APT 18, Dynamite Panda, Wekby

APT group: APT 18, Dynamite Panda, Wekby

Names	APT 18 *(Mandiant)* Dynamite Panda *(CrowdStrike)* TG-0416 *(SecureWorks)* Wekby *(Palo Alto)* Scandium *(Microsoft)* Satin Typhoon *(Microsoft)* Red Wraith *(PWC)* SILVERVIPER *(?)* G0026 *(MITRE)*
Country	China
Sponsor	State-sponsored, PLA Navy
Motivation	Information theft and espionage
First seen	2009
Description	Wekby was described by Palo Alto Networks in a 2016 report as: 'Wekby is a group that has been active for a number of years, targeting various industries such as healthcare, telecommunications, aerospace, defense, and high tech. The group is known to leverage recently released exploits very shortly after those exploits are available, such as in the case of Hacking Team's Flash zero-day exploit.' This threat group has been seen since 2009. APT 18 may be related to Night Dragon and/or Nitro, Covert Grove.
Observed	Sectors: Aerospace, Construction, Defense, Education, Engineering, Healthcare, High-Tech, Telecommunications, Transportation and Biotechnology. Countries: USA.
Tools used	AtNow, Gh0st RAT, hcdLoader, HTTPBrowser, Pisloader, StickyFingers and 0-day exploits for Flash.

Operations performed	Apr 2014	Community Health Systems data breach <https://threatpost.com/apt-gang-branches-out-to-medical-espionage-in-community-health-breach/107828/> <https://www.venafi.com/blog/infographic-how-an-attack-by-a-cyber-espionage-operator-bypassed-security-controls>
	Jun 2015	Attacks using DNS Requests as Command and Control Mechanism Method: Phishing with obfuscated variants of the HTTPBrowser tool. <https://www.anomali.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop> <https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html>
	May 2016	Attacks using DNS Requests as Command and Control Mechanism Target: Organizations in the USA. Method: Phishing with Pisloader dropper. <https://unit42.paloaltonetworks.com/unit42-new-wekby-attacks-use-dns-requests-as-command-and-control-mechanism/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0026/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
