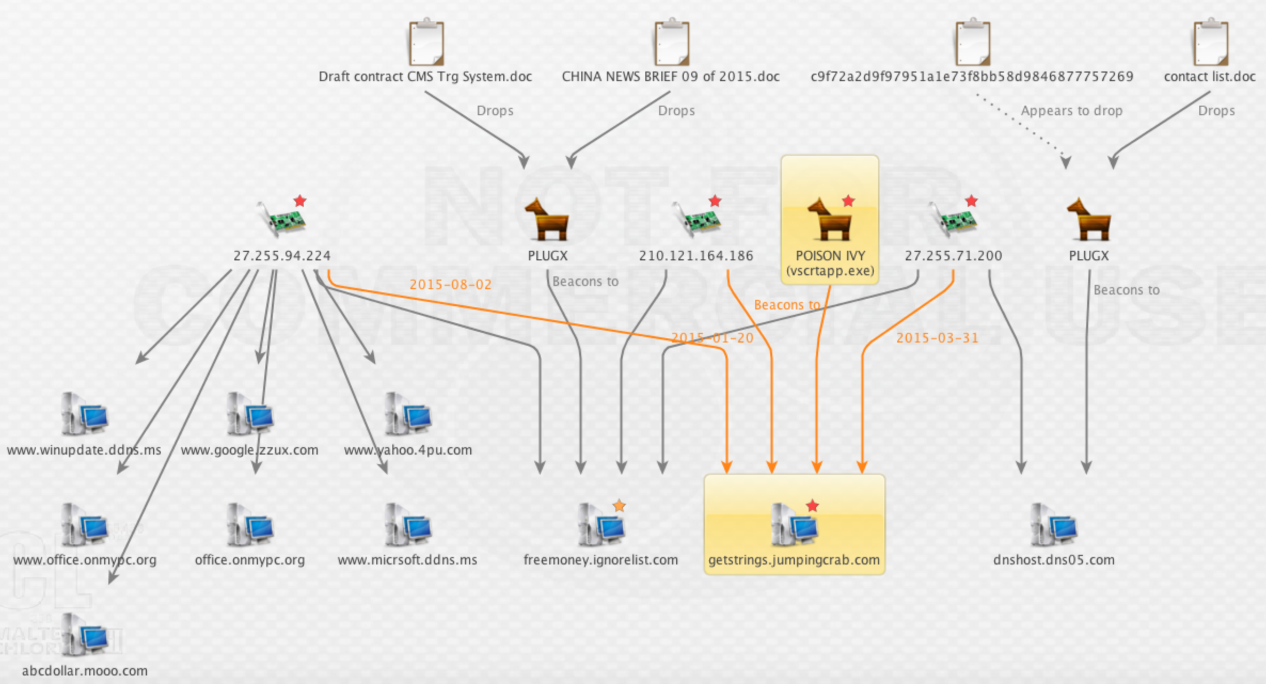
in Analysis

Threat Analysis: Poison Ivy and Links to an Extended PlugX Campaign

Key Points & Assessment:

- Japan CERT identified a new Poison Ivy RAT variant (**SHA1 44073031790e5ba419374dc55f6ac1cba688b06c**) with updated C2 functionality.
- The malware was created in September 2014 and uploaded to Virus Total in January 2015. It uses the dynamic DNS-provided C2 **getstrings[.]jumpingcrab[.]com**. This domain has resolved to at least 3 IP addresses: **210.121.164.186**, **27.255.71.200**, and **27.255.94.224**.
- I identified several decoy documents (see Maltego graph) that deliver the PlugX malware and call-out to one of two IP addresses mentioned above. These documents were reportedly used in a campaign identified by SOPHOS that spanned from September 2014 to February 2015. India was one target of the campaign.
- Given the infrastructure and timing overlaps, the Poison Ivy sample discussed in this post was likely just one payload involved in a broader campaign targeting India, the Tibetan community, and others, that spanned from approximately September 2014 to February 2015.
- The Poison Ivy sample in this case thus appears to be tied to

