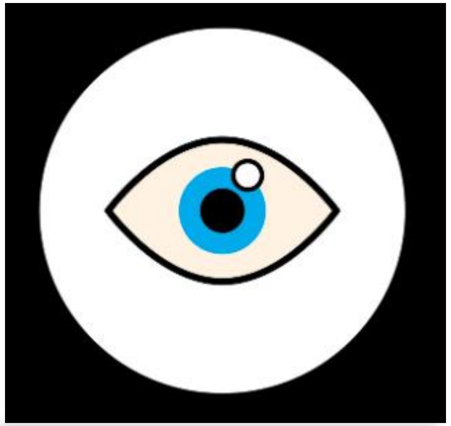


EternalBlue

One of the most potent exploits ever seen!

IST 623 – Introduction to Information Security
Case Study Presentation
2/25/2020

Team: Group 2

- Samantha Brennen-Lisko
- Assadour Derderian
- Rose Ochoa
- Nicolas Reyes
- Ryan Timbrook

Case Summary

- Per NY Times: “Since 2017, when the N.S.A. lost control of the tool, EternalBlue.
- It has been picked up by state hackers in North Korea, Russia and, more recently, China, to cut a path of destruction around the world, leaving billions of dollars in damage.”
- Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid.
- Although ransomware aims at individuals, it also caters to Institutions for financial profit.

Origination

- The National Security Agency discovered vulnerabilities in Microsoft's system that could be used as an exploitation device but did not notify Microsoft until a breach had occurred.
- Microsoft then created a patch to fix the vulnerabilities but not in enough time for widespread affect before attack was carried out.
- A group of hackers known as **Shadow Brokers** were able to obtain information from the NSA regarding the vulnerabilities.
- The **Shadow Brokers** group then released the secrets on the internet which were then picked up by such groups who created the **WannaCry** ransomware attack which targeted systems across the globe.

Victims

- Governments
- Businesses
- Constituents
- Possibly Critical Information

Question & Answer

EternalBlue – Case Summary - Victims

Mechanism of attack

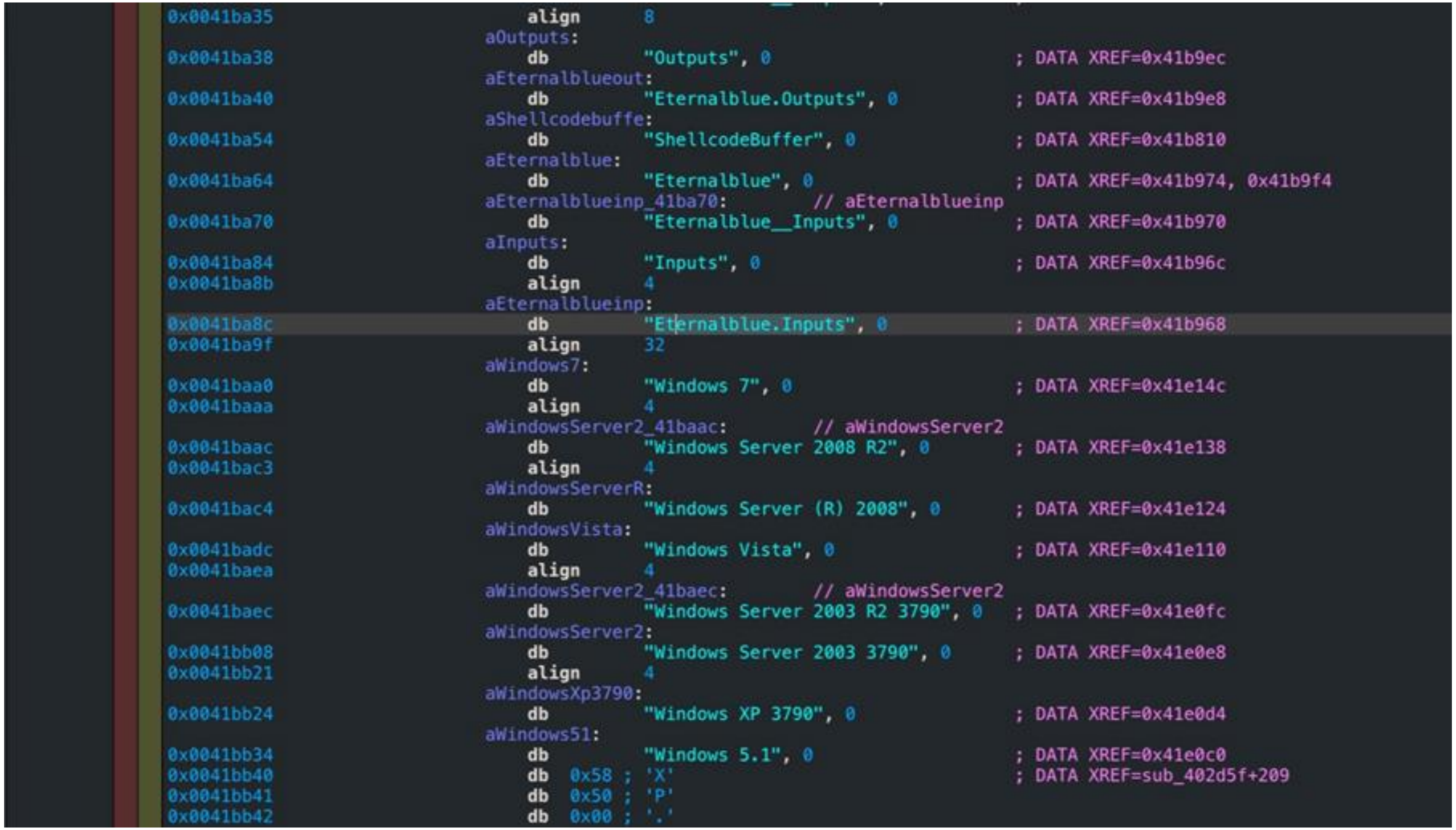
- EternalBlue exploited “vulnerabilities in the windows implementation of Windows Server Message Block protocol.”

- Three bugs were exploited

- Once the attacker takes control of the system, they can use a multi-layered encryption approach to encrypt a victim’s files and hold them for ransom.

- Unpatched systems are still vulnerable to this day.

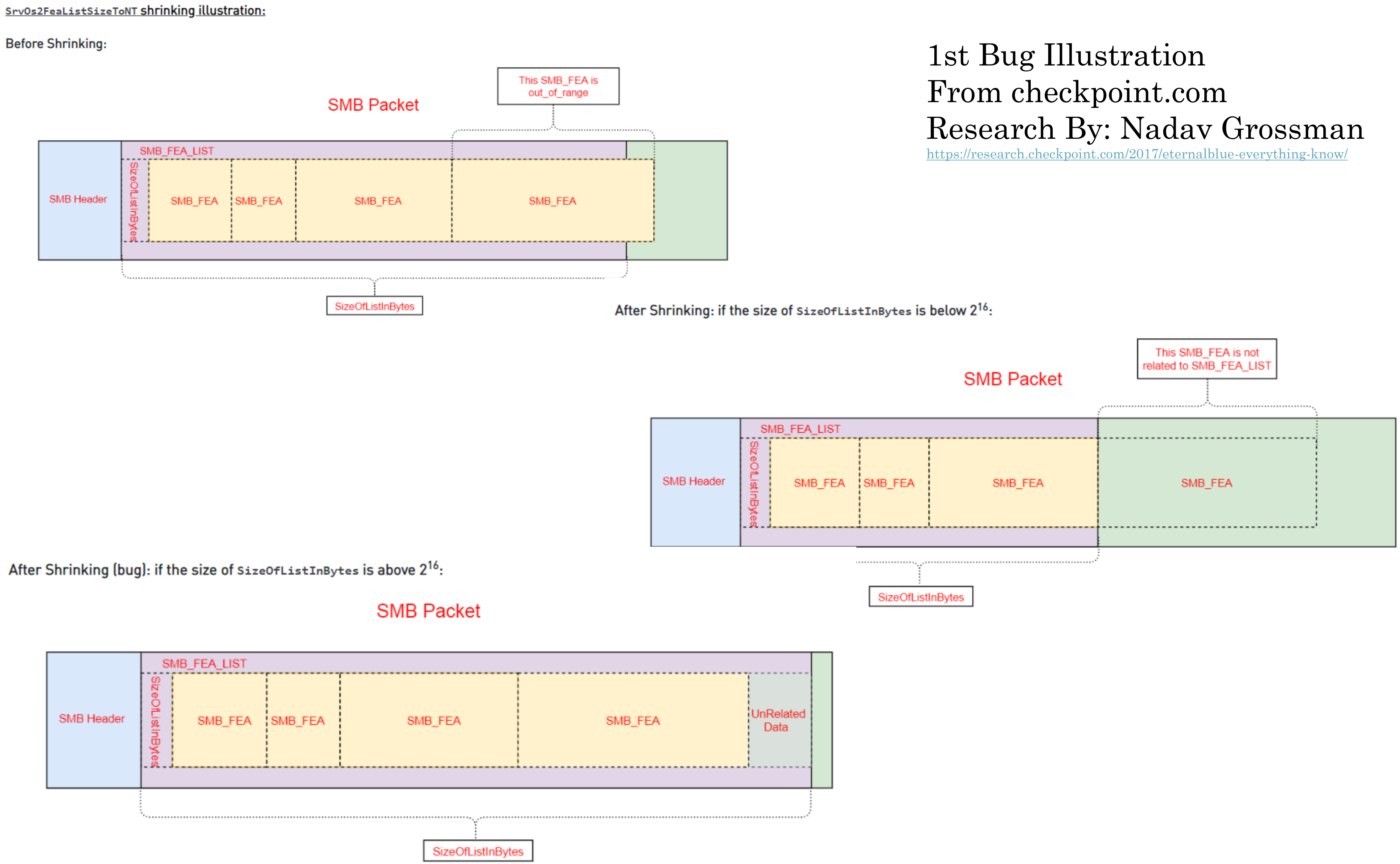
[1]Vulnerable Windows Systems:



```
0x0041ba35                align      8
                      aOutputs:
0x0041ba38                db         "Outputs", 0                      ; DATA XREF=0x41b9ec
                      aEternalblueout:
0x0041ba40                db         "Eternalblue.Outputs", 0          ; DATA XREF=0x41b9e8
                      aShellcodebuffe:
0x0041ba54                db         "ShellcodeBuffer", 0              ; DATA XREF=0x41b810
                      aEternalblue:
0x0041ba64                db         "Eternalblue", 0                  ; DATA XREF=0x41b974, 0x41b9f4
                      aEternalblueinp_41ba70:        // aEternalblueinp
0x0041ba70                db         "Eternalblue__Inputs", 0          ; DATA XREF=0x41b970
                      aInputs:
0x0041ba84                db         "Inputs", 0                       ; DATA XREF=0x41b96c
0x0041ba8b                align      4
                      aEternalblueinp:
0x0041ba8c                db         "Eternalblue.Inputs", 0           ; DATA XREF=0x41b968
0x0041ba9f                align      32
                      aWindows7:
0x0041baa0                db         "Windows 7", 0                    ; DATA XREF=0x41e14c
0x0041baaa                align      4
                      aWindowsServer2_41baac:        // aWindowsServer2
0x0041baac                db         "Windows Server 2008 R2", 0       ; DATA XREF=0x41e138
0x0041bac3                align      4
                      aWindowsServerR:
0x0041bac4                db         "Windows Server (R) 2008", 0      ; DATA XREF=0x41e124
                      aWindowsVista:
0x0041badc                db         "Windows Vista", 0                ; DATA XREF=0x41e110
0x0041baea                align      4
                      aWindowsServer2_41baec:        // aWindowsServer2
0x0041baec                db         "Windows Server 2003 R2 3790", 0  ; DATA XREF=0x41e0fc
                      aWindowsServer2:
0x0041bb08                db         "Windows Server 2003 3790", 0     ; DATA XREF=0x41e0e8
0x0041bb21                align      4
                      aWindowsXp3790:
0x0041bb24                db         "Windows XP 3790", 0              ; DATA XREF=0x41e0d4
                      aWindows51:
0x0041bb34                db         "Windows 5.1", 0                  ; DATA XREF=0x41e0c0
0x0041bb40                db   0x58 ; 'X'                              ; DATA XREF=sub_402d5f+209
0x0041bb41                db   0x50 ; 'P'
0x0041bb42                db   0x00 ; '.'
```

