Malware Analysis Report

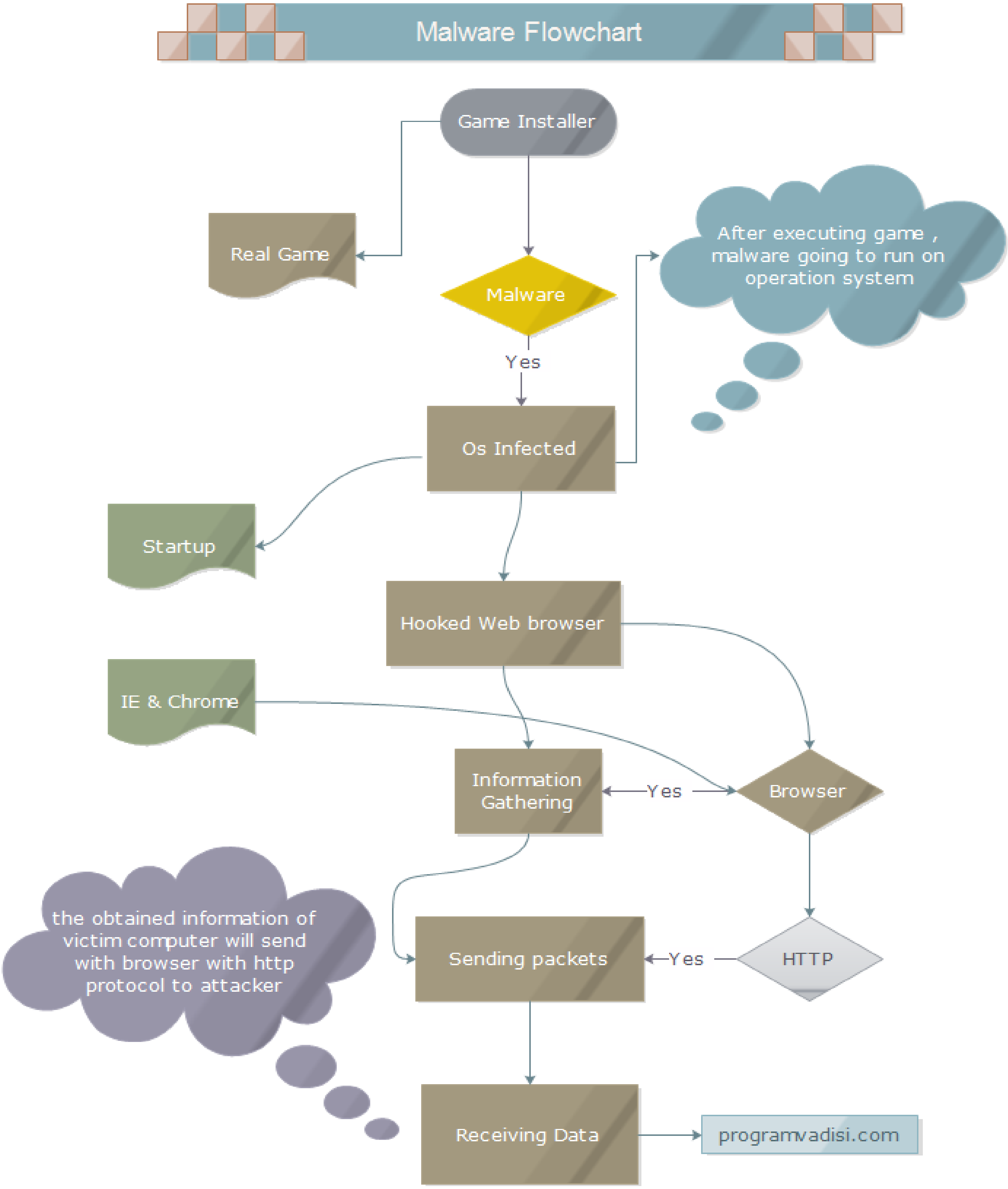
THREAT REPORT: SYS32.EXE TROJAN.GENERIC (TURKISH)

Dariush Nasirpour (Net.Editor)

Home Page: Black-hg.org Or Nasirpour.info

Contact: Dariush.Nasirpour@Gmail.com , Me@Nasirpour.info

Contents


Malware Flowchart
Game Installer
Real Game
Malware
Yes
After executing game , malware going to run on operation system
Os Infected
Startup
Hooked Web browser
IE & Chrome
Information Gathering
Yes
Browser
the obtained information of victim computer will send with browser with http protocol to attacker
Sending packets
Yes
HTTP
Receiving Data
programvadisi.com

Summery

At end of the 2014 one of my colleagues downloaded a Super Mario game from Internet. After a while he suspected the game and told me to analyses that. At first stage of the analysis of that game I discovered the Sys32.exe and in 2 working days the analyzing progress finished.

The sys32.exe was bounded with Super Mario game and distributed to the Internet.

(Sorry for my bad English, I speak with different language)

Stage 1: Analysis Summary:

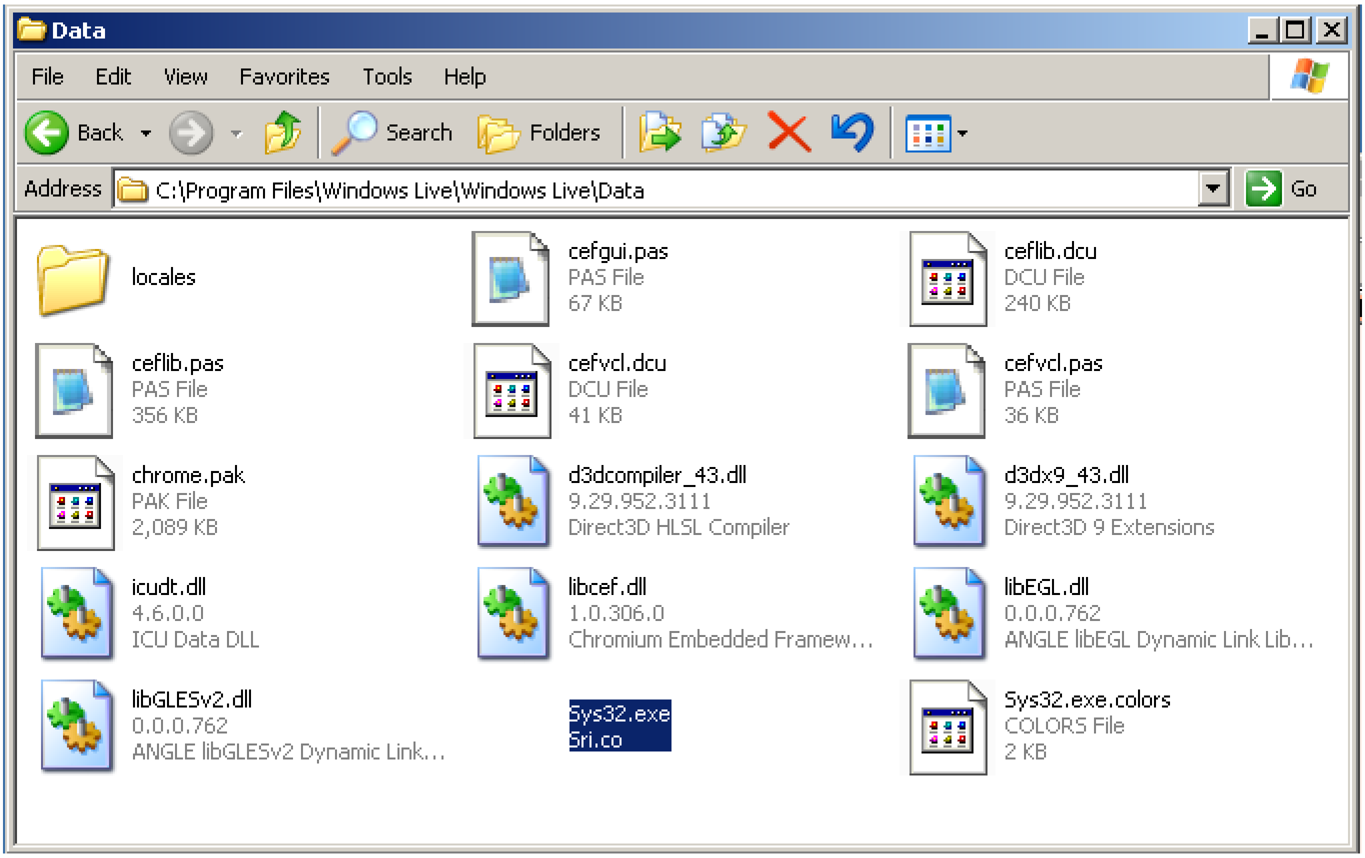
Note: Our analysis was completed using a 32-bit Windows XP Service Pack 3 Virtual Machine.

The attachments received by our client were as shown below:

Name :	Trojan.Generic (Turkish)
MD5 :	bd6af7a726c4a3e6ba1ed9b900e6c9d6
SHA256 :	caae4bb36de9b645567453fbde1d83c18d03ebc969d96cdb1927ee5eb0404e6f
Publisher :	Sri.co
File size :	580.5 KB (594432 bytes)
PEiD :	BobSoft Mini Delphi -> BoB / BobSoft

2.1 Stage 1: Analysis of the attachments

All three files were self-extracting executable, which when double-clicked revealed a set of files as shown below:


Data
File Edit View Favorites Tools Help
Back
Search
Folders
Address
C:\Program Files\Windows Live\Windows Live\Data
Go

locales

cefgui.pas
PAS File
67 KB

ceflib.dcu
DCU File
240 KB

ceflib.pas
PAS File
356 KB

cefvcl.dcu
DCU File
41 KB

cefvcl.pas
PAS File
36 KB

chrome.pak
PAK File
2,089 KB

d3dcompiler_43.dll
9.29.952.3111
Direct3D HLSL Compiler

d3dx9_43.dll
9.29.952.3111
Direct3D 9 Extensions

icudt.dll
4.6.0.0
ICU Data DLL

libcef.dll
1.0.306.0
Chromium Embedded Framew...

libEGL.dll
0.0.0.762
ANGLE libEGL Dynamic Link Lib...

libGLESv2.dll
0.0.0.762
ANGLE libGLESv2 Dynamic Link...

