UNIVERSITY OF SCIENCE AND TECHNOLOGY OF HA NOI

Final Report for IDS/IPS

Bad Rabbit Ransomware Attack

Prepared by:

Nguyen Le Dinh Vu, BI11-291

Under the teaching of :

Assoc. Prof. Pham Thanh Giang, USTH

December 2022

Contents

I. Introduction

1. Context

Ransomware is a type of malware designed to deny a user or organization access to the files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest way to regain access to their documents. The first ransomware attack happened in 1989 (AIDS Trojan). Since a lot of ransomware and dozens of ransomware variants have been developed and used in many attacks (WannaCry in 2017, Petya and NotPetya in 2016,…)

Nowadays, some ransomware still threatens many people although we have improved our knowledge about them. This paper will provide some information and my understanding of one ransomware named Bad Rabbit.

2. Objective

- Provide basic information about the ransomware
- Show the implementation in the virtual environment
- Present solutions to avoid the threat

II. About Bad Rabbit

1. Background

Bad Rabbit is ransomware belonging to the Petya family of ransomware that hit over 200 organizations throughout Eastern Europe in October 2017. Targets were primarily Russian media agencies however various corporate networks throughout Russia, Eastern Europe, and Japan were hit due to the method that ransomware used to spread through networks. Like other strains of ransomware, Bad Rabbit virus locks up victims' computers, servers, or files and prevents them from regaining access until a ransom—usually in Bitcoin—is paid.

Bad Rabbit timeline:

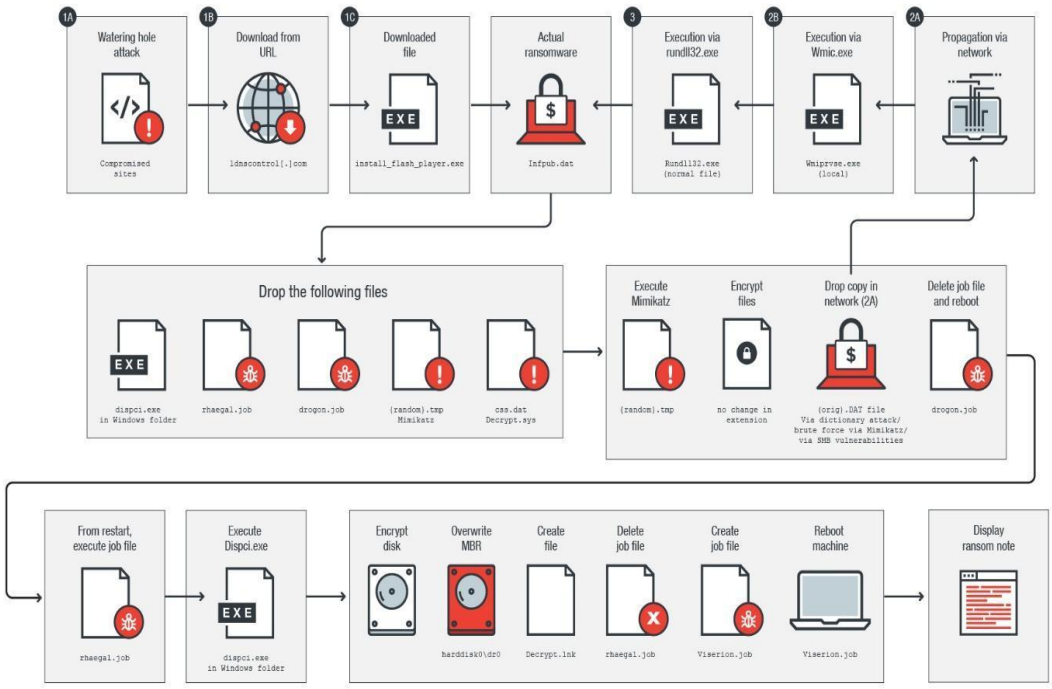
- March 2016 Petya First Spotted
- April 2017 Shadow Brokers Leak EternalRomance
- June 2017 NotPetya First Spotted
- Oct 12th Ukraine's SBU Warns of imminent attack similar to the NotPetya
- Oct 24th 2017 BadRabbit First Spotted

