Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:10:15 UTC

Tool: WINERACK

Names	WINERACK
Category	Malware
Type	Reconnaissance, Backdoor
Description	(FireEye) WINERACK is backdoor whose primary features include user and host information gathering, process creation and termination, filesystem and registry manipulation, as well as the creation of a reverse shell that utilizes statically-linked Wine cmd.exe code to emulate Windows command prompt commands. Other capabilities include the enumeration of files, directories, services, active windows and processes.
Information	<https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0219/>

Last change to this tool card: 23 April 2020

Download this tool card in JSON format

All groups using tool WINERACK

Changed	Name	Country	Observed	
APT groups				
	Reaper, APT 37, Ricochet Chollima, ScarCruft		2012-Mar 2025	

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