An Analysis of NotPetya and EternalBlue: Past Damage and Potential for Future Harm

Kelly Rudder

CPSC 610: Topics in Computer Science and Law

December 13, 2021

Abstract

This paper examines the NotPetya virus and EternalBlue vulnerability, and what they mean for the future of cyber-attacks. It describes the NotPetya attack's impact on the world before outlining the technical methods used in the attack. Next, the paper provides a technical analysis of the potential future harm. After, it looks at the current political and legal landscape surrounding cyberattacks before analyzing how this landscape could present a future risk going forward. After analysis, the paper concludes that NotPetya and EternalBlue pose an almost nonexistent technical risk, but what they reveal about the current state of law and policy surrounding cyberattacks demonstrates a danger to the world.

June 27, 2017 Cyber Attack

On June 27, 2017, devices around the world began mysteriously crashing left only with a message demanding a payment of $300 worth of bitcoin, or the computer's files would be forever encrypted and unusable.[1] The outages spread quickly, seemingly limited to a network of specific companies. Those hit experienced rapid outages and damages that affected others' day-to-day lives. Merck Pharmaceuticals, the corporation hit the hardest, had 15,000 machines infected in just 90 seconds leading to $870 million worth in damages.[2] Other notable disruptions included Maersk, the world's largest shipping firm, which experienced $300 million in damages.[3] The total estimated damages from the attack reached more than $10 billion.[4]

[1] Greenberg, Andy, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired. August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
[2] Burdova, Carly, "What is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?" Avast, June 18, 2020. https://www.avast.com/c-eternalblue#gref.
[3] Ibid.
[4] Greenberg, "Untold Story of NotPetya."

Interestingly, the damages - though widespread - seemed mainly concentrated in one country: Ukraine. While companies in other countries had been affected, Ukraine experienced widespread outages in hospitals, power companies, airports, banks, and more.[5] An estimated 10% of all computers in Ukraine were infected, disrupting everything from small businesses to larger government-run websites and leaving the country to scramble for a fix.[6]

With large-scale damages across the globe, people soon started demanding answers regarding the attack's cause. Looking at the virus, many researchers noticed its similarities to the Petya ransomware virus, so early reports attributed the attack to Petya ransomware or a variation.[7][8]

What is Ransomware?

To understand the Petya ransomware, first, understand ransomware itself. Ransomware malware prevents users from reaching their data, and in turn, asks users to make a payment to retrieve their data and regain the functionality of their infected machine.[9] Making money from rendering its victim's machine useless until payment occurs serves as ransomware's primary goal, a task that has become much easier with the use of cryptography. Newer ransomware encrypts its victim's computer, so data recoveries will only return encrypted data. This action further incentivizes victims to pay the ransom to regain their unencrypted data.[10] Ransomware, like

[5] Ibid.

[6] Ibid.

[7] Nicole Perlroth, Mark Scott, and Sheera Frenkel, “Cyberattack Hits Ukraine Then Spreads Internationally.” New York Times, June 27, 2017. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.

[8] “Windows 10 platform resilience against the Petya ransomware attack.” Microsoft, June 29, 2017. https://www.microsoft.com/security/blog/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/.

[9] Aurélien Palisse et al, “Ransomware and the Legacy Crypto API,” in *Risks and Security of Internet and Systems*. Frédéric Cuppens et al. (Roscoff, France: Springer, Cham 2016) pp. 11-28.

[10] Ibid.

other malware, typically targets regular people and spreads through methods such as malicious links online or email attachments.

Identifying the Culprit: Petya Ransomware

Petya ransomware first appeared in early 2016 spreading via email attachments containing the ransomware.[11] The ransomware was straightforward. It encrypted the device then demanded its victims pay $300 of Bitcoin to unencrypt it.[12] The similar messaging, code breakdown, and appearance of the June 27, 2017 attack led researchers to believe Petya ransomware was responsible. However, a few key differences between the attack and Petya emerged. First, the malware responsible for the attack could jump across different computers on a single network infecting them as it went along.[13] Second, the attacking malware completely wiped computers. Rather than Petya, where a key could unencrypt infected devices, the new malware affected the Master Boot Record and Master File Record leaving the computer unusable and all data destroyed.[14] This destruction meant that the virus was not ransomware at all, but rather a different type of malicious malware. Thus, researchers gave the responsible malware a new name, NotPetya, to help distinguish it from its Petya counterpart.