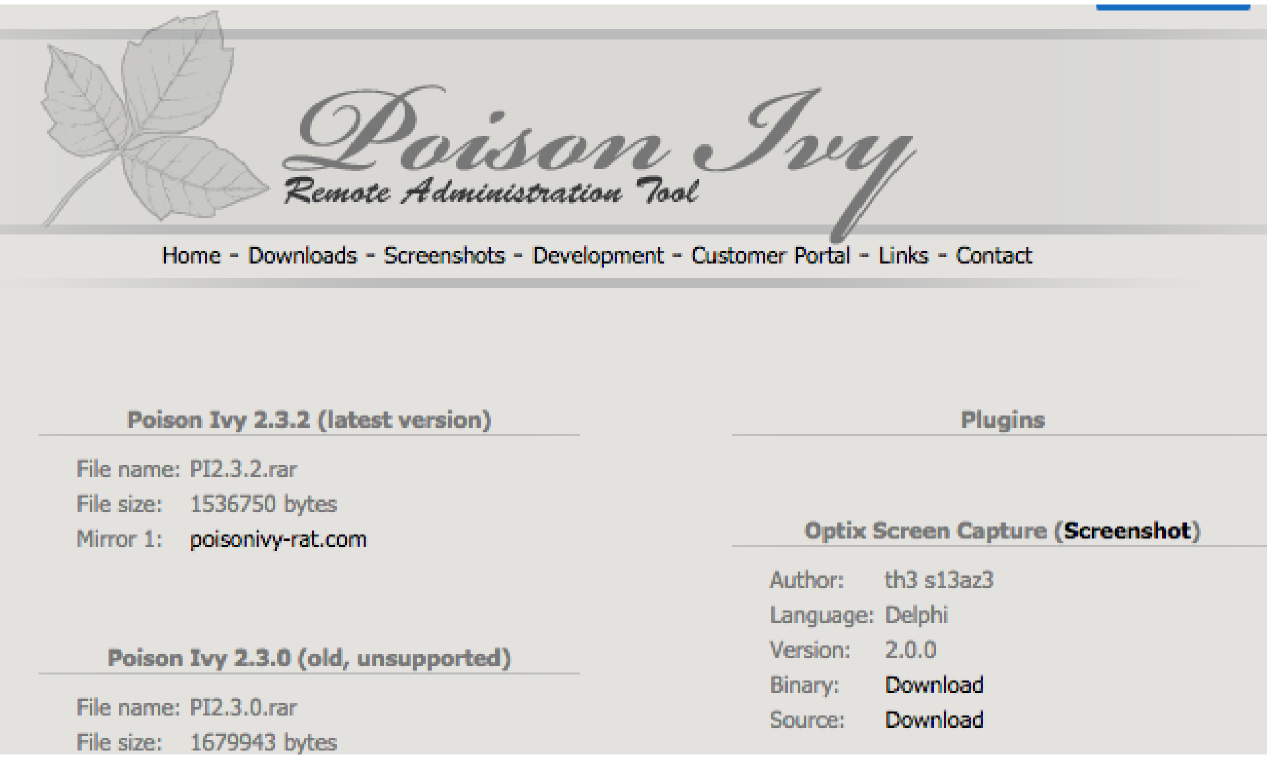
attacks by one or more adversaries acting on behalf of Chinese interests.



Poison Ivy: New C2 Proxy Functionality

Poison Ivy (PIVY) is a well-known, fully-featured remote access tool (RAT) that has existed since about 2005. It offers a user-friendly GUI, a variety of plugins to enhance functionality, and can be found online by any prospective attacker.

And, although anyone can acquire the tool, PIVY is often associated with actors who have a nexus to China.


Poison Ivy
Remote Administration Tool
Home - Downloads - Screenshots - Development - Customer Portal - Links - Contact

Poison Ivy 2.3.2 (latest version)

File name: PI2.3.2.rar
File size: 1536750 bytes
Mirror 1: poisonivy-rat.com

Poison Ivy 2.3.0 (old, unsupported)

File name: PI2.3.0.rar
File size: 1679943 bytes

Plugins

Optix Screen Capture (Screenshot)

Author: th3 s13az3
Language: Delphi
Version: 2.0.0
Binary: Download
Source: Download

The malware has been extensively documented–including its use in espionage-motivated intrusions–and continues to show signs of active development [1]. A recent blog post from Japan CERT (JPCERT) details new Poison Ivy communications functionality. According to JPCERT, the malware now uses HTTP POST requests (earlier variants use a custom HTTP CONNECT request method) and supports proxy authentication to command-and-control (C2) servers.

