Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:17:10 UTC

Tool: SDBbot

Names	SDBbot
Category	Malware
Type	Backdoor, Loader, Info stealer, Tunneling
Description	(Proofpoint) SDBbot is a new remote access Trojan (RAT) written in C++ that has been delivered by the Get2 downloader in recent TA505 campaigns. Its name is derived from the debugging log file (sdb.log.txt) and DLL name (BotDLL[.]dll) used in the initial analyzed sample. It also makes use of application shimming for persistence. SDBbot is composed of three pieces: an installer, a loader, and a RAT component.
Information	<https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader> <https://www.cyber.gov.au/acsc/view-all-content/alerts/sdbbot-targeting-health-sector>
MITRE ATT&CK	<https://attack.mitre.org/software/S0461/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sdbbot>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool SDBbot

Changed	Name	Country	Observed	
APT groups				
	TA505, Graceful Spider, Gold Evergreen		2006-Nov 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8b99f47b-f765-4128-8f44-31881f1bd3c0