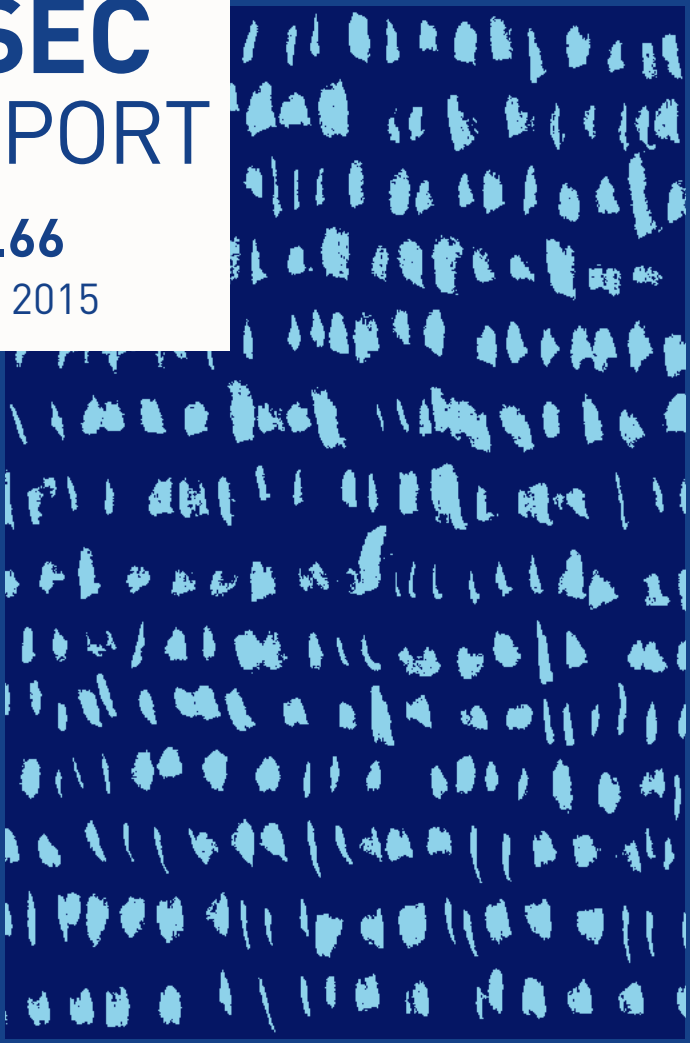
Security Trend

ASEC REPORT

VOL.66

June, 2015



AhnLab

ASEC REPORT

VOL.66 June, 2015

ASEC (AhnLab Security Emergency Response Center) is a global security response group consisting of virus analysts and security experts. This monthly report is published by ASEC and focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.'s homepage (www.ahnlab.com).

