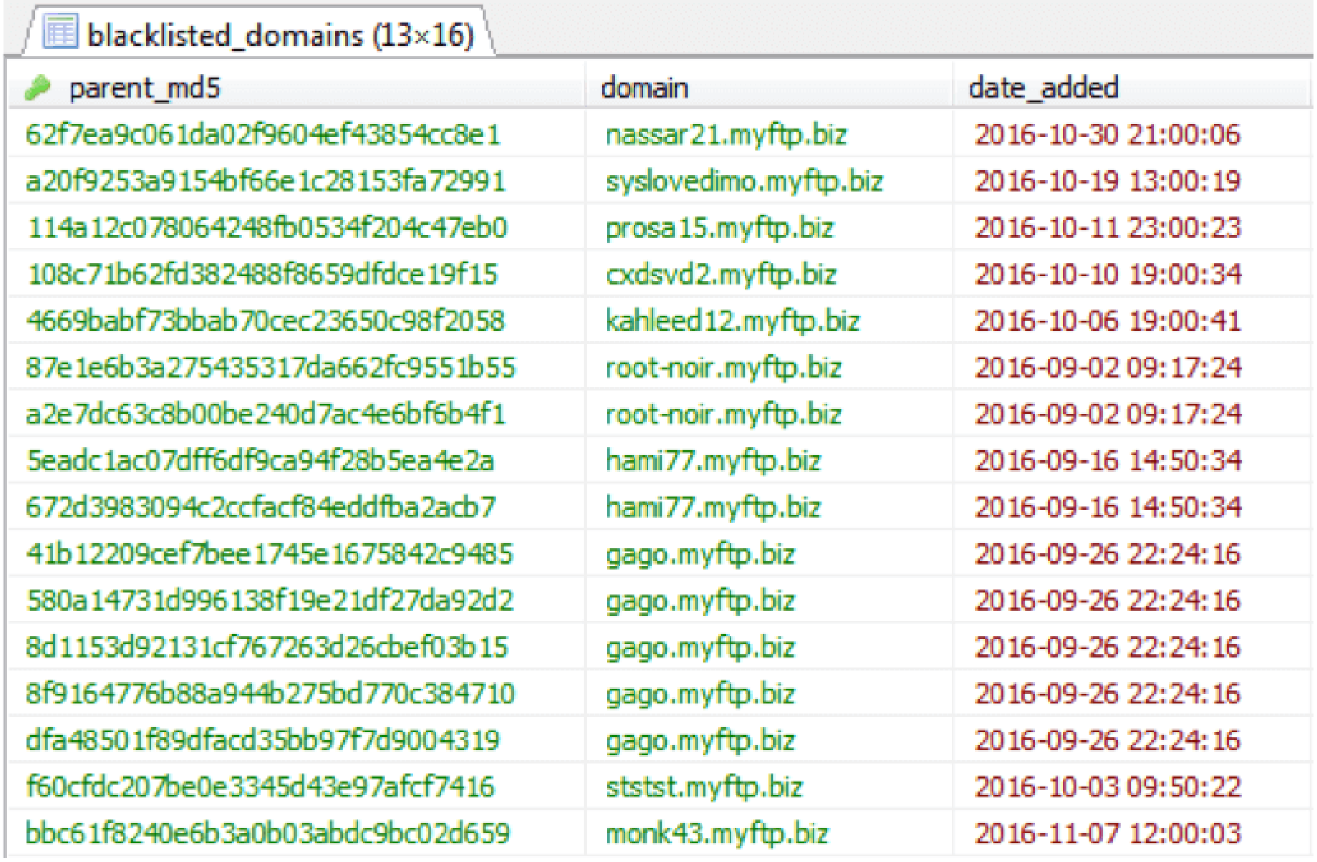
Bladabindi Remains A Constant Threat By Using Dynamic DNS Services

blog.fortinet.com/2016/11/30/bladabindi-remains-a-constant-threat-by-using-dynamic-dns-services

November 30, 2016



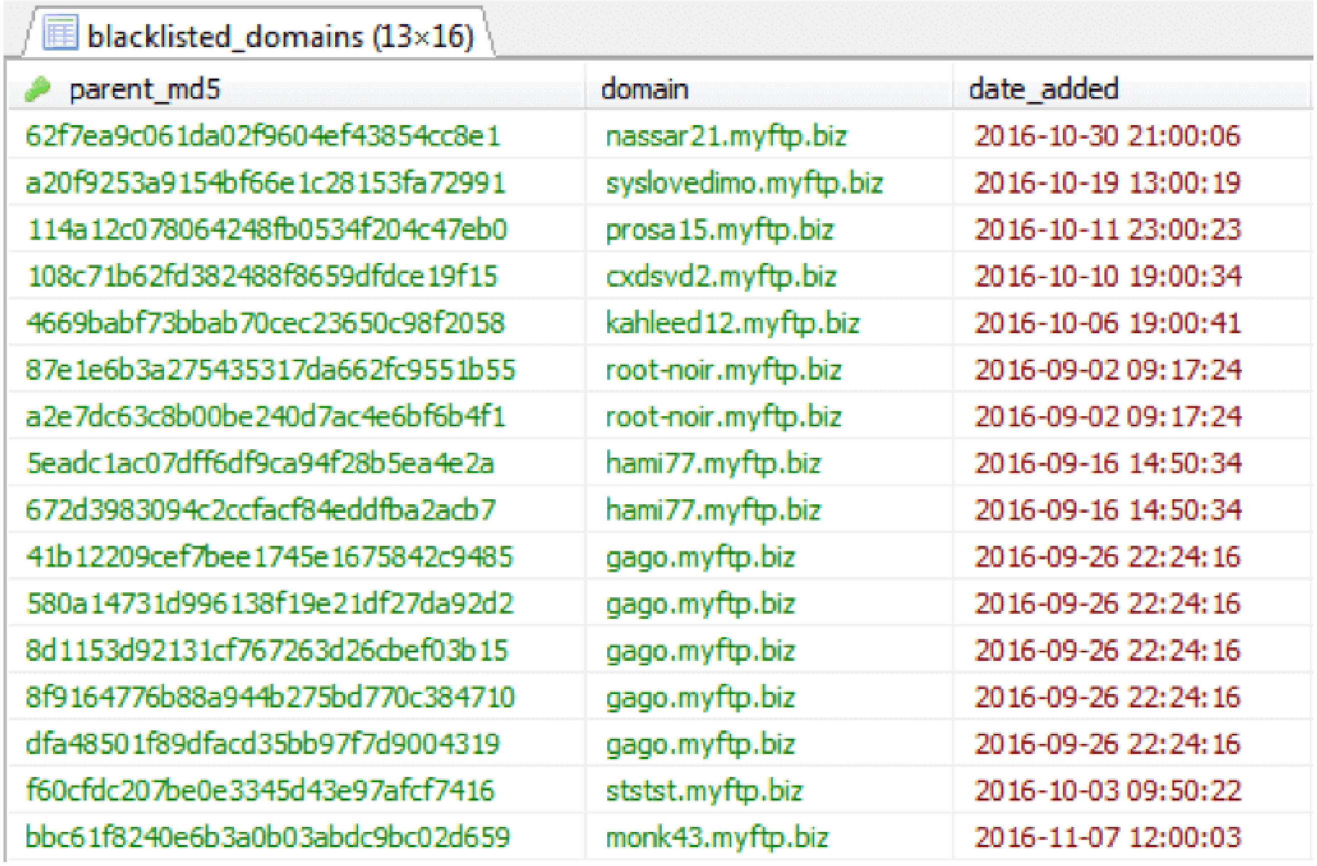
blacklisted_domains (13×16)

