ServHelper (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:09:21 UTC

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 infected host via Remote Desktop Protocol (RDP). Once ServHelper establishes remote desktop access, the malware contains functionality for the threat actor to 'hijack' legitimate user accounts or their web browser profiles and use them as they see fit. The 'downloader' variant is stripped of the tunneling and hijacking functionality and is used as a basic downloader."

▶ [TLP:WHITE] win_servhelper_auto (20201014 | autogenerated rule brought to you by yara-signator)
