# Eternal Blue and the Shadow Brokers

Alex Corak

alex.corak@eagles.ewu.edu
Eastern Washington
University
CSCD 434

***Abstract*—The Shadow Brokers are a foreign hacking group that specifically targeted the NSA in 2017 and got a multitude of extremely powerful tools, including Eternal Blue, the driving force of the most recent surge in ransomware.**

## I. Who are the Shadow Brokers

The Shadow Brokers are known entirely through their actions and their pastebin announcements. No one within the organization itself has been caught or charged, and their location or nationality is also a mystery. Their English is far from perfect, giving it a broken English sound that gives it a distinct sign of translation. Edward Snowden went on record to say there was "circumstantial evidence and conventional wisdom indicates Russian responsibility" [1]. I would add on the surface possibility of the Chinese as well. The Shadow Brokers have also made public statements in reaction to the Russian DNC hacking, claiming they would retaliate on any US counter operation. Between that, and Snowden's thoughts on the matter, it seems they are most likely either a group from Russia, or a government sponsored Russian group. Since they simply released the tools after a failed auction, the former seems more likely. Their name itself is a reference to the 2007 game Mass Effect, to a mysterious information broker that supplies to all sides while keeping themselves on top. This may also rule out the Chinese, as Mass Effect is likely not sold in China due to the content of the game not meeting their strict censorship.

## II. What They Stole

### A. *EternalBlue*

When they announced the sale of their Lost in Translation suite of tools, the crown jewel was EternalBlue. EternalBlue exploits a previously unknown flaw in SMB that targets how they handle certain situations and allows the running of arbitrary code on the infected computer. When the Shadow Broker's auction failed to gather any bids, they released the tools into the wild. EternalBlue became the scariest, as malware using it sprang up everywhere. Explanations of the major malwares using it will come later; but WannaCry uses it as its entry point for the ransomware to take effect and infect the computer. The UIWIX Ransomware, and a cryptocurrency miner also uses it as an entry point, according to analysis done by TrendMicro [3].

### B. *Double Pulsar*

Double Pulsar is a backdoor made in windows machines by the NSA. The man who dissected it, Sean Dillon, claimed it to be "10 times worse than the Heartbleed exploit."[4] Double Pulsar's payload can do four things to a computer it has infected, from secpod's analysis [5]. Firstly, it can respond to a ping request as a heartbeat, to show that it is still alive. The second thing it can do is uninstall itself in order to avoid easy analysis of the malware, both to protect the maker and avoid patches being made. The capability to run any shell code it wants on the infected computer is its third capacity. Finally, it can execute an included DLL on the computer, to do any additional damage or setup. Clearly the last two points are where Double Pulsar becomes truly dangerous. The running of shell code means it can start tampering with anything on your pc, erasing or modifying files, and worse. Being able to execute a DLL that it carried with it is even more dangerous, as that's how ransomware that spread all over the world is setup. Infections of it soared in the weeks after it was released, and all sorts of malware used it, including the previously mentioned ransomware, and crypto miners.

### C. *Exploding Can*

Exploding Can is less world changing than EternalBlue, but it still has some dangers. It is an exploit of Windows Server 2003, which is still ran on some 42 thousand machines across the world [6]. What is interesting about this exploit is that with the others, despite the age of

their targets, they've had security patches to fix the holes in security. However, with this version of Windows Server, Microsoft has decided it isn't worth fixing. So any machines running Windows Server 2003 will continue to have a massive backdoor in them, which could be troubling for any low budget government organization that has anything of value on those servers.

### *D. EchoWrecker*

EchoWrecker is an exploit specifically for Samba 3.0.x on linux. Samba is a software suite that is cross-compatible with both linux and windows. It runs as a sort of mail server with SMB, and that is likely what EchoWrecker targets, as some of the leaked tools use this.

### *E. The Rest*

This list comes from a post on medium.com's tech section [7]. As far as I can find, these are most of them with accurate descriptions.

