CaddyWiper, Software S0693 | MITRE ATT&CK®

Archived: 2026-04-05 15:50:36 UTC

Domain	ID		Name	Use
Enterprise	T1485		Data Destruction	CaddyWiper can work alphabetically through drives on a compromised system to take ownership of and overwrite all files.[1][2]
Enterprise	T1561	.002	Disk Wipe: Disk Structure Wipe	CaddyWiper has the ability to destroy information about a physical drive's partitions including the MBR, GPT, and partition entries.[1][2]
Enterprise	T1083		File and Directory Discovery	CaddyWiper can enumerate all files and directories on a compromised host.[3]
Enterprise	T1222	.001	File and Directory Permissions Modification: Windows File and Directory Permissions Modification	CaddyWiper can modify ACL entries to take ownership of files.[2]
Enterprise	T1106		Native API	CaddyWiper has the ability to dynamically resolve and use APIs, including `SeTakeOwnershipPrivilege`.[2]
Enterprise	T1057		Process Discovery	CaddyWiper can obtain a list of current processes.[3]

Domain	ID	Name	Use
Enterprise	T1082	System Information Discovery	CaddyWiper can use `DsRoleGetPrimaryDomainInformation` to determine the role of the infected machine. CaddyWiper can also halt execution if the compromised host is identified as a domain controller.[2][3]

Source: https://attack.mitre.org/software/S0693