VIRTUALPITA, Software S1217 | MITRE ATT&CK®

Archived: 2026-04-05 13:26:53 UTC

Domain	ID		Name	Use
Enterprise	T1037		Boot or Logon Initialization Scripts	VIRTUALPITA can persist as an init.d startup service on Linux vCenter systems.[1]
Enterprise	T1059	.004	Command and Scripting Interpreter: Unix Shell	VIRTUALPITA has the ability to spawn a bash shell for script execution.[1]
		.006	Command and Scripting Interpreter: Python	VIRTUALPITA can call a Python script to run commands on a targeted guest virtual machine.[1]
Enterprise	T1675		ESXi Administration Command	VIRTUALPITA can execute commands on guest virtual machines from compromised ESXi hypervisors.[1]
Enterprise	T1562	.003	Impair Defenses: Impair Command History Logging	VIRTUALPITA can impair logging by setting the `HISTFILE` environmental variable to `0` and stopping the `vmsyslogd` service.[1]
Enterprise	T1105		Ingress Tool Transfer	VIRTUALPITA has the ability to upload and download files.[1]
Enterprise	T1570		Lateral Tool Transfer	VIRTUALPITA is capable of file transfer and arbitrary command execution.[1]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	VIRTUALPITA has utilized VMware service names and ports to masquerade as legitimate services.[1]

Domain	ID		Name	Use
		.005	Masquerading: Match Legitimate Resource Name or Location	VIRTUALPITA samples have been found in `/usr/libexec/setconf/ksmd` and `/usr/bin/ksmd`, named to spoof the legitimate Kernel Same-Page Merging Daemon binary. [1]
Enterprise	T1571		Non-Standard Port	VIRTUALPITA has created listeners on hard coded TCP ports such as 2233, 7475, and 18098.[1]
Enterprise	T1489		Service Stop	VIRTUALPITA can start and stop the `vmsyslogd` service.[1]
Enterprise	T1673		Virtual Machine Discovery	VIRTUALPITA can target specific guest virtual machines for script execution.[1]
