Into the Fog -
The Return of ICEFOG APT

Chi-en (Ashley) Shen
Senior Researcher
WHOIS

- Chi En Shen (Ashley)
- Senior Researcher at FireEye Global Intelligence Collection and Research Team.
- Co-founder of HITCON GIRLS security community in Taiwan
- Review board of Black Hat Asia, Blue Hat Shanghai, Hack in the Box
- 2nd time to SecTor~! Thank you!
The Story Starts From A Tweet...

- Tweetel! (Tweet + Intel)
- Thanks for sharing 😊

**Tweet**

Brian Bartholomew @Mao_Ware · 26 Feb 2018

Replying to @ClearskySec

I wouldn’t be too quick to call this “IceFog” (the group). The payload is a newer variation of Fucobha that has been used since early 2016. There are potentially multiple “groups” using this based on region / language responsibilities.
What is ICEFOG (aka Fucobha)?

- Now ICEFOG is referred as a Malware family, a report, sometimes referred as a group. (is it?)

Icefog Espionage Campaign is ‘Hit and Run’ Targeted Operation

Kaspersky Lab has uncovered Icefog, a series of targeted attacks against sensitive organizations in South Korea and Japan.

An espionage campaign featuring precise targeting of victims and malware that allows the attackers one-on-one interaction with compromised systems has been uncovered. Government agencies, manufacturers, high tech companies and media organizations in South
The ICEFOG Campaign Return?

- No public reporting on the new ICEFOG campaign after 2014. What happened between these 5 years?
- The samples discovered recently has changed the target scope. Is this the same group as in 2013?
- Goal: find out what happened between these 5 years and find out who are using ICEFOG.

Release of ICEFOG report

Blog about Java version ICEFOG.
Why Do We Care?
Why Do We Care?

Know your **Pokemon** and know yourself, you will always be victorious.

- Ashley
Let’s start HUNTING!

• **Tools:**
  • Yara, signature detections on appliance,

• **Method:**
  • Strings
  • Malware Functions
  • PDB & GUID
  • Exploit document template
  • Infrastructure pivoting, correlation.
### ICEFOG Variants (<2014)

<table>
<thead>
<tr>
<th></th>
<th>Old ICEFOG</th>
<th>ICEFOG Type 1</th>
<th>ICEFOG Type 2 (No sample)</th>
<th>ICEFOG Type 3 &amp; 4</th>
<th>ICEFOG-NG</th>
<th>ICEFOG OSX (aka Macfog)</th>
<th>ICEFOG Java (aka Javafog)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Support platform</strong></td>
<td>Windows</td>
<td>Windows</td>
<td>Windows (shellcode &amp; standalone)</td>
<td>Windows</td>
<td>Windows</td>
<td>Mac OSX</td>
<td>Java</td>
</tr>
<tr>
<td><strong>Support Functions</strong></td>
<td>• upload_</td>
<td>• upload_</td>
<td>• upload_</td>
<td>Unknown</td>
<td>• Cmd</td>
<td>• upload_</td>
<td>• upload_</td>
</tr>
<tr>
<td></td>
<td>• download_</td>
<td>• download_</td>
<td>• download_</td>
<td></td>
<td>• Download</td>
<td>• download_</td>
<td>• cmd_Update Domain</td>
</tr>
<tr>
<td></td>
<td>• Cmd_</td>
<td>• Cmd_</td>
<td>• Cmd_</td>
<td></td>
<td>• Upload</td>
<td>• Cmd_</td>
<td>• cmd_</td>
</tr>
<tr>
<td></td>
<td>• code_</td>
<td>• code_</td>
<td>• Code_</td>
<td></td>
<td>• sleep</td>
<td>• code_</td>
<td></td>
</tr>
<tr>
<td><strong>Communication Method</strong></td>
<td>Communicate with emails</td>
<td>Communicate with C&amp;C server with “.aspx” scripts</td>
<td>Script based proxy server</td>
<td>C&amp;C server with scripts named “view.asp”, “update.asp”, “upfile.asp”</td>
<td>TCP connection to port 5600</td>
<td>Communicate with C&amp;C server with “.aspx” scripts</td>
<td>Communicate with C&amp;C server with “.aspx” scripts</td>
</tr>
</tbody>
</table>
Common ICEFOG Strings

Communication Traffic

XOR Keys

Old ICEFOG Mail

ICEFOG-Type2

ICEFOG-Type1
Hunting Malware Functions

ICEFOG-NG Communication

ICEFOG-NG Encrypt Function

ICEFOG OSX Encrypt Function

ICEFOG-Type 1 Encrypt Function
The CVE2017-11882 Exploit Template

- Drops into %temp%
- Shellcode decode & execute
- Malware

Open Document ➔ Encoded (0xFC) Dropper (8.t) ➔ Dropper ➔ Malware

Can be hunted by the RTF Object

- Also, great research from Anomali.
The Shared Exploit Builder

- CVE 2017-11882 exploit template.
- Actually, shared among at least 3 different groups. (APT40, Conimes team aka Goblin Panda, ICEFOG Operators)

