WannaCry ransomware

Team 5: Davide De Vittorio, Luca Catalano

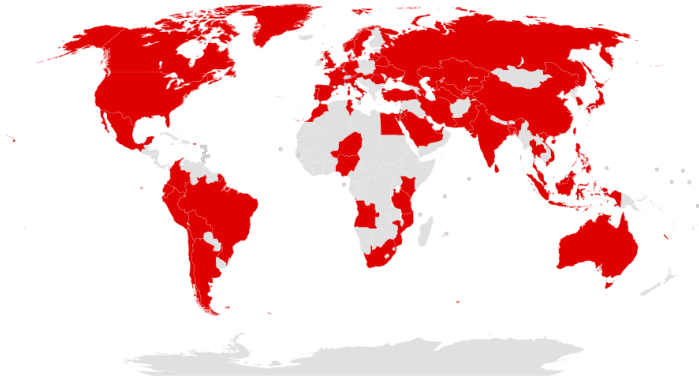
davide.devittorio01@universitadipavia.it

luca.catalano01@universitadipavia.it

Outline

- What is the Wannacry Ransomware?
- Wannacry analysis via the Cyber Kill Chain
- CVE-2017-0144 analysis
- Windows of exposure
- YARA Rules to detect WannaCry
- Limiting the damage of the attack
- Conclusions

What is the Wannacry Ransomware?

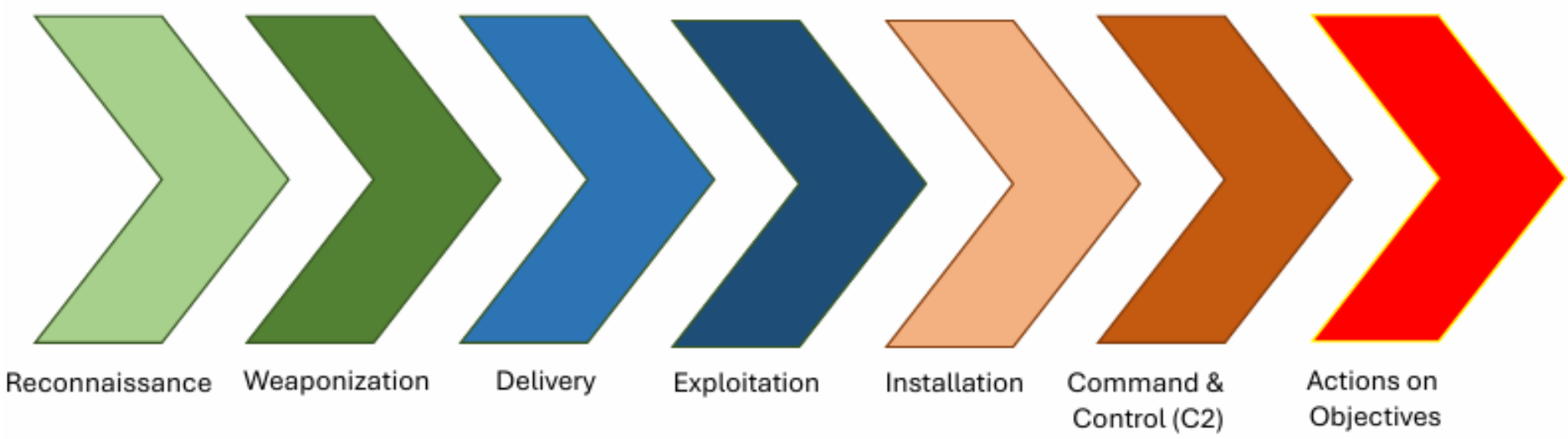


Source: Wikipedia

- Ransomware worm in May 2017 targeted computers running Microsoft Windows.
- It encrypts files and demands a ransom to decrypt them.
- In late 2017, US and UK announced that the government of North Korea was behind WannaCry.

Wannacry analysis via the Cyber Kill Chain

- A description of the process used to carry out the cyber attack



Source: Luca Caviglione - Foundation of cybersecurity – Introduction and Basics.

