WannaCry Ransomware Overview

WannaCry ransomware, which surfaced in May 2017, became one of the most notable and destructive ransomware attacks to date due to its widespread impact and rapid propagation. It primarily leveraged a vulnerability in the Windows Server Message Block (SMB) protocol, known as EternalBlue, which was initially developed by the U.S. National Security Agency (NSA) and later leaked by a group called the Shadow Brokers. This exploit enabled WannaCry to spread across networks without requiring any user action, making it exceptionally virulent and capable of infecting a vast number of systems in a short time frame.

Upon infection, WannaCry encrypted numerous file types on the compromised machine, appending the ".wncry" extension to affected files. Victims were then shown a ransom note demanding payment in Bitcoin, typically amounting to a few hundred dollars, to receive the decryption key necessary for restoring their files. This ransom note contained multilingual messages, making it accessible to users worldwide. Additionally, WannaCry's ransom demands threatened to increase over time if the payment was not made promptly, pressuring victims to act quickly.

WannaCry spread through a "worm" mechanism, which enabled it to propagate automatically to other vulnerable computers on the same network, vastly increasing its reach and amplifying its damage. This made it unique from other ransomware attacks, as it combined both ransomware and worm characteristics, allowing it to compromise large organizations, critical infrastructure, and health services globally. Among the most heavily impacted was the United Kingdom's National Health Service (NHS), which suffered widespread disruptions to healthcare services and patient care due to encrypted medical records and inaccessible systems.

Following its initial success, various adaptations and versions of WannaCry were discovered. These versions generally retained the ".wncry" extension and core encryption methods but introduced minor tweaks to evade evolving security defenses. Although the original strain used a "kill switch" domain as an anti-sandboxing technique, researchers discovered and activated this kill switch, effectively halting the primary outbreak. However, subsequent variants removed or altered this kill switch mechanism, allowing for continued, albeit reduced, spread of WannaCry in different regions.

WannaCry employed both RSA and AES encryption algorithms to ensure that decrypting the files without paying the ransom would be nearly impossible. Its efficient use of dual encryption increased the complexity of the decryption process, leaving victims few options aside from payment. Despite widespread ransomware countermeasures, WannaCry's use of a then-unpatched SMB exploit enabled it to bypass conventional defenses and infiltrate networked environments, resulting in estimated damages ranging from hundreds of millions to billions of dollars.

The impact of WannaCry underscored the need for timely software updates and cybersecurity practices across industries. In response to the attack, Microsoft released critical patches for the SMB vulnerability and even took the unprecedented step of issuing updates for outdated and unsupported Windows systems, such as Windows XP, to mitigate the risk. Additionally, the WannaCry outbreak intensified global discussions around cybersecurity preparedness, particularly within essential service sectors and government institutions, and accelerated the adoption of improved patch management strategies.

Despite its eventual containment, WannaCry's ability to exploit a known vulnerability demonstrated the potential consequences of delayed cybersecurity updates and insufficient defenses. WannaCry remains a focal point in discussions about ransomware preparedness and serves as a cautionary example of how fast-moving malware can exploit lapses in security to create widespread havoc.

EternalBlue Exploit and Its Role in WannaCry's Spread

EternalBlue's significance in WannaCry's spread lies in its automation and low requirement for user interaction. As an exploit targeting the Windows SMB protocol, EternalBlue allowed WannaCry to act as a "worm" that could propagate autonomously within and across networks. This attribute enabled WannaCry to target systems that were not directly exposed to external threats but shared a network with an infected machine, greatly amplifying its impact in organizational environments.

EternalBlue specifically exploited the SMBv1 protocol, which had known vulnerabilities related to buffer overflow issues. By sending specially crafted packets to vulnerable systems, the exploit gained unauthorized access, facilitating WannaCry's installation and execution without triggering typical security alerts. Once WannaCry gained a foothold, it leveraged EternalBlue's capability to scan and identify other vulnerable devices on the same network, continuing the cycle of infection.

This propagation method was particularly damaging in environments with a mix of outdated and newer systems, as WannaCry could compromise one vulnerable machine and subsequently spread to any connected but unpatched systems, regardless of whether they were typically isolated from internet-facing threats. This capability caused critical issues in healthcare, finance, and transportation sectors, where internal networks often lack stringent compartmentalization, thus amplifying EternalBlue’s effectiveness.

One important technical note is that EternalBlue operates independently of typical user permissions or user-driven actions, making it both stealthy and challenging to intercept once it begins spreading. Security researchers observed that even standard antivirus tools had limitations in halting its progress in real time due to its network-based mechanism rather than traditional malware behavior. This propagation technique highlighted gaps in network segmentation and patch management within large organizations.

In sum, EternalBlue’s role in WannaCry’s spread was central to its design as a self-replicating, network-propagating ransomware. EternalBlue transformed WannaCry from a conventional ransomware attack into a wide-scale cybersecurity incident, emphasizing the risks inherent in unpatched, network-dependent vulnerabilities.

Encryption Process Employed by WannaCry

WannaCry’s encryption process was strategically designed to maximize the ransomware’s impact by targeting a wide array of file types while using a dual-layer encryption method. Upon infection, WannaCry first generated a unique AES (Advanced Encryption Standard) key for each targeted file. AES, a symmetric encryption algorithm, was used because it is both secure and efficient, allowing WannaCry to encrypt files rapidly without excessive processing overhead. This speed was essential, as it enabled WannaCry to lock down as many files as possible before detection or mitigation could occur.

Once files were encrypted with AES, WannaCry used an RSA (Rivest-Shamir-Adleman) public key to encrypt the AES keys themselves. This RSA encryption, an asymmetric encryption method, ensured that the AES keys were only retrievable through the corresponding private RSA key, held by the attackers. This layered encryption meant that even if victims accessed the encrypted files, they would lack the necessary keys to decrypt the data independently, creating a secure lock on all affected files.

The choice of combining AES and RSA encryption offered two main advantages. First, it allowed WannaCry to encrypt files quickly with AES, while still maintaining the security of those AES keys via RSA's robust encryption. Secondly, this approach minimized the storage requirements on the ransomware itself, as only a single public RSA key was needed to encrypt each AES key, rather than storing a unique decryption mechanism for each file.

WannaCry's encryption also included specific file extensions that it targeted, ensuring that valuable and commonly used files, such as documents, images, and databases, were prioritized. By focusing on such files, WannaCry maximized the pressure on victims to pay the ransom. Furthermore, each encrypted file received a distinctive ".wncry" extension, making it clear to victims which files had been compromised.

The encryption approach used by WannaCry was significant not just for its technical execution but for the psychological impact it generated. By rendering files unusable without the decryption key, WannaCry left victims with few options outside of paying the ransom. Its reliance on secure and tested encryption standards (AES and RSA) underscored the ransomware's ability to hold data hostage with little to no risk of easy decryption by affected users or organizations.

Mitigation Techniques: System Patching, Network Defense, and Ransomware Detection Mechanisms

Mitigating WannaCry and similar ransomware threats relies heavily on several proactive and layered defense strategies, each addressing different stages of a ransomware attack.

1. System Patching: One of the most direct and effective responses to WannaCry was Microsoft's patch MS17-010, which closed the SMB vulnerability that EternalBlue exploited. Regular patching and updates are essential because they address newly discovered vulnerabilities before attackers can exploit them. Beyond simply applying individual patches, organizations benefit from establishing a structured patch management strategy to ensure that all systems, including legacy systems that may lack vendor support, receive updates regularly. Automated patch management tools are particularly useful in larger networks to ensure no systems are missed and to maintain a consistent security baseline across devices.

2. Network Defense: Network segmentation and internal firewall controls are critical in limiting the spread of ransomware. By dividing a network into isolated segments, organizations

can prevent ransomware from moving laterally between systems, which was a key feature in WannaCry’s rapid spread. Using network access control (NAC) to restrict device connectivity and implementing intrusion detection and prevention systems (IDPS) can help identify unusual traffic patterns, like those created by WannaCry's worm behavior. Additionally, disabling the SMBv1 protocol, which is outdated and unnecessary in many environments, can reduce exposure to similar exploits.

3. Ransomware Detection Mechanisms: Effective ransomware detection mechanisms utilize both behavior-based and signature-based detection methods. While signature-based methods identify known ransomware by matching it against databases of known malware, behavior-based detection tools can recognize suspicious activities—such as unusual file encryption activity, rapid renaming of files, or access to sensitive data directories—indicative of ransomware. Endpoints with anti-ransomware features are designed to halt encryption processes if they detect ransomware-like behavior, potentially stopping ransomware before it completes encryption. Advanced solutions may use machine learning to improve detection accuracy and adaptability to new, unidentified strains.

4. Data Backup and Recovery: Although not a direct form of prevention, regular, secure data backups are among the most reliable defenses against ransomware. For WannaCry victims who could restore from unaffected backups, the impact of the attack was minimal. Organizations should store backups in isolated environments (e.g., offline or offsite) to prevent ransomware from reaching them and should test backups periodically to ensure their reliability.

5. User Education and Phishing Awareness: Although WannaCry primarily spread via EternalBlue rather than phishing, user education remains critical for other ransomware types. Training users to recognize phishing attempts and social engineering tactics reduces the risk of initial infection, especially for variants that rely on email-based attacks. Combined with other techniques, user awareness strengthens the overall resilience of the network.

In summary, mitigation of WannaCry-like attacks involves a combination of prompt system patching, robust network segmentation, advanced ransomware detection mechanisms, and reliable data backup practices. By addressing vulnerabilities at multiple points, these techniques collectively reduce the likelihood of infection and minimize damage if an attack does occur.

