BYTE Reserved {**#**ú{**#**Ò'**#**'....g&**#** a#Á{#{<{#ú{#ss. ..R)LÇ≌∭Ó∭uú[¹∭Ö '∎ûú[z:Úù∎²≣w<{∎ DWORD CmdSize ¹º#6##uú[¹.#..xF eÊ;∎∎Q.....å..'À 7∎∎«ÏX■....∎.. BBİBLEB....B..NE DWORD Key1 **■**H 'HQ**■....**5■ g∎0æ∎∎∎..........%? ő4öR∎∎3ó∎ÒsSÒs3Ò **■3....ôp!■!Q■■3**■ DWORD Key2 ÓÒ3**■**ÓÒ**■**ÓÒ3Ó.■..O ÝF`**■**V■■36ÓÒº■Ò33 ∎ò3óS.∎..i∎×t∎;∎ û∎Ò∎úú∎ÒÚ∎∎Òú[ù. BytesArray Cmd ■.. È-BÁ∎∎û3ÒÌúú **■**ÒÚ**■**■Òú[ù.■..û4+ ?¥#ûÚ:{#Ò'##'[# {º:Òyúº.■..Ì■\$Ô■ Õùu∎∎...¤..RSA1. ∎..∎.∎.∎`»6%0∎Íμ /Ïú∎.∎Ø≣\$p∎≣≡ ØÝ `∎jñ'¬∎é¥'©∎Þo]b Ìö;∎∎∎-.eîG®Ò∎"× ¤ë∎?Ig¢Rå∎S[1]!∎ ì∭óf'-9⊪°#J|SÍÛ5 }Ö∎¿∎∎Ôúj̆=.B∎s ∎FíĨö°ý'Õ∎ŒĈÖ¯(v "²«\_∎ÆÇ.≣..þ∎hê. ÿÙÃōyù:²Y:Úò{{Òy ù:.∎..AÔéÄçzÝ}Z< ù<∎ûz'ùY■{Yú■9■z yÒº¹.■..x■@/■yÝ} ú**m**>>{9**■■■**''Û**■**ÔY:■ Decrypted configuration file Configuration file is in format Struct( BYTE Reserved; DWORD Size; DWORD Key1; DWORD Key2; BYTEARRAY Data; **Command Searching** It uses special format for commands. Commands look like random data predefined Key1 and Key2 are used to search for commands in configuration file. if these keys are found it means commands are implemented that specific variant. Following function is used to search for commands: 55 **PUSH EBP** 8BEC MOV EBP, ESP 56 PUSH ESI JMP SHORT < 0089000.loc 406D2F> EB 13 CMP ECX, DWORD PTR SS:[EBP+8] 10c\_406D1C 3B4D 08 JNZ SHORT <\_0089000.1oc\_406D26> 75 05 3B55 0C CMP EDX, DWORD PTR SS:[EBP+C] JE SHORT < 0089000.loc 406D3D> 74 17 MOV ECX, DWORD PTR DS:[EAX] 8B 08 1oc\_406D26 SHR ECX,8 C1E9 08 8D4408 0C LEA EAX, DWORD PTR DS:[EAX+ECX+C] 8B48 04 MOV ECX, DWORD PTR DS:[EAX+4] 1oc\_406D2F MOV EDX, DWORD PTR DS:[EAX+8] 8B50 08 **8BF1 HOU ESI, ECX** ØBF2 OR ESI, EDX 75 E1 LJNZ SHORT <\_0089000.loc\_406D1C> 3300 XOR EAX,EAX POP ESI loc\_406D3D 5E POP EBP 5D Search in configuration file

Find Configuration loop

Value

ny"..%.)..y...y.

/J....\*.......

16...4.. "T....r

. p. . . . m8 . 8 . . u . .

. . . . B7 . 8 . . . T . t . .

..?n..u....L.

.wy\*....<.F..\_9n

..y\*..(.n.w.W8n

..y\*..l...5\*..6n

. . . } . . . < . } . . . . . .

.QXa......j...

.k..u...q\2b...

B. . 2 . 7 . u " . . | . . . n

] }.y[J...]N....9.

. uO. . . t [ v . . &. . . o

. . y . E. . . YH. . / . . .

