A. Introduction:

I chose “dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000” from dasmalwerk.eu.

Environment set up: Window10 X64 VM

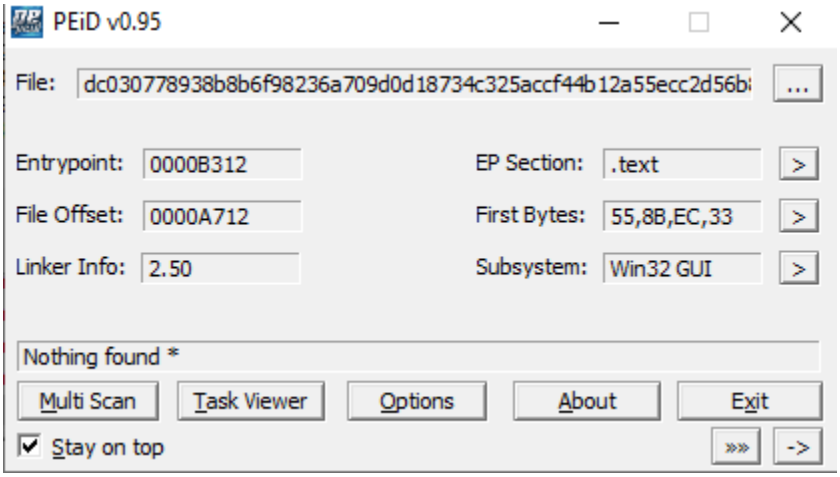
Tools: Wireshark, strings, dependency walker, ollydbg, ida,…

Procedure: I’d do Basic Static Analysis, then Advanced Static Analysis, Basic Dynamic Analysis then Advanced Dynamic Analysis.

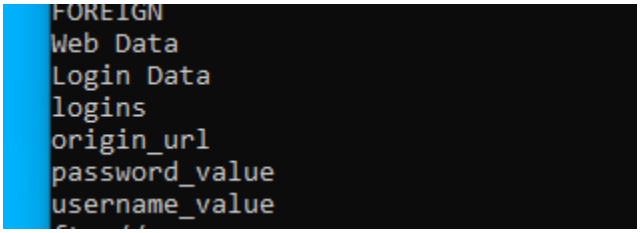
B. Analysis:

Basic Static Analysis:

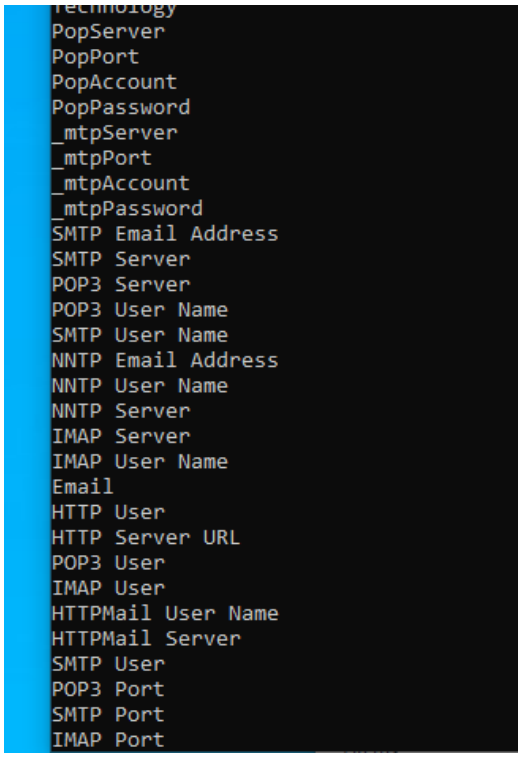
Checking Peid, we can see that it is not packed



Using strings on the exe, I found some interesting string



It also listing many popular internet browser like Chrome, Moz and Mail, outlook, thunderbird, even services like SMTP, NNTP, HTTP, POP3 with repeatedly include “password” and “username”



Checking dependency walker, we can find some net indicator imports.