EARLYSHOVEL RedHat 7.0–7.1 Sendmail 8.11.x exploit

EBBISLAND (EBBSHAVE) root RCE via RPC XDR overflow in Solaris 6, 7, 8, 9 & 10 (possibly newer) both SPARC and x86.

ECHOWRECKER remote Samba 3.0.x Linux exploit.

EASYBEE appears to be an MDaemon email server vulnerability

EASYFUN EasyFun 2.2.0 Exploit for WDaemon / IIS MDaemon/WorldClient pre 9.5.6

EASYPI is an IBM Lotus Notes exploit that gets detected as Stuxnet

EWOKFRENZY is an exploit for IBM Lotus Domino 6.5.4 & 7.0.2

ETERNALROMANCE is a SMB1 exploit over TCP port 445 which targets XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2, and gives SYSTEM privileges (MS17–010)

EDUCATEDSCHOLAR is a SMB exploit (MS09–050)

EMERALDTHREAD is a SMB exploit for Windows XP and Server 2003 (MS10–061)

EMPHASISMINE is a remote IMAP exploit for IBM Lotus Domino 6.6.4 to 8.5.2

ENGLISHMANSDENTIST sets Outlook Exchange WebAccess rules to trigger executable code on the client's side to send an email to other users

EPICHERO 0-day exploit (RCE) for Avaya Call Server

ERRATICGOPHER is a SMBv1 exploit targeting Windows XP and Server 2003

ETERNALSYNERGY is a SMBv3 remote code execution flaw for Windows 8 and Server 2012 SP0 (MS17–010)

ETERNALCHAMPION is a SMBv1 exploit

ESKIMOROLL is a Kerberos exploit targeting 2000, 2003, 2008 and 2008 R2 domain controllers

ESTEEMAUDIT is an RDP exploit and backdoor for Windows Server 2003

ECLIPSEDWING is an RCE exploit for the Server service in Windows Server 2008 and later (MS08–067)

ETRE is an exploit for IMail 8.10 to 8.22

ETCETERABLUE is an exploit for IMail 7.04 to 8.05

FUZZBUNCH is an exploit framework, similar to MetaSploit

ODDJOB is an implant builder and C&C server that can deliver exploits for Windows 2000 and later, also not detected by any AV vendors

EXPIREDPAYCHECK: IIS6 exploit

EAGERLEVER NBT/SMB exploit for Windows NT4.0, 2000, XP SP1 & SP2, 2003 SP1 & Base Release

EASYFUN WordClient / IIS6.0 exploit

EPICBANNANA Cli code execution for Cisco ASA

EXTRABACON SNMP Remote code execution for multiple cisco services

## III. How They Did It

Prior to 2017, Harold Martin was a former Navy vet, and pursuing a PH.D in computer science. In 2017 he stole 50 terabytes of data from the NSA, and a twitter accounted linked to him, messaged Kapersky labs, and the shadow brokers

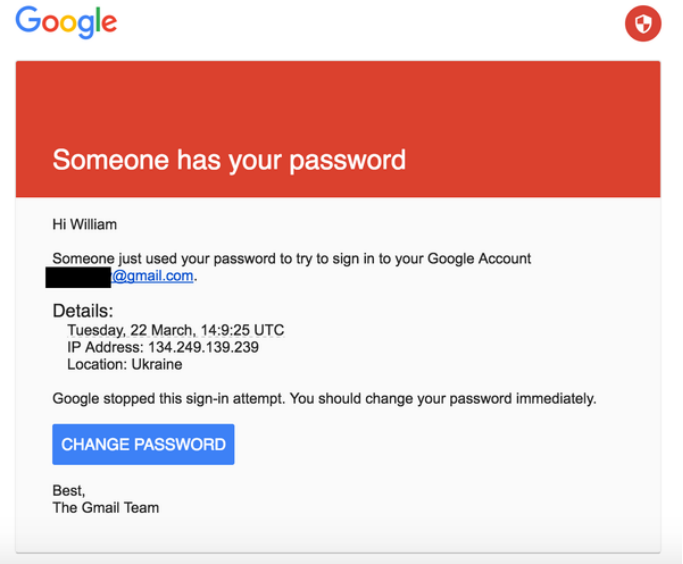
directly, and 30 minutes later, the tools were released. Now, in March of 2019, he has pled guilty to 20 counts of unauthorized and willful retention of national defense information. The case has been followed closely by cyberscoop, who also point to the "rash of NSA contractors being charged" in the 2 years since the Shadow Broker attack [8]. His home was raided for the data in late 2016 by the police. While the US Government has not made the ties with the Shadow Brokers part of the case, it has been "long been tied" [8] to the attacks. So the question of how they did it, could be partly attributed to an inside man leaking the data for them.

