

A. Introduction:

I chose “dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000” from dasmalwerk.eu.

Environment set up: Window10 X64 VM

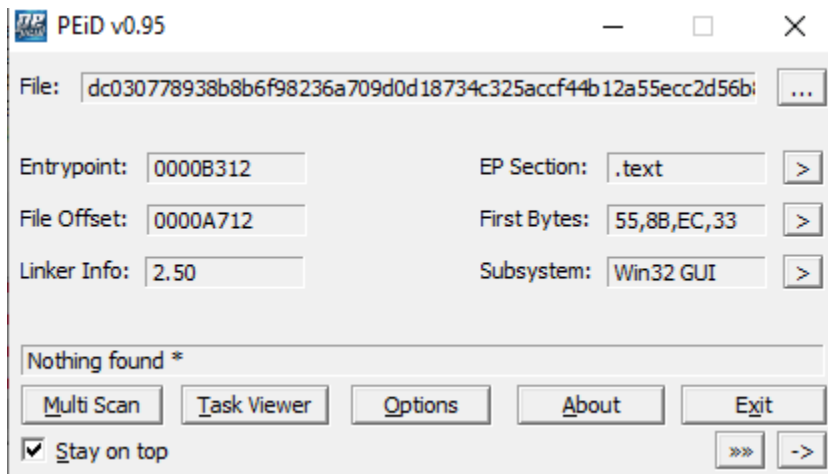
Tools: Wireshark, strings, dependency walker, ollydbg, ida,...

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

```
FOREIGN
Web Data
Login Data
logins
origin_url
password_value
username_value
```

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”

```

Technology
PopServer
PopPort
PopAccount
PopPassword
_mtpServer
_mtpPort
_mtpAccount
_mtpPassword
SMTP Email Address
SMTP Server
POP3 Server
POP3 User Name
SMTP User Name
NNTP Email Address
NNTP User Name
NNTP Server
IMAP Server
IMAP User Name
Email
HTTP User
HTTP Server URL
POP3 User
IMAP User
HTTPMail User Name
HTTPMail Server
SMTP User
POP3 Port
SMTP Port
IMAP Port

```

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

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

PI	Ordinal ^	Hint	Function	Entry Point
	N/A	33 (0x0021)	WSAStartup	Not Bound
	N/A	38 (0x0026)	closesocket	Not Bound
	N/A	39 (0x0027)	connect	Not Bound
	N/A	42 (0x002A)	gethostbyname	Not Bound
	N/A	54 (0x0036)	inet_addr	Not Bound
	N/A	62 (0x003E)	recv	Not Bound
	N/A	67 (0x0043)	select	Not Bound
E	Ordinal ^	Hint	Function	Entry Point
	1 (0x0001)	37 (0x0025)	accept	ws2_32.accept
	2 (0x0002)	38 (0x0026)	bind	ws2_32.bind
	3 (0x0003)	39 (0x0027)	closesocket	ws2_32.closesocket
	4 (0x0004)	40 (0x0028)	connect	ws2_32.connect
	5 (0x0005)	46 (0x002E)	getpeername	ws2_32.getpeername
	6 (0x0006)	51 (0x0033)	getsockname	ws2_32.getsockname
	7 (0x0007)	52 (0x0034)	netshknt	0x00001D80

```

4| rL:WrcfSn{1192
c\n4qiyygu.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.....SOF TW

```

In preview, 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
6	N/A	455 (0x01C7)	RegEnumValueA	Not Bound
6	N/A	462 (0x01CE)	RegOpenCurrentUser	Not Bound
6	N/A	463 (0x01CF)	RegOpenKeyA	Not Bound
6	N/A	464 (0x01D0)	RegOpenKeyExA	Not Bound
6	N/A	474 (0x01DA)	RegQueryValueExA	Not Bound
6	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:

```

IDA View-A
* .data:10010490 ; char aLoginData[]
* .data:10010490 aLoginData db 'Login Data',0 ; DATA XREF: sub_100091D2+1Bfo
* .data:10010490 ; sub_100091D2+45fo ...
* .data:1001049B ; char aLogins[]
* .data:1001049B aLogins db 'logins',0 ; DATA XREF: sub_1000902C+36fo
* .data:100104A2 ; char aOrigin_url[]
* .data:100104A2 aOrigin_url db 'origin_url',0 ; DATA XREF: sub_10008D9E:loc_10008E01fo
* .data:100104AD ; char aPassword_value[]
* .data:100104AD aPassword_value db 'password_value',0 ; DATA XREF: sub_10008D9E:loc_10008E1Bfo
* .data:100104BC ; char aUsername_value[]
* .data:100104BC aUsername_value db 'username_value',0 ; DATA XREF: sub_10008D9E:loc_10008E35fo
* .data:100104CB ; char aFtp_1[]