Simulation

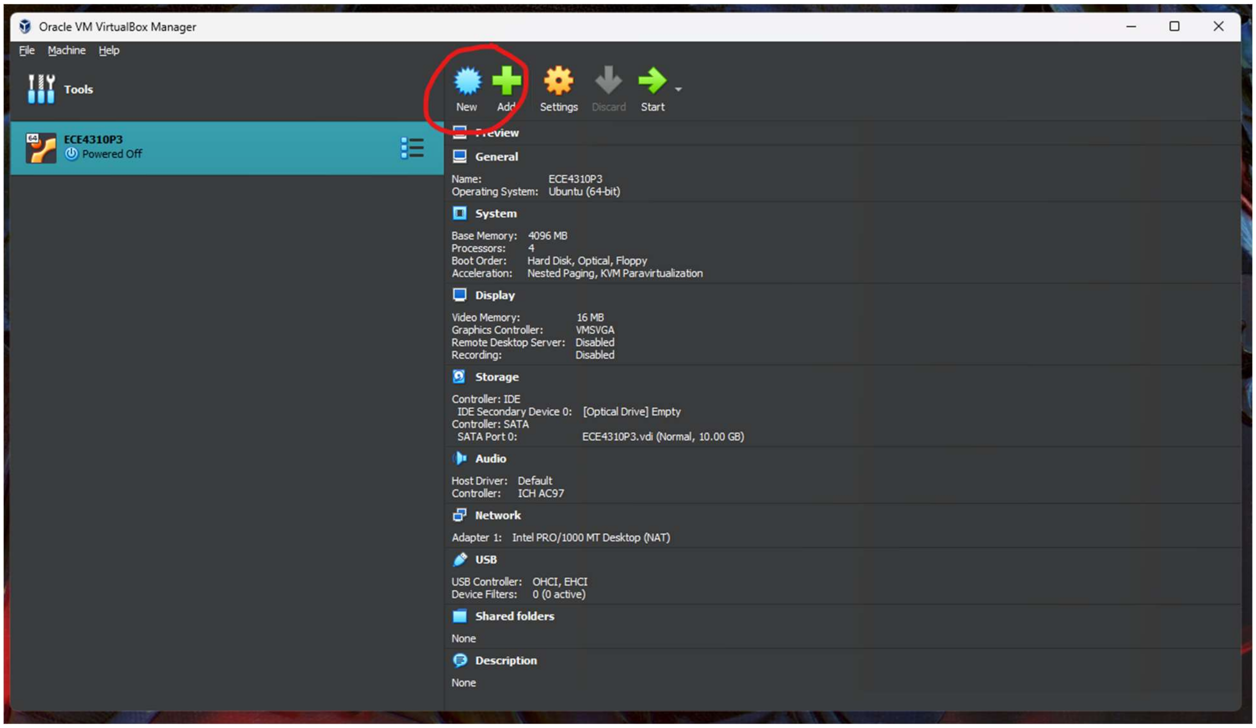
Why VMOracle is the Best Choice for Simulating WannaCry Ransomware

VMOracle (Oracle VirtualBox) is an excellent choice for simulating the WannaCry ransomware due to its robust features, user-friendly interface, and compatibility with a wide range of operating systems. Here are the primary reasons why VMOracle stands out for this project:

1. **Ease of Setup and Use**
   VMOracle is straightforward to download, install, and configure, making it accessible even to users with minimal experience in virtualization. Its intuitive GUI allows for quick setup of virtual machines (VMs), enabling the replication of complex environments without unnecessary overhead.
2. **Cross-Platform Compatibility**
   VMOracle supports a variety of host operating systems, including Windows, macOS, and Linux. This ensures flexibility regardless of the system you're using to execute the WannaCry simulation. Additionally, it supports guest operating systems like Windows XP and Windows 7, which are critical for testing WannaCry since these were the primary targets of the attack.
3. **Snapshot Functionality**
   One of VMOracle's most useful features is its snapshot capability. This allows users to create a restore point before executing potentially destructive malware, like WannaCry, ensuring that the environment can be easily reset without the need for a full reinstallation.
4. **Networking Flexibility**
   WannaCry's propagation relies heavily on network vulnerabilities. VMOracle provides advanced networking options, such as NAT, bridged, and host-only modes, which allow the creation of isolated or interconnected test environments. This flexibility is essential for replicating WannaCry's worm-like behavior safely within a controlled environment.
5. **Open Source and Free**
   Being open-source software, VMOracle is entirely free to use, making it a budget-friendly option for researchers, students, and professionals. Its accessibility ensures that cost does not become a barrier to running comprehensive simulations.
6. **Extensive Documentation and Community Support**
   VMOracle has a well-established community and extensive documentation. This is particularly advantageous when troubleshooting or fine-tuning virtual machines for specific simulation requirements, such as creating vulnerable SMB environments for WannaCry.

VMOracle intro

Once in VMOracle, create a new machine by clicking in New



ECE4310P3
Powered Off

General

Name: ECE4310P3
Operating System: Ubuntu (64-bit)

System

Base Memory: 4096 MB
Processors: 4
Boot Order: Hard Disk, Optical, Floppy
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: ECE4310P3.vdi (Normal, 10.00 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

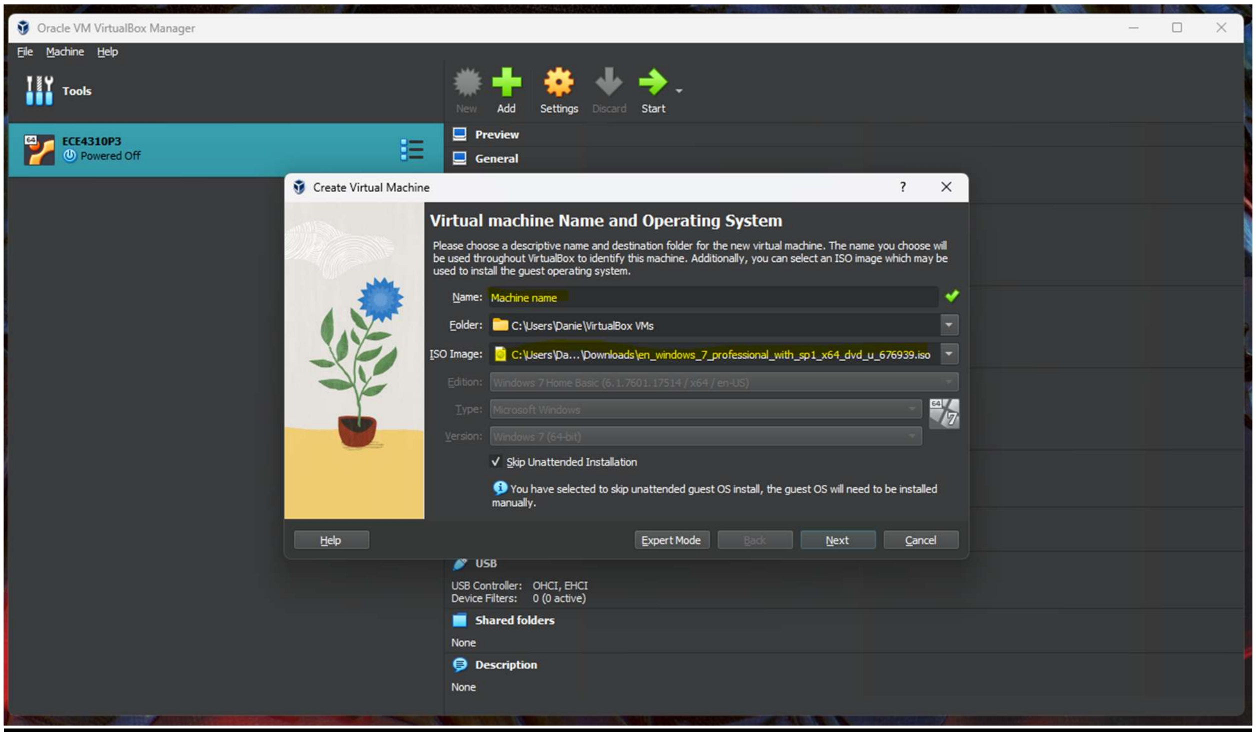
Shared folders

None

Description

None

Set a name for the machine and select an ISO (optical disc image) – In this case, a Windows 7 as that's the OS that was mostly affected back in 2017.



ECE4310P3
Powered Off

Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: Machine name
Folder: C:\Users\Danie\VirtualBox VMs
ISO Image: C:\Users\Da...\Downloads\en_windows_7_professional_with_sp1_x64_dvd_u_676939.iso
Edition: Windows 7 Home Basic (6.1.7601.17514 / x64 / en-US)
Type: Microsoft Windows
Version: Windows 7 (64-bit)

✓ Skip Unattended Installation

You have selected to skip unattended guest OS install, the guest OS will need to be installed manually.

