Issues in Information Systems
Volume 23, Issue 4, pp. 183-191, 2022

DOI: https://doi.org/10.48009/4_iis_2022_116

Ransomware in local government: Risk factors, vulnerabilities, and exploitation during a global pandemic

Alexander F. Ruggiero, *Palm Beach State College, ruggieroaf@my.palmbeachstate.edu*
Theophilus D. Owusu, *Keiser University, towusu@keiseruniversity.edu*
Jermario J. Staley, *Palm Beach State College, staleyjj1@my.palmbeachstate.edu*

Abstract

This research concentrates on ransomware attacks and their effects in local government. With attacks dating back to the late 1980's, this classification of malware has shifted its focus from end-users to a more lucrative high-profile, big-game hunting style. This resurgence in recent years has proven that the size and variety of threats faced today needs solutions to efficiently identify and examine more comprehensive ransomware security strategies. In this research, the evidence dictates that it is necessary to broaden current security methods to protect local government and municipality systems as well as data from the ever-increasing number of ransomware attacks. In favor of this assertion, the beginning of the research will examine the evolution of ransomware, its damaging characteristics, and its advancements. Furthermore, the financial and economic impacts these attacks have on local governments is outlined. This will be followed by methodologies with results and findings to outline a wireless audit and a survey of government employees. Finally, defense-in-depth measures to mitigate the proliferation of ransomware outbreaks will be defined.

Keywords: Ransomware, government, cybersecurity, COVID, wireless, bitcoin

Introduction

Over the past few years, local governments have been frequently targeted for ransomware attacks. Due to the critical nature of their functionality, lack of IT resources, and aging legacy infrastructures, municipalities have been forced to pay hundreds of thousands to millions of dollars in Bitcoin to regain access to their systems (Orcutt, 2018). While this type of attack vector is not new, the response of paying out these ransom demands has only led to more sophisticated attacks. In this research, a deeper dive into ransomware will be presented. Its past iterations, status, and future state will also be examined. The financial and economic fallout of such an attack will also be evaluated. A multi-layered risk-based methodology will be established to impede these attacks, incorporating a defense-in-depth hypothesis to keep local governments protected from ransomware.

In recent years across the United States and in more than 50 cities, ransomware attacks have successfully occurred (McAfee, 2020). Among them, cities like Albany, N.Y.; Atlanta, G.A.; Baltimore M.D.; Imperial County, C.A.; Rivera Beach , F.L. Malware attacks continue to be one of the most popular attack vectors. Of the many classifications, ransomware is prevalent among malware authors. While this tactic is not new and these types of attacks have occurred in the past, recent high-profile ransomware strikes have grown into an intensifying apprehension on how to protect municipalities and local governments against this classification of malware.

According to the FBI, the year 2020 recorded a 400% increase in cyberattacks (Rhame, 2021). It is extremely concerning that ransomware attacks have become more precise, well-organized, and wide-ranging as malware authors are pursuing local governments and municipalities (Thirupathi, 2018). These targets are softer and less secure but hold critical data. When ransomware attacks are seen on the news and broadcasted to the entire world, they no longer elicit shock or disbelief because these attacks have become so commonplace.

Ransomware as a Service (RaaS) is available to criminals who do not have the ability to code and distribute their own works. These novice attackers want a piece of the lucrative action that is earning well organized groups millions of dollars per year (Palmer, 2021). Currently, RaaS is being leased on the dark web to low-level attackers with the capability to deliver and manage ransomware attacks. The developers and authors behind the coded extortion schemes (ransomware) are consequently receiving a cut of each ransom paid out for the decryption key.

With ransomware attacks rising at exponential rates, threat actors and malware authors are developing more complex methods of infecting networks. The days of "spray and pray practices" have been left behind in favor of strategically selecting appealing targets like local governments and municipalities. However, when you consider the rise in overall security hygiene and advanced threat protections attacks that come from a wide area network approach are easy to identify and can be quickly thwarted. In response to these protection strategies, more comprehensive attacks are using reconnaissance, social engineering, and spear phishing. Every one of these methods is designed to help an intruder slip through the defense of softer targets like local governments and are exceedingly effective (Thirupathi, 2018). Ransomware has a firm grasp in the current and future technological landscape and will become more dreadful in the coming years. As IT innovators, we need to move past primitive and outdated prevention measures to build up the newer defense-in-depth strategies to improve security against ransomware attacks.