### A. *Just an inside job?*

Details on whether those physically stolen files were all that the attack contained are hard to find. Some sources, like RiskBased Security, claim that all the tools are freely available, most likely to contractors [9]. While Cisco confirmed that two exploits, EPICBANANA and EXTRABACON are legitimate [10]. The internal turmoil inside the NSA afterwards proves in my mind that these tools are of their making. We'll likely never know exactly what happened unless the Shadow Brokers tell us.

### B. *Russias History of Hacking the US*

According to a New York Times article about the use of Russian cyber firepower, the DNC was compromised by a group called the Dukes as early as 2015. When the FBI were informed, they responded with an unnerving "we know [11]". The time between the weak FBI response and the DNC hiring cybersecurity experts to help them was a full seven months. The chief of the US Cyber Command was quoted saying "This was a conscious effort by a nation-state to attempt to achieve a specific effect," [11], operations have been continuing since then.




*The phishing email that got into the DNC.*

### C. *The NSA's reaction to the attack*

The cybersecurity community at large has focused entirely on the tools and what hackers have been doing with them. However, the internal reaction within the NSA has larger impacts on continual national security and whether America will continue to be a victim of politically fueled hacking attacks and leaks. Another New York Times article did a deep dive into the organization's response. The Shadow Brokers had approached and mocked a man attached to the Tailored Access Operations division of the NSA, the place the tools originated. Even worse for this employee, they knew of classified operations they had operated on. Obviously, the secrecy of their tools is the critical piece of if they can do their job. With a massive suite of the NSA's tools exposed, they're ability to continue doing their job became extremely difficult. Especially with most exploits being immediately patched by Microsoft and other companies whose software is affected. The reputation of the NSA is also being destroyed on an international scale. After privately explaining the breach and apologizing to each company affected by malware created with their tools. Internal arguments have been raging within the NSA since the attacks. A senior official was quoted within the article saying "We've got extraordinary capabilities, and it's a huge responsibility to manage them on behalf of the nation, [12]" showing the internal

questioning about their power both within the building and within the nation.

## IV. What the Tools Became

In the rest of 2017 the world at large became familiar with a new type of malware, one that held victims hostage until a ransom was paid. Ransomware swooped into media coverage and the populace's mind after Wannacry and NotPetya were taking over millions of computers and affecting critical systems like the NHS in the United Kingdom and Eastern Europe respectively. These two swept through the world as well, as Wannacry infected 200,000 machines until the kill switch was discovered inside the code. The common thread between these two ransomwares was that they were made possible by the power of EternalBlue and the Shadow Brokers robbery of the NSA's tools.