Bad Rabbit ransomware encrypts the following types of files: [7]
.3ds .7z .accdb .ai .asm .asp .aspx .avhd .back .bak .bmp .brw .c .cab .cc .cer .cfg .conf .cpp .crt .cs .ctl .cxx .dbf .der .dib .disk .djvu .doc .docx .dwg .eml .fdb .gz .h .hdd .hpp .hxx .iso .java .jfif .jpe .jpeg .jpg .js .kdbx .key .mail .mdb .msg .nrg .odc .odf .odg .odi .odm .odp .ods .odt .ora .ost .ova .ovf .p12 .p7b .p7c .pdf .pem .pfx .php .pmf .png .ppt .pptx .ps1 .pst .pvi .py .pyc .pyw .qcow .qcow2 .rar .rb .rtf .scm .sln .sql .tar .tib .tif .tiff .vb .vbox .vbs .vcb .vd .vfd .vhd .vhdx .vmc .vmdk .vmsd .vmtm .vmx .vsdx .vsv .work .xls .xlsx .xml .xvd .zip

2. Description

a) Inflection way

Bad Rabbit uses a typical watering hole attack. With several compromised sites it attempts to convince users to install a fake Flash installer. If clicked, the installer drops malicious files.



Infection chain of Bad Rabbit

The following sites were hacked, and visitors were forced to download the Bad Rabbit installer. [7]

- hxxp://www.fontanka[.]ru
- hxxp://www.otbrana[.]com
- hxxp://grupovo[.]bg
- hxxp://i24.com[.]ua

- hxxp://spbvoditel[.]ru
- hxxp://blog.fontanka[.]ru
- hxxp://www.pensionhotel[.]cz
- hxxp://www.sinematurk[.]com
- hxxp://most-dnepr[.]info
- hxxp://www.imer[.]ro
- hxxp://calendar.fontanka[.]ru
- hxxp://an-crimea[.]ru
- hxxp://www.online812[.]ru
- hxxp://www.aica.co[.]jp
- hxxp://www.mediaport[.]ua
- hxxp://ankerch-crimea[.]ru
- hxxp://novayagazeta.spb[.]ru
- hxxp://osvitaportal.com[.]ua
- hxxp://www.grupovo[.]bg
- hxxp://argumenti[.]ru
- hxxp://bg.pensionhotel[.]com
- hxxp://argumentiru[.]com
- hxxp://www.t.ks[.]ua

b) Spreading way

It uses a dictionary attack to harvest credentials from the infected computer and tries to access computers from the same network and spread laterally. Bad Rabbit also spreads via the SMB file sharing protocol. It attempts to brute force any administrative shares it finds; if successful it drops a copy of itself into these shares. If these bruteforce attacks fails, it uses an exploit targeting the EternalRomance SMB vulnerability resolved in MS17-010. Bad Rabbit would

also run full disk encryption with DiskCryptor an open-source encryption application.[1]

c) Execution process [2]

Drop and create the sample (scheduled task):

- **install_flash_player.exe**: masqueraded as the Flash Player installer, which is actually the BadRabbit dropper
- **infpub.dat**: dropped DLL file, which is the ransomware BadRabbit for subsequent encryption and ransom
- **cscc.dat**: for disk encryption (DiskCryptor)
- **dispci.exe**: used for installing BootLocker, encrypting files, and decrypting files after a reboot
- **4.tmp**: Mimikatz module
- **rhaegal.job**: scheduled task for executing discpci.exe to encrypt files (/c schtasks /Create /RU SYSTEM /SC ONSTART /TN rhaegal /TR "C:\WINDOWS\system32\cmd.exe /C Start \"\" \"C:\Windows\dispci.exe\" -id 848053675 && exit")
- **drogon.job**: scheduled task for rebooting the infected host and displaying the ransom note (/c schtasks /Create /SC once /TN drogon /RU SYSTEM /TR "C:\WINDOWS\system32\shutdown.exe /r /t 0 /f" /ST ::<HH>:<MM>:<SS>)

When clicked, the file **install_flash_player.exe** (we have seen SHA1:de5c8d858e6e41da715dca1c019df0bfb92d32c0) drops the file *infpub.dat* (SHA1: 79116fe99f2b421c52ef64097f0f39b815b20907) into the ***%SystemRoot%*** folder and runs it as "rundll32.exe ***%SystemRoot%*** \infpub.dat,#1 15".

