Hat-tribution to PLA Unit 61486

June 9, 2014 NH Research & Threat Intel

Attribution is a key component of cyber-intelligence, by knowing the adversary you can effectively understand their intentions and objectives. Deep understanding of the adversary allows organizations to plan to defend their information and systems in some cases years into the future. Through attribution you can achieve spectacular disruptive activity against the adversary and send a clear message that 'we know who you are, and we want you to stop'. Some weeks ago, the US Government filed a criminal indictment against hackers affiliated with the Chinese People's Liberation Army (PLA), today CrowdStrike released a report on an adversary we call PUTTER PANDA.

The release of this report is meant to provide additional attribution around threat actors associated with activity targeting western enterprises and governments for espionage purposes. PUTTER PANDA is sometimes referred to as "MSUpdater" by the security research community, this group has been operating since at least 2007 and has heavily targeted the US defense and European satellite/aerospace industries. They focus their exploits against popular productivity applications such as Adobe Reader and Microsoft Office to deploy custom malware through targeted email attacks. PUTTER PANDA has been observed conducting operations with a nexus to Shanghai, China, likely on behalf of the Chinese PLA 3rd Department 12th Bureau Unit 61486.

This blog will provide some high level information to support this conclusion, including CrowdStrike's first use of 'hattribution' techniques that tie an actor using the handle 'cpyy' to a physical location corresponding to the headquarters of the 3rd Department of the General Staff Department (GSD) 12th Bureau within the PLA

registered to email addresses containing variants of a handle “cpyy” such as:

Domain	Email
ctable.org	cpyy.chen[@]gmail.com
gamemuster.com	cpyy.chen[@]gmail.com
kyoceras.net	cpyy.chen[@]gmail.com
nestlere.com	cpyy.chen[@]gmail.com
raylitoday.com	cpyy.chen[@]gmail.com
renewgis.com	cpyy.chen[@]gmail.com
siseau.com	cpyy[@]qq.com
bmwauto.org	cpyy[@]sina.com
t008.net	cpyy[@]sina.com
vssigma.com	cpyy[@]sina.com

Investigation of the domain siseau.com showed that the PUTTER PANDA operators deliberately changed registration information for it and several other domains such as vssigma.com in the late summer or fall of 2009. The other domains associated with this email address may have also been associated with personal email accounts of PUTTER PANDA actors before this timeframe, but historical data was not available. Similarly, domains associated with a mike.johnson_mj[@]yahoo.com address underwent registration changes during March 2014. These changes may indicate a new awareness of Operation Security (OPSEC) by the PUTTER PANDA actors, who may have attempted to obfuscate their real identities or to prevent infrastructure association through email address re-use.

CPYY

As well as the addresses shown above, “cpyy” appears to use several other email addresses, as well as the alternate handles “cpiyy” and “cpyy.chen”:

•cpyy[@]sina.com
•cpyy[@]hotmail.com
•cpyy.chen[@]gmail.com
•cpyy[@]cpyy.net
The cpyy.net domain lists “Chen Ping” as the registrant name, which may be cpyy’s real name, as this matches the initials “cp” in “cpyy”. Personal blogs relating to cpyy contain several interesting items of information:

- The profile on cpiyy.blog.163.com shows that the user is male, was born on 25 May 1979, and works for the “military/police” (其他- 军人/警察). It also contains postings indicating an interest in networking and programming topics around 2002/2003. This blog also contains several photographs that also appear on a picasa site (see below).
- www.tianya[.]cn/1569234/bbs indicates that cpyy was living in Shanghai as recently as 2007

military or police-based career.

A number of photographs were also published by cpyy on his picasa page, picasaweb.google[.]com/cpyy.chen, including a portrait of himself:

As well as several images of a younger cpyy that could be associated with military activities, two albums named 宿舍 and 办公室 ("dormitory" and "office") contain compelling images. Firstly, a shot of probably cpyy's dormitory room shows in the background two military hats that appear to be Type 07 PLA Army officer peak hats:

An enlarged version of these hats can be easily compared to a recently published photograph of a PLA officer in uniform, Sun Kailiang from Unit 61398:

This album also contains a shot of the exterior of a building with several large satellite dishes outside, which also appears in the “office” album:

Further imagery from the “office” album is shown below.

