09/19/2019 - Emissary Panda APT: Recent infrastructure and RAT analysis

meltx0r.github.io/tech/2019/09/19/emissary-panda-apt.html

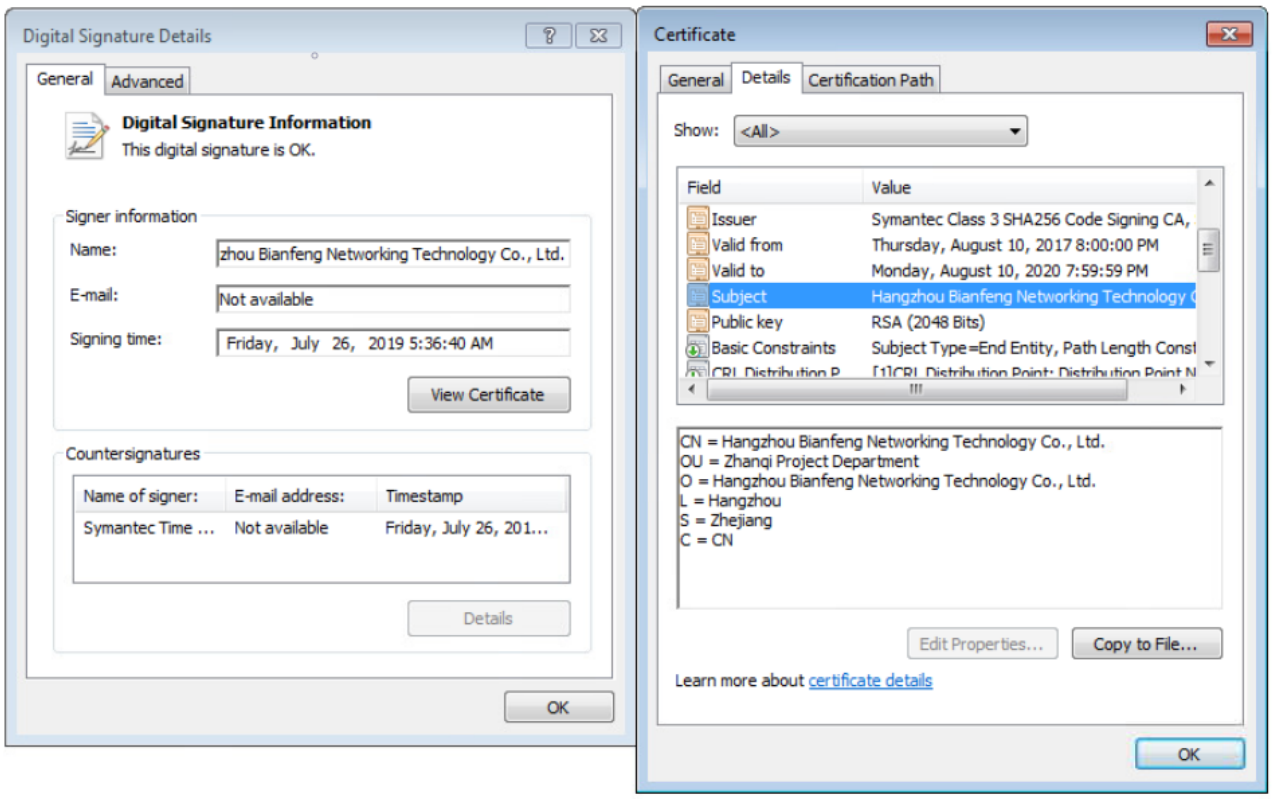
MELTX0R September 19, 2019

Summary

Emissary Panda, a group that goes by many names (APT27, IronTiger, BronzeUnion, TG-3390, and LuckyMouse), is a Chinese APT that is suspected of being active for nearly a decade. This group has been known to target aerospace, government, defense, technology, energy, and manufacturing sectors. Not much activity has been publicly recorded on this group as of late, but research indicates they are not dormant.

Analysis

While performing research, I identified a suspect binary titled "*odbcad32.exe*". What immediately piqued my interest was that this binary, while having the appearance of the legitimate "*Open Database Connectivity Data Source Administrator utility*" by Microsoft, was not signed with a Microsoft certificate. Instead, this binary was signed with a certificate belonging to "*Hangzhou Bianfeng Networking Technology Co., Ltd.*". Open source research on this company name indicates that it is a Chinese software company, and a subsidiary of the media organization "Zhejiang Daily Digital", which is headquartered in Hangzhou, China.



