APT17 is run by the Jinan bureau of the Chinese Ministry of State Security


intrusiontruth.wordpress.com/2019/07/24/apt17-is-run-by-the-jinan-bureau-of-the-chinese-ministry-of-state-security/

intrusiontruth July 24, 2019

In previous articles we identified Jinan Quanxin Fangyuan Technology Co. Ltd. ( ), Jinan Anchuang Information Technology Co. Ltd. (), Jinan Fanglang Information Technology Co. Ltd. (朗) and RealSOI Computer Network Technology Co. Ltd. () as companies associated with Guo Lin (), a likely MSS Officer in Jinan.

We also identified two hackers from Jinan – Wang Qingwei (), the representative of the Jinan Fanglang company and Zeng Xiaoyong () the individual behind the online profile 'envymask'.

ZoxRPC

The Chinese variant of MS08-067 is particularly interesting because it forms part of a hacking tool frequently used by Chinese APT groups called ZoxRPC. This report from Novetta details ZoxRPC's incorporation in its code of specific memory addresses from the port of MS08-067 to Chinese operating systems (for which envymask takes responsibility).

That is to say, Zeng's code is used in ZoxRPC.

Evolution

Sample SHA1:b51e419bf999332e6b5501c62c5b4aee5b070219 appears to have a tangential relationship to the ZoxPNG samples listed above. The sample, known as ZoxRPC, has a compile date of 11 July 2008 at 04:28:21, placing it nearly 5 years ahead of the known ZoxPNG samples. Given the large time differential between ZoxRPC and ZoxPNG, making a direct relationship between the two generations is difficult. There are several attributes that would appear to indicate a connection between the two Zox variants:

1. The use of the term "iiscmd" with a relationship to the remote shell functionality
2. The identifiers used for each command roughly align.

ZoxRPC ID	ZoxPNG ID	Function Description
0x80061001	0x80061001	Initiate a remote shell
0x80061005	0x80061002	Interact with the remote shell (send command, read response)
0x80061003	0x80061003	Download a file from the C2 to the victim's machine
0x80061002	0x80061004	Upload a file to the C2 from the victim's machine

ZoxRPC uses the MS08-067 vulnerability, specifically portions of code found on this public website: http://www.pudn.com/downloads183/sourcecode/hack/exploit/detail861817.html. One interesting aspect of the ZoxRPC malware is the list of targeting offsets for the MS08-067 exploit. The offsets are associated with specific regional version of Windows. The following identifiers were found within ZoxRPC:

- KR Windows All bypass DEP
- JP Windows All bypass DEP
- EN Windows All bypass DEP
- TW Windows All bypass DEP
- CN Windows All bypass DEP

The list itself indicates a specific set of regional targets that the operators of ZoxRPC are going after.

Novetta report on ZoxRPC evolution

If there were any doubt that it was envymask's code used in ZoxRPC, have a look at the code found on pudn[.]com and you will see that it says: 'MS08-067 Exploit for CN by EMM@ph4nt0m.org'.

```
94.     if(strlen(Server) == 0)
95.     {
96.         Usage(argv[0]);
97.         return;
98.     }
99.
100.    printf("\nMS08-067 Exploit for CN by EMM@ph4nt0m.org\n\n");
101.
102.    lpNetResource.dwScope=RESOURCE_CONNECTED;
103.    lpNetResource.dwType =RESOURCETYPE_DISK;
104.    lpNetResource.dwDisplayType=RESOURCEDISPLAYTYPE_SHARE;
105.    lpNetResource.dwUsage=RESOURCEUSAGE_CONNECTABLE;
106.    lpNetResource.lpLocalName=NULL;
107.    lpNetResource.lpRemoteName = RemoteName;
108.    lpNetResource.lpComment=NULL;
109.    lpNetResource.lpProvider=NULL;
```