Because JPCERT has already tackled this variant's communications functionality, I will examine other aspects of the malware.

File & Execution Details

Unfortunately, we do not know the delivery vector or target. The intended target may have been one or more Japanese organizations, given that JPCERT was the first to dissect this PIVY sample. Alternatively, it is just as likely that JPCERT simply observed attacks against other victims.

```
File Name: vscrtapp.exe
File size 67.0 KB (68608 bytes)
MD5 1aca09c5eefb37539e86ec86dd3be72f
```

```
SHA1 44073031790e5ba419374dc55f6ac1cba688b06c
SHA256 d1aa00b6b11fbefd2dda3b458d9fb5e975865b564bf1c289a6f464b14ad748cc
imphash 6fcb46b0cf3f3baf36d97eba47832406
Compilation timestamp 2014-09-14 01:30:49
First submission 2015-01-19 11:03:27 UTC ( 6 months, 1 week ago )
```

The sample will write the file **vscrta0ps.log** to C:\Documents and Settings\All Users\AppData\. There appear to be no legitimate applications that would write this file to disk.

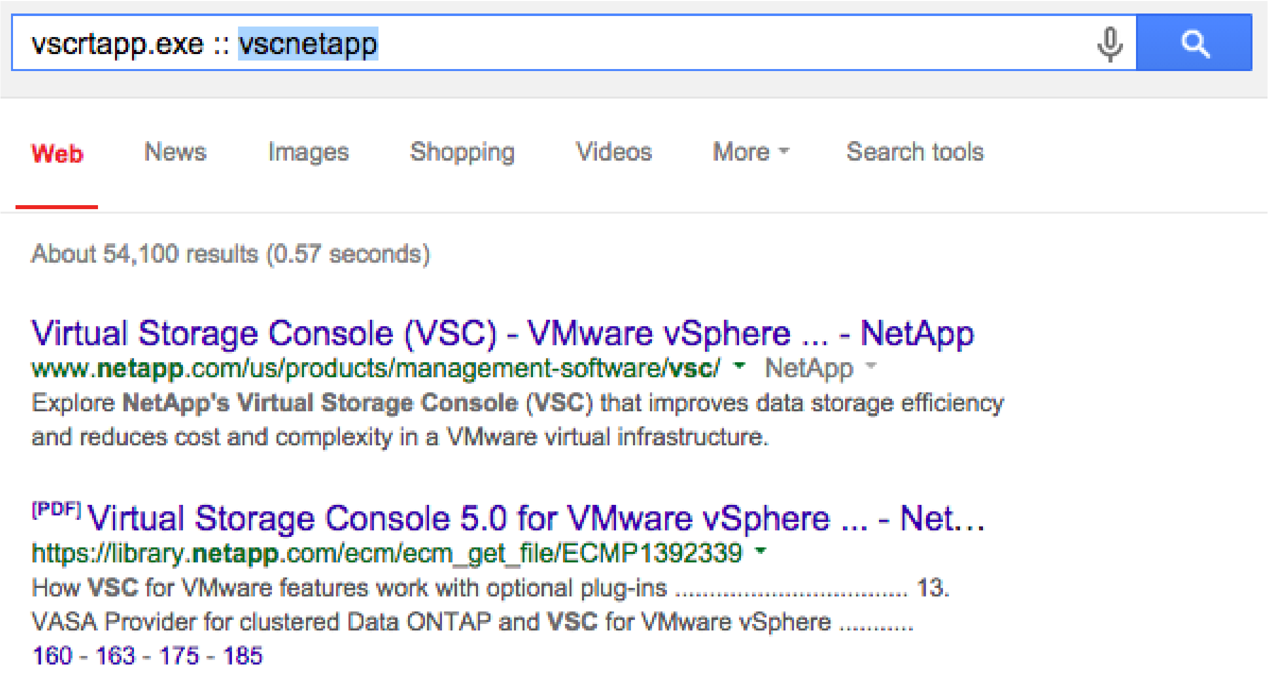
```
C:\Documents and Settings\All Users\AppData\vscrta0ps.log
```