Shown above: Certificate used to sign malicious binary used by Emissary Panda APT

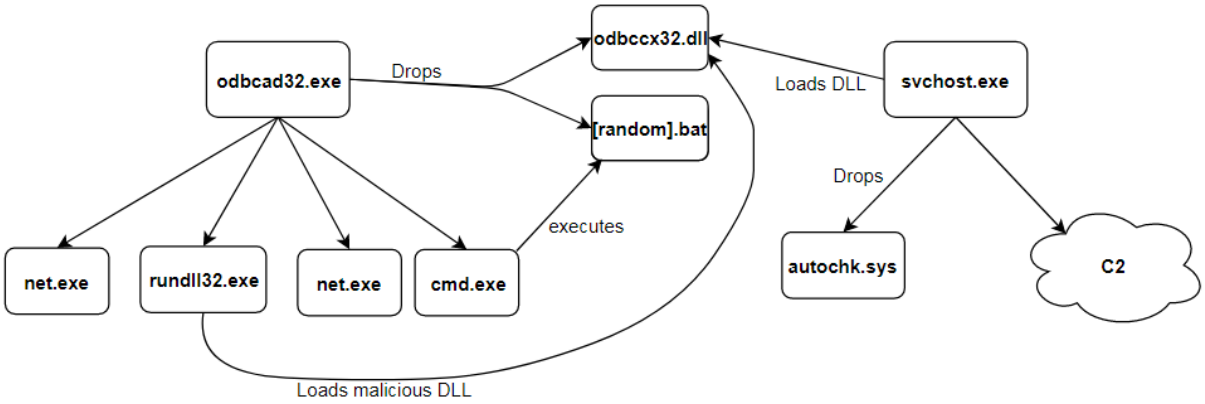
At this point, I decided to dig deeper into this binary and see why it was attempting to disguise itself as a legitimate Microsoft utility. Upon execution, the binary would elevate privileges and drop two files - *odbccx32.dll* in the *C:\Windows\system32* folder, and a randomly named batch file in the user's local temp folder.

```
@echo off
:err
del "c:\Users\[Username]\Desktop\odbcad32.exe" >nul
if exist "c:\Users\[Username]\Desktop\odbcad32.exe" goto err
>nul
@echo on
del "c:\Users\[Username]\AppData\Local\Temp\[random].bat"
```

Shown above: Content within the batch file

Net.exe was then launched with the parameters "*stop "Remote Registry Configuration"*". Next, rundll32.exe loads the aforementioned "odbccx32.dll", and then another *net.exe* is launched with the parameters "*start "Remote Registry Configuration"*". Once the malicious DLL is loaded via *rundll32.exe*, it then establishes persistence via a new service. *Cmd.exe* then executes the dropped batch file, which deletes the originally executed file, as well as the batch file itself.

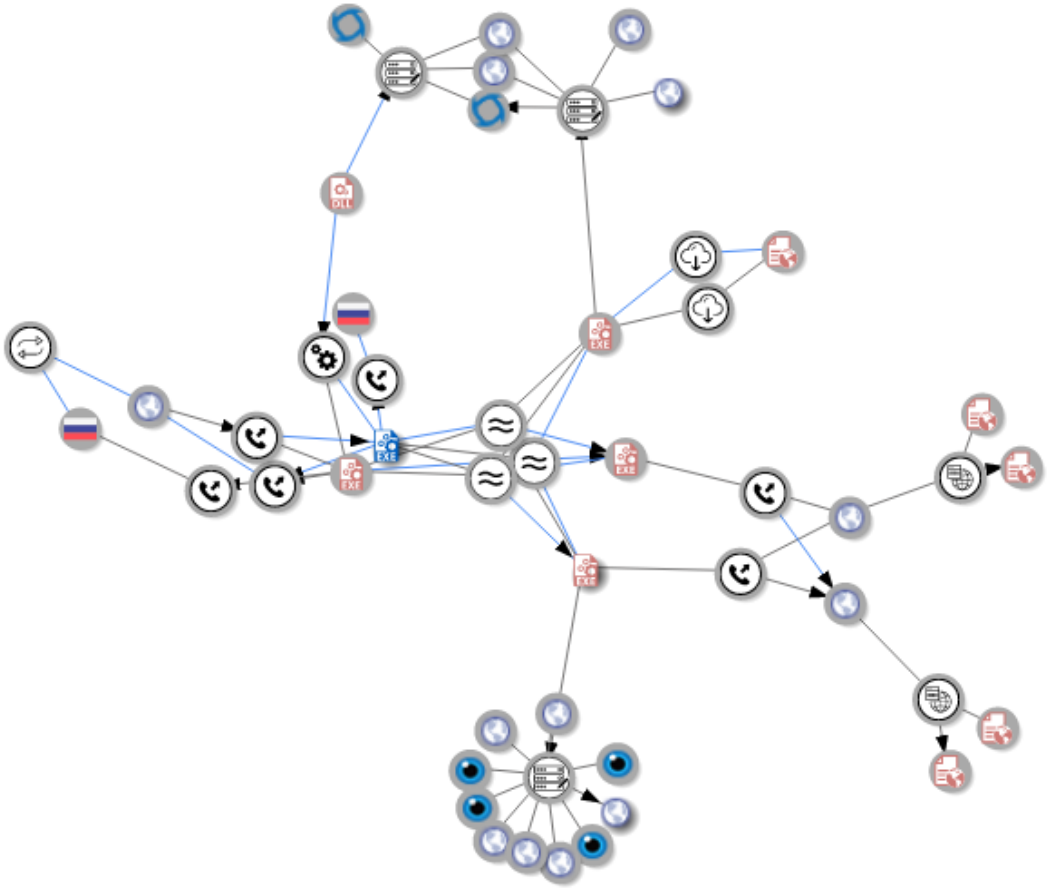
Following this, *Svchost.exe* is executed and loads the malicious *odbccx32.dll*. It then drops the file "*autochk.sys*" in the *C:\Windows\system32\drivers* folder, and reads the hosts file located in the C:\Windows\system32\drivers\etc\hosts folder (this file contains the mappings of IP addresses to host names). Command & Control is then initiated to "*yofeopxuuehixwmj.redhatupdater.com*" over ports 53, 80, and 443. While this domain currently resolves to *80.85.153.176*, no response was received from probing attempts, and no secondary payload was observed.



