Between Hong Kong and Burma: Tracking UP007 and SLServer Espionage Campaigns

April 18, 2016

Tagged: Burma, Hong Kong, Malware, Targeted Threats

Categories: Jakub Dalek, Masashi Crete-Nishihata, Matthew Brooks, Reports and Briefings, Research News

By Matthew Brooks, Jakub Dalek, and Masashi Crete-Nishihata

Summary

In this research note, we analyze an espionage campaign targeting Hong Kong democracy activists. Two new malware families are used in this campaign that we name UP007 and SLServer.

The UP007 malware family was previously observed by Arbor Security Emergency Response Team (ASERT) in the report "Uncovering the Seven Pointed Dagger," which analyzes a set of samples that were hosted on the national level electoral commission of Myanmar (Burma): the Myanmar Union Election Commission. One of the samples analyzed was described as "unknown malware", which we call UP007 based on an identifier in the malware's network traffic. In a report released today, ASERT describes a series of campaigns targeting Tibetan, Hong Kong, and Taiwanese interests, which also includes details on the same UP007 sample we analyze.

A recent PricewaterhouseCoopers (PwC) report includes analysis of the SLServer sample we analyze (PwC refers to the family as SunOrcal). We refer to the malware as SLServer due to a resource dialog in the file. These previous reports collected samples from VirusTotal. We received the original email lure and samples used in the campaign from a targeted source, and found that both UP007 and SLServer were sent to targets in the same attack.

This research note builds on previous reporting by more closely examining UP007 and SLServer, variations of these samples found "in the wild", and the connections between these attacks and other campaigns. Previous reports have shown overlap in the tactics, techniques, and procedures used in this campaign in other operations targeting groups in Burma, Hong Kong, and the Tibetan community. We speculate that either a single threat actor is targeting these groups or some level of formal or informal resource sharing is occurring between the operators behind the campaigns.

Espionage Campaign Targeting Hong Kong Activists

In the week prior to the January 2016 Taiwanese General Election, Hong Kong-based pro-democracy activists received a targeted email purporting to come from a Taiwanese non-profit organization with information about the upcoming election. The email included a Google Drive link to a RAR archive file: "`2016總統選舉民情中心預測值.rar`", which translates to "Predictive Forecast from Centre of Public Sentiment in 2016 Presidential Elections.rar".

寄件者：[redacted]
日期：2016/1/7 10:22 上午
主旨：(涂謹申,黃之峰,张秀贤)收.
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).
收件者：[redacted]
副本：

2016大選進入最後關鍵10天，民進黨總統候選人蔡英文6日在中常會呼籲支持者將政黨票集中選票，她說，
這次政黨票的競爭真的非常激烈，很多人開始擔心如果選票分散，可能連第15、16名這2席都沒有把握了。

16日就將進行投票。除了總統選舉外，立委部分還有區域立委與不分區立委2項選舉。其中，不分區立委共有34席，民進黨上次選舉得到13席，這次支持度大漲，安全名單上看16席。不過，最近由於時代力量聲勢大漲，對民進黨造成威脅。

為了拉抬不分區立委聲勢，民進黨下午中常會則安排造勢活動。黨主席蔡英文表示，距離要投票只剩下10天，現在她最擔心的就是3件事情；第1個擔心就是賄選買票，讓民進黨的激
戰區被翻盤；第2個擔心是年輕朋友1/16會不會從外地返鄉去投票；第3個擔心是政黨票分散，讓不分區優秀的候選人落榜。
2016總統選舉民情中心預測值.rar
<hxxps://drive.google.com/file/d/0B-mV_7alj6P7UGhfVXRLSjRiS3M/view?usp=drive_web>

Figure 1: Targeting email sent to Hong Kong democracy activists

Translated Email Text:
To recipients: Jinshen Tu, Zhifeng Huang, and Xiuxian Zhang. The 2016 general election enters its crucial final 10 days, and 73 electoral districts conclude their voting (1041229); Centre of Public Sentiment's predicted forecast in the 2016 presidential elections (104.12.28).The 2016 Election enters its crucial final 10 days. On the 6th, Ing-wen Tsai, the DPP (Democratic Progressive Party) candidate, called on DPP supporters to consolidate their votes. She warned that the intense internal competition within the DPP had caused people to be worried about a splitting of the votes, potentially leading to the loss of the 15th and 16th seats.