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

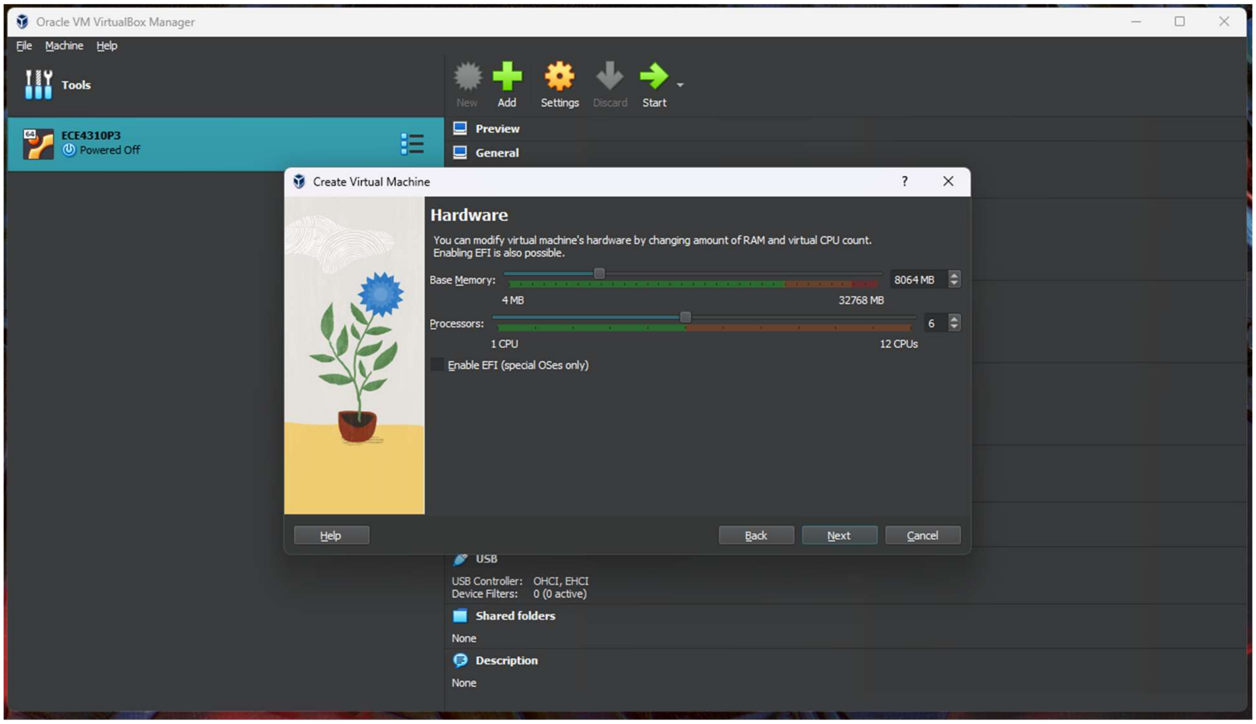
Shared folders

None

Description

None

Set the memory and amount of processors. In my case, I wanted to secure a smooth virtualization so I decided to utilize half of my hardware for this VM. A quarter of my specs would have been enough to demonstrate this.



Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 8064 MB (4 MB – 32768 MB)

Processors: 6 (1 CPU – 12 CPUs)

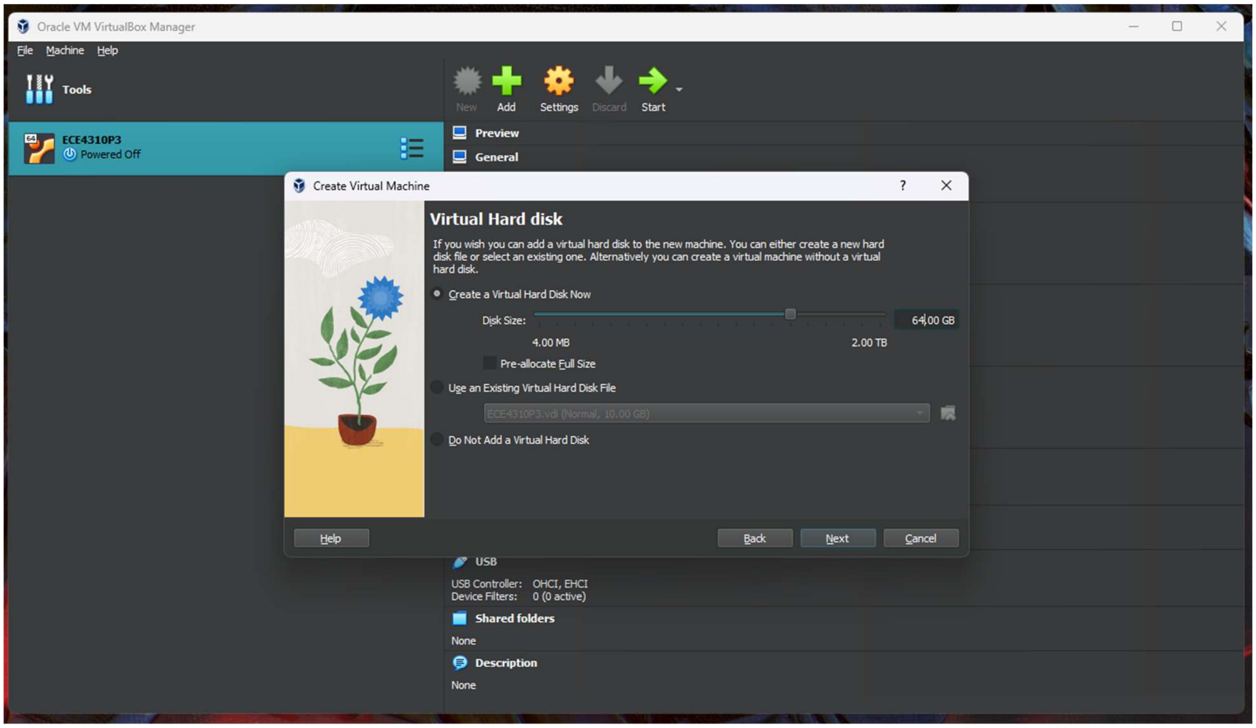
□ Enable EFI (special OSes only)

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders: None

Description: None

Set some storage for the machine, in this case I chose 64Gbs, ~20Gbs would've been enough to easily demonstrate this demo as win7 takes 10-14Gb of storage.



Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 64.00 GB (4.00 MB – 2.00 TB)

□ Pre-allocate Full Size

○ Use an Existing Virtual Hard Disk File

ECE4310P3.vdi (Normal, 10.00 GB)

