APT30 refers to a threat group committed to a long-term information gathering mission that spanned Southeast Asia and India (FireEye Labs, 2015). It is believed that the Chinese government sponsored the group. This group had confirmed targets in India, South Korea, Malaysia, Vietnam, Thailand, Saudi Arabia, and the United States, with suspected targets in ten other countries. Throughout their run, the group responsible for APT30 mainly used five malware applications: Backspace, Flashflood, Neteagle, Shipshape, and Spaceship. These five applications were consistently refined with multiple versions and even self-update capabilities.

Additionally, APT30 used spearphishing techniques to target members of the Association of Southeast Asian Nations, India, Nepal, and journalists. Their interests revolve around gathering information regarding political, economic, and military issues, including disputed territories and the legitimacy of the Chinese Communist Party (FireEye Labs, 2015). Overall, APT30 was highly successful for over a decade.

Backspace is one of two backdoors used to gain access to various systems. The earliest version of this application has been traced back to 2005, with the possibility of earlier versions. This application has a variety of uses, such as modifying registry keys, file manipulation, including downloads and searching, and extracting information (Backspace, 2020). There are two variants called “ZR” and “ZJ.” The ZR variant checks for installed host-based firewalls at this point, Backspace opens a communication channel and examines all open windows for a pop-up notification from the firewall (Backspace, 2020). Backspace simulates a mouse click in the window if a notification is found and allows the firewall to enable further connections. The ZJ variant creates “ZJ links” that grant internet access to relay traffic to command servers (Backspace, 2020).

The second backdoor developed by this group is Neteagle, and has been in use since at least 2008. Neteagle allows threat actors to enumerate and modify the file system of victim computers (Neteagle, 2020). This helps the threat actor search and create directories, read and write files, and even obtain volume information. Like Backspace, Neteagle has two variants named “Norton” and “Scout.”

Spaceship, Shipshape, and Flashflood all target removable media devices. Spaceship targets files and directories by looking for specific file extensions and modifications (Spaceship, 2020). Shipshape is used to target air-gapped networks. It spreads by modifying Autorun or hiding in legitimate files and copying itself into executable files (Shipshape, 2018). Flashflood targets “interesting files” with specific default or customized file extensions (Flashflood, 2020). These files are searched for in My Recent Documents, Desktop, Temporary Internet Files, and TEMP Directories.

MITRE ATT&CK. (2018, October 18). *Shipshape*. Retrieved from https://attack.mitre.org/software/S0028/

MITRE ATT&CK. (2020, March 30). *Backspace*. Retrieved from https://attack.mitre.org/software/S0031/

MITRE ATT&CK. (2020, March 30). *Flashflood*. Retrieved from https://attack.mitre.org/software/S0036/

MITRE ATT&CK. (2020, March 30). *Neteagle*. Retrieved from https://attack.mitre.org/software/S0034/

MITRE ATT&CK. (2020, March 30). *Spaceship*. Retrieved from https://attack.mitre.org/software/S0035/