Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:16:41 UTC

Tool: VIRTUALGATE

Names	VIRTUALGATE
Category	Malware
Type	Dropper
Description	(Mandiant) The Windows guest virtual machines which were hosted by the infected hypervisors also contained a unique malware sample located at C:\Windows\Temp\avp.exe. This malware, which we refer to as VIRTUALGATE, is a utility program written in C that is comprised of two (2) parts, a dropper, and the payload. The memory only dropper deobfuscates a second stage DLL payload that uses VMware's virtual machine communication interface (VMCI) sockets to run commands on a guest virtual machine from a hypervisor host, or between guest virtual machines on the same host.
Information	<https://cloud.google.com/blog/topics/threat-intelligence/esxi-hypervisors-malware-persistence>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.virtualgate>

Last change to this tool card: 27 August 2024

Download this tool card in JSON format

All groups using tool VIRTUALGATE

Changed	Name	Country	Observed	
APT groups				
	UNC3886		2021-Early 2025	

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