ZeroCleare, Software S1151 | MITRE ATT&CK®

Archived: 2026-04-05 16:38:12 UTC

Domain	ID		Name	Use
Enterprise	T1059		Command and Scripting Interpreter	ZeroCleare can receive command line arguments from an operator to corrupt the file system using the RawDisk driver.[3]
		.001	PowerShell	ZeroCleare can use a malicious PowerShell script to bypass Windows controls.[4]
Enterprise	T1561	.002	Disk Wipe: Disk Structure Wipe	ZeroCleare can corrupt the file system and wipe the system drive on targeted hosts.[3][2][4]
Enterprise	T1068		Exploitation for Privilege Escalation	ZeroCleare has used a vulnerable signed VBoxDrv driver to bypass Microsoft Driver Signature Enforcement (DSE) protections and subsequently load the unsigned RawDisk driver.[4]
Enterprise	T1070	.004	Indicator Removal: File Deletion	ZeroCleare has the ability to uninstall the RawDisk driver and delete the `rwdsk` file on disk.[3][2]
Enterprise	T1680		Local Storage Discovery	ZeroCleare can use the `IOCTL_DISK_GET_DRIVE_GEOMETRY_EX`, `IOCTL_DISK_GET_DRIVE_GEOMETRY`, and `IOCTL_DISK_GET_LENGTH_INFO` system calls to compute disk size.[3]
Enterprise	T1106		Native API	ZeroCleare can call the `GetSystemDirectoryW` API to locate the system directory.[3]

Domain	ID		Name	Use
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	ZeroCleare can deploy a vulnerable, signed driver on a compromised host to bypass operating system safeguards. [4]

Source: https://attack.mitre.org/software/S1151