NotPetya: Technical Overview

The NotPetya malware's success in widespread destruction began with its seamless initial infection. Researchers found that NotPetya originated in a software update sent out by M.E.Doc,

[11] Burdova, "EternalBlue MS17-010 Still Relevant."

[12] Ibid.

[13] Kroustek, Jakub, "Things we have learned about Petna, the Petya-based malware." Avast, June 30, 2017. https://blog.avast.com/things-we-have-learned-about-petna-the-petya-based-malware?_ga=2.177441189.1440778063.1637123550-103372661.1637004001.

[14] Fayi, Sharifah, "What Petya/NotPetya Is and What Its Remediations Are," in *Information Technology – New Generations*. Shahram Latifi. (Springer, Cham 2018) pp. 93-100.

a Ukrainian accounting software similar to TurboTax.[15] Attackers successfully infiltrated M.E.Doc's update servers and issued an update of the software that contained NotPetya thereby infecting all computers which used the software.[16]

Once NotPetya gained access to a computer, it continued spreading across computers on the same network. Because of this infection method, some infections outside Ukraine were traced back to corporations having subsidiaries in Ukraine and a shared network between all machines.[17] NotPetya primarily spread using the EternalBlue exploit on Windows devices and by stealing credentials using tools like Mimikatz, a tool that looks through a computer's memory to gather authentication information.[18]

The overall explanation of NotPetya's attack follows. First, it infects at least one computer on a network, achieved through the M.E.Doc update mentioned previously. Next, the virus works on infecting new devices. The virus attempts to use the EternalBlue exploit, discussed later, to infect others and further infects by retrieving any credentials it can find on the current machine using Mimikatz, mentioned above. Using those credentials, the virus can move across the network by logging into SMB, which grants it the ability to infect other devices.[19] After some time of spreading itself, typically an hour, the virus encrypts the Master Boot Record (MBR) and Master File Table (MFT) leaving the device useless.[20] Since your device needs the

[15] Kroustek, "Things learned about Petna."
[16] Ibid.
[17] Ibid.
[18] Ibid.
[19] "NotPetya Technical Analysis." LogRhythm, June 30, 2017. https://logrhythm.com/blog/notpetya-technical-analysis/.
[20] Fayi, "Petya/NotPetya and Its Remediations."

MBR and MFT to locate files such as your operating system on startup, your computer cannot operate.[21] Therefore, the NotPetya virus succeeded in making a computer and its files unusable.

The EternalBlue Vulnerability and Patch: Technical Overview

NotPetya's other primary method of spread came from the EternalBlue vulnerability. EternalBlue refers to an issue with the "Microsoft Server Message Block 1.0 (SMBv1) server."[22] Microsoft uses the Server Message Block protocol to share files within a network to other places.[23] In SMBv1, an unauthenticated attacker could send a special package to another device running SMBv1 that would be accepted.[24] This package could contain a malicious file, in this case, a copy of NotPetya, which would then run on the receiving device.[25]

Interestingly, Microsoft patched the EternalBlue vulnerability in security bulletin MS17-010 that went out on March 14, 2017[26] – more than three months before the NotPetya attack. This patch to EternalBlue disabled SMBv1 in Windows 10 and Windows Servers 2012 and 2016 while fixing the flaws in SMBv1 in older systems.[27] After the WannaCry attack, discussed later, utilized EternalBlue on May 12, 2017, Microsoft took a further step to remedy the vulnerability by releasing patches for unsupported operating systems on May 13, 2017, an unprecedented step showing the severity of the exploit.[28] Luckily, the EternalBlue "patch closes the security

[21] Ibid.

[22] "MS17.010: Security update for Windows SMB Server: March 14, 2017." Microsoft, March 14, 2017. https://support.microsoft.com/en-us/topic/ms17-010-security-update-for-windows-smb-server-march-14-2017-435c22fb-5f9b-f0b3-3c4b-b605f4e6a655.

[23] "Microsoft SMB Protocol and CIFS Protocol Overview." Microsoft, January 7, 2021. https://docs.microsoft.com/en-us/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview.

[24] "Microsoft Security Bulletin MS17-010 – Critical." Microsoft, September 2, 2020. https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010?redirectedfrom=MSDN.

[25] Ibid.

[26] Ibid.

[27] Burdova, "EternalBlue MS17-010 Still Relevant."