The election day is on the 16th. Besides the presidential election, there is also the legislative election which includes district seats and non-district seats. There are 34 non-district seats in total, of which the DPP won 13 during the last election. Given the higher degree of support this time, the DPP should be able to secure 16 seats. But as the New Power Party's (NPP) influence and support grows, it might threaten the DPP.

In order to promote support for non-district legislators, the DPP Central Standing Committee organized a campaign event this afternoon. The chairwoman of the DPP, Ing-wen Tsai, said there are only ten days left before the election, and the three things she worried the most about were: 1) ballot bribery, which may cause DPP's loss in certain swing areas; 2) whether young people would return home to vote on Jan 16th; 3) vote splitting that may lead good candidates to lose in non-district legislative elections.

Predictive Forecast from Centre of Public Sentiment in the 2016 Presidential Elections.rar

Delivery Mechanism

We have observed the use of Google Drive links as a delivery vector in recent campaigns targeting Tibetan organizations. In these campaigns, Google Drive links were used to send malware and phishing pages. We have also seen the tactic used in recent espionage campaigns targeting an NGO working on environmental issues in Southeast Asia. The prior use of Google Drive as a delivery vector against Tibetan groups is significant, as Tibetan groups are promoting Google Drive as an alternative to sending file attachments to prevent infection from document-based malware.

Examining the RAR Archive

Within the linked RAR archive, the top three directories contain a mix of malicious and benign documents, as well as shortcuts that run two executables that are deeply nested within hidden directories in the archive. The file structure of this archive is shown in Figure 2.

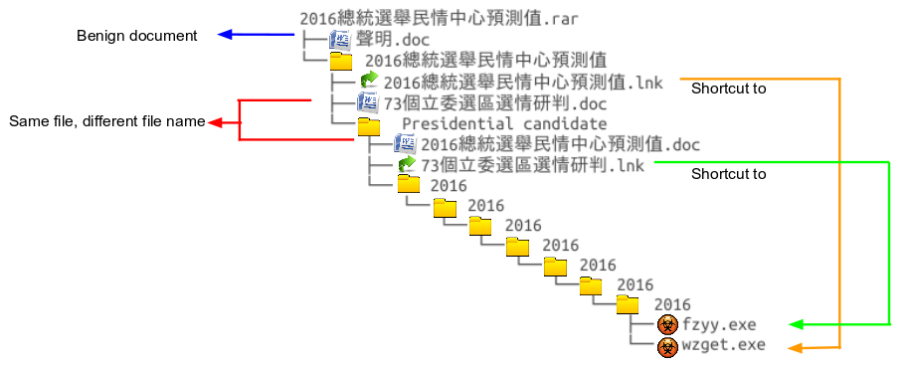

Figure 2: File structure of delivered RAR archive.

The top level directory of this archive contains a benign Word document named 聲明.doc, which translates to "Statement.doc". The text of this document is written in Chinese and is related to the Taiwanese election.

Document Text:
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).
文件內容僅代表個人立場，僅供參閱。解壓選舉民情中心預測值到桌面即可查閱全部數據.

English Translation:
Election polling of 73 legislative electoral districts（12/29/104).
Predicted forecast from Centre of Public Sentiment in the 2016 presidential elections (12/28/104).
All the documents represent personal views and are for reference only. Unzip Election Polling Centre's forecast to the desktop to view all data.

The first two directories contain separate Windows shortcuts, each of which runs an executable that is nested down in seven hidden subdirectories. Table 1 shows details of the two executables contained in this nested directory along with their detection rate by antivirus vendors according to VirusTotal.

