Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:33:06 UTC

Tool: ChewBacca

Names	ChewBacca
Category	Malware
Type	POS malware, Keylogger, Credential stealer
Description	(Trend Micro) ChewBacca is a PoS RAM scraper family, first discovered at the end of 2013, which uses the Tor network to exfiltrate stolen data. When first executed, ChewBacca copies itself to %USERPROFILE%\START MENU\Programs\Startup\spoolsv.exe and adds itself to an Auto Start runkey to remain persistent. It is self-contained and installs obfsproxy v0.2.3.25—a Tor proxy application—in %TEMP%. It then hooks WH_KEYBOARD_LL, which monitors keyboard input events. This allows ChewBacca to capture all keyboard events, which are then logged to %TEMP%\system.log.
Information	<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf> <https://www.securelist.com/en/blog/208214185/ChewBacca_a_new_episode_of_Tor_based_Malware> <https://threatpost.com/chewbacca-point-of-sale-malware-campaign-found-in-10-countries/103985/> <https://threatpost.com/points-of-sale-poorly-secured-facing-sophisticated-attacks/106027/> <http://vinsula.com/2014/03/01/chewbacca-tor-based-pos-malware/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.chewbacca>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool ChewBacca

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

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