<table>
<thead>
<tr>
<th>Threat Group</th>
<th>Hash</th>
<th>Malware</th>
<th>Create Date</th>
<th>Author</th>
<th>Targeted Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>APT40</td>
<td>d5a7dd7441dc2b05464a21ddc0871ff</td>
<td>BEACON</td>
<td>2017-12-07 08:17:00</td>
<td>Windows User</td>
<td>USA</td>
</tr>
<tr>
<td>Temp.CONIMES</td>
<td>f223e4175649fa2e34271db8c968db12</td>
<td>TEMPFUN</td>
<td>2018-01-15 14:47:00</td>
<td>Windows User</td>
<td>LAO</td>
</tr>
<tr>
<td>Temp.CONIMES</td>
<td>07544892999b91ae2c9280d8ee3c663a</td>
<td>TEMPFUN</td>
<td>2018-01-17 09:04:00</td>
<td>Windows User</td>
<td>VNM</td>
</tr>
<tr>
<td>Temp.CONIMES</td>
<td>45a94b3b13101c932a72d89ff5eb715a</td>
<td>TEMPFUN</td>
<td>2018-01-31 11:24:00</td>
<td>Windows User</td>
<td>VNM</td>
</tr>
<tr>
<td>ICEFOG Operator</td>
<td>46d91a91ecdf9c0abc7355c4e7cf08fc</td>
<td>ICEFOG</td>
<td>2018-02-22 20:07:00</td>
<td>T</td>
<td>TUR</td>
</tr>
<tr>
<td>ICEFOG Operator</td>
<td>80883df4e89d5632fa72a85057773538</td>
<td>ICEFOG</td>
<td>2018-02-22 20:07:00</td>
<td>T</td>
<td>KZ, RU</td>
</tr>
<tr>
<td>SOURCANDLE Operator</td>
<td>ac845ad6a5ac75842ead069f5daf29a1</td>
<td>SOURCANDLE</td>
<td>2019-01-24 13:24:00</td>
<td>Windows [ U [</td>
<td>JP</td>
</tr>
</tbody>
</table>
# Two ICEFOG Variants (2014 - 2019)

<table>
<thead>
<tr>
<th></th>
<th>ICEFOG - P</th>
<th>ICEFOG - M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support platform</td>
<td>Windows (x86 &amp; x64)</td>
<td>Windows (shellcode)</td>
</tr>
<tr>
<td>First Seen</td>
<td>2014</td>
<td>2018</td>
</tr>
<tr>
<td>Communication Protocol</td>
<td>HTTP</td>
<td>HTTPS (port 443)</td>
</tr>
</tbody>
</table>
### ICEFOG-P (New)

#### Command List

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cmd_</td>
<td>Execute the command received from C&amp;C</td>
</tr>
<tr>
<td>download_</td>
<td>Download file from specified URL</td>
</tr>
<tr>
<td>filelist_</td>
<td>Obtaining the list of files within specified folder.</td>
</tr>
<tr>
<td>upload_</td>
<td>File loading from the server to computer.</td>
</tr>
<tr>
<td>delete_</td>
<td>Delete specified file</td>
</tr>
<tr>
<td>rename_</td>
<td>Move file to specified location</td>
</tr>
<tr>
<td>newdir_</td>
<td>Create specified directory</td>
</tr>
<tr>
<td>beforecontinuefile_</td>
<td>Reset connection to the server</td>
</tr>
<tr>
<td>continuefile_</td>
<td>Resume the file download from the server.</td>
</tr>
<tr>
<td>exit_</td>
<td>Terminate Process.</td>
</tr>
<tr>
<td>transover_</td>
<td>Termination of current thread.</td>
</tr>
<tr>
<td>screen_</td>
<td>Send screenshot to C&amp;C server.</td>
</tr>
<tr>
<td>key_</td>
<td>Send keylogger’s log file to C&amp;C</td>
</tr>
<tr>
<td>disklist_</td>
<td>Setting monitored folders</td>
</tr>
<tr>
<td>disklog_</td>
<td>Upload monitored folder’s data</td>
</tr>
<tr>
<td>code_—(removed)</td>
<td>run code from file to memory</td>
</tr>
</tbody>
</table>

**New supported commands**

Gentle reminder for entering the main function

Check if system date < 20130505

#### Anti-sandbox?

Check if system date < 20130505
ICEFOG-P (New)

**Traffic of ICEFOG Type 1**

POST
/news/upload.aspx?filepath=ok&filename=<hostname>_<host IP>.jpg HTTP/1.1
Host: icefog.8.100911.com
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
User-Agent: MyAgent
Content-Length: 0

**Traffic of ICEFOG-P**

POST /upload.aspx?filepath=info&filename=<hostname>_<MAC address>.jpg HTTP/1.1
User-Agent: Internet Explorer
Host: foo.com
Content-Length: 862
Cache-Control: no-cache

HOST NAME: WINDOWS7
USER NAME: user
OS Version: Microsoft Windows 7  x86 Service Pack 1 (Build 7601)
CPU: GenuineIntel Intel64 Family 6 Model 142 Stepping 9 0MHZ
Physical memory: Total physical memory:1023MB, Available memory:388MB
Windows Directory: C:\\Windows
System Directory: C:\\Windows\\system32
Hard Disk: C:\\ (NTFS)
CD-ROM Disk: D:\
Disk space: Total disk space:39G, The remaining disk space:15G