Key1

(ey2

(ey1 Modified

Key2 Modified

ConfigSize

ConfigSize

ConfigData

ASCII

.∎..¶∎\$xö∎ºÀÖ:∎[ õU.∎..Ò∎èø∎"˺{<

it starts searching from start to end of file.

pFile

000000800

0000C820

0000C830

0000C840

0000C850

0000C870

0000C880 0000C890

0000C8A0

0000C8B0 0000000 0000C8D0 00000C8E0

00000C8F0

000000900 0000C910

0000C920

0000C960

0000C970

0000C980

0000C990 0000C9A0 0000C9BD 000000900 0000C9D0

0000C9E0

0000C9F0 0000CA00 0000CA10

0000CA60 0000CA70

Decryption

🜃 🎿 🔤

imul

add

xor

inc

dec

jnz

This file is decrypted using loop

encrypted configuration file is present in last section of file

Raw Data

11 36 F4 DC D2 34 C2 D2 - 22 54 D3 D5 D2 DC 80 72

03 34 02 B5 6A DD B9 CE - 59 4E AB 87 D5 C9 83 60 | .4...j....YN......`

00000C930 03 55 62 FC E3 D5 40 EE 57 4E F9 0E 51 23 E6 AF .Ub...@.WN..Q#..

C 48 2A 75 28 D3 98 76 - E5 D3 0A C8 20 A3 00 61 | <H\*u(..v.... ..a

9 CB 33 52 4A 60 62 DB 24 98 E3 11 01 9E ED 94 | i.3RJ`b.\$......

06 CE 79 DO 08 E6 53 E3 - A6 97 3C 5C E0 F7 03 DC ...y...S...<\....

Two DWORDs are read and modified then compared with next two DWORDs if match config file is

0000CA20 80 F4 A3 DC 62 F5 6B 97 A0 74 F9 E8 99 0E 78 EA ....b.k..t...x. 0000CA30 30 0A 9E 54 C4 F3 E3 D2 A0 72 60 55 E3 B7 C0 37 0..T....r `U...7 0000CA40 40 B5 20 D4 03 B7 23 94 20 90 43 17 99 1E 39 6E @. ...#. .C...9n 0000CA50 A1 CB 39 01 0A F7 64 93 A3 55 42 D5 A0 95 A2 74 ...9...d..UB....t

short Decrypt\_Config\_loc\_406B6D

Decrypt Configuration

found, next two DWORDs are size of config file.

Decrypt\_Config\_loc\_406B6D:

ebx, esi

[eax], bl

After decryption configuration file looks like:

Copy Data from ".rdata" section

83F8 FF CMP EAX,-1

75 7A

85C0

85C0

74 22

74 11

59

59

5F

5E

5B

C9

 $c_3$ 

74 F4

85C0

75 19 33C0

74 24

functions, this trick is used to thwart static analysis.

JNZ SHORT 003D1522 FF15 B43 CALL DWORD PTR DS:[3D30B4]

JE SHORT 003D14D6

JE SHORT 003D14D6

FF75 14 PUSH DWORD PTR SS:[EBP+14] FF75 10 PUSH DWORD PTR SS:[EBP+10]

JNZ SHORT 003D14EF

3975 08 CMP DWORD PTR SS:[EBP+8],ESI

3975 OC CMP DWORD PTR SS:[EBP+C],ESI=

8975 FC MOU DWORD PTR SS:[EBP-4],ESI

8D85 F4F LEA EAX, DWORD PTR SS:[EBP-10C]

FF15 A03 CALL DWORD PTR DS:[3D30A0]

FF15 A43 CALL DWORD PTR DS:[3D38A4]

8B3D DC4MOV EDI, DWORD PTR DS:[3D30DC]

8D85 F4F LEA EAX, DWORD PTR SS:[EBP-30C]

8D85 F4F LEA EAX, DWORD PTR SS:[EBP-30C]

8D85 F4F LEA EAX, DWORD PTR SS:[EBP-10C]

8D85 F4F LEA EAX, DWORD PTR SS:[EBP-20C]

8D85 F4F LEA EAX, DWORD PTR SS:[EBP-20C]

Service is created and if system is 64 bit "TESTSIGNING mode" is enables

FF15 D83 CALL DWORD PTR DS:[3D30D8]

FF15 283 CALL DWORD PTR DS:[3D3028]

JE SHORT 003D1141

PUSH EAX

PUSH ESI

PUSH ESI

POP ESI

XOR EDI,EDI

MOV EBX,EAX

CMP EBX,EDI

PUSH EDI PUSH 1F0FFF

TEST EAX,EAX

CALL <syshost.Process32NextW>

L<mark>JNZ SHORT (syshost.loc\_40798D)</mark>

E8 9DFEFFFF CALL <syshost.TriggerExceptions sub 407

PUSH DWORD PTR SS:[EBP+8]