Background and Literature Review

Bischoff (2021) explains the financial and operational impacts which ransomware has on local government entities. It dives into the scope of impact that ransomware attacks had on US government organizations in 2020 and the estimated cost of $18.8 billion in for recovery and downtime. Bischoff (2021) goes on to state that half of the country's population has been touched in some way by these attacks. Most of the attacks had the end goal of disrupting services and stopping processes, not stealing data. The key findings of the research are presented immediately in the opening portion of the article. There is a heavy use of bulletin points to present the data in an easily consumable format.

Palmer (2021) goes into detail about how prevalent in the business world ransomware has become. The new variants of ransomware are easy to use and are provided as a service by threat actors. This ransomware as a service (RaaS) has become the most common way that companies are getting attacked. Palmer goes into detail about the financial incentives behind the attacks. He also provides statistics on the percentage of attacks which fall into the RaaS category, 2/3 of attacks.

EvilSocket's (2019) documentation was the foundation for the knowledge which allowed the implementation of the pwnagotchi. The information presented on the face of the site outlines an introduction of the device, its features, an installation process, configuration methods, usage, API, plugins, and several other community focused keynotes/elements. There is a whimsical yet intensely direct tone to the literature written by evilSocket. The information gives high- and low-level explanations of the technology that is integrated by the tool.

The components needed to construct the pwnagotchi are a Raspberry Pi Zero W board, a microSD card, a micro USB cord, an e-ink display, and a portable power bank. To build it, the 20-pin GPIO header was soldered onto the board, the display was inserted on top of the header, the firmware was pulled from evil-Socket's public git repo, and the housing was 3D-printed.

Notable Florida Ransomware Attacks: 2018-2020

- In 2019, Riviera Beach FL paid $600K in ransom to hackers and spent an additional $300K on security upgrades.
- In 2019, Stuart FL fell victim to an attack and refused to pay. The estimated cost of downtime and upgrades are believed to be $800K.
- In 2020, Florida Keys Mosquito Control District and City Hall paid $291K in ransom.

While researching the impact of ransomware attacks in Florida, a few IT professionals, under the condition of anonymity, said they believe ransomware attacks are a big deal, but have a hard time getting the resources to properly protect against attacks. As recently as 2018-2019, a survey conducted by Sophos found that at least 50% of organizations were hit with some form of a ransomware attack. Furthermore, 77% of organizations believed they were up to date with security patches when attacked and 50% of those organizations did not even have dedicated ransomware protection in place (Bischoff, 2021).

Methodology

This study was composed of qualitative research which involved wireless auditing of 5 separate COVID testing sites in South Florida where WPA authentication packets were captured and brute forced. This Testing sites were alerted to their vulnerability, amenable to advice given, and will remain anonymous. This was conducted as a white hat exercise and no confidential, PII, or PHI was accessed, and all keys have been deleted. It also includes a survey regarding ransomware which was given to cybersecurity professionals in city and state government with a minimum of 10 years' experience who will remain anonymous.

Our research was centered upon the following two research questions:

1. How can covid testing sites better protect themselves against ransomware/cyber-attacks?
2. What can we learn from surveying IT professionals in the industry on ransomware attacks?

The testing sites were found to have vulnerable wireless networks and they can protect themselves by reinforcing physical security and perimeter restrictions. They can also enforce stricter network policies and protocols. Implementing this defense-in-depth approach will allow quicker detection and mitigation of the attack. Ransomware attacks in government are far too common. The consensus being not enough is being done to effectively protect against attacks.

Results

Wireless Audit of COVID Testing Sites

During Q1 of 2021 when this research was conducted, widespread testing had only been available for a short while. With the physical vulnerability of the population being at the forefront of everyone's minds, digital vulnerability had taken a backseat. Rapidly deployed, mass COVID testing sites were being organized at malls, stadiums, convention centers, gymnasiums, and libraries. There were 5 emergency COVID testing site networks that were targeted for this study and they were all located in South Florida.

