THE NOTPETYA CASE

Attack against Ukraine on 27th of June 2017

Team GAIT

ELEC-E7470 - Cybersecurity P

Contents

Introduction

In this case study we investigate the 2017 cyber attack targeted at Ukrainian businesses. It has been called one of the most devastating cyber attacks in history and caused an estimated 10 billion USD in damage to not only Ukrainian businesses but foreign companies as well.

Apart from the huge damage caused by the attack, another reason why we found this case interesting is its hybrid nature. It is a good example of hybrid warfare, which means a combination of conventional and unconventional forms of warfare, such as cyberwarfare, and by being a new phenomenon it came with a fair bit of interesting responses from the public.

Definitions

Cybersecurity is a complicated topic with a lot of its own terminology. In order to make the study easier to understand we will go through a few of the important lingo in detail and define them.

First off, we have ransomware, which is a word you'll hear a lot in this study. It can be defined as software which demands a ransom from the victim. There are several ways used by ransomware to encourage the users to pay the ransom, ranging from making the victim's data unavailable by encrypting their storage drives to accusing the victim of the possession of socially unacceptable content. Our case study is closer related to hard drive encryption, as will be explained later.

We touched on the word hybrid warfare in the introduction, but as it is a complicated concept, we would like to give some examples in order to give a concrete image of what it involves.

In recent years influencing the internal politics of foreign states has become a common example of hybrid warfare/hybrid threats. For example, strong evidence suggests that the US presidential elections were influenced by the Russian government. Similar cases have been discovered in other countries as well.

Other examples of hybrid warfare would be the GPS jamming case in military practises in Lapland in 2018, or the damaging of Ukrainian artillery via an infected Android application between 2014 and 2016. Both cases are also suspected to have been enacted by the Russian government.

The NotPetya attack

The attack started off by spreading the ransomware used to execute the attack to the victims' computers. This was done via a software called M.E.Doc, which most businesses in Ukraine were required to use for tax filing purposes by the Ukrainian government. The ransomware was sent to the victims' disguised as an update to the popular M.E.Doc program.

At first the ransomware was not activated by the attackers, meaning it was installed on the victims' computers, but was not given the order to execute the attack. The ransomware could spread laterally in networks from the infected computers, allowing it to infect an even larger number of computers.

Not only were computers in Ukrainian businesses infected, but a significant amount of the computers of companies with branches or offices in Ukraine were also infected. About 20% of the infected computers were not Ukrainian. About 9% of the total infected computers were in Germany, which was affected the worst after Ukraine by the attack. Most notably global logistics company Maersk was reported to have suffered tremendous losses.[4]

After enough computers had been infected, an order to activate the software was sent out to the software by the attackers. The ransomware proceeded to restart the infected computer and encrypt the storage drives which was then followed by a message on the computer's screen informing the user of the encryption and demanding a payment of approximately 300€ in Bitcoin for the user to regain access to their computer.

However, unlike previous ransomware cases, paying the ransom did not allow the user to regain access to their computer, as the ransomware was never intended to decrypt the encrypted storage drives. This means the ransomware caused permanent damage to the victims in the form of computers rendered useless and data which could not be restored.

Due to the unconventional nature of the ransomware total ransoms paid have been estimated to be around 10 000 USD while total damage suffered has been estimated to have cost approximately 10 billion USD in the form of lost data, revenue etc. The timing of the attack was also a key factor in racking up the cost: by starting the attack on the eve of Ukraine's Independence Day, the attackers ensured that most offices were void of employees who could prevent the ransomware from fulfilling its purpose.

Technical aspects of the attack

The NotPetya attack is a combination of old techniques used in earlier cyber attacks. It is described as a more sophisticated version of old techniques as it combines multiple lateral movement techniques and shares similar codes with the ransomware attack Petya in 2016, therefore the name of the attack. NotPetya also shares code with open-source application Mimikatz, which can steal credentials and escalate privileges and was created in 2011 to prove that Microsoft were vulnerable to attacks, and ransomware attack WannaCrypt, which was a worldwide cyberattack in May 2017.[1, 2]

There is evidence that the attack started from a software called M.E.Doc, which was used widely in Ukraine, because it was demanded by the Ukrainian government to fill tax reports with it. The attackers first hijacked the M.E.Doc update servers. They gathered information from the servers and created a false update patch, which would be then distributed to all computers using the M.E.Doc software.