parent_md5	domain	date_added
62f7ea9c061da02f9604ef43854cc8e1	nassar21.myftp.biz	2016-10-30 21:00:06
a20f9253a9154bf66e1c28153fa72991	syslovedimo.myftp.biz	2016-10-19 13:00:19
114a12c078064248fb0534f204c47eb0	prosa15.myftp.biz	2016-10-11 23:00:23
108c71b62fd382488f8659dfdce19f15	cxdsvd2.myftp.biz	2016-10-10 19:00:34
4669babf73bbab70cec23650c98f2058	kahleed12.myftp.biz	2016-10-06 19:00:41
87e1e6b3a275435317da662fc9551b55	root-noir.myftp.biz	2016-09-02 09:17:24
a2e7dc63c8b00be240d7ac4e6bf6b4f1	root-noir.myftp.biz	2016-09-02 09:17:24
5eadc1ac07dff6df9ca94f28b5ea4e2a	hami77.myftp.biz	2016-09-16 14:50:34
672d3983094c2ccfacf84eddfba2acb7	hami77.myftp.biz	2016-09-16 14:50:34
41b12209cef7bee1745e1675842c9485	gago.myftp.biz	2016-09-26 22:24:16
580a14731d996138f19e21df27da92d2	gago.myftp.biz	2016-09-26 22:24:16
8d1153d92131cf767263d26cbef03b15	gago.myftp.biz	2016-09-26 22:24:16
8f9164776b88a944b275bd770c384710	gago.myftp.biz	2016-09-26 22:24:16
dfa48501f89dfacd35bb97f7d9004319	gago.myftp.biz	2016-09-26 22:24:16
f60cfdc207be0e3345d43e97afcf7416	ststst.myftp.biz	2016-10-03 09:50:22
bbc61f8240e6b3a0b03abdc9bc02d659	monk43.myftp.biz	2016-11-07 12:00:03

Threat Research

By Lilia Elena Gonzalez Medina | November 30, 2016

The Fortinet research team has been developing a industrial-grade analysis system that allows us to concentrate information from samples collected from a variety of sources. Using this tool, we recently started to see the recurrence of URLs from the domains hopto.org and myftp.biz. In most cases, each sample was connected to a unique URL in one of the domains, although we also found some samples that connected to the same URL.



blacklisted_domains (13×16)

parent_md5	domain	date_added
62f7ea9c061da02f9604ef43854cc8e1	nassar21.myftp.biz	2016-10-30 21:00:06
a20f9253a9154bf66e1c28153fa72991	syslovedimo.myftp.biz	2016-10-19 13:00:19
114a12c078064248fb0534f204c47eb0	prosa15.myftp.biz	2016-10-11 23:00:23
108c71b62fd382488f8659dfdce19f15	cxdsvd2.myftp.biz	2016-10-10 19:00:34
4669babf73bbab70cec23650c98f2058	kahleed12.myftp.biz	2016-10-06 19:00:41
87e1e6b3a275435317da662fc9551b55	root-noir.myftp.biz	2016-09-02 09:17:24
a2e7dc63c8b00be240d7ac4e6bf6b4f1	root-noir.myftp.biz	2016-09-02 09:17:24
5eadc1ac07dff6df9ca94f28b5ea4e2a	hami77.myftp.biz	2016-09-16 14:50:34
672d3983094c2ccfacf84eddfba2acb7	hami77.myftp.biz	2016-09-16 14:50:34
41b12209cef7bee1745e1675842c9485	gago.myftp.biz	2016-09-26 22:24:16
580a14731d996138f19e21df27da92d2	gago.myftp.biz	2016-09-26 22:24:16
8d1153d92131cf767263d26cbef03b15	gago.myftp.biz	2016-09-26 22:24:16
8f9164776b88a944b275bd770c384710	gago.myftp.biz	2016-09-26 22:24:16
dfa48501f89dfacd35bb97f7d9004319	gago.myftp.biz	2016-09-26 22:24:16
f60cfdc207be0e3345d43e97afcf7416	ststst.myftp.biz	2016-10-03 09:50:22
bbc61f8240e6b3a0b03abdc9bc02d659	monk43.myftp.biz	2016-11-07 12:00:03

Figure 1. Examples of the domains and samples collected by the team's FortiGuard analysis system

This threat, also known as njRAT, is detected as MSIL/Bladabindi.U!tr or MSIL/Agent.LI!tr by the Fortinet AntiVirus service. If installed, the user's private data is compromised because of the malware's capability to provide the malicious actor with unauthorized access to the infected computer in order to collect different kinds of information, such as: screenshots, words typed (which often include usernames, passwords, websites, documents, etc.),running processes, pictures taken with the webcam, etc.

Threat Description

This malware family uses the .NET framework. And this sample in particular has two important classes called kl and OK.

kl

This class uses the functions GetAsyncKeyState, GetKeyboardLayout, GetKeyboardState, GetWindowThreadProcessId, MapVirtualKey and ToUnicodeEx to capture keystrokes.

OK

This class contains the other functionalities of the RAT. The important activities are summarized below:

Makes the following modifications to the registry:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\050ed846adcc1b8729af0a70a0fefe4d: “”C:\Users\\AppData\Local\Temp\server.exe” ..”

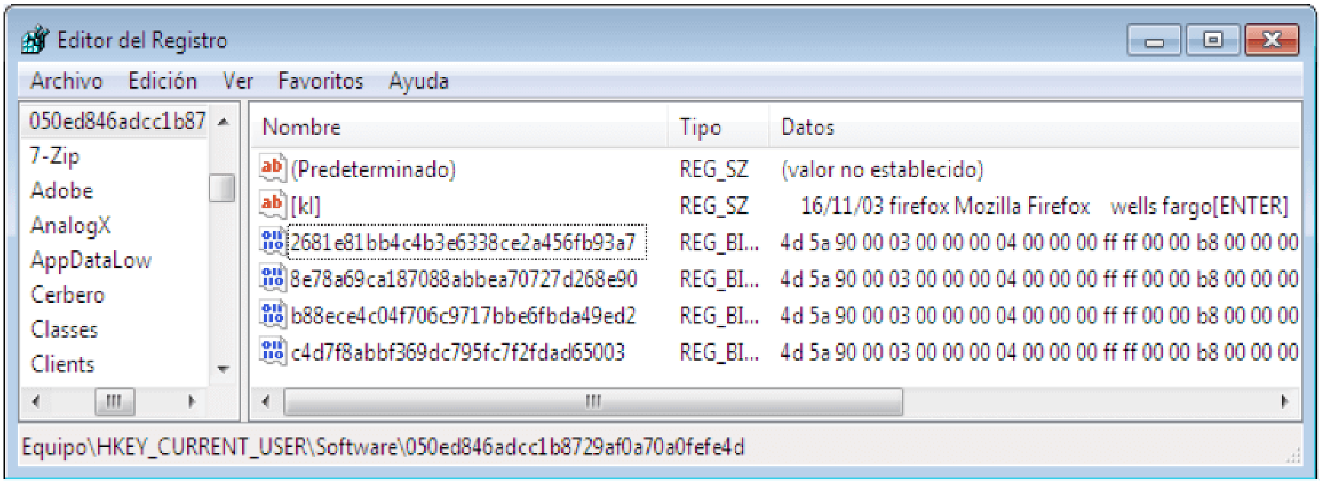
HKCU\Software\050ed846adcc1b8729af0a70a0fefe4d\[kl]: “”

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\050ed846adcc1b8729af0a70a0fefe4d: “”C:\Users\\AppData\Local\Temp\server.exe” ..”

