Alexander Gardner

Susan Zehra

CS 462: Cybersecurity Fundamentals

April 16, 2023

NotPetya

The theatre of war has expanded past land, sea, and air. Our entire cyberspace has become a battlefield in the new digital age. It is a war that is not seen and fought entirely in a meta-physical space, our internet. One major battle took place during the Russo-Ukrainian War that began in 2014. A Russian state-backed group named "Sandworm" set their sites on Ukraine to launch the most destructive cyberattack since the invention of the internet that would go on to cost the world an estimated $10 billion, NotPetya. (Wolff 2021). The attack began on the Constitution Day in Ukraine, "a Ukrainian public holiday commemorating the signing of the post-Soviet Ukrainian constitution." (Shepherd 2019). This not only served a political purpose, but also a strategic purpose. Everyone would be at home celebrating the holiday and be completely unprepared to defend against the most devastating cyber-attack known to mankind.

This attack created by the Russian "Sandworms" by combining two exploits: EternalBlue and Mimikatz. (Greenberg 2018). EternalBlue is a penetration tool that was allegedly created by the United States' National Security Agency which got leaked in a breach of the agency's files in 2017. (Greenberg 2018). EternalBlue takes advantage of Windows systems that use SMBv1 (Server Message Block version 1) file-sharing protocol. (Burdova 2020). SBMv1 was first developed in 1983 as a network communication protocol which enabled shared access to files, printers, or ports which allowed Windows machines to talk to each other for remote services

(Burdova 2020). EternalBlue takes advantage of this by sending a malicious packet to the target server to activate worm-like malware. (Burdova 2020). The next tool used by the Sandworm group is Mimikatz. This was used to gain unauthorized access to networks, systems, and other applications to gain access to sensitive information. Mimikatz takes advantage of Windows Systems by exploiting WDigest. "Prior to 2013, Windows loaded encrypted passwords into memory, as well as the decryption key for said passwords. Mimikatz simplified the process of extracting these pairs form memory, revealing their credential sets." (SentinelOne n.d.).

NotPetya began its pandemic like spread by compromising a popular Ukrainian tax software named M.E.Doc. This software is widely used amongst businesses and Sandworm just so happened to create a backdoor in an update that had been present for up to six weeks before the attacks to place. Once installed NotPetya used EternalBlue to penetrate the system that had not been patched, and then used Mimikatz to find the passwords to the computers that had been patched. This not only caused the malware to spread rapidly amongst Ukrainian businesses, but it also caused collateral damage to innocent bystanders like "hospitals in Pennsylvania to a chocolate factory in Tasmania." (Greenberg 2018). Once NotPetya had successfully infected its victims it displays a screen with a message: "Oops, your important files are encrypted." Then it follows this with a request for $300 worth of bitcoin to get your information back, but Sandworm created this malware so that the encryption was irreversible. NotPetya irreversibly encrypted master boot record and did not create a decryption key.

The aftermath of the Notpetya attack was disastrous. The total damages following the attack are estimated to be $10 billion. Some of the victims were large, multinational enterprises they "suffered staggering losses: $870 million lost to pharmaceutical giant Merck, $188 million to maker of Cadbury chocolate Mondelez ($188 million), and $400 million to FedEx's European subsidiary TNT Express." (Hypr n.d). This attack even impacted hospitals, airports, power companies, and banks which critically endangers Ukraine's critical infrastructure.

