Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:00:38 UTC

Tool: VIRTUALPITA

Names	VIRTUALPITA
Category	Malware
Type	Backdoor
Description	(Mandiant) VIRTUALPITA is a 64-bit passive backdoor that creates a listener on a hardcoded port number on a VMware ESXi server. The backdoor often utilizes VMware service names and ports to masquerade as a legitimate service. It supports arbitrary command execution, file upload and download, and the ability to start and stop vmsyslogd. During arbitrary command execution, the malware also sets the environmental variable HISTFILE to 0 to further hide activity that occurred on the machine. Variants of this malware were found to listen on a Virtual Machine Communication Interface (VMCI) and log this activity to the file sysclog.
Information	<https://cloud.google.com/blog/topics/threat-intelligence/esxi-hypervisors-malware-persistence>

Last change to this tool card: 26 August 2024

Download this tool card in JSON format

All groups using tool VIRTUALPITA

Changed	Name	Country	Observed	
APT groups				
	UNC3886		2021-Early 2025	

1 group listed (1 APT, 0 other, 0 unknown)