The Shadow Brokers (TSB) and the 2016 NSA Data Breach

Illustration from Darknet Diaries

Case Study Report

Rohan Senthil

Disclaimer: This report is an extract of an assignment I had to do for one of my modules

Table of Contents

Executive Summary

In August 2016, a mysterious group who called themselves ‘The Shadow Brokers’ began a series of devastating data dumps of sophisticated hacking tools and exploits widely believed and linked to the US National Security Agency (NSA) Tailored Access Operations (TAO) unit or more specifically, their elite hacking unit, The Equation Group.

Upon announcing their possession of The Equation Group's cyber weapons, they began an auction, selling these tools to the highest bidder. The auction, however, was largely unsuccessful and in a surprising change of events, The Shadow Brokers released the passwords to the encrypted files containing The Equation Group’s cyber weapons. The Shadow Brokers themselves hinted at this change of heart being a response to then US President, Donald Trump’s foreign policy in Syria and their disappointment in his administration since taking power. Though this could of course be an attempt to conceal their real motives and hence their real identity.

However, what really matters is what followed because of these leaks. With the NSA’s cyber weapons now released into the wild, many were concerned with its implications and rightfully so. Microsoft, however, released patches about a month before these dumps for many of the exploits that were part of these dumps. This eased the concerns of many. Few could have imagined the disastrous impacts of these patched exploits.

ETERNALBLUE, one of the exploits released in the Shadow Brokers dumps was utilised in the months that followed in some of the most devastating and consequential cyberattacks in history, namely the WannaCry ransomware attack which began in May 2017 and the NotPetya wiper-malware ‘ransomware’ cyberattacks which began in June 2017. Both attacks are believed to have caused billions of dollars of damage globally with NotPetya even shutting down critical infrastructure and operations in mostly Ukraine but also globally.

Due to the classified nature of their organisation, the exact actions and responses of the NSA remain unknown. However, we can assume that they would have launched an immediate investigation into the source of the breach and likely would have to reassess their operations, especially those where the leaked tools were in use. With the NSA already suffering from several breaches including the Edward Snowden leaks in 2013, we can also assume that if there did not already exist plans for the restructuring of the organization and to reassess its capabilities, especially in securing their assets, there would most certainly be in the aftermath of the breaches. Evidently, the NSA later went on the form the Cybersecurity Directorate (CSD) as well as various other directorates. However, the NSA’s response was not the greatest, and they could have definitely done a lot more to minimise the impacts of their exploits being leaked.

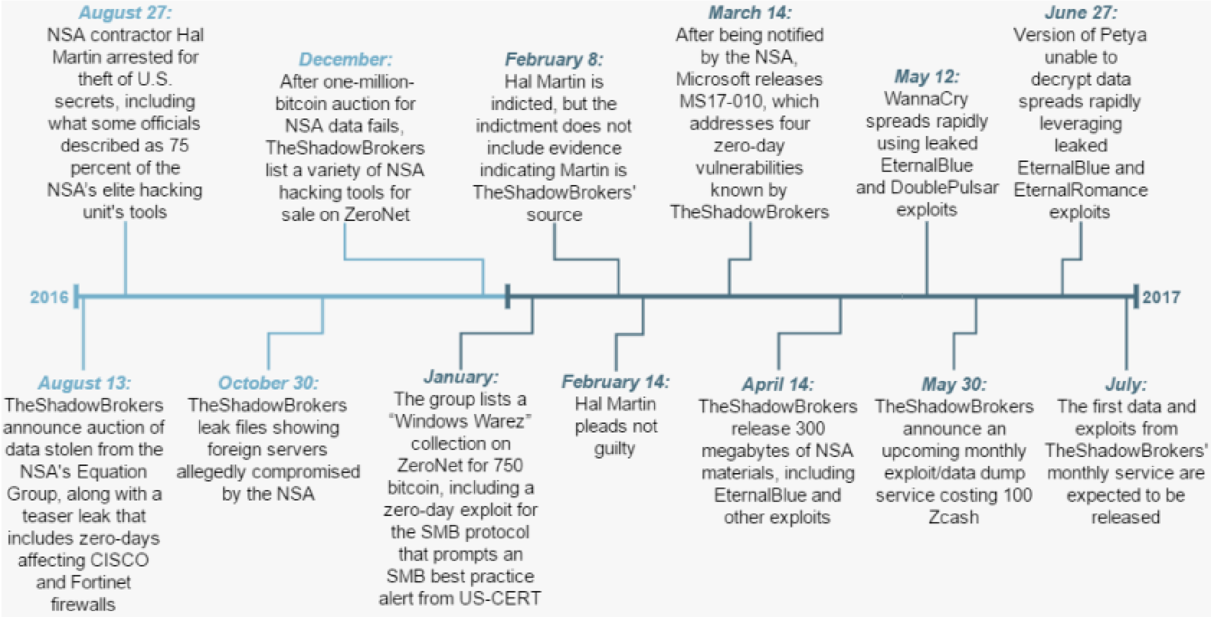
Introduction

The Shadow Brokers first appeared in August 2016, their opening act: an invitation to the Equation Group Cyber Weapons Auction. Their invitation was poorly written and phrased. It included some free files meant to prove the authenticity of their claims. They claimed that they had followed the Equation Group traffic, found its source range, and hacked it, hence obtaining their cyber weapons. The Equation Group is one of the most advanced threat actors and is widely believed to be part of the Tailored Access Operations (TAO) unit of the US National Security Agency (NSA). They are also believed to be the authors of Stuxnet a computer worm used in one of the most impressive targeted cyber-attacks in history. This initial post was met with skepticism but the exploits that were dumped were indeed working on fully patched firewalls. Yet, it was not conclusive enough to prove that the Shadow Brokers possessed NSA exploits. At this time, many would assume that The Shadow Brokers had one motive, financial gain. However, in the months that followed their real motives became clouded, baffling even the best analysts. The next few messages contain interesting information and references to the Equation Group, however, contain no actual exploits and tools.