HKCU\di: “!”

The string “050ed846adcc1b8729af0a70a0fefe4d” is hardcoded in the sample.

Besides storing the keylogger logs, the sub registry key HKCU\Software\050ed846adcc1b8729af0a70a0fefe4d\ also contains malicious executables loaded from the sample as binary data.



Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
[kl]	REG_SZ	16/11/03 firefox Mozilla Firefox wells fargo[ENTER]
2681e81bb4c4b3e6338ce2a456fb93a7	REG_BI...	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00
8e78a69ca187088abbea70727d268e90	REG_BI...	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00
b88ece4c04f706c9717bbe6fbda49ed2	REG_BI...	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00
c4d7f8abbf369dc795fc7f2fdad65003	REG_BI...	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00

Equipo\HKEY_CURRENT_USER\Software\050ed846adcc1b8729af0a70a0fefe4d

Figure 2. Malicious executables stored in Windows Registry

All those samples are, of course, detected by the Fortinet AntiVirus service:

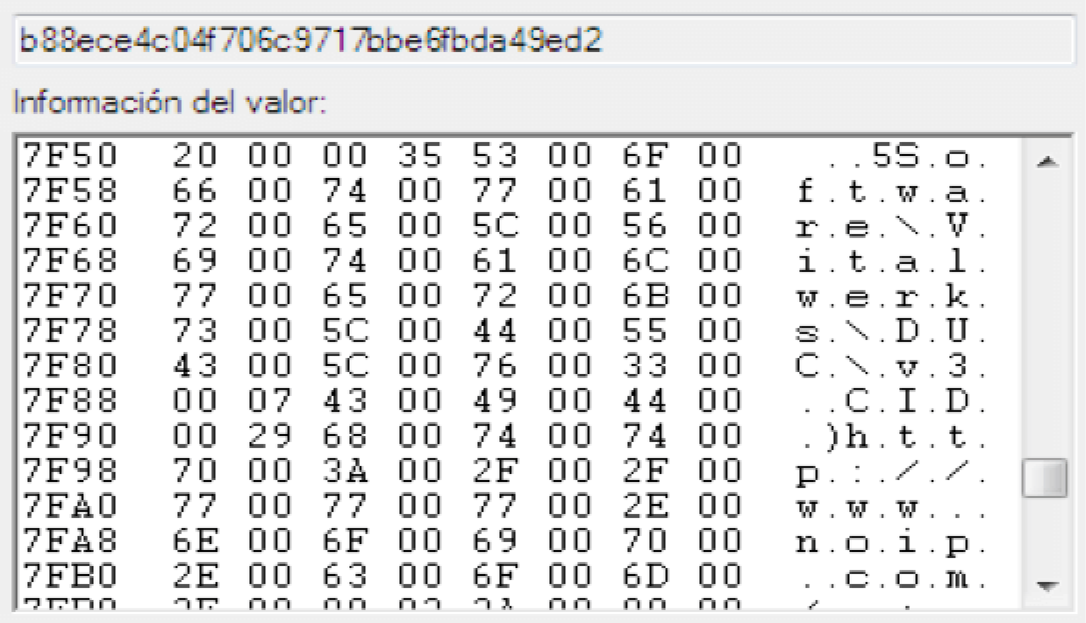
2681e81bb4c4b3e6338ce2a456fb93a7 Detected as MSIL/Bladabindi.U!tr

8e78a69ca187088abbea70727d268e90 Detected as MSIL/Bladabindi.U!tr

b88ece4c04f706c9717bbe6fbda49ed2 Detected as W32/Agent.CPGR!tr

c4d7f8abbf369dc795fc7f2fdad65003 Detected as MSIL/Bladabindi.U!tr

The strings in b88ece4c04f706c9717bbe6fbda49ed2 reference No-IP’s Dynamic Update Client (DUC) that automatically updates the IP address if it changes, but also contain lines like “SELECT * FROM moz_logins” to obtain Firefox’s stored credentials.



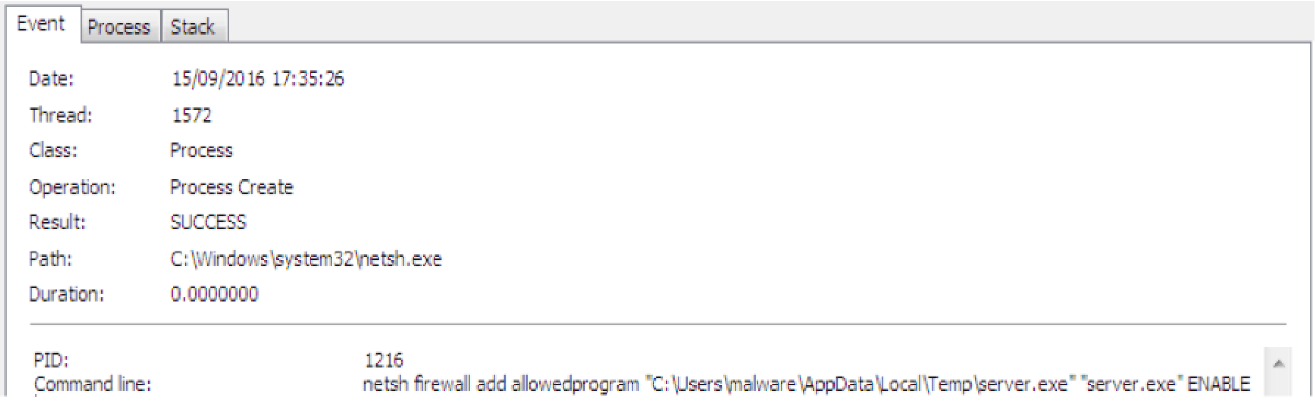
b88ece4c04f706c9717bbe6fbda49ed2

Información del valor:

```
7F50  20 00 00 35 53 00 6F 00   ..5S.o.
7F58  66 00 74 00 77 00 61 00   f.t.w.a.
7F60  72 00 65 00 5C 00 56 00   r.e.\.V.
7F68  69 00 74 00 61 00 6C 00   i.t.a.l.
7F70  77 00 65 00 72 00 6B 00   w.e.r.k.
7F78  73 00 5C 00 44 00 55 00   s.\.D.U.
7F80  43 00 5C 00 76 00 33 00   C.\.v.3.
7F88  00 07 43 00 49 00 44 00   ..C.I.D.
7F90  00 29 68 00 74 00 74 00   .)h.t.t.
7F98  70 00 3A 00 2F 00 2F 00   p.:././.
7FA0  77 00 77 00 77 00 2E 00   w.w.w...
7FA8  6E 00 6F 00 69 00 70 00   n.o.i.p.
7FB0  2E 00 63 00 6F 00 6D 00   ..c.o.m.
```

Figure 3. Part of a malicious executable stored as data

- Creates the mutex 050ed846adcc1b8729af0a70a0fefe4d. If the mutex already exists, the sample calls ProjectData.EndApp to close all related files and stop the process.
- Checks whether a file called server.exe already exists in C:\Users\\AppData\Local\Temp\. If it exists, the sample deletes it. Otherwise, the file is created and executed. The file server.exe is a copy of the sample.
- Creates an environment variable called “SEE_MASK_NOZONECHECKS” and sets its value to 1.
- Creates a rule to allow the process server.exe on the Windows firewall.