MS08-067 for China written by envymask aka EMM

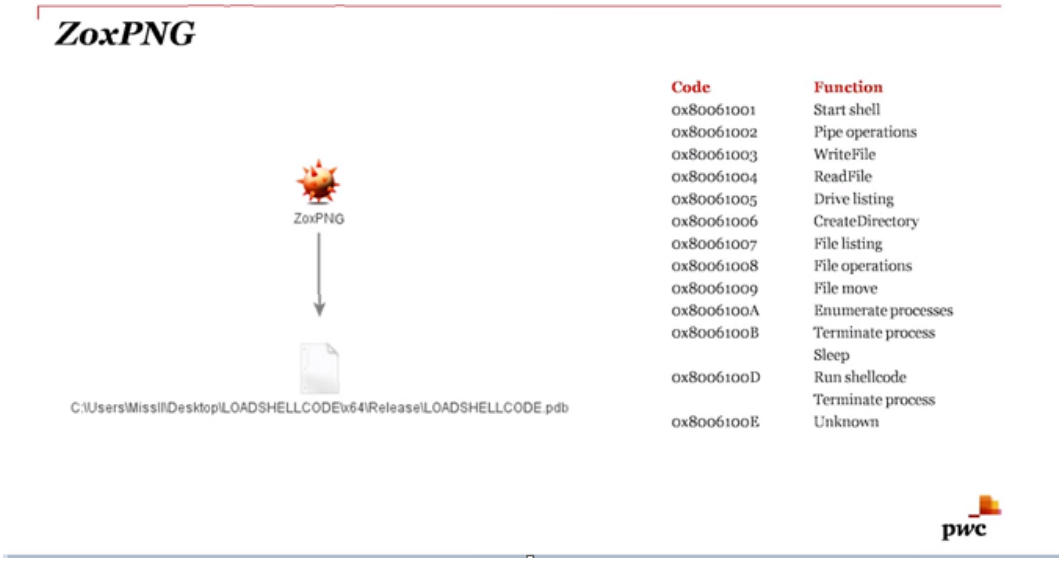
ZoxPNG

In a timeline analysis, the Novetta report identifies that ZoxRPC was evolved from code dating back to 2002 and was eventually released in 2008. It was then further developed into a new tool called ZoxPNG in 2013.

By researching the unique strings related to the iiscmd, iisput, and iisget strings, it appears that the original source code, upon which all Zox variants are based, dates back to 2002. As part of the IIS vulnerability disclosure of 2002 for the vulnerability MS02-018, the source code for the proof of concept code contains not only several strings found within the Zox binaries, but several of the functions as well. The source code upon which the Zox family is based is found at http://www.exploit-db.com/download/21371/, which was written by well-known Chinese hacker yuange. Given the several years between the original source code (2002) and both ZoxPNG (2013) and ZoxRPC (2008), the code upon which Zox is based has mutated and evolved, but there are clearly sections of code that have remained largely unaltered.

Novetta timeline analysis

A PwC presentation given at the Kaspersky Security Analyst Summit in 2015 showed that Chinese hacker Zhang Peng () aka 'missll' was the author of the newer ZoxPNG variant.



PwC presentation on ZoxPNG

APT17

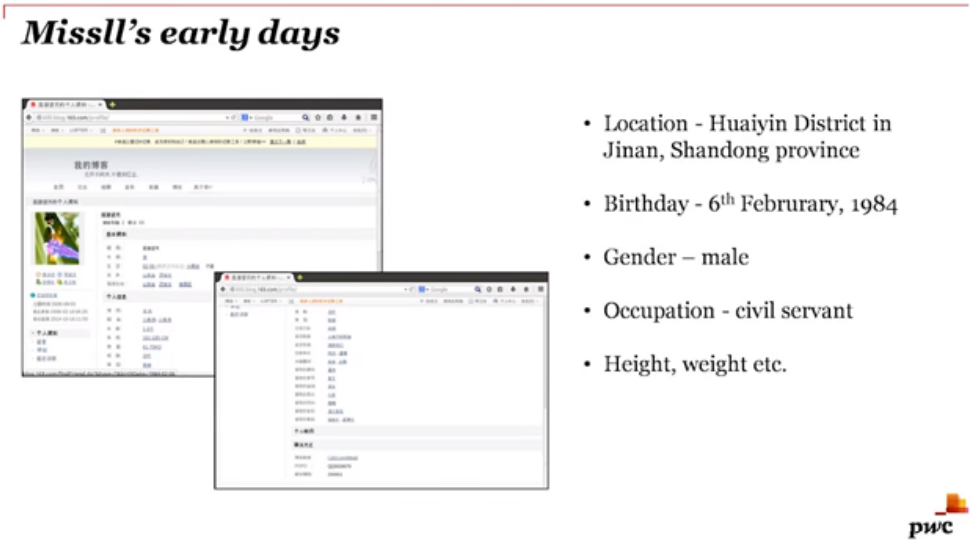
As FireEye noted in their 'Hide and Seek' report, ZoxPNG is also known as BLACKCOFFEE. And as V3 showed in their blog article, APT17 aka DeputyDog used BLACKCOFFEE malware as a key part of multiple campaigns.

V3 blog article on APT17 using BLACKCOFFEE malware

So Zeng wrote the MS08-067 code in ZoxRPC.

And Zhang Peng aka missll evolved it into the APT17 tool ZoxPNG aka BLACKCOFFEE.

Where was Zhang Peng from? **Jinan, China**.



PWC presentation on missll

In summary:

Either, one of the authors of code in APT17's primary malware just happens to be associated with a series of Cyber Security outfits that claim the MSS as their clients and are coincidentally managed by an MSS Officer.

Or, **MSS Officer Guo Lin of the Jinan bureau of the Ministry of State Security manages APT17.**

#thereismore…