieved December 7, 2019, from https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/.
4. Capital Journal. (2019). Will Government Ransomware Outbreak Spur More Legislation? Retrieved December 7, 2019, from https://www.lexisnexis.com/en-us/products/state-net/news/2019/09/06/will-government-ransomware-outbreak-spur-more-legislation.page.
5. Cimpanu, C. (2019, September 7). No municipality paid ransoms in 'coordinated ransomware attack' that hit Texas. Retrieved December 7, 2019, from https://www.zdnet.com/article/no-municipality-paid-ransoms-in-coordinated-ransomware-attack-that-hit-texas/.
6. Dobran, B. (2019, April 18). 27 Shocking Ransomware Statistics That Every IT Pro Needs To Know. Retrieved December 7, 2019, from https://phoenixnap.com/blog/ransomware-statistics-facts.
7. Fernandez, M., Sanger, D. E., & Martinez, M. T. (2019, August 22). Ransomware Attacks Are Testing Resolve of Cities Across America. Retrieved December 7, 2019, from https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html.
8. Frederick, K. (2019, September 3). The Rise of Municipal Ransomware. Retrieved December 7, 2019, from https://www.city-journal.org/ransomware-attacks-against-cities.
9. Freed, B. (2019, May 22). One year after Atlanta's ransomware attack, the city says it's transforming its technology. Retrieved December 7, 2019, from https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology/.
10. *Hidden Tear Ransomware Setup*. (2018). Retrieved from https://www.youtube.com/watch?v=ILlTB0-xT-k
11. Jain, K. (2015, August 19). Script Kiddies can Now Create their Own Ransomware using This Kit. Retrieved December 7, 2019, from https://thehackernews.com/2015/08/ransomware-creator-toolkit.html.
12. Johansen, A. G. (2019). Ransomware is malicious software that can take over your computer or mobile device, holding your precious data hostage and demanding cash. Retrieved December 7, 2019, from https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html.
13. LaMar, A. (2016, September 27). Gov. Brown Signs Legislation Punishing Ransomware. Retrieved December 7, 2019, from https://sd18.senate.ca.gov/news/9272016-gov-brown-signs-legislation-punishing-ransomware.
14. Muncaster, P. (2019, September 30). Senate Passes Ransomware Law. Retrieved December 7, 2019, from https://www.infosecurity-magazine.com/news/senate-passes-ransomware-law/.
15. Nocturnus, C. (2019, August 5). Sodinokibi: The Crown Prince of Ransomware. Retrieved December 7, 2019, from https://www.cybereason.com/blog/the-sodinokibi-ransomware-attack.

16. O'Connor, F. (2018, June 22). The associated expenses that add to the cost of a ransomware attack. Retrieved December 7, 2019, from https://www.cybereason.com/blog/how-much-does-a-ransomware-attack-cost.
17. Perez, Y. B. (2019, October 14). Sodinokibi ransomware earns hacker $287K worth of Bitcoin in 3 days. Retrieved December 7, 2019, from https://thenextweb.com/hardfork/2019/10/14/sodinokibi-ransomware-earns-hacker-287k-worth-of-bitcoin-in-3-days/.
18. Reeser, S. (2019). How does Ransomware attacks affect municipal governments?: Tennessee Municipal League. Retrieved December 7, 2019, from https://www.tml1.org/town-and-city/how-does-ransomware-attacks-affect-municipal-governments.
19. Security Response Attack Investigation Team, & Symantec Security Response. (2018, November 29). SamSam: Targeted Ransomware Attacks Continue. Retrieved December 7, 2019, from https://www.symantec.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks.
20. Sheridan, K. (2019, October 15). Sodinokibi Ransomware: Where Attackers' Money Goes. Retrieved December 7, 2019, from https://www.darkreading.com/endpoint/sodinokibi-ransomware-where-attackers-money-goes/d/d-id/1336097.
21. Tell Me How. (2017, August 29). How to Create Your Own Ransomware Virus. Retrieved December 7, 2019, from http://www.tellmehow.co/create-ransomware-virus/.
22. US Department of Homeland Security CISA Cyber and Infrastructure . (2018, December 3). SamSam Ransomware: CISA. Retrieved December 7, 2019, from https://www.us-cert.gov/ncas/alerts/AA18-337A.