APT 4, Maverick Panda, Wisp Team

APT group: APT 4, Maverick Panda, Wisp Team

Names	APT 4 *(Mandiant)* APT 4 *(FireEye)* Maverick Panda *(CrowdStrike)* Wisp Team *(Symantec)* Sykipot *(AlienVault)* TG-0623 *(SecureWorks)* Bronze Edison *(SecureWorks)* Sodium *(Microsoft)* Salmon Typhoo *(Microsoft)*	
Country	China	
Sponsor	State-sponsored, PLA Navy	
Motivation	Information theft and espionage	
First seen	2007	
Description	(Trend Micro) Sykipot has a history of primarily targeting US Defense Initial Base (DIB) and key industries such as telecommunications, computer hardware, government contractors, and aerospace. Open source review of 15 major Sykipot attacks over the last 6 years confirm this. Recently, we encountered a case where Sykipot variants were gathering information related to the civil aviation sector. The exploitation occurred at a target consistent with their history, the information sought raises new interest. The intentions of this latest round of targeting are unclear, but it represents a change in shift in objectives or mission.	
Observed	Sectors: Aerospace, Aviation, Defense, Government, Telecommunications. Countries: USA.	
Tools used	Sykipot, XMRig.	
Operations performed	Dec 2011	Are the Sykipot's authors obsessed with next generation US drones? <https://cybersecurity.att.com/blogs/labs-research/are-the-sykipots-

		authors-obsessed-with-next-generation-us-drones>
	Jan 2012	Sykipot variant hijacks DOD and Windows smart cards <https://cybersecurity.att.com/blogs/labs-research/sykipot-variant-hijacks-dod-and-windows-smart-cards>
	Jul 2012	Sykipot is back <https://cybersecurity.att.com/blogs/labs-research/sykipot-is-back>
	Mar 2013	New Sykipot developments <https://cybersecurity.att.com/blogs/labs-research/new-sykipot-developments>
	Sep 2013	Sykipot Now Targeting US Civil Aviation Sector Information <https://blog.trendmicro.com/trendlabs-security-intelligence/sykipot-now-targeting-us-civil-aviation-sector-information/>
	2015	A group dubbed APT4 is suspected to be behind a breach of an Asian airline company discovered in the second quarter of this year. Its attack style uses well-written and researched 'spear-phishes' with industry themes. The attacks were aimed at public key infrastructure targets. <https://www.digitalnewsasia.com/digital-economy/asia-in-the-crosshairs-of-apt-attackers-fireeye-cto>
	Oct 2018	The report also mentions some attacks conducted by APT4 which includes sending malicious emails to a blockchain gaming start-up last year and attacking a cryptocurrency exchange in June 2018. In last October, the group also used XMRig, a Monero cryptocurrency mining tool in the target's computer. <https://mycryptomag.com/2019/08/08/cryptocurrency-firms-are-targets-of-state-sponsored-hacking-group-from-china/>
Information	<https://blog.trendmicro.com/trendlabs-security-intelligence/sykipot-now-targeting-us-civil-aviation-sector-information/> <https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/>	

Last change to this card: 06 March 2024

Download this actor card in PDF or JSON format