Adds physical machine information likely for filtering out sandbox or analysis environment
ICEFOG-P (New)

Harvests Windows and browser credentials

Source code seems to download from internet

Loading sqlite3 library for collecting Firefox credentials
Malware also embedded some of the functions

Use the code from fgdump project

// Description: Firefox Password Cache Decrypter
// Versions: Firefox 1, 2, and 3
// Author: Krippler
// Language: C
// Released: 9/9/2008
// URL: http://www.krippler.com/
// Credit: http://securityxploded.com/ (PD 2 Source)
// Original Source: http://megmatrix.50web.com/download/Firepassword_arc.zip

SecurityXploded
250+ Free Softwares & 25 Million+ Downloads
ICEFOG-P (New)

Monitor directory changes with ReadDirectoryChangesW API, logs save to fmonitor.dat

disklist_ save the directory list to filecfg_temp.dat

Change log output format

upload.aspx?filepath=disklog/hostname_<MAC Address>&filename=20131314.jpg

_disklog send changes log to C2
ICEFOG-M (The latest)

- Supports same functions as ICEFOG–P.
- Communication changed to HTTPS via port 443.
- Payload became file-less (stored in registry), applied a customized loader launched by benign loader (DLL hijacking).
- Loads an external sqlite3.dll library.

Encrypted ICEFOG payload stored in registry
# PDB in ICEFOG

## ICEFOG Samples > 2013

More developers?

<table>
<thead>
<tr>
<th>PDB</th>
<th>Associated ICEFOG Variant</th>
</tr>
</thead>
<tbody>
<tr>
<td>E:\zc\HTTPS\HTTPS\86AuthenticateProxy\ExeLoader\Release\RasTls.pdb</td>
<td>ICEFOG-P</td>
</tr>
<tr>
<td>C:\Users\apper\Desktop\86AuthenticateProxy (copy)\ExeLoader\Release\RasTls.pdb</td>
<td>ICEFOG-P</td>
</tr>
<tr>
<td>C:\0426\86authenticateproxy\ExeLoader\Release\RasTls.pdb</td>
<td>ICEFOG-P</td>
</tr>
<tr>
<td>C:\Documents and Settings\Administrator\Desktop\86AuthenticateProxy (copy)\ExeLoader\Release\RasTls.pdb</td>
<td>ICEFOG-P</td>
</tr>
<tr>
<td>D:\www\downloadccc0301\chen_http0301\source\Server\64\ExeLoader\x64\Release\linkinfo.pdb</td>
<td>ICEFOG-P</td>
</tr>
<tr>
<td>F:\worktmp\2014.11.05\ff\Server\86AuthenticateProxy\ExeLoader\Release\linkinfo.pdb</td>
<td>ICEFOG-P</td>
</tr>
</tbody>
</table>
MacOS X ICEFOG (aka MacFog)

- Among all the samples we collected, some are the MacOS X MachO executable files.
- The MacOS X ICEFOG was first distributed in Chinese forums, forged as image process software.
- Newly uploaded old samples, having the same default C&C setting.
- Only one new sample with a private IP setting (testing?).
ICEFOG Samples Compile Timestamp Distribution

Sept 25, 2013

Kaspersky Published Report
The Icefog APT: A Tale of Cloak and Three Daggers
How to determine the timeframe of the sample?

• When we found the sample after the campaign finished.
• Consider:
  • PDNS time
  • Domain create date
  • Compile timestamp (dropper? Payload? Wrapper?)
  • Exploit document last saved time (template?)
  • Decoy document timestamp
  • Date sample was first seen in the wild
  • PDB

<table>
<thead>
<tr>
<th>Sample</th>
<th>Sample First Seen in the wild</th>
<th>Exploit Doc Last saved date</th>
<th>Dropped Malware Compile Date</th>
<th>C&amp;C Domain Passive DNS First Seen</th>
<th>Decoy File Last Modified date</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3ed6b34707e92f7aa35859a9647f044</td>
<td><strong>2017-08-03 10:48:09</strong></td>
<td><strong>2014/04/11 00:00:00</strong></td>
<td><strong>2016-09-27 02:23:30</strong></td>
<td><strong>2017-08-03</strong></td>
<td><strong>2017-08-02 19:17:00</strong></td>
</tr>
</tbody>
</table>
Infrastructure Clustering

• Connecting the dots with passive DNS, registrant email
• Tool: Maltego
• Problems / difficulty
  • Incomplete PDNS data
  • Actor might have changed the infrastructure entirely after the report.
  • Sinkholes filtering. (not all in db....)
  • Parking filtering.
  • Hosting server.
One Eternity Later
- A lot of sinkhole connected to "sinkhole.yourtrap.com"
- Usually 153.xxx.xxx.xxx in Japan registered by NTT.
Attack targeted Agriculture Company in Europe (2015)

• 64 bit ICEFOG-P found in the compromised environment.
• Persistent attack started from 2011.
• Actor mainly used SOGU and FUNRUN backdoor to gain initial access.
• Also, found VICEROY backdoor, which has been used by APT9.
• We also found malware connects to APT10 infrastructure.
• The ICEFOG backdoor found at the scene was a customized version.
Attack targeted Agriculture Company in Europe (2015)

- Leveraged as post exploitation tool.
- Getting C&C configuration from two files and decode with 0x99.
# 2015 TOPNEWS Campaign

- Campaign targets Mongolia and Russia, suspected media, finance and government.
- Sample delivered by spear-phishing email.
- The ICEFOG samples are all ICEFOG-P variant.
- Some samples includes suspected campaign code information.