It then drops the file cscc.dat in %windows%. This file is a driver for an open-source encryption solution, DiskCryptor. It then writes "cscc" into the registry:

- Write "cscc" to HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}\LowerFilters
- Write "cscc" to KEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}\UpperFilters
- Write "cscc" to HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CrashControl\DumpFilters

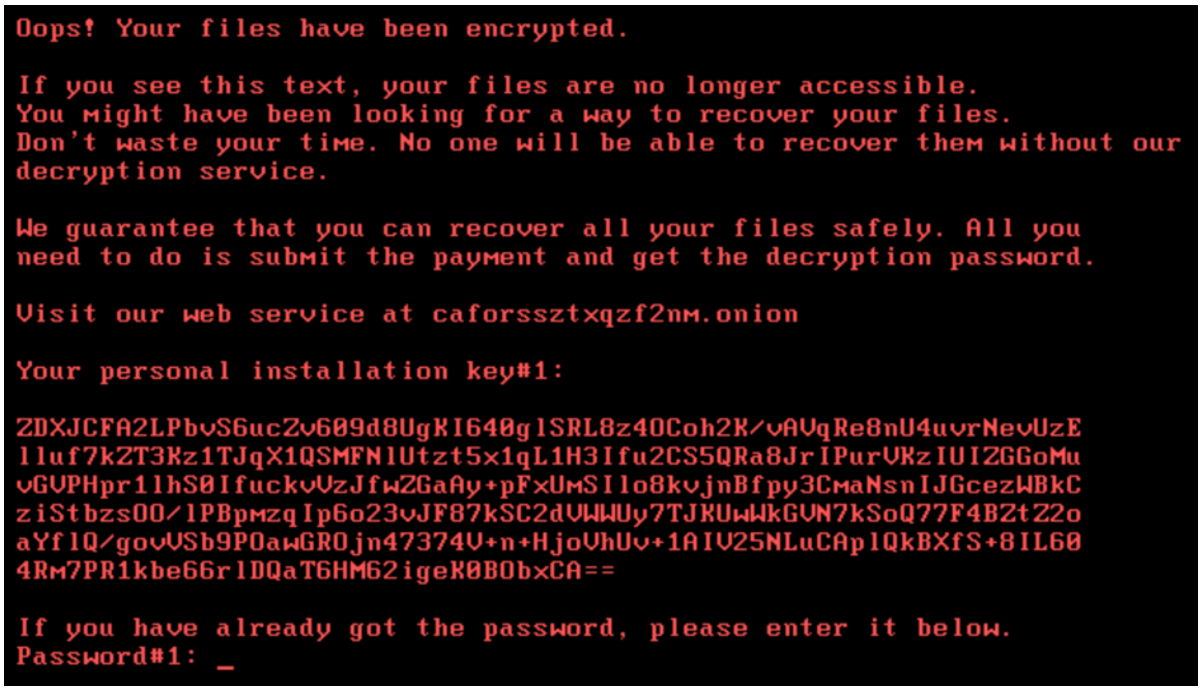
It also drops a malicious version of the DiskCryptor program (dispci.exe, we have seen SHA1: afeee8b4acff87bc469a6f0364a81ae5d60a2add) into ***%SystemRoot%***.

The infpub.dat file starts the encryption with the following commands by using cmd.exe:

- cmd.exe schtasks /Delete /F /TN rhaegal
- cmd.exe schtasks /Create /RU SYSTEM /SC ONSTART /TN rhaegal /TR "C:\Windows\system32\cmd.exe /C Start \"\" \"C:\Windows\dispci.exe\" -id 848053675 && exit"
- cmd.exe /c schtasks /Create /SC once /TN drogon /RU SYSTEM /TR "C:\Windows\system32\shutdown.exe /r /t 0 /f" /ST 17:14:00
- cmd.exe /c wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D C:

- cmd.exe /c schtasks /Delete /F /TN drogon

As part of the process, it creates a number of scheduled tasks to run the encryption program at every Windows start, reboots the computer, deletes or modifies the history of file changes, and then deletes the scheduled tasks.