Filename	Sample MD5	AV Detection Rate
`fzyy.exe`	d579d7a42ff140952da57264614c37bc	Date / Time: 01-11-2016 Detection Rate: 8/55
`wzget.exe`	d8becbd6f188e3fb2c4d23a2d36d137b	Date / Time: 03-21-2016 Detection Rate: 30/57

Table 1: Sample overview

These samples, when executed, create two separate infection chains. The lack of emphasis on tricking targets into running a single malicious file is interesting. We are unsure as to why the operators chose to deploy two separate infection chains within the same delivery mechanism. It is also unclear why the benign document was included at the top directory, as this would require more user interaction for a compromise to be successful. It is possible that this mixture of benign and malicious files is intended to lull the targets into a false sense of security.

Within the archive there are two Microsoft Word files: `2016總統選舉民情中心預測值.doc` (translation: "Predictive forecast from Centre of Public Sentiment in 2016 Presidential Elections") and `73個立委選區選情研判.doc` (translation: "Election polling of 73 legislative electoral districts"). Despite having different filenames, they are the same file (MD5 hash: 09ddd70517cb48a46d9f93644b29c72f). This infected document was analyzed in the recent PwC report and the malware family was named SunOrcal by the researchers. In this report we take a closer look at the two nested executables: `fzyy.exe` and `wzget.exe` and the two separate infection chains they produce.

UP007 Malware Family

The `fzyy.exe` executable is a dropper responsible for creating multiple files and starting this particular infection chain. When the file is run it creates the following files in the directory: `%APPDATA%\Microsoft\Internet Explorer\`

Filename	MD5	Purpose
`conhost.exe`	f70b295c6a5121b918682310ce0c2165	Loads `SBieDll.dll`
`SBieDll.dll`	f80edbb0fcfe7cec17592f61a06e4df2	Loads `maindll.dll`
`maindll.dll`	d8ede9e6c3a1a30398b0b98130ee3b38	Loads `dll2.xor`
`dll2.xor`	ce8ec932be16b69ffa06626b3b423395	Payload
`runas.exe`	6a541de84074a2c4ff99eb43252d9030	Establishes persistence; Not utilized in this loading chain
`nvsvc.exe`	e0eb981ad6be0bd16246d5d442028687	Unknown – possibly older component

Table 2: Executable infection chain for `fzyy.exe`

These files are all initially stored as resources within `fzyy.exe`. Some of the files are stored in encoded form while `maindll.dll` is stored as a packed executable. When writing the files to disk, the dropper will decode and write the files stored in encoded form. In addition the infection chain will check multiple registry keys before writing `maindll.dll`.

The keys largely seem to check for the presence of popular Chinese antivirus products: 360 Security, Kingsoft Antivirus, Rising AV, Jiangmin, and Micropoint as well as a popular free antivirus product Avira. Interestingly, in this instance, even if the registry keys are present, maindll.dll will still be written and the infection chain will still continue. The registry keys that are checked by the infection chain are summarized in Table 3.

Key	Subkey
`HKLM\SOFTWARE\360Safe\Liveup`	`curl`

HKCU\Software\360safe	DefaultSkin
HKLM\SOFTWARE\kingsoft\Antivirus	WorkPath
HKLM\SOFTWARE\Avira\Avira Destop	Path
HKLM\SOFTWARE\rising\RAV	installpath
HKLM\SOFTWARE\JiangMin	InstallPath
HKLM\SOFTWARE\Micropoint\Anti-Attack	MP100000

Table 3: Registry keys that `fzyy.exe` checks for before writing `maindll.dll`

Once all the files are created, `conhost.exe` starts, loads `SBieDll.dll`, then ultimately loads `maindll.dll` and the final payload, which we have named UP007 (`dll2.xor`) due to an identifier in the network traffic. The primary function of UP007 appears to be to log keystrokes to the `%USERPROFILE%\Local Settings\Temp\keylog\` directory and send them to a remote server.