SECURITY TREND OF June 2015

Table of Contents

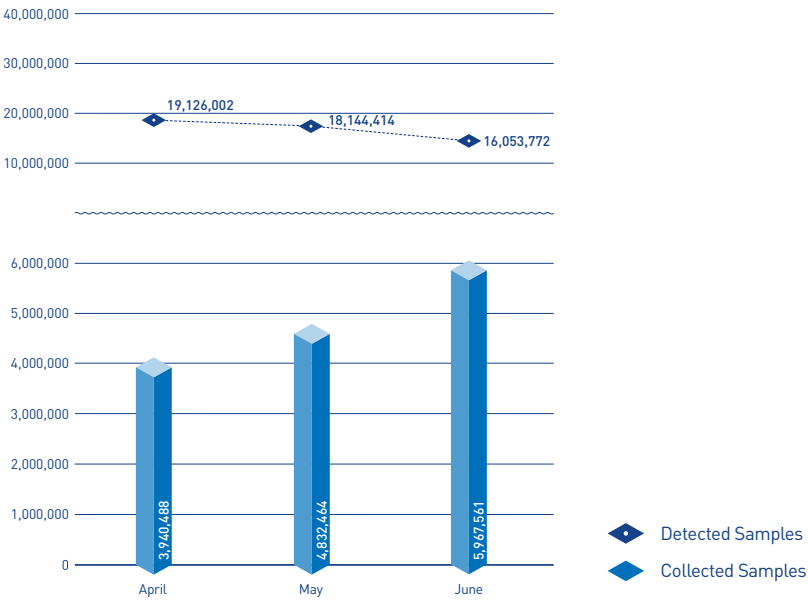
1

SECURITY STATISTICS

SECURITY STATISTICS

01
Malware Statistics

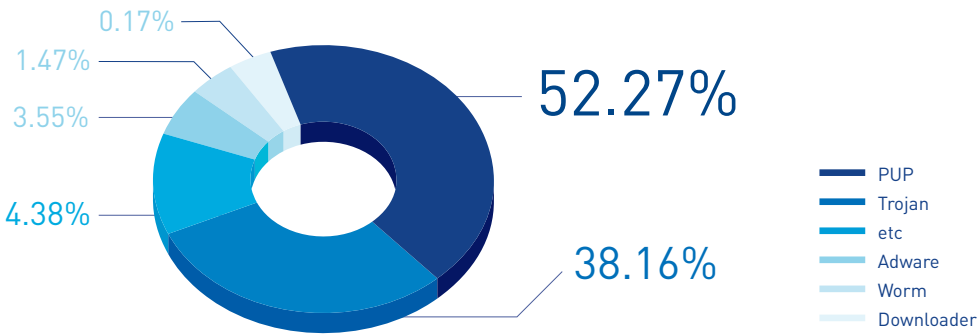
According to the ASEC (AhnLab Security Emergency Response Center), 16,053,772 malware were detected in June 2015. The number of detected malware decreased by 2,090,642 from 18,144,414 detected in the previous month as shown in Figure 1-1. A total of 5,967,561 malware samples were collected in June.



[Figure 1-1] Malware Trend

* "Detected Samples" refers to the number of malware detected by AhnLab products deployed by our customers.
* "Collected Samples" refers to the number of malware samples collected autonomously by AhnLab that were besides our products.

Figure 1-2 shows the prolific types of malware in June 2015. It appears that PUP (Potentially Unwanted Program) was the most distributed malware with 52.27% of the total. It was followed by Trojan (38.16%) and Adware (3.55%).



[Figure 1-2] Proportion of Malware Type in June 2015

Table 1-1 shows the Top 10 malware threats in June categorized by alias. PUP/Win32.BrowseFox was the most frequently detected malware (2,247,767), followed by PUP/Win32.MicroLab (1,637,087).

[Table 1-1] Top 10 Malware Threats in June 2015 (by Alias)

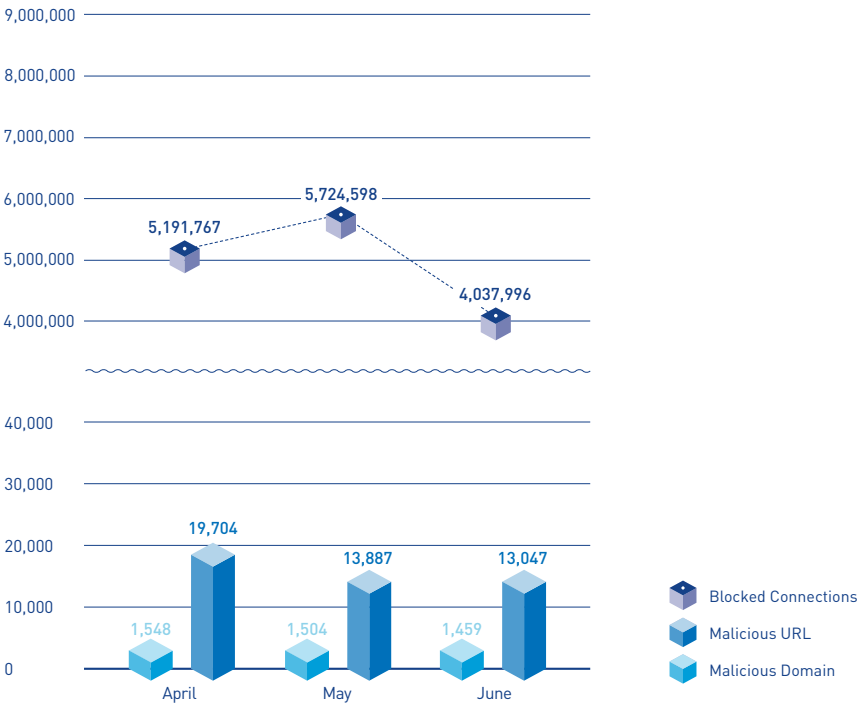
Rank	Alias from AhnLab	No. of detections
1	PUP/Win32.BrowseFox	2,247,767
2	PUP/Win32.MicroLab	1,637,087
3	PUP/Win32.Helper	566,168
4	PUP/Win32.Enumerate	469,069
5	PUP/Win32.SearchProtect	464,081
6	PUP/Win32.MyWebSearch	423,805
7	PUP/Win32.Generic	317,718
8	PUP/Win32.CloverPlus	316,134
9	PUP/Win32.CrossRider	313,411
10	PUP/Win32.IntClient	294,997