Sys32.exe
Sri.co

Sys32.exe.colors
COLORS File
2 KB

FIGURE 1: EXTRACTED FORM OF SUSPECTED FILE

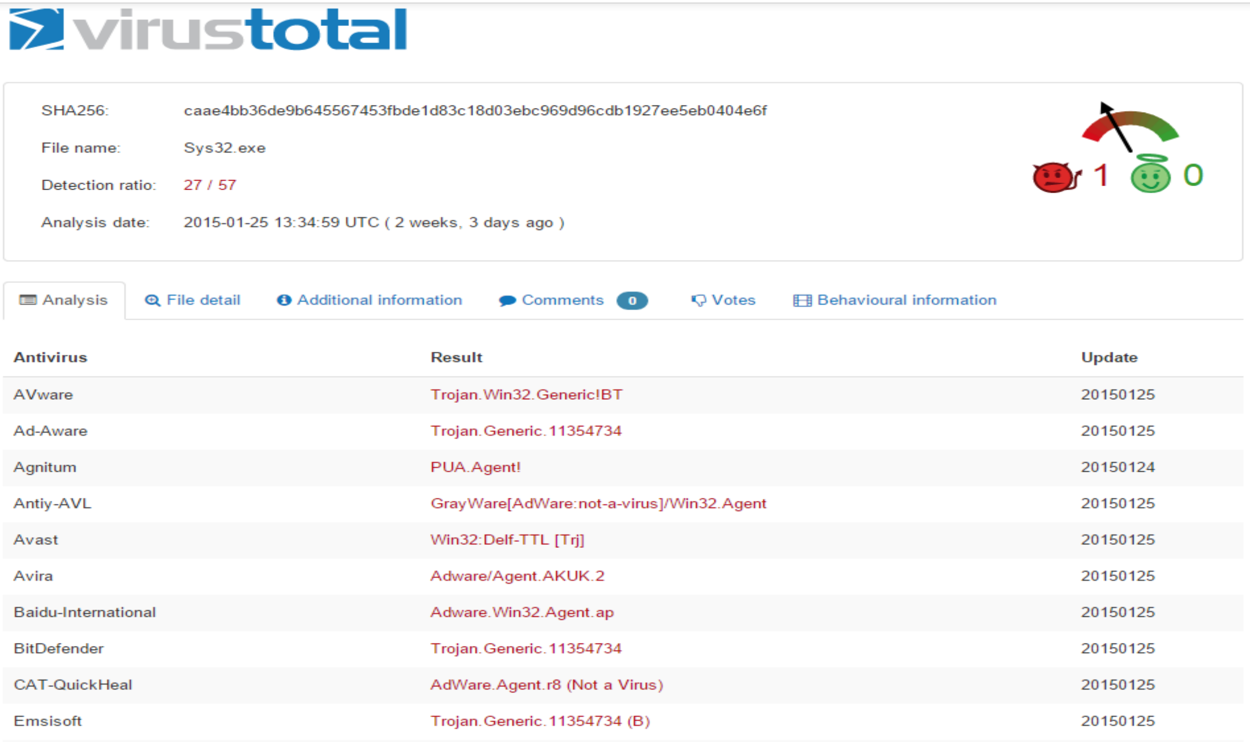
- ✓ These files are extracted to a folder “C:\Program Files\Windows Live\Windows Live\Data “by default.

When Sys32.exe process starts it creates 30 files and put them into your system that you can see them below.

```
+----+-------------------+-------------------------+----------------------------------+------+
| #  | Name              | Mime                    | MD5                              | Tags |
+----+-------------------+-------------------------+----------------------------------+------+
| 1  | Sys32.exe         | application/x-dosexec   | bd6af7a726c4a3e6ba1ed9b900e6c9d6 |      |
| 2  | avformat-53.dll   | application/x-dosexec   | d1b495032f5760edb341c43d4732fd19 |      |
| 3  | avcodec-53.dll    | application/x-dosexec   | ac5db309b4390402044066f4d3e8b787 |      |
| 4  | cefgui.pas        | text/plain              | 7f956844c85320f2f4d610a5724f420e |      |
| 5  | ceflib.pas        | text/plain              | 5538dec4cca812de6d2c91a89ee35777 |      |
| 6  | ceflib.dcu        | application/octet-stream| 13e6f5c7e0cfc0fc8d2188a44e821d3e |      |
| 7  | cefgui.dcu        | application/octet-stream| fd569b54ce7079d9fef97c90c9a9b382 |      |
| 8  | avutil-51.dll     | application/x-dosexec   | b70b9c4e47ff1f0e1f95fbdfd8b74a8a |      |
| 9  | chrome.pak        | application/octet-stream| 3fb67d97df5e94f01b779b0c61dfc021 |      |
| 10 | libEGL.dll        | application/x-dosexec   | 404b6b560e235ba28287eee79b60d1af |      |
| 11 | d3dcompiler_43.dll| application/x-dosexec   | 1c9b45e87528b8bb8cfa884ea0099a85 |      |
| 12 | libGLESv2.dll     | application/x-dosexec   | 8d2434e951d6aeee9309b59f5d130d20 |      |
| 13 | cefvcl.pas        | text/plain              | b016e5d4bb657c45ad64448401618ce8 |      |
| 14 | icudt.dll         | application/x-dosexec   | 360b5e2c91140cca141b5cf51969f5b0 |      |
| 15 | cefvcl.dcu        | application/octet-stream| 4210c49b4121147bf39b58719cf32829 |      |
| 16 | ceffmx.pas        | text/plain              | 1b693eb85ff41a26901d9c8e253fe12e |      |
| 17 | cef.inc           | text/plain              | 41dc7a1e1165af61f98300fec7dbdd65 |      |
| 18 | libcef.dll        | application/x-dosexec   | 937afaba204777af6fb691a1b4dc86fa |      |
| 19 | d3dx9_43.dll      | application/x-dosexec   | 86e39e9161c3d930d93822f1563c280d |      |
| 20 | fr.pak            | application/octet-stream| c16e944c85241b128f1201125f327509 |      |
| 30 | en-GB.pak         | application/octet-stream| 6fb0a8b58f431f746d48e8c7ddf2ec23 |      |
+----+-------------------+-------------------------+----------------------------------+------+
```

2.2 Stage 2: Virus total Analysis

Submitting the malware to VirusTotal's scanner resulted in a detection ratio of 27/57. We did a very rudimentary check of "Sys32.exe" on virustotal.org and it was found to be a Trojan with keylogging capability



SHA256: caae4bb36de9b645567453fbde1d83c18d03ebc969d96cdb1927ee5eb0404e6f

File name: Sys32.exe

Detection ratio: 27 / 57

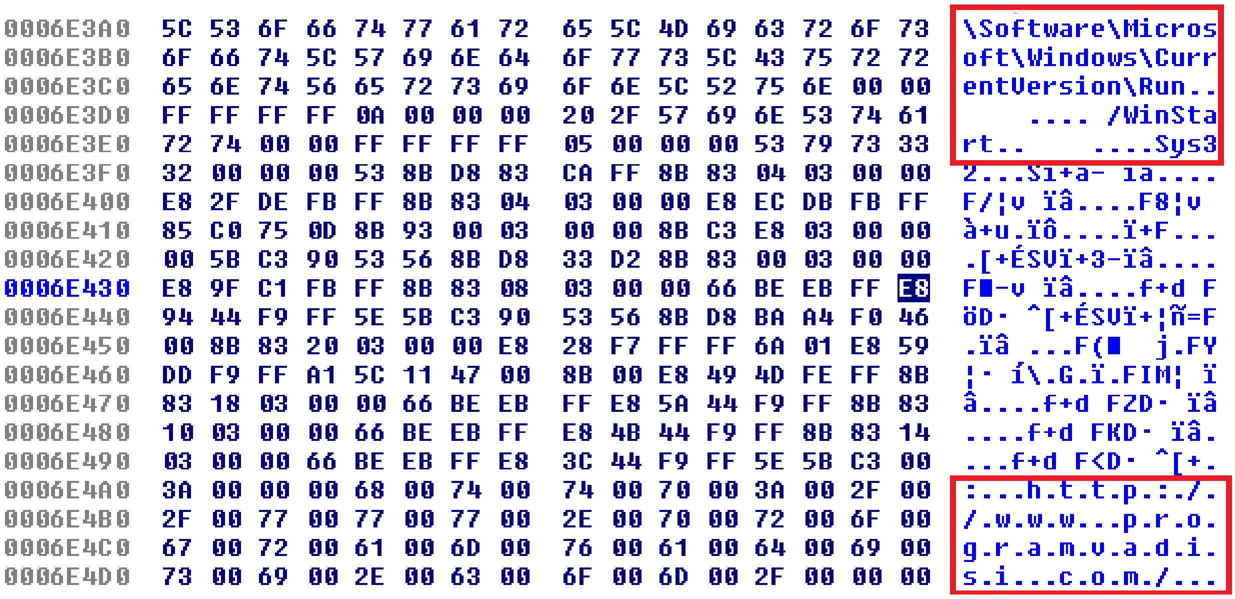
Analysis date: 2015-01-25 13:34:59 UTC (2 weeks, 3 days ago)

Antivirus	Result	Update
AVware	Trojan.Win32.Generic!BT	20150125
Ad-Aware	Trojan.Generic.11354734	20150125
Agnitum	PUA.Agent!	20150124
Antiy-AVL	GrayWare[AdWare:not-a-virus]/Win32.Agent	20150125
Avast	Win32:Delf-TTL [Trj]	20150125
Avira	Adware/Agent.AKUK.2	20150125
Baidu-International	Adware.Win32.Agent.ap	20150125
BitDefender	Trojan.Generic.11354734	20150125
CAT-QuickHeal	AdWare.Agent.r8 (Not a Virus)	20150125
Emsisoft	Trojan.Generic.11354734 (B)	20150125