UP007 uses Windows Sockets to communicate with its command and control server (C2). While doing so, it sends a hardcoded HTTP header disguised as Microsoft Update traffic. This is likely an attempt to escape notice by casual inspection of network traffic. On connection, UP007 downloads another payload directly from the C2 server. This secondary payload we have named "DownLoad" given the way it identifies itself in the traffic with the C2 server. This secondary payload is injected into memory. The initial network traffic observed from the UP007 sample is seen in Figure 3.

```
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
UP00700:FF:49:03:DD:2
6.....
HTTP/1.1 200 OK
Server: Microsoft-IIS/6.0
Content-Type: text/html
Content-Length: 2

OKHTTP/1.1 200 OK
Server: Microsoft-IIS/6.0
Content-Type: text/html
Content-Length: 4

....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.

$.....JZO..ZO..ZO..li..RO...S..LO..li..>O..ZO...O..8P..WO...P..AO...P..
[O..RichZO.....PE..L...K4TU.....!.....z.....
F.....`.....
w.....@..`
.....text.....
```

Figure 3: Network capture of the initial communication by UP007.

Once the entire payload is received from the C2 server, UP007 sends basic system information such as operating system version, IP address, and username and the C2 responds with a "READY" announcement (see Figure 4).

```
okPOST /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

00-FF-49-03-
DD-26.....WINXP.....use
r.....XP.....10.0.2.
15.....admin||
090
2.....
@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

READYHTTP/1.1 200 OK
```

Figure 4: Network capture of the infected system sending system information to the C2.

The secondary payload (DownLoad) initiates its own separate TCP connection with the C2 server. A sample of the network traffic of this secondary payload is seen in Figure 5.

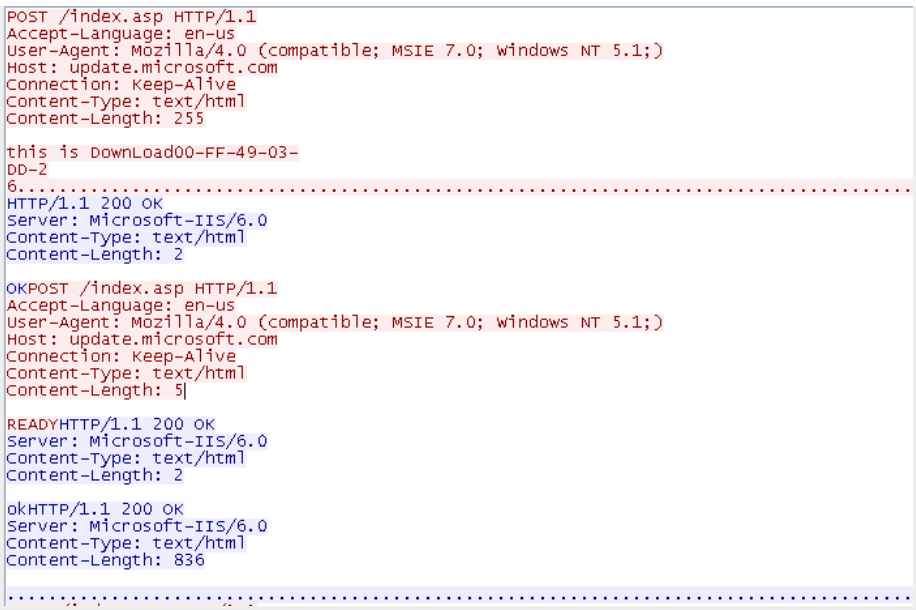

Figure 5: Network capture of DownLoad connection to the C2.

Unfortunately, even though the connection with the C2 was established, we did not observe any further activity from this payload. However, DownLoad's strings show references to the following:

```
this is cmd
this is Desktop
```

It is possible these are in reference to additional components or capabilities of the malware. Further analysis is required to determine the function of these components.

UP007 Command and Control Infrastructure

The command and control server for the UP007 sample is hosted on Hong Kong provider New World Telecom at the IP address `59.188.12[.]123`. Passive DNS data from PassiveTotal indicates that the domain name `yeaton.xicp[.]net` pointed to this IP from January 8 2016 to March 19 2016. In their recent report ASERT notes that the domain: `yeaton.xicp[.]net` was used to advertise a Chinese VPN service in 2012. However, as ASERT explains given the long period between the use of the domain for advertising and the recent threat activity the past uses of the domain may not be related to the threat actors.