SECURITY STATISTICS

02

Web Security Statistics

In June 2015, a total of 1,459 domains and 13,047 URLs were comprised and used to distribute malware. In addition, 4,037,996 malicious domains and URLs were blocked.



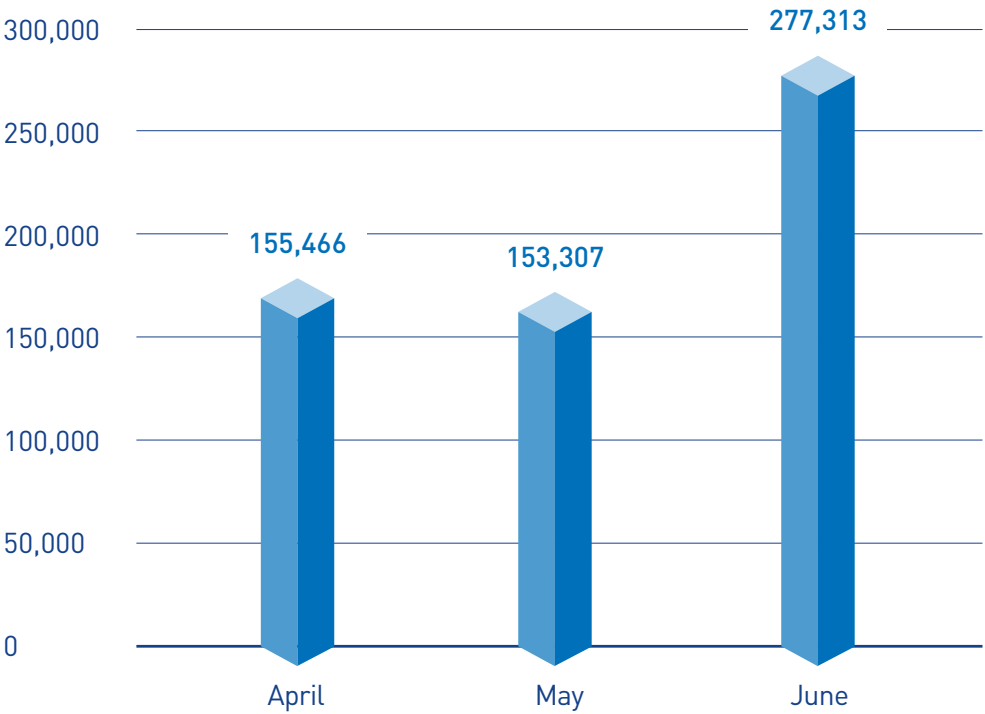
[Figure 1-3] Blocked Malicious Domains/URLs in June 2015

* "Blocked Connections" refers to the number of blocked connections from PCs and other systems to the malicious website by AhnLab products deployed by our customers.

SECURITY STATISTICS

03 Mobile Malware Statistics

In June 2015, 277,313 mobile malware were detected as shown in Figure 1-4.



[Figure 1-4] Mobile Malware Trend

Table 1-2 shows the top 10 mobile malware detected in June 2015. Android-PUP/SMSReg was the most distributed malware with 127,710 of the total, following the previous month.