When analysing a situation like this, it is important to understand the context. Around the time of the initial dumps, the US was having their 2016 presidential elections. Donald Trump eventually won, though this victory was overshadowed by the idea of the Russians potentially meddling in the election. Whether a coincidence or not, the Shadow Brokers announced their 'retirement' in January 2017, right as Donald Trump was inaugurated as the US President. Their reason for retirement was that they could not get the amount they wanted from their auction and were instead going to release more information for free. This dump included 60 over files. Then they went dark.

On the morning of 7 April 2017, in response to the Khan Shaykhun chemical attack that occurred 3 days earlier, the US launched a missile strike at an airbase controlled by the Syrian government. This strike was executed under the responsibility of then-US President Donald Trump. Around this time, the Russians were being blamed for cyber-attacks, hacks, and interfering in the US elections. One day after the strikes, The Shadow Brokers came back into the spotlight, dumping even more stolen hacking tools. In their post titled 'Don't Forget Your Base', they stated that they had supported Trump but were now losing their faith and believed he had abandoned those who got him elected.

A few days later, on 14 April 2017, The Shadow Broker released their final and most damaging dump yet. This dump contained ETERNALBLUE and ETERNALROMANCE among many other NSA exploits. The deadly NSA exploits were now in the wild. Though there were concerns about the implications of this dump, many were quick to point out that Microsoft had already patched many of the vulnerabilities these tools exploited, including ETERNALBLUE a month before the dumps. That was their last public dump and after a few monthly subscription dumps, posts and comments every now and then the Shadow Brokers went dark post 2017.



August 13: TheShadowBrokers announce auction of data stolen from the NSA's Equation Group, along with a teaser leak that includes zero-days affecting CISCO and Fortinet firewalls

August 27: NSA contractor Hal Martin arrested for theft of U.S. secrets, including what some officials described as 75 percent of the NSA's elite hacking unit's tools

October 30: TheShadowBrokers leak files showing foreign servers allegedly compromised by the NSA

December: After one-million-bitcoin auction for NSA data fails, TheShadowBrokers list a variety of NSA hacking tools for sale on ZeroNet

January: The group lists a "Windows Warez" collection on ZeroNet for 750 bitcoin, including a zero-day exploit for the SMB protocol that prompts an SMB best practice alert from US-CERT

February 8: Hal Martin is indicted, but the indictment does not include evidence indicating Martin is TheShadowBrokers' source

February 14: Hal Martin pleads not guilty

March 14: After being notified by the NSA, Microsoft releases MS17-010, which addresses four zero-day vulnerabilities known by TheShadowBrokers

April 14: TheShadowBrokers release 300 megabytes of NSA materials, including EternalBlue and other exploits

May 12: WannaCry spreads rapidly using leaked EternalBlue and DoublePulsar exploits

May 30: TheShadowBrokers announce an upcoming monthly exploit/data dump service costing 100 Zcash

June 27: Version of Petya unable to decrypt data spreads rapidly leveraging leaked EternalBlue and EternalRomance exploits

July: The first data and exploits from TheShadowBrokers' monthly service are expected to be released

Figure 1 - Timeline of the NSA Shadow Brokers Breach

Root Cause

The NSA is an intelligence agency of the United States Department of Defense. Besides having some of the best cybersecurity talents in America, it also receives billions of dollars in funds. That begs the question, how did the Shadow Brokers come to obtain their hacking tools? Surely it was by no means an easy task.

With the NSA being an intelligence agency, naturally, they would not release much information if they even decided to release anything. In this case, the NSA did not release any information to the public regarding Shadow Brokers and how the breach occurred. We can merely judge based on the actions of the perpetrators, the context of the situation and the actions that we know the NSA took.

A breach of this scale attracted many researchers, all trying to figure out who exactly the Shadow Brokers could be. However, they could not find anything conclusive nor could the NSA or the FBI, at least according to what we are allowed to know. All we are left with are theories, but among all the different theories lie TWO very well-supported theories:

1. The breach was a result of an **insider threat**.
2. The breach was a result of a **sophisticated attack** likely linked to **Russian state-sponsored attacks**.

Before we discuss these theories in depth, to evaluate the theories, we need to analyse the Shadow Brokers and their possible motives for this breach.

We know that their first action was to auction off the NSA tools that they had in their possession. This suggests that the Shadow Brokers. especially initially, were likely motivated by financial gain. However, their motivations could also be political. Perhaps it was to influence the elections somehow or simply to damage the NSA's reputation and capabilities because they did not agree with what the NSA had been doing such as zero-day 'hoarding' or their offensive actions. It could also be just to sow chaos and disrupt the world. We do not know for sure but the Shadow Brokers themselves did mention that their final two dumps were in response to the actions of the Trump Administration. In their medium article titled ‘Don’t Forget Your Base’, the Shadow Brokers stated a whole bunch of suggestions to the Trump Administration and that they were unhappy with his presidency thus far. They then concluded that this was their ‘form of protest’ and then released the passwords for the Equation Group auction files for free. Their motives could hence be financial gain initially before then becoming political. Of course, this could all be a façade for their real motives.

