Promethium, StrongPity - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:52:28 UTC

APT group: Promethium, StrongPity

Names	Promethium *(Microsoft)* StrongPity *(Kaspersky)* APT-C-41 *(Qihoo 360)* Magenta Dust *(Microsoft)* G0056 *(MITRE)*	
Country	Turkey	
Motivation	Information theft and espionage	
First seen	2012	
Description	Promethium is an activity group that has been active since at least 2012. The group conducted a campaign in May 2016 and has heavily targeted Turkish victims. Promethium has demonstrated similarity to another activity group called Neodymium due to overlapping victim and campaign characteristics. (Microsoft) Promethium is an activity group that has been active as early as 2012. The group primarily uses Truvasys, a first-stage malware that has been in circulation for several years. Truvasys has been involved in several attack campaigns, where it has masqueraded as one of server common computer utilities, including WinUtils, TrueCrypt, WinRAR, or SanDisk. In each of the campaigns, Truvasys malware evolved with additional features—this shows a close relationship between the activity groups behind the campaigns and the developers of the malware.	
Observed	Countries: Algeria, Belgium, Canada, Colombia, Cote d'Ivoire, Egypt, France, Germany, India, Iraq, Italy, Morocco, Netherlands, Poland, Senegal, South Africa, Syria, Tunisia, Turkey, USA, Vietnam.	
Tools used	StrongPity, StrongPity2, StrongPity3, Truvasys.	
Operations performed	Mar 2018	Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?

		<https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/>
	Mar 2018	Two months after the Citizen Lab report, Cylance found new Promethium/StrongPity activity, utilizing new infrastructure. The observed domains all appeared to have been registered about two weeks after Citizen Lab's report. The malware has continued to adapt as new information is published. Minimal effort and code changes were all that was required to stay out of the limelight. Cylance observed new domains, new IP addresses, filename changes, and small code obfuscation changes. <https://threatvector.cylance.com/en_us/home/whack-a-mole-the-impact-of-threat-intelligence-on-adversaries.html>
	Jul 2019	In early July 2019 Alien Labs began identifying new samples resembling StrongPity. The new malware samples have been unreported and generally appear to have been created and deployed to targets following a toolset rebuild in response to the above public reporting during the fourth quarter of 2018. <https://www.alienvault.com/blogs/labs-research/newly-identified-strongpity-operations#When:13:00:00Z>
	2019	PROMETHIUM extends global reach with StrongPity3 APT <https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html>
	Feb 2020	We recently detected a new, ongoing data exfiltration campaign targeting victims in Turkey that started in February 2020. <https://securelist.com/apt-trends-report-q1-2020/96826/>
	Jul 2021	StrongPity APT Group Deploys Android Malware for the First Time <https://www.trendmicro.com/en_us/research/21/g/strongpity-apt-group-deploys-android-malware-for-the-first-time.html>
	Nov 2021	A new StrongPity variant hides behind Notepad++ installation <https://blog.minerva-labs.com/a-new-strongpity-variant-hides-behind-notepad-installation>
	Nov 2021	StrongPity espionage campaign targeting Android users <https://www.welivesecurity.com/2023/01/10/strongpity-espionage-campaign-targeting-android-users/>
Information	<https://www.microsoft.com/security/blog/2016/12/14/twin-zero-day-attacks-promethium-and-neodymium-target-individuals-in-europe/> <https://securelist.com/on-the-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users/76147/>	

	<https://www.bitdefender.com/files/News/CaseStudies/study/353/Bitdefender-Whitepaper-StrongPity-APT.pdf> <https://anchorednarratives.substack.com/p/recover-your-files-with-strongpity>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0056/>

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=c33e0a3e-f5b9-46e2-9fab-f19869292c11