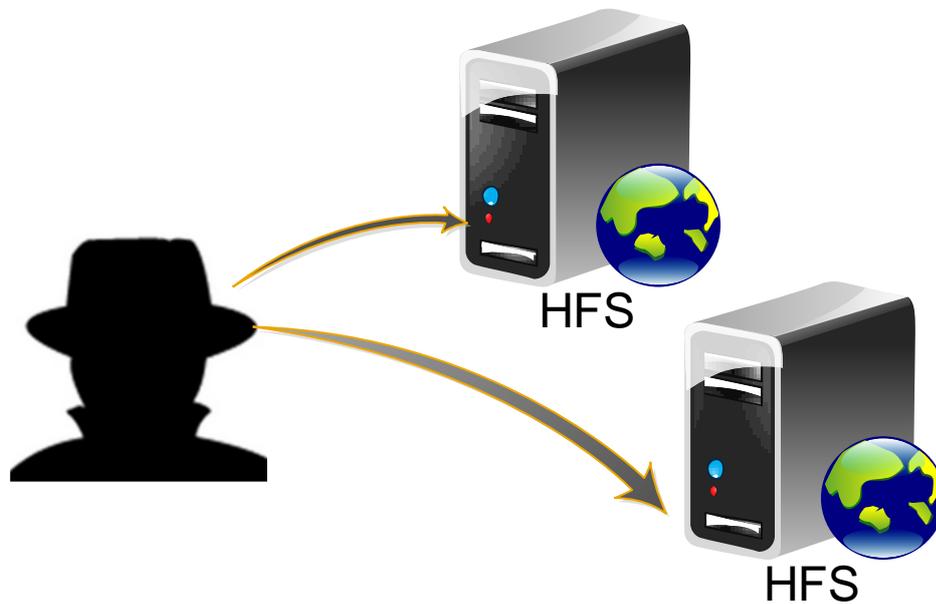




A LARGE NUMBER OF SERVERS BY HFS ARE EXPLOITED TO SPREAD MALWARE

Antiy CERT



First publish time: 17:00, Sep 15, 2015.

Update time: 17:00, Sep 15, 2015.

1 Production

Recently, the third generation HoneyPot Wind-capture System of Antiy captured a downloader sample. After the samples being executed, it will access to an Http File Server built by hackers. Through a tracking and analysis by wind-capture system, analysts found that there are many servers built by HFS. With monitoring one of the downloading servers, the total hits reach to nearly 30 thousand during 6 online days, which can show that it has a wide spread. The extremely simple operation of this software is favored by primary attackers; meanwhile, it has been used by hackers many times because of its convenient construction and easy to spread, etc. Through an associated analysis, Antiy CERT researchers have found that this kind of lightweight server tools has been prevalent currently.

1.1 Sample label

Virus name	Trojan[Downloader]/Win32.Agent
Original file name	non
MD5	A52B473888FA975D37048D5959533001
Processor Architecture	X86-32
File size	180KB(184427Bytes)
File format	BinExecute/Microsoft.EXE[:X86]
Timestamp	2015-08-29
Digital signature	non
Shell type	Unknown shell

Compiled language	Microsoft Visual C++ v6.0
-------------------	---------------------------

Graph 1 Sample label

Hackers use weak passwords to intrude MySQL database server, use MySQL commands to set up tables and new variable, write executable binary codes into the variable and insert into the table, then dump the binary executable file in the table to the database server and execute it finally, which is also commonly used by hackers to intrude database.

After being executed, it will access to its own code dynamically, and then elevate privileges with the main function of enumerating antivirus software Kingsoft guards process name "KSafeTray.exe" . If the process appears, end it.

<pre> je 100024C1 push 0x0 push 0x100192CC call dword ptr ds:[0x100131A8] push 0x0 </pre>	<pre> kill KsafeTray.exe ASCII "taskkill /f /im KSafeTray.exe" kernel32.WinExec </pre>
---------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------

Graph 2 End Kingsoft guards process

Malware connection server (IP: 118.193**.**.1010)

<pre> 53 push eax FF15 04340110 call dword ptr ds:[0x10013404] 8BF8 mov edi, eax 85FF test edi, edi </pre>	<pre> ws2_32.gethostbyname </pre>	<pre> 0 0 LastErr E EFL 00000246 (ST0 empty +UN0 ST1 empty 0.01 ST2 empty -UN0 ST3 empty +UN0 ST4 empty -UN0 </pre>									
<pre> 3404]=71A24FD4 (ws2_32.gethostbyname) </pre>											
HEX 数据	ASCII	<table border="1"> <tr> <td>00125A44</td> <td>1001A514</td> <td>LName = "118.193.1010"</td> </tr> <tr> <td>00125A48</td> <td>00000000</td> <td></td> </tr> <tr> <td>00125A4C</td> <td>7C801D77</td> <td>kerne132.LoadLibraryA</td> </tr> </table>	00125A44	1001A514	LName = "118.193.1010"	00125A48	00000000		00125A4C	7C801D77	kerne132.LoadLibraryA
00125A44	1001A514	LName = "118.193.1010"									
00125A48	00000000										
00125A4C	7C801D77	kerne132.LoadLibraryA									