UP007 Samples and Variations

In November 2013, an exploit document (MD5: 983333e2c878a62d95747c36748198f0) was uploaded to various malware sites with the filename 中国国家安全委员会机构设置和人员名单提前曝光`.docx` (which translates to "Chinese National Security Council's Institutional Structure and Member list") and `131106 minutes.docx`. Instead of receiving the Stage 2 binary in the C2 protocol as in the recent UP007 sample, the November 2013 sample directly requested `ok.exe` via an HTTP GET request to `103.19.85[.]89`. The `ok.exe` sample communicated with `tenday.mysecondarydns[.]com` which resolved to `103.19.85[.]89`. It was signed with a certificate with serial number `04 DE 6E CB 4B A2 A5 54 2B 5E 0C 71 EE FD 2A AA`.

One year later, in November 2014, another instance of the UP007 dropper (MD5: e2ac89b5c820fc598b92a635a7d8bc33) signed with a certificate using the serial number `3A 72 A8 34 FB EC E5 4F A5 E5 2F 67 BA 63 4D CA` was uploaded to VirusTotal. According to VirusTotal, this file was observed being hosted at `http://103.19.85[.]89/chin.jpg`. The final payload was designed to communicate with the same host for command and control.

In August 2015, an instance of the UP007 dropper (MD5: 639c7239f40d95f677a99abb059e8338) signed with the same certificate (Serial: `5D 11 78 4F B8 17 65 02 3F 89 A4 F4 24 3F E1 A9`) as `fzyy.exe` was uploaded to VirusTotal spotted in the wild as `http://hkemail.f3322[.]org/32.zip`. This sample communicated with `hk2[.]upupdate[.]cn` which resolved to `103.27.108[.]122` at the time of analysis.

The samples detailed in Table 4 were identified by import hash and other structural similarities related to the UP007 dropper. They were uploaded to VirusTotal by the same submitter on November 14, 2014 and February 27, 2015. They were signed with the same `3A 72...4D` CA and `5D 11...E1 A9` certificates, respectively.

MD5	Import Hash	C2
21455a5c2496e2603f6ba911fbaaed80	820438f3f1efede11425a9cc13ae2dbd	hihihihihahaha.vicp[.]cc (113.204.17[.]59)
be378f3d66ecd38cda09508015de71f7	820438f3f1efede11425a9cc13ae2dbd	172.16.10[.]124

Table 4: UP007 Variants

The RAR archive detailed in Table 5 reportedly drops the same files responsible for loading the UP007 sample. It also reportedly communicates with `59.188.12[.]123`. We have not been able to obtain this sample directly.

MD5	File Name	C2
19866e7566373028799abd6844ac16d1	`QiHua.rar`	219.133.40[.]1, 59.188.12[.]123

Table 5: UP007 Variants

SLServer Malware Family

The SLServer sample we received was also recently analyzed and reported by PwC. It was presented in an overview of threat actors making use of the recent Taiwanese presidential election in email lures to entice targets to open malicious documents. As noted by PwC, this file is a self-extracting archive ultimately responsible for downloading a binary from a website that was likely compromised. Like PwC, we were unable to obtain the final `Keyainst.exe` binary due to the behaviour of the C2 during the time of analysis.

Based on common behavioural characteristics and shared C2 it appears the downloaded file analyzed by PwC was MD5: e5e7dcbda781dd0bf5f5da3cccdb094d. This sample was referred to as SunOrcal by PwC. This name was based on a folder misspelling. We refer to the malware family as SLServer due to a resource dialog in the file (see Figure 6).