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	121 (0x0079)	InternetCrackUrlA	Not Bound
C	N/A	123 (0x007B)	InternetCreateUrlA	Not Bound

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	33 (0x0021)	WSAStartup	Not Bound
C	N/A	38 (0x0026)	closesocket	Not Bound
C	N/A	39 (0x0027)	connect	Not Bound
C	N/A	42 (0x002A)	gethostbyname	Not Bound
C	N/A	54 (0x0036)	inet_addr	Not Bound
C	N/A	62 (0x003E)	recv	Not Bound
C	N/A	67 (0x0043)	select	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	37 (0x0025)	accept	ws2_32.accept
C	2 (0x0002)	38 (0x0026)	bind	ws2_32.bind
C	3 (0x0003)	39 (0x0027)	closesocket	ws2_32.closesocket
C	4 (0x0004)	40 (0x0028)	connect	ws2_32.connect
C	5 (0x0005)	46 (0x002E)	getpeername	ws2_32.getpeername
C	6 (0x0006)	51 (0x0033)	getsockname	ws2_32.getsockname
C	7 (0x0007)	52 (0x0034)	getsockopt	0x00001D80

```
4|rL:wrcrsn{1192
c\n4qiygu.http:/
/reninparwil.com
/zapoy/gate.php.
http://leftthenh
ispar.ru/zapoy/g
ate.php.http://r
eptertinrom.ru/z
apoy/gate.php..Y
UIPWDFILE0YUIPKD
FILE0YUICRYPTED0
YUI1.0.......MOD
U..........SOFTW
```

In peview, I found 3 urls in the .data section:

leftthenhispar.ru

reninparwill.com

reptertinrom.ru

I also found it might be changing and creating Registrykey

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	455 (0x01C7)	RegEnumValueA	Not Bound
C	N/A	462 (0x01CE)	RegOpenCurrentUser	Not Bound
C	N/A	463 (0x01CF)	RegOpenKeyA	Not Bound
C	N/A	464 (0x01D0)	RegOpenKeyExA	Not Bound
C	N/A	474 (0x01DA)	RegQueryValueExA	Not Bound
C	N/A	487 (0x01E7)	RegSetValueExA	Not Bound

From the basic analysis, I suspect this might taking password and username of the computer and send it to the connected url. It might be program to start at power on cause of the registry changing.

Advanced Static Analysis:

Open IDA, I can't seem to find the main function of the program. I found the string that we found from strings:

```
IA View-A
.data:10010490 ; char aLoginData[]
.data:10010490 aLoginData      db 'Login Data',0       ; DATA XREF: sub_100091D2+1B↑o
.data:10010490                                         ; sub_100091D2+45↑o ...
.data:1001049B ; char aLogins[]
.data:1001049B aLogins         db 'logins',0           ; DATA XREF: sub_1000902C+36↑o
.data:100104A2 ; char aOrigin_url[]
.data:100104A2 aOrigin_url     db 'origin_url',0       ; DATA XREF: sub_10008D9E:loc_10008E01↑o
.data:100104AD ; char aPassword_value[]
.data:100104AD aPassword_value db 'password_value',0   ; DATA XREF: sub_10008D9E:loc_10008E1B↑o
.data:100104BC ; char aUsername_value[]
.data:100104BC aUsername_value db 'username_value',0   ; DATA XREF: sub_10008D9E:loc_10008E35↑o
.data:100104CB ; char aFtp_1[]
```

And

```
01
01 loc_10008E01:                          ; CODE XREF: sub_10008D9E+5C↑j
01                  push    offset aOrigin_url ; "origin_url"
06                  push    [ebp+lpString]  ; lpString1
09                  call    lstrcmpiA
0E                  and     eax, eax
10                  jnz     short loc_10008E1B
12                  push    [ebp+arg_4]
15                  pop     dword_10012D3C
1B
1B loc_10008E1B:                          ; CODE XREF: sub_10008D9E+72↑j
1B                  push    offset aPassword_value ; "password_value"
20                  push    [ebp+lpString]  ; lpString1
23                  call    lstrcmpiA
28                  and     eax, eax
2A                  jnz     short loc_10008E35
2C                  push    [ebp+arg_4]
2F                  pop     dword_10012D40
35
35 loc_10008E35:                          ; CODE XREF: sub_10008D9E+8C↑j
35                  push    offset aUsername_value ; "username_value"
3A                  push    [ebp+lpString]  ; lpString1
3D                  call    lstrcmpiA
42                  and     eax, eax
44                  jnz     short loc_10008E4F
46                  push    [ebp+arg_4]
49                  pop     dword_10012D44
```

It seems like these are the steps to obtain username and password. I suspect the info is stored in ebp+arg_4.