<table>
<thead>
<tr>
<th>Hash</th>
<th>Compile Timestamp</th>
<th>Drop by</th>
<th>C&amp;C</th>
<th>PDB</th>
<th>Campaign Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>eb2d297d099f3d39874 efa3f89735a01</td>
<td>2015/03/12 10:18:13</td>
<td>f8cc15db9c85da19555a7232 b543c726</td>
<td>dnservers.itemdb.com</td>
<td>C:\Documents and Settings\Administrator\Desktop\86AuthenticateProxy\copy\ExeLoader\Release\RasTls.pdb</td>
<td>02-03</td>
</tr>
<tr>
<td>c7d2c170482d17e2e76 e6937bd8ab9a5</td>
<td>2015/05/14 5:11:42</td>
<td>B3EFDA0E130373DAF6CB17 801714B66F (rarsfx)</td>
<td>bulgaa.sportsnewsa.net</td>
<td>C:\0426\86AuthenticateProxy\ExeLoader\Release\RasTls.pdb</td>
<td>120</td>
</tr>
<tr>
<td>7dc1f0e60f11c456aa15 cc3546716c17</td>
<td>2015/05/14 6:11:42</td>
<td>e84b74f07ae803852f2ed194 58a1539d (tsalin.docx.exe) 74583d7355113ad3e58e355 b003083e5 (winword.scr)</td>
<td>zaluu.dellnewsup.net</td>
<td>C:\0426\86AuthenticateProxy\ExeLoader\Release\RasTls.pdb</td>
<td>100</td>
</tr>
<tr>
<td>09d8f865bccfb239afab 4f4f564081ff</td>
<td>2016/09/27 3:23:30</td>
<td>47713144ae08560ba939ea01 620a0a2d (toot.docx.exe)</td>
<td>zaluu.dellnewsup.net</td>
<td>E:\zc\HTTPS\HTTPS\86AuthenticateProxy\ExeLoader\Release\RasTls.pdb</td>
<td>b</td>
</tr>
</tbody>
</table>
2015 TOPNEWS Campaign

- Most ICEFOG payloads are dropped by RARSFX dropper.
- Decoy uses government related content.

ТӨРИЙН ТУСГАЙ АЛБАН ТУШААЛЫН ЦАЛИНГИЙН СУЛЖЭЭ” (Mongolian translation: SPECIAL OFFICES OF JURISDICTION)
2015 TOPNEWS Campaign

- The domain “dellnewsup.net” has 13 sub-domains.
- Pivoting these sub-domains, we found other malwares connected to the infrastructure.
- Campaign also leveraged SOGU, TEMPFUN and FUNRUN to attack Mongolian targets from 2014 to 2015.

<table>
<thead>
<tr>
<th>Hash</th>
<th>Malware Family</th>
<th>Compile timestamp</th>
<th>C&amp;C</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>664318c95c4a48debd3562ea602796b9</td>
<td>TEMPFUN</td>
<td>2014-07-23 12:44:56</td>
<td>win.dellnewsup.net</td>
<td></td>
</tr>
<tr>
<td>a489f2b4505b8f291804e3931cf16ed8</td>
<td>TEMPFUN</td>
<td>2014-07-23 12:44:56</td>
<td>win.dellnewsup.net</td>
<td>MN</td>
</tr>
<tr>
<td>2e74505cc08c0d0d88146d46915f37af</td>
<td>SOGU</td>
<td>2015-02-06 02:56:28</td>
<td>mn.dellnewsup.net</td>
<td>MN</td>
</tr>
<tr>
<td>a0389879ea435e647d29f6966b1d601f</td>
<td>FUNRUN</td>
<td>2015-02-07 09:34:05</td>
<td>date.dellnewsup.net</td>
<td></td>
</tr>
<tr>
<td>1a93c0257f52e2b1e8e4f52c033a61b3</td>
<td>SOGU</td>
<td>2011-03-02 07:40:24</td>
<td>dwm.dnsedc.com</td>
<td>RU</td>
</tr>
</tbody>
</table>
Roaming Tiger Hackers targets Russian organizations for espionage

Security researchers from ESET uncovered the Roaming Tiger hacking campaign, bad actors in the wild are targeting Russian organizations.

Roaming Tiger is the name of a cyber espionage campaign targeting high profile organizations in Russia and former Soviet Union countries, including Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, Ukraine, and Uzbekistan.

The Roaming Tiger campaign was discovered by experts at ESET in 2014; the researcher Anton Cherepanov presented the findings of their investigation at the 2014 ZeroNights security conference.