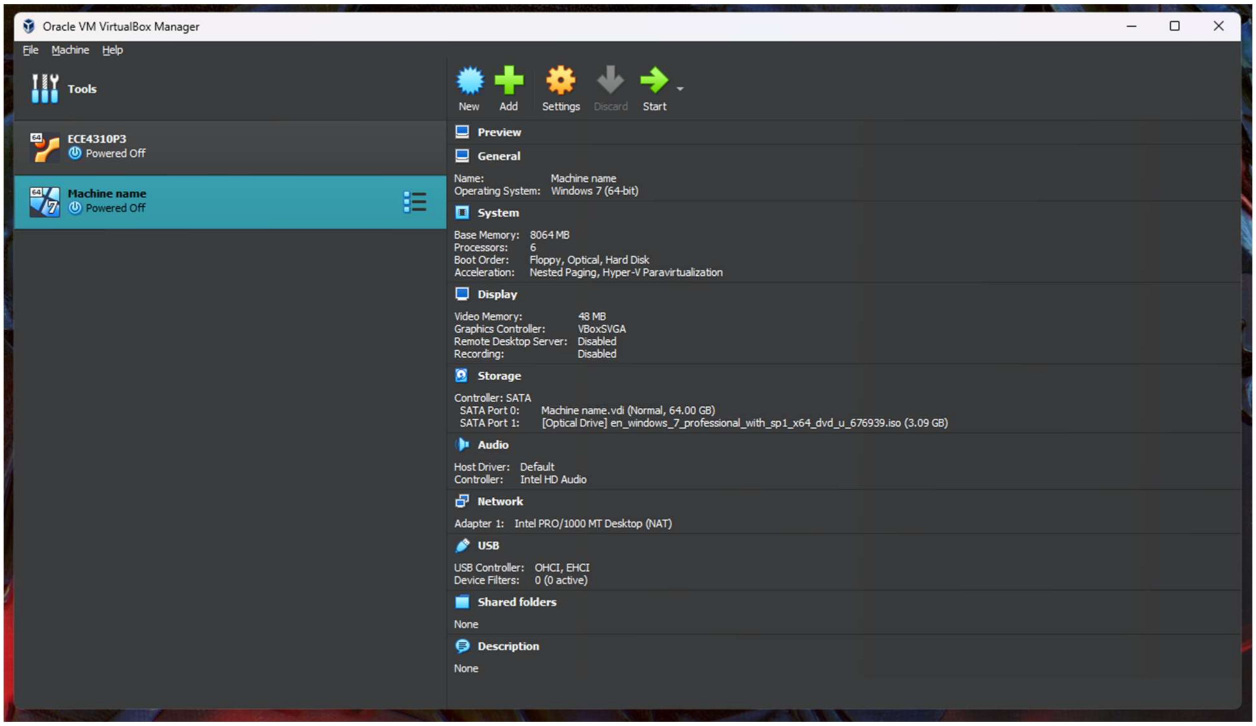
○ Do Not Add a Virtual Hard Disk

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders: None

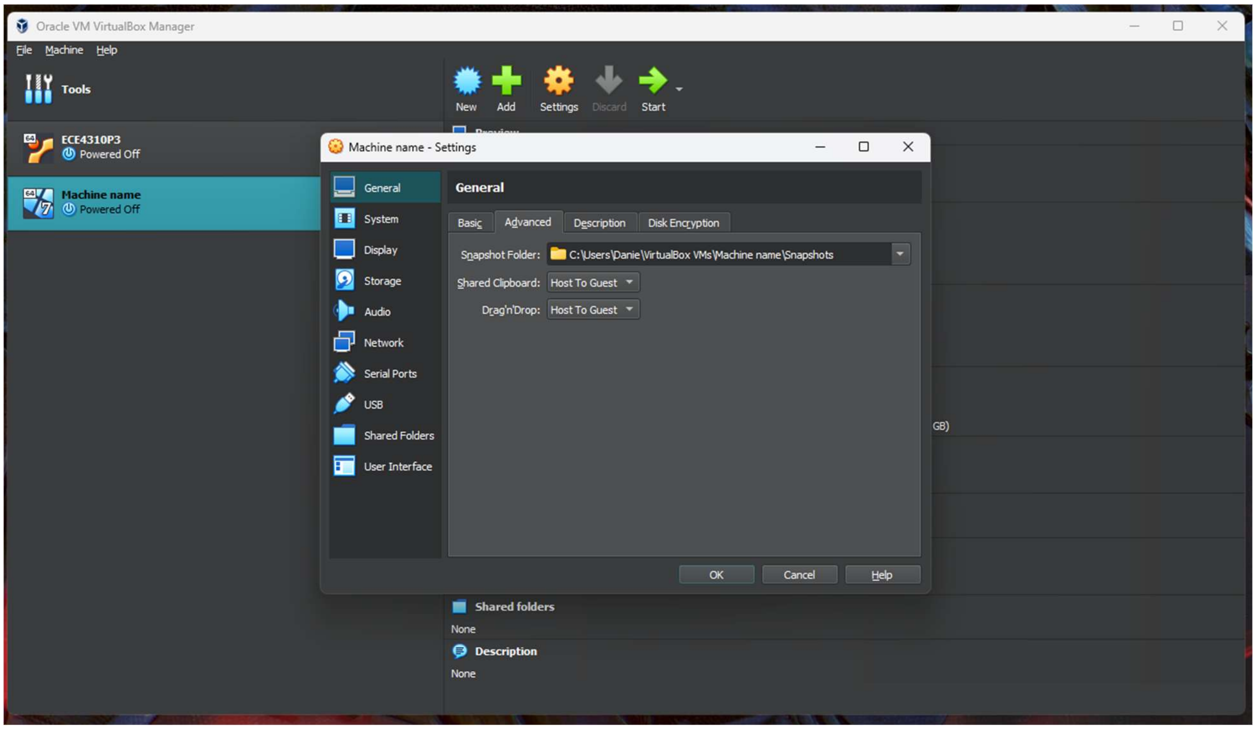
Description: None

This should be the results



```
ECE4310P3
Powered Off
Machine name
Powered Off

Preview

General
Name:              Machine name
Operating System:  Windows 7 (64-bit)

System
Base Memory:   8064 MB
Processors:    6
Boot Order:    Floppy, Optical, Hard Disk
Acceleration:  Nested Paging, Hyper-V Paravirtualization

Display
Video Memory:            48 MB
Graphics Controller:     VBoxSVGA
Remote Desktop Server:   Disabled
Recording:               Disabled

Storage
Controller: SATA
 SATA Port 0:     Machine name.vdi (Normal, 64.00 GB)
 SATA Port 1:     [Optical Drive] en_windows_7_professional_with_sp1_x64_dvd_u_676939.iso (3.09 GB)

Audio
Host Driver:   Default
Controller:    Intel HD Audio

Network
Adapter 1:   Intel PRO/1000 MT Desktop (NAT)

USB
USB Controller:   OHCI, EHCI
Device Filters:   0 (0 active)

Shared folders
None

Description
None
```

For this demo, I made sure I had drag n drop enabled from host to guest (PC to VM) to facilitate some files that will be required



```
ECE4310P3
Powered Off
Machine name
Powered Off

General
Snapshot Folder:  C:\Users\Danie\VirtualBox VMs\Machine name\Snapshots
Shared Clipboard: Host To Guest
Drag'n'Drop:      Host To Guest

Shared folders
None
Description
None
```

Note: Make sure to disable this at the moment of the malware download!

Ransomware preparations

Once that's setup, we can easily start our Windows 7 machine and proceed with the steps instructed. Make sure to download the basic drivers that can be found in the machine network (to easily access the internet).

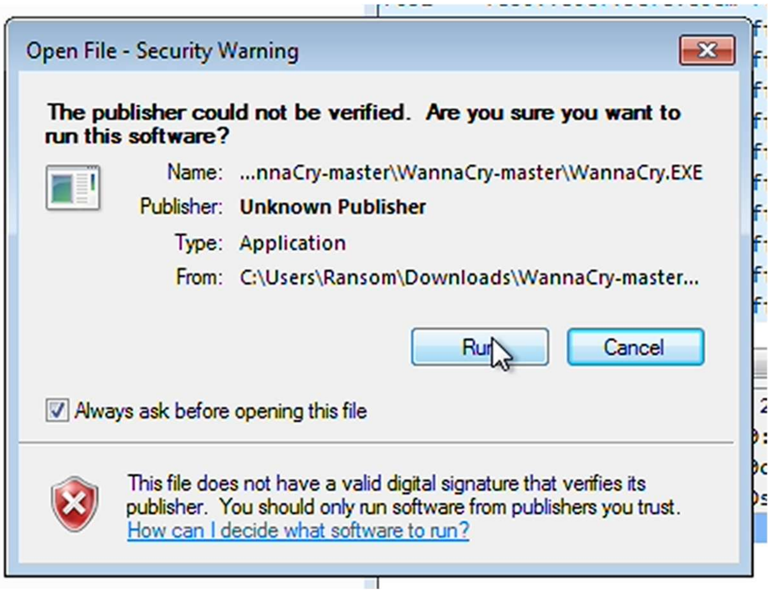
The only steps left to do would be to download the directory (.zip file) from the GitHub that contains the desired Ransomware. However, due to internet explorer being obsolete/unusable, we had to find a way to browse the internet to enter into GitHub as we didn't want to download the ransomware from any of our local machines. To do so, we found out that there's a basic chromium based browser called supermium [https://github.com/win32ss/supermium/releases], so we downloaded the files onto our local machines and then dragged them onto the VM.

Now with access to internet and a usable browser, we can access to the ransomware [https://github.com/SomeCodingCoolGuy/WannaCry], and before executing it, we downloaded Wireshark [https://www.wireshark.org/download/win32/all-versions] in our VMs as well to monitor the traffic. Due to the nature of ransomware, it will require some access to our network to download the software and notify the ransomware server to proceed with the attack.

We also transferred some files from our local machine to the VM so we can see some encryption by the malware on action, such as school projects and even a text note with some random text on it.

Ransomware attack

First, we extracted the folder of the ransomware that initially contained 3 files, two .txt files (LICENSE, README) and the .exe (executable ransomware). Once we clicked on it, Windows asked us if we were sure as the publisher was not verified, but obviously we proceeded.



Open File - Security Warning

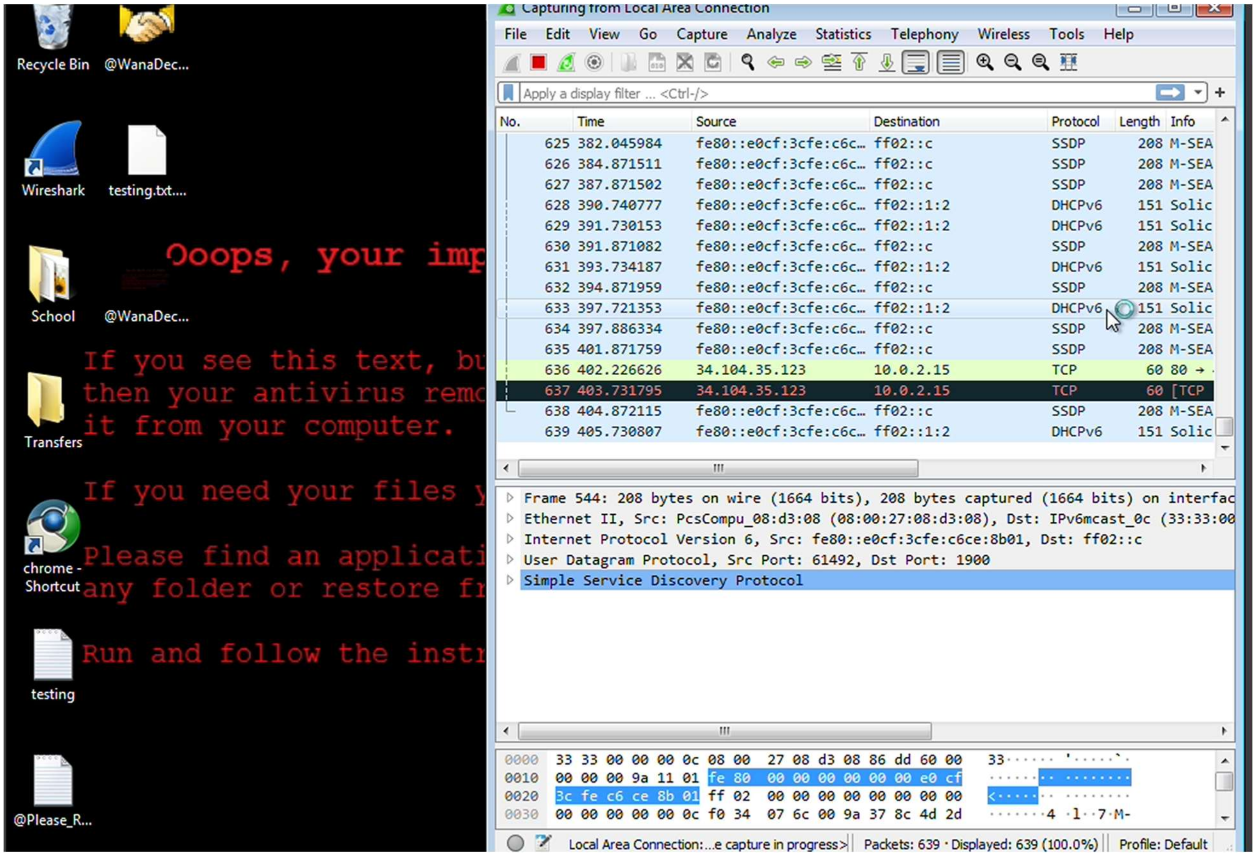
The publisher could not be verified. Are you sure you want to run this software?