On June 27, 2017 the attackers decided to launch the attack by sending out an update from the M.E.Doc update servers for all the M.E.Doc users. For users it should as a regular software update, but it didn't contain update for the M.E.Doc software, but the attacker's malware software. As the users downloaded and installed the fake update, the malware got installed to their computer. The malware started executing in the background unnoticeable for the user.

The malware started to intercept passwords and capture administrative privileges with a credential dumping tool like Mimikatz. As it found the needed credentials it started to encrypt all the files on all drivers on the computer. When the encryption was done going on it set a timer of 10 minutes to reboot the computer and gain full control of it. As the timer started, the malware presented a fake message on the screen stating that there has been an error with the C-drive and users shouldn't turn off the computer. This message was shown until the timer ran out and the computer rebooted itself. As the computer turn back on, a ransom note appeared on the screen of the computer. The ransom note stated that all the user's files have been encrypted and if they don't pay a ransom of 300 USD in Bitcoins, they won't get their files back.

Differing from normal ransomware attacks, this malware was never designed to decrypt the user's files. If the malware got administrative privileges to the computer it overwrote all the encrypted files, making it impossible to recover any files that were affected. Even if the malware didn't have administrative privileges and it couldn't overwrite the files, the encryption keys were not provided for the people who paid the ransom. The attack was designed to cause as much damage as possible, not to make money out of taking users files as a hostage.

As the malware got control of the computer it deleted the logs of System, Setup, Security and Application events to ensure that it would be hard to override.
What made the attack so sophisticated and devastating was its ability move laterally in the networks. It had worm like capabilities and as mentioned before used multiple techniques infect as many computers on the network as possible. This meant that only one computer infected was needed to infect the whole network.

The first way that the malware tried to infect the network was by stealing network credentials or re-using existing active sessions in the network. This way it could scan the network for all the computers that the one infected computer was connected to. After scanning and finding other computers, it used normal file-share ways to send the malicious file to other computers. As the file was transferred to other computers, the malware then tried to execute the malicious file remotely on the other computers.

If it succeeded, it started the process described above on the other computers on the network, spreading even more rapidly.

The other way that the malware tried to infect the network was by using existing legitimate functionalities to execute the payload on the other computers or to abuse server message block (SMB) vulnerabilities. These vulnerabilities were also well known from earlier attack and are called EternalBlue and EternalRomance. The EternalBlue vulnerability was used for instance in the WannaCrypt attack just a month earlier.[3]

The NotPetya attack combined old techniques from earlier attacks and known vulnerabilities to gain access to users' files and spread itself like a worm infecting whole networks with the malware. Therefore, it is called sophisticated and devastating version of ransomware.

Target and motivation of the attack

Hybrid warfare against Ukraine

The NotPetya attack is believed to be part of Russian hybrid warfare against Ukraine. After the Russia's annexation of Crimea in 2014, the relationship between Russia and Ukraine have been cold. There are evidence of Russian Federation backing up fighters against the Ukrainian government in Crimea.

Ukraine is believed to be the main target of this cyber attack. There are number of evidences pointing to that statement. Of all the infected computers, 80% of them were in Ukraine. Also, the software M.E.Doc, which was used to carry out this attack is widely used in Ukraine as a tax filing software. This indicates that the attack was not a ransomware but designed to cause maximum destruction and disruption in Ukraine, and it spread unintentionally to other countries[5]. Few experts believe that the outbreak was directed against businesses and government in Ukraine, and the attackers underestimated the spreading capabilities of the malware[4].

The attack came on the eve of Ukrainian public holiday, the Constitution Day, which means that most government and business offices where empty at the time. This seems odd for a ransomware, which needs humans to see the ransom note and pay to get their files decrypted. What was even more odd for a ransomware, was that the malware overwrote and destroyed important files and drives, despite showing a ransom note ensuring the user that they could get their files back safely and easily. This indicates that the malware wasn't designed for monetary purposes but to cripple the Ukrainian state. The ransomware made only 10 000 USD out of the payments of users but is estimated to cause over 10 Billion USD worth of damage.

The malware also had an ability to identify specific computer systems and bypass infection of those systems. This is believed to be a sign of more surgical goal than just making money. Security experts also found a backdoor in the M.E.Doc update system which is believed to be installed as early as April 2017, over two months before the attack. The backdoor installation timing indicates clearly a well-planned and well-executed operation behind the NotPetya attack. Because of the large file size of the NotPetya malware, 1,5 gigabytes, it is also believed that there might be other backdoors that haven't been founded yet.

