Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:18:44 UTC

Tool: STASHLOG

Names	STASHLOG
Category	Malware
Type	Loader
Description	(Cybereason) STASHLOG (shiver.exe / forsrv.exe) is a 32 bit executable that is being used to prepare the victim machine for further compromise, and to “stash” a malicious, encrypted payload to a CLFS log file. This payload will be decrypted at each phase to deliver the next phase in the infection.
Information	<https://www.cybereason.com/blog/operation-cuckoobees-a-winnti-malware-arsenal-deep-dive> <https://www.mandiant.com/resources/unknown-actor-using-clfs-log-files-for-stealth>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.stashlog>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool STASHLOG

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=073125dd-411b-4292-bb14-5b42780ee33d