According to the experts, the threat actors behind the Roaming Tiger relied on RTF exploits and the PlugX RAT; the analysis of the command and control (C&C) infrastructure suggests the involvement of Chinese hackers.

2015 TOPNEWS Campaign

• Domains registrant email linked to the Roaming Tiger group and rotten tomato campaign.

yuminga1@126.com

2016 APPER Campaign

• In September 2015, KZCERT published a blog about an ICEFOG sample targeting Kazakhstan.

• The sample is an XLS embedded malicious macro that drops an RARSFX dropper, which further deploys ICEFOG-P.
2016 APPER Campaign

- Pivoting the C&C infrastructure, we found 8 related ICEFOG-P samples suspected of being used in the same campaign.
- Same PDB strings in the samples suggest a possible developer “apper”.

<table>
<thead>
<tr>
<th>Hash</th>
<th>Compile Timestamp</th>
<th>C&amp;C</th>
<th>Campaign code</th>
<th>pdb</th>
</tr>
</thead>
<tbody>
<tr>
<td>aae3e322</td>
<td>2016/05/22 10:35:41</td>
<td>ddns.epac.to</td>
<td>cyexy</td>
<td>C:\Users\apper\Desktop\86AuthenticateProxy (copy) \ExeLoader\Release\RasTls.pdb</td>
</tr>
<tr>
<td>dbef5b18</td>
<td>2016/05/19 8:26:23</td>
<td>ddns.epac.to (45.125.13.1 99)</td>
<td>cyexy</td>
<td>C:\Users\apper\Desktop\86AuthenticateProxy (copy) \ExeLoader\Release\RasTls.pdb</td>
</tr>
<tr>
<td>94a412ca08afdf03</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0e25aa79</td>
<td>2016/05/10 9:24:38</td>
<td>45.125.13.1 99</td>
<td>dxx</td>
<td>C:\Users\apper\Desktop\86AuthenticateProxy (copy) \ExeLoader\Release\RasTls.pdb</td>
</tr>
<tr>
<td>1c9119108af073bc9e9d0fa2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a4dc9763</td>
<td>2016/03/21 4:20:25</td>
<td>poff.wha.la</td>
<td>soums</td>
<td>C:\Users\apper\Desktop\86AuthenticateProxy (copy) \ExeLoader\Release\RasTls.pdb</td>
</tr>
<tr>
<td>d296c45a8461556f02479ecde</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0a9dcf6d274443cda067b13eb04c7d0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a9ecf6d26</td>
<td>2016/03/21 4:20:25</td>
<td>poff.wha.la</td>
<td>soums</td>
<td>C:\Users\apper\Desktop\86AuthenticateProxy (copy) \ExeLoader\Release\RasTls.pdb</td>
</tr>
<tr>
<td>74443cda067b13eb04c7d0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>404b1b78b4f34612e61dd4af3bf5083f1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0a682172fa38ef1078b300a492997fc02</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 2018 The WATERFIGHT CAMPAIGN

- Campaign targeted suspected water source provider, banks and government.
- Targeted countries include Turkey, India, Kazakhstan, Uzbekistan and Tajikistan.

<table>
<thead>
<tr>
<th>Hash</th>
<th>File name</th>
<th>Exploit</th>
<th>Default codepage</th>
<th>Creation Date</th>
<th>Last Modified</th>
<th>Author</th>
<th>Last modify by</th>
</tr>
</thead>
<tbody>
<tr>
<td>9ca6d45643f89bf233f08b7d74910346</td>
<td>Address Book 2018.doc</td>
<td>CVE-2017-11882</td>
<td>Western European</td>
<td>2018/02/22 20:07:00</td>
<td>2018/02/22 20:08:00</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>d00a34baad19d40dcefbadb0942a2e4d</td>
<td>WorkPlan.doc</td>
<td>CVE-2017-11882</td>
<td>Western European</td>
<td>2018/02/22 20:07:00</td>
<td>2018/02/22 20:08:00</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>88d667cc01c4d8ee32e9de116f3bfdeb</td>
<td>AMU_SLA_Agreement_Final_Dt_20-Spr_.14.doc</td>
<td>CVE-2017-11882</td>
<td>Simplified Chinese</td>
<td>2018/02/22 20:07:00</td>
<td>2018/03/14 17:34:00</td>
<td>T</td>
<td>Administrator</td>
</tr>
<tr>
<td>46d91a91ecdf9c0abc7355c4e7cf08fc</td>
<td>katalimcilar listesi.doc</td>
<td>CVE-2017-11882</td>
<td>Western European</td>
<td>2018/02/22 20:07:00</td>
<td>2018/02/22 20:08:00</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>80883df4e89d5632fa7a85057773538</td>
<td>Внутренняя описание документов AGAT.doc</td>
<td>CVE-2017-11882</td>
<td>Western European</td>
<td>2018/02/22 20:07:00</td>
<td>2018/02/22 20:08:00</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>7fa8c07634f937a1fce9180531dc2e4</td>
<td>счет.doc</td>
<td>CVE-2017-11882</td>
<td>Simplified Chinese</td>
<td>2017/05/22 11:52:00</td>
<td>2017/05/22 11:52:00</td>
<td>Windows</td>
<td>Windows</td>
</tr>
<tr>
<td>e7c5307691772a058fa7d9e8ea426a59</td>
<td>Задание.doc</td>
<td>CVE-2017-11882</td>
<td>Simplified Chinese</td>
<td>2017/05/22 11:52:00</td>
<td>2017/05/22 11:52:00</td>
<td>Windows</td>
<td>Windows</td>
</tr>
<tr>
<td>63f9eaf7a80231480687b134b1915bd0</td>
<td>Российский фигурист выиграл зимние Олимпийские игры PyeongChang в Южной Корее.doc</td>
<td>CVE-2012-0158</td>
<td>Simplified Chinese</td>
<td>2017/05/22 11:52:00</td>
<td>2017/05/22 11:52:00</td>
<td>Windows</td>
<td>Windows</td>
</tr>
</tbody>
</table>
2018 The WATERFIGHT CAMPAIGN