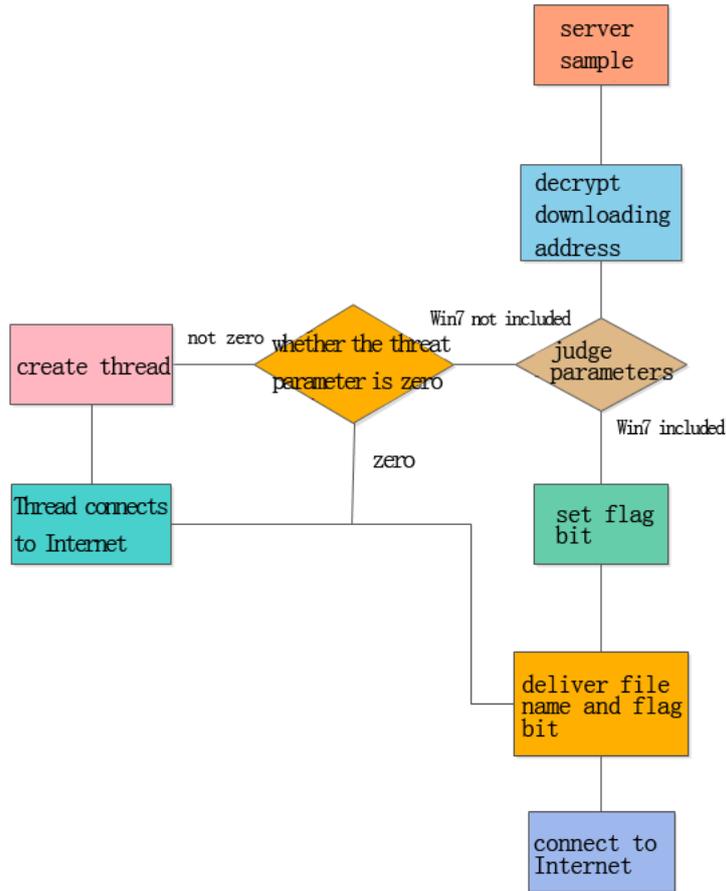
Graph 3 Network connected operation

When malware connects to the server port, the server port will be invalid. Antiy CERT analysts found a lightweight server with a malware (1010. Exe) when connected to the IP.

1.2 Server sample analysis

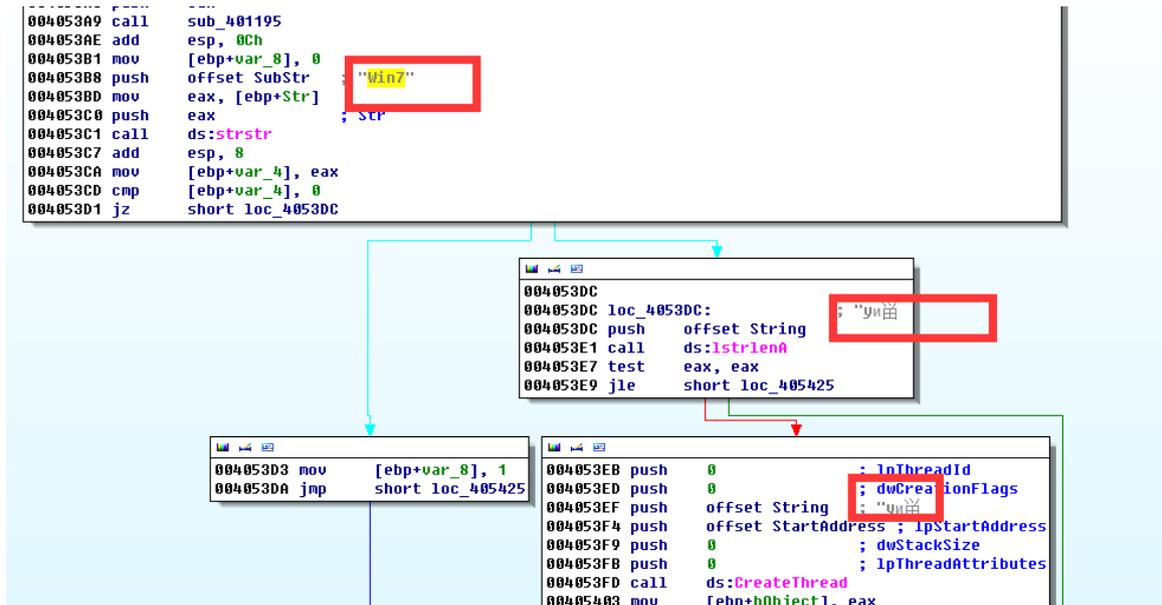
Virus name	Trojan[Downloader]/Win32.Agent
Original file name	1010.exe
MD5	FF5ED4E0F8A968643F49E1FDF1D76338
Processor Architecture	X86-32
File size	80.0 KB (81,988 bytes)
File format	BinExecute/Microsoft.EXE[:X86]
Timestamp	2015-08-29
Digital signature	non
Shell type	non
Compiled language	Microsoft Visual C++ 6.0

Graph 4 Sample label



Graph 5 Server sample flow

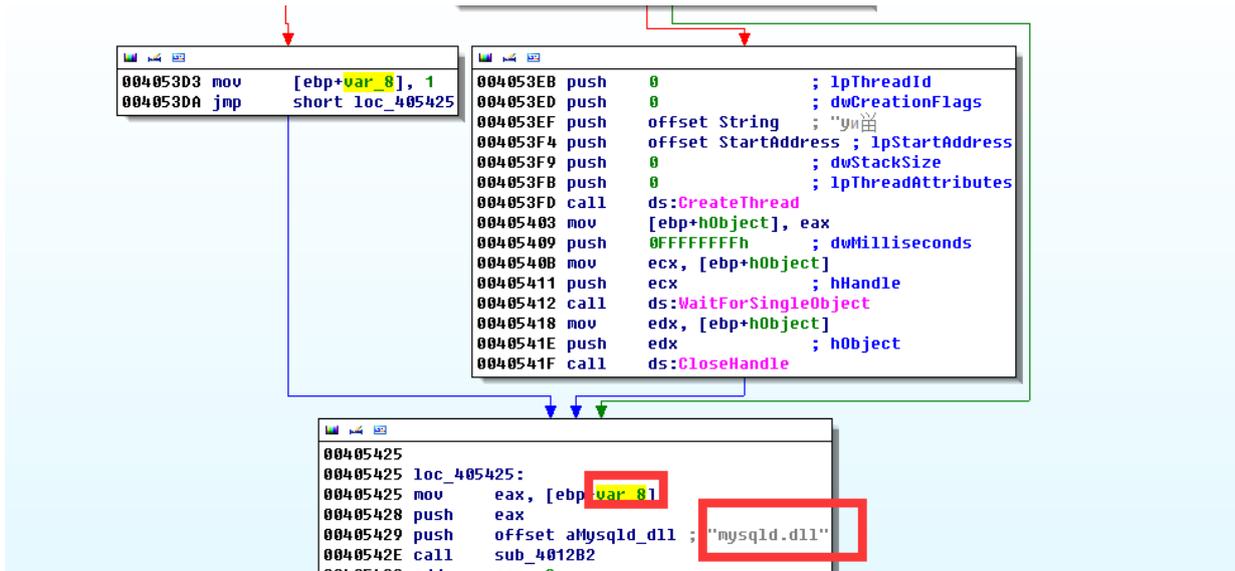
The hacker server is captured by Antiy CERT in less than 2 online hours. The sample will first decrypt the download server address, and then judge whether the sample runs with parameters and whether the parameters include the “Windows 7” string. If it does not include or runs without parameters, it will execute a thread with downloading function, judge if the transferred parameters are empty when executes thread. If not, it will execute thread creation process, as shown in the figure below.