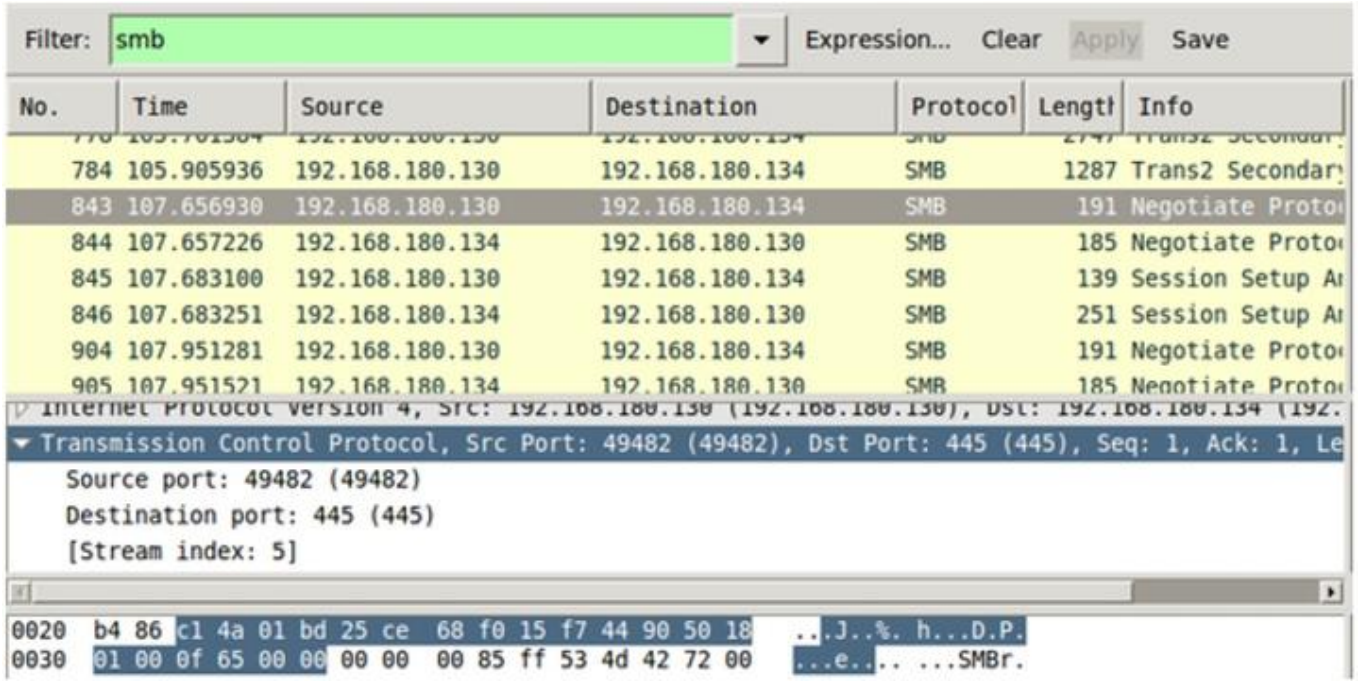
Wannacry analysis via the Cyber Kill Chain

- **Reconnaissance**: The malware scans the network for any system that accepts data on port 445.
- **Waponization**: The malicious package contains:
  - EternalBlue
  - DoublePulsar backdoor
  - Ransomware payload (Wana Decrypt0r)