It will also run the below command:

```
 schtasks /create /sc minute /mo 1 /tn Update Assist" /tr "\"C:\Do
cuments and Settings\All Users\AppData\vscrtapp.exe\"" /ru "system
""
```

This command will create a scheduled task named “Update Assist.” I assume this is a non-English speaker’s attempt to create an “Update Assistant” task name. This task will run the malware every minute on the victim’s machine as **vscrtapp.exe** in the %AppData% directory. The task therefore serves as a basic method of persistence, ensuring that the malware runs regularly. I found no indications that the malware creates any registry keys; the scheduled task appears to be the malware’s only means of persistence.

It is not clear what, if any, legitimate EXE **vscrtapp.exe** is attempting to mimic. One possibility may be NetApp’s Virtual Storage Console (VSC) for VMWare (note that the below image is not the query I ran; I simply wanted to show the similarity between the names). Although developers of PIVY could easily change the name, the presence of the **vscrtapp.exe** filename could serve as a simple host-based method of detection.



vscrtapp.exe :: vscnetapp

About 54,100 results (0.57 seconds)

Virtual Storage Console (VSC) - VMware vSphere ... - NetApp
www.netapp.com/us/products/management-software/vsc/ NetApp
Explore **NetApp's Virtual Storage Console** (**VSC**) that improves data storage efficiency and reduces cost and complexity in a VMware virtual infrastructure.

[PDF] Virtual Storage Console 5.0 for VMware vSphere ... - Net...
https://library.netapp.com/ecm/ecm_get_file/ECMP1392339
How **VSC** for VMware features work with optional plug-ins .... 13.
VASA Provider for clustered Data ONTAP and **VSC** for VMware vSphere ....
160 - 163 - 175 - 185

The malware will set a mutex (it imports the function CreateMutexA), although I was unable to determine the value.

PIVY Infrastructure

C2 communications will be made to **getstrings[.]jumpingcrab[.]com** using HTTP POST requests. It is important to note that the domain jumpingcrab[.]com is a dynamic DNS (DDNS) service. While not inherently malicious, DDNS providers are often abused by threat actors so they do not have to rely on static infrastructure; IP resolution for a host could change at any time.

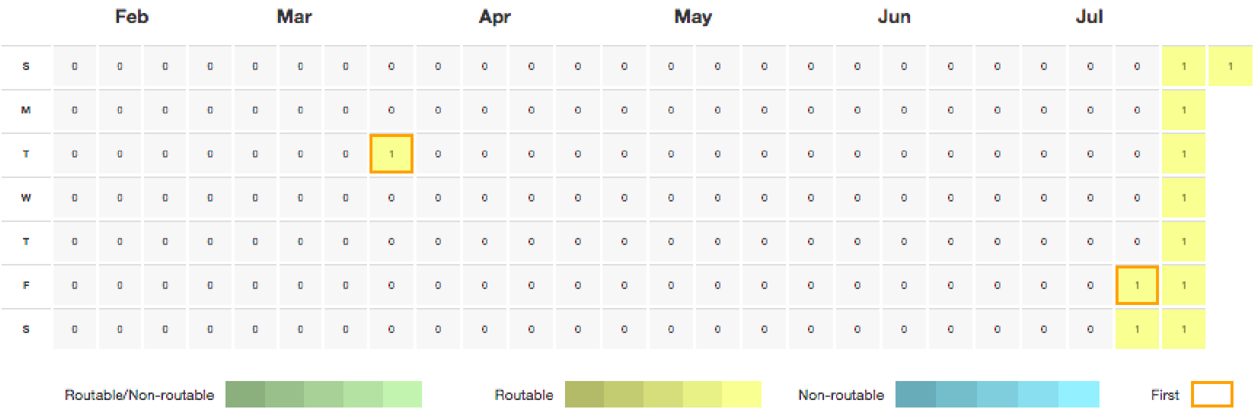
Analysis of an attacker's infrastructure is thus made more difficult. The use of DDNS also means that the relevancy and reliability of any infrastructure pivots must be carefully considered.