[28] Palmer, Danny, "WannaCrypt ransomware: Microsoft issues emergency patch for Windows XP." ZDNet, May 13, 2017. https://www.zdnet.com/article/wannacrypt-ransomware-microsoft-issues-patch-for-windows-xp-and-other-old-systems/.

vulnerability completely."[29] For this reason, it seems odd that the vulnerability was able to be so effective in the NotPetya attack. However, a patch only works on an updated system.

EternalBlue: A Brief History

The patch to EternalBlue seems like a tidy end to an unfortunate vulnerability. In reality, the EternalBlue vulnerability has a long history that now leads the debate around cyber ethics. The National Security Agency discovered EternalBlue around 2012.[30] Rather than tell Microsoft of the immense threat they had discovered, the NSA utilized EternalBlue in their cyber endeavors for five years.[31] While the NSA has never confirmed their involvement, many documents attribute EternalBlue to the NSA, and Microsoft has publicly named the NSA as responsible for the exploit.[32]

Shadow Brokers, a group of hackers, allegedly breached the NSA and began releasing tools used by the NSA.[33] On April 14, 2017, the Shadow Brokers released EternalBlue to the world providing all hackers the knowledge of the exploit's existence.[34] The EternalBlue patch had already been released exactly a month earlier by Microsoft. This action caused speculation that the NSA, aware Shadow Brokers may have EternalBlue, warned Microsoft about its impending release so they could create a patch.[35]

Although Microsoft developed a patch, many are slow to update their devices, and on May 12, 2017, the first significant attack utilizing EternalBlue occurred: WannaCry. The

[29] Burdova, "EternalBlue MS17-010 Still Relevant."
[30] Ibid.
[31] Ibid.
[32] Newman, Lily, "The Leaked NSA Spy Tool That Hacked the World." Wired, March 7, 2019. https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.
[33] Ibid.
[34] Burdova, "EternalBlue MS17-010 Still Relevant."
[35] Newman, "Leaked NSA Spy Tool."

WannaCry ransomware attack used EternalBlue to jump from computer to computer encrypting files and demanding Bitcoin to decrypt them.[36] The attack spread quickly infecting over 230,000 devices in one day and causing $4 billion worth of damages.[37] However, WannaCry, unlike the later NotPetya, had an easy kill switch. In the code, WannaCry checked to see if a web address existed before executing, so one researcher registered the domain and thus stopped the ransomware.[38]

The WannaCry attack led to the previously mentioned Microsoft update for unsupported software to further patch EternalBlue. Yet on June 27, 2017, many devices remained outdated, so NotPetya continued to exploit EternalBlue months after the patch.

Analyzing Future Technical Risk of NotPetya and EternalBlue

Though EternalBlue had been patched, NotPetya had still been able to occur, thus begging the question of whether the virus or vulnerability could cause future destruction. Even now, estimates of "the number of unpatched vulnerable Windows systems remain in the millions."[39] This statistic poses the greatest threat for EternalBlue and NotPetya to continue causing damage to computers.

However, one possible saving grace comes in the form of antivirus software. Common antiviruses, like McAfee, can now recognize Petya variants, including NotPetya, thus preventing them from causing harm if found on a computer.[40] Of course, this would mean the computer

[36] Hern, Alex, "WannaCry, Petya, NotPetya: how ransomware hit big time in 2017." The Guardian, December 30, 2017. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.
[37] Burdova, "EternalBlue MS17-010 Still Relevant."
[38] Hern, "Ransomware hit big time."
[39] Burdova, "EternalBlue MS17-010 Still Relevant."
[40] "Protecting against modified Petya and BadRabbit ransomware variants." McAfee, Last Modified March 3, 2021. https://kc.mcafee.com/corporate/index?page=content&id=KB89540.

would have to have an updated version of the antivirus program. If a computer does not update its operating system, the possibility it updates its antivirus may be slim. But either an up-to-date operating system or an up-to-date antivirus should work to prevent future harm from NotPetya.

All Windows updates have focused on fixing the EternalBlue vulnerability to prevent future attacks, and the patch seems to be mostly stable. The patch disables SMBv1 on Windows 10 devices, but users still have the option of enabling the protocol.[41] Nevertheless, the patch addresses the protocol itself by changing the process SMBv1 handles the special requests used to gain access to devices using the EternalBlue vulnerability preventing the type of attack.[42] Even though EternalBlue seems patched, Microsoft itself acknowledges that the SMBv1 protocol remains unsafe, and Microsoft even has strong recommendations against using or reinstalling SMBv1 citing the protocol's history of being vulnerable to ransomware attacks.[43] With this in mind, EternalBlue seems like it no longer poses a threat though the possibility of another SMBv1-related exploit does not seem impossible.