1st Bug Illustration
From checkpoint.com
Research By: Nadav Grossman

https://research.checkpoint.com/2017/eternalblue-everything-know/

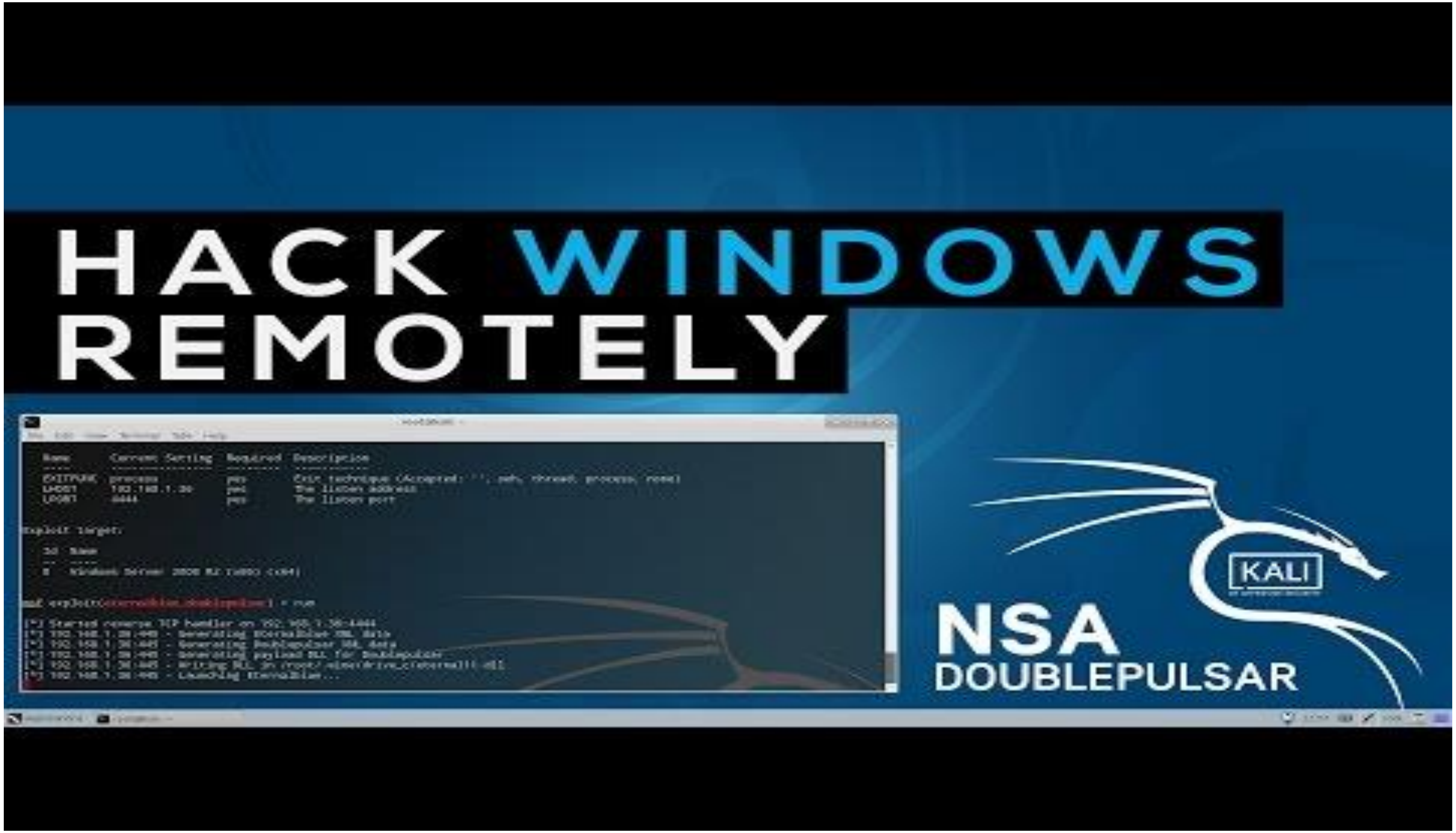


`SrvOs2FeaListSizeToNT` shrinking illustration:

Before Shrinking:

After Shrinking: if the size of `SizeOfListInBytes` is below 2^{16}:

After Shrinking (bug): if the size of `SizeOfListInBytes` is above 2^{16}:



```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.30     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Server 2008 R2 (x86) (x64)


msf exploit(eternalblue_doublepulsar) > run

[*] Started reverse TCP handler on 192.168.1.30:4444
[*] 192.168.1.30:445 - Generating Eternalblue XML data
[*] 192.168.1.30:445 - Generating Doublepulsar XML data
[*] 192.168.1.30:445 - Generating payload DLL for Doublepulsar
[*] 192.168.1.30:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.1.30:445 - Launching Eternalblue...
```

Hack Windows 7 Remotely Using DOUBLEPULSAR — NSA Hacking Tool
Video by: ArcaneHacks

Question & Answer

EternalBlue – Mechanism of Attack

Fallout

- Affected over an estimated 500,000 computers across 150 countries in 2017.
- Estimated damage range from hundreds of millions to billions of dollars for businesses and governments
  - Cybercriminals asked for 13 bitcoins ($113,000) from Balitmore authorities
- Governments had to pay to get data back
  - Baltimore decided not to pay Wannacry – had to pay $18 million
  - Citizens now pose the question, "should the government be responsible and liable to cover the costs of damages just like any other war/military or state-created weapon?"
  - No such thing as a *safe* cyber weapon
  - Active war – not an act for profit, but more of resent
- Buy/replace new IT equipment
  - Even after purchasing data back, they need to cover the software damages to take care of virus in devices
    - Users had to update their programs and system for patch updates
- Public fear that their data is not safe/secure anymore

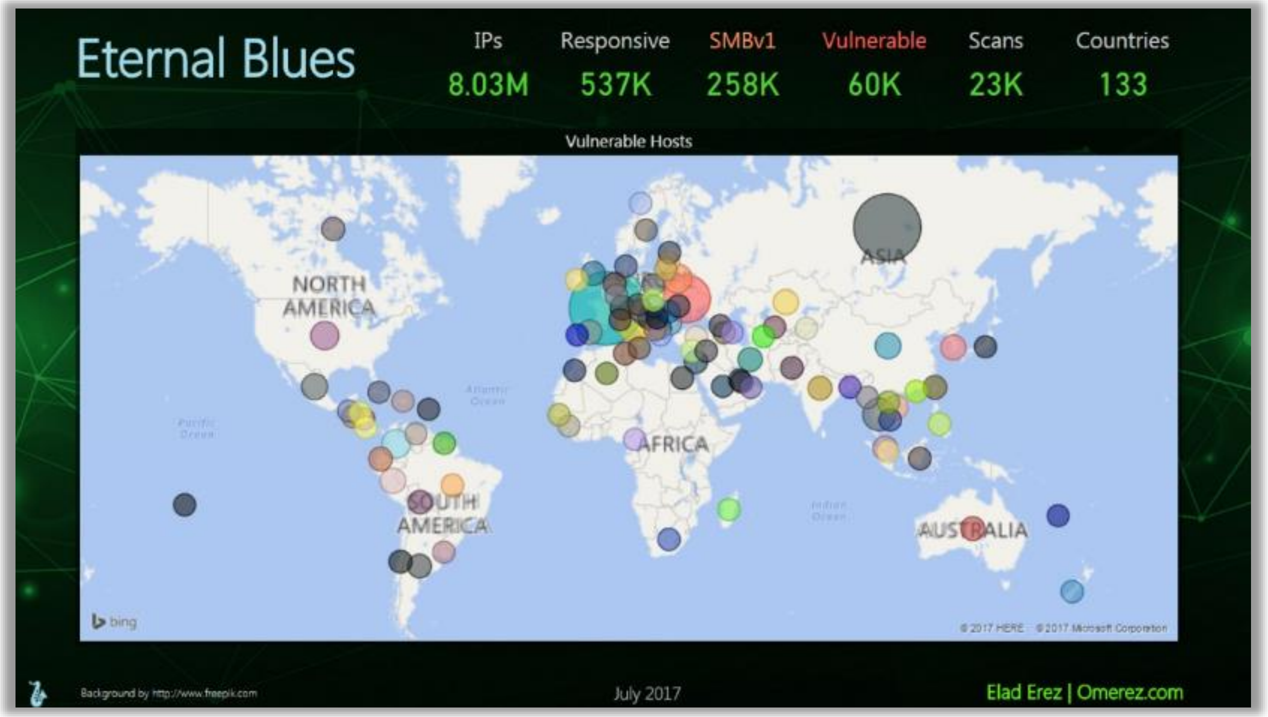
Eternal Blues Scan Statistics

- Eternal Blues app found more than 50,000 vulnerable computers around the world in the past two weeks, since official release date