Leveraged the shared exploit template
2018 The WATERFIGHT CAMPAIGN

- Exploit document ICEFOG-P samples.
- C&C domain and file name shows interest in a water source company in Uzbekistan.
- Compiled a lot samples in 2 days

<table>
<thead>
<tr>
<th>Hash</th>
<th>Compile date</th>
<th>Drop by</th>
<th>C&amp;C</th>
<th>Campaign code</th>
</tr>
</thead>
<tbody>
<tr>
<td>4178d9b22efe7044540043b5c770b6a</td>
<td>2018/02/24 5:20:16</td>
<td>9ca6d45643f89bf233f08b7d74910346</td>
<td>tele.zyns.com</td>
<td>umde</td>
</tr>
<tr>
<td>1c2d4c95c1b4e9d5193423719a7bb075</td>
<td>2018/02/23 8:13:20</td>
<td>d00a34baad19d40dcefbdab0942a2e4d</td>
<td>uzwatersource.dynamic-dns.net</td>
<td>osbc</td>
</tr>
<tr>
<td>71e5b89d5a804ddbe84fa4950bf97ac7</td>
<td>2018/02/26 11:58:57</td>
<td>88d667cc01c4d8ee32e9de116f3bfdeb</td>
<td>trendis.sixth.biz</td>
<td>hgmpy</td>
</tr>
<tr>
<td>6fffd88292eed0483b4030e5f8401e</td>
<td>2018/02/23 8:13:20</td>
<td>46d91a91edf9c0abc7355c4e7cf08fc</td>
<td>uzwatersource.dynamic-dns.net</td>
<td>osbc</td>
</tr>
<tr>
<td>6850e553445c09eac3206331eb0429</td>
<td>2018/02/23 9:44:25</td>
<td>80883df4e89d5632fa72a85057773538</td>
<td>laugh.toh.info</td>
<td>jkmsy</td>
</tr>
<tr>
<td>d5c67718e35bd1083dd50335ba9e89d</td>
<td>2018/02/23 8:44:25</td>
<td>7fa8c07634f937a1fcef9180531dc2e4</td>
<td>laugh.toh.info</td>
<td>jkmsy</td>
</tr>
<tr>
<td>9344e542cc1916b9db587daa70f0652</td>
<td>2018/02/23 9:35:38</td>
<td>e7c5307691772a058fa7d9e8ea426a59</td>
<td>aries.epac.to</td>
<td>gskv</td>
</tr>
<tr>
<td>c2893fecnadb7fed4fe74ea56133901</td>
<td>2018/02/23 14:49:58</td>
<td>63f9eaf7a80231480687b134b1915bd0</td>
<td>kastygost.compress.to</td>
<td>msxdg</td>
</tr>
</tbody>
</table>
2018 PHKIGHT Campaign

• On April 26, 2018, our appliance detected ICEFOG traffic from out of the Philippines.

• We also found the traffic of ICEFOG from the scanned URL on a public scanning service. The timestamp indicates that this campaign was likely still ongoing in July and October 2018:

```plaintext
POST /Home/upload.aspx?filepath=*&filename=*
HTTP/1.1
User-Agent: Internet Explorer
Host: yahzee.eyellowarm.com:443
Content-Length: 908
Connection: Keep-Alive
Cache-Control: no-cache
```
2018 PHKIGHT Campaign

• Investigating the C&C domain “eyellowarm.com”, we found two other sub-domains:
  - news.eyellowarm.com
  - meal.eyellowarm.com

• The domain “news.eyellowarm.com” is connected by an ENDCMD (aka (Hussarini, Sarhust) malware, which we have observed in APT15’s (aka Social Network Team) campaign.

<table>
<thead>
<tr>
<th>Hash</th>
<th>filename</th>
<th>Malware</th>
<th>Compile Timestamp</th>
<th>C&amp;C</th>
</tr>
</thead>
<tbody>
<tr>
<td>e5bdc78c686e15dfeed6696b</td>
<td>NvSmartMax.dll</td>
<td>ENDCMD</td>
<td>2010-12-19 04:51:39</td>
<td>news.eyellowarm.com</td>
</tr>
<tr>
<td>cd5989c3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note that although the sample has the compile timestamp in 2010, it is observed in the wild in 2018 and the C&C remains active during our analysis in 2018.
2018 PHKIGHT Campaign

- Correlated (through passive DNS) infrastructure show strong interest in the Philippines.