FIGURE 2: VIRUSTOTAL ONLINE RESULT

Of bits and bytes

We can see in the screenshot that I have opened up the malware file in my hex editor and in the characters “5C 53 & 3A00” I found “Registry Address & URL” that the malware is using for sending information and the startup process.



```
0006E3A0  5C 53 6F 66 74 77 61 72  65 5C 4D 69 63 72 6F 73  \Software\Micros
0006E3B0  6F 66 74 5C 57 69 6E 64  6F 77 73 5C 43 75 72 72  oft\Windows\Curr
0006E3C0  65 6E 74 56 65 72 73 69  6F 6E 5C 52 75 6E 00 00  entVersion\Run..
0006E3D0  FF FF FF FF 0A 00 00 00  20 2F 57 69 6E 53 74 61      .... /WinSta
0006E3E0  72 74 00 00 FF FF FF FF  05 00 00 00 53 79 73 33  rt..    ....Sys3
0006E3F0  32 00 00 00 53 8B D8 83  CA FF 8B 83 04 03 00 00  2...Sï+a- ïâ....
0006E400  E8 2F DE FB FF 8B 83 04  03 00 00 E8 EC DB FB FF  F/¦v ïâ....F8¦v
0006E410  85 C0 75 0D 8B 93 00 03  00 00 8B C3 E8 03 00 00  à+u.ïô....ï+F...
0006E420  00 5B C3 90 53 56 8B D8  33 D2 8B 83 00 03 00 00  .[+ÉSVï+3-ïâ....
0006E430  E8 9F C1 FB FF 8B 83 08  03 00 00 66 BE EB FF E8  F█-v ïâ....f+d F
0006E440  94 44 F9 FF 5E 5B C3 90  53 56 8B D8 BA A4 F0 46  öD· ^[+ÉSVï+¦ñ=F
0006E450  00 8B 83 20 03 00 00 E8  28 F7 FF FF 6A 01 E8 59  .ïâ ...F(█  j.FY
0006E460  DD F9 FF A1 5C 11 47 00  8B 00 E8 49 4D FE FF 8B  ¦· í\.G.ï.FIM¦ ï
0006E470  83 18 03 00 00 66 BE EB  FF E8 5A 44 F9 FF 8B 83  â....f+d FZD· ïâ
0006E480  10 03 00 00 66 BE EB FF  E8 4B 44 F9 FF 8B 83 14  ....f+d FKD· ïâ.
0006E490  03 00 00 66 BE EB FF E8  3C 44 F9 FF 5E 5B C3 00  ...f+d F<D· ^[+.
0006E4A0  3A 00 00 00 68 00 74 00  74 00 70 00 3A 00 2F 00  :...h.t.t.p.:./.
0006E4B0  2F 00 77 00 77 00 77 00  2E 00 70 00 72 00 6F 00  /.w.w.w...p.r.o.
0006E4C0  67 00 72 00 61 00 6D 00  76 00 61 00 64 00 69 00  g.r.a.m.v.a.d.i.
0006E4D0  73 00 69 00 2E 00 63 00  6F 00 6D 00 2F 00 00 00  s.i...c.o.m./...
```

FIGURE 3: HEX VIEW SHOW MALWARE STRING DATA

Registry Activities

I monitored the Registry activities after running the Sys32.exe. You can see what malware changes in the Registry that includes creating and modifying.

Values added: 2

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Sys32: "C:\Windows Live\Data\Sys32.exe /WinStart"

HKU\S-1-5-21-1292428093-261903793-725345543-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Cebtenz Svyrf\Jvaqbjf Yvir\Jvaqbjf Yvir\Qngn\Flf32.rkr: 01 00 00 00 06 00 00 00 B0 B5 F5 E2 33 48 D0 01

HKU\S-1-5-21-1292428093-261903793-725345543-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Program Files\Windows Live\Windows Live\Data\Sys32.exe: "Sys32"

Values modified: 2

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: D9 7E 56 A6 E6 DF 62 6F 4D B4 F0 C7 A3 E5 BC AA C7 5D 0E AD 4D 6E B1 8B B6 CF 67 45 9B 6D AC 21 85 CB 7E E7 DE 76 75 8E 54 63 2C 62 A5 01 EC 42 2D 5C E6 57 4A A2 08 A9 E9 3A DB 81 D9 1B 62 8B DD CF F5 C6 A3 CA DA F7 14 CD 9C 94 EF DE 6C 1B

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: DC DA E3 25 B4 43 4F D1 13 D3 C0 80 79 79 1B 3A 1B 9D A8 EE 81 38 3B FF 86 9F B9 C8 43 74 5E 4C 7A F0 50 90 E1 35 B4 A3 A4 12 CC 12 97 8B D9 24 28 CB 1B 54 C2 78 FE 56 C5 FA 6A 52 88 DC 39 6F 87 33 17 FE C3 78 C9 E5 71 09 6D CF AF 56 91 C8

HKU\S-1-5-21-1292428093-261903793-725345543-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU: 01 00 00 00 39 00 00 00 90 20 AB D8 33 48 D0 01

HKU\S-1-5-21-1292428093-261903793-725345543-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU: 01 00 00 00 3A 00 00 00 B0 B5 F5 E2 33 48 D0 01

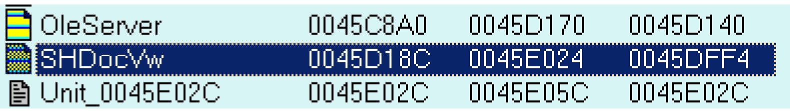
HKU\S-1-5-21-1292428093-261903793-725345543-1003\Software\Microsoft\Direct3D\MostRecentApplication\Name: "Sys32.exe"

Registry Activity After Run Browser

```
"RegQueryValue","HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\EnableFileTracing","SUCCESS","Type: REG_DWORD, Length: 4, Data: 0"
"RegQueryValue","HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\FileTracingMask","SUCCESS","Type: REG_DWORD, Length: 4, Data: 4294901760"
"RegQueryValue","HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\EnableConsoleTracing","SUCCESS","Type: REG_DWORD, Length: 4, Data: 0"
"RegQueryValue","HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\ConsoleTracingMask","SUCCESS","Type: REG_DWORD, Length: 4, Data: 4294901760"
"RegQueryValue","HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\MaxFileSize","SUCCESS","Type: REG_DWORD, Length: 4, Data: 1048576"
"RegQueryValue","HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\FileDirectory","SUCCESS","Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\tracing"
"RegQueryValue","HKLM\SOFTWARE\Microsoft\Tracing\RASAPI32\FileDirectory","SUCCESS","Type: REG_EXPAND_SZ, Length: 34, Data: %windir%\tracing"
"RegOpenKey","HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings","SUCCESS","Desired Access: Query Value"
"RegQueryValue","HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ProxySettingsPerUser","NAME NOT FOUND","Length: 144"
"RegCloseKey","HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings","SUCCESS",""
"RegOpenKey","HKCU","SUCCESS","Desired Access: Query Value, Set Value"
"RegOpenKey","HKCU\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections","SUCCESS","Desired Access: Query Value"
"RegQueryValue","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings","BUFFER OVERFLOW","Length: 144"
"RegQueryValue","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings","BUFFER OVERFLOW","Length: 144"
"RegQueryValue","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings","SUCCESS","Type: REG_BINARY, Length: 184, Data: 46 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00"
"RegCloseKey","HKCU","SUCCESS",""
"RegCloseKey","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections","SUCCESS",""
"RegOpenKey","HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings","SUCCESS","Desired Access: Query Value"
"RegQueryValue","HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ProxySettingsPerUser","NAME NOT FOUND","Length: 144"
"RegCloseKey","HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings","SUCCESS",""
"RegOpenKey","HKCU","SUCCESS","Desired Access: Query Value, Set Value"
"RegOpenKey","HKCU\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections","SUCCESS","Desired Access: Query Value"
"RegQueryValue","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings","BUFFER OVERFLOW","Length: 144"
"RegQueryValue","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings","BUFFER OVERFLOW","Length: 144"
"RegQueryValue","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings","SUCCESS","Type: REG_BINARY, Length: 184, Data: 46 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00"
"RegCloseKey","HKCU","SUCCESS",""
"RegCloseKey","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections","SUCCESS",""
```

What Is SHDocVw ?

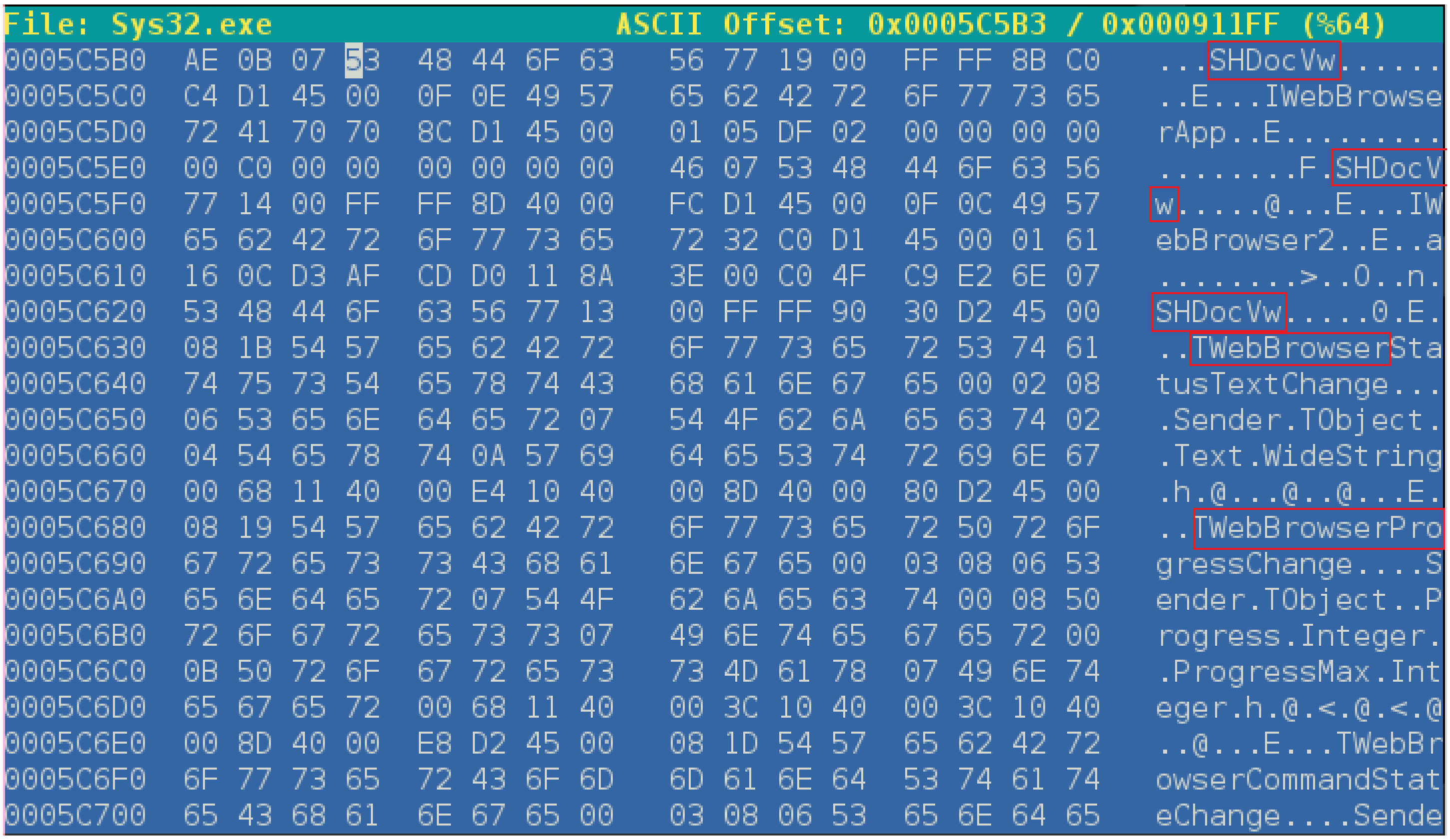
The malware uses SHDocVw for controlling the victim's Internet Explorer (IE) for information gathering.



```
OleServer        0045C8A0   0045D170   0045D140
SHDocVw          0045D18C   0045E024   0045DFF4
Unit_0045E02C    0045E02C   0045E05C   0045E02C
```