Name: ...nnaCry-master\WannaCry-master\WannaCry.EXE
Publisher: **Unknown Publisher**
Type: Application
From: C:\Users\Ransom\Downloads\WannaCry-master...

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?

Shortly after we noticed a change in the wallpaper and some TCP protocols in our Wireshark.


Recycle Bin
@WanaDec...
Wireshark
testing.txt....
School
@WanaDec...
Transfers
chrome - Shortcut
testing
@Please_R...
Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Local Area Connection:...e capture in progress> Packets: 639 · Displayed: 639 (100.0%) Profile: Default

Ooops, your imp

If you see this text, bu
then your antivirus remo
it from your computer.

If you need your files y

Please find an applicati
any folder or restore fr

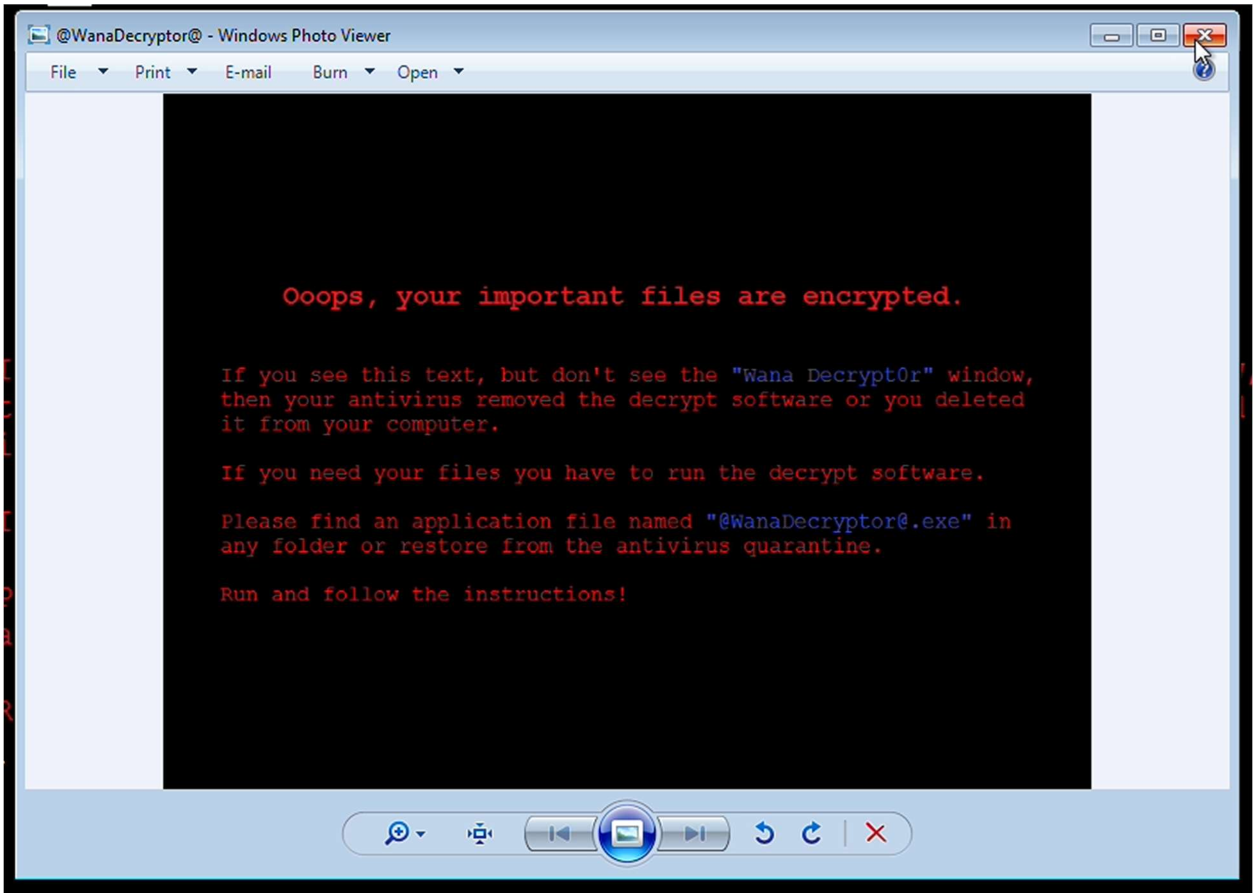
Run and follow the instr

```
No.   Time        Source               Destination  Protocol  Length Info
  625 382.045984  fe80::e0cf:3cfe:c6c… ff02::c      SSDP         208 M-SEA
  626 384.871511  fe80::e0cf:3cfe:c6c… ff02::c      SSDP         208 M-SEA
  627 387.871502  fe80::e0cf:3cfe:c6c… ff02::c      SSDP         208 M-SEA
  628 390.740777  fe80::e0cf:3cfe:c6c… ff02::1:2    DHCPv6       151 Solic
  629 391.730153  fe80::e0cf:3cfe:c6c… ff02::1:2    DHCPv6       151 Solic
  630 391.871082  fe80::e0cf:3cfe:c6c… ff02::c      SSDP         208 M-SEA
  631 393.734187  fe80::e0cf:3cfe:c6c… ff02::1:2    DHCPv6       151 Solic
  632 394.871959  fe80::e0cf:3cfe:c6c… ff02::c      SSDP         208 M-SEA
  633 397.721353  fe80::e0cf:3cfe:c6c… ff02::1:2    DHCPv6       151 Solic
  634 397.886334  fe80::e0cf:3cfe:c6c… ff02::c      SSDP         208 M-SEA
  635 401.871759  fe80::e0cf:3cfe:c6c… ff02::c      SSDP         208 M-SEA
  636 402.226626  34.104.35.123        10.0.2.15    TCP           60 80 →
  637 403.731795  34.104.35.123        10.0.2.15    TCP           60 [TCP
  638 404.872115  fe80::e0cf:3cfe:c6c… ff02::c      SSDP         208 M-SEA
  639 405.730807  fe80::e0cf:3cfe:c6c… ff02::1:2    DHCPv6       151 Solic
```

```
Frame 544: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interfac
Ethernet II, Src: PcsCompu_08:d3:08 (08:00:27:08:d3:08), Dst: IPv6mcast_0c (33:33:00
Internet Protocol Version 6, Src: fe80::e0cf:3cfe:c6ce:8b01, Dst: ff02::c
User Datagram Protocol, Src Port: 61492, Dst Port: 1900
Simple Service Discovery Protocol
```

```
0000  33 33 00 00 00 0c 08 00  27 08 d3 08 86 dd 60 00   33······ '·····`·
0010  00 00 00 9a 11 01 fe 80  00 00 00 00 00 00 e0 cf   ········ ········
0020  3c fe c6 ce 8b 01 ff 02  00 00 00 00 00 00 00 00   <······· ········
0030  00 00 00 00 00 0c f0 34  07 6c 00 9a 37 8c 4d 2d   ·······4 ·l··7·M-
```

The wallpaper seems to be an automatic process of the ransomware, which downloads the image and sets it up as the wallpaper shortly after executing it.



Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

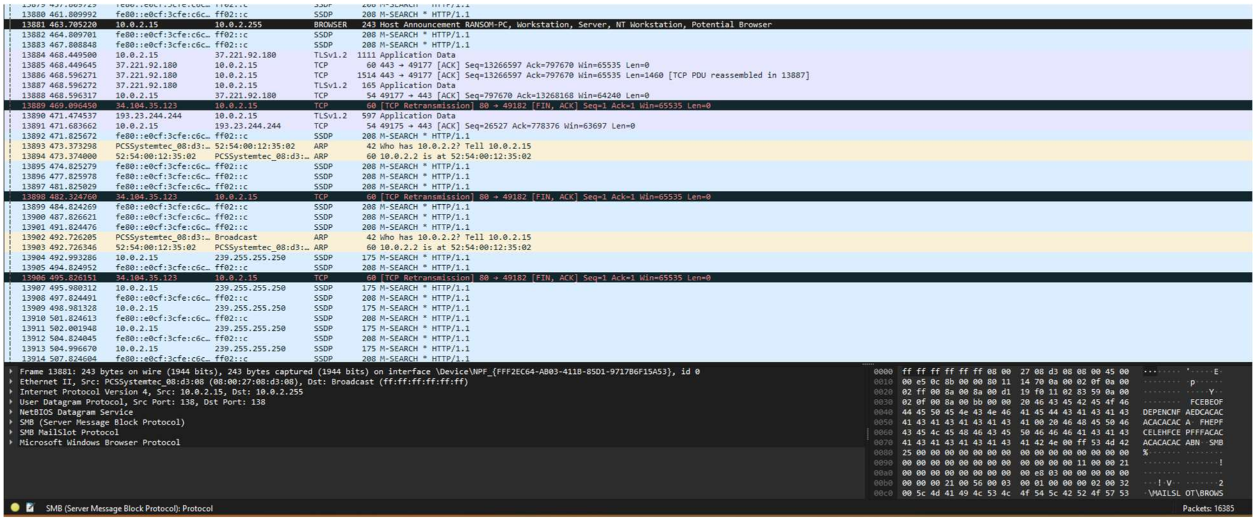
Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

When it comes to our Wireshark monitoring, we see multiple protocols happening, mostly done through Google.