- Users scanned over **eight million IPs**
- **53.8%** of scanned hosts still had the **SMBv1** protocol **enabled**
- **Most** had applied MS17-010 patch, leaving 50,000 still vulnerable

"Eternal Blues" Tool Tests Computers Against NSA's ETERNALBLUE Exploit

By Catalin Cimpanu June 30, 2017 03:56 PM

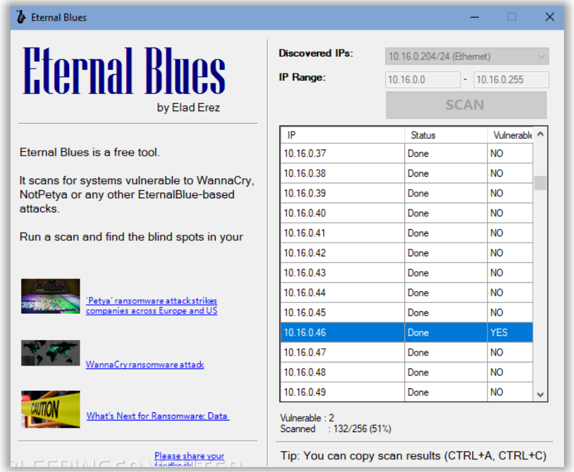


Eternal Blues

IPs	Responsive	SMBv1	Vulnerable	Scans	Countries
8.03M	537K	258K	60K	23K	133

Vulnerable Hosts

Background by http://www.freepik.com July 2017 Elad Erez | Omerez.com



Eternal Blues

Eternal Blues
by Elad Erez

Eternal Blues is a free tool.

It scans for systems vulnerable to WannaCry, NotPetya or any other EternalBlue-based attacks.

Run a scan and find the blind spots in your

'Petya' ransomware attack strikes companies across Europe and US

WannaCry ransomware attack

What's Next for Ransomware: Data

Please share your feedback!

Discovered IPs: 10.16.0.204/24 (Ethernet)

IP Range: 10.16.0.0 - 10.16.0.255

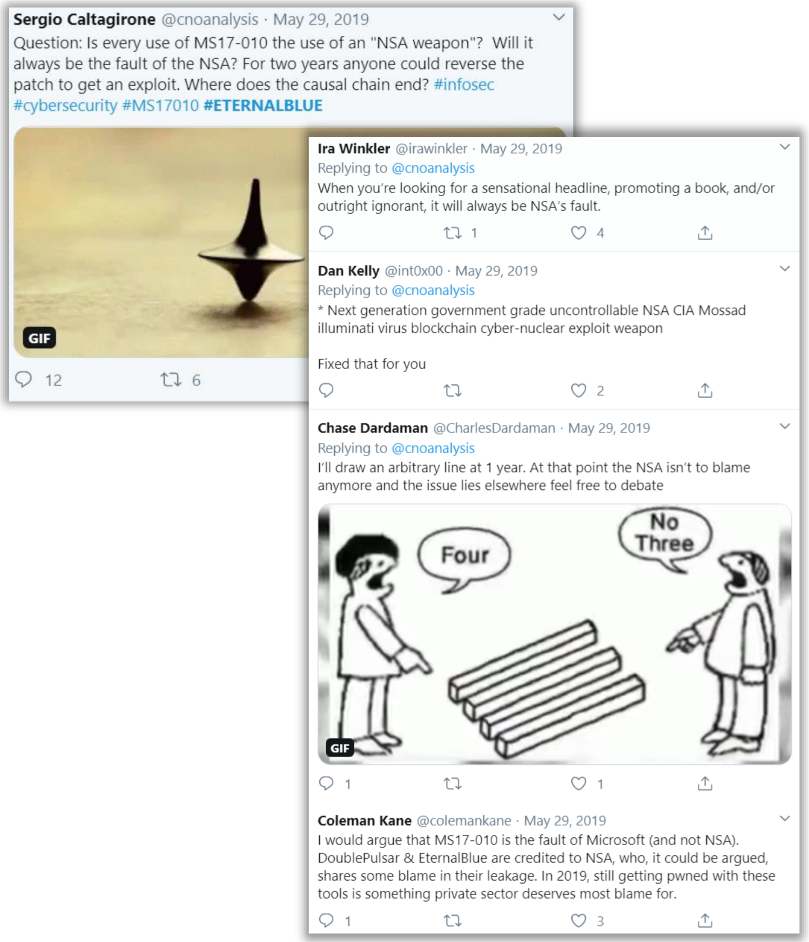
IP	Status	Vulnerable
10.16.0.37	Done	NO
10.16.0.38	Done	NO
10.16.0.39	Done	NO
10.16.0.40	Done	NO
10.16.0.41	Done	NO
10.16.0.42	Done	NO
10.16.0.43	Done	NO
10.16.0.44	Done	NO
10.16.0.45	Done	NO
10.16.0.46	Done	YES
10.16.0.47	Done	NO
10.16.0.48	Done	NO
10.16.0.49	Done	NO

Vulnerable : 2
Scanned : 132/256 (51%)

Tip: You can copy scan results (CTRL+A, CTRL+C)

*"Security researcher Elad Erez has created a tool named Eternal Blues that system administrators can use to test if computers on their network are **vulnerable to exploitation** via NSA's ETERNALBLUE exploit. Erez released his tool on **Wednesday, a dafter the NotPetya ransomware** caused damages to thousands of computers across the globe." – BleepingComputer.com*

Social Media Clippings



Sergio Caltagirone @cnoanalysis · May 29, 2019

Question: Is every use of MS17-010 the use of an "NSA weapon"? Will it always be the fault of the NSA? For two years anyone could reverse the patch to get an exploit. Where does the causal chain end? #infosec #cybersecurity #MS17010 **#ETERNALBLUE**

Ira Winkler @irawinkler · May 29, 2019

Replying to @cnoanalysis

When you're looking for a sensational headline, promoting a book, and/or outright ignorant, it will always be NSA's fault.

Dan Kelly @int0x00 · May 29, 2019

Replying to @cnoanalysis

* Next generation government grade uncontrollable NSA CIA Mossad illuminati virus blockchain cyber-nuclear exploit weapon

Fixed that for you

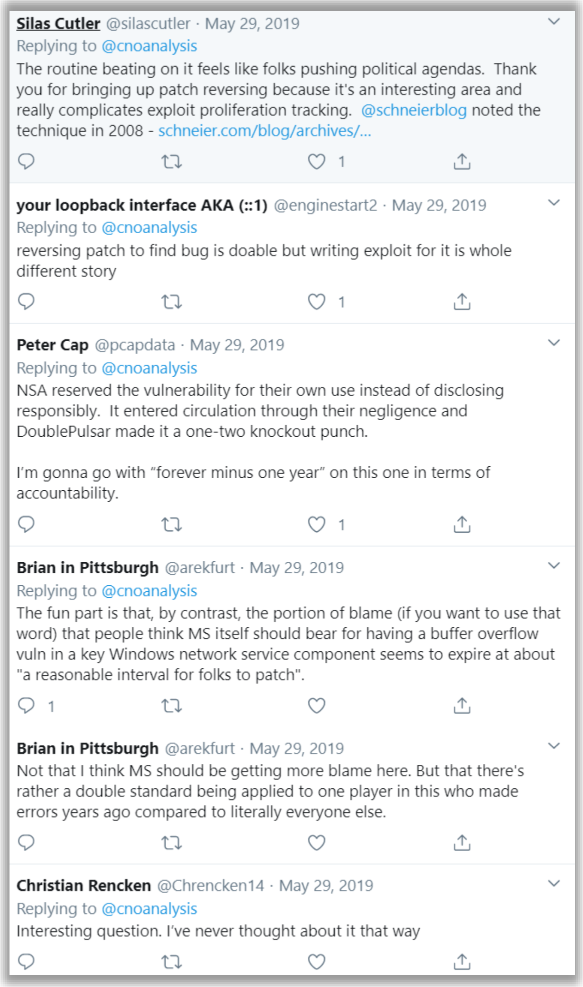
Chase Dardaman @CharlesDardaman · May 29, 2019

Replying to @cnoanalysis

I'll draw an arbitrary line at 1 year. At that point the NSA isn't to blame anymore and the issue lies elsewhere feel free to debate

Coleman Kane @colemankane · May 29, 2019

I would argue that MS17-010 is the fault of Microsoft (and not NSA). DoublePulsar & EternalBlue are credited to NSA, who, it could be argued, shares some blame in their leakage. In 2019, still getting pwned with these tools is something private sector deserves most blame for.



