Sharp Panda Utilizes New Version of the Soul Framework

Sharp Panda, (also known as APT19, Emissary Panda, or Iron Tiger) is a sophisticated Chinese Advanced Persistent Threat (APT) group. The group has been active since at least 2012 and is known for sharing tools and infrastructure with other Chinese APT groups.

These threat actors are highly motivated by cyber espionage and intelligence gathering. They utilize custom malware frameworks to execute attacks to include the new version of the Soul modular framework. The group applies sophisticated tactics such as spear-phishing emails, waterhole attacks, and supply chain attacks.

Sharp Panda primarily targets government organizations, defense contractors, and research institutions in Southeast Asia, Europe, and the United States, posing a significant threat to organizations. These cyber activities align with China's strategic interests in gaining access to sensitive data and intellectual property from foreign governments and organizations. Organizations should remain vigilant and take appropriate steps to protect themselves from these types of threats, including implementing strong cybersecurity measures, investing in employee training and awareness, and regularly updating their security protocols.

The Critical Start Cyber Threat Intelligence (CTI) team will continue to monitor the situation and work closely with the Threat Detection Engineering (TDE) team and the SOC to implement any relevant detections. For future updates, the CTI team will post via ZTAP® Bulletins and on the Critical Start Intelligence Hub.