However, we can identify some indicators:

Some traffic in SMB (IPs: 34.104.35.123 and 37.221.92.180)

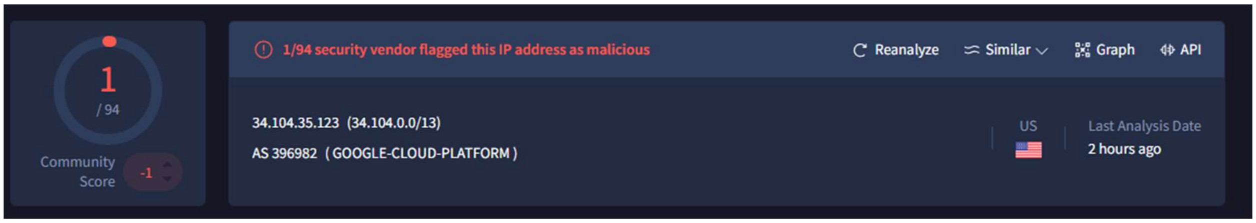


```
13879 457.809729  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13880 461.809992  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13881 463.705220  10.0.2.15            10.0.2.255          BROWSER   243 Host Announcement RANSOM-PC, Workstation, Server, NT Workstation, Potential Browser
13882 464.809701  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13883 467.808848  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13884 468.449500  10.0.2.15            37.221.92.180       TLSv1.2  1111 Application Data
13885 468.449645  37.221.92.180        10.0.2.15           TCP        60 443 → 49177 [ACK] Seq=13266597 Ack=797670 Win=65535 Len=0
13886 468.596271  37.221.92.180        10.0.2.15           TCP      1514 443 → 49177 [ACK] Seq=13266597 Ack=797670 Win=65535 Len=1460 [TCP PDU reassembled in 13887]
13887 468.596272  37.221.92.180        10.0.2.15           TLSv1.2   165 Application Data
13888 468.596317  10.0.2.15            37.221.92.180       TCP        54 49177 → 443 [ACK] Seq=797670 Ack=13268168 Win=64240 Len=0
13889 469.096450  34.104.35.123        10.0.2.15           TCP        60 [TCP Retransmission] 80 → 49182 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
13890 471.474537  193.23.244.244       10.0.2.15           TLSv1.2   597 Application Data
13891 471.683662  10.0.2.15            193.23.244.244      TCP        54 49175 → 443 [ACK] Seq=26527 Ack=778376 Win=63697 Len=0
13892 471.825672  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13893 473.373298  PCSSystemtec_08:d3:… 52:54:00:12:35:02   ARP        42 Who has 10.0.2.2? Tell 10.0.2.15
13894 473.374000  52:54:00:12:35:02    PCSSystemtec_08:d3:… ARP       60 10.0.2.2 is at 52:54:00:12:35:02
13895 474.825279  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13896 477.825978  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13897 481.825029  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13898 482.324760  34.104.35.123        10.0.2.15           TCP        60 [TCP Retransmission] 80 → 49182 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
13899 484.824269  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13900 487.826621  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13901 491.824476  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13902 492.726205  PCSSystemtec_08:d3:… Broadcast           ARP        42 Who has 10.0.2.2? Tell 10.0.2.15
13903 492.726346  52:54:00:12:35:02    PCSSystemtec_08:d3:… ARP       60 10.0.2.2 is at 52:54:00:12:35:02
13904 492.993286  10.0.2.15            239.255.255.250     SSDP      175 M-SEARCH * HTTP/1.1
13905 494.824952  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13906 495.826151  34.104.35.123        10.0.2.15           TCP        60 [TCP Retransmission] 80 → 49182 [FIN, ACK] Seq=1 Ack=1 Win=65535 Len=0
13907 495.980312  10.0.2.15            239.255.255.250     SSDP      175 M-SEARCH * HTTP/1.1
13908 497.824491  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13909 498.981328  10.0.2.15            239.255.255.250     SSDP      175 M-SEARCH * HTTP/1.1
13910 501.824613  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13911 502.001948  10.0.2.15            239.255.255.250     SSDP      175 M-SEARCH * HTTP/1.1
13912 504.824045  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
13913 504.996670  10.0.2.15            239.255.255.250     SSDP      175 M-SEARCH * HTTP/1.1
13914 507.824604  fe80::e0cf:3cfe:c6c… ff02::c             SSDP      208 M-SEARCH * HTTP/1.1
```

```
› Frame 13881: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface \Device\NPF_{FFF2EC64-AB03-411B-85D1-9717B6F15A53}, id 0
› Ethernet II, Src: PCSSystemtec_08:d3:08 (08:00:27:08:d3:08), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.255
› User Datagram Protocol, Src Port: 138, Dst Port: 138
› NetBIOS Datagram Service
› SMB (Server Message Block Protocol)
› SMB MailSlot Protocol
› Microsoft Windows Browser Protocol
```

```
0000  ff ff ff ff ff ff 08 00  27 08 d3 08 08 00 45 00   ········ '·····E·
0010  00 e5 0c 8b 00 00 80 11  14 70 0a 00 02 0f 0a 00   ········ ·p······
0020  02 ff 00 8a 00 8a 00 d1  19 f0 11 02 83 59 0a 00   ········ ·····Y··
0030  02 0f 00 8a 00 bb 00 00  20 46 43 45 42 45 4f 46   ········  FCEBEOF
0040  44 45 50 45 4e 43 4e 46  41 45 44 43 41 43 41 43   DEPENCNF AEDCACAC
0050  41 43 41 43 41 43 41 43  41 00 20 46 48 45 50 46   ACACACAC A· FHEPF
0060  43 45 4c 45 48 46 43 45  50 46 46 46 41 43 41 43   CELEHFCE PFFFACAC
0070  41 43 41 43 41 43 41 43  41 42 4e 00 ff 53 4d 42   ACACACAC ABN··SMB
0080  25 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   %······· ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 11 00 00 21   ········ ·······!
00a0  00 00 00 00 00 00 00 00  00 e8 03 00 00 00 00 00   ········ ········
00b0  00 00 00 21 00 56 00 03  00 01 00 00 00 02 00 32   ···!·V·· ·······2
00c0  00 5c 4d 41 49 4c 53 4c  4f 54 5c 42 52 4f 57 53   ·\MAILSL OT\BROWS
```

Here the reports of these two IPs respectively (through https://www.virustotal.com/)



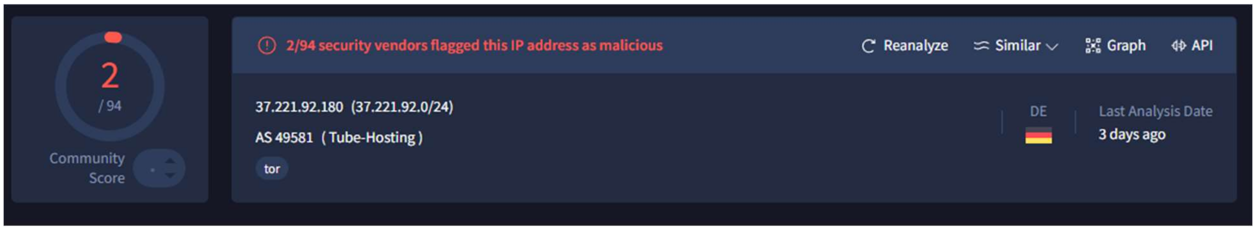
1/94 security vendor flagged this IP address as malicious

34.104.35.123 (34.104.0.0/13)

AS 396982 (GOOGLE-CLOUD-PLATFORM)

US

Last Analysis Date
2 hours ago



2/94 security vendors flagged this IP address as malicious

37.221.92.180 (37.221.92.0/24)

AS 49581 (Tube-Hosting)