Data has been found showing that this is not the first attack by the same perpetrators. It is believed that either Telebots, BlackEnergy or Sandworm, all claimed to be backed up by the Russian Federation, is behind this attack. Traces have led to the conclusion that whoever was behind the NotPetya attack, was also behind the attack in December 2016 which was targeted against Ukrainian financial system. The traces lead also to the Petya attack being by the same perpetrators. US and UK have also claimed that Russia is behind this attack and that the Russian Main Intelligence Directorate designed NotPetya. Russia have denied all accusations, stating that Russian systems were also impacted by the attack.

Despite denying responsibility for the attack, the Russian Federation also has some clear interests in carrying out an attack. In addition to paralysing and causing damage to Ukraine, the attack could have served as a demonstration of Russia's power in the cyber domain. A demonstration of power like this could be used as a deterrent against cyber attacks planned against the Russian Federation. In this case denying the attack was merely a formality, and intentionally left people with a strong feeling that the Russian Federation was behind the attack.

Lastly a point to support that NotPetya was a hybrid warfare attack against Ukraine is that a Ukrainian intelligence officer responsible of special forces was assassinated in the morning of the attack. He was killed by a car bomb in Kiev.[4]

Alternative theory

As no concrete evidence have been found to tie Russian Federation or certain hacker group to the attack, it has been proposed that the attack was just a ransomware with monetary goals. It is believed that it's the fault of the Intellect Service company, the company behind M.E.Doc accounting software. They had been warned multiple times of their lax security measures on their servers. The company had dismissed these warnings and consequently made it possible to infect computers through their servers.

Effects of the attack

The NotPetya attack has been called the most destructive and costly cyber attack in the history to that date. What started from Ukraine, spread for five days around the world infecting computers in the USA, Europe and Asia, before the actual attack was launched crippling more than 200 000 computers worldwide. The estimated damage of the whole attack is more than 10 billion USD.[13] To put the attack in scale, WannaCry attack, just a month before the NotPetya attack, affected worldwide and is estimated to have caused damages from 4 to 8 billion USD.[16]

Ukraine

As Ukraine was the main target of the attack, it was hit the hardest. The National Police of Ukraine was contacted by 1 500 legal entities and individuals reporting that they have been affected by the attack. More than 300 companies were hit and 10 % of all computers in Ukraine were estimated to be infected. Vital functions in the society seemed to be the primary targets of the attack. “The government was dead”, said Ukrainian minister of infrastructure.[16] Multiple ministries, central bank, state postal service and electricity companies were infected, and their computers went offline. The electricity companies though managed to continue operations fully without computers. One of the biggest banks in Ukraine Oshchadbank had to close all its over 3 000 physical branches and regained full functionality not until 3rd of July, almost a week after the attack. Over 90 % of their computers were infected by the malware. Because of the hit on central bank and most banks in Ukraine, all the ATMs were don’t for the day and no draws could be made. The metro system was also partially down as card payments didn’t work, but they still managed to keep the traffic going.

Most facilities and companies that were infected couldn’t use their computers or smartphones, which meant that many of them resolved to use pen and paper as a backup. Chernobyl nuclear plant reported that they had to monitor radiation levels manually as they are ordinary done by computers. The Health ministry said that the attack took them back 30 years. They do central monitoring of drugs and it coordinate reallocation of them to hospitals that in need. This everyday task is usually done by one email to all 24 regions, but now they had to call the 24 regions by phone to reallocate one shipment.[14]

Rest of the world

Although 80% of the infected computers were in Ukraine, the attack was still a global incident. Most of the companies outside Ukraine that were affected had branches in Ukraine, which gave the malware a steppingstone to spread outside Ukrainian borders. There were also few cases of companies that used the M.E.Doc software and weren’t in Ukraine but were still hit by the attack. There are reports that over a dozen countries, including Spain, India, Russia, Israel, Germany, the US and the UK, were infected by the malware.[15]

Maersk is the world’s largest shipping conglomerate situated in Copenhagen, Denmark. It represents close to fifth of the entire world’s shipping capacity and was one of the major victims in the attack. Maersk had installed the M.E.Doc software on a single computer in a single port, but that was enough for the malware to spread through the whole company. 17 out of 76 of Maersk terminals had to be shutdown. This meant that tens of thousands of trucks were turned away on the gates. Luckily the ships computers were not infected, but without terminal software they were handicapped to do their job. It took Maersk almost two weeks to get their IT infrastructure back and running, and they reported over 300 million USD losses in revenues.[16]

Other big non-Ukrainian companies that were hit were pharmaceutical giant Merck, FedEx European operator TNT Express, French construction company Saint-Gobain, food producer Mondelez and manufacturer Reckitt Benckiser. All these companies reported nine-figure costs because of the attack. Even Russian state oil company Rosneft was hit by the NotPetya attack.