Taking the use of DDNS into consideration, here are current and historical resolutions for **getstrings[.]jumpingcrab[.]com** (courtesy of PassiveTotal):

```
 Resolve Location Network First Last
27.255.94.224 KR 27.255.94.0/24 2015-07-24 00:00:00 2015-08-02 15:
```

```
47:31
27.255.71.200 KR 27.255.71.0/24 2015-03-31 20:29:15 2015-03-31 20:
29:15
210.121.164.186 KR 210.121.128.0/17 2015-01-19 23:16:35 2015-01-20
 04:36:15
```

The timing of the earliest known resolution–**210.121.164.186**–directly correlates with the first submission time of the sample. The Passive Total heat map (shown below) tells us there were almost no active resolutions for this host from February until late July suggesting that the adversary may have observed the submission and deactivated DNS for the host on or around January 19. (Unfortunately, the 12 day gap between January 19 and the beginning of February is an unknown.)



		Feb				Mar				Apr				May					Jun				Jul			
S	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
M	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	
T	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	
W	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	
T	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	
F	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	
S	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	

The host briefly resolved to **27.255.71.200** for one day in March and, as of publication, points to **27.255.94.224** where we see eight additional hosts (which also use DDNS domains):

```
 www.yahoo.4pu.com
www.google.zzux.com
www.winupdate.ddns.ms
freemoney.ignorelist.com
www.micrsoft.ddns.ms
office.onmypc.org
www.office.onmypc.org
abcdollar.mooo.com
```

Both **winupdate[.]ddns[.]ms** and **www[.]micrsoft[.]ddns[.]ms** are undoubtedly attempting to resemble legitimate Windows and Microsoft sites, respectively. However, it is unknown if any of these hosts are related to the actors who created **getstrings[.]jumpingcrab[.]com**.

Related Threat Activity

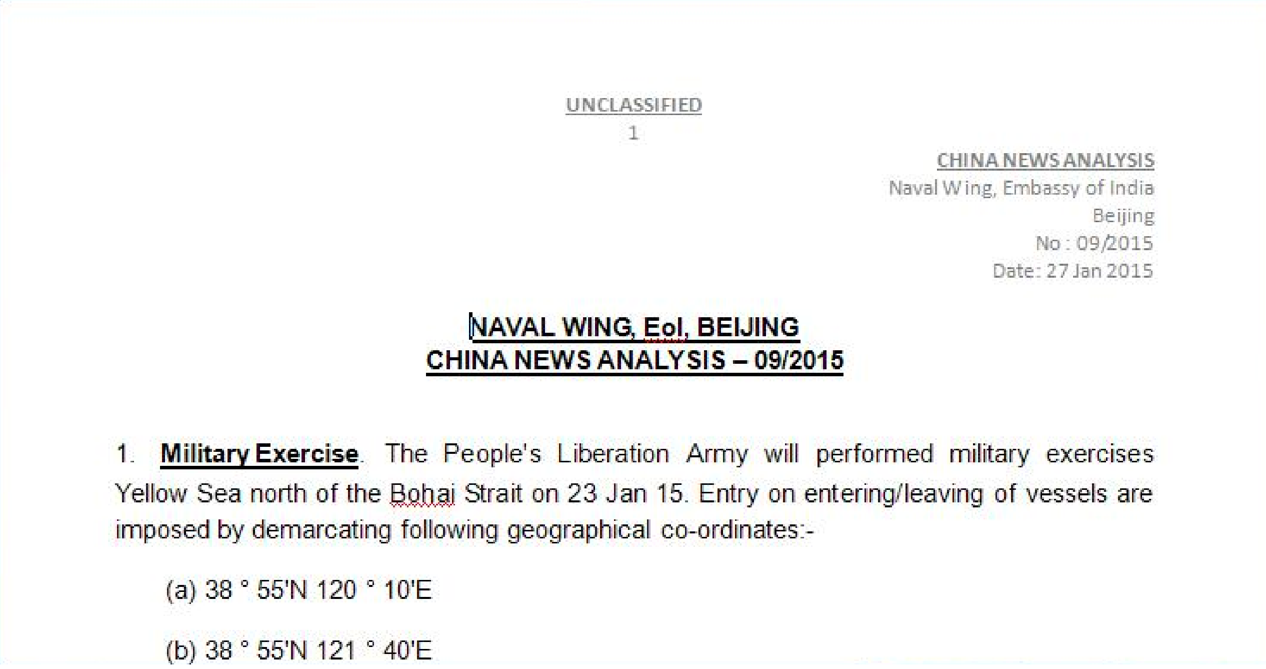
There are several documents that appear to target victims interested in Chinese affairs, attempt to install the PlugX malware (aka Korplug, SOGU), and communicate to two of the above identified IP addresses (**210.121.164.186** or **27.255.71.200**). PlugX is another ubiquitous RAT commonly linked to Chinese threat actors.