Theory 1: The Insider Theory

The Insider leak theory is supported by the possible financial and political motives that the Shadow Brokers are believed to have possessed. The Shadow Brokers could be a disgruntled employee who did the dumps either for financial gain, political and ideological beliefs or because he was dissatisfied at work or with the direction the NSA was heading or was currently at. It is important to note that there was some political turmoil in the NSA in 2016 after the director was abruptly fired due to clashes with the current administration at that time. This could support that the insider was unhappy with the direction the NSA was heading.

The Shadow Brokers also knew some other interesting information including an ex-NSA and employee part of the Equation Group, Jake Williams, and publicly announced this information online after Jake made several posts analysing who the Shadow Brokers might be. This information could have been part of the breaches, however, that would mean the Shadow Brokers compromised quite a large portion of the NSA for them to retrieve information that was likely stored separately. Hence, this could hint at the Shadow Brokers being an insider such as a former colleague of Jake.

Interestingly, the NSA together with the FBI did make some arrests after the breach that could hint at an insider. In August 2016, Harold T. Martin II, was arrested and accused of stealing classified NSA documents and leaking them. Many, including the FBI, had suspected him of being the leaker. However, to our knowledge, though he did steal over 50 TBs of classified NSA documents there is no evidence to strongly suggest he was behind The Shadow Brokers leak or that he even sold or shared the information he possessed. He is not suspected of being Shadow Brokers themselves since they continued to be active after his arrest. But he could very likely be the insider who sent information to the Shadow Brokers.

Another arrest was made in 2018 of a TAO employee, Nghia Hoang Pho for the retention of classified material. Though details of his hearing and arrest are classified there are some possible indications that the data Nghia Hoang Pho stole included exploits such as the Eternal exploits which links to The Shadow Brokers.

To access all the information that the Shadow Brokers had in their possession, if they were an insider, they would likely need to have high clearance, access to specialized programs and in a cybersecurity or intelligence-related role. These are likely to be members of the NSA’s Tailored Access Operations (TAO) unit, NSA employees with a need-to-know basis or NSA contractors involved in specific projects.

This fits into the profile of Harold T. Martin II who was a contractor who worked for NSA’s Tailored Access Operations (TA0) unit and Nghia Hoang Pho a TAO employee. The unit is believed to be associated with the Equation Group from which the exploits were obtained and leaked.

Additionally, linguistic analysis of the messages The Shadow Brokers found that their bad English was likely intentional. The study concluded that their texts included many grammatical errors in idioms that a low-skilled English speaker probably would not know and instead was someone well versed in English intentionally inserting errors.

The Shadow Brokers also mentioned “Did you know most of theshadowbrokers’ members have taken the oath ‘…to protect and defend the constitution of the United States against all enemies foreign and domestic…’. Yes sir! Most of us used to be TheDeepState everyone is talking about. But we realized TheDeepState is being the enemy of the constitution, individualism, life, liberty, and the pursuit of happiness.” With that being said, why would they still fake bad English?

Analysts of the files that the Shadow Brokers leaked have mentioned also that the files are likely to have been directly copied from the source repository. Yet, the repository containing the NSA TAO Toolkit is stored on a physically segregated network which did not and has no reason to touch the internet. Unless some deliberately did it.

Whatever the case, for so much information to be exfiltrated from the NSA’s systems, the NSA likely lacked proper insider prevention protocols and had slow insider detection systems. Harold T. Martin II had been stealing information for more than 20 years and another insider, Nghia Hoang Pho for 5 years before they were eventually caught. Had they had proper and effective techniques to monitor their employees, detect potential insiders and prevent them, insiders like Harold T. Martin II would likely not have gotten away with so much information and would have been caught much earlier.

Theory 2: Russian state-actors

Another popular theory is that The Shadow Brokers could be a Russian Advanced Persistent Threat (APT) or otherwise Russian state actors.

Events that occurred around this period that involved the US and Russia include the 2016 US presidential elections, where Russia was accused of meddling in the elections, the Syrian War where Russia was supporting the Syrian government and the US, the rebels and the Ukrainian crisis after Russia annexed Crimea in 2014. The US supported Ukraine.

The periods of their dumps also took place after the Democratic National Committee (DNC) server breaches and Russia was beginning to appear in the news. These dumps coincidentally took the focus away from Russian hacking and to the fact that the NSA had lost important tools. The group also ‘retired’ after Trump’s inauguration and the Russians were known to have meddled in the elections to aid Trump in victory. Coincidence?

The political views of the Shadow Brokers also seem to line up with what a Russian APT group would have, particularly, when they expressed their dissatisfaction at the US increasing involvement in the Syrian War.

It is also important to note that the Shadow Brokers are a group not afraid of going to ‘war’ with the NSA. They managed to get the exploits out of the NSA, publish them and have so far gotten away with it. To do so would require either being extremely lucky (unlikely) or very skilled and sophisticated. That points to an APT group.

If it was the Russians, how could they have gotten into the NSA’s systems? Well once again we do not really have much information on this, and we can really only speculate. The group could have exploited some vulnerability in the NSA software such as zero-days or conducting supply chain attacks by targeting NSA contractors or even by recruiting NSA insiders. This would also likely require extensive reconnaissance and overall would be quite complex to pull off and get away with. In addition, they were willing to hold this information for around 3 years before announcing it to the public. However, one thing that pokes a hole in this theory is that if it were a Russian APT group would it not be more valuable to keep the leaked tools a secret?

