MultiLayer Wiper, Software S1135 | MITRE ATT&CK®

Archived: 2026-04-05 18:27:00 UTC

Domain	ID		Name	Use
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	MultiLayer Wiper uses a batch script launched via a scheduled task to delete Windows Event Logs.[1]
Enterprise	T1485		Data Destruction	MultiLayer Wiper deletes files on network drives, but corrupts and overwrites with random data files stored locally.[1]
Enterprise	T1565	.001	Data Manipulation: Stored Data Manipulation	MultiLayer Wiper changes the original path information of deleted files to make recovery efforts more difficult.[1]
Enterprise	T1561	.002	Disk Wipe: Disk Structure Wipe	MultiLayer Wiper opens a handle to `\\\\.\\PhysicalDrive0` and wipes the first 512 bytes of data from this location, removing the boot sector.[1]
Enterprise	T1083		File and Directory Discovery	MultiLayer Wiper generates a list of all files and paths on the fixed drives of an infected system, enumerating all files on the system except specific folders defined in a hardcoded list.[1]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	MultiLayer Wiper removes the Volume Shadow Copy (VSS) service from infected devices along with all present shadow copies.[1]
Enterprise	T1070		Indicator Removal	MultiLayer Wiper uses a batch script to clear file system cache memory via the

Domain	ID		Name	Use
				`ProcessIdleTasks` export in `advapi32.dll` as an anti-analysis and anti-forensics technique.[1]
		.001	Clear Windows Event Logs	MultiLayer Wiper removes Windows event logs during execution.[1]
		.004	File Deletion	MultiLayer Wiper uses a batch file, `remover.bat` to delete malware artifacts and the batch file itself during execution.[1]
		.006	Timestomp	MultiLayer Wiper changes timestamps of overwritten files to either 1601.1.1 for NTFS filesystems, or 1980.1.1 for all other filesystems.[1]
Enterprise	T1490		Inhibit System Recovery	MultiLayer Wiper wipes the boot sector of infected systems to inhibit system recovery.[1]
Enterprise	T1027	.009	Obfuscated Files or Information: Embedded Payloads	MultiLayer Wiper contains two binaries in its resources section, MultiList and MultiWip. MultiLayer Wiper drops and executes each of these items when run, then deletes them after execution.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	MultiLayer Wiper creates a malicious scheduled task that launches a batch file to remove Windows Event Logs.[1]
Enterprise	T1529		System Shutdown/Reboot	MultiLayer Wiper reboots the infected system following wiping and related tasks to prevent system recovery.[1]

Source: https://attack.mitre.org/software/S1135