Graph 6 Create thread flow

When malware enters into the thread, it will deliver the parameter string (address of connected server in fact) to the functions that connect to the server. The thread is responsible for downloading other malware.

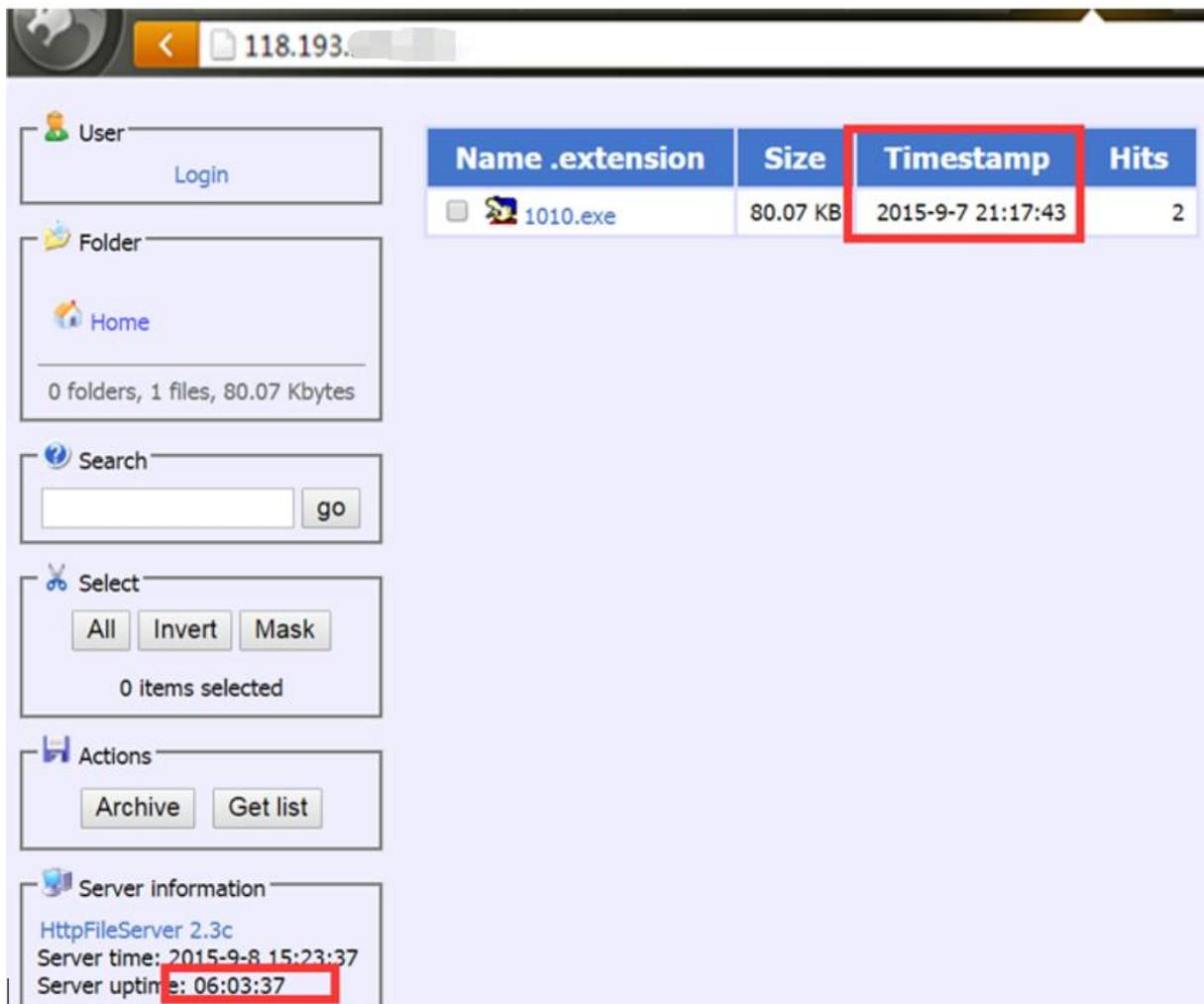
If the malware with parameters and includes “Windows 7” string, it will skip the thread to create process, deliver file name and flag bit server functions, then re-connect to the server address, re-download 1011. exe file and store it in C: \ Windows \ AppPatch directory and names it as “mysqld. dll” to run.



