Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:15:07 UTC

Tool: ServHelper

Names	ServHelper
Category	Malware
Type	Backdoor, Credential stealer, Downloader
Description	ServHelper is written in Delphi and according to ProofPoint best classified as a backdoor. ProofPoint noticed two distinct variant - 'tunnel' and 'downloader' (citation): 'The 'tunnel' variant has more features and focuses on setting up reverse SSH tunnels to allow the threat actor to access the infecte contains functionality for the threat actor to 'hijack' legitimate user accounts or their web browser profiles and use them as they see downloader.'
Information	<https://www.proofpoint.com/us/threat-insight/post/servhelper-and-flawedgrace-new-malware-introduced-ta505> <https://e.cyberint.com/hubfs/Report%20Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%20Tool <https://www.deepinstinct.com/2019/04/02/new-servhelper-variant-employs-excel-4-0-macro-to-drop-signed-payload/> <https://ti.360.net/blog/articles/excel-4.0-macro-utilized-by-ta505-to-target-financial-institutions-recently-en/> <https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware>
MITRE ATT&CK	<https://attack.mitre.org/software/S0382/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.servhelper>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool ServHelper

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

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