Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:24:17 UTC

Other threat group: Karakurt

Names	Karakurt *(self given)* Mushy Scorpius *(Palo Alto)*	
Country	[Unknown]	
Motivation	Financial gain	
First seen	2021	
Description	(Accenture) Accenture Security has identified a new threat group, the self-proclaimed Karakurt Hacking Team, that has impacted over 40 victims across multiple geographies. The threat group is financially motivated, opportunistic in nature, and so far, appears to target smaller companies or corporate subsidiaries versus the alternative big game hunting approach. Based on intrusion analysis to date, the threat group focuses solely on data exfiltration and subsequent extortion, rather than the more destructive ransomware deployment. In addition, Accenture Security assesses with moderate-to-high confidence that the threat group's extortion approach includes steps to avoid, as much as possible, drawing attention to its activities.	
Observed	Sectors: Energy, Entertainment, Healthcare, Hospitality, Industrial, Manufacturing, Retail, Technology. Countries: USA and Europe.	
Tools used	7-Zip, AnyDesk, Cobalt Strike, FileZilla, Mimikatz, WinZip, Living off the Land.	
Operations performed	Sep 2022	Migration policy org confirms cyberattack after extortion group touts theft <https://therecord.media/migration-policy-org-confirms-cyberattack-after-extortion-group-touts-theft/>
Information	<https://www.accenture.com/us-en/blogs/cyber-defense/karakurt-threat-mitigation> <https://www.cisa.gov/uscert/ncas/alerts/aa22-152a> <https://blog.malwarebytes.com/cybercrime/2022/06/karakurt-extortion-group-threat-profile/>	

Last change to this card: 27 June 2025

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=a0013d64-bbae-4488-876b-b8ee9d364f3a