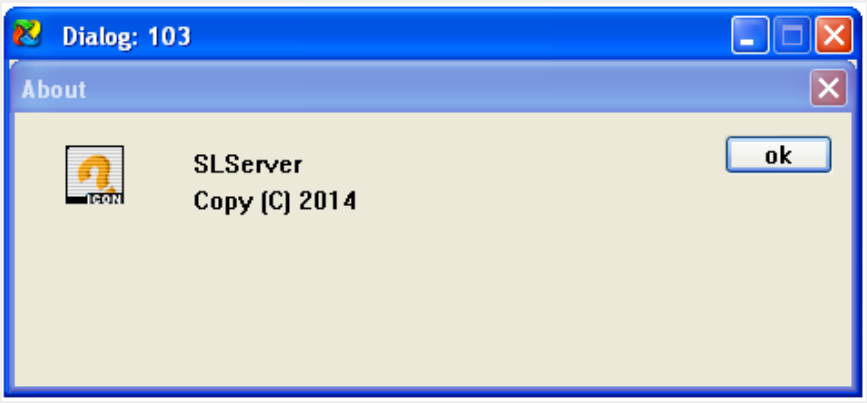

Figure 6: SLServer dialog resource.

Another recently observed instance of this malware found on VirusTotal (MD5: cfcd2a90e87156e1a811f9c7b0051002) was designed to communicate with the same C2 server and contains the following debug path:

```
e:\Working\SVNProject\SLServer\SLServer2.0\release\SLServer.pdb
```

Interestingly, according to VirusTotal, the previously mentioned UP007 dropper `fzyy.exe` was also observed hosted as `wthk.txt` at the same URL as this downloaded SLServer sample. The precise timeframes during which these samples were hosted and changed remains unknown. Table 6 shows the timestamps of their initial upload to VirusTotal.

File Name	Malware Family	MD5	First Submission Time
wzget.exe	SLServer	e5e7dcbda781dd0bf5f5da3cccdb094d	2016-01-07 19:03:25 UTC
fzyy.exe	UP007	d579d7a42ff140952da57264614c37bc	2016-01-08 05:21:18 UTC

Table 6: Times for Sample Upload to VirusTotal

SLServer – Possible Second Stage

The SLServer sample (MD5: e5e7dcbda781dd0bf5f5da3cccdb094d) calls "`FunctionWork`" from a `DLL`:

```
loc_408BCB:                             ; CODE XREF: sub_408860+344↑j
                push    offset aFunctionwork ; "FunctionWork"
                mov     ecx, [ebp+hModule]
                push    ecx             ; hModule
                call    ds:GetProcAddress
                mov     [ebp+var_38C], eax
                call    [ebp+var_38C]
```

On VirusTotal we discovered a file named `javaupdata.dll` (MD5: 7332245f67b6b8a256ab22a6496b4536), which exports a function by the same name. Strings in the SLServer sample also reference a file by this name. When executed, this `DLL` contacts `210.61.12[.]153` using SSL. This host is the same one pointed to by the SLServer's C2 domain, `safetyssl.security-centers[.]com`. Interestingly, while the `210.61.12[.]153` host did not respond to the SLServer connections during analysis time, the host did accept the SSL connections from `javaupdata.dll`. Further analysis of this file is ongoing.

SLServer Command and Control Infrastructure

The SLServer C2 server: `safetyssl.security-centers[.]com` resolved to the IP address: `210.61.12[.]153` at the time of analysis. This IP is hosted in Taiwan on the hosting provider Chunghwa Telecom, specifically their Data Communication Business Group offering. It appears to host the site of a Taiwanese auto parts manufacturer, Yowjung Autoparts. This site may have been either compromised or copied from a legitimate source.

The domain name `security-centers.com` was registered on September 11 2015 by the e-mails: `janmiller-domain@googlemail[.]com` and `an_ardyth@123mail[.]org`. Using Passive DNS data we find the following subdomains were used in the time period after domain registration:

```
safetyssl.security-centers[.]com
computer.security-centers[.]com
security-centers[.]com
www.security-centers[.]com
```

The domain `computer.security-centers[.]com` was a C2 server previously reported by ASERT related to a sample of the Trochilus RAT analyzed in the report. ASERT retrieved that sample from the compromised Myanmar Union Election Commission website. The other subdomains (www and the the top level `security-centers[.]com`) are likely the default IP addresses for GoDaddy registered domains. The hosting information for this infrastructure is presented in the Figure 7.

