Cyber warfare

The changing landscape

As we look back to understand where everything starts to escalate, let's take a peak into the beginning. The largest cyber incident of its time and the point where the cyber world begins to be used in the world of warfare. Setting the stage in summer of 2017, the Russian government launches an attack against Ukraine. What is unknown is if they realize the extent and reach the attack would take on the world. Now known as notpetya, the attack used a known attack type, the Petya malware and leveraging the mimikatz open-source software and the NSA EternalBlue exploit to spread, the attack reached global impact and will wind up costing billions in recovery.

Let's look at how this all started. Beginning with the Petya malware strain. The malware was developed as a form of ransomware. The first known use of the encryption malware comes around in March of 2016. This has been identified as the next progression in ransomware. Initially spread through Email attachments, the malware encrypted victim machines. The process starts with infecting the MBR and forcing a reboot. After the system turns back on, the NTFS master file system becomes encrypted. After encryption, a ransom's note is displayed instructing the victim on how to pay the ransom. Threat actors use this method for financial gain at this point and because the attack vector targets the MBR and NTFS, it can have Devastating effects.

Also emerging in 2016, let's introduce the shadow brokers. A hacking group that is responsible for releasing the toolset used by the NSA in 2017. Up to this point, most countries that work in the intelligence community are at the whims of tools that they are able to purchase. There are not many nation states or groups with the capabilities that the NSA have. As we take a look into this, the importance of the EternalBlue will have in the forth coming attack cannot be understated. Although this is just one in an entire toolset of things released by the shadow brokers, this one will go down in history for the part it will play.

The last piece of the puzzle lays with the open-source tool created by Benjamin Delpy in 2007. The security research developed the tool as a proof of concept to point out the weaknesses in how windows stores account and password information. While the tool was created without malicious intent, the impact of implementation can only be described as devastating. With four main functions, extracting passwords, bypassing MFA, escalating privileges and moving laterally, the tool continues to be a big part of many red team and penetration testers toolkits. It has continued to provide updates and is still in use as of the writing of this article.

Now that we know the pieces of the puzzle that where put together to form the largest, most devastating attack, we will dive into how it took place. By targeting a Ukrainian accounting softwares server, the attack begins. While it may seem benign, the planning and execution will go flawlessly. By chaining the three tools together, systems throughout Ukraine begin to feel the affects. Starting of with a few computers, workers begin the day with slight concern as computers begin to boot up encrypted. Unfortunately for Ukraine, and some to be many, many more countries, the encryption and ransom are not the end goal of the attack. Spreading from banks to grocery stores to gas stations, more and more companies are impacted. As the virus moves from company to company, industry to industry the panic is just beginning.

As IT teams around the country work tirelessly to try and isolate and mitigate the damage, this is only the beginning. For context, let’s think of it like this, imagine the most stressful and busy day possible and you finally get to the point where you need to just leave and collect yourself. You head from your office and get to the train you ride everyday to and from work and the RFId card you use to pay for it is not scanning to get you on the train. You try and your try with no success. Since you are already so stressed because of the day you had, you head to the ATM to get cash to pay for the ticket directly only to find the first ATM is down. Walking to the next and that too is down. After looking all over and spending an excess amount of time, you finally find an ATM that is still working. Unfortunately, there is a line of 20 people. Since you have already spent time just trying to find the ATM, you wait your turn and see the limit that has been put on withdrawals. After hours spent just trying to find a way to pay to get onto the train, you have finally made it. You are inching closer to home and the relief of ending the day.

As you arrive home, you look in the kitchen to get sustenance and a nice glass of wine to unwind from the day you have survived. The fridge is empty of all but a bottle of ketchup. The cabinet is bare. Your wine bottle is empty. A frustration but the market is just on the corner. As you arrive to the store, you are met with locked doors and signs stating that all of the computers are down and they are only accepting cash payments. Your journey to find an ATM is back on. Making your rounds to all of the banks and ATMs in the area, you finally found one and yet again are met with a severely limited withdrawal amount.

While this would be terrible if it was limited to a town or city, just imagine the caps this would cause with the affects spanning an entire country. This is the just the beginning of the notpetya attack. From the first signs of the infection at the beginning of the day on June 27th, 2017 till June 28th, more than 2000 companies will become infected. Although the attack was meant to target Ukraine, any company that does business in the country and uses the MeDoc accounting software will be affected. Not long after the attack takes place, companies start to realize that this is not the normal ransomware attack and that the affected systems will be unrecoverable.

Now that we see the devastation to the everyday activities and normal life, let’s look at one of the larger impacted companies, Merck. Holding the title as the worlds largest shipping and receiving company for multiple decades and spanning ports across the world. Since the impact is spread from machine to machine, anything that is connected will become a target. Looking at how systems are administered, many have multiple domain controllers that accomplish convergence by replicating the settings and information between each other. In doing so, this creates a redundancy. If you think of it in simple terms, this is like having a spare key to your car. If you lose one, you can still drive and get to where you are going, now imagine that you have 100 spare keys. This is how Merck was setup. The notpetya attack will steal 99 of these keys at the same time. Scrambling to restore the network, the company will start to reach out to competitors and contacts, begging for help and permission to you their backend to get operations back up and going.

Since this is one of the largest shipping companies, this causes backups of trucks at ports spanning for miles. To add to this, the just-in-time manufacturing and the perishable goods will sit in ports. As we think hard about the implications of this, let’s keep in mind that this all started with a plan to target a specific country. The ports from Ukraine to turkey, New Jersey to Los Angeles are filled with goods just waiting to go out and trucks waiting to pick them up.

As we look back through the attack that started to gain an advantage in the battlefield, effects have now spread to a worldwide stage. Although the threat actors will become known after the DOJ indictments, justice may never come. Since the attackers are protected by the GRU, the US courts may never see them.

As we look back at how this started, knowing that tools where put together and a single server was targeted, the beginning of the cyber war begins. With an estimated $10 billion in damages, the notpetya attack will make history as the largest attack with the most damage.

Lessons learned

As we look back in history, we must learn from it. The attack shows the importance of patch management, vendor responsibility and physical security cannot be understated. By taking a known malware or ransomware and chaining it with an open-source tool and an NSA bug, attackers are able to target a single supply chan server with devastating consequences. Remember, it only takes one breach, and the threat actors only need to succeed once.

Thank you,

Caleb Leggett

https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware

https://en.m.wikipedia.org/wiki/Petya_(malware_family)#:~:text=Variants%20of%20Petya%20were%20first,been%20developed%20by%20the%20U.S.

https://www.hypr.com/security-encyclopedia/shadow-brokers

https://www.sentinelone.com/cybersecurity-101/mimikatz/?utm_source=gdn-paid&utm_medium=paid-display&utm_campaign=nam-pmax-brand-ppc&utm_term=&campaign_id=19502097988&ad_id=&gad_source=1

https://www.tripwire.com/state-of-security/notpetya-timeline-of-a-ransomworm