[Table 1-2] Top 10 Mobile Malware Threats in June (by alias)

Rank	Alias from AhnLab	No. of detections
1	Android-PUP/SmsReg	127,710
2	Android-PUP/Zdpay	17,427
3	Android-Trojan/Opfake	15,558
4	Android-Trojan/AutoSMS	14,364
5	Android-PUP/Noico	11,804
6	Android-Trojan/FakeInst	9,422
7	Android-PUP/Mulad	9,400
8	Android-PUP/SmsPay	7,386
9	Android-Trojan/SmsSpy	5,452
10	Android-PUP/Airpush	5,272

2

SECURITY ISSUE

Fileless Malware? The Malware Hidden in the Registry

SECURITY ISSUE

Fileless Malware? The Malware Hidden in the Registry

Extreme care is again being urged of users as a malware has once again begun to rampage across systems that executes after concealing itself in a registry and doesn't remain as a file.

The Poweliks malware became an issue last year and has been known to have infected approximately 200,000 computers around the world during the first half of this year alone. Poweliks' method of executing malicious behaviors on Windows systems doesn't differ greatly from other malware, but the difference is that it doesn't appear to exist as a file on the system.

After it is executed, Poweliks downloads a Windows Update that is related to a PowerShell that contains the malicious behavior.

Figure 2-1 | Installation of Windows PowerShell

Then, the malware adds the registry key value to the path as below Figure 2-2. Generally, to ensure that a malware executes once the system starts, this path is the one that registers its own file path value. However, the point to note here is the key value that has been registered in the registry.

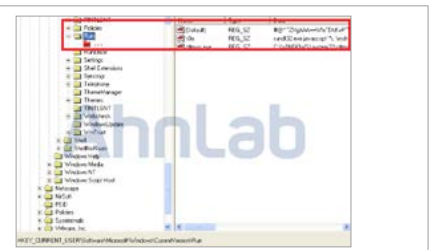


Figure 2-2 | Registry Key Value Registered by Malware

Generally, malware erases its original file, and then copies itself into a path that escapes the user's notice and registers this in the registry as in the following example:

```
* Example of general malicious code's self-replication path

C:\Windows\System32
C:\Documents and Settings\[UserID]\Local Settings\Temp
```

However, the Poweliks malware as seen in Figure 2-3 uses the normal processes of rundll.exe and mshtml.dll and reads the contents of the specific key value.

Figure 2-3 | Specific key value that summons and uses normal process

After Poweliks decrypts the encrypted key value of the path "HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\(Default)", it loads the DLL file into the system memory through PowerShell that the user previously installed without recognition. It then comes not to remain an actual file in the system.

This malware executes only in the system's memory and poses the threat of stealing system information and executing received commands from a C&C server. However, at the time of analysis, it did not connect with the relevant C&C server address.

Figure 2-4 | C&C IP

Also, in order to protect its registry key, Poweliks used a Unicode at the time of registeration. Because the Registry Editor Regedit.exe cannot read the Non-ASCII character, an Error Opening (Open Error) message occurs when the user accesses the registry.

In order for malware to avoid detection by security solutions as much as possible, attackers continuously attempt wide variety of attack methods. This is only the beginning for Poweliks, which is called a "fileless malware."

On the other hand, the corresponding aliases from V3, AhnLab anti-virus products, are as below:

< Alias from V3 Products >

Trojan/Win32.Caphaw (2014.08.04.02)

Trojan/Win32.Poweliks (2014.08.05.00)

3

IN-DEPTH ANALYSIS

Dyre: The Most Notorious Banking Malware Ever

SECURITY ISSUE

Dyre: The Most Notorious Banking Malware Ever

Last year, a malware known as Dyre was discovered in over 1,000 banks and management systems around the world. Early in 2015, the Dyre malware was discovered to have included domestic Korean banks among its targets. Dyre is a malware that is downloaded by Upatre malware. Now it targets the entire world's online banking system in an attempt to steal internet banking information.

When a user connects to a bank site that is included on a targeted bank URL list from a computer infected with the Dyre malware, the malware is executed and malicious behavior ensues, such as the seizure of bank account information or keylogging. Dyre malware's malicious behaviors are as follows:

- Connects C&C server with I2P
- Shuts down the system
- Steals browser information
- Steals banking information
- Keylogging
- Steals user information
- Backdoor and other malicious functions that use TV and VNC modules.