Bad Rabbit Ransom Note

It is not definitively known if the files can be recovered after the ransom is paid, so the usual recommendations for defending against and remediating ransomware still apply.

d) File recovery possibility

Bad Rabbit does not delete shadow copies after encrypting the victim's files. It means that if the shadow copies had been enabled prior to infection and if the full disk encryption did not occur for some reason, then the victim can restore

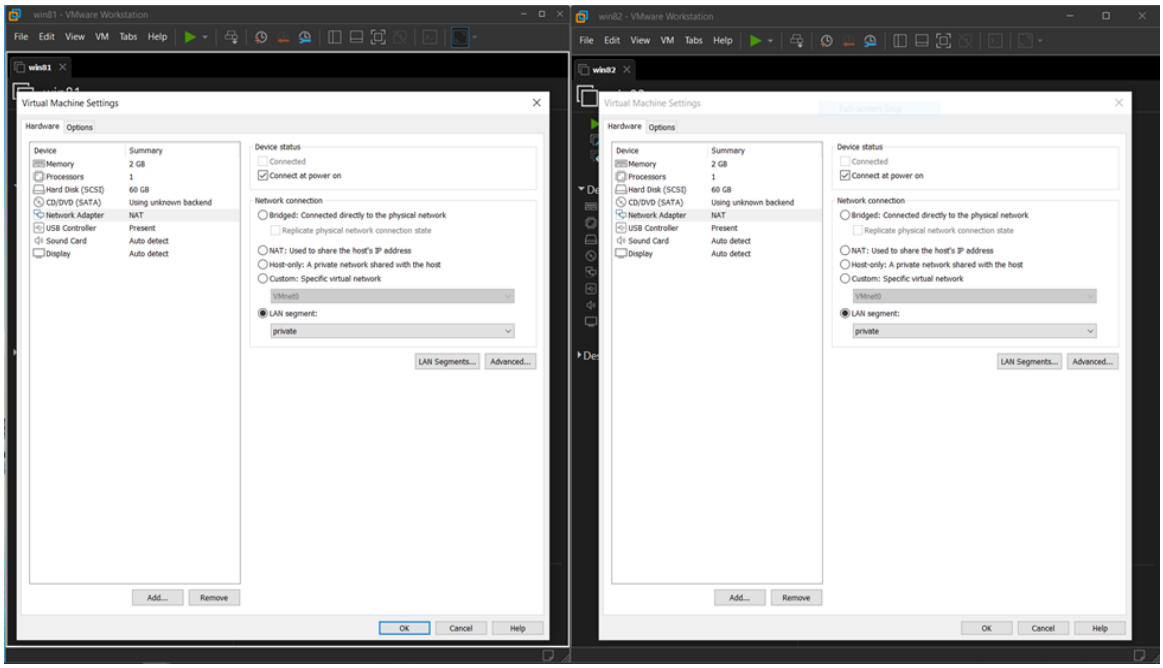
the original versions of the encrypted files by the means of the standard Windows mechanism or 3rd-party utilities.[3]

III. Implement on virtual machines

1. Implement

I will use VMWorkstation to study this ransomware. Ask I mentioned before, ransomware can spread via SMB protocol so in the implementation, I will try to demonstrate it.

I have 2 virtual machines named “Win81” and “Win82”. They are in the same LAN network named “Private”.