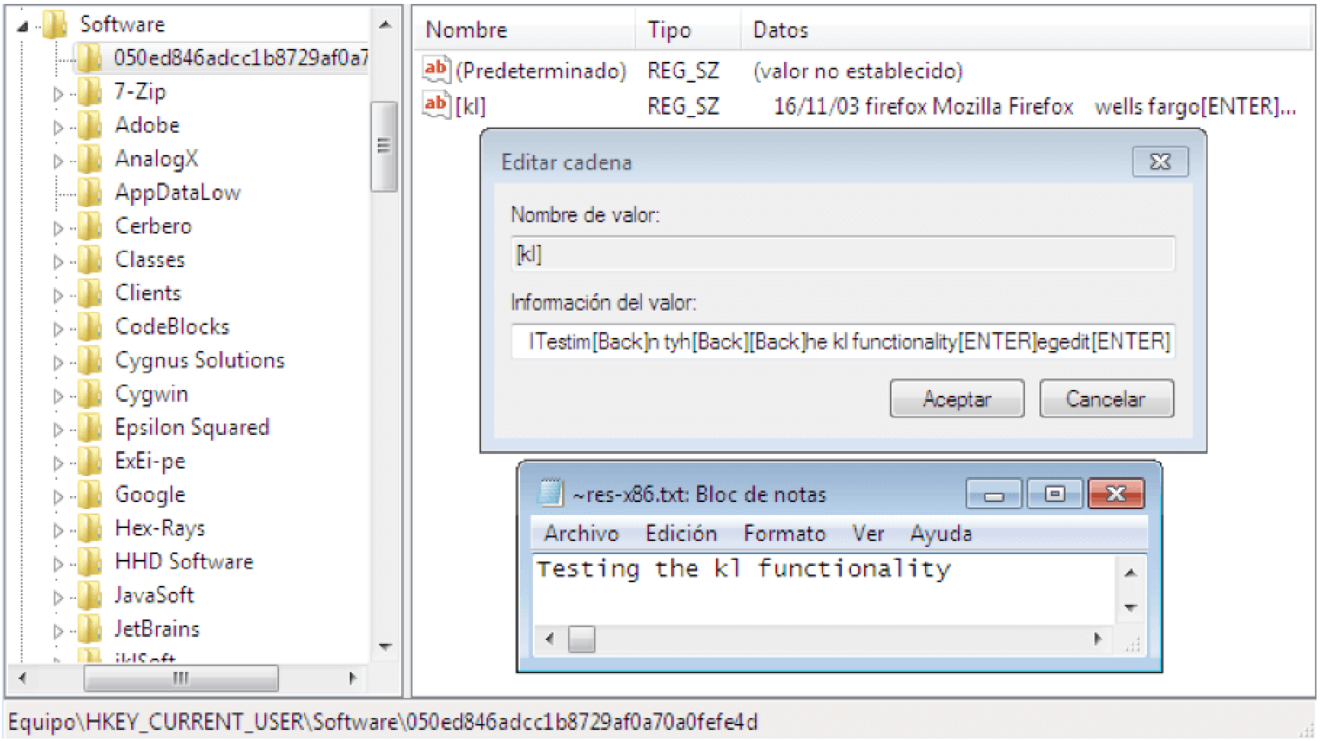


```
Date:          15/09/2016 17:35:26
Thread:        1572
Class:         Process
Operation:     Process Create
Result:        SUCCESS
Path:          C:\Windows\system32\netsh.exe
Duration:      0.0000000

PID:           1216
Command line:  netsh firewall add allowedprogram "C:\Users\malware\AppData\Local\Temp\server.exe" "server.exe" ENABLE
```

Figure 4. Command used by the sample to create a firewall rule

- Copies server.exe in the Startup folder.
- Checks the value of HKCU\Software\050ed846adcc1b8729af0a70a0fefe4d\[kl] because the keylogger stores what it captures in this registry key, to later send to its C&C.



Nombre	Tipo	Datos
(Predeterminado)	REG_SZ	(valor no establecido)
[kl]	REG_SZ	16/11/03 firefox Mozilla Firefox wells fargo[ENTER]...

Nombre de valor:
[kl]

Infomación del valor:
lTestim[Back]n tyh[Back][Back]he kl functionality[ENTER]egedit[ENTER]

```
Testing the kl functionality
```