Graph 7 Running process with parameters

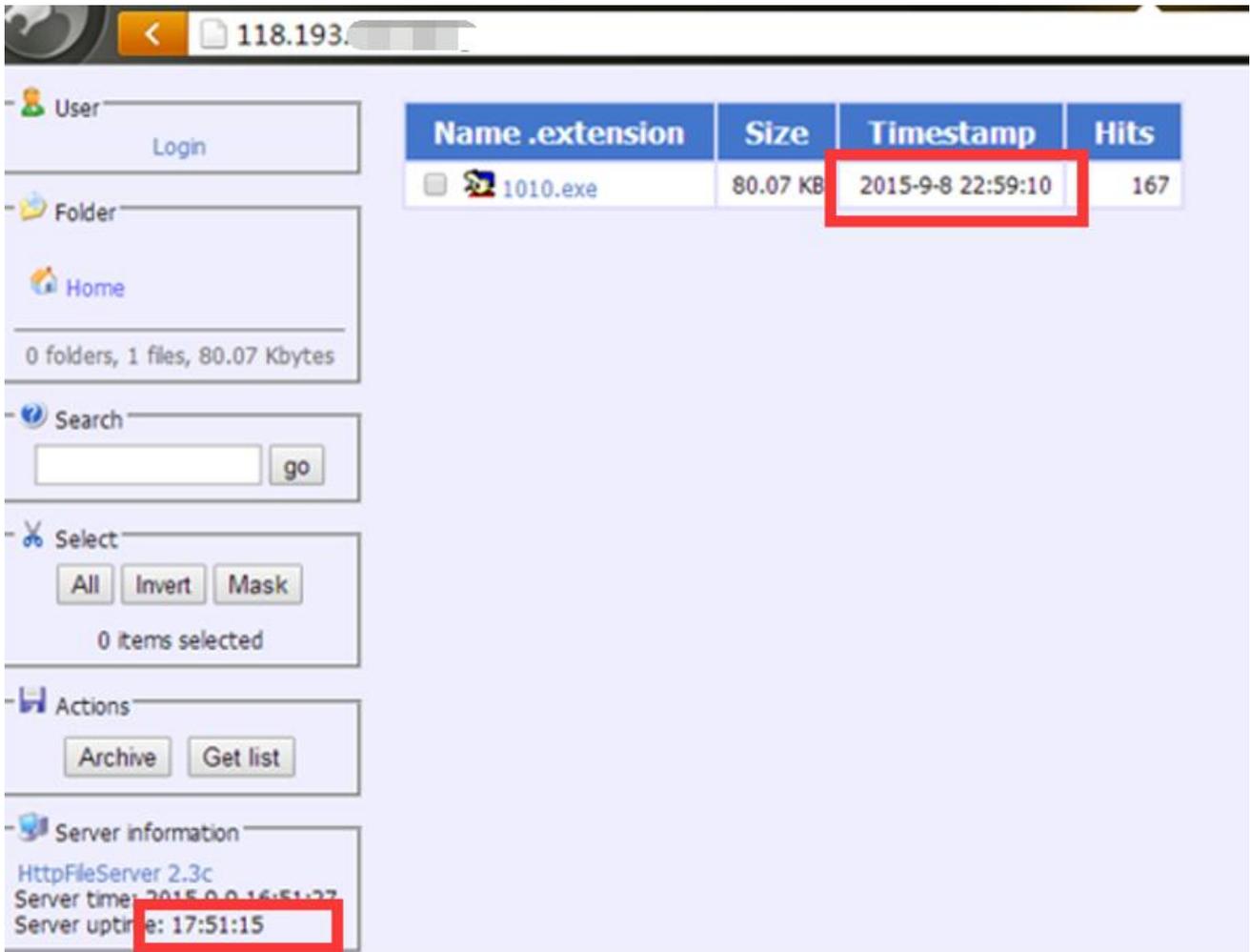
The server has just launched on September 8 with infecting rate increasing gradually, as shown in the figure below:

IP address: 118.193. * * . * * (China Telecom ShaTian international data center, Hong Kong special administrative region)



The screenshot shows a web interface for a file server. On the left, there are several control panels: 'User' with a 'Login' button, 'Folder' with a 'Home' link and a summary '0 folders, 1 files, 80.07 Kbytes', 'Search' with an input field and a 'go' button, 'Select' with 'All', 'Invert', and 'Mask' buttons and '0 items selected', 'Actions' with 'Archive' and 'Get list' buttons, and 'Server information' with 'HttpFileServer 2.3c', 'Server time: 2015-9-8 15:23:37', and 'Server uptime: 06:03:37'. On the right, a table lists files. The 'Timestamp' column for the file '1010.exe' is highlighted with a red box.

Name	.extension	Size	Timestamp	Hits	
<input type="checkbox"/>		1010.exe	80.07 KB	2015-9-7 21:17:43	2

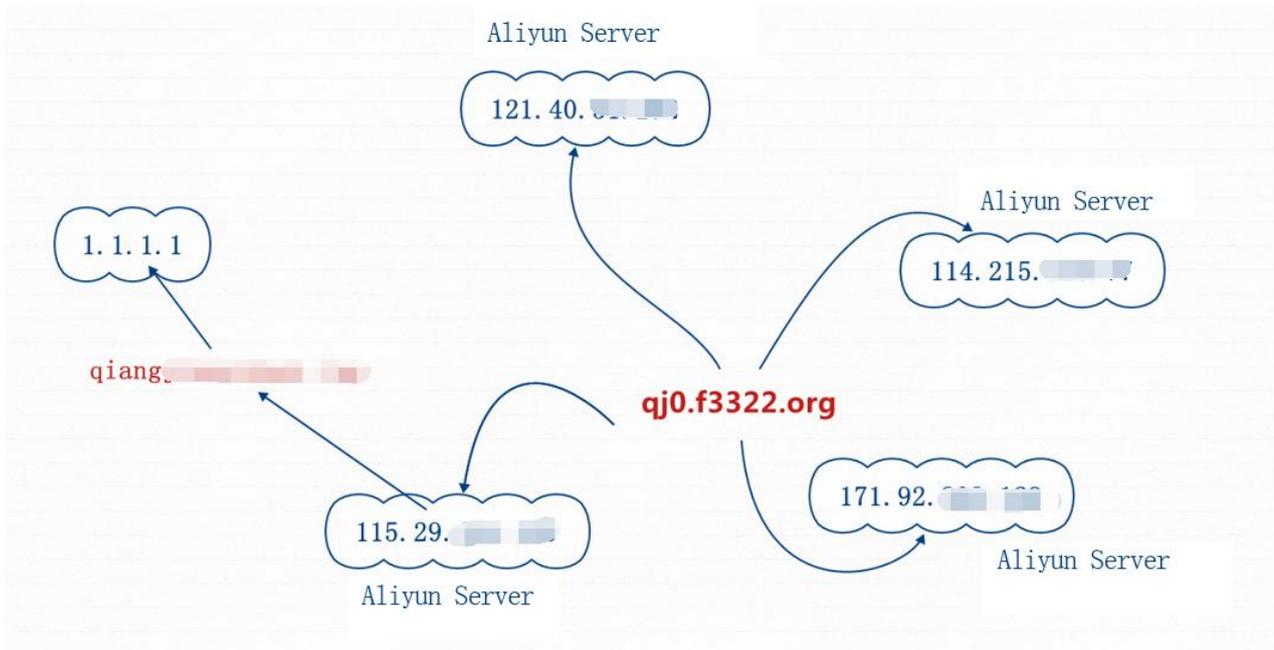


Graph 8 Hits of online server in a day

2 Correlate similar server

Through a further correlation analysis, it can be found that another sample link address is the server built by Http File Server in another Antiy HoneyPot System with the server domain name is qj0. * *. * *. By tracking a few days, they found that the domain names have changed IP four times (as shown in the figure below), and all the servers are provided by Aliyun Server. The combination of dynamic domain name and Aliyun Server make the malicious groups more concealed. Hackers have purchased multiple Aliyun Servers to spread malware, often change IP

and expand malware spreading by binding IP with other domain names with a better hiding at the same time.