FF15 B091400 CALL DWORD PTR DS:[<&KERNEL32.CloseHand] CloseHandle

FF15 B898488 CALL DWORD PTR DS:[<&KERNEL32.OpenProces LOpenProcess

Enumerate and Inject

50

56

85C0 75 D5

FF75 08

68 FF0F1F00

33FF

8BD8

3BDF

Regards,

Atinder

Analysis Necurs Threats

57

E8 36000000

8B35 2C4MOV ESI,DWORD PTR DS:[3D302C

JE SHORT 003D14D6

JE SHORT 003D14D6 FF75 OC PUSH DWORD PTR SS:[EBP+C] FF75 08 PUSH DWORD PTR SS:[EBP+8]

EB DC JMP SHORT 003D14CB

PHSH EST

PUSH ESI

PUSH EAX

PUSH EDI

PUSH EAX

PUSH EAX

CALL EDI

PUSH EAX

PUSH EAX

PUSH EAX

CALL EDI

PUSH EAX

MOV EDI,EAX

PUSH EAX

PUSH EBX

**PUSH EBX** 

MOV EDI,EAX

CMP EDI,EBX

0F84 44( JE 003D1177

68 64313 PUSH 3D3164

68 50313 PUSH 3D3150

68 4C313 PUSH 3D314C

83C4 24 ADD ESP.24

57

50

50

50

FFD7

3BFB

53

57

74 13 53

FFD7

TEST EAX,EAX

JE SHORT <key1\_32bit>

3975 10 CMP DWORD PTR SS:[EBP+10],ESI

3975 14 CMP DWORD PTR SS:[EBP+14],ESI = 74 11 JE SHORT 003D14D6

TEST EAX,EAX

TEST EAX,EAX

E8 7203(CALL <is 64bit>

→E8 30FBF<mark>CALL <DropDriver></mark>

POP ECX

POP ECX

POP EDI

POP ESI

POP EBX

LEAVE

RETN

TEST EAX,EAX

XOR EAX,EAX

**Driver Dropping and TESTSINGING mode** 

If command is build it can Drop 32 or 64 bit driver using following code:

eax

ecx

Structure of Config file

ebx, 19661Fh

Driver name is generated randomly 895D FC MOV DWORD PTR SS:[EBP-4],EBX E8 2E09(CALL <EnableWow64FsRedir> 8945 F8 MOV DWORD PTR SS:[EBP-8],EAX BE 0001(MOV ESI,100

Drop Driver

It copies code from ".rdata " section in newly allocated memory and uses that for some important

SHELL32.IsUserAnAdmin

Offset and Size for

Offset and Size for

kernel32.GetSystemDirectoryA

kernel32.GetTickCount

ASCII "%s\drivers\%s.sys"

msvcrt.sprintf

ASCII "%x"

sprintf

sprintf

ADVAPI32.CreateServiceA

ADVAPI32.CloseServiceHandle

ASCII "wb"

msvcrt.fopen

JMP to kernel32.Process32NextW

rh0bject

Inheritable => FALSE

Access = PROCESS\_ALL\_ACCESS

ProcessId

32bit driver

64bit driver

PUSH EDI FF15 303 CALL DWORD PTR DS:[3D3030] ADVAPI32.StartServiceA 57 PUSH EDI CALL ESI FFD6 C745 FC MOV DWORD PTR SS:[EBP-4],1 FF75 F4 PUSH DWORD PTR SS:[EBP-C] CALL ESI FFD6 395D FC CMP DWORD PTR SS:[EBP-4], EBX 74 1D JE SHORT 003D1168 E8 D906(CALL <is\_64bit> TEST EAX, EAX 85C0 74 22 JE SHORT 003D1176 6A 0A PUSH 0A 5E POP ESI **PUSH** EBX 53 ASCII "bcdedit.exe -set TESTSIGNING ON" 68 2C313 PUSH 3D312C FF15 8C3 CALL DWORD PTR DS:[3D308C] kernel32.WinExec 4E DEC ESI 75 F1 JNZ SHORT 003D1157 JMP SHORT 003D1176 EB ØE 8D85 F4F LEA EAX, DWORD PTR SS:[EBP-20 PUSH EAX FF15 CC3 CALL DWORD PTR DS:[3D30CC] msvcrt.\_unlink POP ECX POP EDI 5F FF75 F8 PUSH DWORD PTR SS:[EBP-8] E8 0008(CALL <DisableWow64FsRedir> ODIC CO MOII CAY NUMBER DID CC-FCDD\_HI Enable TESTSIGNING mode **DeadByte Injection** May inject DeadBytes Into running processes. These bytes generate exceptions and can crash the process, if some critical process crashes system will restart and Driver agent will be activated. LA2H FHV C785 D4FDFFF MOV DWORD PTR SS:[EBP-22C],22C E8 23060000 CALL <syshost.memset> Lmemset 83C4 OC ADD ESP, GC PUSH 0 6A 00 rProcessID = 0 PUSH 2