Let's look more closely at its method of attacking and the main functions of the Dyre malware, which threatens the entire world banking system. Dyre is a file that has been downloaded by Upatre, it consists of an Injector and injected DLLs (system process, browser, etc.) as in Figure 3-1.

1. Injector

Fig. 3-1 shows the operational process of the Dyre malware. When Dyre is first executed, it decrypts the PE file in the resource section and replaces the memory's section image. After this, it decrypts the PE file again in the resource section and injects the decrypted PE file into the currently running system process.

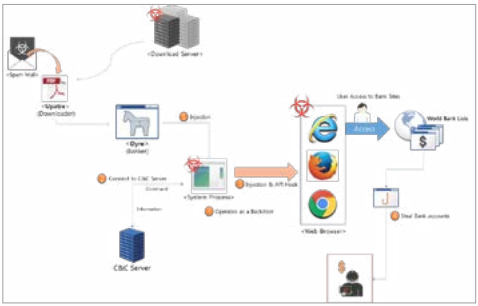


Figure 3-1 | Dyre Malware Operational Process

The PE file that has been injected into the system process operates as a thread and attempts to connect to a C&C server. Through the C&C server, it then receives commands and performs its malicious function, and in particular, attempts to patch the browser code to seize online banking information.

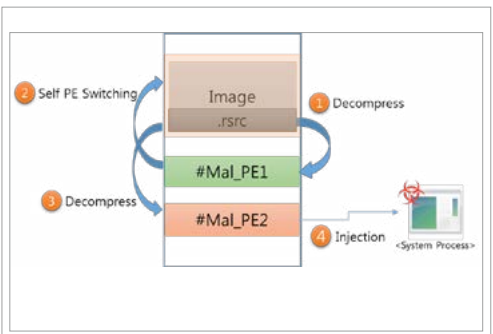


Figure 3-2 | Decryption Routine

To bypass Virtual Machine (henceforth, "VM")-based detection, the Dyre malware confirms the following content.

<Anti-VM routine>
- Checks number of processors
- Checks power status of system

1.1. Dyre's main function

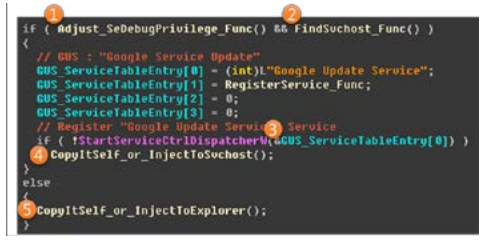


Figure 3-3 | Dyre Main Function

Dyre's main function performs the following operations:

① Enables privilege after confirming that the current process authority is SeDebugPrivilege.

② Finds svchost.exe from among the list of processes and confirms that the file has system privileges.

③ Registers the malware as "Google Update Service."

④ a. When the process is running in C:\Windows path: injects into Svchost.exe

b. When the process is running outside C:\Windows path: it copies itself and runs in C:\Windows

⑤ a. When the process is running in C:\Windows path: injects into Explorer.exe

b. When the process is running outside C:\Windows path: it copies itself and runs in C:\Windows

1.2. Injected Dll - System process

Table 3-1 | Command and Functions

Command	Function
AUTOKILLOS	Shuts down the computer
AUTOBACKCONN	Commands execution of Backconn, vnc32, tv32
I2P_EVENT	Performs I2P-related functions
I2P_NODESTAT	Performs I2P-related functions
malware	Unknown
wg32	requests module wg32
m_i2p32	Attempts to communicate with I2P (Not applied to Vista system)
backconn	Performs backdoor-related functions
vnc32	Requests VNC module
tv32	Requests TV module
bcsrv	Unknown
browsnapshot	Collects data such as browser cookie authentication, etc.
btid	Acquires Bot Id
ccsr	Acquires C&C server address
dpsr	Retrieves data through POST Method
btnt	Unknown
slip	Receives C&C IP list
netDB	Unknown
httprex, httprdc, respparser	Receives set data
bccfg(backconn)	Receives backdoor set data
spk	Transmits status information