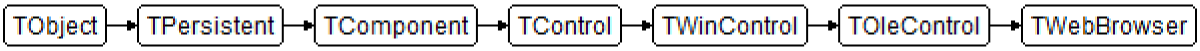
FIGURE 4: USING DELPHI DECAMPILER FOR UNIT FINDING

✓ You can see the string of the SHDocVw that used for hooking IE.



```
File: Sys32.exe                  ASCII Offset: 0x0005C5B3 / 0x000911FF (%64)
0005C5B0   AE 0B 07 53  48 44 6F 63   56 77 19 00  FF FF 8B C0   ...SHDocVw......
0005C5C0   C4 D1 45 00  0F 0E 49 57   65 62 42 72  6F 77 73 65   ..E...IWebBrowse
0005C5D0   72 41 70 70  8C D1 45 00   01 05 DF 02  00 00 00 00   rApp..E.........
0005C5E0   00 C0 00 00  00 00 00 00   46 07 53 48  44 6F 63 56   ........F.SHDocV
0005C5F0   77 14 00 FF  FF 8D 40 00   FC D1 45 00  0F 0C 49 57   w.....@...E...IW
0005C600   65 62 42 72  6F 77 73 65   72 32 C0 D1  45 00 01 61   ebBrowser2..E..a
0005C610   16 0C D3 AF  CD D0 11 8A   3E 00 C0 4F  C9 E2 6E 07   ........>..O..n.
0005C620   53 48 44 6F  63 56 77 13   00 FF FF 90  30 D2 45 00   SHDocVw.....0.E.
0005C630   08 1B 54 57  65 62 42 72   6F 77 73 65  72 53 74 61   ..TWebBrowserSta
0005C640   74 75 73 54  65 78 74 43   68 61 6E 67  65 00 02 08   tusTextChange...
0005C650   06 53 65 6E  64 65 72 07   54 4F 62 6A  65 63 74 02   .Sender.TObject.
0005C660   04 54 65 78  74 0A 57 69   64 65 53 74  72 69 6E 67   .Text.WideString
0005C670   00 68 11 40  00 E4 10 40   00 8D 40 00  80 D2 45 00   .h.@...@..@...E.
0005C680   08 19 54 57  65 62 42 72   6F 77 73 65  72 50 72 6F   ..TWebBrowserPro
0005C690   67 72 65 73  73 43 68 61   6E 67 65 00  03 08 06 53   gressChange....S
0005C6A0   65 6E 64 65  72 07 54 4F   62 6A 65 63  74 00 08 50   ender.TObject..P
0005C6B0   72 6F 67 72  65 73 73 07   49 6E 74 65  67 65 72 00   rogress.Integer.
0005C6C0   0B 50 72 6F  67 72 65 73   73 4D 61 78  07 49 6E 74   .ProgressMax.Int
0005C6D0   65 67 65 72  00 68 11 40   00 3C 10 40  00 3C 10 40   eger.h.@.<.@.<.@
0005C6E0   00 8D 40 00  E8 D2 45 00   08 1D 54 57  65 62 42 72   ..@...E...TWebBr
0005C6F0   6F 77 73 65  72 43 6F 6D   6D 61 6E 64  53 74 61 74   owserCommandStat
0005C700   65 43 68 61  6E 67 65 00   03 08 06 53  65 6E 64 65   eChange....Sende
```

FIGURE 5: SEARCH FOR THE HEXADECIMAL & STRING IN SYS32.EXE

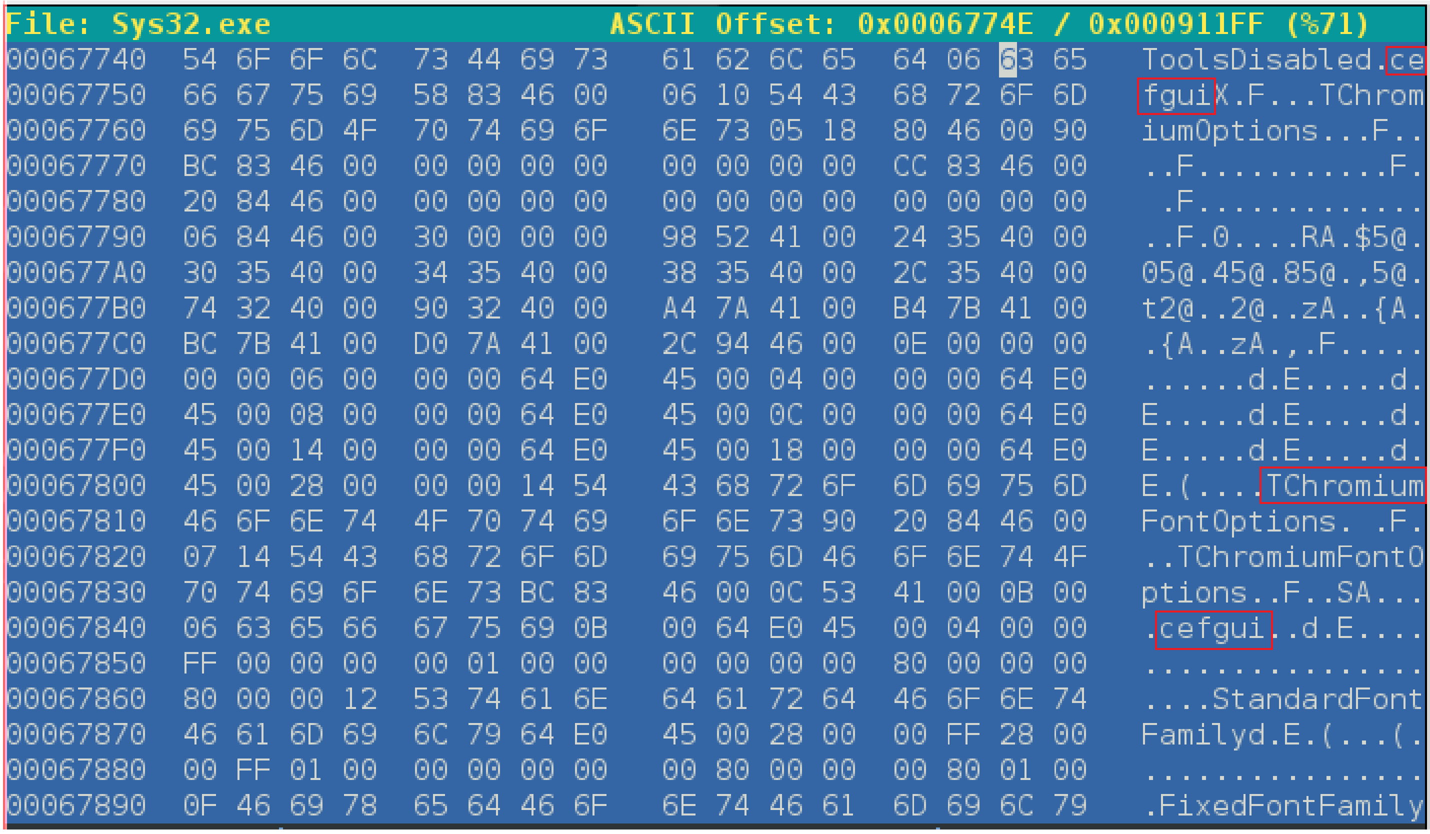


Description

TWebBrowser provides access to the Web browser functionality of Microsoft's Shell Doc Object and Control Library (SHDOCVW.DLL).
TWebBrowser wraps the IWebBrowser2 interface from Microsoft's Shell Doc Object and Control Library (SHDOCVW.DLL) to allow you to create a customized Web browsing application or to add Internet, file and network browsing, document viewing, and data downloading capabilities to your applications.
TWebBrowser wraps the SHDOCVW.DLL, and for this reason you must have **SHDOCVW.DLL** installed in order to use this component. This DLL ships with Internet Explorer 4 and later.
TWebBrowser uses the Internet Explorer component in the run-time environment, and each run-time environment might have different a version of the IE component. By default, **TWebBrowser** uses **IE7 Standards** mode even if the run-time environment installed the latest IE
(for example, IE11). To control the TWebBrower component's Browser Emulation mode, set the following registry entry:

What Is CEF (Cheromium Embedded Framwork) ?

Sys32.exe uses SHDocVw for controlling IE so if the victim is using Google Chrome the malware uses the CEF instead of SHDocVw .



```
File: Sys32.exe                 ASCII Offset: 0x0006774E / 0x000911FF (%71)
00067740  54 6F 6F 6C  73 44 69 73  61 62 6C 65  64 06 63 65  ToolsDisabled.ce
00067750  66 67 75 69  58 83 46 00  06 10 54 43  68 72 6F 6D  fguiX.F...TChrom
00067760  69 75 6D 4F  70 74 69 6F  6E 73 05 18  80 46 00 90  iumOptions...F..
00067770  BC 83 46 00  00 00 00 00  00 00 00 00  CC 83 46 00  ..F..........F.
00067780  20 84 46 00  00 00 00 00  00 00 00 00  00 00 00 00   .F.............
00067790  06 84 46 00  30 00 00 00  98 52 41 00  24 35 40 00  ..F.0....RA.$5@.
000677A0  30 35 40 00  34 35 40 00  38 35 40 00  2C 35 40 00  05@.45@.85@.,5@.
000677B0  74 32 40 00  90 32 40 00  A4 7A 41 00  B4 7B 41 00  t2@..2@..zA..{A.
000677C0  BC 7B 41 00  D0 7A 41 00  2C 94 46 00  0E 00 00 00  .{A..zA.,.F.....
000677D0  00 00 06 00  00 00 64 E0  45 00 04 00  00 00 64 E0  ......d.E.....d.
000677E0  45 00 08 00  00 00 64 E0  45 00 0C 00  00 00 64 E0  E.....d.E.....d.
000677F0  45 00 14 00  00 00 64 E0  45 00 18 00  00 00 64 E0  E.....d.E.....d.
00067800  45 00 28 00  00 00 14 54  43 68 72 6F  6D 69 75 6D  E.(....TChromium
00067810  46 6F 6E 74  4F 70 74 69  6F 6E 73 90  20 84 46 00  FontOptions. .F.
00067820  07 14 54 43  68 72 6F 6D  69 75 6D 46  6F 6E 74 4F  ..TChromiumFontO
00067830  70 74 69 6F  6E 73 BC 83  46 00 0C 53  41 00 0B 00  ptions..F..SA...
00067840  06 63 65 66  67 75 69 0B  00 64 E0 45  00 04 00 00  .cefgui..d.E....
00067850  FF 00 00 00  00 01 00 00  00 00 00 00  80 00 00 00  ................
00067860  80 00 00 12  53 74 61 6E  64 61 72 64  46 6F 6E 74  ....StandardFont
00067870  46 61 6D 69  6C 79 64 E0  45 00 28 00  00 FF 28 00  Familyd.E.(...(.
00067880  00 FF 01 00  00 00 00 00  00 80 00 00  00 80 01 00  ................
00067890  0F 46 69 78  65 64 46 6F  6E 74 46 61  6D 69 6C 79  .FixedFontFamily
```