Shown above: Process graph

The TTP's (Tactics, Techniques, and Procedures) observed in this sample are consistent with those seen in past attacks conducted by the *Emissary Panda APT group*, specifically in relation to the *ZxShell Remote Access Trojan (RAT)* which they have been observed using.

I then pivoted into VirusTotal's relational graphing utility to see if I could gather additional information on this campaign's infrastructure. This revealed four structurally similar binaries that I suspect of also being *ZxShell RAT installers* - one of which beaconed to the same Command & Control server as the original sample (*yofeopxuuehixwmj.redhatupdater.com*). The second and third binaries beaconed to *language.wikaba.com* and *solution.instanthq.com* - both of which have been documented as being Command & Control servers for past Emissary Panda APT campaigns. I was unable to confirm the fourth binary being a ZxShell RAT installer, which beacons to *awvsf7esh.dellrescue.com*, however VirusTotal deems that it is structurally similar to previously confirmed installers. Please note that the domain "*dellrescue.com*" has been documented by *Cylance* as having been used in a campaign conducted by PassCV APT group in 2016, although the subdomain utilized was different (*sc.dellrescue.com*).



Shown above: VirusTotal Graph

At this time, I was unable to obtain evidence of target attribution - however in the past Emissary Panda APT has been observed targeting Asia, Middle East, US, and UK based organizations and infrastructure. What struck me as most interesting from my analysis of this sample was how the Emissary Panda APT group was able to obtain a valid certificate to sign their Remote Access Trojan binary, which sparks the question - was this group able to compromise the Chinese based software company and steal their certificate(s), or are there possible insider threats lurking within? Regardless, it is an interesting sample and displays that Emissary Panda is still active.

Indicators

Indicator	Type	Description
70cff7c176c7df265a808aa52daf6f34	MD5	odbcad32.exe - ZxShell RAT Installer
37fc73c754ef2706659a18837a90ddaa	MD5	odbcad32.exe - ZxShell RAT Installer

A9C2FF438C73E865624EEB0763235A14	MD5	odbccx32.dll - ZxShell RAT service DLL
yofeopxuuehixwmj.redhatupdater.com	Domain	ZxShell RAT Command & Control server
1b2d75f9c7717f377100924cdbdb10b1	MD5	odbcad32.exe - Unconfirmed ZxShell RAT Installer
awvsf7esh.dellrescue.com	Domain	Unconfirmed ZxShell RAT Command & Control server
850df4a726a71f50d3cc7192c8cf7e6a	MD5	odbcad32.exe - older ZxShell RAT Installer from 2018
b7f958f93e2f297e717cffc2fe43f2e9	MD5	odbcad32.exe - ZxShell RAT Installer previously documented by Dell SecureWorks CTU
language.wikaba.com	Domain	ZxShell RAT Command & Control server previously documented by Dell SecureWorks CTU
solution.instanthq.com	Domain	ZxShell RAT Command & Control server previously documented by Dell SecureWorks CTU

References/Further Reading

1. https://www.secureworks.com/research/a-peek-into-bronze-unions-toolbox
2. https://securelist.com/luckymouse-hits-national-data-center/86083/
3. https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/
4. https://thehackernews.com/2018/06/chinese-watering-hole-attack.html
5. https://arstechnica.com/information-technology/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/
6. https://attack.mitre.org/groups/G0027/
7. https://threatvector.cylance.com/en_us/home/digitally-signed-malware-targeting-gaming-companies.html
8. https://app.any.run/tasks/91aee60c-6982-461a-a006-e601c8879fb0/