Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:45:40 UTC

APT group: TA530

Names	TA530 *(Proofpoint)*	
Country	[Unknown]	
Motivation	Financial crime	
First seen	2016	
Description	(Proofpoint) Since January 2016, a financially motivated threat actor whom Proofpoint has been tracking as TA530 has been targeting executives and other high-level employees, often through campaigns focused exclusively on a particular vertical. For example, intended victims frequently have titles of Chief Financial Officer, Head of Finance, Senior Vice President, Director and other high level roles. Additionally, TA530 customizes the email to each target by specifying the target's name, job title, phone number, and company name in the email body, subject, and attachment names. On several occasions, we verified that these details are correct for the intended victim. While we do not know for sure the source of these details, they frequently appear on public websites, such as LinkedIn or the company's own website. The customization doesn't end with the lure; the malware used in the campaigns is also targeted by region and vertical.	
Observed	Sectors: Automotive, Construction, Education, Energy, Engineering, Financial, Food and Agriculture, Healthcare, Hospitality, Manufacturing, Media, Pharmaceutical, Retail, Technology, Telecommunications, Transportation, Utilities. Countries: Australia, UK, USA.	
Tools used	AbaddonPOS, August Stealer, CryptoWall, Dridex, Gozi ISFB, H1N1 Loader, Nymaim, Smoke Loader, TeamSpy, TinyLoader.	
Operations performed	Nov 2016	August in November: New Information Stealer Hits the Scene <https://www.proofpoint.com/uk/threat-insight/post/august-in-december-new-information-stealer-hits-the-scene>
Information	<https://www.proofpoint.com/us/threat-insight/post/phish-scales-malicious-actor-target-execs>	

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=dc4db7a7-996d-4e90-8468-4ab4393b490d