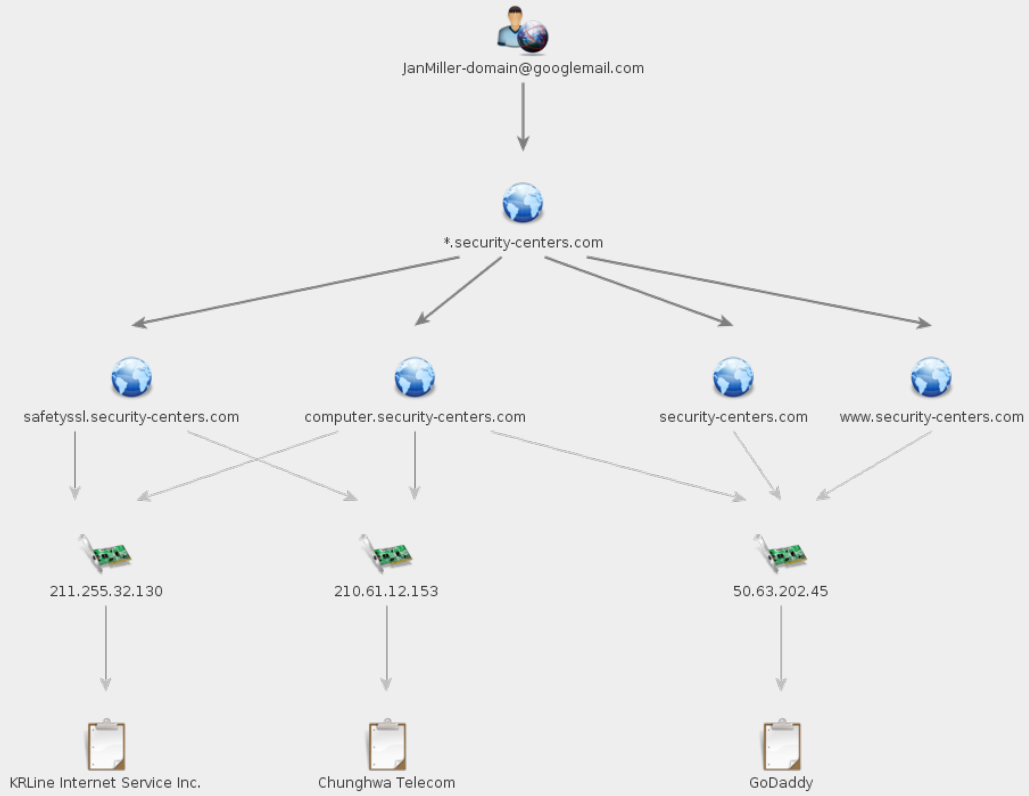

*Figure 7: Hosting infrastructure over time for *.security-centers[.]com*

SLServer Samples and Variations

We discovered three additional SLServer samples using VirusTotal. We list the hash, submission time, as well as C2 domains associated with the sample in Table 7.

MD5	First Submission	C2
d07b2738840ce3419df651d3a0a3a246	2016-02-25 01:14:15	www.olinaodi[.]com (74.126.181[.]10)
397021af7c0284c28db65297a6711235	2016-02-22 18:30:19	safetyssl.security-centers[.]com (210.61.12[.]153)
dc195d814ec16fe91690b7e949e696f6	2016-02-17 11:32:02	www.olinaodi[.]com (74.126.181[.]10)
cfcd2a90e87156e1a811f9c7b0051002	2015-11-09 05:20:33	safetyssl.security-centers[.]com (211.255.32[.]130)

