Cheerscrypt, Software S1096 | MITRE ATT&CK®

Archived: 2026-04-02 10:37:47 UTC

Domain	ID		Name	Use
Enterprise	T1059	.012	Command and Scripting Interpreter: Hypervisor CLI	Cheerscrypt has leveraged `esxcli` in order to terminate running virtual machines.[2]
Enterprise	T1486		Data Encrypted for Impact	Cheerscrypt can encrypt data on victim machines using a Sosemanuk stream cipher with an Elliptic-curve Diffie–Hellman (ECDH) generated key.[2][1]
Enterprise	T1083		File and Directory Discovery	Cheerscrypt can search for log and VMware-related files with .log, .vmdk, .vmem, .vswp, and .vmsn extensions.[2]
Enterprise	T1489		Service Stop	Cheerscrypt has the ability to terminate VM processes on compromised hosts through execution of `esxcli vm process kill`.[2]
Enterprise	T1673		Virtual Machine Discovery	Cheerscrypt has leveraged `esxcli vm process list` in order to gather a list of running virtual machines to terminate them.[2]

Source: https://attack.mitre.org/software/S1096