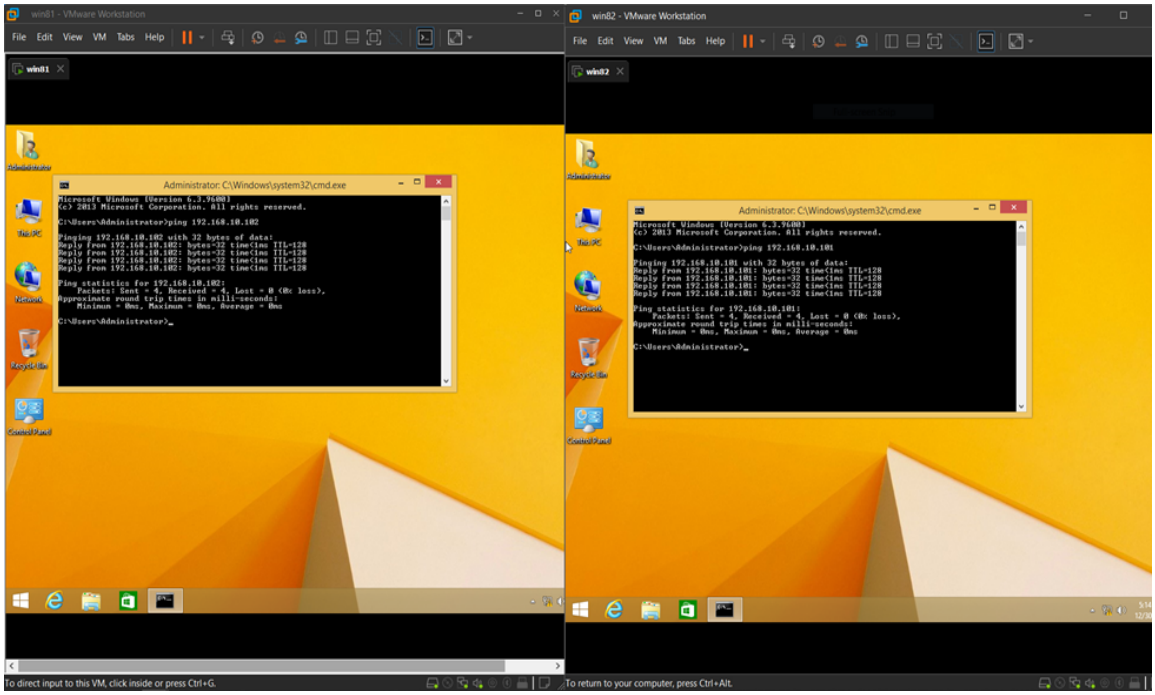


I set their IP addresses:

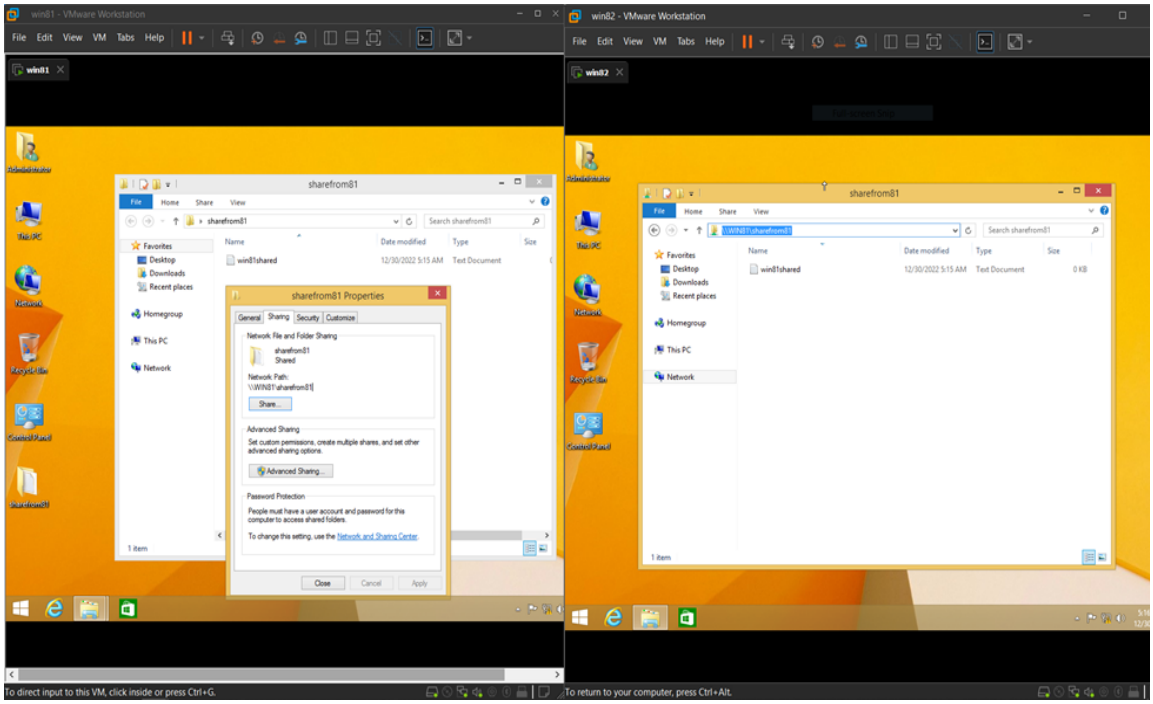
- Win81: 192.168.10.101. Subnet mark: 255.255.255.0