Of course, the NotPetya attack circumvented the Windows update on some computers by using Mimikatz to extract credentials from a computer's memory. Since the NotPetya attack, Microsoft has released more software updates, all of which include Credential Guard software. This security measure "fully protects from the credential dump executed by Petya using the external Mimikatz-like tool,"[44] according to Microsoft. Because of this, even more recently

[41] Burdova, "EternalBlue MS17-010 Still Relevant."
[42] "Microsoft Security Bulletin MS17-010."
[43] "SMBv1 is not installed by default in Windows 10 version 1709, Windows Server version 1709 and later versions." Microsoft, November 2, 2021. https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/smbv1-not-installed-by-default-in-windows.
[44] "Windows 10 platform resilience."

updated device owners should not have to worry about others' lack of updates to keep themselves safe.

NotPetya and EternalBlue seem to be just the beginning of cyber threats. Shadow Brokers also released a vulnerability called EternalRocks, an exploit composed of seven other exploits (including EternalBlue) working together to penetrate devices.[45] No one has ever used this vulnerability, and the tinier exploits, like EternalBlue, have seemingly been patched. But this demonstrates a new reality in malicious cyber-attacks. Whereas NotPetya relied on EternalBlue and Mimikatz to achieve spread and harm, future attacks could be composed of many more exploits making it harder to prevent them. The technical advancements in these attacks seem to be growing, as seen in the jump in effectiveness between WannaCry and NotPetya in just under two months. So, while NotPetya's future risk may be minor, it demonstrates a new warning about the potential harm these types of attacks can cause in the future.

Overall, I believe the greatest technical threat comes from potential future cyber-attacks, and thus, the focus should shift towards preparing systems to fight future events. NotPetya and EternalBlue's ability to harm has decreased immensely because of the widespread coverage of the attack forcing action by tech companies. Meanwhile, attackers have had time to shift their focus towards developing new malicious software yet to be released into the world.

Attribution of Blame

With a $10 billion attack having already occurred and a minor risk for future attacks to come, blaming the NotPetya virus on someone or some entity seems like an easy way to hold a party accountable and potentially squash their ability to cause future harm using NotPetya or

[45] Burdova, "EternalBlue MS17-010 Still Relevant."

another attack. Unfortunately, in this case, like many cases relating to cyber-attacks and malware, pinpointing the responsible party is easier said than done.

On the surface level, the responsible party seems rather obvious. Less than a day after the attack began, Ukraine suggested Russia was the responsible party.[46] After taking a few months to analyze the attack, official recognition of Russia as the responsible party came in February 2018 from countries including the UK, Denmark, and the United States in official statements from the respective governments.[47] The statements recognized that the GRU, the Russian military intelligence agency, was responsible for NotPetya.[48]

With this knowledge, seeing Russia as the only offender, in this case, seems like an easy resolution to this story. However, only acknowledging Russia refuses to recognize the steps that led NotPetya to become incredibly damaging. For one, NotPetya demonstrates remarkable similarity to WannaCry. The United States attributed that attack to North Korea.[49] Of course, no evidence suggests the North Korean team simply gave the Russians the basis for NotPetya. But the similarity between the attacks demonstrates the complicated task of blaming one party for the entire attack's development.

More glaringly, there exists the matter of the National Security Agency's amount of fault in the attack. NotPetya's success at transmission came primarily from EternalBlue that the NSA had developed and been using for five years before warning Microsoft of its existence.[50] Of

[46] Hern, Alex, "Ransomware attack 'not designed to make money,' researchers claim." The Guardian, June 28, 2017. https://www.theguardian.com/technology/2017/jun/28/notpetya-ransomware-attack-ukraine-russia.
[47] Greenberg, Andy, "The White House Blames Russia for NotPetya, the 'Most Costly Cyberattack In History.'" Wired, February 15, 2018. https://www.wired.com/story/white-house-russia-notpetya-attribution/.
[48] Ibid.
[49] "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." The United States Department of Justice, September 6, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.
[50] Burdova, "EternalBlue MS17-010 Still Relevant."

course, systems could have remained outdated even if Microsoft had received the warning five years prior. However, five years would have given people much more time to update their systems than the three-month window they had between the actual release of the update and the NotPetya attack. The NSA came under fire for EternalBlue in the WannaCry and NotPetya attacks. Tom Bossert, the Homeland Security officer at the time, when discussing the WannaCry attack argued that EternalBlue was just one part of a much larger element used in the attack.[51] Of course, someone else could have found the EternalBlue vulnerability even if Shadow Brokers never released it. Yet that scenario would have arguably been worse for the world.

