Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:51:09 UTC

APT group: Platinum

Names	Platinum *(Microsoft)* TwoForOne *(FireEye)* ATK 33 *(Thales)* G0068 *(MITRE)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2009	
Description	(Microsoft) Platinum has been targeting its victims since at least as early as 2009, and may have been active for several years prior. Its activities are distinctly different not only from those typically seen in untargeted attacks, but from many targeted attacks as well. A large share of targeted attacks can be characterized as opportunistic: the activity group changes its target profiles and attack geographies based on geopolitical seasons, and may attack institutions all over the world. Like many such groups, Platinum seeks to steal sensitive intellectual property related to government interests, but its range of preferred targets is consistently limited to specific governmental organizations, defense institutes, intelligence agencies, diplomatic institutions, and telecommunication providers in South and Southeast Asia. The group's persistent use of spear-phishing tactics (phishing attempts aimed at specific individuals) and access to previously undiscovered zero-day exploits have made it a highly resilient threat.	
Observed	Sectors: Defense, Financial, Government, Telecommunications and Intelligence agencies. Countries: China, India, Indonesia, Malaysia, Singapore, Thailand, Vietnam.	
Tools used	adbupd, AMTsol, DvDupdate.dll, JPIN, psinstrc.ps1, RedPepper, RedSalt, Titanium, Living off the Land.	
Operations performed	2017	Since the 2016 publication, Microsoft has come across an evolution of PLATINUM's file-transfer tool, one that uses the Intel Active Management Technology (AMT) Serial-over-LAN (SOL) channel for communication. This channel works independently of the operating system (OS), rendering any communication over it invisible to firewall and network monitoring applications running on the host device. Until this incident, no malware had been discovered misusing the AMT SOL feature for communication. <https://www.microsoft.com/security/blog/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility>
	Mid 2017	Operation "EasternRoppels" In the middle of 2017, Kaspersky Lab experts discovered a new malicious threat

		that is believed to be related to the famous PLATINUM APT group, which had been widely regarded as inactive. They named the campaign 'EasternRoppels'. <https://aavar.org/avar2018/index.php/the-easternroppels-operation-platinum-group-is-back/> <https://securelist.com/platinum-is-back/91135/>
	Nov 2019	During recent analysis we discovered Platinum using a new backdoor that we call Titanium (named after a password to one of the self-executable archives). Titanium is the final result of a sequence of dropping, downloading and installing stages. <https://securelist.com/titanium-the-platinum-group-strikes-again/94961/>
Information	<https://download.microsoft.com/download/2/2/5/225BFE3E-E1DE-4F5B-A77B-71200928D209/Platinum%20feature%20article%20-%20Targeted%20attacks%20in%20South%20and%20Southeast%20Asia%20April%202016.pdf> <https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/twoforonefinal.pdf> <https://en.wikipedia.org/wiki/PLATINUM_(cybercrime_group)>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0068/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
