Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:43:45 UTC

Tool: Remy

Names	Remy Remy RAT WINDSHIELD
Category	Malware
Type	Backdoor
Description	(Cylance) Arriving as an obfuscated PowerShell script built using the MSFvenom psh-reflection payload, the Remy DLL payload is ultimately unpacked, injected into memory, and executed via a Veil shellcode payload. The Remy DLL shares code with Backdoor.Win32.Denis (Kaspersky), and appears to be related to the “WINDSHIELD” malware (described in the FireEye APT32 report).
Information	<https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SpyRATsofOceanLotusMalwareWhitePaper.pdf> <https://threatvector.cylance.com/en_us/home/report-oceanlotus-apt-group-leveraging-steganography.html>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.remy>

Last change to this tool card: 29 December 2022

Download this tool card in JSON format

All groups using tool Remy

Changed	Name	Country	Observed	
APT groups				
	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	

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