Weighing the Theories

Now with two well-established theories, which one triumphs over the other? Well, we cannot really say for sure. The situation is too complex and there is simply little information to judge on. However, in my opinion, if I had to assume, I would think that an insider is involved. With the NSA already suffering several insider leaks prior, I believe that the Russians saw this as a weakness in the NSA's ecosystem. They likely targeted and tried to recruit NSA contractors or employees. From the insiders, they were able to gather information about their exploits. It is either that or instead of the Russians some other hacking group or hacktivists. Whatever the case I believe an insider was likely involved. With that being said, I believe that the NSA lacked efficient and effective employee monitoring and insider detection and prevention practices.

Impacts

Following the breach, the most immediate impact was the damage this breach had on the NSA's reputation and its operations. The cybersecurity industry was also on high alert as the threat of cyber-attacks was now much higher, especially with deadly cyber weapons floating around the internet for free. Regarding their reputation, many begin to question the NSA's ability to protect the US if they could even protect themselves. As the Times put it:

"Current and former agency officials say the Shadow Brokers disclosures, which began in August 2016, have been catastrophic for the NSA, calling into question its ability to protect potent cyberweapons and its very value to national security. The agency regarded as the world's leader in breaking into adversaries' computer networks failed to protect its own."

With that being said, the NSA operations were also affected. They could now no longer effectively and safely deploy the cyber weapons that were leaked in future and present operations as they run the risk of being detected.

There were also questions raised on the ethics of stockpiling cyber weapons, especially zero-day vulnerabilities instead of informing the relevant parties and patching them.

Yet the greatest damages of this breach were to come in the months that followed. With the NSA's cyber weapons in the wild, various malware utilising the exploits from the Shadow Brokers breach such as ETERNALBLUE, ETERNALROMANCE and DoublePulsar, started appearing on the internet. Their impact was devastating.

In May 2017, the WannaCry ransomware, which uses the EternalBlue exploit to gain access and propagate and the DoublePulsar tool to install and execute a copy of itself, began infecting computers around the world. Though the attack lasted only a few hours after a kill switch was discovered, it had already done significant damage. Around 300,000 to 400,000 computers were affected in more than 150 countries – one of the biggest ransomware outbreaks in history. Singapore was one of the many countries hit by the WannaCry ransomware worm. Kiosks in many malls were infected and displayed the infamous WannaCry malware message. Even critical agencies such as the National Health Service (NHS) were not sparred. Many of their computers, MRI scanners, theatre equipment and blood-storage refrigerators were affected, forcing them to turn away some ambulances and non-critical emergencies. Overall, the attack is estimated to have caused up to US$4 billion in damages globally.

