APT 5, Keyhole Panda - Threat Group Cards: A Threat Actor Encyclopedia

APT group: APT 5, Keyhole Panda

Names	APT 5 *(FireEye)* Keyhole Panda *(CrowdStrike)* TEMP.Bottle *(iSight)* Bronze Fleetwood *(SecureWorks)* TG-2754 *(SecureWorks)* Poisoned Flight *(Kaspersky)* Manganese *(Microsoft)* Mulberry Typhoon *(Microsoft)*
Country	China
Motivation	Information theft and espionage
First seen	2007
Description	(FireEye) We have observed one APT group, which we call APT5, particularly focused on telecommunications and technology companies. More than half of the organizations we have observed being targeted or breached by APT5 operate in these sectors. Several times, APT5 has targeted organizations and personnel based in Southeast Asia. APT5 has been active since at least 2007. It appears to be a large threat group that consists of several subgroups, often with distinct tactics and infrastructure. APT5 has targeted or breached organizations across multiple industries, but its focus appears to be on telecommunications and technology companies, especially information about satellite communications. APT5 targeted the network of an electronics firm that sells products for both industrial and military applications. The group subsequently stole communications related to the firm's business relationship with a national military, including inventories and memoranda about specific products they provided. In one case in late 2014, APT5 breached the network of an international telecommunications company. The group used malware with keylogging capabilities

	to monitor the computer of an executive who manages the company's relationships with other telecommunications companies. There is some overlap with PittyTiger, Pitty Panda.	
Observed	Sectors: Defense, High-Tech, Industrial, Technology, Telecommunications. Countries: Southeast Asia.	
Tools used	LEOUNCIA.	
Operations performed	Aug 2019	A group of Chinese state-sponsored hackers is targeting enterprise VPN servers from Fortinet and Pulse Secure after details about security flaws in both products became public knowledge last month. <https://www.zdnet.com/article/a-chinese-apt-is-now-going-after-pulse-secure-and-fortinet-vpn-servers/>
Information	<https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-southeast-asia-threat-landscape.pdf>	

Last change to this card: 26 April 2023

Download this actor card in PDF or JSON format