tor

DE

Last Analysis Date
3 days ago

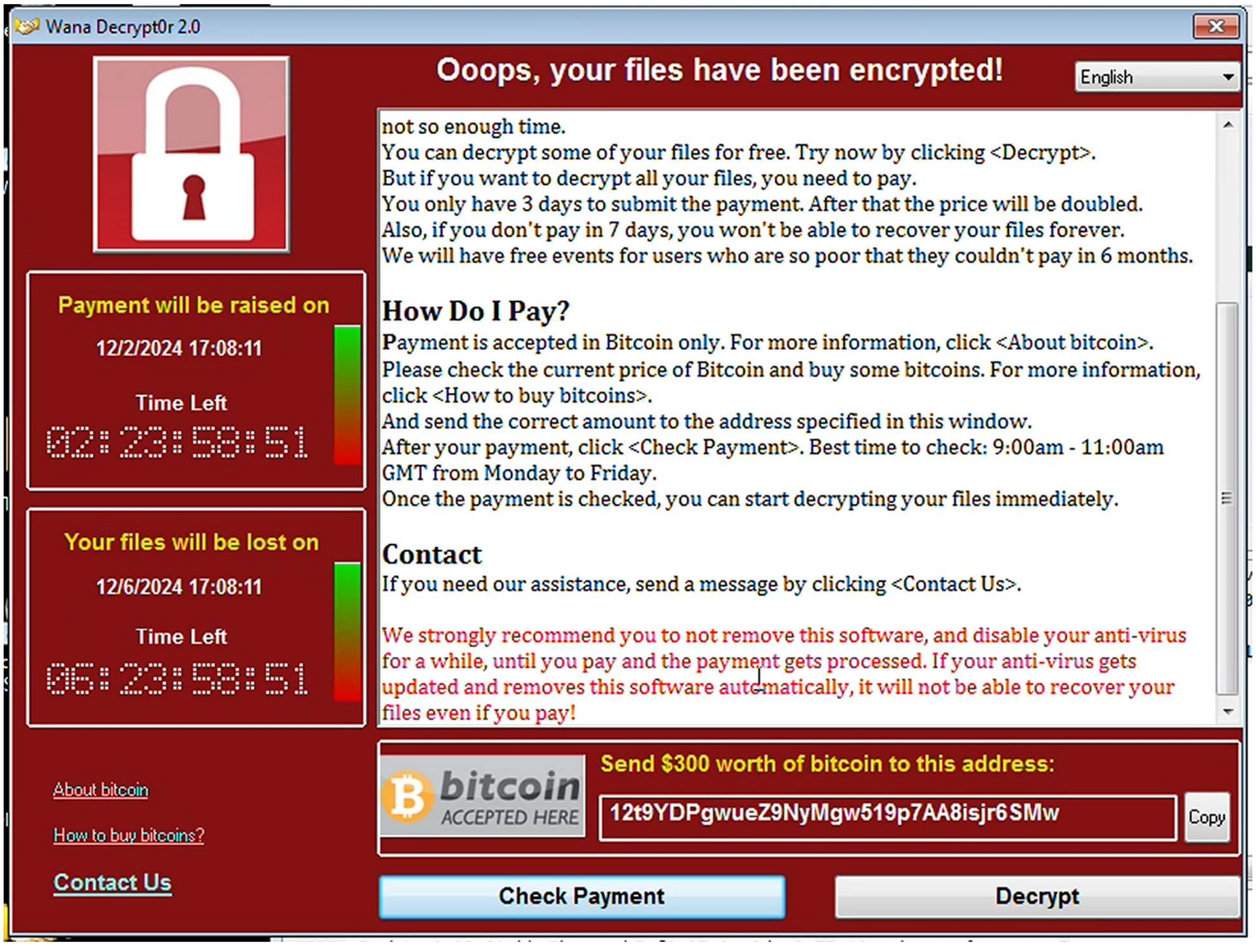
We also found quite some traffic in the DNS with requests to the, possibly, the execution of the ransomware “ iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com “.

Furthermore, some malformed SMB commands like “TreeConnectAndX” and “WriteAndX”.

Last but not least, we also found some extensive queries to TLSv1.3 and QUIC traffic, which indicates a possible malicious activity.

When it comes to “raw” data from Wireshark, these were the findings. While the report was quite large, with multiple protocols happening at the same time, it is obvious that the ransomware was communicating with a server as there’s barely any logs before the malware is executed.

Once the malware is activated, it will be prompting a payment request in Bitcoin to the bad actors so they could "decrypt" the victim's files.



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 GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.

Contact
If you need our assistance, send a message by clicking <Contact Us>.

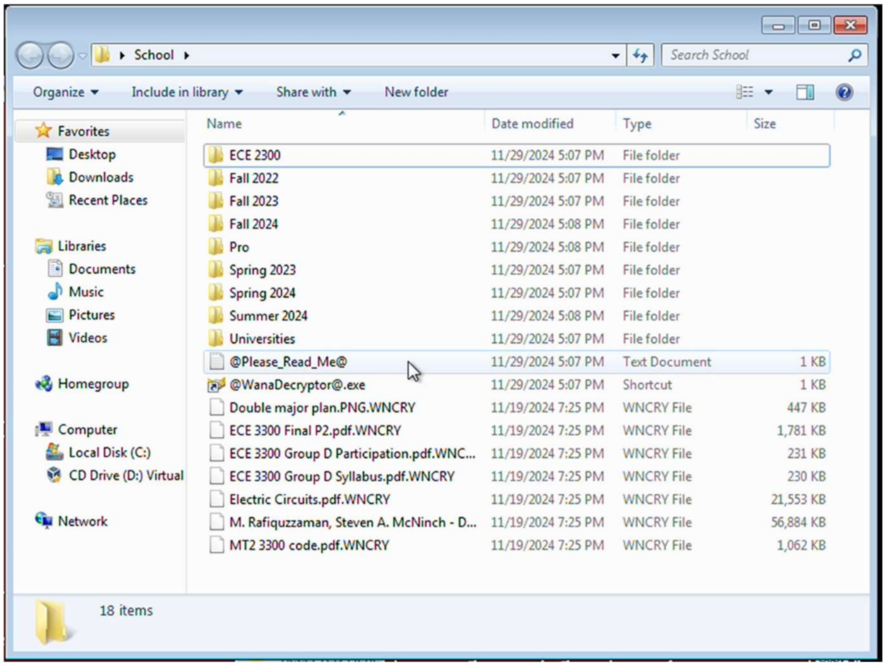
We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

Payment will be raised on
12/2/2024 17:08:11
Time Left
02:23:58:51

Your files will be lost on
12/6/2024 17:08:11
Time Left
06:23:58:51

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

The hyperlinks this window offer us are a Wikipedia link to what is Bitcoin, a google search of "how to buy bitcoin" and contact us wasn't prompting an error. Check payment will load a "payment" checker which probably would do nothing, and the decrypt might be a way of the hacker to send an activation key to "disarm" the ransomware.

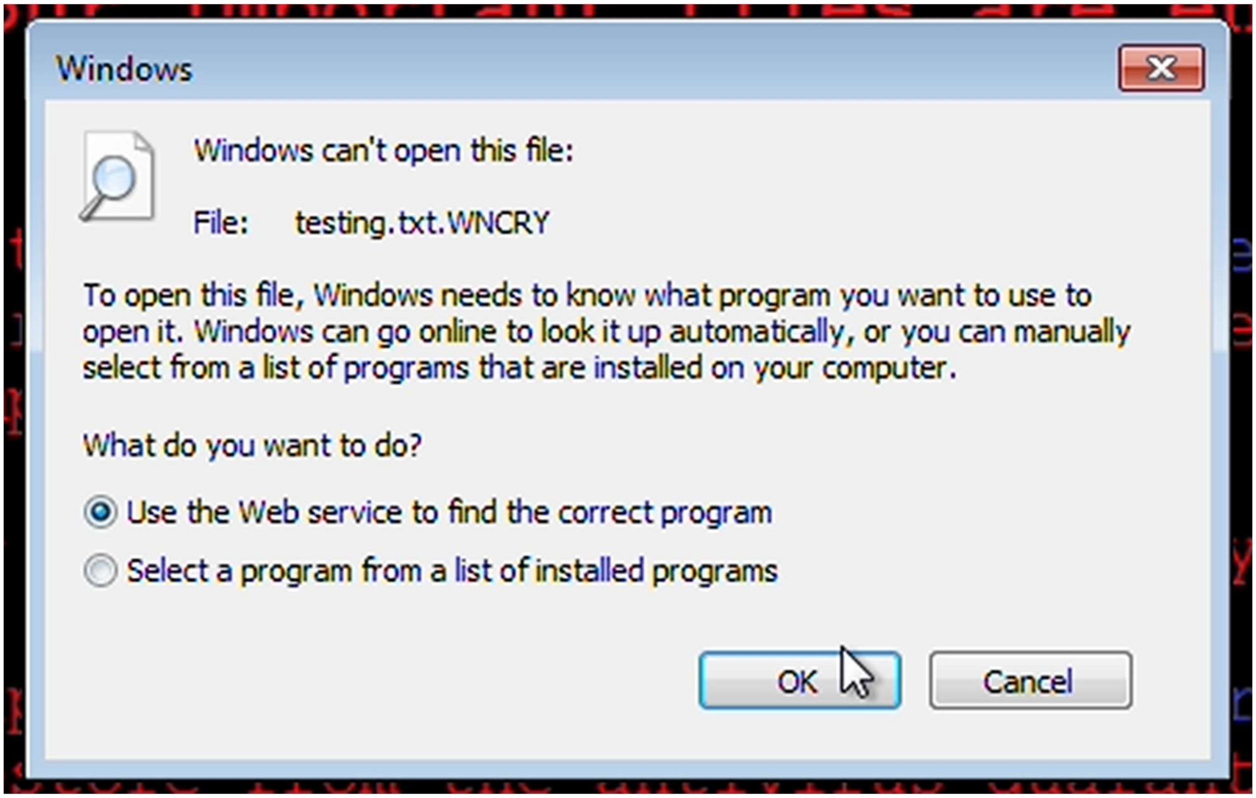


Name	Date modified	Type	Size
ECE 2300	11/29/2024 5:07 PM	File folder	
Fall 2022	11/29/2024 5:07 PM	File folder	
Fall 2023	11/29/2024 5:07 PM	File folder	
Fall 2024	11/29/2024 5:08 PM	File folder	
Pro	11/29/2024 5:08 PM	File folder	
Spring 2023	11/29/2024 5:07 PM	File folder	
Spring 2024	11/29/2024 5:07 PM	File folder	
Summer 2024	11/29/2024 5:08 PM	File folder	
Universities	11/29/2024 5:07 PM	File folder	
@Please_Read_Me@	11/29/2024 5:07 PM	Text Document	1 KB
@WanaDecryptor@.exe	11/29/2024 5:07 PM	Shortcut	1 KB
Double major plan.PNG.WNCRY	11/19/2024 7:25 PM	WNCRY File	447 KB
ECE 3300 Final P2.pdf.WNCRY	11/19/2024 7:25 PM	WNCRY File	1,781 KB
ECE 3300 Group D Participation.pdf.WNC...	11/19/2024 7:25 PM	WNCRY File	231 KB
ECE 3300 Group D Syllabus.pdf.WNCRY	11/19/2024 7:25 PM	WNCRY File	230 KB
Electric Circuits.pdf.WNCRY	11/19/2024 7:25 PM	WNCRY File	21,553 KB
M. Rafiquzzaman, Steven A. McNinch - D...	11/19/2024 7:25 PM	WNCRY File	56,884 KB
MT2 3300 code.pdf.WNCRY	11/19/2024 7:25 PM	WNCRY File	1,062 KB

18 items

Once we check the files we transfer to the VM machine, we can see how images and documents were encrypted with .WNCRY.

