Ransomware Characteristics by Country

Joshua Mitchell

December 12, 2018

Abstract

This paper will discuss the characteristics and behavior of North Korean, Russian, and Chinese ransomware attacks. Ransomware is a type of malware that extorts its victims into paying ransom by threatening to make the victim's data public or by blocking the victim's access to said data. Each ransomware attack may have different characteristics and/or behavior depending on what country the attack originates from. This paper will explore the similarities and differences between ransomware attacks and some of the hacking groups behind the attacks originating from the aforementioned countries.

1 Introduction

Ransomware is a kind of malicious software, or malware, that is designed to deny its victims access to their computer system or data until a specified ransom is paid. Depending on the origin of the ransomware attack and/or the attackers behind it, the ransomware is likely to have certain characteristics that make it unique. In order to show how the characteristics of a ransomware attack can vary based on who the attackers are and the origin of the attack, this paper will explore a few notable ransomware attacks and hacking groups.

1.1 WannaCry Ransomware Attack

On May 12, 2017, the WannaCry ransomware attack suddenly appeared and managed to spread itself in a short amount of time. In only a matter of hours, thousands of computers around the world were infected. What made this attack particularly dangerous was its ability to self-propagate and spread itself over an organization's network and to other organizations using the internet. The attack propagated by exploiting a vulnerability in some Microsoft Windows operating systems. This exploit is known as "EternalBlue". The attack was stopped prematurely due to how easy it was to find the killswitch. [6]

1.2 NotPetya Ransomware Attack

On June 27, 2017, the NotPetya ransomware attack appeared using tactics similar to the WannaCry attack, showing that it was likely inspired by the earlier outbreak. Hundreds of organizations were infected as a result of the attack. Like the WannaCry attack, NotPetya could self-propagate using the "EternalBlue" exploit; however, it seemed to mainly target organizations in Ukraine rather than performing indiscriminate attacks as WannaCry did. [6]

1.3 Iron Cybercrime Group

In 2015, a notorious cyber-arms dealer known as HackingTeam was breached, leaking its wares online for anyone to copy. Recently, a sophisticated Chinese cybercrime group has made use of the old, leaked computer code in order to breach thousands of companies, mostly based in Asia. The Israel cybersecurity firm Intezer dubbed the group as the "Iron Cybercrime Group". The group has made use of ransomware, among other malware, to carry out their attacks. [1]

2 To the Community

Before we begin discussing and comparing the various characteristics of ransomware attacks and hacker groups, a few points should be addressed, namely, why I chose to write on this topic, and why you should even care.

2.1 Why did I choose this topic?

Initially, I wasn't planning on writing about how ransomware characteristics varied based on the country they originated from or the hacking groups behind them. The topic I originally chose was

ransomware as a whole. In other words, I was only planning to write about the workings behind ransomware and how to defend against it – Admittedly, a pretty uninteresting topic. The reason I chose to write about ransomware was due to one simple fact: I like money. Due to this fact, I found it very intriguing that hacking groups could coerce people to pay them by holding their files for ransom. Of course, I would never condone their actions, but I have to admit that it's pretty interesting.

Now, the reason why I narrowed down this paper to discussing the characteristics of different ransomware attacks was so that people would actually be interested in reading it. After discussing the topic of this paper with Ming Chow, a computer science lecturer at Tufts University, we determined that a paper covering ransomware as a whole would be too broad and uninteresting. Since I wanted to keep the topic on ransomware, we decided that a paper discussing the characteristics of ransomware based on its origin would be an interesting topic to write about.

2.2 Why should you care?

We are currently in a period of time in which attacks being carried out with ransomware, among other malware, is commonplace. During such a time, it is important for us to be knowledgeable on the attacks that may be carried out against us. Obviously, knowing how to protect yourself from these ransomware attacks is important. Not as obvious, however, is the importance of knowing the characteristics of ransomware attacks. The characteristics of ransomware attacks can tell us several things about the attackers and even where the attack originated from. Later in this paper we'll even discuss how the characteristics of ransomware can help in attributing attacks to certain groups or people.

3 Discussion of Ransomware Characteristics

The ransomware attacks and hacking groups previously mentioned all originate from different countries around the world. Due to the variance of their origins, these ransomware attacks adopt different characteristics and behavior. Here we'll explore some of what those characteristics are.