EternalBlue was not a zero-day vulnerability as Microsoft was aware of its existence and released a patch for it allegedly due to a tipoff from the National Security Agency as stated previously. Imagine a scenario where Shadow Brokers had not hacked the NSA, and attackers discovered EternalBlue on their own. In this hypothetical scenario, the NSA would have no reason to inform Microsoft of the exploit. After all, they had not said anything for five years. Consequently, the release of the WannaCry virus would have been the first time Microsoft knew of EternalBlue, and they would have had to scramble to patch EternalBlue. In turn, the patch may not have been ready or widely implemented for NotPetya, and both attacks could have been much more costly and damaging than they already were.

Admittedly, an argument could be made that Microsoft itself should have been at fault for creating buggy software to begin. Brad Smith, the president of Microsoft at the time, stated, “Instead of nation-state attacks being met by responses from other nation-states, they are met by

[51] "Microsoft's president says global cyberattack is a 'wakeup call.'" PBS, May 15, 2017. https://www.pbs.org/newshour/show/microsofts-president-says-global-cyberattack-wakeup-call.

us."[52] This statement can be seen as an argument for and against Microsoft's responsibility. Smith acknowledges that Microsoft needs to protect its users. But, there seemingly exists no reason why Microsoft must take on the role of sole protector and be held liable if they fail.

Challenging Practices: Stockpiling Vulnerabilities

Regardless of the guilty party, one, many, or all of the aforementioned ones, holding someone accountable for the NotPetya seems easier said than done. First, the issue of the NSA's role in developing EternalBlue. The NSA appeared to know it was in the wrong withholding EternalBlue as one former employee stated "using EternalBlue was 'like fishing with dynamite.'"[53] Yet, the agency did so in the name of national security. In general, the NSA stockpiles vulnerabilities to compete with nations doing the same.[54] While researchers may be encouraged to disclose their findings of vulnerabilities to practice responsible disclosure, the NSA's responsibility lies more towards protecting the nation as a whole rather than individual people or corporations.[55]

To encourage people to stop stockpiling vulnerabilities, companies like Microsoft have bug bounty programs where people who find bugs in their code can receive payment for reporting them to the company.[56] Unfortunately, these payments are often less than the price hackers will pay for the same information, and these payments do not matter to national security agencies.[57] Thus, this method does not seem adequate in preventing stockpiling.

[52] Smith, Brad, "The Need for a Digital Geneva Convention." Keynote Address at the RSA Conference, San Francisco, CA, February 14, 2017.
[53] Jon Watkins, "No Good Deed goes Unpunished: The Duties Held by Malware Researchers, Penetration Testers, and White Hat Hackers," Minnesota Journal of Law, Science and Technology 19, no. 2 (Summer 2018): 535-564.
[54] Ibid.
[55] Ibid.
[56] Ibid.
[57] Ibid.

One possible solution could come from a relationship between the NSA and companies like Microsoft. However, this seems unlikely. Brad Smith stated that Microsoft would protect customers everywhere and would not assist in attacking any customers.[58] The NSA would likely only agree to a partnership where companies like Microsoft assist in its hacking effort, something the company said it would not do. Alternatively, the NSA could change its policies to alert tech companies of vulnerabilities either right after discovery or after a decided amount of time. While this policy change sounds good on paper, the NSA has no incentive to do so. That would require the organization to spend more time discovering new vulnerabilities as the NSA alerts companies of their old ones. Because of this stalemate, a stockpiling policy change likely remains far from reality. As such, it can be hard to hold the NSA accountable as the organization seemingly protects itself under the umbrella of national security.

Challenging Policies: Charging Cyberweapons

While changing stockpiling seems unlikely, action against the offending party could achieve accountability. In other words, harsher action against the attacking software developers could deter them from future attacks.

