**Chinese Red Hacker Army // Personas**

Lion / Lin Yong

**Criminal History:**

* Hacking and DDoS’ing US and Japanese government, military, and media networks
* Organizing the HUC
* Involved with Topsec Technology, a firm in Beijing potentially linked to nation-state backed hacking of the US
* Developed HTran, a tool used in APT1 breaches.

**Lion, real name Lin Yong, was the founder and website administrator for the Hacker Union of China (HUC) and its associated website and forum. Lion was a patriotic computer science student who joined the Hacker War in 2001 after the Hainan Island incident.**

**Lion created the group and lead many of its activities. He administered the official site for the Hacker Union of China, and developed HTran, a proxy-like tool used to aid in the monitoring of targets in APT1 breaches. Though he posted the tool publicly online, this creates a veritable link between the HUC, Lion, and the CPC.**

**Lion went on to shut down the HUC, before bringing it back with the help of Liu Qing, a participant in the hacker war and now a mobile games developer and one-time bug bounty hunter. They co-authored an online manifesto, urging the members of the union to spend their time researching defensive technologies instead of hacking foreign governments. After the early 2000’s cyber conflict, the Chinese government spoke (softly) against hacktivist attacks on Western targets, even though they didn’t pursue charges.**

**Lion now works for Topsec Technology, a cyber security firm in Beijing with ties to the CPC. They were mentioned in a leaked State Department memo, detailing their worries that private firms were being used as a proxy to launch attacks. Topsec has ties to CNITSEC, a Chinese government organization that has been known to develop Microsoft OS exploits. The chairman of the company, He Weidong, also states that the majority of their start-up funding came from the CPC, and that they required no bank loans to turn into a 440M USD company.**

**Lion is also attributed to be the author of the Lion worm, a worm affecting RedHat Linux. The worm is not terrifically advanced, communicating with the author via a hardcoded email and scanning for vulnerable victims using a particularly noisy command. The exploit, written by Last Stage of Delirium (LSD), only affected a small subset of RedHat operating systems at the time. It appeared that, overall, the Lion Worm was basically a copy and paste version of another existing worm.**

**Lion, surprisingly, has a GitHub account, under the username zcnhonker. He has three repositories: HTran, trtool (a fork from another user), and mytools. Htran is the aforementioned proxy tool, a hacked together piece of software that was used in the APT1 breaches. The software repo named trtool, forked from user neroanelli, is a similar piece of proxy software that predates HTran. Trtool is written in C, while HTran is in C++, so it’s possible that HTran is a port of trtool, and that trtool was used as a reference.**

**The zcnhonker profile has a link to the HUC website, to a personal blog that seems to have been deleted. The profile’s three public repos have been inactive since 2015, which leads the author to believe that the purpose may be to us the git as a method to deploy git wherever Lion needs it, and to make the tool public to any other actors who may need it. He also may see the tool as burned, so, in the last effort to brag, Lion posted the tool online to show off the tool that was used in the breach of military and government networks.**

**Regardless of motive, the code offers an interesting look into the development cycle of an advanced threat, and gives some insight into the Clearnet network between the Chinese threat actors. It would appear that neroanelli is also a Chinese developer, with projects in Tomato firmware, Modbus, realtime, and several other technologies, and a repository history dating back to 2012. There are several other Chinese developers with connections to Lion, showing that they have a deep network on the Clearnet and the confidence to operate overtly and covertly.**

**Connections:**

* **HUC**
* **CPC**
* **APT1**
* **HTran**
* **He Weidong**
* **Topsec**

**Targets:**

* **USG and US media networks**