Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:21:32 UTC

Other threat group: TA516

Names	TA516 *(Proofpoint)* SmokingDro *(Proofpoint)*	
Country	[Unknown]	
Motivation	Financial crime, Financial gain	
First seen	2016	
Description	(Proofpoint) This actor typically distributes instances of the SmokeLoader intermediate downloader, which, in turn, downloads additional malware of the actor's choice -- often banking Trojans. Figure 3 shows a lure document from a November campaign in which TA516 distributed fake resumes with malicious macros that, if enabled, launch a PowerShell script that downloads SmokeLoader. In this instance, we observed SmokeLoader downloading a Monero coinminer. Since the middle of 2017, TA516 has used similar macro-laden documents as well as malicious JavaScript hosted on Google Drive to distribute both Panda Banker and a coinminer executable via SmokeLoader, often in the same campaigns.	
Observed	Countries: Worldwide.	
Tools used	AZORult, Chthonic, Smoke Loader, Zeus Panda.	
Operations performed	Jul 2016	Threat Actors Using Legitimate PayPal Accounts To Distribute Chthonic Banking Trojan <https://www.proofpoint.com/us/threat-insight/post/threat-actors-using-legitimate-paypal-accounts-to-distribute-chthonic-banking-trojan>
	Jul 2018	New version of AZORult stealer improves loading features, spreads alongside ransomware in new campaign <https://www.proofpoint.com/us/threat-insight/post/new-version-azorult-stealer-improves-loading-features-spreads-alongside>
	Nov 2019	New AZORult campaign abuses popular VPN service to steal cryptocurrency <https://www.kaspersky.com/about/press-releases/2020_new-

		azorult-campaign-abuses-popular-vpn-service-to-steal-cryptocurrency>
	Feb 2020	AZORult Campaign Adopts Novel Triple-Encryption Technique <https://threatpost.com/azorult-campaign-encryption-technique/152508/>
	Feb 2020	AZORult spreads as a fake ProtonVPN installer <https://securelist.com/azorult-spreads-as-a-fake-protonvpn-installer/96261/>
Information	<https://www.proofpoint.com/us/threat-insight/post/dialing-dollars-coinminers-appearing-malware-components-standalone-threats>	

Last change to this card: 01 January 2023

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=24184e42-b04f-4878-8fd3-e53acf7526f2