Below are the documents and their relevant metadata (some details were not available).

```
CHINA NEWS BRIEF 09 of 2015.doc
MD5 9d0388251cbaf3648aba463f66a8fee8
SHA1 a4602a357360b0ed8e9b0814b1322146156fb7f6
SHA256 89ab2d9643bdefd6d46618b2f11fb1357bb555a0e33d5d8fc8bb33eba3fe7cc3
Create Time/Date: Wed Sep 3 02:25:00 2014
First submission 2015-01-30 04:44:34 UTC ( 6 months, 1 week ago )
C2:freemoney.ignorelist.com (210.121.164.186)

################################

Draft contract CMS Trg System.doc
MD5 5bb6be7fcddcd1cc51957ebc17ed872a
SHA1 03b2a660d68004444a5189173e3b8001f4a7cd0b
SHA256 add84116acee953f6606a2240059a05fb4658cfacdee6dd75be752e183c5cab7
Create Time/Date: Fri Jan 30 02:41:00 2015
First submission 2015-02-01 09:49:08 UTC ( 6 months, 1 week ago )
C2:freemoney.ignorelist.com (210.121.164.186)

################################

(Appears to have multiple filenames)
MD5 29a3b53eb1008af2fccbf34df3b68aca
SHA1 c9f72a2d9f97951a1e73f8bb58d9846877757269
C2:dnshost.dns05.com (27.255.71.200)

################################

contact list.doc
Title: Suggested Invitees for Ambassador
MD5 971d49f78387e47fa57a13080b8d317f
```

```
SHA1 f4342ac81450c119429b1b9363fa5e941b0c4266
SHA256 58c6e1bbb1c70568476aeec1471ddba74f1fbd31beb1fff471434d3042ee315d
Create Time/Date: Mon Jul 19 07:59:00 2010
C2:dnshost.dns05.com (27.255.71.200)
```

Two of the above RTF files (**CHINA NEWS BRIEF 09 of 2015.doc** and **Draft contract CMS Trg System.doc**) exploit CVE-2012-0158 to install PlugX (aka Korplug/SOGU), which then calls to **210.121.164.186**, the IP that **getstrings[.]jumpingcrab[.]com** pointed to in January. The "China News Brief" document is shown below.



UNCLASSIFIED
1

CHINA NEWS ANALYSIS
Naval Wing, Embassy of India
Beijing
No : 09/2015
Date: 27 Jan 2015