2. System Process - Injected Dll

2.1. Main Function

The main function of the Injected Dll system process performs the following operations:

① Checks and Creates Mutex

It creates a unique Mutex as seen below and confirms that the malware is operating.

```
MutexName = "Global₩zx5fwtw4ep"
InitialOwner = TRUE
pSecurity = test9600.10014678
CreateMutexW
```

Figure 3-4 | Unique Mutex

② Confirms OS version

It checks OS version of the victim system. As seen in Figure 3-5, even Windows 8.1 is targeted by Dyre malware.

```
ASCII "Win_7"
ASCII "Win_7_SP1"
ASCII "Win_XP"
ASCII "Win_8"
ASCII "Win_8.1"
ASCII "Win_Server_2003"
ASCII "Win_Vista_SP2"
ASCII "Win_Vista"
ASCII "Win_Vista_SP1"
ASCII "unknown"
```

Figure 3-5 | Confirmation of OS version

③ Reads/Writes Log (Settings) files

The following Log files are loaded.

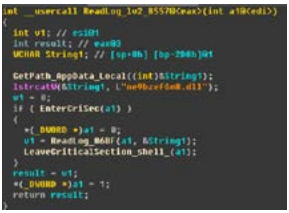


Figure 3-6 | Log (setting) files loaded

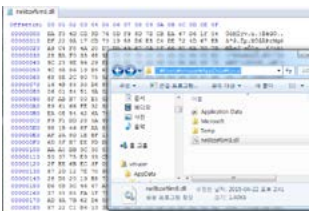


Figure 3-7 | Encoded Log (Settings) file

2.2. Get Child Window Handle Function

The Get Child Window Handle function is created as a thread, then finds a Window that has the interactive dialogue "#32770" and acquires a Window Handle from that child thread. Because the browser creates a new process for each function and for each browser tab, it is assumed that it essentially hooks into the process that executes the functions.

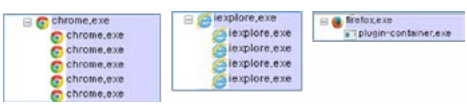


Figure 3-8 | General Browser Processes

The process that is actually hooked becomes the parent process as well as the child process just below that parent process.

2.3. Confirmation of Internet Connection

The following is the process of confirming three types of Internet connection. If connection to the internet fails, there is no attempt to communicate with the C&C server.

① Connection 1:google.com / microsoft.com

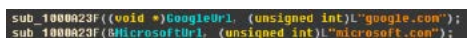


Figure 3-9 | Confirmation of Connection 1

② Connection 2: STUN server

Connection is made to STUN (Session Traversal Utilities for NAT), which is an open source server, and confirmation is made as to whether there is an internet connection.

Table 3-2 | STUN Server List

STUN Servers	
stun1.voiceeclipse.net	stunserver.org
stun.callwithus.com	203.183.172.196:3478
stun.sipgate.net	s1.taraba.net
stun.ekiga.net	s2.taraba.net
stun.ideasip.com	stun.l.google.com:19302
stun.internetcalls.com	stun1.l.google.com:19302
stun.noc.ams-ix.net	stun2.l.google.com:19302

stun.phonepower.com	stun3.l.google.com:19302
stun.voip.aebc.com	stun4.l.google.com:19302
stun.voipbuster.com	stun.schlund.de
stun.voxgratia.org	stun.rixtelecom.se
stun.ipshka.com	stun.voiparound.com
stun.faktortel.com.au	numb.viagenie.ca
stun.iptel.org	stun.stunprotocol.org
stun.voipstunt.com	stun.2talk.co.nz

③ Connection 3: A connection is then made for http://icanhazip.com to acquire a public IP

After connecting to http://icanhazip.com, it phishes and saves the acquired public IP here.

Figure 3-10 | Connection 3

2.4. C&C Server Address Decoding and Parsing

The encoded data from within a file is decoded and the C&C address is obtained.

