Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:09:58 UTC

APT group: Evilnum

Names	Evilnum *(Palo Alto)* Jointworm *(Symantec)* TA4563 *(Proofpoint)* G0120 *(MITRE)*	
Country	[Unknown]	
Motivation	Information theft and espionage	
First seen	2018	
Description	(Palo Alto) We witnessed attacks targeting the financial technology (FinTech) sector, primarily focused on organizations based in Israel. While researching these attacks, we discovered a possible relationship between Cardinal RAT and another malware family named EVILNUM. EVILNUM is a JavaScript-based malware family that is used in attacks against similar organizations. There is overlap between this group and Deceptikons, DeathStalker.	
Observed	Sectors: Financial, Government. Countries: Albania, Australia, Belgium, Canada, Cyprus, Czech, Israel, Italy, UK, Ukraine.	
Tools used	Bypass-UAC, Cardinal RAT, ChromeCookiesView, Evilnum, IronPython, LaZagne, MailPassView, More_eggs, ProduKey, PyVil RAT, TerraPreter, TerraStealer, TerraTV.	
Operations performed	May 2020	Operation “Phantom in the [Command] Shell” Prevailion’s Tailored Intelligence Team has detected two new criminal campaigns targeting the global financial industry with the EVILNUM malware, one of which became active on May 3rd 2020. <https://blog.prevailion.com/2020/05/phantom-in-command-shell5.html>
	Aug 2020	In recent weeks, the Nocturnus team has observed new activity by the group, including several notable changes from tactics observed previously.

		<https://www.cybereason.com/blog/no-rest-for-the-wicked-evilnum-unleashes-pyvil-rat>
	Dec 2021	Buy, Sell, Steal, EvilNum Targets Cryptocurrency, Forex, Commodities <https://www.proofpoint.com/us/blog/threat-insight/buy-sell-steal-evilnum-targets-cryptocurrency-forex-commodities>
	2022	Return of the Evilnum APT with updated TTPs and new targets <https://www.zscaler.com/blogs/security-research/return-evilnum-apt-updated-ttps-and-new-targets>
Information	<https://unit42.paloaltonetworks.com/cardinal-rat-sins-again-targets-israeli-fin-tech-firms/> <https://www.welivesecurity.com/2020/07/09/more-evil-deep-look-evilnum-toolset/> <https://github.com/eset/malware-ioc/tree/master/evilnum> <https://symantec.broadcom.com/hubfs/SED-Threats-Financial-Sector.pdf>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0120/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