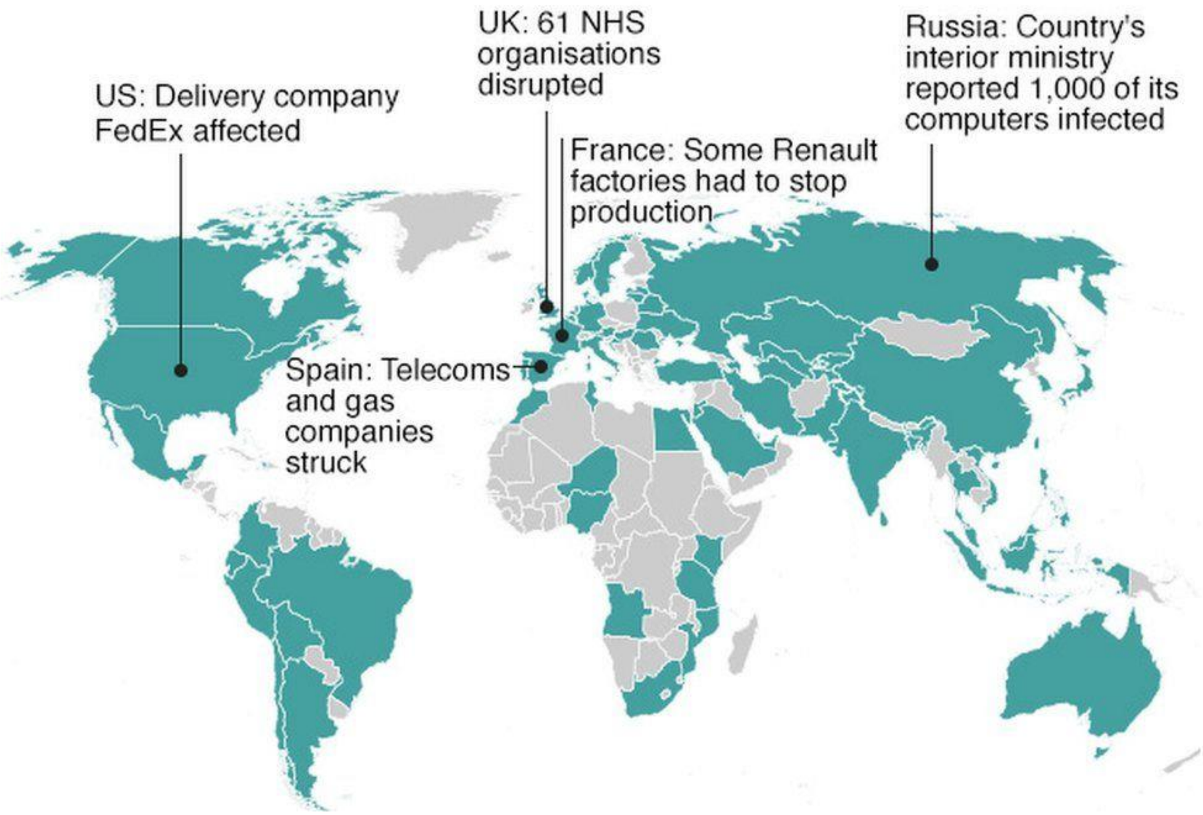

UK: 61 NHS organisations disrupted
Russia: Country's interior ministry reported 1,000 of its computers infected
US: Delivery company FedEx affected
France: Some Renault factories had to stop production
Spain: Telecoms and gas companies struck

Figure 2 – Critical hits of the WannaCry attack

That was not the worst of it. A month later, in June 2017, NotPetya began. Attributed as the biggest cyber-attack and espionage in history, NotPetya utilised the EternalBlue exploit as one of its two methods to propagate. The attack though mainly targeted on Ukraine, had implications globally. NotPetya disguised itself as a ransomware however was actually more of a wiper-malware, its aim was not to get ransom but to wipe and erase all the data it could possibly get its hand on. Many Ukrainian companies and even government agencies were hit hard by this attack. Most of the country's infrastructure such as banks, the metro and various ministries went down as all the key players were either forced to shut down their networks and servers to prevent further damages or already lost the data they needed to stay operational. The attack also turned off the radiation monitoring system of Ukraine's Chernobyl Nuclear Power Plant, which could have turned out really bad.

International companies were not spared either. Maersk a Danish company and the largest shipping company in the world were also hit hard. With all their systems down, all their terminals around the world were left with trucks lined up waiting to load goods delivered but could not as no one knew where anything was supposed to go with their systems down. Ships that contain what the modern economy runs on such as food and consumer goods were now left dormant. All their domain controllers were also either ruined, wiped or destroyed. With their domain controllers gone, their network was gone. Luckily, they had one domain controller in Ghana still working as it was offline during the attacks. Even so, Maersk had to rebuild their whole network and their whole operation from scratch. They had to succeed as they were simply too big to fail, as failing would have devasting impacts on the global economy. This cost them US$300 million. NotPetya also affected FedEx and cost over US$400 million.

Overall, the NotPetya attack is estimated to have caused damages of more than US$10 billion globally.

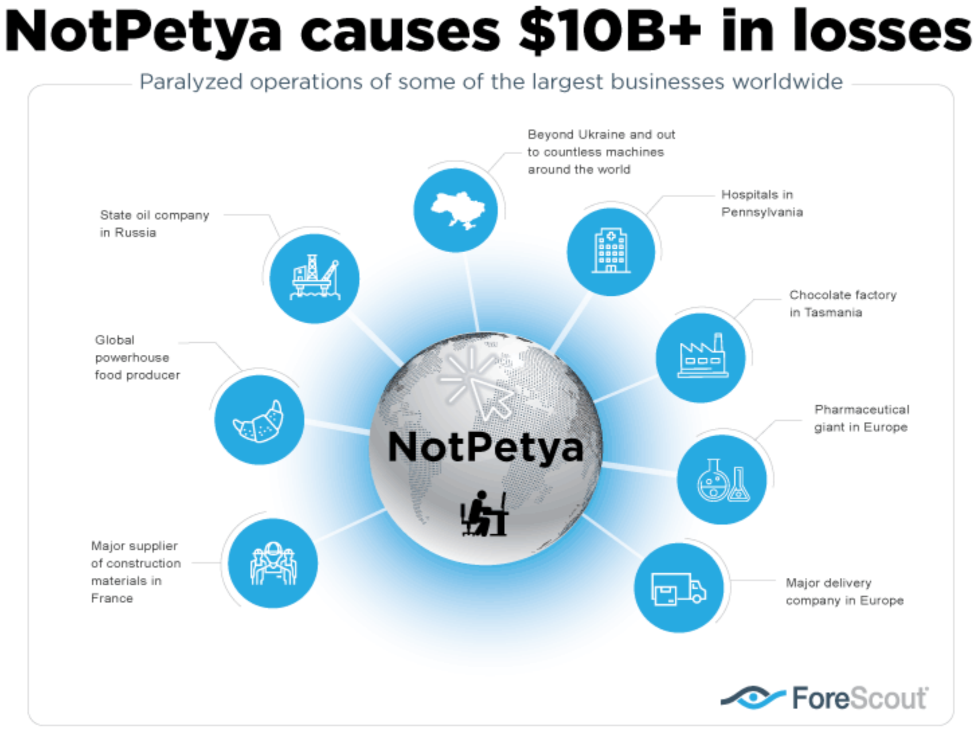

NotPetya causes $10B+ in losses
Paralyzed operations of some of the largest businesses worldwide
Beyond Ukraine and out to countless machines around the world
Hospitals in Pennsylvania
State oil company in Russia
Chocolate factory in Tasmania
Global powerhouse food producer
Pharmaceutical giant in Europe
NotPetya
Major supplier of construction materials in France
Major delivery company in Europe
ForeScout

Figure 3 – NotPetya victims globally

These were both attacks that were a result of the Shadow Brokers breach as the breach released dangerous hacking tools that these various malwares were built on top of.

