Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:03:15 UTC

Tool: XClient

Names	XClient
Category	Malware
Type	Info stealer, Credential stealer
Description	(Talos) The XClient stealer plugin performs anti-VM and anti-virus software checks on the victim's machine. It executes its functions to collect the victim's browser data, including cookies, stored credentials, and financial information such as credit card details. It also collects the victim's data from social media accounts, including Facebook, Instagram, TikTok business ads, and YouTube. It also collects the application data from the Telegram desktop and Discord application on the victim's machine. The stealer plugin can capture screenshots of the victim's desktop and save them as a PNG file in the victim's machine's temporary folder. With PNG files, the stealer plugin dumps the collected victim's data from the browser and social media accounts in a text file and creates a ZIP archive. The PNG and ZIP files are exfiltrated to the attacker's Telegram bot C2.
Information	<https://blog.talosintelligence.com/coralraider-targets-socialmedia-accounts/>

Last change to this tool card: 18 June 2024

Download this tool card in JSON format

All groups using tool XClient

Changed	Name	Country	Observed	
Other groups				
	CoralRaider		2023-Feb 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=37bd4995-f8b8-4ee3-b310-1d1566d767ae