Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:42:33 UTC

Tool: CyberGate RAT

Names	CyberGate RAT CyberGate Rebhip
Category	Tools
Type	Reconnaissance, Backdoor, Info stealer, Exfiltration, Downloader
Description	(Citizen Lab) The CyberGate implant comes with the same credential stealing capabilities as the infector, and is extended by routines to spy on Chrome and STEAM credentials as well. Also inherited from the infector, the implant owns the same anti-analysis routine protecting it from sandboxes and debuggers. Beyond the capabilities seen in the infector, CyberGate has a range of features that provide an attacker with a full spectrum of monitoring and remote control functionality. CyberGate capabilities include: • Collecting detailed information about the infected system • Activation and control of the webcam and microphone • Screenshot capture • Blocking user input (e.g. keyboard and mouse) • Control over processes, windows, applications, devices, drive, ports, TCP & UDP connections, the clipboard, registry keys and values etc. • Control over the filesystem • Download and execution of further binaries • Exfiltration via FTP • Collection of information on installed security products
Information	<https://citizenlab.ca/2015/12/packrat-report/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.cybergate>

Last change to this tool card: 28 December 2022

Download this tool card in JSON format

All groups using tool CyberGate RAT

Changed	Name	Country	Observed	
APT groups				
	Operation Layover		2013	
	Packrat	[Latin America]	2008	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ba93b300-b8b3-4a37-8aa5-28a1f3e4014f