3.1 North Korean Ransomware

The United States, United Kingdom, and Australia all came to the conclusion that North Korea was responsible for the WannaCry ransomware attack in May 2017. [3] The attack was confidently attributed to North Korea due to it having certain characteristics.

On the last day of the attack's occurrence, there were already similarities found between WannaCry and other North Korean malware. Researchers found that WannaCry ransomware shared code with malware written by the Lazarus Group, a group of North Korean hackers. Neel Mehta, a security researcher at Google, was the first to point out the shared code. Cybersecurity firms Symantec and Kaspersky also found instances of code that overlapped between WannaCry and malware written by the Lazarus Group. [7]

The coding and implementation mistakes made by the WannaCry developers gives us some more insight into North Korean ransomware characteristics. After analyzing both the malware and the leaked NSA EternalBlue exploit used to spread the attack, malware expert Jake Williams stated that there are "mind-blowing mistakes" in the ransomware code. Among the mistakes that Williams found was the use of only three Bitcoin addresses for remittance; these types of attacks

usually have addresses for each infection to correlate payments to victims. Williams explains that this mistake makes it simple for law enforcement and security researchers to track the transactions, thus making the $140,000 in Bitcoin that was collected completely meaningless. Another mistake Williams mentioned was the killswitch that was instrumental in putting a premature halt to the attack. Williams stated that normally the killswitch wouldn't be so easily found and expected there to be some sort of cryptographic challenge-response in place. [5]

Williams argues that the WannaCry developers failed to properly contain it and the Eternal Blue exploit before it was ready to be released. He came to this conclusion due to North Korean malware authors being well aware of the types of errors that were in the WannaCry code. The lack of cryptographically validated connections to command and control is what makes Williams especially certain that WannaCry was never intended to be released as it was. [5] The fact that it was released despite this is what gives us some insight into the characteristics of ransomware from North Korea. Williams believes that the cause of its premature release was that "the North Koreans don't have a lot of experience with very virulent, worming malware". [5]

3.2 Russian Ransomware

Based on research conducted by the Czech cybersecurity firm ESET, a hacking group with suspected ties to Russia and a history of releasing computer viruses is the main suspect behind the NotPetya ransomware attack. ESET has attributed the attack to a hacking group known as Telebots or Sandworm. [2]

As stated in Section 1.2, NotPetya was mainly directed against businesses in Ukraine rather than an indiscriminate attack like WannaCry. [6] NotPetya follows a pattern of hackers using wiper malware and defunct ransomware (code designed to either lock or destroy data) against targets in Ukraine. Researchers attributed some of these attacks against targets in Ukraine to Telebots. [2] This creates a common link between the NotPetya ransomware attack and the Russian hacking group Telebots.

Further linking NotPetya to Telebots, analysts found that the ransomware contained code that aligned with the tactics, techniques and procedures of the Russian hacking group. For instance, Telebots launched a ransomware attack in 2016 that did not give victims a way to pay off the hackers. Also included in the attack was KillDisk malware to destroy files. Rather than making money, Telebots was more concerned with spreading their malware. In the NotPetya incident, the malware provided a ransom note that demanded a massive payment of $250,000 in bitcoin to unlock each computer. Researchers concluded that the unreasonable payment indicated that the hackers' intent was not financial; this aligns with methods used by Telebots. The hackers' goals being unrelated to finance is further shown by how NotPetya would wipe a victim's data before they even had a chance to communicate with attackers. [2]

Researchers also warmed up to the idea that the Russian government may have had a hand in the NotPetya attack. They believe that the non-monetary goals of the attack may indicate that the government was responsible. [2]

3.3 Chinese Ransomware

As stated in Section 1.3, the Iron Cybercrime Group is making use of old, leaked computer code from the cyber-arms dealer HackingTeam to breach thousands of companies using ransomware along with other malware. [1] While the ransomware attacks carried out by this group aren't nearly

as infamous as WannaCry or NotPetya, they still have their share of characteristics that make them unique.