Graph 9 Change Aliyun Servers frequently

Name.	extension	Size(type)	Timestamp	Hits
[Latest]	is.war	15.8 KB	2015/8/15 10:27:48	291
	syn20160	1.2 MB	2015/8/18 19:53:40	926
[Latest]	win.exe	450.5 KB	2015/8/18 19:58:16	88
	xxa.exe	28.0 KB	2015/8/28 18:24:56	272
	Zesr68f4.dll	194.5 KB	2015/9/3 0:12:34	573

Graph 10 Hits of malicious servers

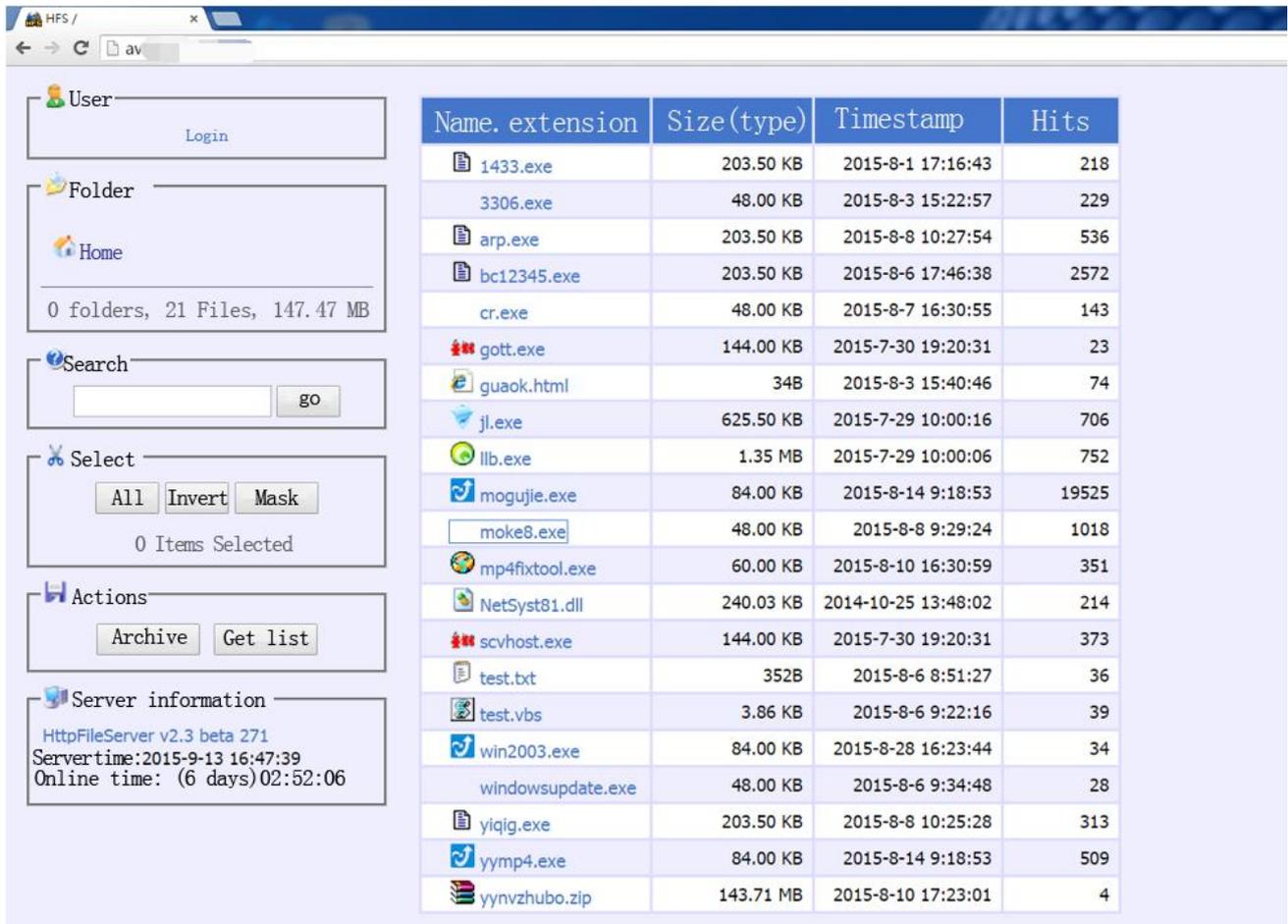
Malicious server regularly updates malware with an increasing infecting rate.

List of malware virus name is as below:

Sample name	Uploading time	Hits	MD5	Virus name
is.war	2015-8-15 10:27:48	291	5F0926A42D2F1042013F45A2B755699E	Trojan[Backdoor]/Java.JSP.I
syn20160	2015-8-18 19:53:40	926	1D3C681B99B98F0D8DDE23758DD98C07	Trojan[Backdoor]/Linux.Ganiw
win.exe	2015-8-18 19:58:16	88	28ACC38A08B44B76EA85A0853961EBC9	Trojan/Win32.Reconyc.esqI
xxa.exe	2015-8-28 18:24:56	272	31ED5DBFF8EFB9D61C68084FC3F20E22	Trojan[Backdoor]/Win32.Farfli
Zesr68f4.dll	2015-9-3 0:12:34	573	8A65DB08D158060F60DF68732FB34D84	Trojan/Win32.Generic

On September 7, Antiy CERT captures another address of similar malware downloading server