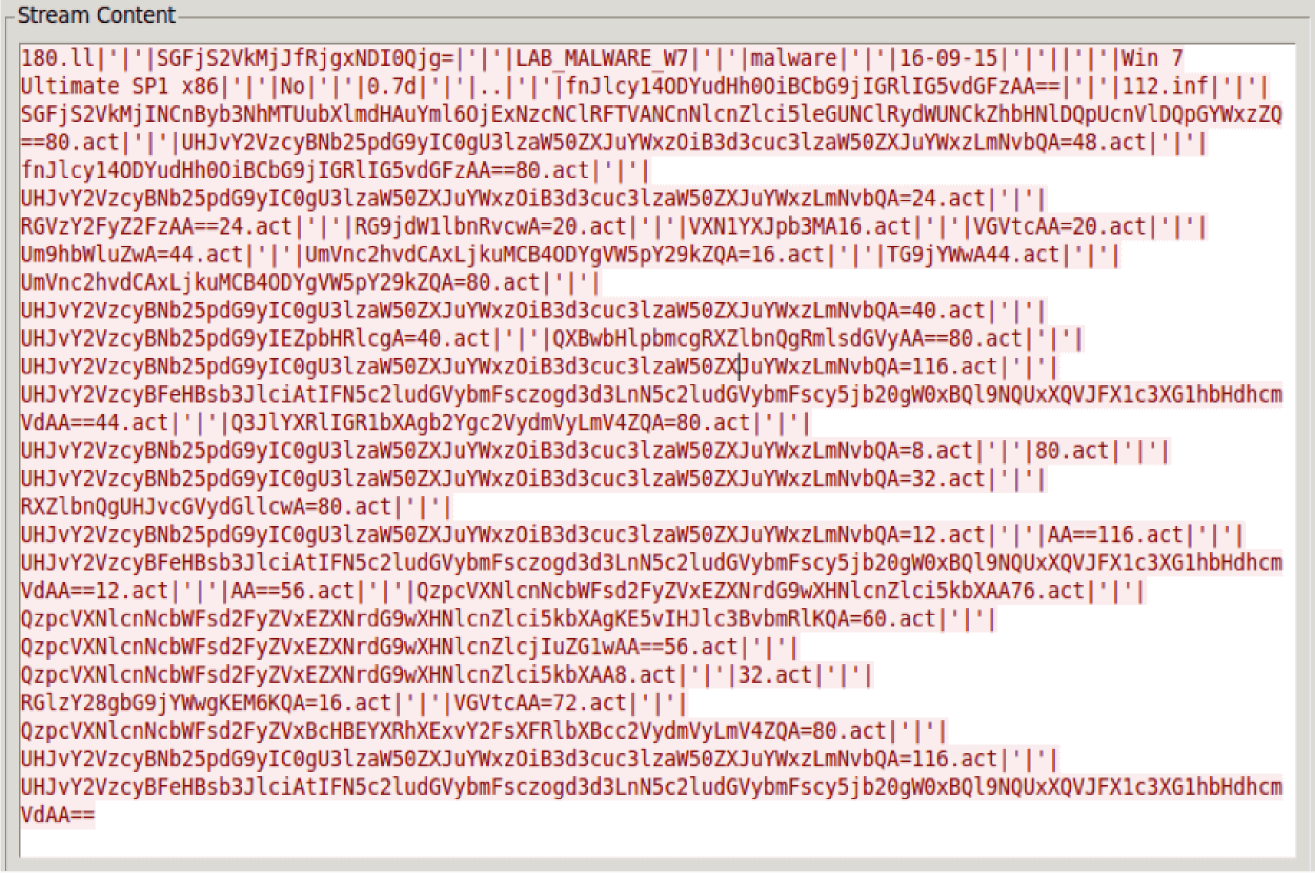
Equipo\HKEY_CURRENT_USER\Software\050ed846adcc1b8729af0a70a0fefe4d

Figure 5. Example of the keylogging functionality

- Uses GetWindowText to copy the text of the active window's title bar to later send to the remote server coded in base64.
- Gets information about the C: drive, particularly the volume serial number.
- When all the necessary information has been collected, the sample generates a string with the data coded in base64, and with this structure:

“ll” + HacKed22_VolumeSerialNumber + ComputerName + Username + LastWriteTimeOfSampleinTemp + OSandServicePack + Architecture + Camera(Yes/No) + 0.7d (PossiblyTheMalwareVersion) + .. + ActiveWindowName + ActiveWindowName…

This stolen information is sent to the malicious URL in hopto.org or myftp.biz domain using port 1177, 5552, or 5112, depending on the sample. The traffic can be detected by Fortinet IPS signature Bladabindi.Botnet.



```
180.ll|'|'|SGFjS2VkMjJfRjgxNDI0Qjg=|'|'|LAB_MALWARE_W7|'|'|malware|'|'|16-09-15|'|'||'|'|Win 7
Ultimate SP1 x86|'|'|No|'|'|0.7d|'|'|..|'|'|fnJlcy14ODYudHh0OiBCbG9jIGRlIG5vdGFzAA==|'|'|112.inf|'|'|
SGFjS2VkMjINCnByb3NhMTUubXlmdHAuYml6OjExNzcNClRFTVANCnNlcnZlci5leGUNClRydWUNCkZhbHNlDQpUcnVlDQpGYWxzZQ
==80.act|'|'|UHJvY2VzcyBNb25pdG9yIC0gU3lzaW50ZXJuYWxzOiB3d3cuc3lzaW50ZXJuYWxzLmNvbQA=48.act|'|'|
fnJlcy14ODYudHh0OiBCbG9jIGRlIG5vdGFzAA==80.act|'|'|
UHJvY2VzcyBNb25pdG9yIC0gU3lzaW50ZXJuYWxzOiB3d3cuc3lzaW50ZXJuYWxzLmNvbQA=24.act|'|'|
RGVzY2FyZ2FzAA==24.act|'|'|RG9jdW1lbnRvcwA=20.act|'|'|VXN1YXJpb3MA16.act|'|'|VGVtcAA=20.act|'|'|
Um9hbWluZwA=44.act|'|'|UmVnc2hvdCAxLjkuMCB4ODYgVW5pY29kZQA=16.act|'|'|TG9jYWwA44.act|'|'|
UmVnc2hvdCAxLjkuMCB4ODYgVW5pY29kZQA=80.act|'|'|
UHJvY2VzcyBNb25pdG9yIC0gU3lzaW50ZXJuYWxzOiB3d3cuc3lzaW50ZXJuYWxzLmNvbQA=40.act|'|'|
UHJvY2VzcyBNb25pdG9yIEZpbHRlcgA=40.act|'|'|QXBwbHlpbmcgRXZlbnQgRmlsdGVyAA==80.act|'|'|
UHJvY2VzcyBNb25pdG9yIC0gU3lzaW50ZXJuYWxzOiB3d3cuc3lzaW50ZXJuYWxzLmNvbQA=116.act|'|'|
UHJvY2VzcyBFeHBsb3JlciAtIFN5c2ludGVybmFsczogd3d3LnN5c2ludGVybmFscy5jb20gW0xBQl9NQUxXQVJFX1c3XG1hbHdhcm
VdAA==44.act|'|'|Q3JlYXRlIGR1bXAgb2Ygc2VydmVyLmV4ZQA=80.act|'|'|
UHJvY2VzcyBNb25pdG9yIC0gU3lzaW50ZXJuYWxzOiB3d3cuc3lzaW50ZXJuYWxzLmNvbQA=8.act|'|'|80.act|'|'|
UHJvY2VzcyBNb25pdG9yIC0gU3lzaW50ZXJuYWxzOiB3d3cuc3lzaW50ZXJuYWxzLmNvbQA=32.act|'|'|
RXZlbnQgUHJvcGVydGllcwA=80.act|'|'|
UHJvY2VzcyBNb25pdG9yIC0gU3lzaW50ZXJuYWxzOiB3d3cuc3lzaW50ZXJuYWxzLmNvbQA=12.act|'|'|AA==116.act|'|'|
UHJvY2VzcyBFeHBsb3JlciAtIFN5c2ludGVybmFsczogd3d3LnN5c2ludGVybmFscy5jb20gW0xBQl9NQUxXQVJFX1c3XG1hbHdhcm
VdAA==12.act|'|'|AA==56.act|'|'|QzpcVXNlcnNcbWFsd2FyZVxEZXNrdG9wXHNlcnZlci5kbXAA76.act|'|'|
QzpcVXNlcnNcbWFsd2FyZVxEZXNrdG9wXHNlcnZlci5kbXAgKE5vIHJlc3BvbmRlKQA=60.act|'|'|
QzpcVXNlcnNcbWFsd2FyZVxEZXNrdG9wXHNlcnZlcjIuZG1wAA==56.act|'|'|
QzpcVXNlcnNcbWFsd2FyZVxEZXNrdG9wXHNlcnZlci5kbXAA8.act|'|'|32.act|'|'|
RGlzY28gbG9jYWwgKEM6KQA=16.act|'|'|VGVtcAA=72.act|'|'|
QzpcVXNlcnNcbWFsd2FyZVxBcHBEYXRhXExvY2FsXFRlbXBcc2VydmVyLmV4ZQA=80.act|'|'|
UHJvY2VzcyBNb25pdG9yIC0gU3lzaW50ZXJuYWxzOiB3d3cuc3lzaW50ZXJuYWxzLmNvbQA=116.act|'|'|
UHJvY2VzcyBFeHBsb3JlciAtIFN5c2ludGVybmFsczogd3d3LnN5c2ludGVybmFscy5jb20gW0xBQl9NQUxXQVJFX1c3XG1hbHdhcm
VdAA==
```