Silas Cutler @silascutler · May 29, 2019

Replying to @cnoanalysis

The routine beating on it feels like folks pushing political agendas. Thank you for bringing up patch reversing because it's an interesting area and really complicates exploit proliferation tracking. @schneierblog noted the technique in 2008 - schneier.com/blog/archives/...

your loopback interface AKA (::1) @enginestart2 · May 29, 2019

Replying to @cnoanalysis

reversing patch to find bug is doable but writing exploit for it is whole different story

Peter Cap @pcapdata · May 29, 2019

Replying to @cnoanalysis

NSA reserved the vulnerability for their own use instead of disclosing responsibly. It entered circulation through their negligence and DoublePulsar made it a one-two knockout punch.

I'm gonna go with "forever minus one year" on this one in terms of accountability.

Brian in Pittsburgh @arekfurt · May 29, 2019

Replying to @cnoanalysis

The fun part is that, by contrast, the portion of blame (if you want to use that word) that people think MS itself should bear for having a buffer overflow vuln in a key Windows network service component seems to expire at about "a reasonable interval for folks to patch".

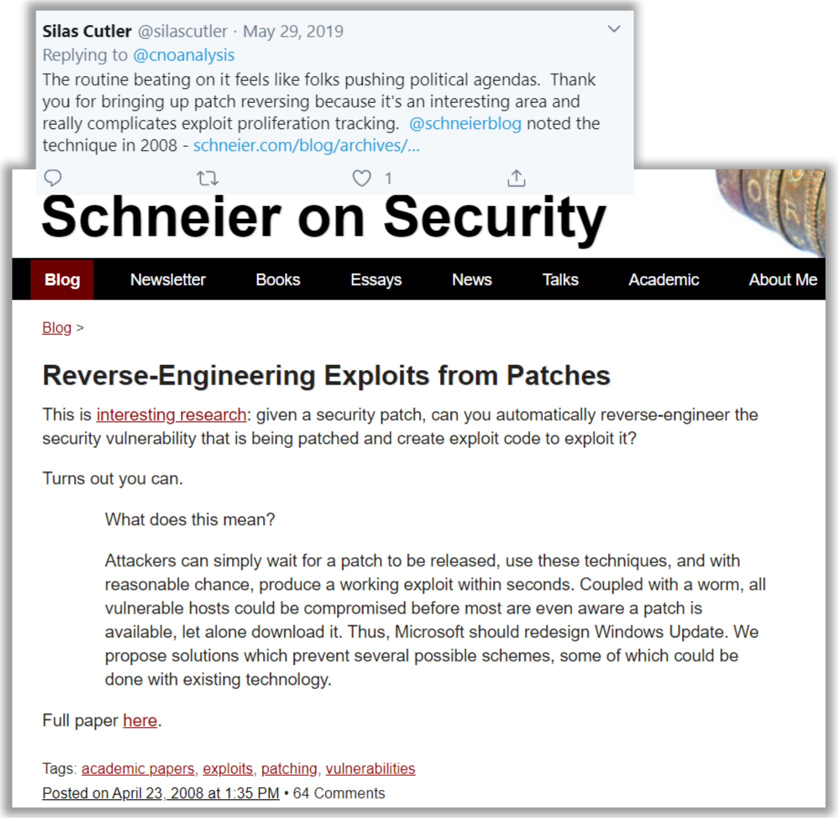
Brian in Pittsburgh @arekfurt · May 29, 2019

Not that I think MS should be getting more blame here. But that there's rather a double standard being applied to one player in this who made errors years ago compared to literally everyone else.

Christian Rencken @Chrencken14 · May 29, 2019

Replying to @cnoanalysis

Interesting question. I've never thought about it that way



Silas Cutler @silascutler · May 29, 2019

Replying to @cnoanalysis

The routine beating on it feels like folks pushing political agendas. Thank you for bringing up patch reversing because it's an interesting area and really complicates exploit proliferation tracking. @schneierblog noted the technique in 2008 - schneier.com/blog/archives/...

Schneier on Security

Blog >

Reverse-Engineering Exploits from Patches

This is interesting research: given a security patch, can you automatically reverse-engineer the security vulnerability that is being patched and create exploit code to exploit it?

Turns out you can.

> What does this mean?
>
> Attackers can simply wait for a patch to be released, use these techniques, and with reasonable chance, produce a working exploit within seconds. Coupled with a worm, all vulnerable hosts could be compromised before most are even aware a patch is available, let alone download it. Thus, Microsoft should redesign Windows Update. We propose solutions which prevent several possible schemes, some of which could be done with existing technology.

Full paper here.

Tags: academic papers, exploits, patching, vulnerabilities

Posted on April 23, 2008 at 1:35 PM • 64 Comments

Question & Answer

EternalBlue - Fallout

Texas

- 22 cities or counties hit in single attack, Federal Investigation [4,5]

- Keene, TX [4,5]
  - No Credit Card payments
  - No Utility payments
  - Analog
  - Ransom demand $2.5 million
  - State IT Dept. Restoring

- Lubbock County, TX [5]
  - Lubbock's IT department isolate the ransomware before it spread
  - Infected computer, not network

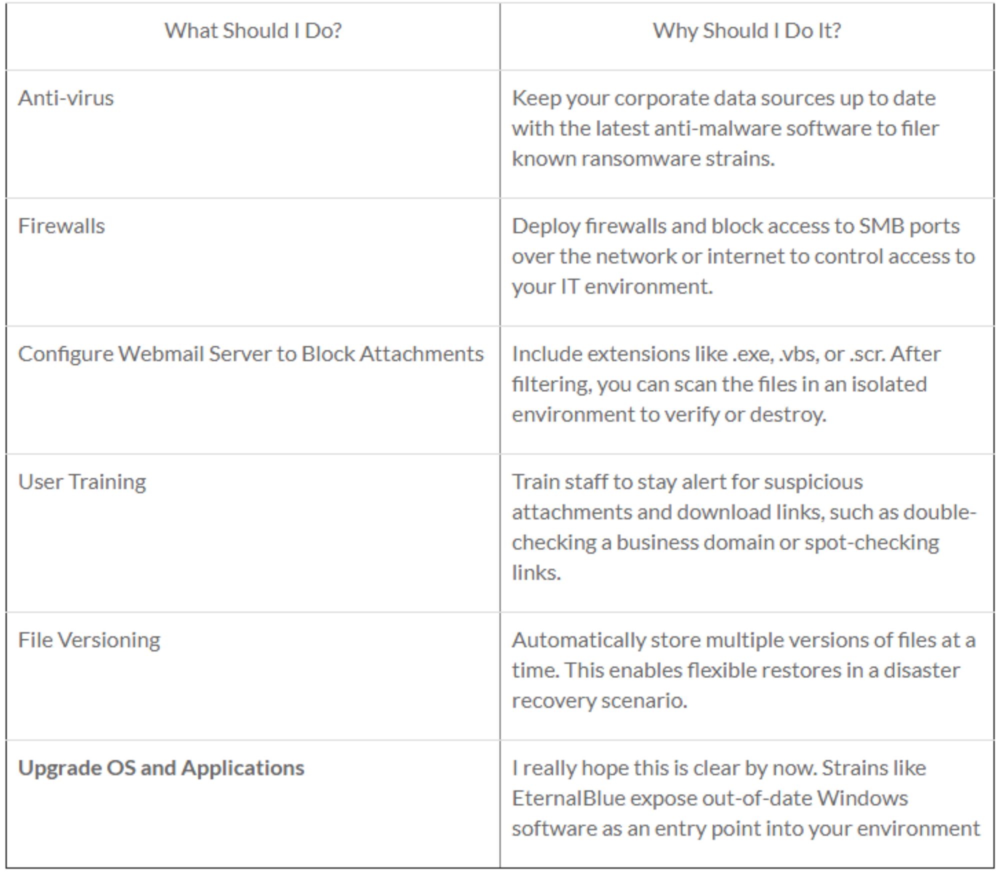
Florida

- Lake City, FL [6]
  - Paid $485,000 in bitcoin (Insurance paid all but $10,000)
  - Hackers: control phone and email system
  - Emergency system not effected
    - Phone calls rerouted through emegency system: no delays to emergency calls
  - Key received: some emails restored, many inoperable
  - Adding training

- Marion County, FL [6]
  - 2 computers infected
  - No important information was jeopardized
  - Increased cyber security and
  - Developed counter measures.

How to Protect Against EternalBlue

- EternalBlue **exploits** a **vulnerability** in **outdated** versions of **Microsoft Server Message Block**.
  - Only known mechanism to protect against EternalBlue is to download the **latest Windows** software **update** and install the **patch**.
  - Additionally, ensure that the following **safeguards** are in place:
    - **Anti-virus** software
    - Secure **offsite backup** with "attack-loop" prevention
    - **Filter** for **.exe attachments** in emails
    - **Encrypt** sensitive data



What Should I Do?	Why Should I Do It?
Anti-virus	Keep your corporate data sources up to date with the latest anti-malware software to filer known ransomware strains.
Firewalls	Deploy firewalls and block access to SMB ports over the network or internet to control access to your IT environment.
Configure Webmail Server to Block Attachments	Include extensions like .exe, .vbs, or .scr. After filtering, you can scan the files in an isolated environment to verify or destroy.
User Training	Train staff to stay alert for suspicious attachments and download links, such as double-checking a business domain or spot-checking links.
File Versioning	Automatically store multiple versions of files at a time. This enables flexible restores in a disaster recovery scenario.
Upgrade OS and Applications	I really hope this is clear by now. Strains like EternalBlue expose out-of-date Windows software as an entry point into your environment

https://www.keepitsafe.com/blog/post/eternalblue-whats-going-on-and-how-to-protect-your-data/

Question & Answer

EternalBlue - Mitigations

NotPetya - Variants of EternalBlue

JUNE 27, 2017

- At the end of 2018, millions of systems were still vulnerable to EternalBlue

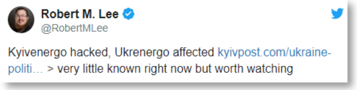
  They aren't just viruses. They are worms…

- On June 27, 2017, a digital attack campaign struck **banks**, **airports** and **power** companies in **Ukraine**, **Russia** and **parts of Europe**.