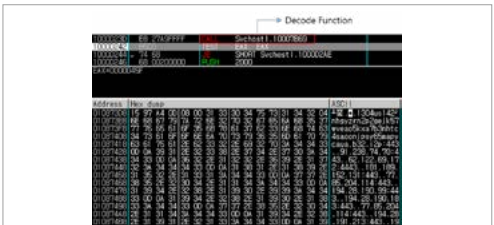


Figure 3-11 | C&C Server Address within the Code

Table 3-3 | C&C Server List 1

Description	
Bot Identifier	1304us142
I2P Address	nhgyzrn2p2gejk57wveao5kxa7b3nhtc4saoonjpsy65mapycaua.b32.i2p:443
https Host	https://5.255.166.200/0.su3

Table 3-4 | C&C Server List 2

91.238.74.70:443	194.12.117.68:443	91.242.53.142:4443	178.18.172.25:4443
62.122.69.172:4443	62.122.102.105:443	85.66.249.207:443	89.189.174.40:443
181.189.152.131:443	46.151.8.149:443	46.175.23.130:443	194.28.190.84:443
77.85.204.114:443	195.34.206.204:443	178.136.123.22:443	91.232.157.139:443
194.28.190.99:443	62.122.69.159:4443	91.194.239.1264443	194.28.191.144:443
194.28.190.183:443	31.28.115.88:443	94.231.178.46:4443	46.151.49.128:443
77.85.204.114:43	62.182.33.16:443	194.28.190.167:443	194.28.191.144:443
194.28.191.213:443	188.123.34.203:443	80.234.34.137:443	46.151.48.97:443
194.28.190.88:443	78.109.34.34:443	213.111.243.60:4443	89.250.145.129:443
94.180.109.121:443	31.28.115.88:443	46.149.253.52:4443	213.87.54.111:443
95.67.88.84:4443	62.182.33.16:443	37.57.101.221:4443	188.123.34.192:443
194.28.190.86:443	188.123.34.203:443	134.249.63.46:443	195.206.25.131:443
176.56.24.229:443	78.109.34.34:443	85.192.165.229:443	46.151.48.184:443

2.5. C&C Request Header

When requesting connection to C&C servers, POST and GET request methods are used according to command.

```
if ( *(_DWORD *)(a1 + 0x13C) )
  result = InternetRead_POST(a1);          // 1
else
  result = InternetRead_GET(a1);           // 0
```

Figure 3-12 | HTTP Request Method

The following shows the use of set HTTP headers.

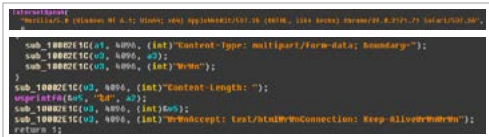


Figure 3-13 | C&C Request function with HTTP headers

2.5. Registry Modification for Remote Access

Malware uses RDP function for remote access, then adds and modifies related registry.

Figure 3-14 | Modifying RDP-related Registry

2.6. System Shutdown

The injected DLL inserted into the system process directly connects with Shutdown.exe and has the ability to shutdown the system.

Figure 3-15 | AUTOKILLOS command

2.7. C&C Transfer Factor Analysis

When the C&C is contacted, the parameters are as follows:

Figure 3-16 | C&C transfer factor analysis

3. Browser - Injected Dll

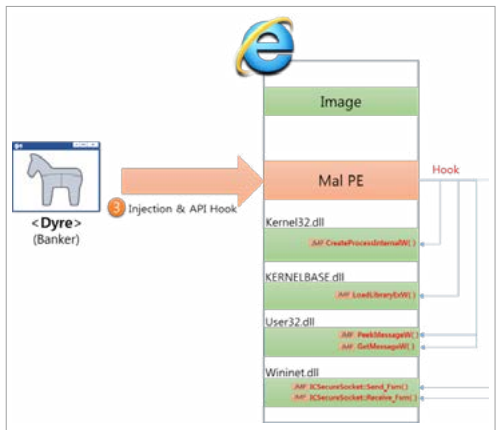


Figure 3-17 | IE Browser Hooking Code Patch

3.1. Main Function

It calls the hooking patch functions according to browser as below:

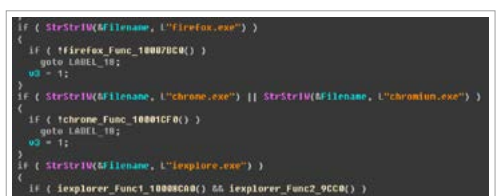


Figure 3-18 | Calls Patch Function for Browsers

3.2. Hooking Patch

It patches code to steal incoming and outgoing banking data through the web browser.