The attempt to open any of these files will result in a error as Windows will not know how to properly open these files



Windows

Windows can't open this file:

File: testing.txt.WNCRY

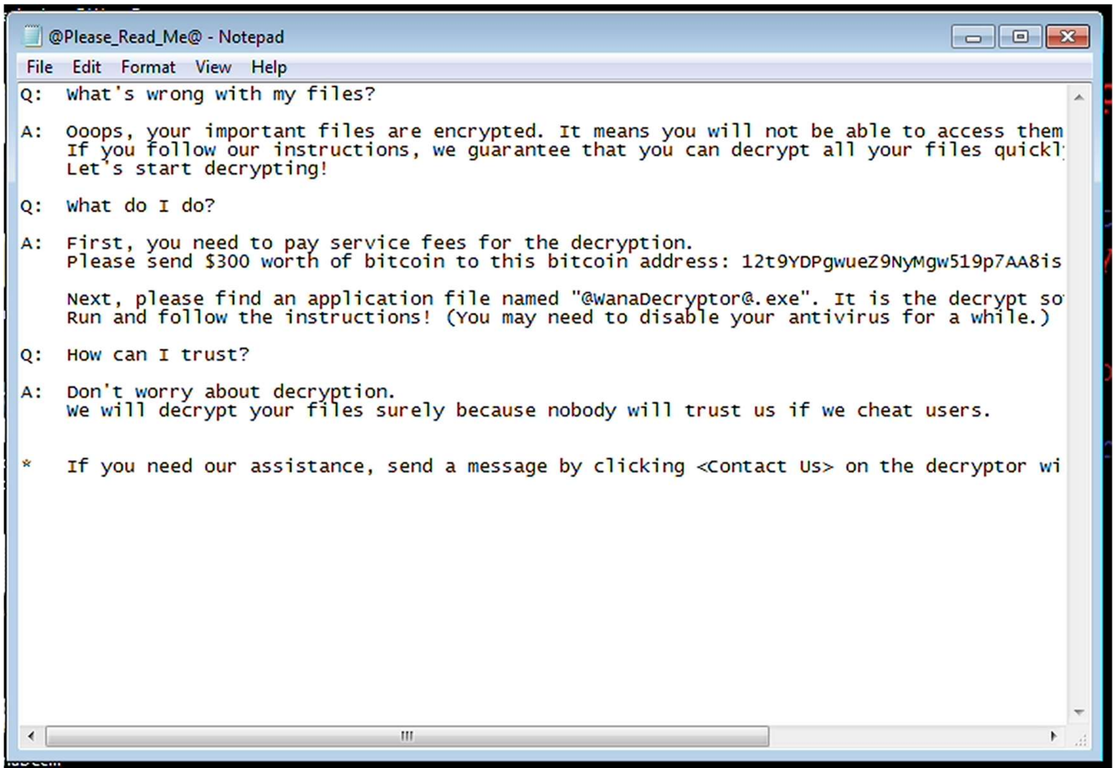
To open this file, Windows needs to know what program you want to use to open it. Windows can go online to look it up automatically, or you can manually select from a list of programs that are installed on your computer.

What do you want to do?

● Use the Web service to find the correct program

○ Select a program from a list of installed programs

Besides of the encryption, we can also see how the creator of this malware made sure to explain to the victim “what was going on” and how to get rid of the issue. He did this by creating .txt files called “@Please_Read_Me@”



```
Q:  What's wrong with my files?

A:  Ooops, your important files are encrypted. It means you will not be able to access them
    If you follow our instructions, we guarantee that you can decrypt all your files quickl
    Let's start decrypting!

Q:  What do I do?

A:  First, you need to pay service fees for the decryption.
    Please send $300 worth of bitcoin to this bitcoin address: 12t9YDPgwueZ9NyMgw519p7AA8is

    Next, please find an application file named "@WanaDecryptor@.exe". It is the decrypt so
    Run and follow the instructions! (You may need to disable your antivirus for a while.)

Q:  How can I trust?

A:  Don't worry about decryption.
    We will decrypt your files surely because nobody will trust us if we cheat users.


*   If you need our assistance, send a message by clicking <Contact Us> on the decryptor wi
```

An interesting fact of this ransomware is continuously active until disarmed, so injecting a flash drive to the VM will cause the USB to also fall under the WannaCry encryption. Although this was a problem when I introduced the flash drive into the VM, we also noticed that not all files are encrypted, but mostly document/images/video files. We presume that the creator didn't want to attack the whole system as that would defeat the whole purpose of his attack, as that could affect files that were critical for the system to operate. Some files that were not affected that are not critical for Windows to operate were .JSON (JavaScript Object Notation) and .pcapng (Wireshark file).

With this, we would finalize the attack to our VM by executing the WannaCry ransomware.

How to defend against WannaCry and similar ransomware

Ransomware attacks, such as WannaCry, have highlighted critical vulnerabilities in modern cybersecurity practices and the devastating impact these attacks can have on individuals, organizations, and governments. To combat such threats effectively, a comprehensive, multi-layered defense strategy is required. This section will outline key methods to defend against ransomware like WannaCry and provide a final summary of this project.

1. System Updates and Patch Management

The WannaCry ransomware exploited the EternalBlue vulnerability in the Windows SMB protocol, which had already been addressed by Microsoft in its MS17-010 patch. However, many systems remained unpatched due to outdated infrastructure, lack of patching policies, or negligence. To prevent such exploits, organizations must implement a structured **patch management process** to ensure that all devices, including legacy systems, are regularly updated. Tools for automated patch management can help track and apply updates systematically, closing vulnerabilities before attackers can exploit them.

2. Network Segmentation and Access Controls

A critical factor in WannaCry's widespread impact was its ability to propagate across networks autonomously. **Network segmentation** mitigates this risk by dividing an organization's network into isolated zones, restricting ransomware's ability to move laterally between systems. Additionally, **network access controls (NAC)** limit device connectivity and prevent unauthorized devices from joining the network. For added security, disabling outdated and unnecessary protocols, such as SMBv1, removes potential attack vectors that ransomware might exploit.

3. Behavior-Based Detection and Anti-Ransomware Tools

Traditional signature-based antivirus software struggled to detect WannaCry due to its novel methods. Modern defenses require **behavior-based detection tools** that identify suspicious activities, such as mass file encryption or unusual network traffic. These tools can flag and halt ransomware-like behavior before it spreads widely. Advanced solutions, powered by machine learning, improve adaptability to new ransomware strains, ensuring better protection against emerging threats.

4. Secure Data Backups and Recovery

Regular **data backups** stored offline or in isolated environments are among the most effective defenses against ransomware. In the case of WannaCry, victims who had reliable backups could recover their data without paying the ransom. Backup solutions should include regular testing to ensure they work effectively and include features like encryption to prevent backup tampering by attackers.

5. User Education and Awareness

While WannaCry primarily relied on EternalBlue, many ransomware attacks use phishing emails and social engineering to gain initial access. Educating users to identify suspicious emails, links, and attachments can significantly reduce the chances of infection. Training sessions and simulated phishing exercises help reinforce good cybersecurity habits among employees and end-users.

6. Advanced Incident Response Planning

Preparedness is key to minimizing the impact of a ransomware attack. Organizations should develop and routinely test **incident response plans** that outline procedures for detecting, containing, and recovering from ransomware incidents. A robust plan ensures that all stakeholders understand their roles, reducing response times and mitigating damage.

Project Summary

This project provided an in-depth exploration of WannaCry ransomware, including its methods of propagation, encryption techniques, and the extensive damage it caused. WannaCry leveraged the EternalBlue exploit to spread rapidly across networks, targeting unpatched systems. Its use of RSA and AES encryption rendered affected files inaccessible without the attackers' decryption key, causing significant financial and operational disruptions.

The simulation conducted during this project demonstrated WannaCry's behavior in a controlled environment, utilizing VMOracle as the virtualization tool. The simulation highlighted how WannaCry infects systems, encrypts data, and attempts to propagate through network vulnerabilities. Additionally, network traffic analysis using Wireshark revealed indicators of compromise and malicious server communication, offering valuable insights into the ransomware's operation.

To conclude, defending against ransomware attacks like WannaCry requires a proactive approach combining timely system updates, network segmentation, advanced detection tools, secure backups, and user education. By implementing these strategies, organizations can strengthen their defenses and minimize the risk of future ransomware incidents. This project underscores the importance of maintaining robust cybersecurity measures and provides a foundation for further research and preparedness in combating evolving cyber threats.

By reflecting on this incident, we are reminded that the digital landscape is continually evolving, requiring constant vigilance, innovation, and collaboration to address emerging challenges.

Sources

- WannaCrypt ransomware worm targets out-of-date systems https://www.microsoft.com/en-us/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

- Investigation: WannaCry cyber attack and the NHS https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/

- Indicators Associated With WannaCry Ransomware https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware

- What is WANNACRY/WANACRYPTOR? https://www.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf

- What you need to know about the WannaCry Ransomware https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware

Software

- https://www.oracle.com/virtualization/technologies/vm/downloads/virtualbox-downloads.html

- https://archive.org/details/windows-7-iso

- https://github.com/win32ss/supermium/releases

- https://www.wireshark.org/download/win32/all-versions

- https://github.com/SomeCodingCoolGuy/WannaCry