Figure 6. Fragment of the coded data sent to the C&C

Here are some examples of the decoded windows names:

Temp: VGVtcAA=

Roaming: Um9hbWluZwA=

Regshot 1.9.0 x86 Unicode: UmVnc2hvdCAxLjkuMCB4ODYgVW5pY29kZQA=

Local: TG9jYWwA

Process Monitor Filter: UHJvY2VzcyBNb25pdG9yIEZpbHRlcgA=

Applying Event Filter: QXBwbHlpbmcgRXZlbnQgRmlsdGVyAA==

Event Properties: RXZlbnQgUHJvcGVydGllcwA=

Create dump of server.exe: Q3JlYXRlIGR1bXAgb2Ygc2VydmVyLmV4ZQA=

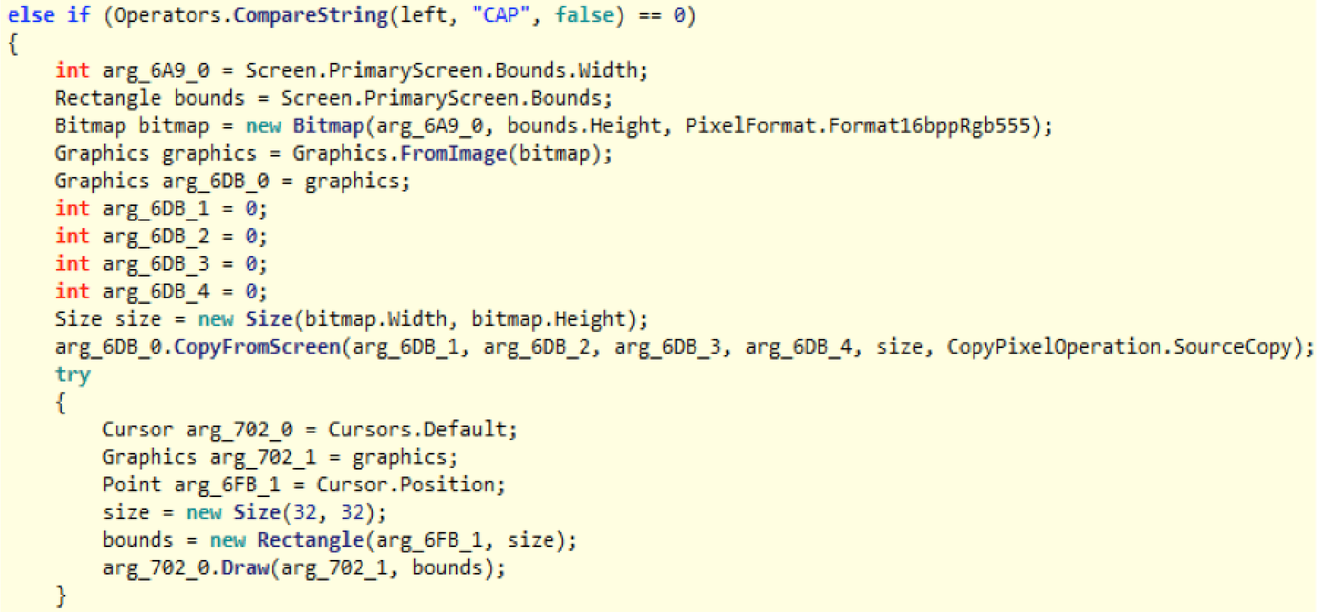
- Uses the function capGetDriverDescriptionA to find out if the infected computer has a webcam installed.
- Deletes the keys and files related to the infection.
- It also includes functions to decompress zip files and obtain MD5 hashes.

- The sample responds to the commands sent from its C&C. The following table explains some of them:

kl	Sends the data collected by the keylogger.
prof + "~"	Adds a value to the subkey HKCU\Software\050ed846adcc1b8729af0a70a0fefe4d\
prof + "!"	Adds a value to the subkey HKCU\Software\050ed846adcc1b8729af0a70a0fefe4d\ Sends data to the C&C.
prof + "@"	Deletes the specified registry key.
rn	Downloads a file and executes it.
ret	Obtains the collected passwords.
CAP	Takes screenshot, saves it as JPEG, and sends it to its C&C.
un + "~"	Deletes the registry keys, the file server.exe in the Startup folder and the firewall rule to allow it.
Un + "!"	Ends current process.
Un + "@"	Ends current process and starts a new one.
Up	Downloads file from a remote server and executes it. Afterwards it deletes the registry keys and the files related to the infection. This command is used for updates.
Ex	Obtains information about the running processes, the services, and the active connections.

CH	Opens a chat window so that the C&C can communicate with the infected computer.

A fragment of the decompiled code for the “CAP” command to take screenshots can be seen below. It basically uses CopyFromScreen to copy the screen’s pixels to the bitmap through a graphic object.

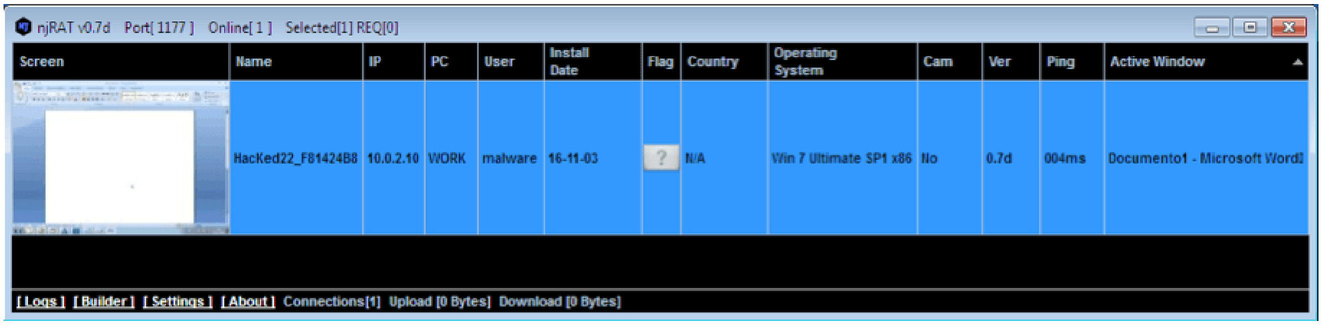


```
else if (Operators.CompareString(left, "CAP", false) == 0)
{
    int arg_6A9_0 = Screen.PrimaryScreen.Bounds.Width;
    Rectangle bounds = Screen.PrimaryScreen.Bounds;
    Bitmap bitmap = new Bitmap(arg_6A9_0, bounds.Height, PixelFormat.Format16bppRgb555);
    Graphics graphics = Graphics.FromImage(bitmap);
    Graphics arg_6DB_0 = graphics;
    int arg_6DB_1 = 0;
    int arg_6DB_2 = 0;
    int arg_6DB_3 = 0;
    int arg_6DB_4 = 0;
    Size size = new Size(bitmap.Width, bitmap.Height);
    arg_6DB_0.CopyFromScreen(arg_6DB_1, arg_6DB_2, arg_6DB_3, arg_6DB_4, size, CopyPixelOperation.SourceCopy);
    try
    {
        Cursor arg_702_0 = Cursors.Default;
        Graphics arg_702_1 = graphics;
        Point arg_6FB_1 = Cursor.Position;
        size = new Size(32, 32);
        bounds = new Rectangle(arg_6FB_1, size);
        arg_702_0.Draw(arg_702_1, bounds);
    }
```