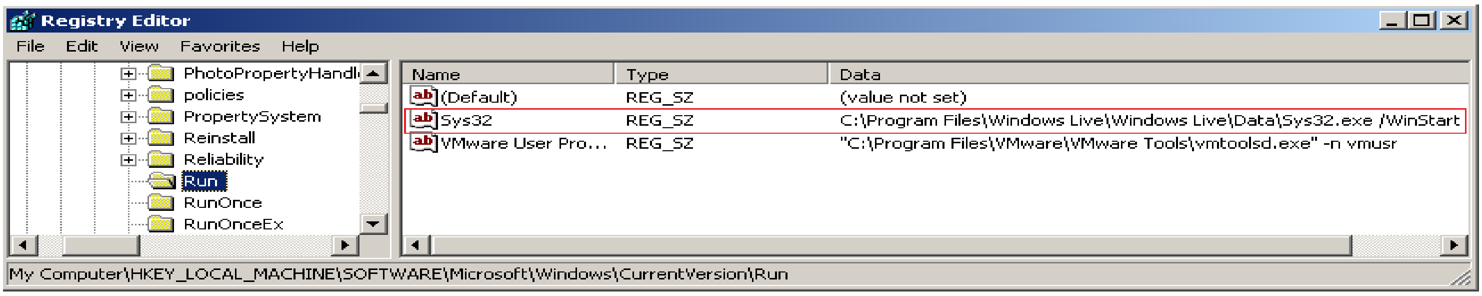
FIGURE 6: SEARCH FPR THE HEXADECIMAL & STRING IN SYS32.EXE

Description

The Chromium Embedded Framework (CEF) is an open source framework for embedding a web browser control based on Chromium. It is a convenient way to implement an HTML5 based GUI in a desktop application or to provide browser capabilities to an application, and provides the infrastructure developers need to quickly add HTML renderer and JavaScript to a C++ project. It also comes with bindings for C, C++, Delphi, Go, Java, .NET / Mono, Python and runs on Linux, Mac OS X and Windows.

Start Up

With the analysis of the data obtained so far, it is easy to approach to startup of the malware. The malware add a key in a registry for execute again.



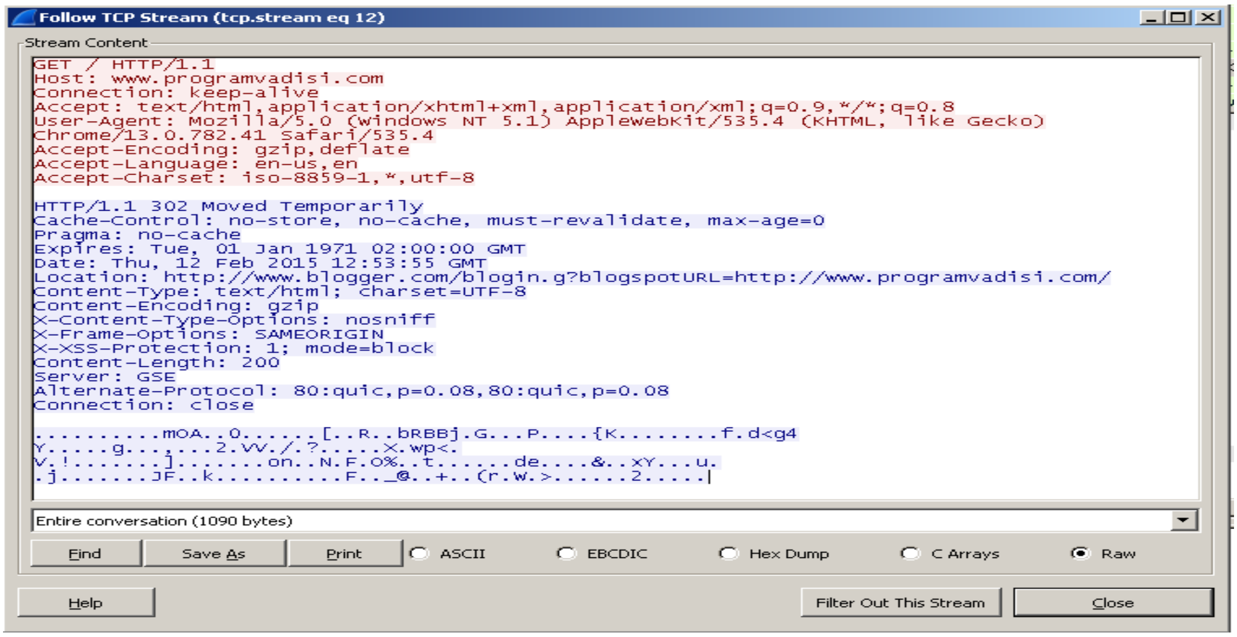
Name	Type	Data
(Default)	REG_SZ	(value not set)
Sys32	REG_SZ	C:\Program Files\Windows Live\Windows Live\Data\Sys32.exe /WinStart
VMware User Pro...	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

FIGURE 7: SYS32.EXE HAS LOADED INTO SYSTEM STARTUP

Network Monitoring

We analyzed the behavior of the Sys32.exe with Wireshark, we understand that Sys32.exe sends packet via HTTP protocol. The victim's information sends to a website (programvadisi.com). This website is responsible for gathering information of victims from Sys32.exe. Currently this website is unavailable by Google.

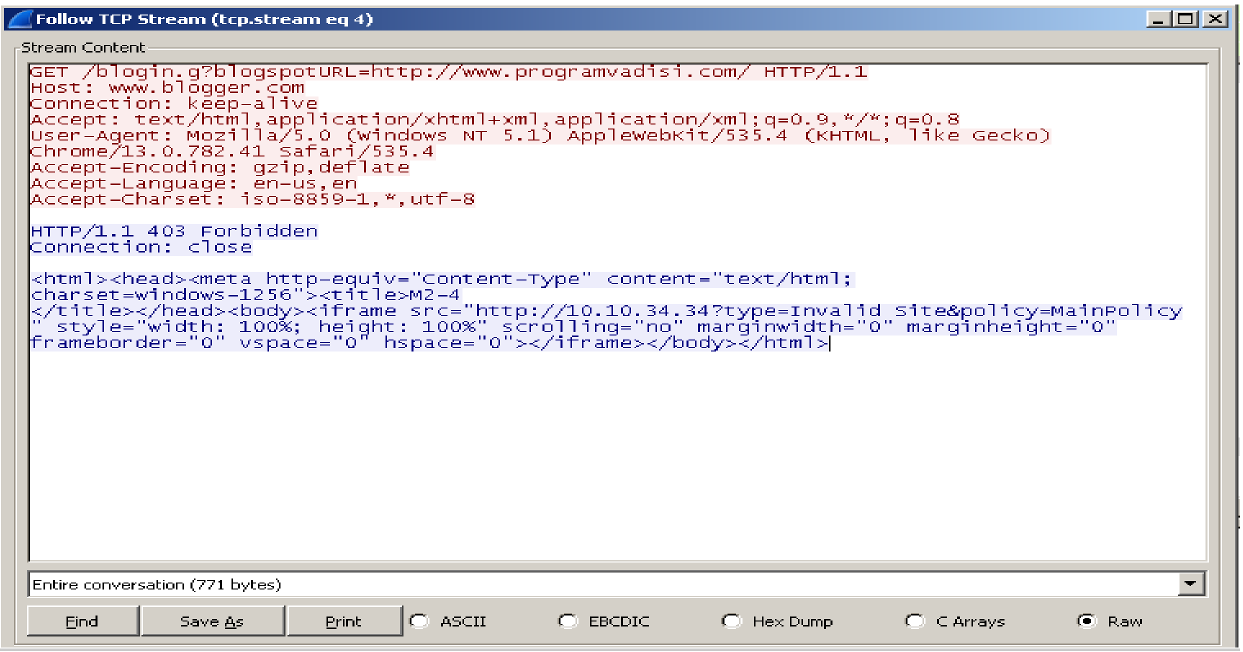


```
GET / HTTP/1.1
Host: www.programvadisi.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/535.4 (KHTML, like Gecko)
Chrome/13.0.782.41 Safari/535.4
Accept-Encoding: gzip,deflate
Accept-Language: en-us,en
Accept-Charset: iso-8859-1,*,utf-8

HTTP/1.1 302 Moved Temporarily
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Pragma: no-cache
Expires: Tue, 01 Jan 1971 02:00:00 GMT
Date: Thu, 12 Feb 2015 12:53:55 GMT
Location: http://www.blogger.com/blogin.g?blogspotURL=http://www.programvadisi.com/
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Length: 200
Server: GSE
Alternate-Protocol: 80:quic,p=0.08,80:quic,p=0.08
Connection: close

.........mOA..0......[..R..bRBBj.G...P....{K........f.d<g4
Y.....g...,...2.VV./.?.....X.wp<.
V.!.......]......on..N.F.O%..t......de....&..xY...u.
.j.......JF..k..........F.._@..+..(r.W.>......2.....
```

Entire conversation (1090 bytes)

FIGURE 8: PACKET CAPTURES OF SCREEN CAPTURE PROCESS USING WIRESHARK

Sys32.exe is still there so trying to sends the victim's information to programvadisi.com. The website hosted by Blogger and currently is not available. Sys32.exe sends the information and because of websites unavailability the victims information redirected to blogger services and the packet dropped by Google.