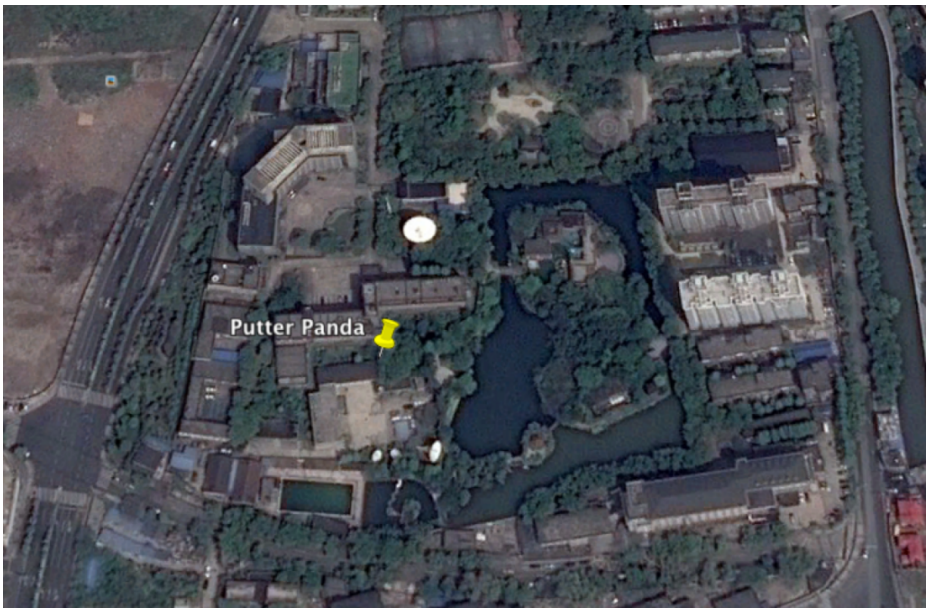
Finding the Office

Looking at historical domain registrations for PUTTER PANDA Command and Control (C2) domains, we observed an interesting address related to a sample (MD5: 15cae06fe5aa9934f96895739e38ca26) that called out to [redacted].checalla.com. This adversary controlled domain was registered to:

```
Domain Name ..................... CHECALLA.COM
Name Server ..................... dns21.hichina.com
                                  dns22.hichina.com
Registrant ID ................... hc437819049-cn
Registrant Name ................. lin liu
Registrant Organization ......... liulin
Registrant Address .............. shanghai yuexiulu 46 45 202#
Registrant City ................. shanghai
Registrant Province/State ....... 200042
Registrant Postal Code .......... 100000
Registrant Country Code ......... CN
Registrant Phone Number ......... +86.01000000000 -
Registrant Fax .................. +86.01000000000 -
Registrant Email ................ httpchen@gmail.com
```

Using google maps with the Shanghai address we arrive at:

Overlay that with satellite imagery:



This location based on imagery analysis is situated at latitude 31°17'17.02"N longitude 121°27'14.51"E, this location is in the heart of the Zhabei District of Shanghai is the headquarters of the 12th Bureau, 3rd Department of the GSD. The satellite dishes in the pictures from cpyy's albumns align perfectly with the dishes observable using multiple opensource maps such as google earth. The image above is particularly interesting when assessing the mission of unit 61486. According to project2049 the 12th Bureau:

Province), Fuqing (Fujian Province), and Kunming (Yunnan Province). 20 It is reported that the GSD Third Department currently employs some 130,000 people."

The mission of 12th Bureau unit 61486 lines up quite nicely with the observed victims, specifically the satellite technology companies associated with this activity.

Additional evidence supporting this comes from Chen Ping's photos, the buildings from this photo from the office album:

Are exceptionally similar to buildings in photos uploaded by a user on panoramio who tags the image as being located in Zhabei, Shanghai, China 31° 17′ 18.86″ N 121° 27′ 9.83″ E:

Links to COMMENT PANDA (Unit 61398)

IP address 100.42.216.230 has resolved several C2 domains associated with both PUTTER PANDA and COMMENT PANDA:

•news.decipherment.net
•res.decipherment.net
•spacenews.botanict.com
•spot.decipherment.net
The decipherment.net domains resolved to this IP address from 11 October 2012 to at least 25 February 2013, and the botanict.com domain resolved from 11 October 2012 to 24 March 2013. During part of this timeframe (30 June 2012 – 30 October 2012), a domain associated with COMMENT PANDA resolved to this same IP address: login.aolon1ine.com. Additionally, for a brief period in April 2012, update8.firefoxupdata.com also resolved to this IP address.

Additionally, cpyy has interacted with at least one actor associated with Unit 61398: "Linxder", including on cpyy's site cpyy.org, which previously hosted a discussion forum for the "711 Network Security Team".

Observations from social engineering topics used by PUTTER PANDA has shown a heavy interest in:

- Space, satellite, and remote sensing technology (particularly within Europe);
- Aerospace, especially European aerospace companies;
- Japanese and European telecommunications.

Aggressive acquisition of intellectual property and trade secrets from these sectors using cyber espionage techniques is consistent with the operations of Chinese state sponsored organizations, such as Unit 61486. While there are no "smoking keyboards" in the unclassified intelligence CrowdStrike has collected on PUTTER PANDA, the balance of evidence available points to an extensive operation conducted by a PLA unit with a nexus to spaced based communication systems. The alleged location and imagery associated with Chen Ping further corroborates the likelihood that this actor is affiliated with the PLA 12th Bureau of the 3rd Department of the GSD.

Putter Panda yara rules are available here. They can be easily used with CrowdStrike's CrowdResponse.

For more on Putter Panda, join us live on Tuesday, June 17th, 2014 at 2PM ET/11AM PT for 'Hat-tribution. The Who, What, and cpyy of Putter Panda' CrowdCast. In this live session, Dmitri Alperovitch, CTO & Co-Founder of CrowdStrike, and Adam Meyers, CrowdStrike's VP of Intelligence, will dive into the full details of the Putter Panda attribution and the toolset used by this actor. Register now!

If you want to hear more about Putter Panda and their tradecraft or any of the other adversaries that CrowdStrike tracks, please contact: intelligence@crowdstrike.com and inquire about Falcon Intelligence, our Cyber Threat Intelligence subscription.

Related Content

Blurring of

years ago that I first posted on the concept of protected processes, making my…

organizations are looking to integrate threat intelligence into their…

evolve, deciphering the purpose of specific malware-driven attacks has…