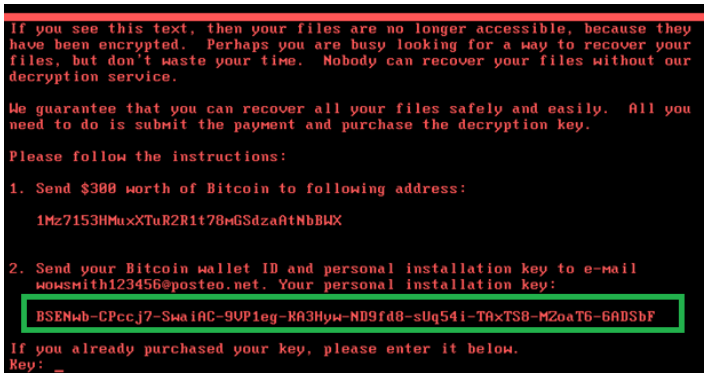
### A. *Wannacry Attacks*

In May of 2017, Wannacry began a worldwide attack, spreading rapidly on un-updated windows machines. These machines were commonly businesses that didn't update to avoid having conflicts with their other systems but ended up costing them. Within a few days Wannacry had spread to the previously mentioned peak before a researcher discovered the kill switch. The kill switch checked a specific domain that was not yet registered, and if it was registered it would stop. He registered it himself, and sure enough, the spread of the malware stopped. According to the researcher "the domain should [have been] random so people can't register it," the implementation was incorrect [13].


*The screen Wannacry displays after infection.*

### B. *NotPetya*

NotPetya targeted all over Ukraine on the 2017 anniversary of Constitution Day, the day the Ukrainian government adopted their constitution. This immediately made it seem like a politically motivated attack, but it seemed to spread indiscriminately. All of Europe was attacked, as Kaspersky Labs reported, but Russia and Ukraine were the main targets [14]. What is interesting about its targets were that they mainly hit infrastructure; airports, power grids, and banks. Unlike WannaCry's poor implementation of their kill switch, NotPetya's uses a proper AES-128-bit encryption and seemed solid to Kaspersky. A later release by them gave insight into another interesting facet of NotPetya's operation. First it had made over 6,000 dollars in the first few days, but it was a "wiper" [15], software that simply encrypts it and leaves it there. It never decrypts after receiving payment, seemingly pretending to be ransomware for either media coverage and attention, or maybe as just something to make some money on top of wiping systems.



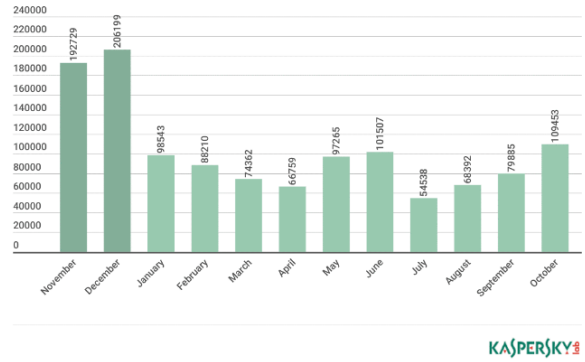

*The screen NotPetya shows after encrypting all system files.*

This makes NotPetya a different classification than just money making obviously. Whether it's an attack by another nation will be a mystery for another time. My thoughts are that it was some sort of cyber terrorism against Ukraine specifically as they had 80% of the infections while it began on a pro-government holiday. Since it attacked Russia too, and the rest of Europe I don't think it was state sponsored. It did no damage in Russia, so it could have been designed so that it infected Russian machines but

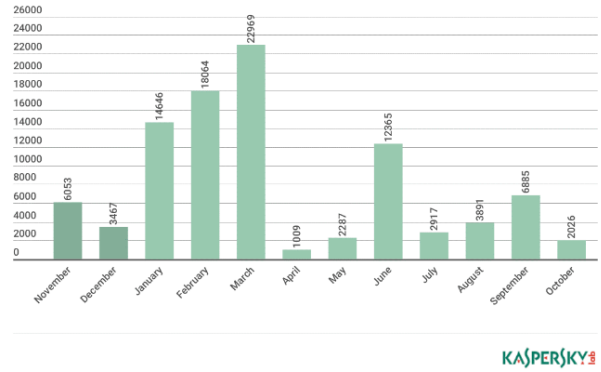
did no real damage, avoiding suspicion. However, this is all just conjecture.