Responses to the attack

As we have mentioned previously, the effect of the attack was large and widespread. Affecting multiple companies and causing financial damage worth billions of dollars. It is then appropriate to investigate how did different actors respond when noticing they were under attack. We will therefore go through what reactions we have found in our research from as Ukrainian government, Maersk and Microsoft.

Ukrainian government

Shortly after the cyber attack the Ukrainian government issued a statement where they acknowledged that state institutions, financial institutions, power, private and transport sectors had all been affected. They were quick to place the blame on Russia without having any concrete evidence. In their statement they said that the attack was a “task-oriented destabilization of social and political situation in the country” and that “the virus is a cover of large-scale attack, oriented against Ukraine”. The Russian were quick to dismiss these allegations. Additionally, the Ukrainians mentioned suspicions against North Korea, but these were quickly dismissed as irrelevant. Later the government issued the M.E.Doc update servers to be seized by the police. This they hoped would put a stop to the further spreading of the virus. They had been able to prove that one of the employee’s computer demonstrated malicious activity. The security service of Ukraine also “published updated guidelines on protection of computers from virus-extorter attack”.[10,11]

It is also noteworthy that the United States and Britain formally blamed Russia for the attack.

Maersk

On June 27, 2017 people holding their laptops started to gather around the Maersk IT help desk. The computer screens contained red and black text instructing the owner not to turn off their computer due to a file system repairment. Other people’s computers were already fully infected and contained the following text: “oops, your important files are encrypted”. Suddenly all computers in the office started to go black in quick succession. Panic quickly ensued and employees began advising others to keep their computers turned off. After two hours Maersk’s whole global network was shut down. All employees were now advised to shut down their computers and leave them by their desk along with their now useless digital phones. Most employees now simply left their stations due to being incapable of doing anything else. The company quickly after continued operations without IT tools and managed to rebuild their IT infrastructure in 10 days. Finally, through what they described as the whole company coming together, they were able to recover. Lewis Woodcock, head of cybersecurity compliance commented that NotPetya served as a wake-up call and emphasized that a data recovery plan must always be in place. So, it seems that in this company’s case, although millions of dollars were lost, they learned from their mistake and realized that even if you are not the target of a cyber attack, you could still be the victim.[8,9]

Microsoft

Microsoft being the owner and developer of Windows, the operating system that contained those security holes that made the attack possible, immediately began investigating the attack. They wanted to help their customers by releasing “cloud-delivered protection updates” and releasing updates to their definition packages. They also made a blog post on their website with details of the characteristics of the malware.[14]

What should have been done?

What was particularly unfortunate in this attack was the fact that the exploits used to spread the malware were already known by the cyber security community. Additionally, Petya, a separate but very similar attack, had only recently been dealt with and was fresh on people's minds. It is therefore odd that better measures had not been taken to prevent these types of attacks from happening. In this chapter we wish to discuss those things that should have been done before, during and after the attack.

Before attack

Before the initial spread of NotPetya there was the similar Petya malware attack. This malware, similarly, to NotPetya encrypted the file system and requested a ransom in the form of bitcoins. Seemingly very little action was taken to prevent this type of attack from happening again. Additionally, the M.E.Doc update servers were also previously breached to spread a different kind of attack, and yet still, NotPetya happened in the large scale that it did. Not only had there been a similar malware attack before NotPetya but also the same backdoor breach in the M.E.Doc update servers had been used previously by other assailants. The backdoor exploit was used not only once but three times and left without update since 2013, an extremely irresponsible lack of action by Intellect Service.[6]

First, fully securing and auditing the update servers should have been the topmost priority after the very first backdoor breach. Secondly, the Petya Microsoft patch had been available since March 2017. This patch fixes the SMB flaw exploited by EternalBlue that NotPetya was using to spread inside the networks. Lastly, companies should have been using the most recent operating systems. Most of the infected computers had been using an older version of Windows when Windows 10 was fully capable of deflecting this attack.