Many people have referred to NotPetya as a cyberweapon or an act of cyberwarfare. On paper, these seem like threatening terms that could lead to swift action, but that would be too simple. Six people, all Russian GRU officers, were charged for NotPetya.[59] The charges against them were "conspiracy, computer hacking, wire fraud, aggravated identity theft, and false

[58] Smith, "Need Digital Geneva Convention."

[59] "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." The United States Department of Justice, October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

recognition of a domain name."[60] None of these charges relate to supposed "war" charges one might expect had NotPetya been considered a cyberweapon. The United States issued sanctions upon Russia in 2018 for the NotPetya attack and other cyber-meddling,[61] but these charges also failed to mention NotPetya as being a cyberweapon.

While these charges and sanctions may be satisfactory to some if NotPetya were classified as a cyberweapon, it would open doors to inflict harsher punishments that could be larger deterrents to responsible parties. For example, NATO has said that its laws apply to cyberspace, indicating officially labeled cyberwarfare acts would fall under NATO's treatment of physical war acts.[62] Unfortunately, classifying a cyberweapon proves not easy. The U.S. Department of Defense has noted that "'There is currently no international consensus regarding the definition of 'cyber weapon.''"[63] Without a clear internationally recognized definition of cyberweapons, the classification of cyberweapons seems far away. With that roadblock in place, the ability to force harsher punishments on cybercriminals seems impossible as a weapon must first be recognized to attribute its creation to a specific party.

Analyzing Future Legal and Political Risk

Currently, NotPetya and EternalBlue have revealed that another cyberattack of the same scale, or larger, could undoubtedly occur in the same manner. The NSA and other security agencies have no reason to start revealing their information, so continued stockpiles could lead to

[60] Ibid.

[61] Hatmaker, Tom, "U.S. issues broad Russian sanctions citing NotPetya attack and Internet Research Agency meddling." TechCrunch, March 15, 2018. https://techcrunch.com/2018/03/15/russian-sanctions-treasury-ira-notpetya/.

[62] "Cyber defence." North Atlantic Treaty Organization, Last updated July 2, 2021. https://www.nato.int/cps/en/natohq/topics_78170.htm.

[63] Roguski, Przemysław. "An Inspection Regime for Cyber Weapons: A Challenge Too Far?" *AJIL Unbound* 115 (2021): 111–15. doi:10.1017/aju.2021.6.

future exploit leaks containing damaging vulnerabilities like EternalBlue. Furthermore, lack of ability to inflict harsher punishments does nothing to incentivize malicious actors to stop cyberattacks. This inaction suggests a looming change in both law and politics.

Cyberwarfare and cyberattacks will go nowhere. To have a better response to when cyberattacks occur, political action should be taken to recognize them appropriately and to navigate the relationship between governmental duty and information disclosure. Additionally, legal action should be taken to ensure all responsible parties see charges placed against them to prevent future attacks.

In reality, I do not see any of this occurring without a catalyst, for it seems the threat is large enough that a change would have been made already if it was going to be made. I think NotPetya could have been that catalyst, but with no action sparked, I believe another massive cyberattack will have to occur for measures to be taken to prevent and regulate cyber warfare. The U.S. government, in particular, does not have a substantial enough incentive to act with NotPetya as Ukraine experienced the brunt of the attack. Unfortunately, the risk here lies in inaction. For now, the lack of legal or political actions means that should a cyberattack occur, governments will be playing catch up to determine how to act.

Conclusion

NotPetya and EternalBlue inspired worldwide action encouraging companies to update software, forcing Microsoft to patch software, and compelling countries to attribute responsibility to and inflict sanctions on Russia. Despite these actions, the NotPetya attack demonstrates the beginning of a new era of cyber attacks rather than the end. The technical patches now successfully prevent EternalBlue from being exploited and prevent NotPetya from causing future damage, but future software vulnerabilities still exist prepared to be exploited. Some of those vulnerabilities may be in the hands of the NSA, already being used in the name of national security just as EternalBlue was. Without action, a replica of NotPetya could play out with slightly different software but similar legal and political fallout. Future attacks will happen, and legal and political changes are necessary to better protect against and criminalize these attacks. The new era of cyber weaponization has arrived, and without future action, the United States and the world will remain steps behind malicious actors with the ability to cause immense damage.

References

Aurélien Palisse et al, “Ransomware and the Legacy Crypto API,” in *Risks and Security of Internet and Systems*. Frédéric Cuppens et al. (Roscoff, France: Springer, Cham 2016) pp. 11-28.