These testing sites did not require an appointment and there were large amounts of people coming and going all day to get tested. There were no physical barriers or forms of access control in place to prevent unauthorized individuals from just walking up to the testing site and the locations where the IT systems were kept. The WAP was throwing out a signal well over 500FT upon arrival, so it was picked up very quickly. The MAC of the first SSID that popped up was deauthenticated from its clients. Then, once the WAP attempted to reconnect, an acronym of the emergency management solution company that had organized the testing site appeared on the list of .pcap files. The handshake capture was complete.

One of the researchers took the device home to hook up to a Linux box with enough resources to conduct the data acquisition and test the strength of the hashed keys. The first action was to SSH into the Pwnagotchi to interact with all of the packet captures. The next action executed was copying the target .pcap files onto the Linux box. Then the .pcap files were run through hashcrack while using a custom rockyou.txt word list. The machine that was used to expose the PSK was a standard, if not under powered system.

The Pwnagotchi is a device which executes its program in two main steps. The first step is a deauthentication attack against a WAP and an end-point, such as a mobile device. The second step is to send a flood of association frames to the WAPs to get them to leak a hashed PSK. It relies on Advantage-Actor-Critic (A2C) reinforcement learning methods to learn from the wireless devices in its surroundings. It does this by using a policy gradient model to maximize the crackable WPA key material that it records over time (evilsocket, 2019).