- Win82: 192.168.10.102. Subnet mark: 255.255.255.0

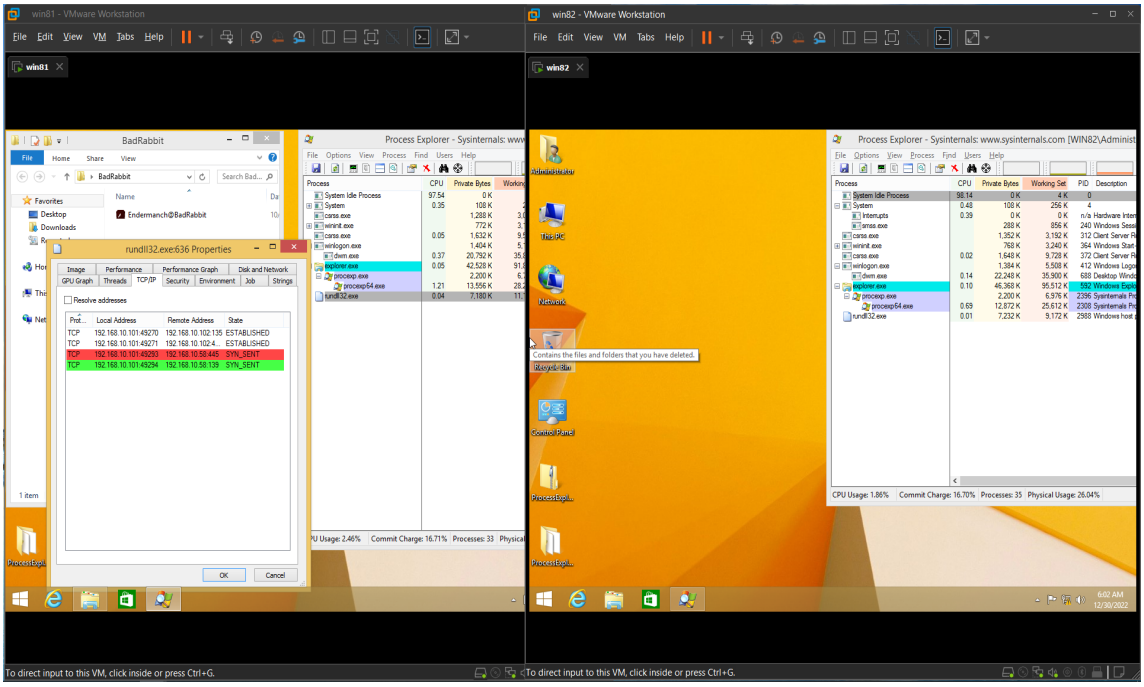
Then I try to ping each other. It works.



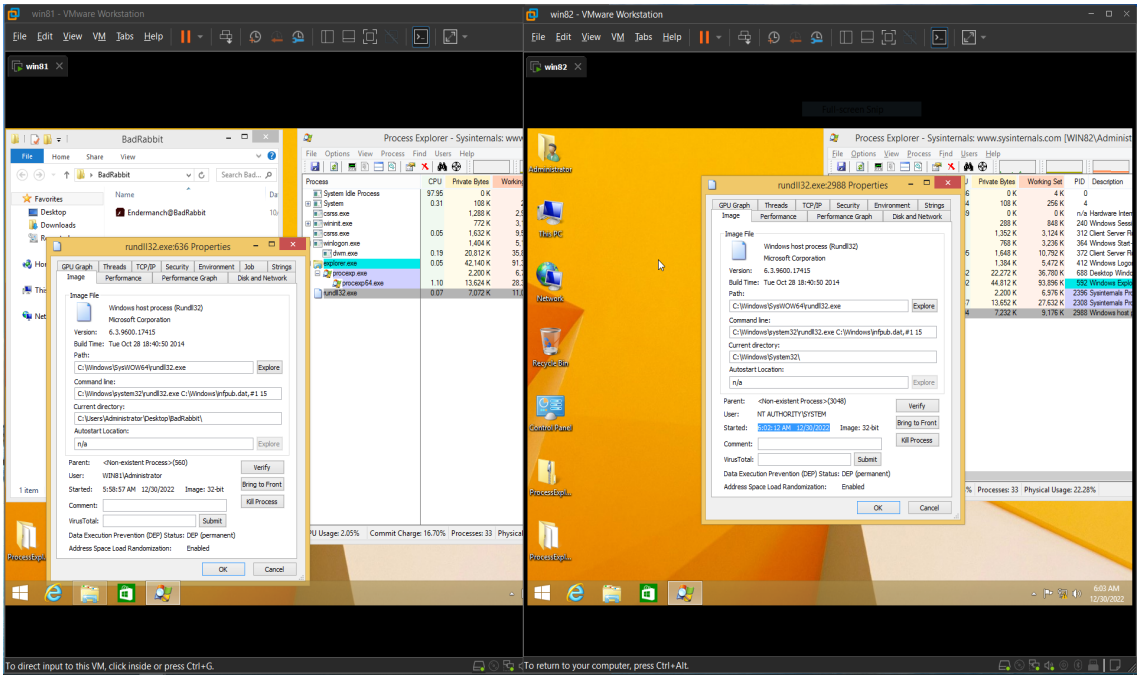
Configure the SMB file share protocol and check if it works.



