Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:15:10 UTC

Tool: Cmstar

Names	Cmstar meciv
Category	Malware
Type	Downloader
Description	(Palo Alto) This specific downloader, Cmstar, is associated with the Lurid downloader also known as 'Enfal'. Cmstar was named for the log message 'CM**' used by the downloader. The Cmstar downloader starts by manually building its import address table (IAT), much like shellcode would; however, it uses a rather unique technique. Instead of finding API function names based on their hashed values, this malware enumerates libraries' export address table (EAT) and searches for the name of the API function the payload needs to load by using a character to offset array. The payload pairs several comma-separated lists of characters with comma-separated lists of numbers. Each list of characters consists of the set found within the API function name the payload seeks to add to its IAT, while the corresponding list of numbers specifies the offset in the function name where those characters should be placed.
Information	<https://unit42.paloaltonetworks.com/cmstar-downloader-lurid-and-enfals-new-cousin/> <https://researchcenter.paloaltonetworks.com/2016/03/digital-quartermaster-scenario-demonstrated-in-attacks-against-the-mongolian-government/> <https://researchcenter.paloaltonetworks.com/2017/09/unit42-threat-actors-target-government-belarus-using-cmstar-trojan> <https://www.votiro.com/single-post/2018/02/13/New-campaign-targeting-Ukrainians-holds-secrets-in-documents-properties>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cmstar>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:cmstar>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool Cmstar

Changed	Name	Country	Observed	
APT groups				
	Vicious Panda		2015-Mar 2020	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fc200bd2-4771-4e16-8d49-e231c20fdf63