Hurricane Panda - Threat Group Cards: A Threat Actor Encyclopedia

APT group: Hurricane Panda

Names	Hurricane Panda *(CrowdStrike)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2013	
Description	(CrowdStrike) We have investigated their intrusions since 2013 and have been battling them nonstop over the last year at several large telecommunications and technology companies. The determination of this China-based adversary is truly impressive: they are like a dog with a bone. Hurricane Panda's preferred initial vector of compromise and persistence is a China Chopper webshell – a tiny and easily obfuscated 70 byte text file that consists of an 'eval()' command, which is then used to provide full command execution and file upload/download capabilities to the attackers. This script is typically uploaded to a web server via a SQL injection or WebDAV vulnerability, which is often trivial to uncover in a company with a large external web presence. Once inside, the adversary immediately moves on to execution of a credential theft tool such as Mimikatz (repacked to avoid AV detection). If they are lucky to have caught an administrator who might be logged into that web server at the time, they will have gained domain administrator credentials and can now roam your network at will via 'net use' and 'wmic' commands executed through the webshell terminal.	
Observed	Sectors: Technology, Telecommunications.	
Tools used	China Chopper, Mimikatz.	
Operations performed	Mar 2014	Operation "Poisoned Hurricane" <https://www.fireeye.com/blog/threat-research/2014/08/operation-poisoned-hurricane.html>

Information	<https://www.crowdstrike.com/blog/cyber-deterrence-in-action-a-story-of-one-long-hurricane-panda-campaign/>

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