Table 7: SLServer Variants Overview

Recent Campaign Connections

In January 2016, Arbor Networks released a report titled "Uncovering the Seven Pointed Dagger" in which they discuss a series of six RAR files hosted on the Myanmar election commission website on 20 October 2015. The focus of the report was on the discovery of the new Trochilus RAT. However, one of the RAR files was noted as unknown malware. This sample (`Security-Patch-Update.exe`, MD5: 82896b68314d108141728a4112618304) is also UP007, signed with the `5D 11 78 4F B8 17 65 02 3F 89 A4 F4 24 3F E1 A9` certificate and configured to communicate with `59.188.12[.]123` directly over port 8008, identical to `fzyy.exe` mentioned above. In this instance, if any of the previously discussed registry keys were present, the sample will execute the dropped `runas.exe` binary. Given this execution, `nvsvc.exe` is likely also an older component. As discussed above the UP007 sample we analyzed shares the same C2 (`computer.security-centers[.]com`) as the Trochilus RAT sample reported by ASERT.

In November 2015, Palo Alto Networks reported on a newly discovered trojan referred to as Bookworm. They revealed a campaign focused on the targeting of government entities in Thailand. The campaign used a malware family known as FFRAT, and the sample described in the report connected to the domain `hkemail.f3322[.]org` for command and control. In August 2015, the same domain was reportedly used to host an instance of UP007 as well.

Finally, the relationship between the SLServer C2 www.olinaodi[.]com and our previous research into the Surtr malware family was highlighted by PwC through the overlap in the `toucan6712@163[.]com` registrant. We tracked malware campaigns using the Surtr family that have targeted Tibetan organizations since 2013.

Conclusion

This latest espionage campaign against Hong Kong activists appears to be connected to a broader set of targets, and operations. The recent detailed reporting by ASERT makes it clear that the UP007 malware family has been found in previous campaigns targeting Burmese interests. In addition, the campaigns share some C2 infrastructure with previous operations against targets in Thailand and the Tibetan community. The domain registration connections between SLServer infrastructure and Surtr infrastructure also suggests some level of potential coordination between campaigns targeting Hong Kong groups and the Tibetan community. Despite these connections, it is unclear if these campaigns are being conducted by the same threat actor.

We cannot exclude the possibility that distinct operators have a degree of sharing of tools and infrastructure. Alternatively, security researcher Ned Moran has articulated a concept of a "digital quartermaster," to refer to an actor that supplies threat infrastructure and malware development resources to multiple groups. While these scenarios are plausible, we do not have enough data to properly assess these competing hypotheses, or to make conclusive statements about the identity of the threat actors.

What is clear from our analysis is that civil society groups across Asia continue to be targeted by persistent and organized cyber espionage campaigns. Civil society often lack the resources and awareness to defend against these operations and closer attention to the threats they face is needed.

Acknowledgements

Special thanks to Valkyrie-X Security Research Group and ASERT. We are grateful to Jason Q. Ng and Kun Cleo Zhang for translation assistance, and Adam Senft, John Scott-Railton, and Ron Deibert for comments.

This research was supported by the John D and Catherine T. MacArthur Foundation and the William and Flora Hewlett Foundation.

Indicators of Compromise

Yara signatures are available for the UP007 and SLServer malware families here

MD5 Hashes

```
d579d7a42ff140952da57264614c37bc
d8becbd6f188e3fb2c4d23a2d36d137b
09ddd70517cb48a46d9f93644b29c72f
f70b295c6a5121b918682310ce0c2165
f80edbb0fcfe7cec17592f61a06e4df2
d8ede9e6c3a1a30398b0b98130ee3b38
ce8ec932be16b69ffa06626b3b423395
6a541de84074a2c4ff99eb43252d9030
e0eb981ad6be0bd16246d5d442028687
639c7239f40d95f677a99abb059e8338
d07b2738840ce3419df651d3a0a3a246
397021af7c0284c28db65297a6711235
dc195d814ec16fe91690b7e949e696f6
cfcd2a90e87156e1a811f9c7b0051002
```

IP Addresses

```
59.188.12[.]123
210.61.12[.]153
```

Domains

```
safetyssl.security-centers[.]com
computer.security-centers[.]com
hkemail.f3322[.]org
www.olinaodi[.]com
tenday.mysecondarydns[.]com
```