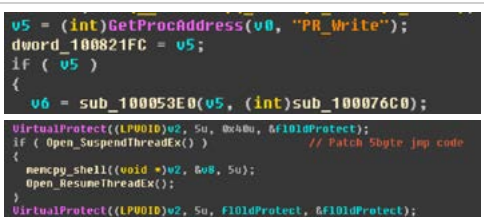


Figure 3-19 | Hooking Patch

Table 3-5 | Hooking Function for Browsers

Browser	Funtion	Module
Internet Explorer	CreateProcessInternalW	kernel32.dll
	LoadLibraryExW	KERNELBASE.dll
	GetMessageW	USER32.dll
	PeekMessageW	USER32.dll
	ICSecureSocket::Send_Fsm	WININET.dll
	ICSecureSocket::Receive_Fsm	WININET.dll
FireFox	PR_Read	nss3.dll
	PR_Write	nss3.dll
	PR_Close	nss3.dll
	GetMessageW	USER32.dll
	PeekMessageW	USER32.dll
Chrome	LoadLibraryExW	kernel32.dll
	GetMessageW	USER32.dll
	PeekMessageW	USER32.dll
	ssl_write	chrome.dll
	ssl_read	chrome.dll
	ssl_close	chrome.dll

As Figure 3-20 shows, the malware has a list of targeted banks to attack. Last April during the first analysis, roughly 500 banks were included on the list; in February of this year, the list was confirmed to have increased with the addition of two more Korean banks.

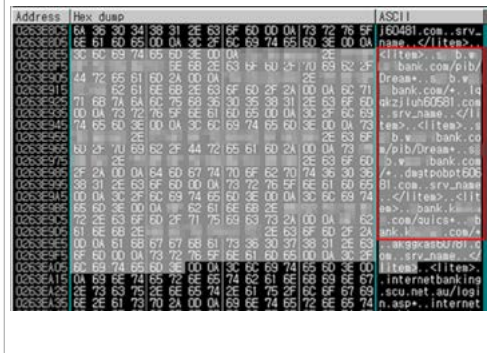


Figure 3-20 | Targeted Banks and Redirected Phishing Pages

3.3. Keylogging

The malware initiates keylogging through the patch code in the GetMessageW() and PeekMessageW() functions.

Figure 3-21 | Message Function for Windows Patch

Dyre is known as a variant of the existing Cridex banking malware and Game Over malware; it is also called Dridex, Dyzap, and Dyreza.

As mentioned above, the Dyre malware's objective is to steal financial data and

finance-related information and money. From the end of last year in 2014, it has been actively spreading and while its form has been constantly changing, the trend of its internal code has not changed.

The Dyre malware is detected by V3, AhnLab anti-virus products, with aliases as below:

< Alias from V3 Products >

Win-Trojan/MDA.D709
Trojan/Win32.Dyre
Trojan/Win32.Dyzap

<References>

http://www.secureworks.com/cyber-threat-intelligence/threats/dyre-banking-trojan/
https://blog.korelogic.com/blog/2014/05/27/malware_callback
F5SOC Dyre Malware Analysis Report November 2014.pdf
Network_insights_of_Dyre_and_Dridex_Trojan_bankers.pdf
http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3139/the-dire-implications-of-dyreza
http://stopmalvertising.com/malware-reports/introduction-to-dyreza-the-banker-that-bypasses-ssl.html
https://portal.sec.ibm.com/mss/html/en_US/support_resources/pdf/Dyre_Wolf_MSS_Threat_Report.pdf
http://nextpage.com/threatinsight/posts/dyreza-takes-stock.php
F5SOC - Dyre Internals.pdf

AhnLab

ASEC REPORT

VOL.66
June, 2015

Contributors	**ASEC Researchers**	Publisher	**AhnLab, Inc.**
Editor	**Content Creatives Team**	Website	**www.ahnlab.com**
Design	**Design Team**	Email	**global.info@ahnlab.com**