CALL <syshost.CreateToolhelp32Snapshot>
Flags - TH32CS\_SNAPPROCESS
CreateToolhelp32Snapshot 6A 02 E8 7F000000 MOV ESI, EAX 8BF 0 CMP ESI,-1 83FE FF 74 41 JE SHORT <syshost.loc\_4079BF>
8D85 D4FDFFFI LEA EAX, DWORD PTR SS:[EBP-22C] .. 74 41 LO2H FHY 56 PUSH ESI JMP to kernel32.Process32FirstW E8 65000000 CALL <syshost.Process32FirstW> EB 27 JMP SHORT <syshost.loc\_407984> FF15 F490400 CALL DWORD PTR DS:[<&KERNEL32.GetCurre| CGetCurrentProcessId 3985 DCFDFFFI CMP DWORD PTR SS:[EBP-224],EAX
74 0C JE SHORT <syshost.loc\_4079A7> FFB5 DCFDFFF[ PUSH DWORD PTR SS:[EBP-224] CALL (syshost.Inject\_sub\_4078C6) E8 20FFFFFF 59 POP ECX 8D85 D4FDFFF[ LEA EAX, DWORD PTR SS:[EBP-22C]

Random Driver Name

., 74 54 JE SHORT <syshost.loc\_407940> PUSH ESI 56 6A 04 PUSH 4 68 00300000 PUSH 3000 BE 80000000 MOU ESI,80 PUSH ESI 56 57 PUSH EDI 53 PUSH EBX FF15 7491488 CALL DWORD PTR DS:[<&KERNEL32.VirtualAl] kernel32.VirtualAllocEx rpBytesWritten 57 PUSH EDI 56 PUSH ESI BytesToWrite 68 56764000 PUSH <syshost.Exception3\_loc\_407656> Buffer = <syshost.Exception3\_loc\_4076562 **PUSH EAX** 50 Address 53 PUSH EBX hProcess MOU DWORD PTR SS:[EBP-4],EAX 8945 FC FF15 7C91400 CALL DWORD PTR DS:[<GKERNEL32.WriteProc( WriteProcessHemory 68 C8000000 PUSH 0C8 PUSH 64 6A 64 68 DOCC4000 PUSH syshost.0040CCD0 . E8 8FCDFFFF CALL (sushost\_GenRndm sub 4046AF) CALL (syshost.\_\_SEH\_prolog)
AND DWORD PTR SS:[EBP-1C],0 E8 A6090000 8365 E4 00 8365 FC 00 AND DWORD PTR SS:[EBP-4],0 PUSH EBX 3300 XOR EAX, EAX 33DB XOR EBX, EBX 3365 XOR ECX, ECX 33D2 XOR EDX, EDX DB 0F Exception **C7** DB C7 C8 01005B ENTER 1,58 = C745 E4 0100 MOV DWORD PTR SS:[EBP-1C],1 JMP SHORT syshost.0040768D EB 0B 3300 XOR EAX, EAX INC EAX Inject Exception generating code Domain names and IP addresses Then it will search and decrypt Domain names and IP's from configuration file and communicate with them. In this file decrypted domain names are: "jygydwkegbdsbohalkc.me" "opusattheend.bit" and IP addresses are: "178.32.31.41" "106.187.47.17" "176.58.118.172" **Error Reporting function** Also Contains an Troubleshooting and error reporting module which send error report to specified remote address. If it is unable to perform some operation like unable to create thread then Error

Uncategorized. Follow any responses to this post through RSS 2.0. You can leave a response or trackback from your own site. 4 comments Reegun (2 MONTHS) Nice analysis

Thanks 😃

sheik (2 MONTHS)

nice post atinder!

Comment

cite=""> <strike> <strong>

Post Comment

reporting function is called. This function collects System info and error code then encodes information

Main Thread call one function after doing all activity and also created some Threads. I am working on

This entry was posted by Atinderpal Singh on August 2, 2013 at 1:05 pm, and is filed under Analysis, MDT, Threats,

analysis of those threads and that function Analysis of those will be covered in future blog posts.

and selects random domain from decrypted domains array, decrypt rest of URL path from config,append to URL and send information. In this case decrypted path: "/cgi-bin/ss.cgi"

Here is the link to Control Flow Graph of Necurs with functionality i have covered so far.

thanks seikh 😃 Leave a Reply Your email address will not be published. Required fields are marked \* Name \* Email \* Website

You may use these HTML tags and attributes: <a href="" title=""> <abbr title=""> <acronym

title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q

19 queries in 0.24 seconds (22.98M)