```

And

```

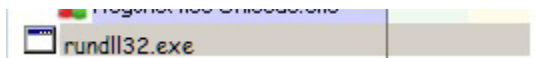
01
01 loc_10008E01:                ; CODE XREF: sub_10008D9E+5C↑j
01      push    offset a0origin_url ; "origin_url"
06      push    [ebp+lpString] ; lpString1
09      call    lstrcmpiA
0E      and     eax, eax
10      jnz     short loc_10008E1B
12      push    [ebp+arg_4]
15      pop     dword_10012D3C
18
18 loc_10008E1B:                ; CODE XREF: sub_10008D9E+72↑j
18      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: `"7B32334637354239432D444131362D343638372D414544432D3338333043353642304238457D"` 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	reinparwill.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

004F0D	. 8945 FC	MOV DWORD PTR SS:[EBP-4],EAX	
004F10	. 23C0	AND EAX,EAX	
004F12	✓ 0F84 8C000000	JE dc030778.10004FA4	
004F18	. 68 6AFC0010	PUSH dc030778.1000FC6A	ASCII "\GlobalSCAPE\CuteFTP"
004F1D	. FF75 FC	PUSH DWORD PTR SS:[EBP-4]	
004F20	. E8 8CCEFFFF	CALL dc030778.10001DB1	
004F25	. 50	PUSH EAX	
004F26	. 68 BBFC0010	PUSH dc030778.1000FCBB	Arg3 = 1000FCBB ASCII "\sm.dat"
004F2B	. 50	PUSH EAX	Arg2
004F2C	. FF75 08	PUSH DWORD PTR SS:[EBP+8]	Arg1
004F2F	. E8 94FEFFFF	CALL dc030778.10004DC8	dc030778.10004DC8
004F34	. F0 3000FFFF	CALL dc030778.10001074	

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

10002BB5	. 90	NOP	
10002BB6	. C3	RETN	RET used as a jump to 10002BB8
10002BB7	> FE	?	Unknown command
10002BB8	> BB 01000000	MOV EBX,1	
10002BBD	. BF E7F60010	MOV EDI,dc030778.1000F6E7	ASCII "SeImpersonatePrivilege"
10002BC2	> 6A 01	PUSH 1	Arg2 = 00000001
10002BC4	. 57	PUSH EDI	Arg1
10002BC5	. E9 77FDFFFF	CALL dc030778.10002941	dc030778.10002941
10002BCA	. 5308	AND EBX,EAX	
10002BCD	. EC	INC EAX	

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.

10002120	✓ 0F84 10010000	JE dc030778.10002274	
1000212E	. 68 3BF10010	PUSH dc030778.1000F13B	
10002133	. 68 EBF00010	PUSH dc030778.1000F0EB	
10002136	. 68 74FCFFFF	CALL dc030778.10001DB1	ASCII "SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall"
1000213D	. 23C0	AND EAX,EAX	
1000213F	✓ 0F84 F1000000	JE dc030778.10002236	
10002145	. 8B00	MOV EDI,EAX	
10002147	. 8085 FCEFFFFF	LEA EAX,DWORD PTR SS:[EBP-1004]	
1000214D	. 50	PUSH EAX	
1000214E	. 52	PUSH EDI	
1000214F	. 68 B1FCFFFF	CALL dc030778.10001E05	
10002154	. 23C0	AND EAX,EAX	
10002156	✓ 0F84 D0000000	JE dc030778.10002236	
1000215C	. 8985 E0FFFFFF	MOV DWORD PTR SS:[EBP-1020],EAX	
10002162	. 8085 E0FFFFFF	LEA EAX,DWORD PTR SS:[EBP-1018]	
10002168	. 50	PUSH EAX	
10002169	. 68 1FF10010	PUSH dc030778.1000F11F	ASCII "UninstallString"
1000216E	. FF85 E0FFFFFF	PUSH DWORD PTR SS:[EBP-1020]	
10002174	. 68 02000000	PUSH 00000002	
10002179	. E8 ACFBFFFF	CALL dc030778.10001D2A	

10002E71	. 57	PUSH EDI	
10002E72	. 8B7D 08	MOV EDI,DWORD PTR SS:[EBP+8]	
10002E75	✓ EB 0C	JMP SHORT dc030778.10002E83	
10002E77	> EB 04	JMP SHORT dc030778.10002E7D	
10002E79	> 8037 01	XOR BYTE PTR DS:[EDI],1	
10002E7C	. 47	INC EDI	
10002E7D	> 803F 00	CMP BYTE PTR DS:[EDI],0	
10002E80	. ^75 F7	JNZ SHORT dc030778.10002E79	
10002E82	. 47	INC EDI	
10002E83	> 803F 00	CMP BYTE PTR DS:[EDI],0	
10002E86	. ^75 EF	JNZ SHORT dc030778.10002E77	
10002E88	. 5F	POP EDI	
10002E89	. C9	LEAVE	
10002E8A	. C2 0400	RETN 4	

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.