Wannacry analysis via the Cyber Kill Chain

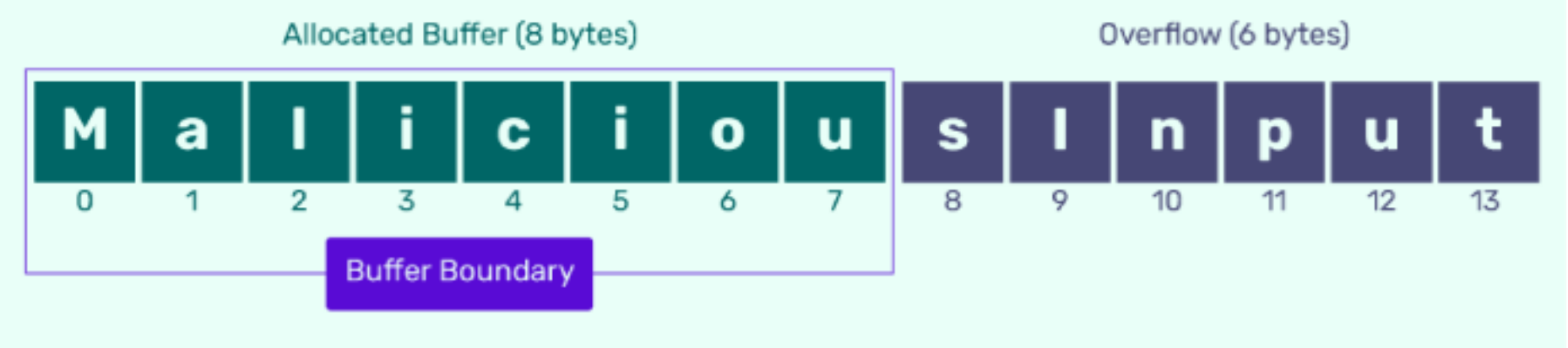
- **Delivery**: Achieved via network propagation by sending malicious SMB packets.

The infected machine 192.168.180.130 sends SMB packets in the local network through port 445.



Wannacry analysis via the Cyber Kill Chain

The **Delivery** exploit the buff overflow to rewrite the system memory of the SMB



Source: https://www.indusface.com/learning/what-is-buffer-overflow-attack/

Filter: tcp | Expression... | Clear | Apply | Save

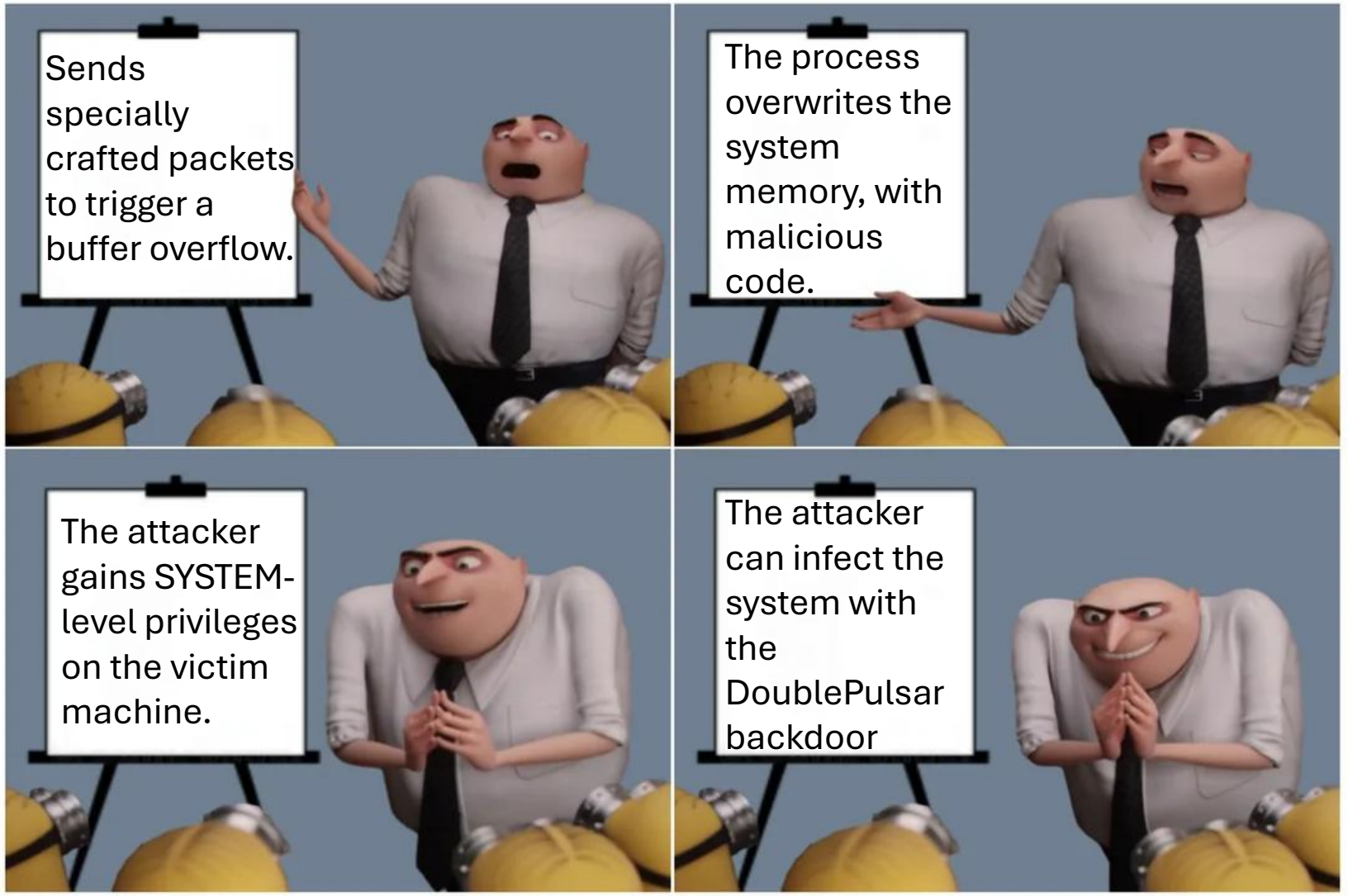
No.	Time	Source	Destination	Protocol	Lengtl	Info
1150	76.598100	192.168.180.130	109.140.223.210	TCP	66	49770 > 445 [SYI
1151	76.598259	192.168.180.130	206.242.244.156	TCP	66	49771 > 445 [SYI
1152	76.598308	192.168.180.130	52.213.90.240	TCP	66	49772 > 445 [SYI
1153	76.598386	192.168.180.130	202.76.26.154	TCP	66	49773 > 445 [SYI
1154	76.598466	192.168.180.130	205.215.5.24	TCP	66	49774 > 445 [SYI
1155	76.598549	192.168.180.130	80.133.73.130	TCP	66	49775 > 445 [SYI
1156	76.598708	192.168.180.130	198.73.58.205	TCP	66	49776 > 445 [SYI
1157	76.931700	192.168.180.130	40.188.28.244	TCP	66	49779 > 445 [SYI
1158	76.931759	192.168.180.130	184.55.110.103	TCP	66	49780 > 445 [SYI

SMB packets sent by the infected machine to external networks using random generated IP addresses

Source: Akbanov, Maxat, Vasilakis, Vasileios and Logothetis, Michael (2019) *Ransomware detection and mitigation using software-defined networking:the case of WannaCry.*

Wannacry analysis via the Cyber Kill Chain

- **Exploitation**: The EternalBlue exploit:



Wannacry analysis via the Cyber Kill Chain

- **Installation**: The DoublePulsar backdoor is used to drop and execute the ransomware payload.

- **Command & Control (C2)**: The malware attempted to connect to a specific, unregistered domain: If the connection fails infection proceeded otherwise it will stop. (Anti-Sandbox mechanism).
  - Principal domain used to avoid dynamic analysis: https://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/

Wannacry analysis via the Cyber Kill Chain

- **Actions on Objectives**: Encrypting user files and displaying the window demanding Bitcoin payment.

Source: https://www.malware-traffic-analysis.net/2017/05/18/index2.html

CVE-2017-0144 analysis

Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability.»

QUICK INFO

CVE Dictionary Entry:

CVE-2017-0144

NVD Published Date:

03/16/2017

NVD Last Modified:

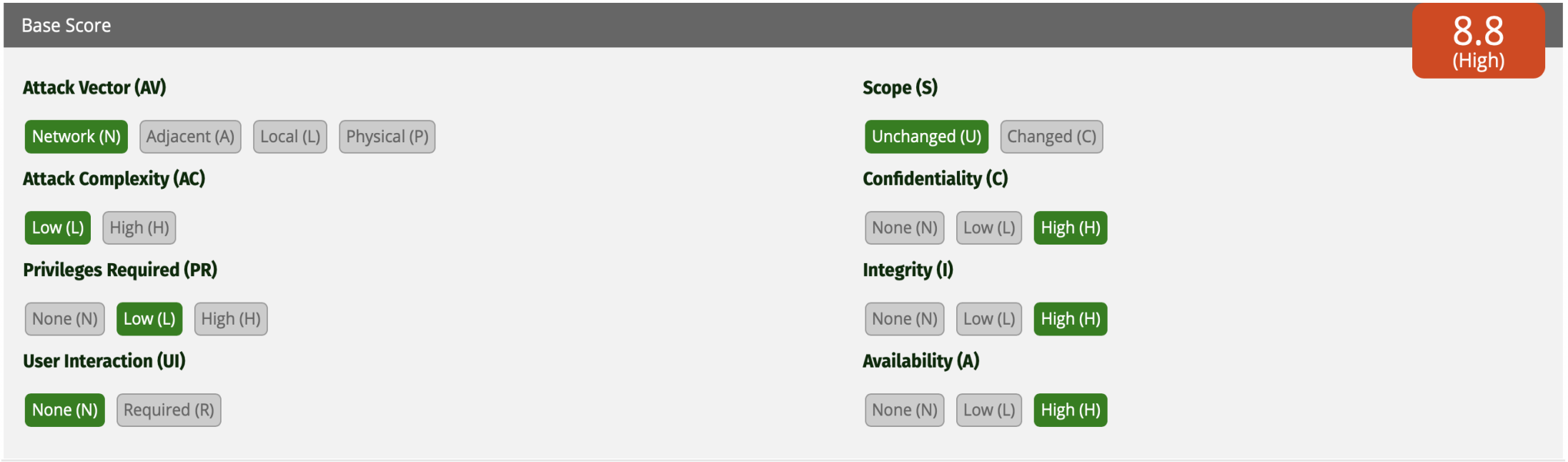
10/21/2025

Source:

Microsoft Corporation

Source:https://nvd.nist.gov/vuln/detail/cve-2017-0144#match-17277599

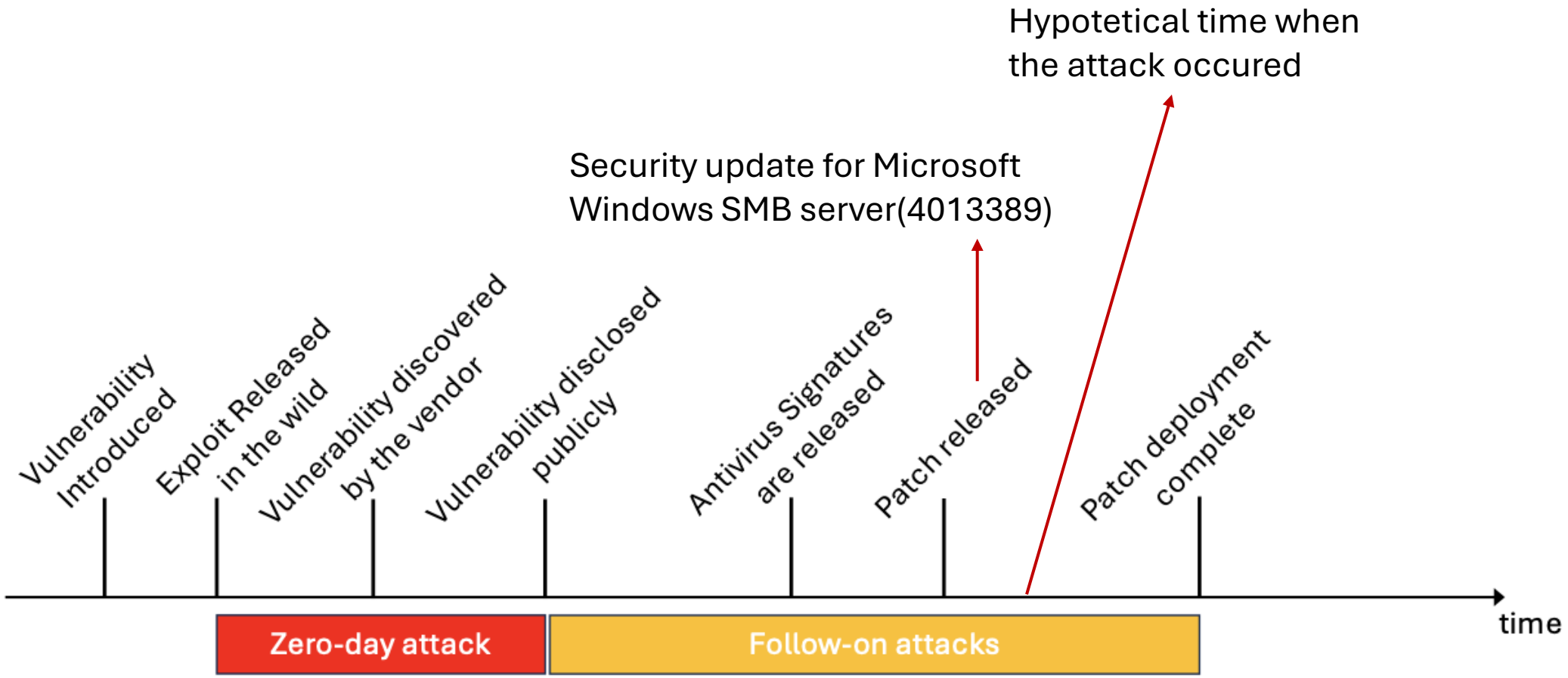
CVE-2017-0144 analysis



Source:https://www.first.org/cvss/calculator/3-1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

No version 4.0 cause deferred

Windows of exposure



Source: Luca Caviglione - Foundation of cybersecurity – Introduction and Basics.

Yara Rules to detect WannaCry

Three YARA rules to detect WannaCry:

- **First rule**: Detects the main executable and network components.

```
rule WannaCry_Dropper_And_Network {
    meta:
        description = "Detects the main executable (Dropper) and network components"
        author = "Maxat Akbanova, Vassilios G. Vassilakisa, Michael D. Logothetis"
        severity = "Critical"

    strings:
        //Textual Indicators (easy for attackers to change)
        $exe1 = "taskdl.exe"                // File used to delete traces
        $exe2 = "tasksche.exe"              // Persistent executable (persistence mechanism)
        $pass = "WNcry@2ol7"                // Hardcoded password in malware ZIP archives
        $kill = "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" // THE KILL SWITCH DOMAIN
        $svc  = "mssecsvc.exe"              // Fake Microsoft service

        // These are hexadecimal sequences of compiled assembly code (hard to change).
        $op1 = { 10 ac 72 0d 3d ff ff 1f ac 77 06 b8 01 00 00 00 }
        $op2 = { 44 24 64 8a c6 44 24 65 0e c6 44 24 66 80 c6 44 }

    condition:
        //Must be a Windows executable (MZ header) and file size under 10MB
        uint16(0) == 0x5a4d and filesize < 10000KB and
        //Logic: Match 1 text string OR 1 code sequence
        (1 of ($exe*, $pass, $kill, $svc) or 1 of ($op*))
}
```

Source: M. Satheesh Kumar, J. Ben-Othman and K. G. Srinivasagan, "An Investigation on Wannacry Ransomware and its Detection,"

Yara Rules to detect WannaCry

```
rule WannaCry_Encryption_Behavior {
    meta:
        description = "Detects artifacts related to file encryption"

    strings:
        //Typical strings found in files
        $wcry1 = "WanaCrypt0r"
        $wcry2 = "WANACRY"
        $ext1 = ".wnry"      //Extension appended to encrypted files
        $ext2 = ".wry"

    condition:
        //Triggers if encrypted file extensions AND the ransomware name are found
        ($ext1 or $ext2) and any of ($wcry*)
}

rule WannaCry_Decryptor_UI {
    meta:
        description = "Detects the Ransomware GUI (The famous red window)"

    strings:
        //Popular language files used by the ransom window interface
        $msg1 = "msg/m_portuguese.wnry"
        $msg2 = "m_bulgarian.wnr"
        $msg3 = "m_vietnamese.wnry"

        // Internal interface components
        $id1 = "r.wnry" // Readme file
        $id2 = "s.wnry" // ZIP archive containing support files

    condition:
        //If at least 3 of these files are found, we are looking at the malware directory
        3 of them
}
```

Source: M. Satheesh Kumar, J. Ben-Othman and K. G. Srinivasagan, "An Investigation on Wannacry Ransomware and its Detection,"

Three YARA rules to detect WannaCry:

- **Second rule**: Detects artifacts related to file encryption
- **Third rule**: Detects the red window that ask money

```python
# Script generator of a fake malware for the YARA test

filename = "fake_wannacry.exe"

signatures = [
    b"MZ",  # Magic Header M=5A, Z=4D, simualates the first two bytes of every windows program
    b"\x00" * 50, # 50 null bytes
    b"www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com", # Kill Switch domain
    b"\x00" * 20,
    b"WanaCrypt0r", # Ransomware Name
    b"\x00" * 20,
    b".wnry", # Estension
    b"\x00" * 20,
    b"msg/m_portuguese.wnry", # Message language
    b"r.wnry", # File readme
    b"s.wnry"  # File zip
]

try:
    with open(filename, "wb") as f:
        for sig in signatures:
            f.write(sig)
except Exception as e:
    print(f"[ERROR]: {e}")
```

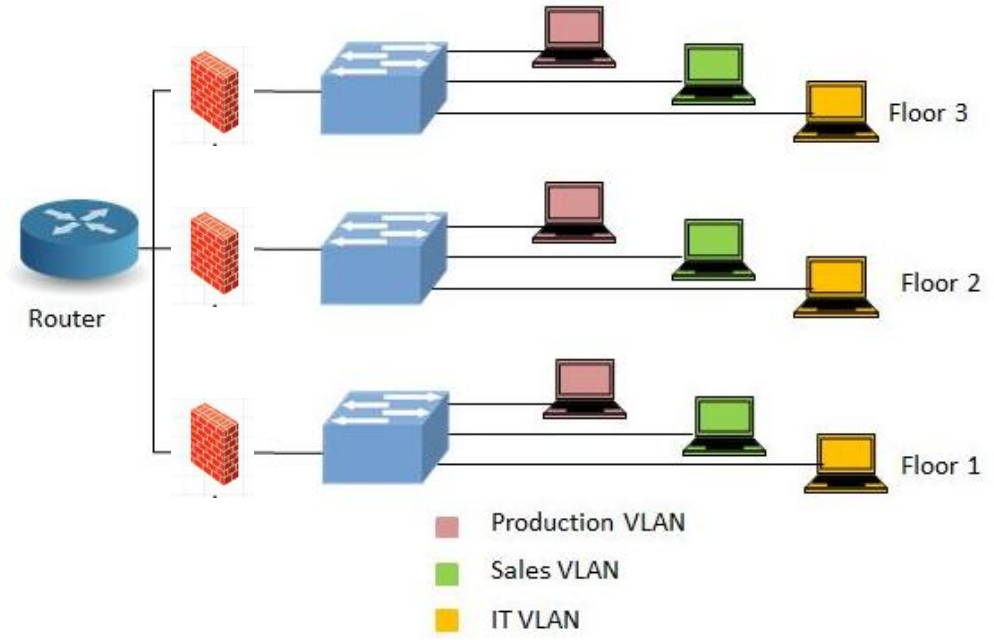
Script to create the fake WannaCry .exe file and YARA scan result

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        18/11/2025     17:26                yara-4.5.5-2368-win64
-a----        18/11/2025     17:23            210 fake_wannacry.exe
-a----        18/11/2025     17:22            931 malware_generator.py
-a----        18/11/2025     17:18           2616 WannaCry_Detection.yar
-a----        18/11/2025     17:25        2232629 yara-4.5.5-2368-win64.zip
-a----        18/11/2025     17:25        2418688 yara64.exe


PS C:\Users\Utente\OneDrive\Desktop\Progetto foundation\Scripts> .\yara64.exe -w WannaCry_Detection.yar fake_wannacry.exe
WannaCry_Dropper_And_Network fake_wannacry.exe
WannaCry_Encryption_Behavior fake_wannacry.exe
WannaCry_Decryptor_UI fake_wannacry.exe
```

Limiting the damage of the attack

- Network segmentation & Zero Trust policy
  - Watertight compartment
  - Avoid ‘flat’ network
  - VLAN segmentation
  - Internal firewall



Source: https://networkhope.in/virtual-lan/

Conclusions

- **Attack results:**
  - Lot of damage but achieved little in economic terms
  - Show of force by North Korea

- **Lessions learned:**
  - **Human factor**: install all security updates and patches immediately.
  - **Architectural improvements**: VLAN segmentation
  - **Resilience**: backup on a separate device, not in the same network, and not with the same technical characteristics