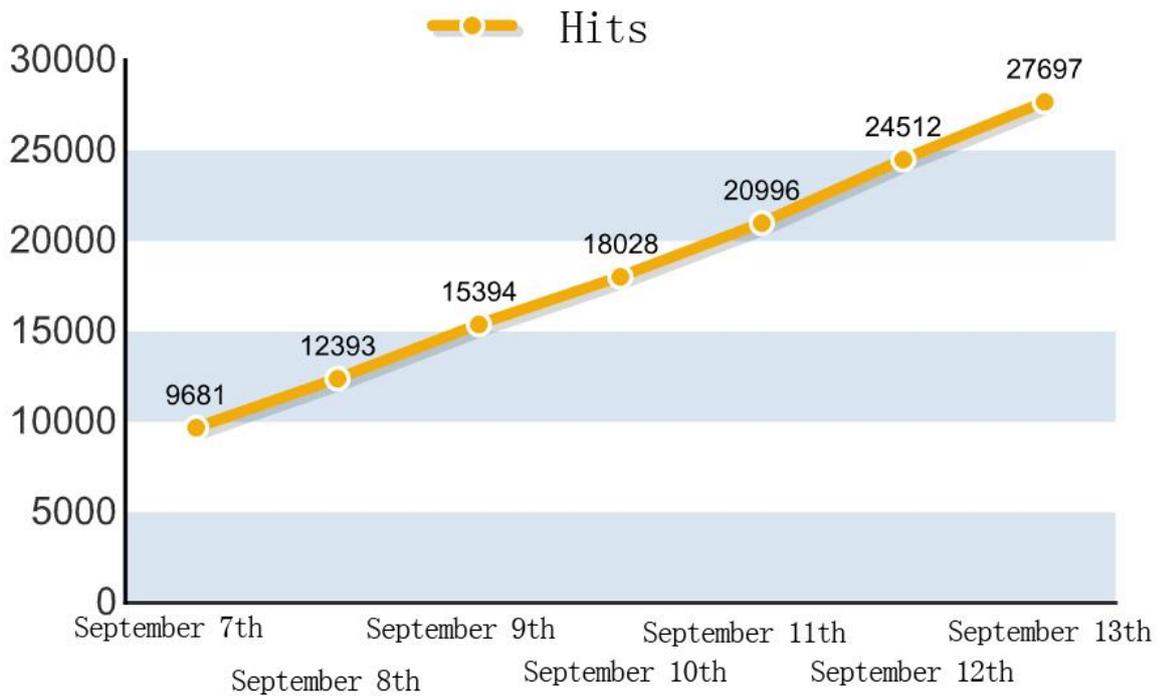
whose hits reach to 10 thousand when being captured. Almost all the software in server is malware most of whom are backdoor and downloaders. Function list of malware is shown as below.



Name.	extension	Size (type)	Timestamp	Hits
1433.exe		203.50 KB	2015-8-1 17:16:43	218
3306.exe		48.00 KB	2015-8-3 15:22:57	229
arp.exe		203.50 KB	2015-8-8 10:27:54	536
bc12345.exe		203.50 KB	2015-8-6 17:46:38	2572
cr.exe		48.00 KB	2015-8-7 16:30:55	143
gott.exe		144.00 KB	2015-7-30 19:20:31	23
guaok.html		34B	2015-8-3 15:40:46	74
jl.exe		625.50 KB	2015-7-29 10:00:16	706
llb.exe		1.35 MB	2015-7-29 10:00:06	752
mogujie.exe		84.00 KB	2015-8-14 9:18:53	19525
moke8.exe		48.00 KB	2015-8-8 9:29:24	1018
mp4fixtool.exe		60.00 KB	2015-8-10 16:30:59	351
NetSyst81.dll		240.03 KB	2014-10-25 13:48:02	214
scvhost.exe		144.00 KB	2015-7-30 19:20:31	373
test.txt		352B	2015-8-6 8:51:27	36
test.vbs		3.86 KB	2015-8-6 9:22:16	39
win2003.exe		84.00 KB	2015-8-28 16:23:44	34
windowsupdate.exe		48.00 KB	2015-8-6 9:34:48	28
yiqiq.exe		203.50 KB	2015-8-8 10:25:28	313
yyp4.exe		84.00 KB	2015-8-14 9:18:53	509
yynvzhuho.zip		143.71 MB	2015-8-10 17:23:01	4

Graph 11 Malicious server

After tracking of this server a week, Antiy CERT analysts found that the total hits increase linearly with an adding of almost 3000 hits per day. As shown in the figure below:



Graph 12 Trend of server hits per day

Statistics of server malware virus name is shown as below:

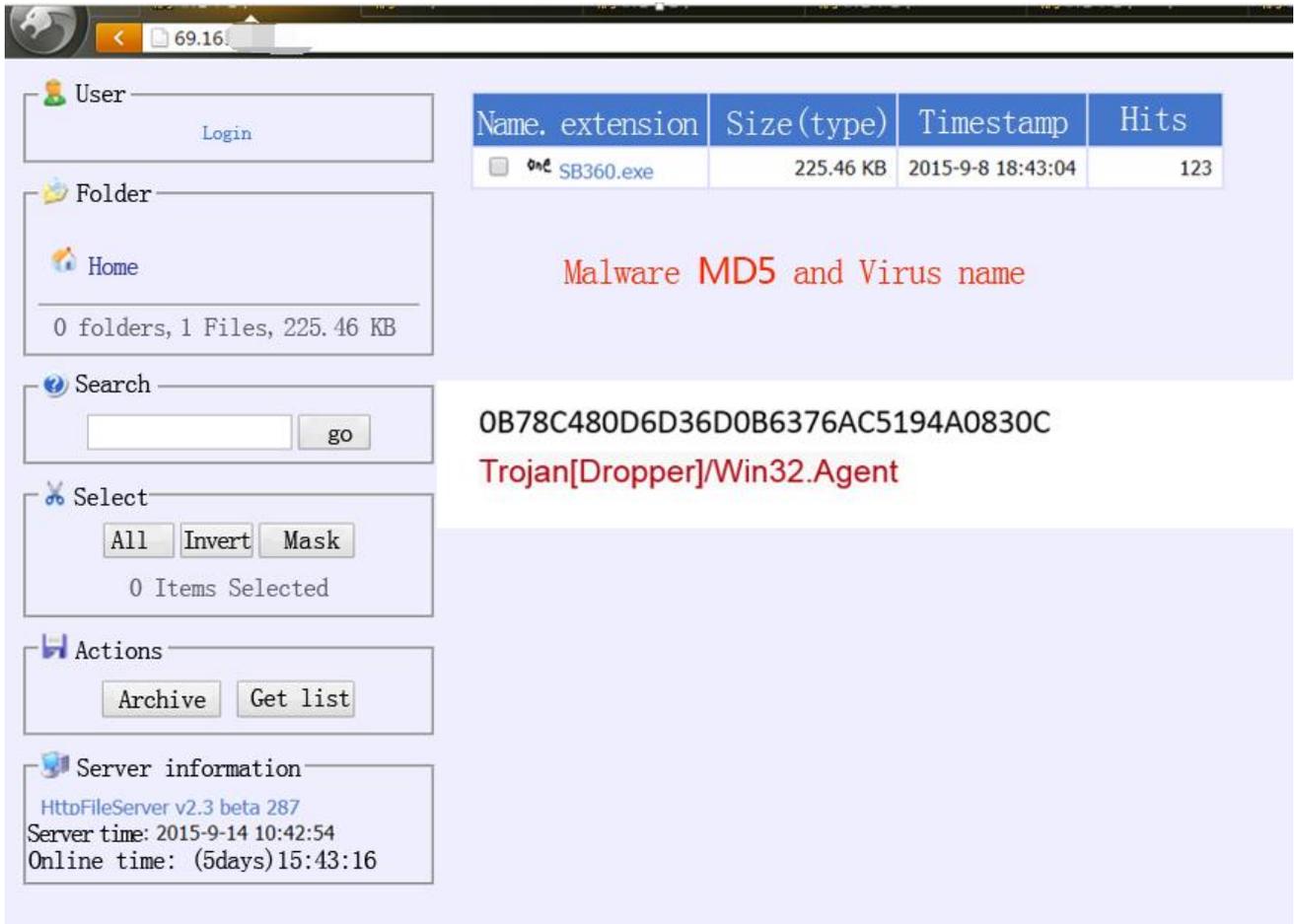
Sample name	Uploading time	Hits	MD5	Virus name
 1433.exe	2015-8-1 17:16:43	218	cc2b9684dc95ea70f052eb8a390 2b0ad	Trojan[Downloader]/Win32.Agent
3306.exe	2015-8-3 15:22:57	229	40d70745cfcdc0574d0a6982362 f1c7d	Trojan[Downloader]/Win32.Agent
 arp.exe	2015-8-8 10:27:54	536	6ff1142bb5b0dc40f1a37dd1cbf5 3e80	Trojan[Downloader]/Win32.Agent
 bc12345.exe	2015-8-6 17:46:38	2572	ab34251ccfcc60005c7b3a29404 0e4cd	Trojan[Downloader]/Win32.Agent
cr.exe	2015-8-7 16:30:55	143	303ff8794e5c6f32870ed55c3357 3e7b	Trojan[Downloader]/Win32.Agent
 gott.exe	2015-7-30 19:20:31	23	c7e9e5566cf3428e25e07868f44f d19c	Trojan[Backdoor]/Win32.Farfli
 mogujie.exe	2015-8-14 9:18:53	1952 5	25c72c1e994f3efec4a1b555d36e f4a4	Trojan[Downloader]/Win32.Agent
moke8.exe	2015-8-8 9:29:24	1018	67b2dbedd5a258258baab0094e 278f96	Trojan[Downloader]/Win32.Agent



A large number of servers by HFS are exploited to spread malware

 mp4fixtool.exe	2015-8-10 16:30:59	351	f005589add550804017349d7a21aa633	Trojan[Downloader]/Win32.Agent
 NetSyst81.dll	2014-10-25 13:48:02	214	0b156ec492ea45d282cf823415ecaf12	Trojan/Win32.Agent
 scvhost.exe	2015-7-30 19:20:31	373	c7e9e5566cf3428e25e07868f44fd19c	Trojan[Backdoor]/Win32.Farfli
 win2003.exe	2015-8-28 16:23:44	34	e8aa9941e88fb172d9a470973834b4c0	Trojan[Downloader]/Win32.Agent
windowsupdate.exe	2015-8-6 9:34:48	28	fc8ee42d829dcc9a12cbe528b6a5f7f4	Trojan[Downloader]/Win32.Agent
 yiqig.exe	2015-8-8 10:25:28	313	f1fbf62e7f04f9e7e223c64e78ff9a99	Trojan[Downloader]/Win32.Agent
 yymp4.exe	2015-8-14 9:18:53	509	25c72c1e994f3efec4a1b555d36ef4a4	Trojan[Downloader]/Win32.Agent

Through a tracking and exploration, Antiy analysts found that this kind of hacker server is very common currently, as shown in the figure below:

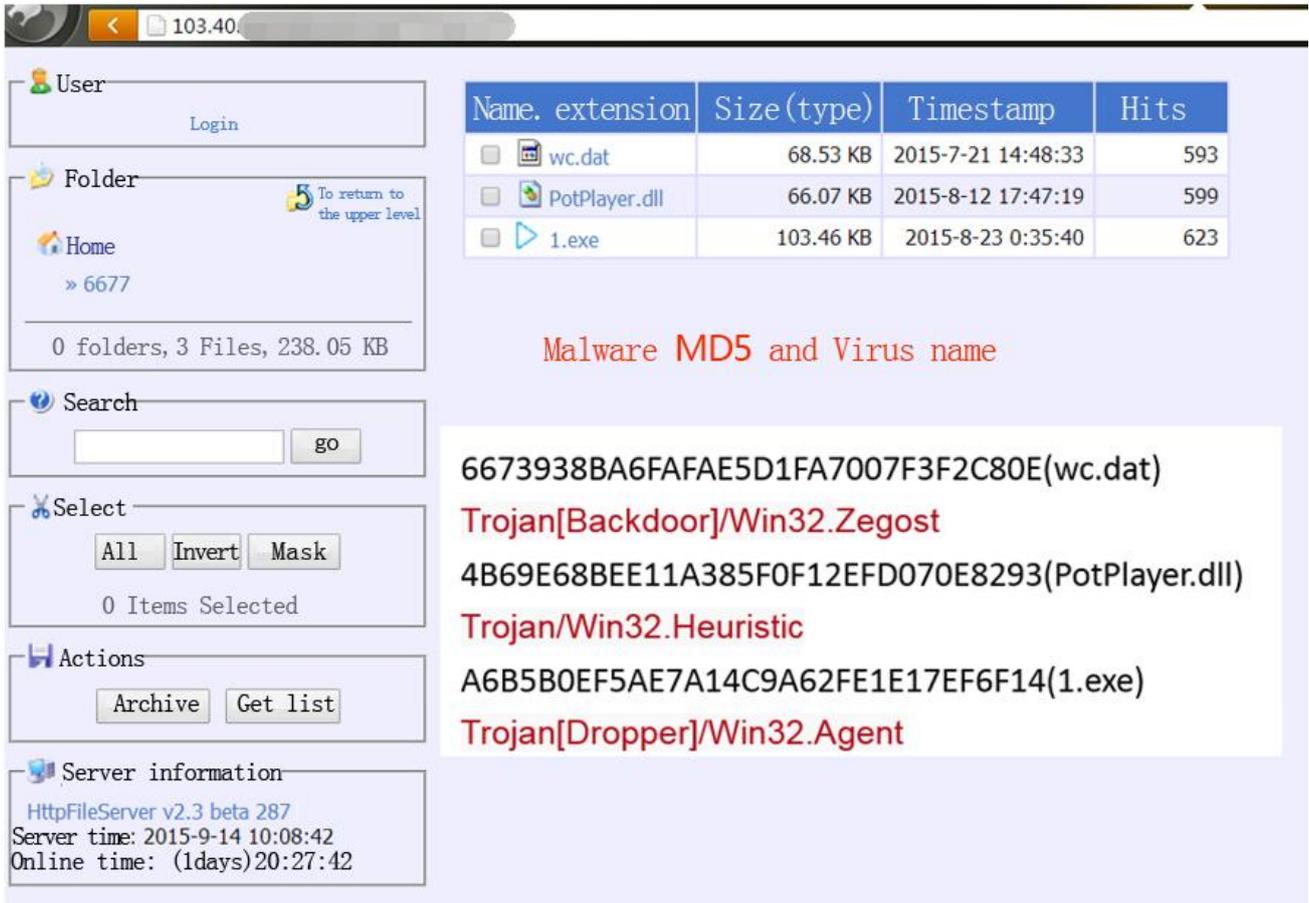


Name. extension	Size (type)	Timestamp	Hits
 SB360.exe	225.46 KB	2015-9-8 18:43:04	123

Malware MD5 and Virus name

0B78C480D6D36D0B6376AC5194A0830C
Trojan[Dropper]/Win32.Agent

Graph 13 Malicious server



The screenshot shows a web interface for a file server. On the left, there are navigation panels for 'User' (with a 'Login' button), 'Folder' (showing 'Home' with a subdirectory '6677'), 'Search' (with an input field and 'go' button), 'Select' (with 'All', 'Invert', and 'Mask' buttons), 'Actions' (with 'Archive' and 'Get list' buttons), and 'Server information' (showing 'HttpFileServer v2.3 beta 287', 'Server time: 2015-9-14 10:08:42', and 'Online time: (1days)20:27:42').

The main area displays a table of files:

Name.	extension	Size (type)	Timestamp	Hits
<input type="checkbox"/>	 wc.dat	68.53 KB	2015-7-21 14:48:33	593
<input type="checkbox"/>	 PotPlayer.dll	66.07 KB	2015-8-12 17:47:19	599
<input type="checkbox"/>	 1.exe	103.46 KB	2015-8-23 0:35:40	623

Below the table, the text 'Malware MD5 and Virus name' is displayed in red. A white box contains the following analysis results:

```

6673938BA6FAFAE5D1FA7007F3F2C80E(wc.dat)
Trojan[Backdoor]/Win32.Zegost
4B69E68BEE11A385F0F12EFD070E8293(PotPlayer.dll)
Trojan/Win32.Heuristic
A6B5B0EF5AE7A14C9A62FE1E17EF6F14(1.exe)
Trojan[Dropper]/Win32.Agent
  
```

Graph 14 Malicious server

3 Summary

At present, with the enormous economic benefit temptation of "Black Industry", commercial hacker toolkit is becoming more and more prevalent. This kind of malware output can make newbies quickly learn the rudiments of malware, even a newbie without any experience can easily master the methods of invasion of computer snooping after a short time study. Not just hacking tools, even an ordinary tool with normal service can also be easily used by hackers, for example, lightweight Http Server (Http File Server) which is favored by users for its convenient construction, easy to operate and other characteristics. Meanwhile, hackers can use the method of combination of building lightweight server in cloud with dynamic DNS to spread malware broader and more



concealed. The increasing use of this kind of lightweight and convenient server tool that is favored by hackers or novice will no doubt accelerate the spread of malware.

This kind of hacking tool techniques can make the production cycle of malware shorter. Relying on commercial tools to attack can reduce the attack cost and improve the testing difficulty and propagation velocity at the same time. This attack technique with less difficulty, low threshold and less cost will make the black industry chain of Internet become a mess and brings more challenges to Internet security.

4 Appendix 1: About Antiy

Starting from antivirus engine research and development team, Antiy now has developed into an advanced security product supplier with four research and development centers, nationwide detection and monitoring ability as well as products and services covering multiple countries. With a fifteen-year continual accumulation, Antiy has formed massive security knowledge and promoted advanced products and solutions against APT with integrated application of network detection, host defense, unknown threat identification, data analysis and security visual experiences. With the recognition of technical capacity by industry regulators, customers and partners, Antiy has consecutively awarded qualification of national security emergency support unit four times and one of the six of CNNVD first-level support units. Antiy detection engine for mobile is the first Chinese product that obtained the first AV - TEST (2013) annual awards and more than ten of the world' s famous security vendors choose Antiy as their detection partner.



A large number of servers by HFS are exploited to spread malware

More information about antivirus engine: <http://www.Antiy.com> (Chinese)

<http://www.Antiy.net> (English)

More information about anti-APT

products: <http://www.Antiy.cn>