
APT
27
AXIAL

A SURVEY ON EMISSARY PANDA: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. ABOUT

Emissary Panda is also known as TG-3390, TEMP.Hippo, Group 35, Bronze Union, Iron Tiger APT, and Lucky Mouse is an adversarial group from China that targets foreign embassies to collect data on government, defence, and technology sectors. The group has been active since 2010 and has conducted strategic web compromises (SWCs), also known as watering hole attacks, on websites associated with the target organizations.

II. TARGET SECTORS

Emissary Panda's observed target sectors are Defense, Education, Embassies, Government, Telecommunications, Think Tanks.

III. ENGAGEMENTS

- In 2015, Emissary Panda compromised networks of 50+ organizations through SWCs launched from over 100 compromised legitimate websites. The group had used CVE-2011-3544 and CVE-2010-0738 to compromise their targets. The group had used many tools but one of them stood out, being PlugX.
- In 2017, a data center in Central Asia was a target of Emissary Panda's campaign. The group used weaponized documents with CVE-2017-11882.
- In April 2019, APT27 installed webshells on SharePoint Servers to compromise Governmental Organizations of two different countries in the Middle East. Actors used the webshells to upload legitimate executables that would use DLL Sideloading to run a malicious DLL.

IV. METHODS USED

APT27 has extensively used Strategic Web Compromises to lure targets for espionage purposes.

AX1AL

V. ATTRIBUTIONS

- The use of well-known malware namely PlugX, previously observed with other Chinese threat actors.HyperBro RAT is commonly associated with APT27.
- The use of ZxShell which was embedded with HTran states that APT27 does not only adapt but evolve their toolset.

VI. IOC

C&C

1. 23.227.207[.]137
2. 89.249.65[.]194
3. update.iaacstudio[.]com
4. bbs.sonypsps[.]com
5. wh0am1.itbaydns[.]com
6. google-updata[.]tk
7. windows-updata[.]tk
8. yofeopxuuehixwmj.redhatupdater[.]com
9. language.wikaba[.]com
10. solution.instanthq[.]com
11. hxxps://185.12.45[.]134:443/ajax
12. 185.12.45[.]134

MD5

- 04dece2662f648f619d9c0377a7ba7c0
- 1b2d75f9c7717f377100924cdbdb10b1

ZxShell

- 70cff7c176c7df265a808aa52daf6f34
- 37fc73c754ef2706659a18837a90ddaa

SHA256

- 006569f0a7e501e58fe15a4323eedc08f9865239131b28dc5f95f750b4767b38
- 2feae7574a2cc4dea2bff4eceb92e3a77cf682c0a1e78ee70be931a251794b86
- d1ab0dff44508bac9005e95299704a887b0ffc42734a34b30ebf6d3916053dbe
- 6b3f835acbd954af168184f57c9d8e6798898e9ee650bd543ea6f2e9d5cf6378

VII. LINKS TO OTHER THREAT GROUPS

- Emissary Panda has some overlap with Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens.

VIII. REFERENCES

- https://arstechnica.com/information-technology/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/
- https://securelist.com/luckymouse-hits-national-data-center/86083/
- https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/
- https://marcoramilli.com/2020/03/19/is-apt27-abusing-covid-19-to-attack-people/