Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 15:44:07 UTC

Tool: sLoad

Names	sLoad StarsLord
Category	Malware
Type	Reconnaissance, Backdoor, Banking trojan, Info stealer, Downloader
Description	(Proofpoint) sLoad is also written in PowerShell. At the time of this writing, the latest version of sLoad was 5.07b, which we will analyze here. It includes noteworthy features such as: • Collection of information to report to the C&C server that includes: o A list of running process o Presence of .ICA files on the system (likely Citrix-related) o Whether an Outlook folder is present on the system o Additional reconnaissance data • The ability to take screenshots • Checking the DNS cache for specific domains (e.g., targeted banks) • Loading external binaries
Information	<https://www.proofpoint.com/us/threat-insight/post/sload-and-ramnit-pairing-sustained-campaigns-against-uk-and-italy> <https://threatpost.com/sload-malware-revamped-starslord-l-features/152084/> <https://cyware.com/news/new-sload-malware-downloader-being-leveraged-by-apt-group-ta554-to-spread-ramnit-7d03f2d9> <https://isc.sans.edu/forums/diary/Malicious+Powershell+Targeting+UK+Bank+Customers/23675/> <https://blog.yoroi.company/research/the-sload-powershell-threat-is-expanding-to-italy/> <https://www.cybereason.com/blog/banking-trojan-delivered-by-lolbins-ramnit-trojan>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/ps1.sload>

Last change to this tool card: 13 May 2020

Download this tool card in JSON format

All groups using tool sLoad

Changed	Name	Country	Observed	
Other groups				
	TA554	[Unknown]	2017	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=02ef4587-9f94-4cfd-869a-7bebeb283516