- Combined, caused over **$1 billion** worth of **damages** over **65 countries**

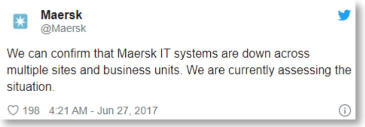
13:00 EDT – JUNE 27, 2017

Security researchers begin to share ways by which affected users and businesses can counteract the ransomware. Some note NotPetya runs on boot. As a result, victims can prevent the ransomware from encrypting their files by quickly powering down before Window boots or if they see a "Check Disk" message.



Robert M. Lee
@RobertMLee

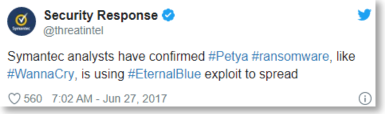
Kyivenergo hacked, Ukrenergo affected kyivpost.com/ukraine-politi… > very little known right now but worth watching



Maersk
@Maersk

We can confirm that Maersk IT systems are down across multiple sites and business units. We are currently assessing the situation.

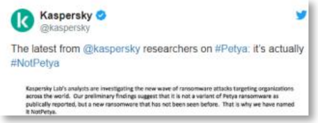
198 4:21 AM - Jun 27, 2017



Security Response
@threatintel

Symantec analysts have confirmed #Petya #ransomware, like #WannaCry, is using #EternalBlue exploit to spread

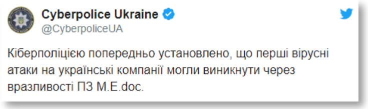
560 7:02 AM - Jun 27, 2017



Kaspersky
@kaspersky

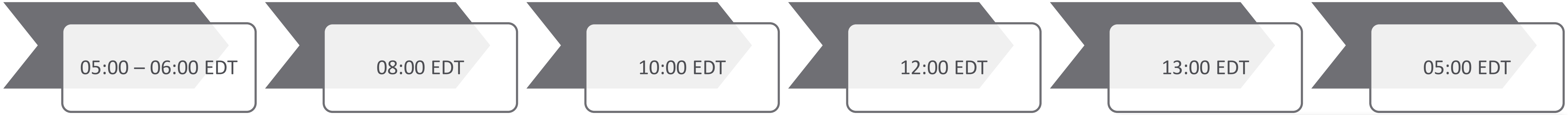
The latest from @kaspersky researchers on #Petya: it's actually #NotPetya

Kaspersky Lab's analysts are investigating the new wave of ransomware attacks targeting organizations across the world. Our preliminary findings suggest that it is not a variant of Petya ransomware as publically reported, but a new ransomware that has not been seen before. That is why we have named it NotPetya.



Cyberpolice Ukraine
@CyberpoliceUA

Кіберполіцією попередньо установлено, що перші вірусні атаки на українські компанії могли виникнути через вразливості ПЗ M.E.doc.



05:00 – 06:00 EDT

08:00 EDT

10:00 EDT

12:00 EDT

13:00 EDT

05:00 EDT

- The **first signs** of a digital attack.
- Other affected organizations coming forward:

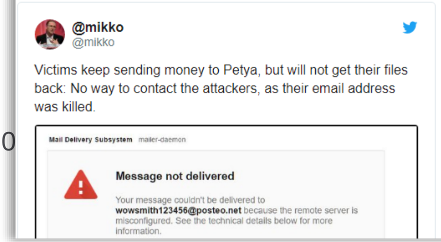
- **Symantec Security** Response confirms that **Petya ransomware** is **responsible** for the digital attacks.

- **Kaspersky** Lab tweets out a statement clarifying that the ransomworm is **not a variant of Petya** but is actually a **new ransomware** they named "**NotPetya**."

- **Ukraine's** police confirm **MeDoc**, an accounting software package that many Ukrainians use to pay their taxes, as a **NotPetya infection vector**.
  - Security researchers' belief that an **update released** by MeDoc at 10:30 GMT on June 27, 2017, allegedly **installed the malware** on the "victim zero" system.

05:00 EDT – JUNE 28, 2017

Some in the security community tweet out that victims who have paid NotPetya are not getting their files back.



@mikko
@mikko

Victims keep sending money to Petya, but will not get their files back: No way to contact the attackers, as their email address was killed.

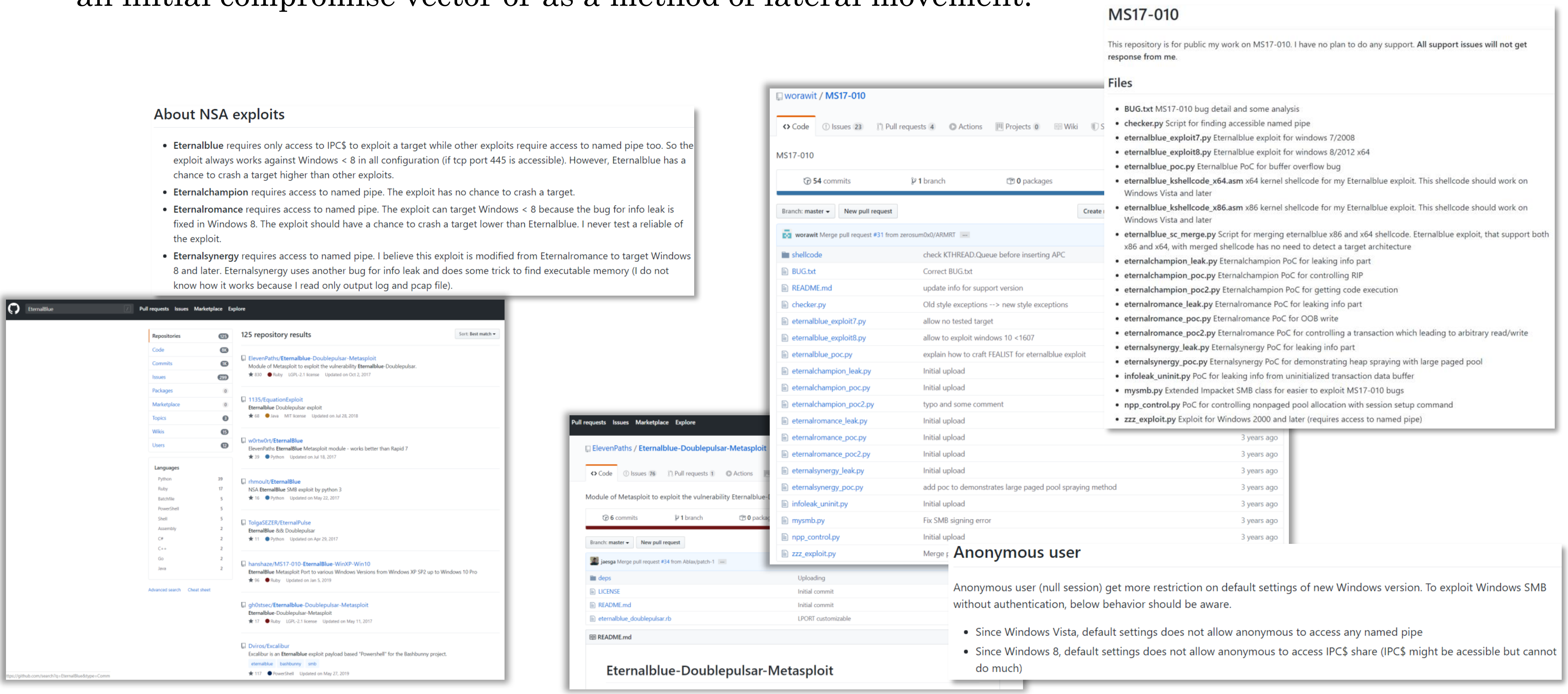
Mail Delivery Subsystem mailer-daemon

Message not delivered

Your message couldn't be delivered to **wowsmith123456@posteo.net** because the remote server is misconfigured. See the technical details below for more information.

EternalBlue OpenSource Code…

- Following the massive impact of WannaCry, both **NotPetya** and **BadRabbit** caused over **$1 billion worth of damages in over 65 countries**, using EternalBlue as either an initial compromise vector or as a method of lateral movement.



MS17-010

This repository is for public my work on MS17-010. I have no plan to do any support. **All support issues will not get response from me.**

Files

- **BUG.txt** MS17-010 bug detail and some analysis
- **checker.py** Script for finding accessible named pipe
- **eternalblue_exploit7.py** Eternalblue exploit for windows 7/2008
- **eternalblue_exploit8.py** Eternalblue exploit for windows 8/2012 x64
- **eternalblue_poc.py** Eternalblue PoC for buffer overflow bug
- **eternalblue_kshellcode_x64.asm** x64 kernel shellcode for my Eternalblue exploit. This shellcode should work on Windows Vista and later
- **eternalblue_kshellcode_x86.asm** x86 kernel shellcode for my Eternalblue exploit. This shellcode should work on Windows Vista and later
- **eternalblue_sc_merge.py** Script for merging eternalblue x86 and x64 shellcode. Eternalblue exploit, that support both x86 and x64, with merged shellcode has no need to detect a target architecture
- **eternalchampion_leak.py** Eternalchampion PoC for leaking info part
- **eternalchampion_poc.py** Eternalchampion PoC for controlling RIP
- **eternalchampion_poc2.py** Eternalchampion PoC for getting code execution
- **eternalromance_leak.py** Eternalromance PoC for leaking info part
- **eternalromance_poc.py** Eternalromance PoC for OOB write
- **eternalromance_poc2.py** Eternalromance PoC for controlling a transaction which leading to arbitrary read/write
- **eternalsynergy_leak.py** Eternalsynergy PoC for leaking info part
- **eternalsynergy_poc.py** Eternalsynergy PoC for demonstrating heap spraying with large paged pool
- **infoleak_uninit.py** PoC for leaking info from uninitialized transaction data buffer
- **mysmb.py** Extended Impacket SMB class for easier to exploit MS17-010 bugs
- **npp_control.py** PoC for controlling nonpaged pool allocation with session setup command
- **zzz_exploit.py** Exploit for Windows 2000 and later (requires access to named pipe)

