Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:32:06 UTC

Tool: TriFive

Names	TriFive
Category	Malware
Type	Backdoor
Description	(Palo Alto) TriFive is a previously unseen PowerShell-based backdoor that the xHunt actors installed on the compromised Exchange server, executing every five minutes via a scheduled task. TriFive provided backdoor access to the Exchange server by logging into a legitimate user's inbox and obtaining a PowerShell script from an email draft within the deleted emails folder. The TriFive sample used a legitimate account name and credentials from the targeted organization. This suggests that the threat actor had stolen the account's credentials prior to the installation of the TriFive backdoor.
Information	<https://unit42.paloaltonetworks.com/xhunt-campaign-backdoors/>

Last change to this tool card: 20 January 2021

Download this tool card in JSON format

All groups using tool TriFive

Changed	Name	Country	Observed	
APT groups				
	xHunt		2018-Aug 2019	

1 group listed (1 APT, 0 other, 0 unknown)