Ari Eitan, the head of research with Intezer, stated that "This is likely an advanced Chinese criminal group" in regard to the attacks. Eitan came to this conclusion due to it being a rarity for people to use the old HackingTeam code since it's not a simple copy and paste. He further explains that there is other source code that is easier to adopt, meaning that these current attacks are a big operation with tools written recently. [1]

Interestingly, the attacks carried out by the Iron Cybercrime Group shows how hacking groups based in China develop their malware to specifically evade well-known domestic anti-virus products. According to Intezer, the ransomware (and other malware) variants attributed to the Iron Cybercrime Croup were all designed to avoid Chinese cybersecurity firm Qihoo 360's anti-virus engine. If the malware detected Qihoo, then the final payload would not be installed on the targeted computer. [1]

4 Defenses

While ransomware attacks may have various characteristics that depend on its origin, the steps that you should take to protect yourself are not as varied. The main thing you should do to protect yourself is to verify that your device's software is up to date. Software updates usually have patches that remove bugs and close security loopholes, thus removing the vulnerabilities that ransomware often exploits. You can update your software by regularly using Windows Update or the Software Update feature on a Mac. If you don't want to deal with software updates regularly, you can set your devices to install those updates automatically. [4] There are a few additional things you can do to protect yourself from ransomware [4]:

- Create backups of your most important files. You can do this by storing them in a cloud-based storage service or downloading them to an external hard drive.
- Use passwords that are unique and hard-to-break. You can use a password manager to keep track of these passwords that are likely hard to remember. Experts say using unique hard-to-remember passwords is much more secure than reusing the same password across multiple sites.
- If you're concerned about your devices at work, check with your IT administrator to make sure your organization's devices are protected from the ransomware that concerns you.
- Treat unexpected emails with caution and be well-informed of phishing attacks.

5 Conclusion

We can see from the ransomware originating from the three countries discussed in this paper how important the origin of the ransomware is in determining what traits and characteristics it has. WannaCry, which originated from North Korea, shared code with malware developed by the Lazarus Group, a North Korean hacking group. [7] NotPetya, which originated from Russia, mainly targeted Ukraine businesses and had a non-monetary goal; both of these tactics align with the Russian hacking group Telebots. [2] Ransomware developed by the China-based Iron Cybercrime Group was designed to avoid Chinese anti-virus products. [1] Each of these instances of ransomware carry some traits or characteristics that indicate where the malware was developed.

Interestingly, these traits and characteristics that indicate the origin of ransomware play an instrumental role in attributing attacks to certain people or groups. Based on WannaCry sharing

code with the Lazarus group, researchers were able to link them to the attack. [7] Similarly, researchers being able to find shared tactics between the NotPetya attack and attacks committed earlier by Telebots made it possible to link the hacking group to the attack. [2] This is not to say that every ransomware attack has characteristics that allow us to attribute an attack to a certain group with one-hundred percent certainty. However, having more people be aware of the fact that ransomware often has some sort of identifying characteristic can only be beneficial in identifying the assailants behind future attacks.

6 References

[1] Bing, Chris. "Chinese Group Said to Use HackingTeam Tools to Spread Ransomware, Cryptominers." *Cyberscoop*, CyberScoop, 29 May 2018, www.cyberscoop.com/chinese-group-said-use-hackingteam-tools-spread-ransomware-cryptominers/?category_news=news.

[2] Bing, Chris. "Early Indications Point to Russian Hacking Group for Petya Attack." *Cyberscoop*, CyberScoop, 30 June 2017, www.cyberscoop.com/petya-expetr-sandworm-eset-ukraine-ransomware/.

[3] Bossert, Thomas P. "It's Official: North Korea Is Behind WannaCry." *The Wall Street Journal*, Dow Jones & Company, 19 Dec. 2017, www.wsj.com/articles/its-official-north-korea-is-behind-wannacry-1513642537.

[4] Fung, Brian. "How to Protect Yourself from the Global Ransomware Attack." *The Washington Post*, WP Company, 15 May 2017, www.washingtonpost.com/news/the-switch/wp/2017/05/15/how-to-protect-yourself-from-the-global-ransomware-attack/?utm_term=.43845b9a3c29.

[5] Mimoso, Michael. "Someone Failed to Contain WannaCry." *The First Stop for Security News | Threatpost*, 16 June 2017, 1:45 pm, threatpost.com/someone-failed-to-contain-wannacry/126335/.

[6] O'Brien, Dick. "Internet Security Threat Report Ransomware 2017." *Symantec*, 16 Aug. 2017, www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf.

[7] O'Neill, Patrick Howell, and Chris Bing. "Researchers: WannaCry Ransomware Shares Code with North Korean Malware." *Cyberscoop*, CyberScoop, 15 May 2017, www.cyberscoop.com/wannacry-ransomware-north-korea-lazarus-group/.