Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens

Archived: 2026-04-05 15:31:52 UTC

APT group: Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens

Names	Turbine Panda *(CrowdStrike)* APT 26 *(Mandiant)* Shell Crew *(RSA)* WebMasters *(Kaspersky)* KungFu Kittens *(FireEye)* Group 13 *(Talos)* PinkPanther *(RSA)* Black Vine *(Symantec)* Bronze Express *(SecureWorks)* JerseyMikes *(?)* Taffeta Typhoon *(Microsoft)*
Country	China
Sponsor	State-sponsored, the Jiangsu Bureau of the MSS (JSSD/江苏省国家安全厅)
Motivation	Information theft and espionage, Financial crime
First seen	2010
Description	(RSA) During recent engagements, the RSA IR Team has responded to multiple incidents involving a common adversary targeting each client's infrastructure and assets. The RSA IR Team is referring to this threat group internally as "Shell_Crew"; however, they are also referred to as Deep Panda, WebMasters, KungFu Kittens, SportsFans, and PinkPanther amongst the security community. Some analysts track Turbine Panda, DarkHydrus, LazyMeerkat and APT 19, Deep Panda, C0d0so0 as the same group, but it is unclear from open source information if the groups are the same. Turbine Panda has some overlap with Emissary Panda, APT 27, LuckyMouse, Bronze Union.
Observed	Sectors: Aerospace, Aviation, Defense, Energy, Financial, Food and Agriculture, Government, Healthcare, Non-profit organizations, Telecommunications, Think Tanks. Countries: Australia, Canada, China, Denmark, France, Germany, India, Italy, UK, USA and Southeast Asia.

Tools used	Cobalt Strike, Derusbi, FormerFirstRAT, Hurix, Mivast, PlugX, Sakula RAT, StreamEx, Winnti, Living off the Land.	
Operations performed	Dec 2012	Attack and IE 0day Information Used Against Council on Foreign Relations Regarding information's posted on the Washington Free Beacon, infected CFR.org website was used to attack visitors in order to extract valuable information's. The "drive-by" attack was detected around 2:00 pm on Wednesday 26 December and CFR members who visited the website between Wednesday and Thursday could have been infected and their data compromised, the specialists said. <https://eromang.zataz.com/2012/12/29/attack-and-ie-0day-informations-used-against-council-on-foreign-relations/>
	Dec 2012	Capstone Turbine Corporation Also Targeted in the CFR Watering Hole Attack <https://eromang.zataz.com/2013/01/02/capstone-turbine-corporation-also-targeted-in-the-cfr-watering-hole-attack-and-more/>
	May 2015	StreamEx malware Cylance SPEAR has identified a newer family of samples deployed by Shell Crew that has flown under AV's radar for more than a year and a half. Simple programmatic techniques continue to be effective in evading signature-based detection. <https://threatvector.cylance.com/en_us/home/shell-crew-variants-continue-to-fly-under-big-avs-radar.html>
Counter operations	Oct 2018	Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years <https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal> <https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading> <https://www.justice.gov/opa/pr/jury-convicts-chinese-intelligence-officer-espionage-crimes-attempting-steal-trade-secrets>
Information	<https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/h12756-wp-shell-crew.pdf> <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf> <https://www.crowdstrike.com/resources/wp-content/brochures/reports/huge-fan-of-your-work-intelligence-report.pdf>	

Last change to this card: 28 June 2025

Download this actor card in PDF or JSON format