Burdova, Carly, “What is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?” Avast, June 18, 2020. https://www.avast.com/c-eternalblue#gref.

“Cyber defence.” North Atlantic Treaty Organization, Last updated July 2, 2021. https://www.nato.int/cps/en/natohq/topics_78170.htm.

Fayi, Sharifah, “What Petya/NotPetya Is and What Its Remediations Are,” in *Information Technology – New Generations*. Shahram Latifi. (Springer, Cham 2018) pp. 93-100.

Greenberg, Andy, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History.” Wired. August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Greenberg, Andy, “The White House Blames Russia for NotPetya, the ‘Most Costly Cyberattack In History.'" Wired, February 15, 2018. https://www.wired.com/story/white-house-russia-notpetya-attribution/.

Hatmaker, Tom, “U.S. issues broad Russian sanctions citing NotPetya attack and Internet Research Agency meddling.” TechCrunch, March 15, 2018. https://techcrunch.com/2018/03/15/russian-sanctions-treasury-ira-notpetya/.

Hern, Alex, “Ransomware attack ‘not designed to make money,’ researchers claim.” The Guardian, June 28, 2017. https://www.theguardian.com/technology/2017/jun/28/notpetya-ransomware-attack-ukraine-russia.

Hern, Alex, “WannaCry, Petya, NotPetya: how ransomware hit big time in 2017.” The Guardian, December 30, 2017. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware.

Jon Watkins, "No Good Deed goes Unpunished: The Duties Held by Malware Researchers, Penetration Testers, and White Hat Hackers," Minnesota Journal of Law, Science and Technology 19, no. 2 (Summer 2018): 535-564.

Kroustek, Jakub, “Things we have learned about Petna, the Petya-based malware.” Avast, June 30, 2017. https://blog.avast.com/things-we-have-learned-about-petna-the-petya-based-malware?_ga=2.177441189.1440778063.1637123550-103372661.1637004001.

"Microsoft's president says global cyberattack is a 'wakeup call.'" PBS, May 15, 2017. https://www.pbs.org/newshour/show/microsofts-president-says-global-cyberattack-wakeup-call.

“Microsoft Security Bulletin MS17-010 – Critical.” Microsoft, September 2, 2020. https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010?redirectedfrom=MSDN.

“Microsoft SMB Protocol and CIFS Protocol Overview.” Microsoft, January 7, 2021. https://docs.microsoft.com/en-us/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview.

"MS17.010: Security update for Windows SMB Server: March 14, 2017." Microsoft, March 14, 2017. https://support.microsoft.com/en-us/topic/ms17-010-security-update-for-windows-smb-server-march-14-2017-435c22fb-5f9b-f0b3-3c4b-b605f4e6a655.

Newman, Lily, "The Leaked NSA Spy Tool That Hacked the World." Wired, March 7, 2019. https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

Nicole Perlroth, Mark Scott, and Sheera Frenkel, "Cyberattack Hits Ukraine Then Spreads Internationally." New York Times, June 27, 2017. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.

"North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions." The United States Department of Justice, September 6, 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

"NotPetya Technical Analysis." LogRhythm, June 30, 2017. https://logrhythm.com/blog/notpetya-technical-analysis/.

Palmer, Danny, "WannaCrypt ransomware: Microsoft issues emergency patch for Windows XP." ZDNet, May 13, 2017. https://www.zdnet.com/article/wannacrypt-ransomware-microsoft-issues-patch-for-windows-xp-and-other-old-systems/.

"Protecting against modified Petya and BadRabbit ransomware variants." McAfee, Last Modified March 3, 2021. https://kc.mcafee.com/corporate/index?page=content&id=KB89540.

Roguski, Przemysław. "An Inspection Regime for Cyber Weapons: A Challenge Too Far?" *AJIL Unbound* 115 (2021): 111–15. doi:10.1017/aju.2021.6.

"Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." The United States Department of Justice, October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

"SMBv1 is not installed by default in Windows 10 version 1709, Windows Server version 1709 and later versions." Microsoft, November 2, 2021. https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/smbv1-not-installed-by-default-in-windows.

Smith, Brad, "The Need for a Digital Geneva Convention." Keynote Address at the RSA Conference, San Francisco, CA, February 14, 2017.

"Windows 10 platform resilience against the Petya ransomware attack." Microsoft, June 29, 2017. https://www.microsoft.com/security/blog/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/.