- www.benzerold.com
- ph4.01transport.com
- news.eyellowarm.com
- durian.appleleveno.com
- adove.benzerold.com
- benzerold.com
- mailback.benzerold.com
- ph2.01transport.com
- phldt.appleleveno.com
- yahzee.eyellowarm.com
- mecaf.benzerold.com
- ipad.appleleveno.com
- course.appleleveno.com
- well.suverycool.com
- pldt.benzerold.com
- www.knightpal.com
- banana.appleleveno.com
- pop3.numnote.com
- afp1.kaboolyn.com
- trans.numnote.com
- usiszero.benzerold.com
- numnote.com
- pldt.knightpal.com
- ph1.numnote.com
- ns1.01transport.com
- pldt.con.knightpal.com
- afp1.knightpal.com
- appdata.appleleveno.com
- ns2.01transport.com
- ns01.knightpal.com
- ph.01transport.com
- support.numnote.com
- ph1.01transport.com
- knightpal.com
- appleleveno.com
- node-ph-mnl2.kyssrcd.pw
- isafp.numnote.com
- ph1vip.blue-vpn.net
- news.numnote.com
- news.kaboolyn.com
- topic.numnote.com
- dns01.comesafe.com
- is01.knightpal.com
- eyellowarm.com
- news.yahzee.eyellowarm.com
- kaboolyn.com
- dns1.kaboolyn.com
- yahzee.yahzee.eyellowarm.com
- ds03.numnote.com
- meal.eyellowarm.com
- message.benzerold.com

- pnoc1.numnote.com
- 01transport.com
## 2018 PHKIGHT Campaign

- ENDCMD and MIRAGE malware were exclusively observed used by APT15 (aka Social Network team). The targets, malware and TTP all align with the profile of APT15.

<table>
<thead>
<tr>
<th>Hash</th>
<th>Malware family</th>
<th>filename</th>
<th>Compile Timestamp</th>
<th>C&amp;C</th>
<th>PDB string</th>
</tr>
</thead>
<tbody>
<tr>
<td>4f11e00b015047642d8ddc306fc90da0</td>
<td>ENDCMD</td>
<td>NvSmartMax.dll</td>
<td>2010-12-19 04:51:39</td>
<td>news.eyellowarm.com</td>
<td>C:\Users\Sun\Desktop\new_test\NvSmart\Release\NvSmart.pdb</td>
</tr>
<tr>
<td>1554900f889c9498c43c9f875e9ee38</td>
<td>MIRAGE</td>
<td>netsh.exe</td>
<td>2013-06-28 09:27:57</td>
<td>pldtcon.knightpal.com</td>
<td></td>
</tr>
<tr>
<td>7b8c955a0f1d6d37833277849a070e37</td>
<td>ENDCMD</td>
<td>Outlib.dll</td>
<td>2016-07-06 02:50:18</td>
<td>well.suverycool.com</td>
<td></td>
</tr>
<tr>
<td>92853e0506ea16c6f17ac32f5ef8f3b3</td>
<td>ENDCMD</td>
<td>Outlib.dll</td>
<td>2015-08-27 07:52:36</td>
<td>ipad.appleleveno.com</td>
<td></td>
</tr>
<tr>
<td>4f11e00b015047642d8ddc306fc90da0</td>
<td>ENDCMD</td>
<td>Outlib.dll</td>
<td>2015-08-27 07:52:36</td>
<td>durian.appleleveno.com</td>
<td></td>
</tr>
<tr>
<td>86409708eb0c716858e30ae15eb7d47</td>
<td>ENDCMD</td>
<td>N/A</td>
<td>2010-12-19 04:53:10</td>
<td>news.kaboolyn.com</td>
<td></td>
</tr>
</tbody>
</table>
2019 SKYLINE Campaign

- Observed the ongoing campaign that likely targeted Turkey and Kazakhstan in 2019.
- The timestamp suggests the campaign might have started from 2018.
- Leveraged CVE 2017-11882 shared exploit template with ICEFOG-M, no payload timestamp.

<table>
<thead>
<tr>
<th>Hash</th>
<th>filename</th>
<th>Exploit</th>
<th>Code Page</th>
<th>Create Date</th>
<th>Last modify date</th>
<th>Author</th>
<th>Last modify by</th>
</tr>
</thead>
<tbody>
<tr>
<td>30528dc0c1e123dff51f40301cc03204</td>
<td>Unknown</td>
<td>CVE-2018-0802</td>
<td>Western European</td>
<td>2018/04/23 1:01:00</td>
<td>2018/04/23 1:01:00</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>4642e8712c8ada8d56bd36416abb4808</td>
<td>doc.rtf</td>
<td>CVE-2017-11882</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>c65b73dde66184bae6ead97afd1b4c4b</td>
<td>doc20190301018.doc</td>
<td>CVE 2017-11882</td>
<td>Western European</td>
<td>2018/04/23 1:01:00</td>
<td>2018/04/23 1:01:00</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>
2019 SKYLINE Campaign