About NSA exploits

- **Eternalblue** requires only access to IPC$ to exploit a target while other exploits require access to named pipe too. So the exploit always works against Windows < 8 in all configuration (if tcp port 445 is accessible). However, Eternalblue has a chance to crash a target higher than other exploits.
- **Eternalchampion** requires access to named pipe. The exploit has no chance to crash a target.
- **Eternalromance** requires access to named pipe. The exploit can target Windows < 8 because the bug for info leak is fixed in Windows 8. The exploit should have a chance to crash a target lower than Eternalblue. I never test a reliable of the exploit.
- **Eternalsynergy** requires access to named pipe. I believe this exploit is modified from Eternalromance to target Windows 8 and later. Eternalsynergy uses another bug for info leak and does some trick to find executable memory (I do not know how it works because I read only output log and pcap file).

worawit / MS17-010

MS17-010

54 commits · 1 branch · 0 packages

Branch: master · New pull request · Create

worawit Merge pull request #31 from zerosum0x0/ARMRT

shellcode	check KTHREAD.Queue before inserting APC	
BUG.txt	Correct BUG.txt	
README.md	update info for support version	
checker.py	Old style exceptions --> new style exceptions	
eternalblue_exploit7.py	allow no tested target	
eternalblue_exploit8.py	allow to exploit windows 10 <1607	
eternalblue_poc.py	explain how to craft FEALIST for eternalblue exploit	
eternalchampion_leak.py	Initial upload	
eternalchampion_poc.py	Initial upload	
eternalchampion_poc2.py	typo and some comment	
eternalromance_leak.py	Initial upload	
eternalromance_poc.py	Initial upload	3 years ago
eternalromance_poc2.py	Initial upload	3 years ago
eternalsynergy_leak.py	Initial upload	3 years ago
eternalsynergy_poc.py	add poc to demonstrates large paged pool spraying method	3 years ago
infoleak_uninit.py	Initial upload	3 years ago
mysmb.py	Fix SMB signing error	3 years ago
npp_control.py	Initial upload	3 years ago
zzz_exploit.py	Merge	

Repositories	125
Code	6K
Commits	1K
Issues	299
Packages	0
Marketplace	0
Topics	3
Wikis	15
Users	12

Languages

Python	39
Ruby	17
Batchfile	5
PowerShell	5
Shell	5
Assembly	2
C#	2
C++	2
Go	2
Java	2

Advanced search · Cheat sheet

125 repository results

Sort: Best match

ElevenPaths/Eternalblue-Doublepulsar-Metasploit
Module of Metasploit to exploit the vulnerability Eternalblue-Doublepulsar.
★ 830 · Ruby · LGPL-2.1 license · Updated on Oct 2, 2017

1135/EquationExploit
Eternalblue Doublepulsar exploit
★ 68 · Java · MIT license · Updated on Jul 28, 2018

w0rtw0rt/EternalBlue
ElevenPaths EternalBlue Metasploit module - works better than Rapid 7
★ 39 · Python · Updated on Jul 18, 2017

rhmoult/EternalBlue
NSA EternalBlue SMB exploit by python 3
★ 16 · Python · Updated on May 22, 2017

TolgaSEZER/EternalPulse
EternalBlue && Doublepulsar
★ 11 · Python · Updated on Apr 29, 2017

hanshaze/MS17-010-EternalBlue-WinXP-Win10
EternalBlue Metasploit Port to various Windows Versions from Windows XP SP2 up to Windows 10 Pro
★ 96 · Ruby · Updated on Jan 5, 2019

gh0stsec/Eternalblue-Doublepulsar-Metasploit
Eternalblue-Doublepulsar-Metasploit
★ 17 · Ruby · LGPL-2.1 license · Updated on May 11, 2017

Dviros/Excalibur
Excalibur is an Eternalblue exploit payload based "Powershell" for the Bashbunny project.
eternalblue · bashbunny · smb
★ 117 · PowerShell · Updated on May 27, 2019

ttps://github.com/search?q=EternalBlue&type=Comm

ElevenPaths / Eternalblue-Doublepulsar-Metasploit

Module of Metasploit to exploit the vulnerability Eternalblue-

6 commits · 1 branch · 0 packag

Branch: master · New pull request

jaesga Merge pull request #34 from Ablax/patch-1

deps	Uploading
LICENSE	Initial commit
README.md	Initial commit
eternalblue_doublepulsar.rb	LPORT customizable

README.md

Eternalblue-Doublepulsar-Metasploit

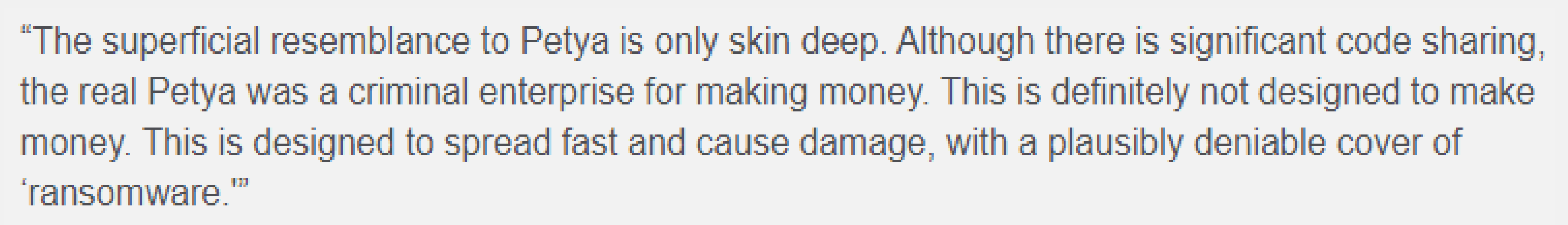
Anonymous user

Anonymous user (null session) get more restriction on default settings of new Windows version. To exploit Windows SMB without authentication, below behavior should be aware.

- Since Windows Vista, default settings does not allow anonymous to access any named pipe
- Since Windows 8, default settings does not allow anonymous to access IPC$ share (IPC$ might be acessible but cannot do much)

NotPetya -Variants of EternalBlue

- *Operation* -



"The superficial resemblance to Petya is only skin deep. Although there is significant code sharing, the real Petya was a criminal enterprise for making money. This is definitely not designed to make money. This is designed to spread fast and cause damage, with a plausibly deniable cover of 'ransomware.'"

- Researchers at **Kaspersky** Lab reveal that the ransomware does use **EternalBlue**, as well as **EternalRomance**, **another exploit** targeting some **Windows** machines as **infection vectors**.

- **Kaspersky** also discloses NotPetya's ability to use **Mimikatz** to extract **administrative credentials** from an infected system using the **lsass.exe** process. The threat can then use other tools, such as Windows Management Instrumentation (**WMI**) or **PsExec**, to **infect other computers** on a network.

- **Encryption** routine was **modified** so that the malware could **not revert** its **changes**

- **Low** unlock fee of $300

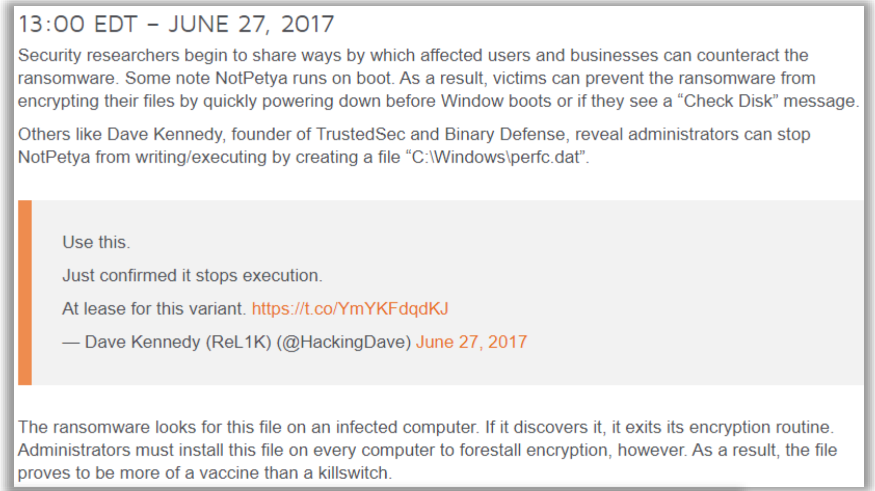
- **Single**, fixed Bitcoin **wallet** to collect ransom payments

- Due to the above, Researchers speculate that this **attack** was **not** intended to be a **profit-generating** venture

- Rather, to **damage devices quickly**, and ride off the media attention WannaCry received by claiming to be ransomware.

