

PittyTiger, Pitty Panda - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:06:02 UTC

[Home](#) > [List all groups](#) > PittyTiger, Pitty Panda

APT group: PittyTiger, Pitty Panda

Names	PittyTiger (<i>FireEye</i>) Pitty Panda (<i>CrowdStrike</i>) G0011 (<i>MITRE</i>)	
Country	 China	
Motivation	Information theft and espionage	
First seen	2011	
Description	<p>(Airbus) Pitty Tiger is a group of attackers that have been active since at least 2011. They have targeted private companies in such as defense and telecommunications, but also at least one government.</p> <p>We have been able to track down this group of attackers and can provide detailed information about them. We were able to c their “malware arsenal”. We also analyzed their technical organization.</p> <p>Our investigations indicate that Pitty Tiger has not used any 0day vulnerability so far, rather they prefer using custom malwa the group’s exclusive usage. Our discoveries indicate that Pitty Tiger is a group of attackers with the ability to stay under the as mature as other groups of attackers we monitor.</p> <p>Pitty Tiger is probably not a state-sponsored group of attackers. They lack the experience and financial support that one wou sponsored attackers. We suppose this group is opportunistic and sells its services to probable competitors of their targets in t</p> <p>We have been able to leverage several attackers profiles, showing that the Pitty Tiger group is fairly small compared to other is probably why we saw them work on a very limited amount of targets.</p> <p>There is some overlap with APT 5, Keyhole Panda.</p>	
Observed	Sectors: Defense , Government , Telecommunications and Web development. Countries: Taiwan and Europe.	
Tools used	Enfal , Gh0st RAT , gsecdump , Leo RAT , Mimikatz , Paladin RAT , pgift , Pitty , Poison Ivy .	
Operations performed	2011	Operation “The Eye of the Tiger” https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2014/2014.07.11.Pitty_Tiger/Pitty_Tig
	Jun 2014	We discovered this malware sample in June 2014, leading to a command & control (c&c) server still in activity Our researches around the malware family revealed the “Pitty Tiger” group has been active since 2011, yet we i makes us believe the group is active since 2010. http://blog.cassidiancybersecurity.com/post/2014/07/The-Eye-of-the-Tiger2
	Jul 2014	During the last month, McAfee Labs researchers have uncovered targeted attacks carried out via spear phishing French company. We have seen email sent to a large group of individuals in the organization. https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/targeted-attacks-on-french-company-exploit-n-vulnerabilities/
	2014	In a recent attack against a French company, the attackers sent simple, straightforward messages in English and email addresses using names of actual employees of the targeted company. https://www.fireeye.com/blog/threat-research/2014/07/spy-of-the-tiger.html
MITRE ATT&CK	https://attack.mitre.org/groups/G0011/	

Last change to this card: 16 August 2025

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=26627515-afdb-421b-b59e-3a5300210001>