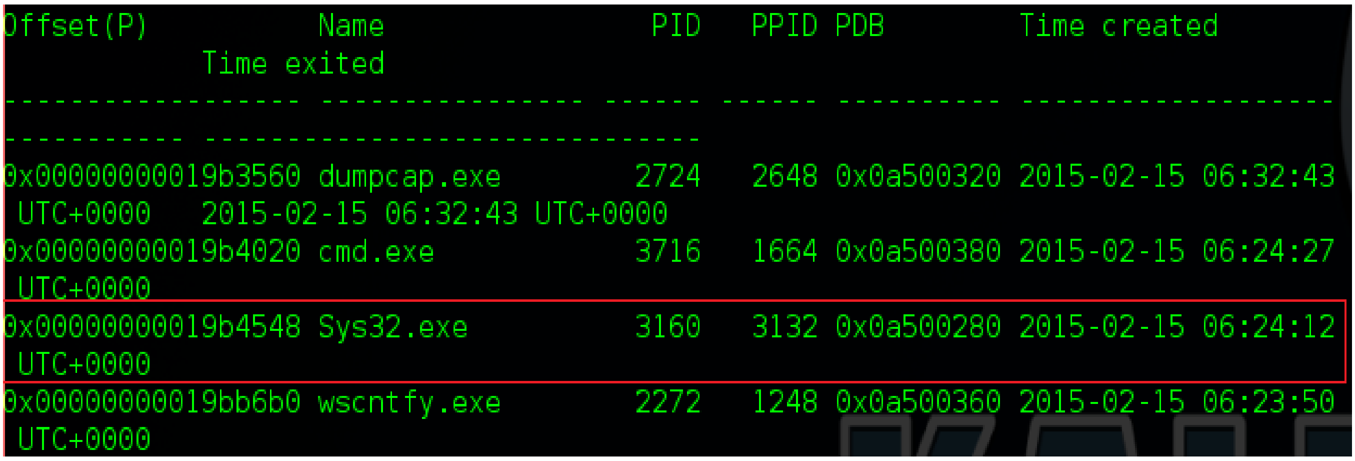


```
GET /blogin.g?blogspotURL=http://www.programvadisi.com/ HTTP/1.1
Host: www.blogger.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/535.4 (KHTML, like Gecko)
Chrome/13.0.782.41 Safari/535.4
Accept-Encoding: gzip,deflate
Accept-Language: en-us,en
Accept-Charset: iso-8859-1,*,utf-8

HTTP/1.1 403 Forbidden
Connection: close

<html><head><meta http-equiv="Content-Type" content="text/html;
charset=windows-1256"><title>M2-4
</title></head><body><iframe src="http://10.10.34.34?type=Invalid Site&policy=MainPolicy
" style="width: 100%; height: 100%" scrolling="no" marginwidth="0" marginheight="0"
frameborder="0" vspace="0" hspace="0"></iframe></body></html>
```

Entire conversation (771 bytes)

FIGURE 9: PACKET CAPTURES OF SCREEN CAPTURE PROCESS USING WIRESHARK

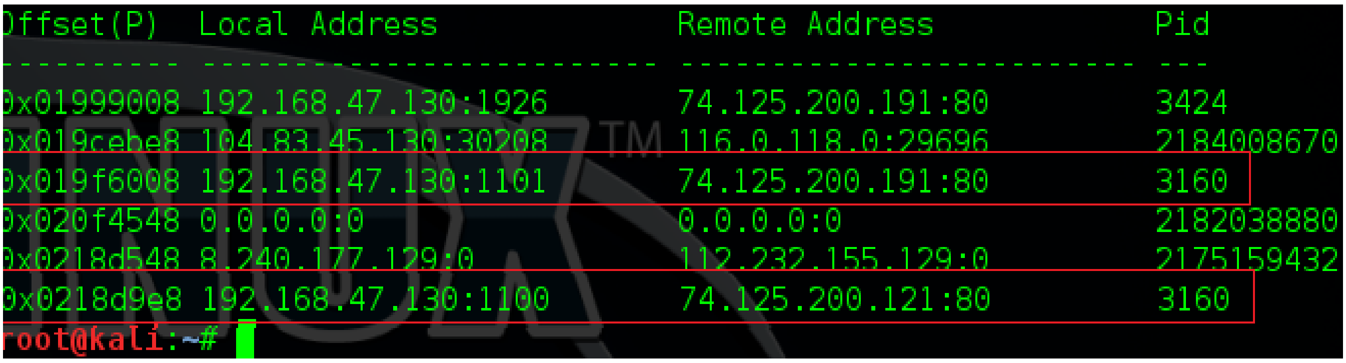
You can see Sys32.exe process running with PID 3160.



```
Offset(P)          Name                    PID   PPID PDB        Time created
           Time exited
------------------ ---------------- ------ ------ ---------- ------------------
---------- ------------------------------
0x00000000019b3560 dumpcap.exe        2724   2648 0x0a500320 2015-02-15 06:32:43
 UTC+0000   2015-02-15 06:32:43 UTC+0000
0x00000000019b4020 cmd.exe            3716   1664 0x0a500380 2015-02-15 06:24:27
 UTC+0000
0x00000000019b4548 Sys32.exe          3160   3132 0x0a500280 2015-02-15 06:24:12
 UTC+0000
0x00000000019bb6b0 wscntfy.exe        2272   1248 0x0a500360 2015-02-15 06:23:50
 UTC+0000
```

FIGURE 10: SYS32 ALONGSIDE OTHER RUNNING PROCESSES

Check all the TCP connections established using “connscan”. The Sys32.EXE process seems to have established a connection here.



```
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x01999008 192.168.47.130:1926       74.125.200.191:80         3424
0x019cebe8 104.83.45.130:30208       116.0.118.0:29696         2184008670
0x019f6008 192.168.47.130:1101       74.125.200.191:80         3160
0x020f4548 0.0.0.0:0                 0.0.0.0:0                 2182038880
0x0218d548 8.240.177.129:0           112.232.155.129:0         2175159432
0x0218d9e8 192.168.47.130:1100       74.125.200.121:80         3160
root@kali:~#
```

FIGURE 11: TCP CONNECTION ESTABLISHED

Thread Activity

After first running of the Sys32.exe we capture its activities. This information includes each file’s memory address and memory changes. Even you can see Sys32.exe after first running creates multiple threads. All Sys32.exe activities on Hard disk is shown below:

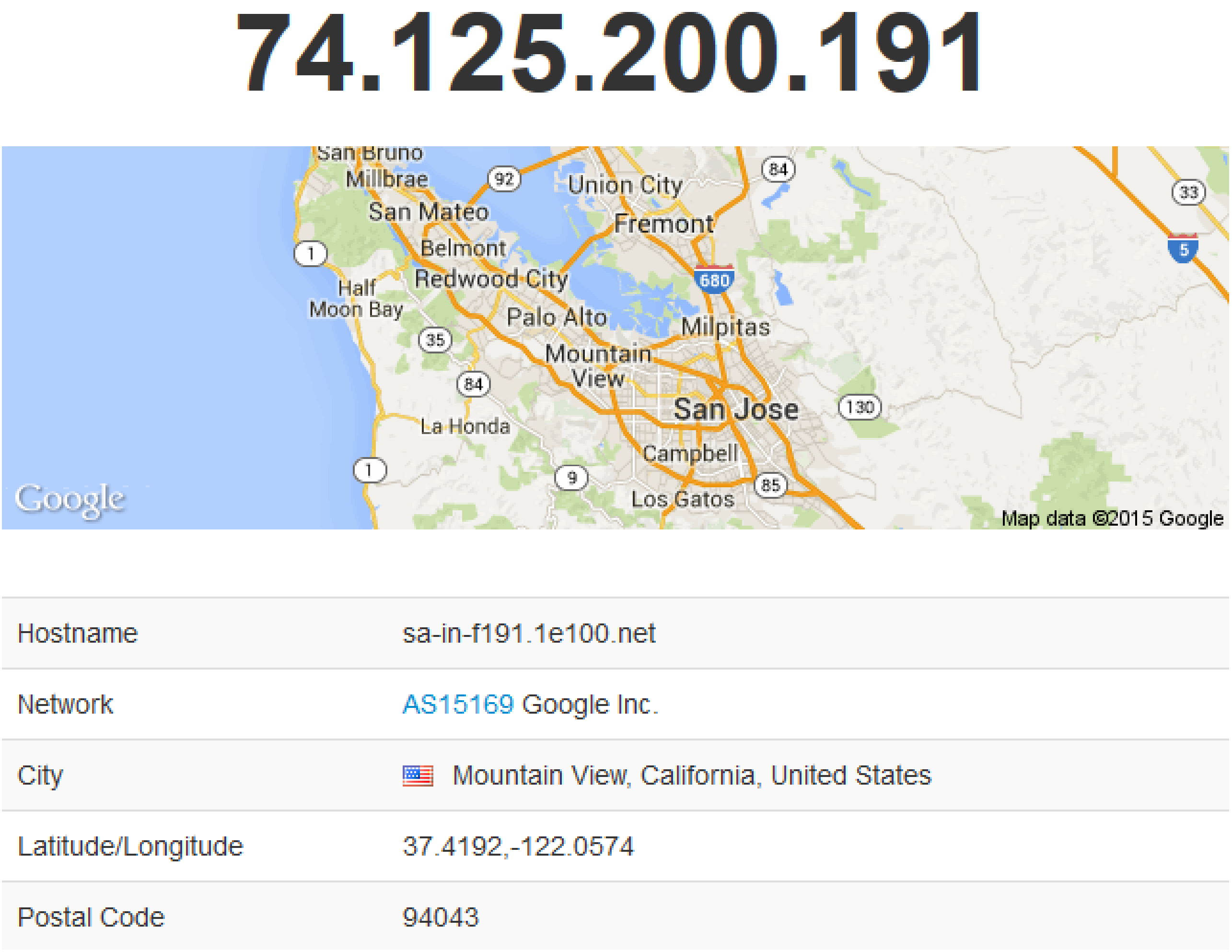
PID

```
"3148","Process Start","","Parent PID: 3128, Command line: ""C:\Program Files\Windows Live\Windows Live\Data\Sys32.exe"" , Current
directory: C:\Program Files\Windows Live\Windows Live\Data\, Environment: ; =::=::\;    ALLUSERSPROFILE=C:\Documents and
Settings\All Users;             APPDATA=C:\Documents and Settings\Lab\Application Data;   CLIENTNAME=Console;
            CommonProgramFiles=C:\Program Files\Common Files;         COMPUTERNAME=LAB-745C78354F4;
            ComSpec=C:\WINDOWS\system32\cmd.exe;            FP_NO_HOST_CHECK=NO;HOMEDRIVE=C:;   HOMEPATH=\Documents and
Settings\Lab;       LOGONSERVER=\\LAB-745C78354F4;            NUMBER_OF_PROCESSORS=1;       OS=Windows_NT;
            Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;
            PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;            PROCESSOR_ARCHITECTURE=x86;
            PROCESSOR_IDENTIFIER=x86 Family 6 Model 42 Stepping 7, GenuineIntel;         PROCESSOR_LEVEL=6;
            PROCESSOR_REVISION=2a07;         ProgramFiles=C:\Program Files;      SESSIONNAME=Console;   SystemDrive=C:;
            SystemRoot=C:\WINDOWS;           TEMP=C:\DOCUME~1\Lab\LOCALS~1\Temp;
            TMP=C:\DOCUME~1\Lab\LOCALS~1\Temp;  USERDOMAIN=LAB-745C78354F4;  USERNAME=Lab;  USERPROFILE=C:\Documents
and Settings\Lab; windir=C:\WINDOWS;
"3148","Thread Create","","Thread ID: 3152"
"3148","Load Image","C:\Program Files\Windows Live\Windows Live\Data\Sys32.exe","Image Base: 0x400000, Image Size: 0x98000"
"3148","Load Image","C:\WINDOWS\system32\ntdll.dll","Image Base: 0x7c900000, Image Size: 0xb2000"
"3148","Load Image","C:\WINDOWS\system32\kernel32.dll","Image Base: 0x7c800000, Image Size: 0xf6000"
"3148","Load Image","C:\WINDOWS\system32\user32.dll","Image Base: 0x7e410000, Image Size: 0x91000"
"3148","Load Image","C:\WINDOWS\system32\gdi32.dll","Image Base: 0x77f10000, Image Size: 0x49000"
"3148","Load Image","C:\WINDOWS\system32\advapi32.dll","Image Base: 0x77dd0000, Image Size: 0x9b000"
"3148","Load Image","C:\WINDOWS\system32\rpcrt4.dll","Image Base: 0x77e70000, Image Size: 0x93000"
"3148","Load Image","C:\WINDOWS\system32\secur32.dll","Image Base: 0x77fe0000, Image Size: 0x11000"
"3148","Load Image","C:\WINDOWS\system32\oleaut32.dll","Image Base: 0x77120000, Image Size: 0x8b000"
"3148","Load Image","C:\WINDOWS\system32\msvcrt.dll","Image Base: 0x77c10000, Image Size: 0x58000"
"3148","Load Image","C:\WINDOWS\system32\ole32.dll","Image Base: 0x774e0000, Image Size: 0x13e000"
"3148","Load Image","C:\WINDOWS\system32\version.dll","Image Base: 0x77c00000, Image Size: 0x8000"
"3148","Load Image","C:\WINDOWS\system32\comctl32.dll","Image Base: 0x5d090000, Image Size: 0x9a000"
"3148","Load Image","C:\WINDOWS\system32\shell32.dll","Image Base: 0x7c9c0000, Image Size: 0x818000"
"3148","Load Image","C:\WINDOWS\system32\shlwapi.dll","Image Base: 0x77f60000, Image Size: 0x76000"
"3148","Load Image","C:\WINDOWS\system32\imm32.dll","Image Base: 0x76390000, Image Size: 0x1d000"
"3148","Load Image","C:\WINDOWS\system32\lpk.dll","Image Base: 0x629c0000, Image Size: 0x9000"
"3148","Load Image","C:\WINDOWS\system32\usp10.dll","Image Base: 0x74d90000, Image Size: 0x6b000"
"3148","Load Image","C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.6028_x-
ww_61e65202\comctl32.dll","Image Base: 0x773d0000, Image Size: 0x103000"
"3148","Load Image","C:\WINDOWS\system32\MSCTFIME.IME","Image Base: 0x755c0000, Image Size: 0x2e000"
"3148","Load Image","C:\WINDOWS\system32\olepro32.dll","Image Base: 0x5edd0000, Image Size: 0x17000"
"3148","Load Image","C:\WINDOWS\system32\clbcatq.dll","Image Base: 0x76fd0000, Image Size: 0x7f000"
"3148","Load Image","C:\WINDOWS\system32\comres.dll","Image Base: 0x77050000, Image Size: 0xc5000"
"3148","Load Image","C:\WINDOWS\system32\ieframe.dll","Image Base: 0x3e1c0000, Image Size: 0xa9d000"
"3148","Load Image","C:\WINDOWS\system32\iertutil.dll","Image Base: 0x3dfd0000, Image Size: 0x1ec000"
"3148","Thread Create","","Thread ID: 3156"
"3148","Load Image","C:\Program Files\Windows Live\Windows Live\Data\libcef.dll","Image Base: 0x10000000, Image Size: 0x12b4000"
"3148","Load Image","C:\WINDOWS\system32\winhttp.dll","Image Base: 0x4d4f0000, Image Size: 0x59000"
"3148","Load Image","C:\WINDOWS\system32\ws2_32.dll","Image Base: 0x71ab0000, Image Size: 0x17000"
"3148","Load Image","C:\WINDOWS\system32\ws2help.dll","Image Base: 0x71aa0000, Image Size: 0x8000"
"3148","Load Image","C:\WINDOWS\system32\winmm.dll","Image Base: 0x76b40000, Image Size: 0x2d000"
"3148","Load Image","C:\WINDOWS\system32\winspool.drv","Image Base: 0x73000000, Image Size: 0x26000"
"3148","Load Image","C:\WINDOWS\system32\comdlg32.dll","Image Base: 0x763b0000, Image Size: 0x49000"
"3148","Load Image","C:\WINDOWS\system32\userenv.dll","Image Base: 0x769c0000, Image Size: 0xb4000"
"3148","Load Image","C:\WINDOWS\system32\setupapi.dll","Image Base: 0x77920000, Image Size: 0xf3000"
"3148","Load Image","C:\WINDOWS\system32\iphlpapi.dll","Image Base: 0x76d60000, Image Size: 0x19000"
"3148","Load Image","C:\WINDOWS\system32\urlmon.dll","Image Base: 0x78130000, Image Size: 0x134000"
"3148","Load Image","C:\WINDOWS\system32\crypt32.dll","Image Base: 0x77a80000, Image Size: 0x97000"
```

```
"3148","Load Image","C:\WINDOWS\system32\msasn1.dll","Image Base: 0x77b20000, Image Size: 0x12000"
"3148","Load Image","C:\WINDOWS\system32\msimg32.dll","Image Base: 0x76380000, Image Size: 0x5000"
"3148","Load Image","C:\WINDOWS\system32\psapi.dll","Image Base: 0x76bf0000, Image Size: 0xb000"
"3148","Load Image","C:\Program Files\Windows Live\Windows Live\Data\icudt.dll","Image Base: 0x4ad00000, Image Size: 0x965000"
"3148","Thread Create","","Thread ID: 3232"
"3148","Thread Create","","Thread ID: 3268"
"3148","Load Image","C:\Program Files\Windows Live\Windows Live\Data\avcodec-53.dll","Image Base: 0x65ec0000, Image Size: 0x1b9000"
"3148","Load Image","C:\Program Files\Windows Live\Windows Live\Data\avutil-51.dll","Image Base: 0x68b80000, Image Size: 0x28000"
"3148","Load Image","C:\Program Files\Windows Live\Windows Live\Data\avformat-53.dll","Image Base: 0x6ab00000, Image Size: 0x34000"
"3148","Load Image","C:\Program Files\Windows Live\Windows Live\Data\d3dcompiler_43.dll","Image Base: 0x35d0000, Image Size: 0x207000"
"3148","Load Image","C:\Program Files\Windows Live\Windows Live\Data\d3dx9_43.dll","Image Base: 0x37e0000, Image Size: 0x1ff000"
"3148","Load Image","C:\Program Files\Windows Live\Windows Live\Data\libGLESv2.dll","Image Base: 0x39e0000, Image Size: 0x9b000"
"3148","Load Image","C:\WINDOWS\system32\d3d9.dll","Image Base: 0x4fdd0000, Image Size: 0x1a6000"
"3148","Load Image","C:\WINDOWS\system32\d3d8thk.dll","Image Base: 0x6d990000, Image Size: 0x6000"
"3148","Load Image","C:\Program Files\Windows Live\Windows Live\Data\libEGL.dll","Image Base: 0x3aa0000, Image Size: 0x1f000"
"3148","Thread Create","","Thread ID: 3272"
"3148","Load Image","C:\WINDOWS\system32\mswsock.dll","Image Base: 0x71a50000, Image Size: 0x3f000"
"3148","Thread Create","","Thread ID: 968"
"3148","Thread Create","","Thread ID: 1012"
"3148","Load Image","C:\WINDOWS\system32\rasapi32.dll","Image Base: 0x76ee0000, Image Size: 0x3c000"
"3148","Load Image","C:\WINDOWS\system32\rasman.dll","Image Base: 0x76e90000, Image Size: 0x12000"
"3148","Load Image","C:\WINDOWS\system32\netapi32.dll","Image Base: 0x5b860000, Image Size: 0x56000"
"3148","Load Image","C:\WINDOWS\system32\tapi32.dll","Image Base: 0x76eb0000, Image Size: 0x2f000"
"3148","Load Image","C:\WINDOWS\system32\rtutils.dll","Image Base: 0x76e80000, Image Size: 0xe000"
"3148","Thread Create","","Thread ID: 940"
"3148","Load Image","C:\WINDOWS\system32\uxtheme.dll","Image Base: 0x5ad70000, Image Size: 0x38000"
"3148","Thread Create","","Thread ID: 1148"
"3148","Thread Create","","Thread ID: 3296"
"3148","Load Image","C:\WINDOWS\system32\dnsapi.dll","Image Base: 0x76f20000, Image Size: 0x27000"
"3148","Load Image","C:\WINDOWS\system32\rasadhlp.dll","Image Base: 0x76fc0000, Image Size: 0x6000"
"3148","Load Image","C:\WINDOWS\system32\hnetcfg.dll","Image Base: 0x662b0000, Image Size: 0x58000"
"3148","Load Image","C:\WINDOWS\system32\wshtcpip.dll","Image Base: 0x71a90000, Image Size: 0x8000"
"3148","Thread Create","","Thread ID: 1448"
"3148","Load Image","C:\WINDOWS\system32\MSCTF.dll","Image Base: 0x74720000, Image Size: 0x4c000"
"3148","Thread Create","","Thread ID: 4092"
"3148","Load Image","C:\WINDOWS\system32\msapsspc.dll","Image Base: 0x71e50000, Image Size: 0x15000"
"3148","Load Image","C:\WINDOWS\system32\msvcrt40.dll","Image Base: 0x78080000, Image Size: 0x11000"
"3148","Load Image","C:\WINDOWS\system32\schannel.dll","Image Base: 0x767f0000, Image Size: 0x29000"
"3148","Load Image","C:\WINDOWS\system32\credssp.dll","Image Base: 0x59c00000, Image Size: 0x7000"
"3148","Load Image","C:\WINDOWS\system32\digest.dll","Image Base: 0x75b00000, Image Size: 0x15000"
"3148","Load Image","C:\WINDOWS\system32\msnsspc.dll","Image Base: 0x747b0000, Image Size: 0x47000"
"3148","Load Image","C:\WINDOWS\system32\msvcrt40.dll","Image Base: 0x78080000, Image Size: 0x11000"
"3148","Load Image","C:\WINDOWS\system32\credssp.dll","Image Base: 0x59c00000, Image Size: 0x7000"
"3148","Load Image","C:\WINDOWS\system32\schannel.dll","Image Base: 0x767f0000, Image Size: 0x29000"
"3148","Load Image","C:\WINDOWS\system32\msv1_0.dll","Image Base: 0x77c70000, Image Size: 0x25000"
"3148","Load Image","C:\WINDOWS\system32\cryptdll.dll","Image Base: 0x76790000, Image Size: 0xc000"
"3148","Thread Exit","","Thread ID: 3296, User Time: 0.0000000, Kernel Time: 0.0312500"
```

Observations regarding hosts / IP addresses / registrars

Sys32.exe is in charge to gathering and sending information to programvadisi.com, so the website hosted by Google Blogger service and the IP addresses we discovered with “Connscan” is also belong to Google .