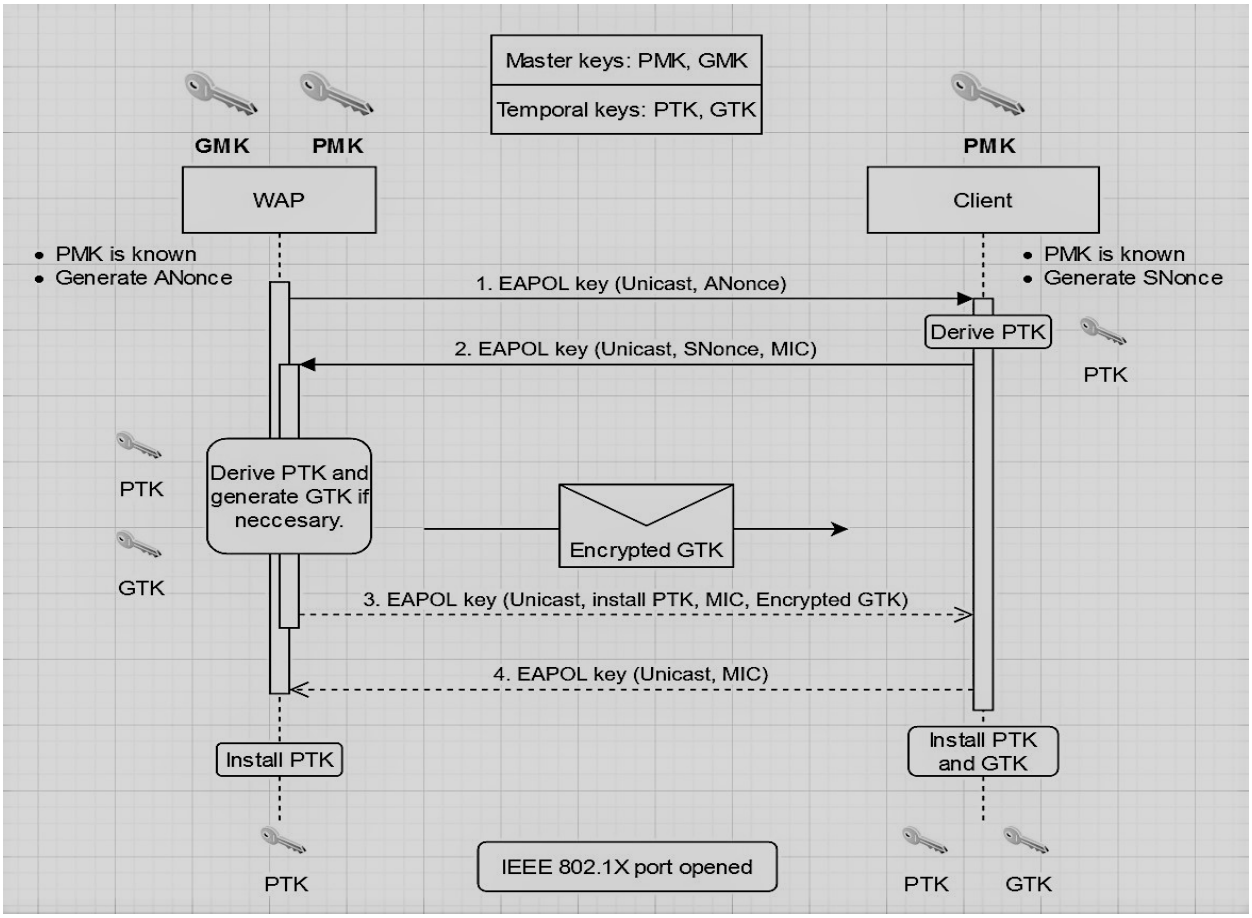

Figure 1: [PMK - (Pairwise Master Key), GMK - (Group Master Key, PTK - (Pairwise Transit Key), GTK - (Group Temporal Key)

The total time that it took to crack the .pcap files that were gathered at the first testing site was 34 minutes and 16 seconds. The second testing site took significantly shorter, at 3 minutes and 43 seconds. The third testing site took 8 minutes and 5 seconds. The fourth testing site was unable to be cracked, which is good. The fifth testing site took 20 minutes and 51 seconds.

Table 1: COVID Testing

COVID testing site #	1	2	3	4	5
Time to decrypt	34:16	03:43	08:05	~ ~:~ ~	20:51

Using this cracked password, it would now be possible to connect directly into the testing center's private networks. Once inside the network, the standard sequence of footprinting, scanning, enumeration, escalation of privilege, covering tracks, and finally planting back-doors can take place (Oriyano, 2014). Once this sequence is completed, the attacker can move laterally in order to gather PHI and PII to exfiltrate, modify,

or delete it. It would also be possible to take control of these machines to further infect other devices and harvest data. This would also provide an opportunity to begin building a botnet.

Government Cybersecurity Employee Survey

The tables below display the results of a survey sent to IT security professionals in the local government. The first table specifically deals with the most recent ransomware attacks that organizations have faced:

Table 2: Employee Survey

First Time Being Attacked?	Attacked Severity	How Organized Was the Attack?	Was A Decryption Key Offered?	Did Your Organization Pay?
Yes – 11% No – 88%	Not Severe – 0% Minor – 0% Severe – 55% Very Severe – 33% Extremely – 11%	Not Organized – 0% Somewhat – 33% Very – 44% Extremely – 22%	Yes – 77% No – 22%	Yes – 0% No – 33% Can't Answer – 66%

The second table deals with the organization of the attack, preventative measures, and future outlook on ransomware attacks:

Table 3: Organization of Attack

How Prepared Was Your Organization?	What Could Have Been Done to Prevent the Attack?	Are Steps Being Taken to Prevent Future Attacks?	Do You Believe They Are Enough?	Are You Better Prepared Today?
Not at all – 0% Could Have Been Better – 33% Somewhat – 33% Moderately – 22% As Prepared As Possible – 11%	Nothing – 22% Better Policy – 22% Budget – 22% Better Planning 33%	Yes – 66% No – 33%	Yes – 11% No – 88%	Yes – 0% No – 99%

A summary of the survey would indicate the common theme between all participants would be not enough is being done to prevent these attacks, organizations are facing this type of attack multiple times and just about all feel like not enough is being done to prevent future attacks.

Discussion

Attacks cost organizations within the US government over 19 billion dollars in 2020 alone (Bischoff, 2021). From a period of 2018 to 2020, it is believed that ransomware attacks account for 53 billion dollars in cost and have affected more than 173 million people. However, it is extremely important to note that a very large percentage of attacks are never reported, and information is rarely readily available for public consumption. Therefore, it is likely that the numbers could in fact be much higher than expert estimations.

