China's Ministry of State Security likely role in cyber attacks

Reference: Memo [190729-1] – Version: 1.0
Keywords: Doxing, China, MSS, espionage, APT
Sources: Publicly available information

Key Points

- Intrusion Truth, an anonymous entity, says that China's MSS regional offices are likely involved in APT activities.

Summary

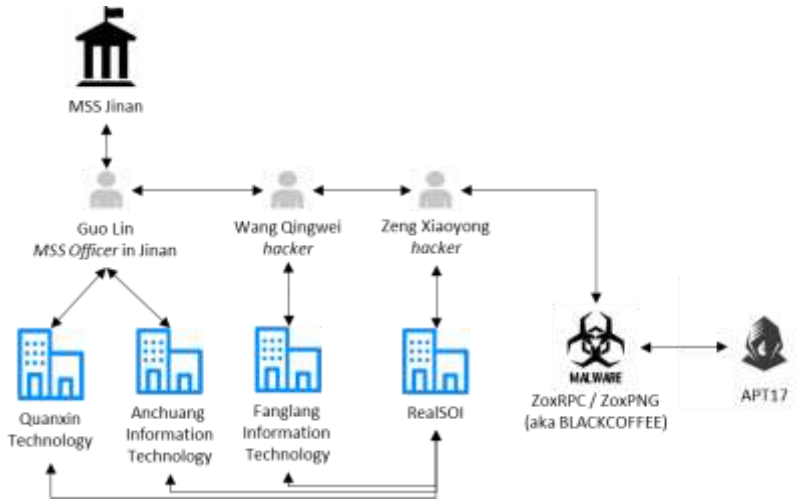
Intrusion Truth is an anonymous entity with an online presence[1], which has been active since 2017. This entity recently resurfaced and started disclosing new information related to the alleged involvement of the Chinese Ministry of State Security (MSS) in cyber-attacks. Intrusion Truth investigations are attempting to verify the following alleged pattern: "a regional office of the MSS creates a company, hires a team of hackers (forming an APT group) and attacks Western targets."

In previous disclosures, Intrusion Truth investigations claimed that APT10 "was managed" by the Tianjin bureau of the Chinese MSS, while APT3 "was" Boyusec, a cyber-security firm and contractor of the MSS in Guangdong. Crowdstrike also reached the same conclusion, in an article released last year[2].

Their most recent investigations are related to the MSS office in Jinan and APT17. Intrusion Truth claims that:

- A likely *MSS Officer* in Jinan (Guo Lin) is associated to two IT companies (Jinan Quanxin Technology, Jinan Anchuang Information Technology).
- An *IT security expert / hacker* (Wang Qingwei) is the official representative of an IT company (Jinan Fanglang Information Technology) and is directly linked to likely MSS Officer Guo Lin, travelling with him on multiple occasions.
- A well-known Chinese *hacker* (Zeng Xiaoyong) worked for RealSOI. A company closely associated with the MSS front companies listed above. Zeng knew Wang Qingwei, having worked as an InfoSec trainer with him.
- Code developed by Zeng Xiaoyong is embedded in hacking tools ZoxRPC / ZoxPNG (aka BLACKCOFFEE) used by APT17 in multiple campaigns, according to FireEye[3].

The diagram below illustrates the alleged relationships revealed by Intrusion Truth.



Comments

In December 2018, the US Department of Justice released indictments[4] of Chinese nationals (allegedly members of APT10), claiming that they were working for the army or the MSS and in the private sector, on offensive cybersecurity matters.

These recent researches by Intrusion Truth tend to confirm that there is likely an eco-system of Chinese governmental structures (MSS regional offices), front IT security companies and hackers for Chinese cyber-espionage. The identity and motives of Intrusion Truth remain unknown. They seem to want to expose actors of the Chinese government's cyber espionage eco-system and they have access to hacked / leaked personal data related to Chinese citizens.

1 https://intrusiontruth.wordpress.com/
2 https://www.crowdstrike.com/blog/two-birds-one-stone-panda/
3 http://www.informationsociety.co.uk/apt17-deputydog-hackers-are-pushing-blackcoffee-malware-using-technet/
4 https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion