ServHelper, Software S0382 | MITRE ATT&CK®

Archived: 2026-04-05 16:46:41 UTC

Domain	ID		Name	Use
Enterprise	T1098	.007	Account Manipulation: Additional Local or Domain Groups	ServHelper has added a user named "supportaccount" to the Remote Desktop Users and Administrators groups.[1]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	ServHelper uses HTTP for C2.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	ServHelper may attempt to establish persistence via the `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\` run key.[2]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	ServHelper has the ability to execute a PowerShell script to get information from the infected host.[3]
		.003	Command and Scripting Interpreter: Windows Command Shell	ServHelper can execute shell commands against cmd.[1][2]
Enterprise	T1136	.001	Create Account: Local Account	ServHelper has created a new user named "supportaccount".[1]

Domain	ID		Name	Use
Enterprise	T1573	.002	Encrypted Channel: Asymmetric Cryptography	ServHelper may set up a reverse SSH tunnel to give the attacker access to services running on the victim, such as RDP.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	ServHelper has a module to delete itself from the infected machine.[1][2]
Enterprise	T1105		Ingress Tool Transfer	ServHelper may download additional files to execute.[1][2]
Enterprise	T1036	.010	Masquerading: Masquerade Account Name	ServHelper has created a new user named `supportaccount`.[1]
Enterprise	T1021	.001	Remote Services: Remote Desktop Protocol	ServHelper has commands for adding a remote desktop user and sending RDP traffic to the attacker through a reverse SSH tunnel.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	ServHelper contains modules that will use schtasks to carry out malicious operations.[1]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	ServHelper contains a module for downloading and executing DLLs that leverages `rundll32.exe`.[2]
Enterprise	T1082		System Information Discovery	ServHelper will attempt to enumerate Windows version and system architecture.[1]
Enterprise	T1033		System Owner/User Discovery	ServHelper will attempt to enumerate the username of the victim.[1]

Source: https://attack.mitre.org/software/S0382/