The Role of Non-State Actors in Cyberwar

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

**The Role of Non-State Actors in Cyberwar**

Nonstate actors added complexity to the cyber warfare world. It is often difficult to determine the funding source and whether they are state-sponsored. For example, a recent research report by a security consulting firm Mandiant disclosed the existence of an advanced threat group known as APT1 (1). Although there is no concrete evidence, APT1 is believed a state sponsor group funded by the Chinese government. A few pieces of information that can be found about APT1:

* The name of the nonstate actor is APT1
* Classify the APT1: APT1 is believed a state-sponsor group funded by the Chinese government. According to Cyware Social (2019), it is considered one of the most prolific cyber espionage groups because of the quantity of information stolen by APT1. The APT1 is also known as Comment Crew, Comment Panda, Brown Fox, Byzantine Candor, Group 3, and GIF89a.
* The role of APT1: APT play many important roles in the global cyberwar from stealing broad categories of information such as intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails, and contact lists from victim organizations’ leadership. According to (1), APT1 has engaged in cyber-warfare against targets around the world for more than ten years.
* The objectives and motivations of APT1 are to conduct computer hacking and economic espionage to steal valuable information to their advance.
* According to (2), incidents involving APT1:
  + Stealing hundreds of terabytes of data from nearly 150 victims across 20 major industries until 2013.
  + Creating dangerous malware and malicious tools such as Poison Ivy malware, Mimikatz exploits tool, SeaSalt, Ecltys trojan, Downbot trojan, Barkiofork Backdoor, AURIGA malware, and BANGAT malware.
  + APT1 launched a minimum of 937 C&C servers hosted on 849 unique IP addresses across 13 countries between 2011 and 2013.
  + Launching a cyber espionage campaign dubbed ‘Operation Oceansalt’ targeted organizations across South Korea, US, and Canada with five attack waves in May 2018.

References

Chapple, M., & Seidl, D. (2023). *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 103–124). essay, Jones & Bartlett Learning. (1)

Cyware Social (2019) *APT1 Threat Actor Group: A deep dive into one of the prolific Chinese cyber espionage groups.* Retrieved from https://cyware.com/news/apt1-threat-actor-group-a-deep-dive-into-one-of-the-prolific-chinese-cyber-espionage-groups-84658f14