Interestingly, prior to EternalBlue being released into the public domain, Microsoft had already released a patch. However, many systems remained unpatched due to a lack of awareness, complexity of patching and companies not wanting to have downtimes.

Though we do not know exactly how much the Shadow Brokers breach caused the NSA, we know that the implications of the breach eventually led to global losses amounting to tens of billions of dollars.

The Shadow Brokers breach itself was not very impactful on the NSA. However, what followed from the information leaked was extraordinarily devastating and destructive. Its impact and legacy is that of being the precursor to some of the worst cyber-attacks in history.

NSA’s immediate response

Again, we do not know for sure what the NSA’s exact immediate actions were in response to the Shadow Brokers leaks. This is not something that a secretive intelligence agency would readily reveal to the public. However, we can assume that they likely took the following actions.

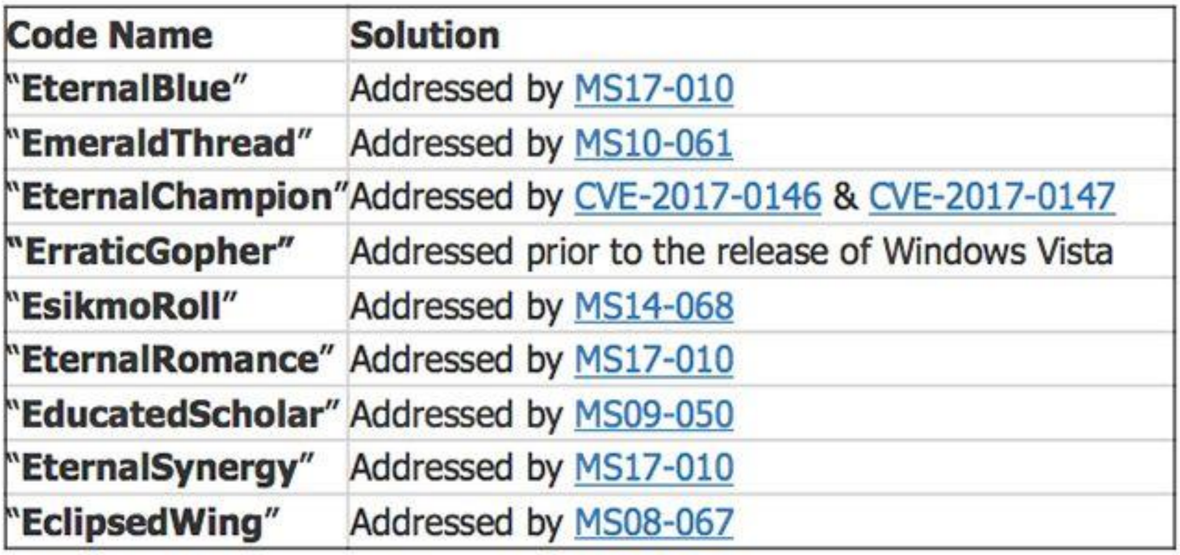
1. Activated their Incident Response Team and Plan
2. Initiated an investigation to determine the extent and cause of the breach including a review of their internal practices and procedures to identify weaknesses that may have contributed to it.
3. Worked with other agencies such as the FBI to investigate the cause of the breach and to coordinate the government’s response.
4. Notified their allies, partners, and the key decision makers within the White House of the breach and the threats of it.
5. Abandoned or scaled down their operations which used the compromised tools and began the development of new tools and techniques.
6. Monitored their systems, to see I the threat actors were still present.

Upon news of the breach, the NSA may have quickly isolated their systems to prevent the theft of more data. If they did manage to find a vulnerability in the system or traces from the attacker, they would also have likely acted swiftly to fix the vulnerability and prevent the attacker from maintaining access or moving laterally among systems.

The above actions would be safe assumptions considering this usually would be the immediate response of most government agencies in response to data breaches. What would differ is in the area of public notification since the NSA is an intelligence agency rather than a public-facing government agency.

The time of their response is also not clear, it could be that the NSA was only made aware of this breach at the same time the public was when Shadow Brokers made their announcement. However, one report claimed that the NSA had been made aware of the breach since 2013 but kept it a secret to avoid damaging trust in the agency to which the NSA has not confirmed or denied. If this were the case, their actions would still likely have been the same as the above but would also include an additional step in trying to prevent this information from being released to the public or to their enemies.

It is also known that Microsoft was aware of the zero-days that were part of the April 2017 leaks much earlier and was able to fix it before the leaks surfaced. However, we do not know for sure how Microsoft came to know of those particular zero-days. Of course, Microsoft could have discovered it independently or may have received this information from other researchers. However, to know and fix pretty much all of the exploits that were included in the April 2017 leaks suggests that Microsoft was likely tipped off either by the Shadow Brokers themselves or the NSA. Why would the Shadow Brokers do such a thing? They may have not wanted to wreak havoc but merely make a statement, which would be likely if they were an insider motivated by only financial gain or political beliefs. However, it is much more likely that it was the NSA who had tipped off Microsoft in an attempt to limit the effects of their exploits once they were released into the wild.



Code Name	Solution
“EternalBlue”	Addressed by MS17-010
“EmeraldThread”	Addressed by MS10-061
“EternalChampion”	Addressed by CVE-2017-0146 & CVE-2017-0147
“ErraticGopher”	Addressed prior to the release of Windows Vista
“EsikmoRoll”	Addressed by MS14-068
“EternalRomance”	Addressed by MS17-010
“EducatedScholar”	Addressed by MS09-050
“EternalSynergy”	Addressed by MS17-010
“EclipsedWing”	Addressed by MS08-067

Figure 4 - Vulnerabilities patched by Microsoft prior to the April 2017 leaks.