During the attack

The initial reaction during the attack was to keep computers offline. A reasonable and correct response in such a situation. First, the user could have checked for a file called “rundll32.exe” running in task manager. If this executable existed, it meant that your computer was infected by the malware and would upon restarts encrypt all your data. So, computers should be kept offline and on hold until the user gets more detailed information on what is happening and how to stop it. Interestingly, some sites were saved completely from the attack due to power outages. Security experts were then able to get their hands-on computers that were already infected but not activated and were able to research the virus that way. Companies then should have informed local authorities and work together to prevent further damage. Going into even more detail, there was also a possibility to ‘trick’ the malware into thinking it was already installed on the computer. The user could create a read only file called perfc and position it in the windows directory. This is the file that the malware looks for when it first runs, and if found will kill itself.[7]

After the attack

Actions that should be taken after the attack are like the ones that should have been taken before it. Secure the update servers, update company computers containing the latest patches and start employee briefing. It is extremely important that as many people as possible are “cyber aware”. Meaning that they should be able to identify suspicious emails and know about best practices when it comes to deterring digital threats. Most importantly, companies should backup their data, so in case of a breach, they could at least partially recover. Also, companies should use reputable security suites that systematically check their file systems for malicious files.

Conclusions

Overall this case has several points we can all learn from. Some of the more obvious ones where improvements should’ve been made were for example the lax security measures taken at the company developing M.E.Doc: they had already suffered an attack using almost the same method (software update servers) yet failed to fix this glaring flaw. We would like to point out some more broader lessons learned from this case.

One of the more important things to realize is the fact that cyber threats keep on evolving. As we saw with this case it combined old tricks, known tricks to produce damage of a completely different scale. It was designed to look like ransomware but act like a weapon of destruction. Preparing for every kind of attack is virtually impossible, however we can anticipate an attack, and be ready to respond correctly.

This leads to our second point: you can suffer great damage from an attack not targeted at you. Maersk’s case is a prime example of this, and it emphasizes the importance of cybersecurity in any business and being prepared accordingly.

On the topic of preparedness, this case proves as an example of where a single weak link can cause tremendous damage. In this case there were several weak links but disabling any one of them could’ve saved millions. For example, keeping the computers updated on the newest security patches alone could’ve saved Maersk from a lot of damage despite there being other weak links in the forms of the M.E.Doc’s lax security.

However, keeping systems up to date is only one of several concrete measures we can take to prevent or minimize damage caused by a potential cyber attack. We would like to end this conclusion with a picked couple of measures especially with businesses and organizations in mind, though they can be applied to anyone.

One good way of preparing for a cyber attack is regularly backing up your data to a cold storage. By cold storage we are referring to a form of storage which is not connected to larger networks. In a case where your computer’s data gets wiped by an attack, you will have most of your data still available. This helps with recovering from an attack, hence minimizing the downtime and losses in revenue in a case where a business or government is the victim of an attack.

Most importantly though, is to focus on improving the weakest link in cybersecurity: humans. In most cases the source of an attack is simply a link in an email sent from a source disguised as something else. By educating people on cybersecurity and improving their know-how, we can significantly reduce the risk of a cyber attack taking place and become better at responding to attacks.

References

1. https://www.varonis.com/blog/what-is-mimikatz/
2. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
3. https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
4. https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine
5. https://www.apnews.com/ce7a8aca506742ab8e8873e7f9f229c2
6. https://www.bleepingcomputer.com/news/security/m-e-doc-software-was-backdoored-3-times-servers-left-without-updates-since-2013/
7. https://www.forbes.com/sites/thomasbrewster/2017/06/28/three-things-you-can-do-to-stop-notpetya-ransomware-wrecking-your-pc/#60264f2f77b0
8. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
9. https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/
10. https://ssu.gov.ua/en/news/1/category/21/view/3660#.C2HJKnpy.dpbs
11. https://www.csoonline.com/article/3205252/ukrainian-police-seize-computers-that-spread-global-notpetya-attack.html
12. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html
13. https://www.cnet.com/news/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/
14. https://www.microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/
15. https://help4it.co.uk/notpetya-goldeneye-ransomware-attack/
16. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/