• New ICEFOG attack vector – file-less payload (ICEFOG-M)

Open Document → Drops into %temp% → Encoded (0xFC) Dropper (8.t) → Shellcode in doc decode and execute → Shellcode write encrypted ICEFOG-M payload to registry → 8.T dropper drops → DLL hijacking loader → Read, decrypt and execute
2019 SKYLINE Campaign

The Dropper’s workflow

Loop to encrypt the payload

Customized loader read register key
2019 SKYLINE Campaign

• Two observed loaders

<table>
<thead>
<tr>
<th>Hash</th>
<th>Compile Timestamp</th>
<th>Drop by</th>
<th>Observed Connected C&amp;C</th>
</tr>
</thead>
<tbody>
<tr>
<td>0b86cc8e56a400f1adeb1e7b6ebe6abe</td>
<td>2018/12/10 14:31:47</td>
<td>4642e8712c8ada8d56bd36416abb4808</td>
<td>nicodonald.accesscam.org</td>
</tr>
</tbody>
</table>
| c6a73e29c770065b4911ef46285d6557 | 2018/04/27 3:49:31 | 30528dc0c1e123dff51f40301cc03204c65b73dde66184bae6ead97afd1b4c4b | skylineqaz.crabdance.com
|                           |                     |                                              | xn—ylineqaz-y25ja.crabdance.com
|                           |                     |                                              | youareexcellent.kozow.com
|                           |                     |                                              | xn--uareexcellent-or3qa.kozow.com |
ICEFOG-M (The latest)

POST /upload.aspx?filepath=info&filename=<hostname>_<MAC address> HTTP/1.1
User-Agent: Internet Explorer
Host: foo.com
Content-Length: 862
Cache-Control: no-cache

HOST NAME:WINDOWS7
USER NAME:user
OS Version: Microsoft Windows 7  x86 Service Pack 1 (Build 7601)
CPU: GenuineIntel Intel64 Family 6 Model 142 Stepping 9 0MHZ
Physical memory: Total physical memory:1023MB, Available memory:388MB
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Hard Disk: C:\ (NTFS)
CD-ROM Disk: D:\
Disk space: Total disk space:39G, The remaining disk space:15G
Group: tttt1

Updated the compared Date

Added Group ID in traffic
Who Are The Actor Behind These Campaigns?
**Roaming Tiger**

**Targeting Country:** UZ, MN, MY, RU, BY, KZ, US, Tibet, UA  
**Targeting Industry:** Gov, Oil and Gas, Aerospace, Defense  
**Malware:** SOGU, GHOST, TEMPFUN, FIRSTBLOOD, PI.

**APT15**

**Targeting Country:** PH, VN, TW, US, UK, IT, PL, UN, SG, NATO  
**Targeting Industry:** Gov, Political party  
**Malware:** ENFAL, ENDCMD, QUICKHEAL, SOGU, CYFREE, MIRAGE, NOISEMAKER, QUICKHEAL, SWALLOWFLY

**APT9**

**Targeting Country:** HK, US, SG, MY, JP, IN, KR, TH, TW  
**Targeting Industry:** Aerospace, Agriculture, Construction, Energy, Healthcare, High Tech, Media, Transportation  
**Malware:** BIGJOLT, FUNRUN, GH0ST, HOMEUNIX, JIM A, PHOTO, POISON, IVY, SKINNYGENE, SOGU, VICEROY, VIPSH ELL, WETHEAD, XDOOR, ZXSHELL
What About Other Campaigns?
Let’s Start Connecting the Dots!

Hint: links are either pdns or observed resolve
2014
Target KZ

2016 – 2017
APPER Campaign
C&C Infra Connected
(103.242.132.197)

2018
WATERFIGHT Campaign
C&C Infra Connected
(154.223.167.20, 45.77.134.195)

2019
SKYLINE Campaign

2015
Targets Tajikistan
C&C Infra Connected
(103.242.132.197)

C&C Infra Connected
(118.193.228.32)
Target TTP

2017
SOGU & QUICKHEAL targets KZ

C&C Infra Connected
(103.242.132.197)
Target TTP

Weak
Medium
Strong
Temp Group A

- Active since (at least): 2014
- Delivery method: Spear-phishing email
- Exploitation method: Malicious macro, RARSFX, CVE 2017-11882, CVE 2012-0158
- Target region: Russia, Kazakhstan, Tajikistan, Uzbekistan and Turkey
- Malware: ICEFOG-P, ICEFOG-M, SOGU, QUICKHEAL
- Connection to other group: Uses ICEFOG-P with the same PDB as Roaming Tiger.
Conclusion

- ICEFOG is malware shared among Roaming Tiger, APT15, Temp Group A and suspected APT9.
- Shared malware is a pitfall for attribution, we should not do attribution only based on malware.
- Temp Group A is aggressively using ICEFOG-P and ICEFOG-M to target Russia, Kazakhstan, Tajikistan, Uzbekistan and Turkey.
- With the file-less ICEFOG-M, host-based detection for payloads are more difficult.
- Continued development indicates there could be more attacks leveraging ICEFOG in future campaigns, and possibly leveraged by more attackers.