Ransomware attacks are becoming more commonplace in critical industries that are fundamental to a functional society like government and healthcare. Research has confirmed that the effort that would be needed to breach a network which is used to transmit, store, and process PHI is extremely minimal and can be done with less than $50 in tools and software. The networks that contain ordinary people's most private and personal data is not being protected by the best practices at a system administrators' disposal. The passwords to the networks at the COVID-19 testing centers should have been more complex. The IT staff responsible for administering the systems in place at these sites should have enforced more stringent password policies. Physical access at most of the sites was completely wide open with no safeguards or physical barriers to IT systems. Any basic NIST security guidelines and standards would have likely bolstered the networks enough to resist being vulnerable.

Based on the survey that was used in this study that was completed by cybersecurity professionals working in the government sector, 99% of them said that they are unprepared for a highly skilled attack even after having a breach. The security that is protecting local government organizations simply is not up to standard (NISTIR 8374). The employees that were surveyed said that 88% of them had been the victim of a ransomware attack in the past. All the attacks were described as moderately severe and well organized. In 77% of the attacks, a decryption key was offered and more than half of those interviewed declined to state

whether their organization paid a ransom. Organizations that voluntarily state that they paid a ransom will likely be targeted again. Over 80% of the employees interviewed stated that they were not as prepared as they should have been. 66% of those interviewed stated that they are actively taking steps to prevent future attacks from occurring but all of them said that it is not enough. This information is deeply concerning and should be heavily taken into consideration by state and federal representatives.

Limitations

This study has a few limitations. First, the study and concepts were applied to the region of South Florida. Although there are municipalities around the country, we intentionally provided statistics and solutions towards the local regional municipalities to provide a positive impact to the community. A broader and larger view would provide robust insight that students and readers could then apply to their local government or other information system entities.

Conclusions

In closing, ransomware represents a serious threat that will likely always remain prevalent. Over the past few years, local governments have been frequently targeted for ransomware attacks. In 2020 alone we saw an increase in ransomware attacks by an estimated 400% (Rhame, 2021). More resources need to be allocated to the security of network infrastructure to protect against these attacks. The financial cost of correctly allocated resources would pale in comparison to that of ransoms paid or the cost incurred after an attack. Just about all surveyed for the purpose of this research acknowledged they could be better prepared. It took just an average of seventeen minutes to compromise the networks of the testing sites. Ransomware is a serious threat, and organizations must act accordingly.

References

Barker, W., Fisher, W., Scarfone, K., & Souppaya M. (2022). *Ransomware Risk Management: A Cyber-security Framework Profile*. NISTIR 8374.

Bischoff, P. (2021). *Ransomware attacks on US government organizations cost $18.9bn in 2020.* Retrieved from https://www.comparitech.com/blog/information-security/government-ransomware-attacks/

evilsocket. (2019). *Pwnagotchi - Deep Reinforcement Learning instrumenting bettercap for WiFi pwning*. Retrieved from https://pwnagotchi.ai/intro/

McAfee. (2020). *Ransomware threats prediction 2020*. Retrieved from https://www.mcafee.com/us/resources/reports/rp-threats-prediction-2020.pdf

Orcutt, M. (2018). Block Chain. *MIT Technology Review*, 23-24.

Oriyano, S. (2014) *Hacker Techniques, Tools, and Incident Handling*. Jones &Bartlett learning.

Palmer, D. (2021). *Ransomware as a service is the new big problem for business.* Retrieved from https://www.zdnet.com/article/ransomware-as-a-service-is-the-new-big-problem-for-business/

Rhame, R. (2021). *The rise, fall and rise of ransomware.* Retrieved from https://www.itpropor-tal.com/features/the-rise-fall-and-rise-of-ransomware/

Thirupathi, R. L. (2018). Understanding the Influence of Ransomware: An Investigation on it Develop-ment. Mitigation and Avoidance Techniques. *Geneze International Society* , pp. 123-126.