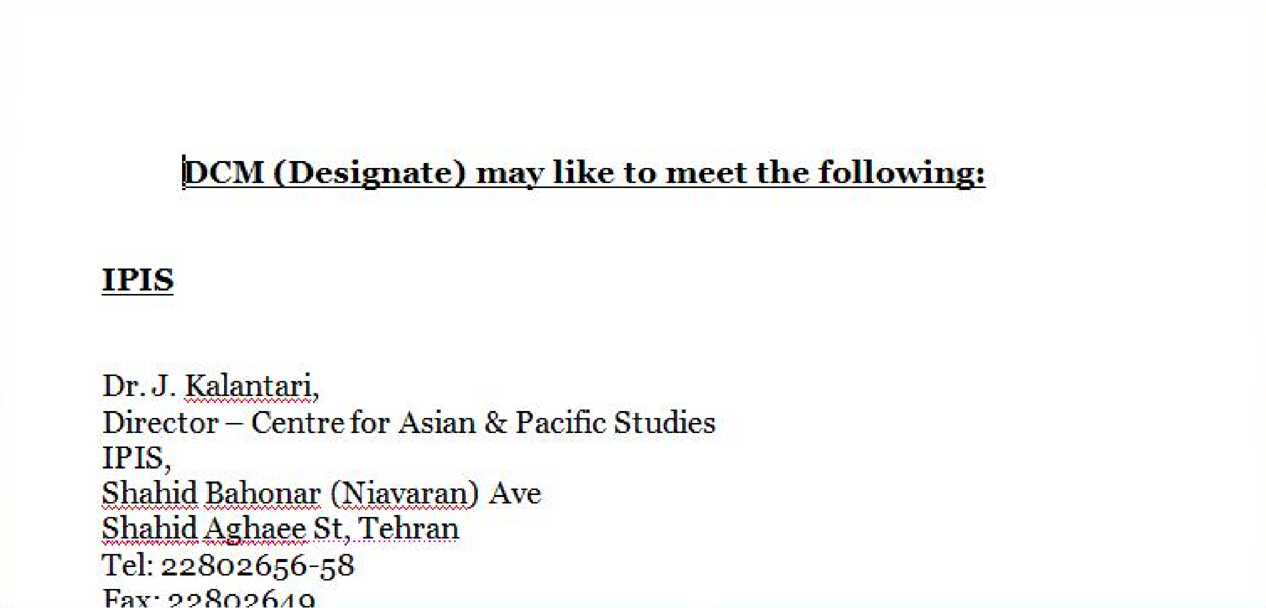
NAVAL WING, EoI, BEIJING
CHINA NEWS ANALYSIS – 09/2015

1. **Military Exercise**. The People's Liberation Army will performed military exercises Yellow Sea north of the Bohai Strait on 23 Jan 15. Entry on entering/leaving of vessels are imposed by demarcating following geographical co-ordinates:-

(a) 38 ° 55'N 120 ° 10'E

(b) 38 ° 55'N 121 ° 40'E

I have not yet concluded what the contents of **SHA1 c9f72a2d9f97951a1e73f8bb58d9846877757269** are. The document **contact list.doc** (shown below) also installs PlugX (**SHA1 7d71593a7d159c754055e16c26b844112e7b4132**, **MD5: 5730866b34ef589bd398c9a9b6d7e307**). This PlugX sample is identified in a June 2105 Citizen Lab post about attacks on the Tibetan diaspora in Hong Kong. (I hope to explore this connection in greater details in a follow-on post.)



DCM (Designate) may like to meet the following:

IPIS

Dr. J. Kalantari,
Director – Centre for Asian & Pacific Studies
IPIS,
Shahid Bahonar (Niavaran) Ave
Shahid Aghaee St, Tehran
Tel: 22802656-58
Fax: 22802649

Interestingly, both **CHINA NEWS BRIEF 09 of 2015.doc** and **Draft contract CMS Trg System.doc** are mentioned in a February 2015 SOPHOS report. The report discusses PlugX attacks on a variety of targets including those on India. The attacks reportedly took place between September 2014 and February 2015. Our PIVY sample was compiled on September 14, 2014 and submitted to Virus Total on January 19, 2015.

In addition to the infrastructure overlap, this correlation in timing also suggests that the Poison Ivy sample was just one payload involved in a much broader, 5-6 month campaign targeting India, the Tibetan community, and likely others of interest to China.

According to the SOPHOS report:

> *Not surprisingly, just like with several other campaigns, in this case* ***it was observed that different malware families were distributed using similar carrier documents****; only the encrypted payload was replaced at the end of the file. The shellcode used in the carrier was very convenient for this purpose: the length and location of the final payload was stored at the end of the file.* ***It was possible to swap the payload without needing to modify the exploit condition and the shellcode itself****.*

Thus, our Poison Ivy sample in this case appears to be tied to extensive attacks by one or more adversaries acting on behalf of Chinese interests.

[1] For example, by FireEye, Conix Security, and Trend Micro.

Tell me what you think!

RELATED CONTENT BY TAG ANALYSIS CHINA MALWARE PLUGX POISONIVY