BASIC DYNAMIC ANALYSIS:

Using Process Explorer I found a weird rundll32.exe

It also writes winrar in the registry HKEY_CURRENT_USER\Software\WinRAR with value: “7B32334637354239432D444131362D343638372D414544432D333833304335364230423845 7D” but I don’t think it is very relevant.

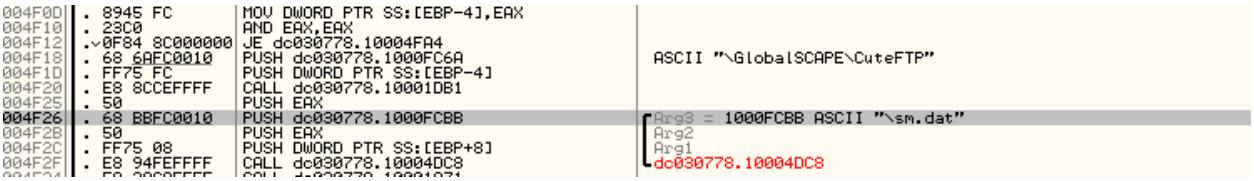
Later on when I search for the hash of the malware on virusTotal and Any.run, it seems that this is a typical Pony virus action.

Time	Domain Requested
12:18:45	reninparwill.com

I also spotted a dns request to reinparwill.com.

ADVANCED DYNAMIC ANALYSIS:

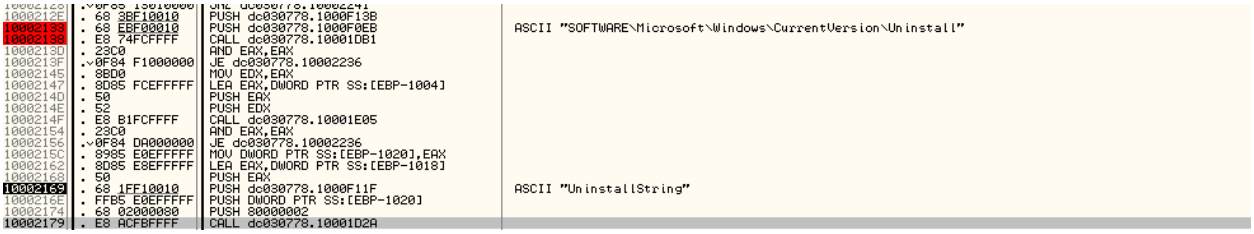
Since this is a suspected username and password stealing malware, I can’t really interact with them through the debugger, but I do find out a file that it might be interacting with

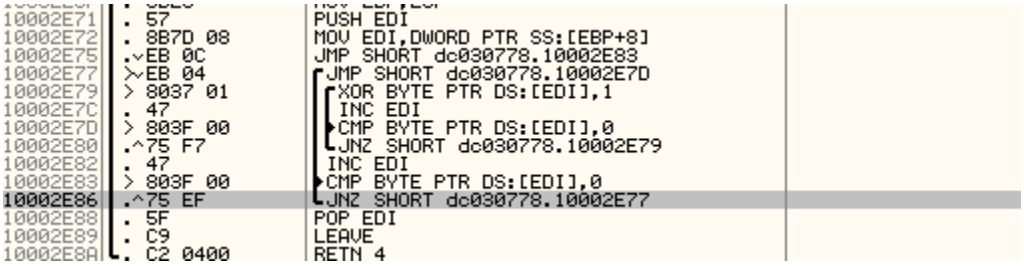


C:\ProgramData\GlobalSCAPE\CuteFTP\sm.dat

The program trying to gain privileged with push-ret

Another suspect is that it might be looking for passwords that is used by the user on the software of the machine by brute force.





C. Challenges:

This project is very challenging to me as the normal malware design is much harder to be analyzed. I can't find the main function and can't really interact with the dynamic tools much.

D. Summary:

To summarize my finding, I'd say that this malware is a information stealing malware, when infected, it will try to gain privileged and start stealing password information and send it to the hardcoded url. I'm not sure how it will send the data, one by one or in packet.

This malware is very dangerous as it targeted a big number of software and services like https, thunderbird, firefox, chromes and even facebook. The risk of information lost is very high, and it can even be used for illegal activity or identity theft.

A way to remove this malware is simply just to disable the suspected malware executable through task manager or Diskcleanup in Windows. You can use Safe Mode reboot to eliminate the malware also.