NotPetya - Variants of EternalBlue

- *Mitigation* -



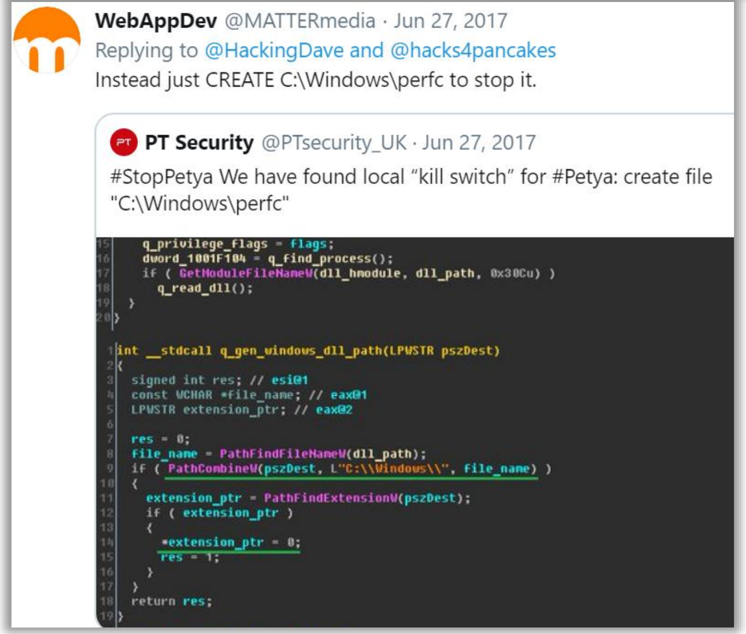
13:00 EDT – JUNE 27, 2017

Security researchers begin to share ways by which affected users and businesses can counteract the ransomware. Some note NotPetya runs on boot. As a result, victims can prevent the ransomware from encrypting their files by quickly powering down before Window boots or if they see a "Check Disk" message.

Others like Dave Kennedy, founder of TrustedSec and Binary Defense, reveal administrators can stop NotPetya from writing/executing by creating a file "C:\Windows\perfc.dat".

> Use this.
>
> Just confirmed it stops execution.
>
> At lease for this variant. https://t.co/YmYKFdqdKJ
>
> — Dave Kennedy (ReL1K) (@HackingDave) June 27, 2017

The ransomware looks for this file on an infected computer. If it discovers it, it exits its encryption routine. Administrators must install this file on every computer to forestall encryption, however. As a result, the file proves to be more of a vaccine than a killswitch.



WebAppDev @MATTERmedia · Jun 27, 2017

Replying to @HackingDave and @hacks4pancakes

Instead just CREATE C:\Windows\perfc to stop it.

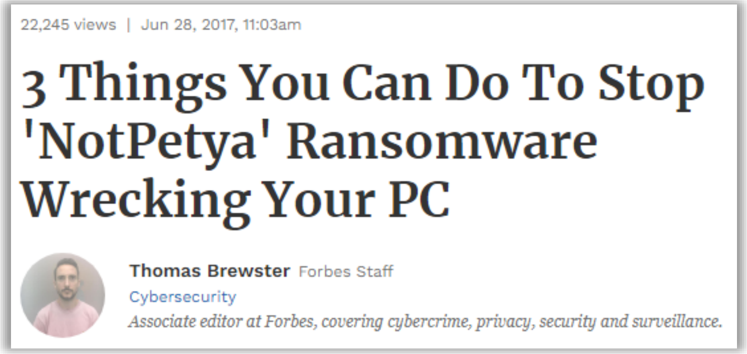
PT Security @PTsecurity_UK · Jun 27, 2017

#StopPetya We have found local "kill switch" for #Petya: create file "C:\Windows\perfc"

```
    q_privilege_flags = flags;
    dword_1001F104 = q_find_process();
    if ( GetModuleFileNameW(dll_hmodule, dll_path, 0x30Cu) )
      q_read_dll();
  }
}

int __stdcall q_gen_windows_dll_path(LPWSTR pszDest)
{
  signed int res; // esi@1
  const WCHAR *file_name; // eax@1
  LPWSTR extension_ptr; // eax@2

  res = 0;
  file_name = PathFindFileNameW(dll_path);
  if ( PathCombineW(pszDest, L"C:\\Windows\\", file_name) )
  {
    extension_ptr = PathFindExtensionW(pszDest);
    if ( extension_ptr )
    {
      *extension_ptr = 0;
      res = 1;
    }
  }
  return res;
}
```



22,245 views | Jun 28, 2017, 11:03am

3 Things You Can Do To Stop 'NotPetya' Ransomware Wrecking Your PC

Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

1. **Trick** the malware into thinking it's **already on the computer**
   a. %WINDIR%perfc – **kill switch**
2. Check whether computer is **already infected**, look for **two** "**rundll32.exe**" files **running** in Windows Task Manager
   a. If found, power off PC and **reinstall windows**.
3. Employ sensible **digital hygiene**.
   a. Make sure your running **latest version** of your **Windows OS**
   b. Ensure Windows **firewall** is turned on
   c. Check **antivirus** is **up-to-date**
   d. Ensure all **third-party software** has been **patched**

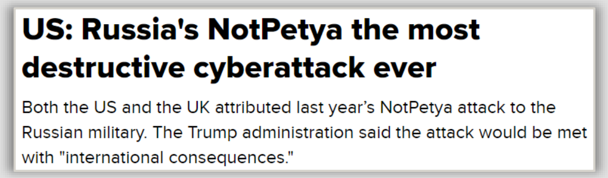
❖ To protect against ransomware campaigns such as NotPetya, users and businesses alike must **update their operating system** software **regularly**, **don't click** on **suspicious attachments**, and **back up** their **critical data** on a **regular** basis.

Variants of EternalBlue

- *Impact* -

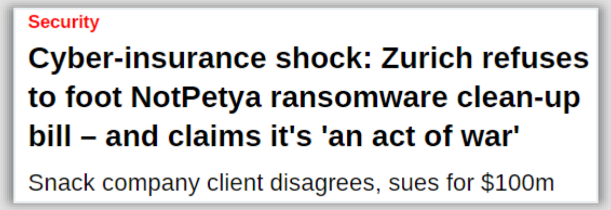
"While there was no loss of life, it was equivalent of using a nuclear bomb to achieve a small tactical victory," Bossert says.

NotPetya



US: Russia's NotPetya the most destructive cyberattack ever

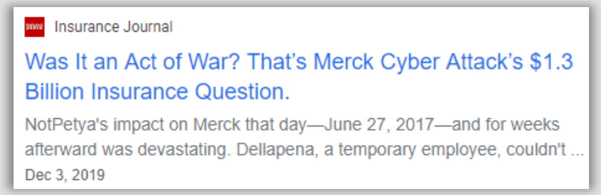
Both the US and the UK attributed last year's NotPetya attack to the Russian military. The Trump administration said the attack would be met with "international consequences."



Security

Cyber-insurance shock: Zurich refuses to foot NotPetya ransomware clean-up bill – and claims it's 'an act of war'

Snack company client disagrees, sues for $100m

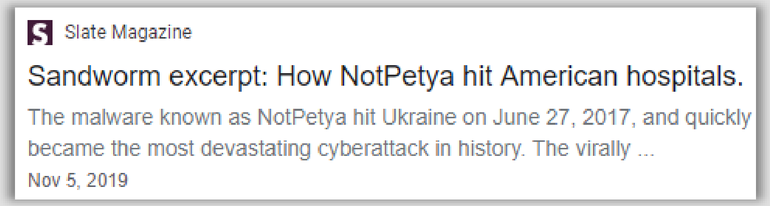


Insurance Journal

Was It an Act of War? That's Merck Cyber Attack's $1.3 Billion Insurance Question.

NotPetya's impact on Merck that day—June 27, 2017—and for weeks afterward was devastating. Dellapena, a temporary employee, couldn't ...

Dec 3, 2019

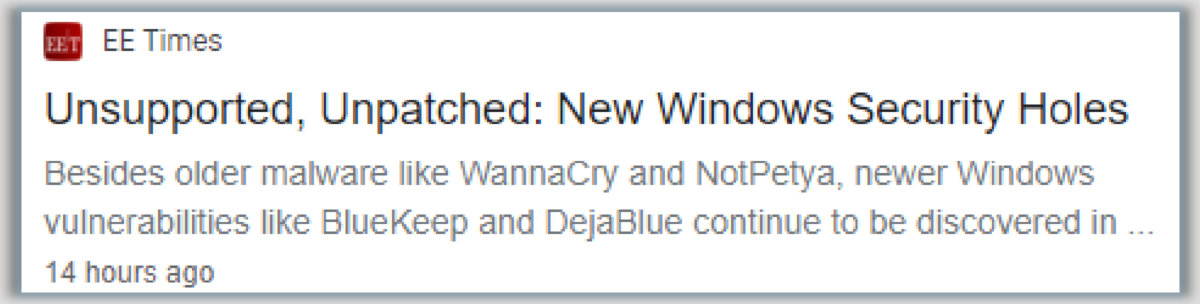


Slate Magazine

Sandworm excerpt: How NotPetya hit American hospitals.

The malware known as NotPetya hit Ukraine on June 27, 2017, and quickly became the most devastating cyberattack in history. The virally ...

Nov 5, 2019



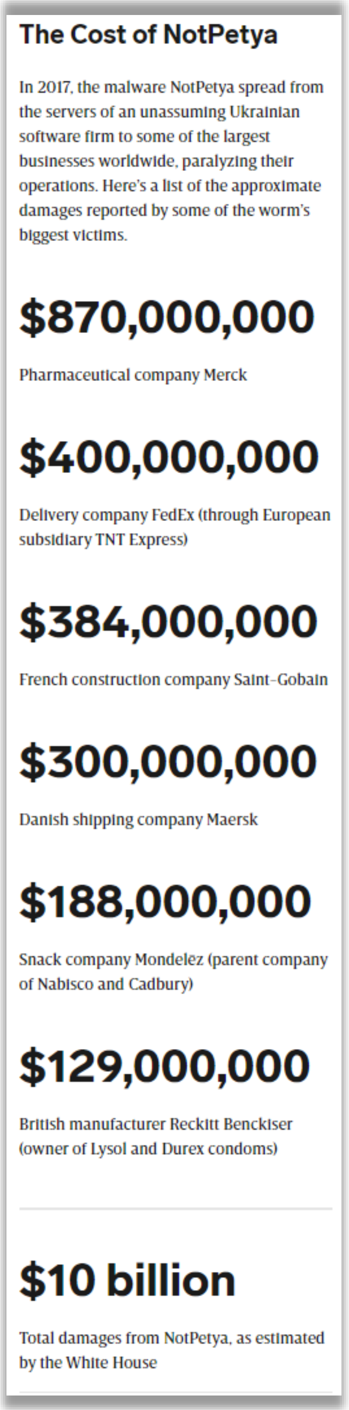
EE Times

Unsupported, Unpatched: New Windows Security Holes

Besides older malware like WannaCry and NotPetya, newer Windows vulnerabilities like BlueKeep and DejaBlue continue to be discovered in ...