NSA’s long-term response

Once again, we can only speculate as to what the NSA’s exact long-term response was and try to use what we know of the NSA to support our speculations. Their long-term response would be different depending on what was the exact root cause.

If the NSA was breached due to an insider, the following would likely be their long-term response:

1. Implement or Enhance their Insider Threat Programs including insider detection and prevention programs.
2. Incorporate Behavior Analytics to monitor employees and detect telltale signs of potential insiders.
3. Conduct even more regular background checks on employees and contractors.
4. Implement Advanced Data Loss Prevention (DLP) solutions to monitor, detect, and prevent the unauthorised exfiltration of sensitive data.

If the NSA was breached due to being the target of an Advanced Persistent Threat (APT) group, the following would likely be their long-term response:

1. Strengthen their attribution capabilities including their threat intelligence of APT groups and nation-state actors.
2. If not done already, air gap critical systems physically or logically to prevent remote access.
3. Improve information sharing with allies and partners.
4. Implement measures to enhance their supply chain security.
5. Improve their incident response and crisis communication plan.

Of course, this is nothing definitive. However, what we know for sure is that the NSA eventually reorganized its cybersecurity operations and created a new cybersecurity centre. The NSA created the Cybersecurity Directorate (CSD), and various other new Directorates and merged the Signals Intelligence Directorate and the Information Assurance Directorate to form the Operations Directorate.

One of the key responsibilities of the CSD is to defend NSA networks by improving its own internal security and bolster collaboration across departments. Overall, the NSA's reorganization aimed to enhance its cyber defence capabilities, conduct cyber intelligence operations, and develop new cybersecurity technologies.

It is unclear whether the reorganization was a direct response to the Shadow Brokers breach or a planned change, but the breach would have significantly influenced the agency's decision to reorganize its cybersecurity operations and likely also accelerated the planning process and led to a swifter implementation.

The NSA also seems to be shifting towards more transparency. In January 2020, the NSA discovered a severe vulnerability in Windows 10 and Server 2016 that could have affected over 900 million PCs, allowing attackers to take control of them. However, instead of practicing zero-day hoarding and weaponizing this exploit like they previously did, they decided to disclose it to Microsoft. Besides disclosing, they also issued public statements and recommendations on actions the public should take. These actions hint that the NSA has learnt from the Shadow Brokers breach and the impact of EternalBlue being leaked. This was likely their attempt to avoid a similar outcome.

The then-head of the newly formed NSA Cybersecurity Directorate Anne Neuberger mentioned that this disclosure was part of a new NSA initiative one where the agency intends to share its vulnerability findings more often and quicker. This effort is part of the Vulnerability Equities Process which is a risk-based approach of weighing the national security importance of keeping hacking tools secret versus disclosing their vulnerabilities. The NSA not only disclosed the vulnerability but made its role public, highlighting their shift in priorities and a step in the right direction.

Analysis & Recommendations

With regards to the NSA's immediate response, the AI recommended that the NSA could have notified not just allies but also those that could be targeted by the leaked exploits (i.e., the public) and worked with vendors affected to remediate the vulnerabilities to prevent future attacks. The NSA could have acted much swifter and alerted Microsoft of the vulnerabilities earlier if they did at all. Besides alerting, they should have worked closely with Microsoft to develop and release the patches such that the public will have more time to apply the patches. After which, they could have also issued public security alerts and guidance to ensure the various organisations and individuals were aware of the risks of these exploits and what they should do. Additionally, it would have been beneficial if they had collaborated with other agencies and industry leaders to develop countermeasures to minimize the impacts of the leaked exploits.

I agree with the AI recommendations. I think the most critically important thing the NSA could have done following the leaks, was to educate the public of the dangers of these exploits and encourage organisations and individuals to patch their systems. The reason this is so critical is because there already existed a patch for the vulnerabilities exploited by NotPetya and WannaCry. However, despite this many systems remain unpatched because many organisations either wanted to avoid downtime, so they decided not to patch yet or because they were not aware of the patch. Had the NSA issued public alerts and warnings, more people would have recognised how important it was to patch their system as soon as possible and would have prioritised it over everything else due to being aware of the dangers of not doing so. With more awareness, less systems would have been vulnerable and therefore the impacts of the malware that originated from the NSA Shadow Brokers leak would have had a much smaller impact and resulted in significantly smaller losses globally.

With regards to the NSA's long-term response, the AI recommended several things. Their best suggestion was that overall, the NSA should not have hoarded so many 'zero-days' and that moving forward they could develop a risk-based approach to exploit disclosure such that they can decide which exploits to disclose and when to disclose them. In addition to this, they should then establish a standard process for disclosing exploits to affected vendors on an organizational and international level. They should have also invested more in 'defensive' security such as securing their networks and systems and the networks and systems of especially critical American and International companies in the interest of national security. In the wake of the breach, they could have also increased transparency by publishing a more detailed report on the breach and the affected parties. Furthermore, the NSA could have developed a more comprehensive plan to identify and mitigate cybersecurity risks including that of a data breach.

