Apostle, Software S1133 | MITRE ATT&CK®

Archived: 2026-04-05 12:44:09 UTC

Domain	ID		Name	Use
Enterprise	T1485		Data Destruction	Apostle initially masqueraded as ransomware but actual functionality is a data destruction tool, supported by an internal name linked to an early version, `wiper-action`. Apostle writes random data to original files after an encrypted copy is created, along with resizing the original file to zero and changing time property metadata before finally deleting the original file.[1]
Enterprise	T1486		Data Encrypted for Impact	Apostle creates new, encrypted versions of files then deletes the originals, with the new filenames consisting of a random GUID and ".lock" for an extension.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Apostle compiled code is obfuscated in an unspecified fashion prior to delivery to victims.[1]
Enterprise	T1561	.001	Disk Wipe: Disk Content Wipe	Apostle searches for files on available drives based on a list of extensions hard-coded into the sample for follow-on wipe activity.[1]
Enterprise	T1480		Execution Guardrails	Apostle's ransomware variant requires that a base64-encoded argument is passed when executed, that is used as the Public Key for subsequent encryption operations. If Apostle is executed without this argument, it automatically runs a self-delete function.[1]

Domain	ID		Name	Use
Enterprise	T1070	.001	Indicator Removal: Clear Windows Event Logs	Apostle will attempt to delete all event logs on a victim machine following file wipe activity.[1]
		.004	Indicator Removal: File Deletion	Apostle writes batch scripts to disk, such as `system.bat` and `remover.bat`, that perform various anti-analysis and anti-forensic tasks, before finally deleting themselves at the end of execution. Apostle attempts to delete itself after encryption or wiping operations are complete and before shutting down the victim machine.[1]
Enterprise	T1057		Process Discovery	Apostle retrieves a list of all running processes on a victim host, and stops all services containing the string "sql," likely to propagate ransomware activity to database files.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Apostle achieves persistence by creating a scheduled task, such as `MicrosoftCrashHandlerUAC`.[1]
Enterprise	T1529		System Shutdown/Reboot	Apostle reboots the victim machine following wiping and related activity.[1]

Source: https://attack.mitre.org/software/S1133