Samurai Panda - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Samurai Panda

Names	Samurai Panda *(CrowdStrike)*
Country	China
Sponsor	State-sponsored, PLA Navy
Motivation	Information theft and espionage
First seen	2009
Description	(CrowdStrike) Samurai Panda is interesting in that their target selection tends to focus on Asia Pacific victims in Japan, the Republic of Korea, and other democratic Asian victims. Beginning in 2009, we've observed this actor conduct more than 40 unique campaigns that we've identified in the malware configurations' campaign codes. These codes are often leveraged in the malware used by coordinated targeted attackers to differentiate victims that were successfully compromised from different target sets. The implant delivered by Samurai Panda uses a typical installation process whereby they: 1. Leverage a spear-phish with an exploit to get control of the execution flow of the targeted application. This file "drops" an XOR-encoded payload that unpacks itself and a configuration file. 2. Next, the implant, which can perform in several different modes, typically will install itself as a service and then begin beaconing out to an adversary-controlled host. 3. If that command-and-control host is online, the malicious service will download and instantiate a backdoor that provides remote access to the attacker, who will see the infected host's identification information as well as the campaign code.
Observed	Sectors: Defense, Government. Countries: Hong Kong, Japan, South Korea, UK, USA.
Tools used	FormerFirstRAT, IsSpace, PlugX, Poldat, Sykipot.
Information	<https://www.crowdstrike.com/blog/whois-samurai-panda/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
