Putter Panda, APT 2 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:13:07 UTC

APT group: Putter Panda, APT 2

Names	Putter Panda *(CrowdStrike)* TG-6952 *(SecureWorks)* APT 2 *(Mandiant)* Group 36 *(Talos)* Sulphur *(Microsoft)* SearchFire *(?)* 4HCrew *(?)* G0024 *(MITRE)*
Country	China
Sponsor	State-sponsored, Unit 61486 of the 12th Bureau of the PLA's 3rd General Staff Department (GSD)
Motivation	Information theft and espionage
First seen	2007
Description	Putter Panda is the name of bad actor responsible for a series of cyberespionage operations originating in Shanghai, security experts linked its operation to the activity of the People's Liberation Army 3rd General Staff Department 12th Bureau Unit 61486. A fake yoga brochure was one of different emails used for a spear-phishing campaign conducted by the stealth Chinese cyber unit according an investigation conducted by researchers at the CrowdStrike security firm. Also in this case the experts believe that we are facing with a large scale cyberespionage campaign targeting government entities, contractors and research companies in Europe, USA and Japan. The group has been operating since at least 2007 and appears very interested in research companies in the space and satellite industry, experts at CrowdStrike have collected evidence of a numerous attacks against these industries.

Observed	Sectors: Defense, Government, Research, Technology. Countries: USA.
Tools used	3PARA RAT, 4H RAT, httpclient, MSUpdater, pngdowner.
Information	<https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf> <https://en.wikipedia.org/wiki/PLA_Unit_61486>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0024/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