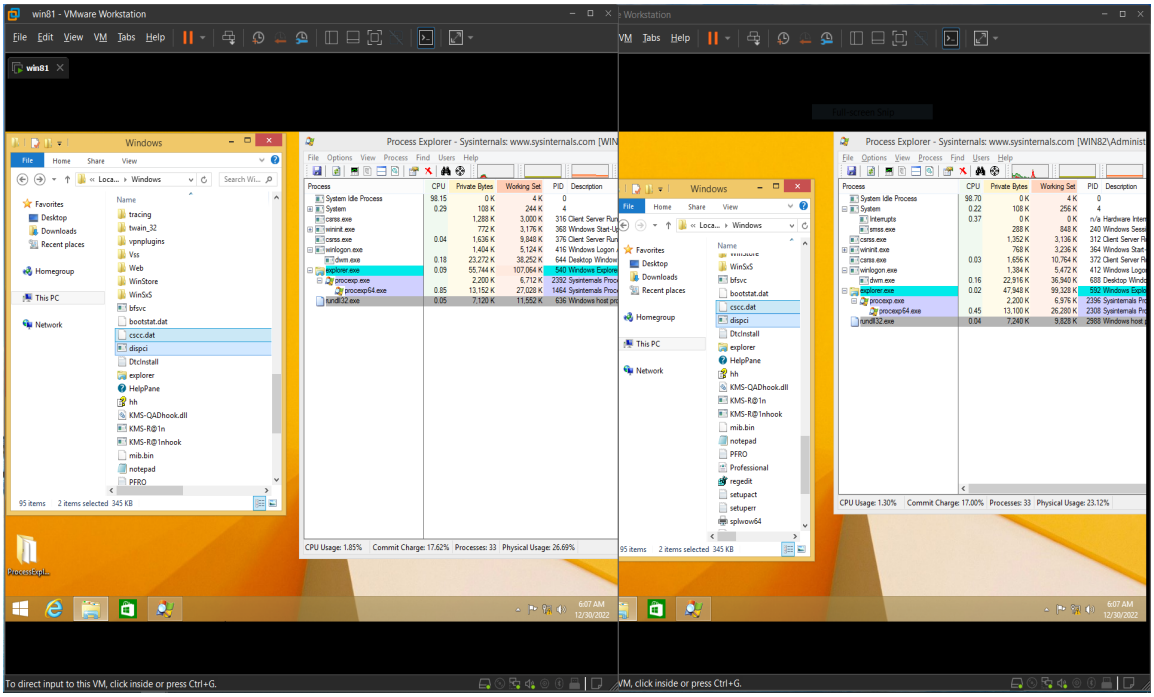
Now, I will use “Process Explorer” on both virtual machines to keep track of what happened. To prove that “BadRabbit” can spread via SMB protocol, I will just run the ransomware on “Win81” and wait for its spread on “Win82”. First, I turn off the Window Defender. Then, I run the ransomware which is in form of a fake Adobe Flash Player update file. A pop-up terminal appears and disappears immediately. Using Process Explorer to capture the processes in the Win81 machine, I saw the file rundll32.exe where the ransomware executes via.



