Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:58:25 UTC

Tool: Rdasrv

Names	Rdasrv
Category	Malware
Type	POS malware, Credential stealer
Description	(Trend Micro) Rdasrv—one of the earliest PoS RAM scrapers—was first discovered at the end of 2011. It has no specific family name so it is called by the service name that it installs—rdasrv. When first executed, the malware is installed as a service called “rdasrv.” Name variations exist but rdasrv is most commonly used. The sample analyzed installed a service called “rdpclip.” The installer script executes the malware using the /install parameter. The malware then passes function cc_data_scraper_main to StartServiceCtrlDispatcher. The cc_data_scraper_main function registers itself to handle service control requests using RegisterServiceCtrlHandler. The malware is now installed and ready to scrape the process memory for Tracks 1 and 2 credit card data.
Information	<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf> <https://www.wired.com/wp-content/uploads/2014/09/wp-pos-ram-scraper-malware.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.rdasrv>

Last change to this tool card: 25 May 2020

Download this tool card in JSON format

All groups using tool Rdasrv

Changed	Name	Country	Observed
Unknown groups			

	[Interesting malware not linked to an actor yet]			

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