The social impact of an attack of this magnitude is also heavy. A cyber attack on Ukraine can put their entire business sector in danger. One may question if they can trust their sensitive personal information with a Ukrainian organization. This can bring distrust to the whole system and how well they can protect critical information. Another societal impact to this attack is how important it is to report exploits and create an open as well as honest discussion about cybersecurity. I believe this entire attack could have potentially been avoided if the United States had not hidden their EternalBlue exploit which was used in the NotPetya attack. If the United States National Security Agency had communicated that they had found a critical exploit in Windows machines this could have been patched earlier. This also adds to the importance of keeping systems up to date. Another way this has impacted society is that it has shown us how vulnerable our critical infrastructure can be. This one cyber-attack shut down "four hospitals in Kiev alone, six power companies, two airports, more than 22 Ukrainian banks, ATMS, and card payment systems in retailers and transport, and practically every federal agency." (Greenberg 2018). Luckily, this attack had zero deaths, but every year more and more devices get added to the cyber space. More equipment in hospitals, more communication devices for airports, and more banking software. An attack in our future can have even more devastating effects and bring the virtual war into the physical world. This attack has only given us a glance at the societal impact this will have on the insurance industry. The Mondelez International organization is at the center of this issue. They were one of the victims of the NotPetya attack and suffered disruptions to their email systems, file access, and their logistics for an extended period of time. This caused them to suffer massive losses and led them to file an insurance claim, but their insurance does not cover losses suffered due to war (Wolf 2021). This has caused a major earth-shattering level of discourse in the cyber insurance world and businesses alike. This discourse mainly lies on what is considered cyber terrorism and cyber war. NotPetya has also shown as not take deals with terrorists. The Sandworms designed the attack to display a message requesting a fee to get your information back, but it was all a rouse, there was no way to decrypt the data. This shows us that paying these fees not only encourages future ransomware attacks, but it also funds these bad actors.

NotPetya is widely considered the most destructive cyber attacks ever. The Russian Sandworms launched a cyber attack that has been compared to a nuclear bomb on the world. This can lead to a larger conversation about cyber security in our world today. More and more devices get connected to our cyber space every day. In 2022 there were an estimated 13.14 billion devices connected to the internet, this is an increase of 1.86 billion from 2021 (Valishery 2022). By the year 2030, there are expected to be 29.42 billion devices connected to the internet (Valihsery 2022). These internet-connected devices can also be seen everywhere from our houses, our jobs, the airports, hospitals, banks, and many more. Our world has become increasingly connected via the internet. The NotPetya attack has shown us how much damage can be brought and how quickly it can take place and spread. It took only 45 seconds for NotPetya and the Russian Sandworms to bring down the largest Ukrainian bank and only 16 seconds to fully infect a major Ukrainian transit hub. (Greenberg 2018). Our critical infrastructure is not as safe as it may seem. Our entire system and government can come to a halt in the matter of seconds. This may seem scary, but the first step to preventing attacks begins with us. Cybersecurity is a surprisingly human-centric field. An estimated 82% of cyberattacks are due to human error (Irwin 2022). The first line of defense in the cyber war begins with us and practicing proper cyber hygiene. For example, NotPetya would not have been able to infect many devices if they had properly updated their Microsoft systems. We must also call upon our governments to have an open and honest way to discuss the cyber vulnerabilities they have found. This attack used an exploit created by the United States' National Security Agency. If we can report and work together to combat cyberwarfare the entire world will become a safer place.

References

Burdova, C. (2023, February 23). *What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?* What is EternalBlue and why is the MS17-010 exploit still relevant? Retrieved April 17, 2023, from https://www.avast.com/c-eternalblue#topic-2

Franko, J. (2022, March 5). *Notpetya: The Cyberattack that shook the world*. The Economic Times. Retrieved April 17, 2023, from https://economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-cyberattack-that-shook-the-world/articleshow/89997076.cms?from=mdr

Greenberg, A. (2018, August 22). *The untold story of notpetya, the most devastating cyberattack in history*. Wired. Retrieved April 17, 2023, from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hypr. (n.d.). *Security encyclopedia*. What is NotPetya? 5 Fast Facts. Retrieved April 17, 2023, from https://www.hypr.com/security-encyclopedia/notpetya

Irwin, L. (2022, July 1). *Human error is responsible for 82% of data breaches*. GRC eLearning Blog. Retrieved April 17, 2023, from https://www.grcelearning.com/blog/human-error-is-responsible-for-85-of-data-breaches

Shepherd, A. (2019, September 13). *What is Notpetya?* ITPro. Retrieved April 17, 2023, from https://www.itpro.com/malware/34381/what-is-notpetya

Vailshery, L. S. (2022, November 22). *IOT connected devices worldwide 2019-2030*. Statista. Retrieved April 17, 2023, from https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

What is Mimikatz? SentinelOne. (2022, December 19). Retrieved April 17, 2023, from https://www.sentinelone.com/cybersecurity-101/mimikatz/

Wolff, J. (2021, December 1). *How the notpetya attack is reshaping cyber insurance*. Brookings. Retrieved April 15, 2023, from https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/