74.125.200.191

Hostname	sa-in-f191.1e100.net
Network	AS15169 Google Inc.
City	Mountain View, California, United States
Latitude/Longitude	37.4192,-122.0574
Postal Code	94043

FIGURE 12: IP ADDRESS INFORMATION

Domain Registrant Info

The domain registry information includes some interesting information that is worth to be man-ed here. The domains included in the binary: Programvidisi.com, Share common elements: they are all registered the same day by the same “person” at the same registrar:

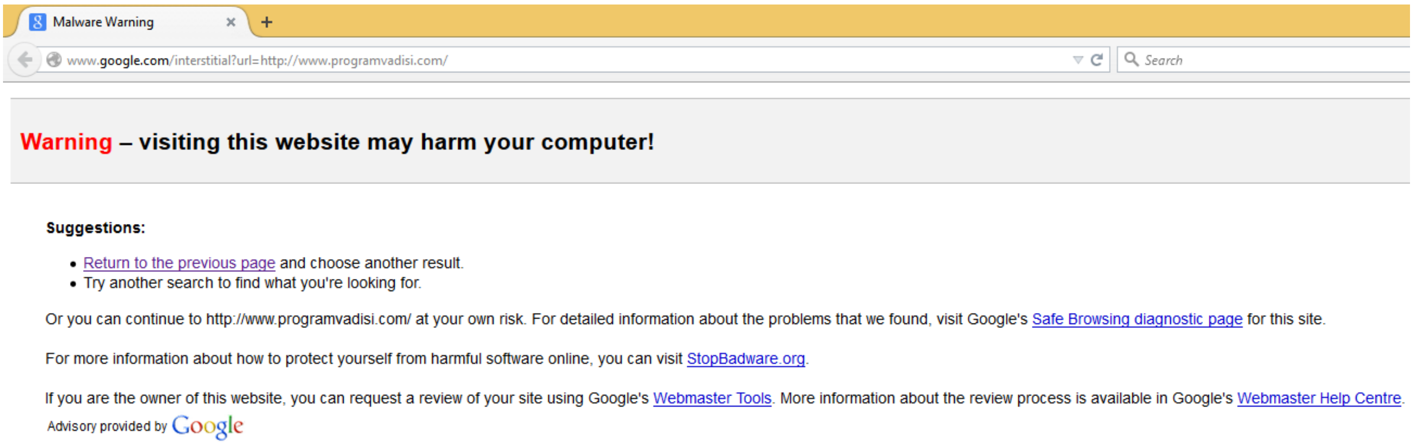
```
Domain Name: PROGRAMVADISI.COM
Registrar WHOIS Server: http://whois.nicproxy.com
Registrar URL: http://www.nicproxy.com
Updated Date: 2014-11-09T21:46:22Z
Creation Date: 2013-05-30T09:09:37Z
Registrar Registration Expiration Date: 2016-05-30T09:09:37Z
Registrar:NICS TELEKOMUNIKASYON TICARET LTD.STI.
Registrar IANA ID: 1454
Registrar Abuse Contact Email: abuse@nicproxy.com
Registrar Abuse Contact Phone: +90.2122132963
```

```
Domain Status: ok http://www.icann.org/epp#OK
Registry Registrant ID: CID-706596PRO
Registrant Name: Unal Cebeci
Registrant Organization: Unal Cebeci
Registrant Street: Alemdar mahallesi
Registrant City: Bursa
Registrant State / Province: Osmangazi
Registrant Postal Code: 16190
Registrant Country: TR
Registrant Phone: 90.2242400990
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: unalsevim16@gmail.com
Registry Admin ID: CID-706596PRO
Admin Name: Unal Cebeci
Admin Organization: Unal Cebeci
Admin Street: Alemdar mahallesi
Admin City: Bursa
Admin State / Province: Osmangazi
Admin Postal Code: 16190
Admin Country: TR
Admin Phone: 90.2242400990
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Name Server: NS1.NATROHOST.COM
Name Server: NS2.NATROHOST.COM
DNSSEC: Unsigned
Unalsevim16
```

- Interestingly, there are around 8 domains listed at domaintools.com which are all registered by the email address 'unalsevim16@gmail.com'. It would be no surprise if those domains are also used for malicious activities. These domains are included in the Appendix.

Google: If Your Site Is Infected

Programvadisi.com has been blocked by Google.


Malware Warning
www.google.com/interstitial?url=http://www.programvadisi.com/
Search

Warning – visiting this website may harm your computer!

Suggestions:

- Return to the previous page and choose another result.
- Try another search to find what you're looking for.

Or you can continue to http://www.programvadisi.com/ at your own risk. For detailed information about the problems that we found, visit Google's Safe Browsing diagnostic page for this site.

For more information about how to protect yourself from harmful software online, you can visit StopBadware.org.

If you are the owner of this website, you can request a review of your site using Google's Webmaster Tools. More information about the review process is available in Google's Webmaster Help Centre.

Advisory provided by Google

FIGURE 13: PAGE DETECTED BY GOOGLE

Relation to Suspicious Web Hosting and Wares Data

Two other domains that share very similar are netrohost.com and muhasebe-tr.net

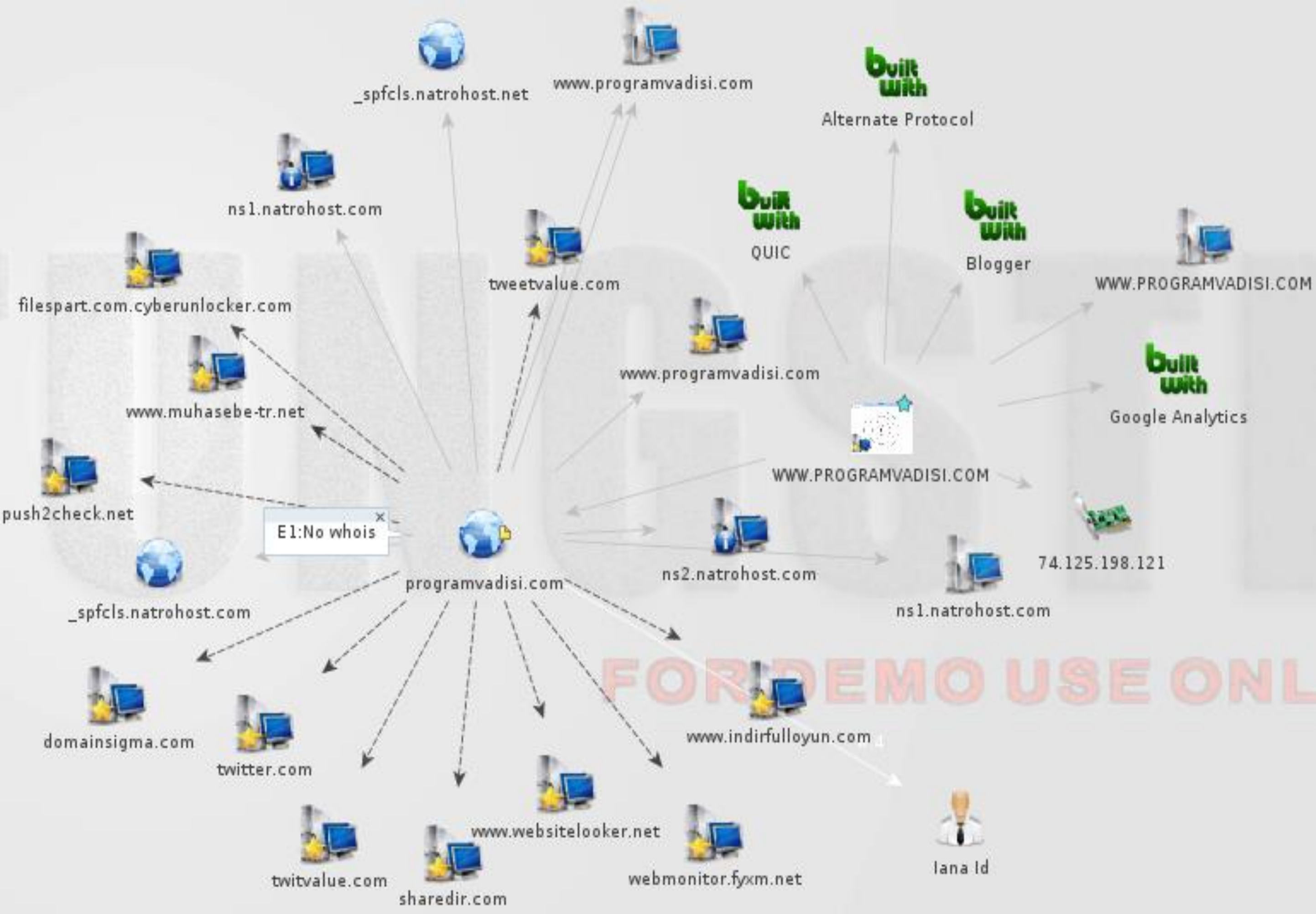


FIGURE 14: ONLINE RESULT OF INTELLIGENCE AND FORENSICS APPLIICATION

Reference:

http://docwiki.embarcadero.com/Libraries/XE7/en/SHDocVw.TWebBrowser
http://en.wikipedia.org/wiki/Chromium_Embedded_Framework
http://who.is/whois/programvadisi.com
https://code.google.com/p/chromiumembedded/
http://reversewhois.domaintools.com/?email=11a0afaddd29ab2ef55fb2a15c3f2d2c
http://en.wikipedia.org/wiki/Maltego