14 hours ago

- ✓ Maersk
- ✓ Merck – Pharmaceutical giant
- ✓ TNT Express - FedEx's European subsidiary
- ✓ Saint-Gobian - French construction company
- ✓ Mondelez – Food producer
- ✓ Reckitt Benckiser – Manufacturing
- ✓ Rosneft – Russian oil company
- ✓ Chernobyl - Nuclear Power Plant
- ✓ Several Ukrainian Ministries
- ✓ WPP – British advertising company
- ✓ Etc…



The Cost of NotPetya

In 2017, the malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations. Here's a list of the approximate damages reported by some of the worm's biggest victims.

$870,000,000

Pharmaceutical company Merck

$400,000,000

Delivery company FedEx (through European subsidiary TNT Express)

$384,000,000

French construction company Saint-Gobain

$300,000,000

Danish shipping company Maersk

$188,000,000

Snack company Mondelez (parent company of Nabisco and Cadbury)

$129,000,000

British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)

$10 billion

Total damages from NotPetya, as estimated by the White House

Question & Answer

Variants of EternalBlue

Works Cited:

1 https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/

2 https://research.checkpoint.com/2017/eternalblue-everything-know/

3 https://techterms.com/definition/smb

4 https://www.govtech.com/security/How-Texas-Cities-Are-Handling-Recent-Ransomware-Attacks.html

5 https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault

6 https://www.govtech.com/security/Lake-City-Fla-Authorizes-Nearly-500K-Ransomware-Payment.html

7 https://www.forbes.com/sites/thomasbrewster/2017/06/28/three-things-you-can-do-to-stop-notpetya-ransomware-wrecking-your-pc/#4280effe77b0

8 https://twitter.com/PTsecurity_UK/status/879779707075665922

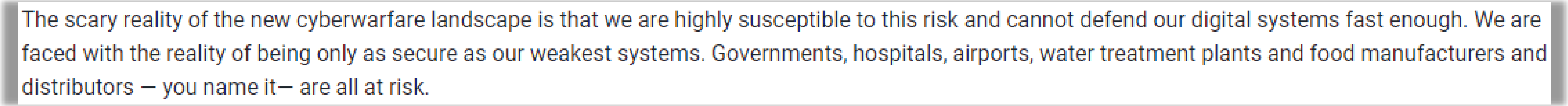
9 https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/

10 https://www.bleepingcomputer.com/news/software/-eternal-blues-tool-tests-computers-against-nsas-eternalblue-exploit/

11 https://www.bleepingcomputer.com/news/security/app-finds-more-than-50-000-computers-vulnerable-to-eternalblue-exploit/

12 https://www.schneier.com/blog/archives/2008/04/reverseengineer.html

13 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/



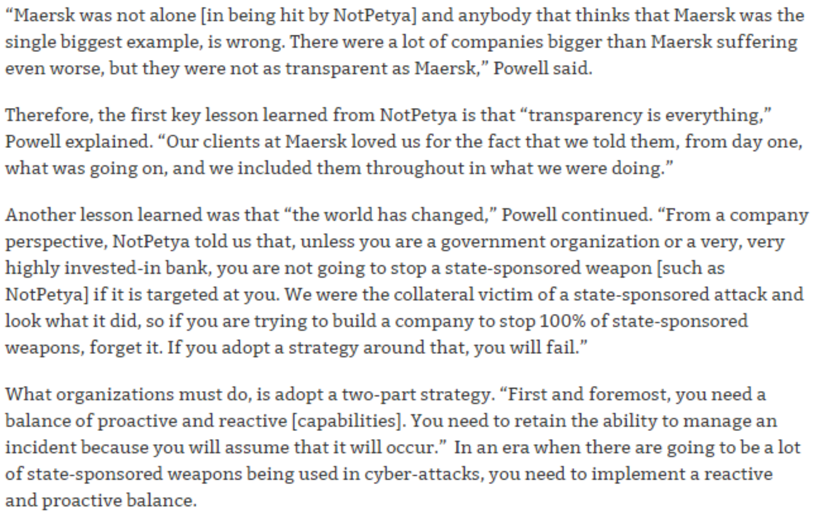
The scary reality of the new cyberwarfare landscape is that we are highly susceptible to this risk and cannot defend our digital systems fast enough. We are faced with the reality of being only as secure as our weakest systems. Governments, hospitals, airports, water treatment plants and food manufacturers and distributors — you name it— are all at risk.

Appendix

Maersk
– Response / Recovery to NotPetya

10 SEP 2019 NEWS

#GartnerSEC: Maersk’s Adam Banks Reflects on NotPetya Response and Recovery

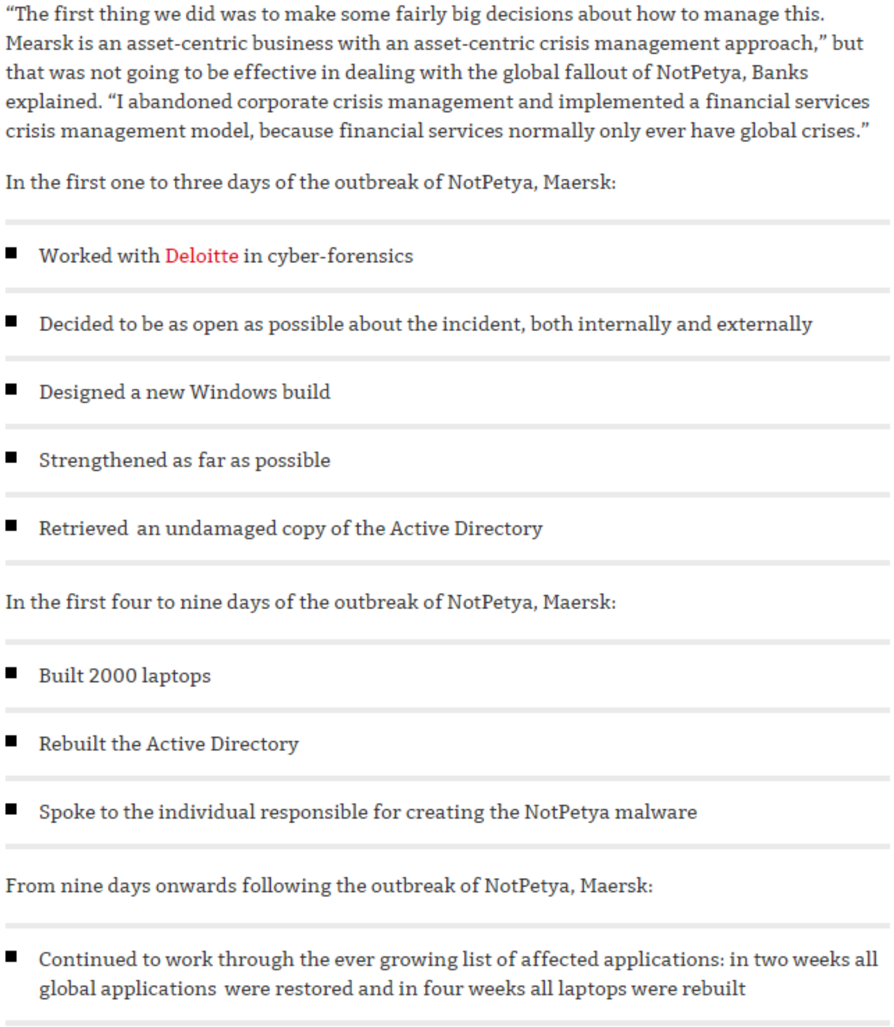


“Maersk was not alone [in being hit by NotPetya] and anybody that thinks that Maersk was the single biggest example, is wrong. There were a lot of companies bigger than Maersk suffering even worse, but they were not as transparent as Maersk,” Powell said.

Therefore, the first key lesson learned from NotPetya is that “transparency is everything,” Powell explained. “Our clients at Maersk loved us for the fact that we told them, from day one, what was going on, and we included them throughout in what we were doing.”

Another lesson learned was that “the world has changed,” Powell continued. “From a company perspective, NotPetya told us that, unless you are a government organization or a very, very highly invested-in bank, you are not going to stop a state-sponsored weapon [such as NotPetya] if it is targeted at you. We were the collateral victim of a state-sponsored attack and look what it did, so if you are trying to build a company to stop 100% of state-sponsored weapons, forget it. If you adopt a strategy around that, you will fail.”

What organizations must do, is adopt a two-part strategy. “First and foremost, you need a balance of proactive and reactive [capabilities]. You need to retain the ability to manage an incident because you will assume that it will occur.” In an era when there are going to be a lot of state-sponsored weapons being used in cyber-attacks, you need to implement a reactive and proactive balance.



“The first thing we did was to make some fairly big decisions about how to manage this. Mearsk is an asset-centric business with an asset-centric crisis management approach,” but that was not going to be effective in dealing with the global fallout of NotPetya, Banks explained. “I abandoned corporate crisis management and implemented a financial services crisis management model, because financial services normally only ever have global crises.”

In the first one to three days of the outbreak of NotPetya, Maersk:

- Worked with Deloitte in cyber-forensics
- Decided to be as open as possible about the incident, both internally and externally
- Designed a new Windows build
- Strengthened as far as possible
- Retrieved an undamaged copy of the Active Directory

In the first four to nine days of the outbreak of NotPetya, Maersk:

- Built 2000 laptops
- Rebuilt the Active Directory
- Spoke to the individual responsible for creating the NotPetya malware

From nine days onwards following the outbreak of NotPetya, Maersk:

- Continued to work through the ever growing list of affected applications: in two weeks all global applications were restored and in four weeks all laptops were rebuilt