I partially disagree with the suggestion of increasing transparency by publishing a more detailed report on the breach. This is because as a national intelligence agency, it would not be in their best interest to inform the public too much about what had happen and this will also expose their operations. However, I only partially disagree because I still believe that the NSA could have at least reported a bit more on the breach. I do, however, completely agree with their suggestion of developing a risk-based approach to exploit disclosure and standardising and institutionalizing practices for responsible disclosure of security vulnerabilities. This would allow them to find a perfect balance between the offensive and defensive aspects of cybersecurity. As mentioned earlier, this also seems to be what the NSA has been doing in recent years. I also agree with the suggestion of the NSA to develop better plans to identify and mitigate risks in the events of data breaches. Had they had better plans, they could have been able to move quicker and minimised the impacts of the breach.

Conclusion

The Shadow Brokers breach, though not the most well-known or documented data breach, resulted in very devastating consequences including two of cyberattacks that could be considered as some of the worst in history, causing tens of billions of dollars in damages. We do not know for sure how the NSA was breached and exactly who it was, but the response of the NSA, as said by many experts, was largely underwhelming and ineffective. However, the future looks bright, with the new reforms in the NSA and their actions in recent years hint that the NSA is moving in the right direction, balancing the two edges of cybersecurity, and increasing their transparency and collaboration. Overall, events such as this emphasises the increasing role data and information plays in our life and the importance of securing it.

Part 4: References

Valentová, A. (2022, February 6). Unveiling the mystery behind one of the most sophisticated hacker groups: Who are The Shadow Brokers?. Security Outlines. Retrieved from https://www.securityoutlines.cz/unveiling-the-mystery-behind-one-of-the-most-sophisticated-hacker-groups-who-are-the-shadow-brokers/

Bleeping Computer. (n.d.). Shadow Brokers Tag. Retrieved from https://www.bleepingcomputer.com/tag/shadow-brokers/

Cyber Law Centre. (2016, August). The Shadow Brokers publishing the NSA vulnerabilities (2016). Retrieved from https://cyberlaw.ccdcoe.org/wiki/The_Shadow_Brokers_publishing_the_NSA_vulnerabilities_(2016)

David, L. (2022, March 18). The NSA Hack, How Did it Happen?. Retrieved from https://www.idstrong.com/sentinel/the-nsa-hack-what-happened-to-nsa/

Wikipedia. (n.d). The Shadow Brokers. Retrieved from https://en.wikipedia.org/wiki/The_Shadow_Brokers

Darknet Diaries. (n.d.). Episode 53 & 54 Transcript. Retrieved from https://darknetdiaries.com/transcript/53/, https://darknetdiaries.com/transcript/54/

Schneier, B. (2017, May 30). Who are the Shadow Brokers? Schneier on Security. Retrieved from https://www.schneier.com/blog/archives/2017/05/who_are_the_sha.html

Joseph, M & John, W. (2016, September 23). Exclusive: Probe of leaked U.S. NSA hacking tools examines operative's 'mistake'. Reuters. Retrieved from https://www.reuters.com/article/us-cyber-nsa-tools-idUSKCN11S2MF

Ms. Smith (2017, April 10). Ticked at President Trump, Shadow Brokers dump password for NSA hacking tools. CSO. Retrieved from https://www.csoonline.com/article/561065/ticked-at-president-trump-shadow-brokers-dump-password-for-nsa-hacking-tools.html

theshadowbrokers (2017, April 8). Don't Forget Your Base. Medium. Retrieved from https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1

Matt, S. (2017, August 17). Shadow Brokers: The insider theory. Medium. Retrieved from https://medium.com/comae/shadowbrokers-the-insider-theory-ded733b39a55#.br7pbm7ar

Matthew, S. (2016, December 20). Report: Shadow Brokers Leaks Trace to NSA Insider. Bank Info Security. Retrieved from https://www.bankinfosecurity.com/report-shadow-brokers-leaks-trace-to-nsa-insider-a-9596

Wikipedia. (n.d). 2017 Shayrat missile strike. Retrieved from https://en.wikipedia.org/wiki/2017_Shayrat_missile_strike

Matan, M. (n.d.). The Long-Term Threats Posed by the Vault 7 Leaks. Cybereason. Retrieved from https://www.cybereason.com/blog/vault-7-leaks-long-term-threats

Taylor, A. (2017, November 15). Shadow Brokers cause ongoing headache for NSA. Sophos. Retrieved from https://news.sophos.com/en-us/2017/11/15/shadow-brokers-cause-ongoing-headache-for-nsa/

Wikipedia. (n.d). DoublePulsar. Retrieved from https://en.wikipedia.org/wiki/DoublePulsar

The Straits Times. (2017, May 16). Singapore malls. Users hit in cyber attack. Retrieved from https://www.straitstimes.com/singapore/global-ransomware-attack-hits-digital-directory-at-tiong-bahru-plaza

Lily, N. (2020, January 14). Windows 10 Has a Security Flaw So Severe the NSA Disclosed It. Wired. Retrieved from https://www.wired.com/story/nsa-windows-10-vulnerability-disclosure/

Figures

Figure 1 - https://blog.surfwatchlabs.com/2017/08/11/theshadowbrokers-continue-to-leak-exploits-and-generate-profits/
Figure 2 - https://www.bbc.com/news/world-39919249
Figure 3 - https://www.forescout.com/company/blog/multibillion-dollar-damage-caused-by-notpetya-and-wannacry-learn-how-forescout-visibility-platform-can-help-address/
Figure 4 - https://www.helpnetsecurity.com/2017/04/15/shadow-brokers-windows-exploits/

~ END ~