### *V. Malware Trends*

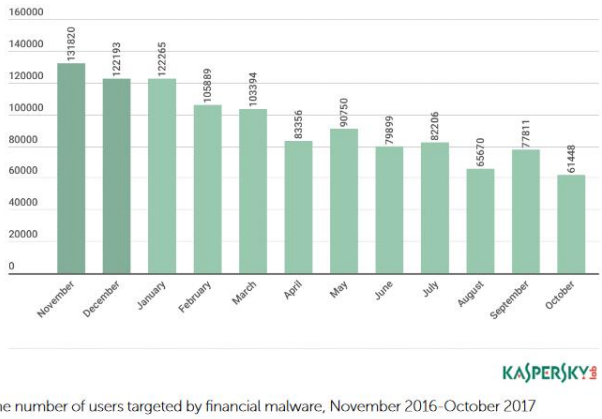
Kapserky reported in 2017, 939 722 unique KSN users were attacked by encryptors, including more than 240 thousand corporate users [16]. 2017 was defined by the large attacks that these malware enabled, with the rise of encryptors (ransomware).




Number of users attacked by crypto-ransomware (November 2016 – October 2017)




Number of new crypto-ransomware modifications, November 2016 – October 2017




The number of users targeted by financial malware, November 2016-October 2017

The most interesting part of the new ransomware modifications graph is how in the months of and following the leaking of tools the new types of these malwares coming out plummeted. The likeliest cause for this is that all the attacks in those months were caused by Wannacry, and in the months after May, new malwares had been finished implementing these tools. June is also when the forms of NotPetya emerged, and its variations as well.

Another important trend that has been coming to light more and more is what Barkly, a threat management company, called "clickless infection," with the use of EternalBlue [17]. Traditionally, viruses came from mistakes on users ends, and most people using computers know not to click on obviously dangerous things like scam emails or malicious ads. If the weaker users of computers like the elderly still struggle with those concepts, being able to be infected without clicking on anything wrong will further frustrate them and require more training to all who only regularly use computers for their work.

The Shadow Brokers are a group of hackers, likely from Russia, that broke into the NSA and stole very powerful tools. They did this with a distinctly likely insider within the organization giving them the information. The sheer number of powerful tools stolen are staggering and led directly to two of the biggest malware attacks in recent memory, shutting down everything from personal computers to government organizations and infrastructure. The rise of ransomware and clickless infections into both the public eye and the eyes of corporations is directly connected to that theft, and numerous other malwares sprung up because of it. No one has been directly arrested for the crime, and the NSA has been thrown into a new series of scrutiny and debate on whether any group should operate with tools that powerful, let alone allow them to escape the building.


[1] https://twitter.com/Snowden/status/765513662597623808

[2] https://blog.trendmicro.com/trendlabs-security-intelligence/ms17-010-eternalblue/

[3] https://blog.trendmicro.com/trendlabs-security-intelligence/ms17-010-eternalblue/

[4] https://en.wikipedia.org/wiki/DoublePulsar

[5] https://www.secpod.com/blog/doublepulsar-a-very-sophisticated-payload-for-windows/

[6] https://www.itnews.com.au/news/exploding can-nsa-exploit-menaces-thousands-of-servers-463985/

[7] https://medium.com/techietalks/security-is-just-an-illusion-7dbfcd2a782d

[8] https://www.cyberscoop.com/harold-martin-guilty-plea-nsa-shadow-brokers/

[9] https://www.wired.co.uk/article/nsa-hacking-tools-stolen-hackers

[10] https://blogs.cisco.com/security/shadow-brokers

[11] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

[12] https://cyber-peace.org/wp-content/uploads/2017/05/NSA-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose.-Then-it-did.pdf

[13] https://www.wired.com/2017/05/accidental-kill-switch-slowed-fridays-massive-ransomware-attack/

[14] https://securelist.com/schroedingers-petya/78870/

[15] https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

[16] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07164706/KSB_statistics_2017_EN_final.pdf

[17] https://cdn2.hubspot.net/hubfs/468115/eBooks/2017-malware-trends-review/barkly-ebooks-2017-malware-trends-review-0917.pdf