Figure 7. Fragment of code to take screenshots

C&C interface

When active, the domain prosa15.myftp.biz is used by the sample to connect to its C&C through port 1177. To simulate the RAT behavior in a controlled environment, a sample of njRAT was downloaded and installed. Once the sample connected to the C&C, the panel displayed information such as its IP address, its computer name, country, whether a webcam was installed, the active window, and a small screenshot.



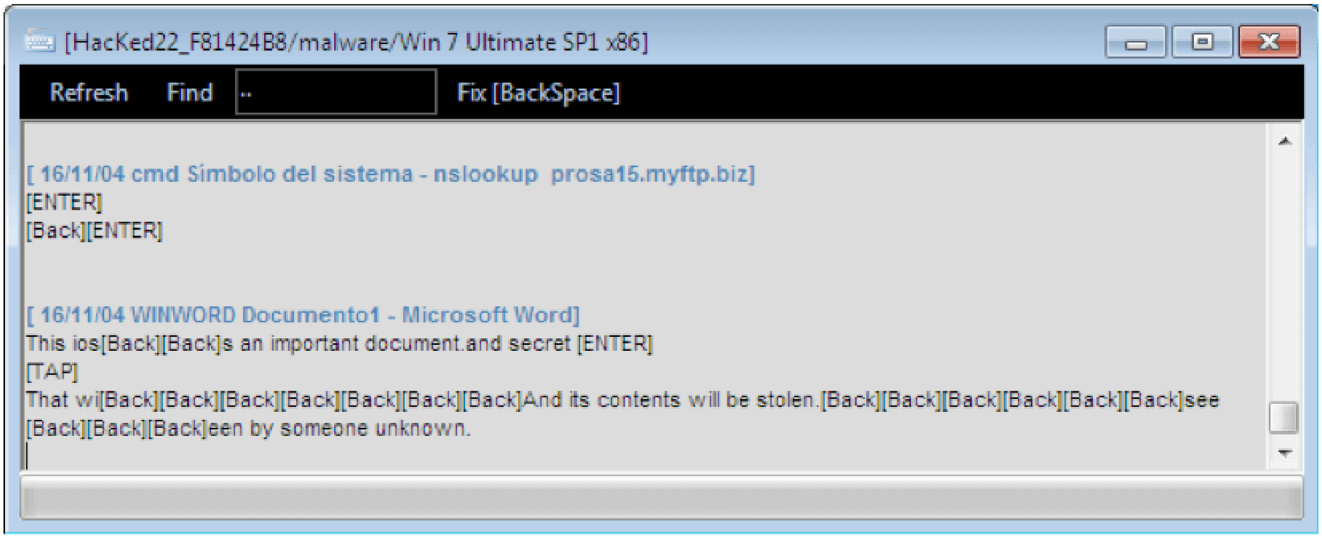
njRAT v0.7d Port[1177] Online[1] Selected[1] REQ[0]

Screen	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window
	HacKed22_F81424B8	10.0.2.10	WORK	malware	16-11-03	?	N/A	Win 7 Ultimate SP1 x86	No	0.7d	004ms	Documento1 - Microsoft Word]

[Logs] [Builder] [Settings] [About] Connections[1] Upload [0 Bytes] Download [0 Bytes]

Figure 8. njRAT’s administration panel

The picture below shows part of the data collected by the keylogger. Not only does it record the pressed keys, but it also specifies the window in which the words were written.

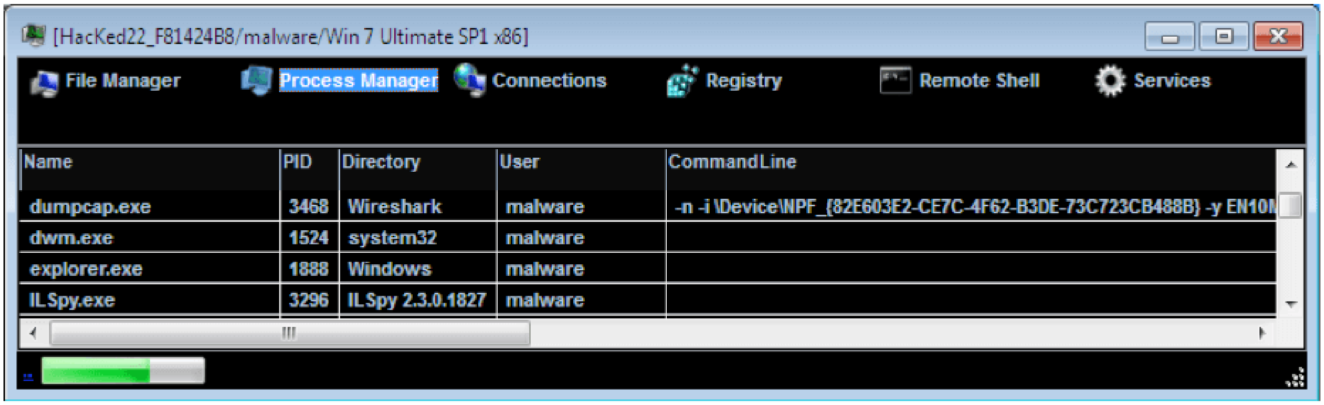


```
[ 16/11/04 cmd Símbolo del sistema - nslookup  prosa15.myftp.biz]
[ENTER]
[Back][ENTER]


[ 16/11/04 WINWORD Documento1 - Microsoft Word]
This ios[Back][Back]s an important document.and secret [ENTER]
[TAP]
That wi[Back][Back][Back][Back][Back][Back][Back]And its contents will be stolen.[Back][Back][Back][Back][Back][Back]see
[Back][Back][Back]een by someone unknown.
```

Figure 9. Keylogger window

As mentioned above, the malware is also capable of collecting active processes, services, and connections, accessing the registry keys, and executing commands with a remote shell.



