NotPetya Cyber Breech

Omarion Branch

Department of Cybersecurity, Old Dominion University

CYSE 300: Introduction to Cybersecurity

Professor Malik A. Gladden

September 10, 2023

Overview

In June of 2017, the whole world was hit with one of the most destructive cyber attacks known. But the thing is it was only intended for Ukraine, but ended up spreading to over 60 other countries, shutting down thousands of computer systems. This attack was shutting down everything worldwide like banks, government, retail stores, trucking businesses, and many more costing more than $10 billion dollars in global damage.

The attack was preformed by a group of Russian GRU agents known as Unit 74455 or as other call them Sandworm. At first people had thought the attack was Petya because after further research they discovered it wasn't because NotPetya was not a ransomware because it couldn't be decrypted. Once the attackers seized the computers, they put up a fake $300 dollar bitcoin ransom in order for them to "unlock" the computers and give Ukraine access back into their systems but truly even if they had paid the $300, they wouldn't have been able to get anything back at all.

What were the cybersecurity vulnerabilities?

On Windows computers there's a program called Lsass.exe. This is program is responsible for the security on windows computers. When anyone logs into a computer Lsass puts their usernames and passwords in clear text into the memory of that computer. This is so it can verify you when you try to log into your email, shared devices, and many more without asking the user for their password over and over again. Now Microsoft knew that this was problem within their systems but still yet tried to fix it. They either just flat out didn't acknowledge it or just didn't fully understand how to fix it. Now how exactly did Russia gain access into this system? Easy Mimikatz and EternalBlue.

What threat(s) exploited the vulnerabilities?

The two threats the exploited the vulnerability are Mimikatz and EternalBlue. Mimikatz was created by Benjamin Delpy or as some call him Gentilkiwi. He made it to where you can access the LSASS file and see the usernames and passwords in clear text. He made this program a open source so literally anyone could use it. Thought out his time with this program he kept building it teaching it how to “trick” windows in so many ways like passing hashes and tokens. Now I know what you’re thinking “why is it dangerous if it can only show one user information?”, that’s where you’re wrong.

If you are able to get to a computer and install Mimikatz on it, then you’ll be able to see every single user that has logged into that computer since it’s been rebooted. This could give a hacker access to hundreds of employees and possibly a admin. Now EternalBlue was just like the icing on the cake once the computer was infected with the worm. EternalBlue exploited a vulnerability in windows function called Server Message Block. Server message block allows machines to share information among each other, with EternalBlue your able to run a code remotely on any windows computer in the world that was vulnerable. Now NSA tried warming Microsoft about EternalBlue when it first appeared, and a patch was made. But it’s extremely hard to get everyone around the world on the same page at the same time.

What were the repercussions of the incident?

The repercussions of the incident were devastating. The world has lost over billions of dollars as the attack did more damage than intended to. As we all know this attack was supposed to be a Russia Vs Ukraine battle but with the powerful tools used in this cyber attack it went global. This costed $10 billion dollars in damage and a incalculable damage on goods, services, and

opportunity. The world had all called out Russia for the attack, but the thing is we can't really do much to them. If we launch a Cyber-attack back on Russia that could lead to collateral damage and possibly the lost of many important files and documents. Also given the fact of how advanced Russia's technology skills are there's no telling how much damage they're fully capable off.

What cybersecurity measures could have been taken to mitigate the consequences or prevent the incident?

In my opinion I feel Microsoft should've pushed a worldwide announcement once they released the patch and knew that text were being stored in clear text. We should also educate more employees on phishing emails with deep explanations on why you shouldn't download them or follow links. It'll also be a good idea to run patch and vulnerabilities managers. And last but not least a data backup procedure should be in place daily with antivirus systems.

Reference page

Brumfield, C. (2022, June 27). *5 years after notpetya: Lessons learned*. CSO Online. https://www.csoonline.com/article/573049/5-years-after-notpetya-lessons-learned.html#:~:text=Highly%20contagious%20malware%20from%20Russia's%20GRU&text=Altogether%20the%20malware%20caused%20more,among%20other%20damaging%20cyber%20incidents.

Cooper, S. (2023, August 16). *What is Notpetya Ransomware & How to protect against it*. Comparitech. https://www.comparitech.com/net-admin/notpetya-ransomware/

Pernik, P. (2018, July 5). *Responding to "the most destructive and costly cyberattack in history."* ICDS. https://icds.ee/en/responding-to-the-most-destructive-and-costly-cyberattack-in-history/#:~:text=When%20the%20UK%20government%20attributed,Combating%20Information%20Crimes%E2%80%9D)%2C%20at

Rhysider, J. (n.d.). *Notpetya – Darknet Diaries*. NotPetya – Darknet Diaries. https://darknetdiaries.com/episode/54/

What is Notpetya? 5 fast facts: Security encyclopedia. What is NotPetya? 5 Fast Facts | Security Encyclopedia. (n.d.). https://www.hypr.com/security-encyclopedia/notpetya#:~:text=4.,Windows%20versions%3A%20EternalBlue%20and%20Mimikatz.