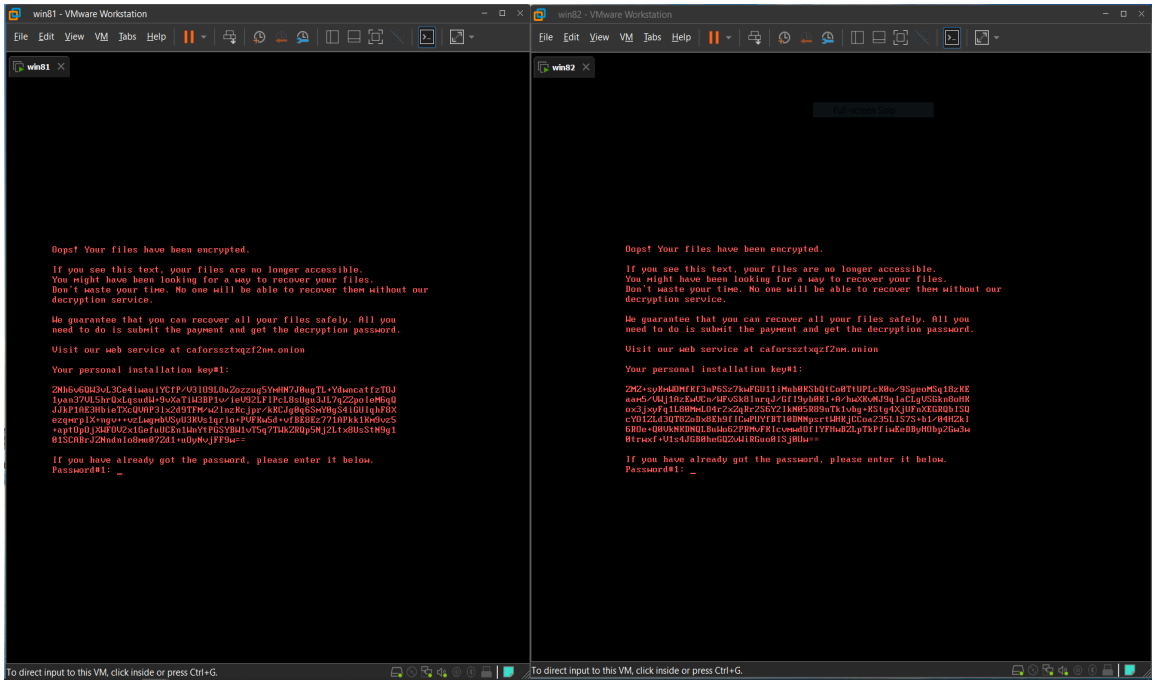
The following figure points out that the ransomware spread successfully from Win81 to Win82. Look at the details, it took about 5 minutes for this process to happen.



Now, check the path “C:\Window\” in both virtual machines, there are some BadRabbit’s signature files like “cscc.dat” or “dispci.exe”.



After about 15 minutes, the machines asked me for an error then they rebooted automatically and this was what I got.



IV. Prevention

- Watch out for malicious or compromised websites where your device can get infected with malware automatically or get tricked into downloading and installing malware.
- Use your firewalls as an intrusion detection and prevention systems.
- Keep track the traffic go in or out of the network.
- Back up your data regularly.
- Keep your systems updated and patched.
- Use Window Defender Antivirus which can detect and removes this threat with protection update 1.255.29.0 and higher.
- Disable SMB protocol

V. Conclusion

In this report, we have discussed the Bad Rabbit ransomware attack, the description, and the demo. Therefore, we also had some solutions to keep us stay safe. Nowadays, malware behavior become more and more sophisticated, the old case studies like Bad Rabbit will help us have a careful strategy to be better protected.

VI. Reference

[1] https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/protecting-yourself-from-bad-rabbit-ransomware

[2] https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Tibbar.A -

[3] https://securelist.com/bad-rabbit-ransomware/82851/

[4] https://www.youtube.com/watch?v=2WhI_bNNCIk&t=239s

[5] https://learn.microsoft.com/en-US/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server – disable SMB

[6] https://github.com/Endermanch/MalwareDatabase - malware database

[7] https://www.varonis.com/blog/bad-rabbit-ransomware