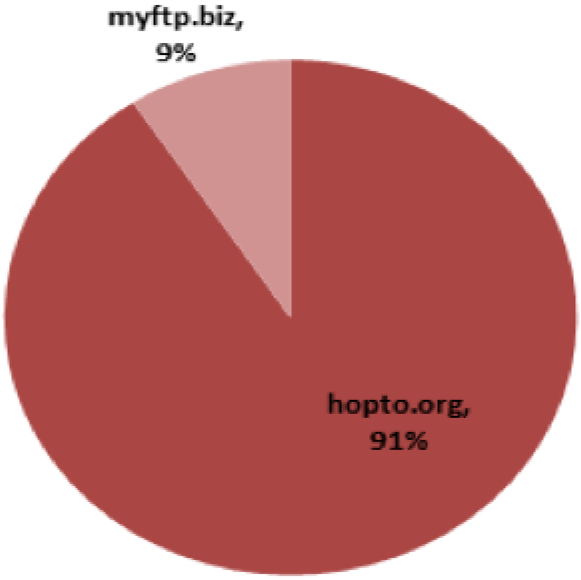
Name	PID	Directory	User	CommandLine
dumpcap.exe	3468	Wireshark	malware	-n -i \Device\NPF_{82E603E2-CE7C-4F62-B3DE-73C723CB488B} -y EN10M
dwm.exe	1524	system32	malware	
explorer.exe	1888	Windows	malware	
ILSpy.exe	3296	ILSpy 2.3.0.1827	malware	

Figure 10. Other capabilities of the RAT

Statistics

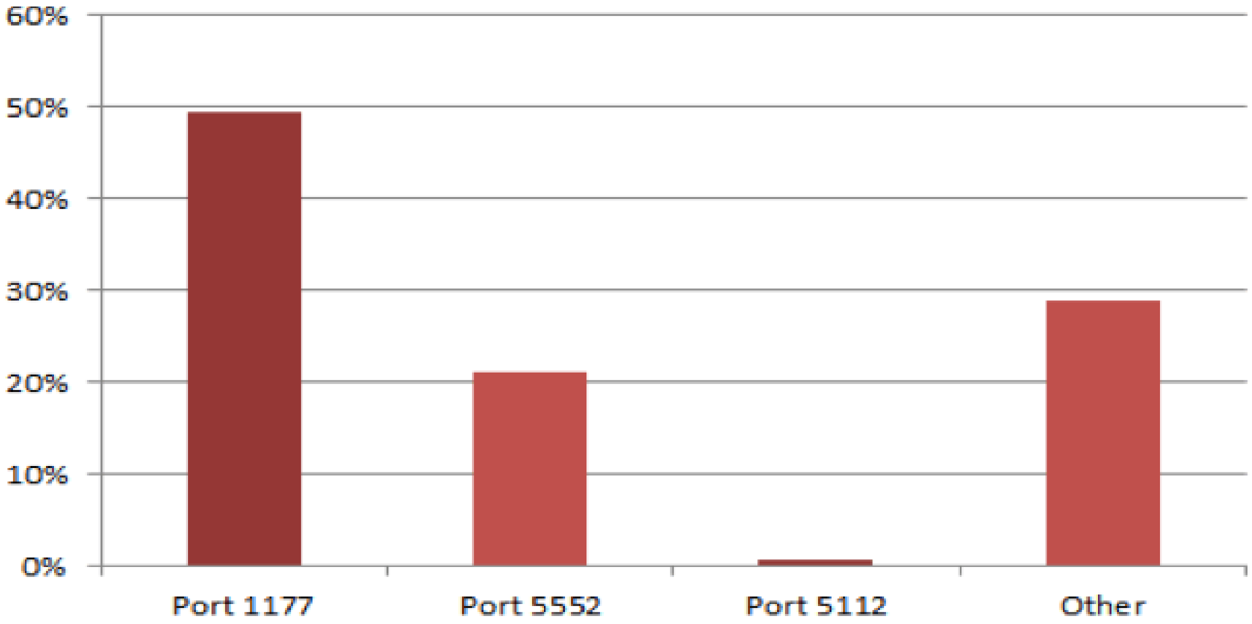
Both hopto.org and myftp.biz domains are available, amongst various other options, from the dynamic DNS provider called No-IP. The use of this service guarantees that an infected PC will be able to maintain communication with its C&C even if it changes the IP address.

From September 12 to November 16, our FortiGuard analysis system collected 194 samples connecting to hopto.org or myftp.biz.

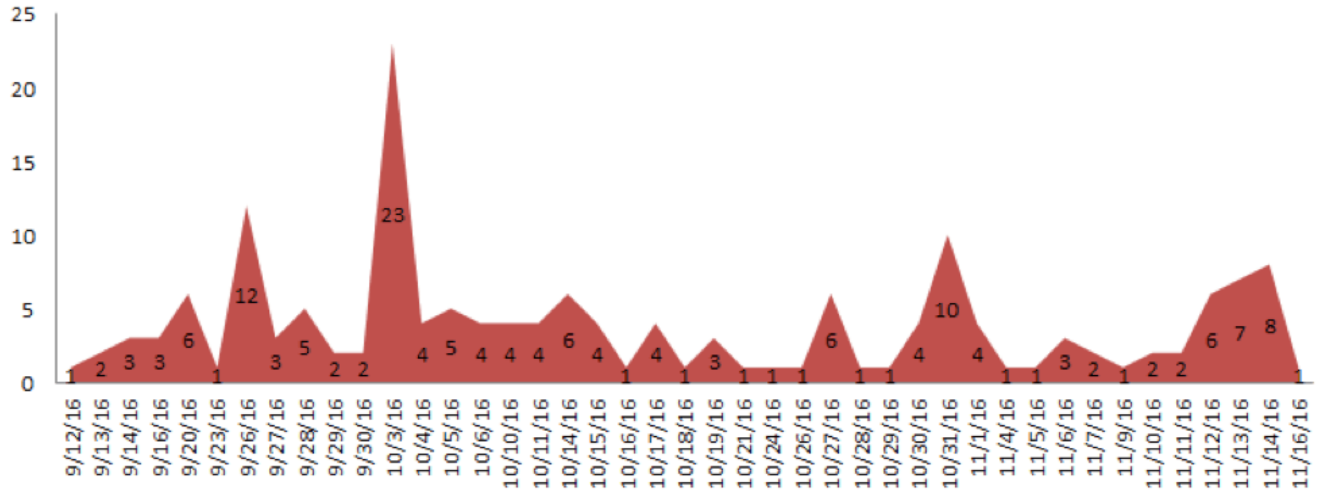


Out of those, 166 were related to Bladabindi samples and the rest to different threats, which indicates that the use of dynamic DNS providers could now be more common amongst malware writers.

Although it is common for this malware family to report to its C&C using port 1177, the information gathered reveals that ports 5552 and 5112 are also now being used.



Finally, the next chart shows the number of samples collected by our FortiGuard analysis system from September 12 to November 16.



Conclusion

The Bladabindi malware family continues to be one of the most popular threats because of how easy it is to download. In fact, there are plenty of videos and websites available that provide detailed tutorials of how to use it. One proof of its ease of use is the fact that many of the collected samples hadn’t been submitted to Virus Total at the time of the analysis. Furthermore, the samples we examined use dynamic DNS services that make it hard to monitor and keep track of the domains and the IP addresses used.

Related Posts

Terms of ServicesPrivacy Policy
| Cookie Settings