Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:08:55 UTC

Tool: Gh0st RAT

Names	Gh0st RAT Ghost RAT AngryRebel Farfli PCRat Moudour Mydoor
Category	Tools
Type	Reconnaissance, Backdoor, Keylogger, Info stealer
Description	(Infosec Institute) Gh0st RAT (Remote Access Terminal) is a trojan “Remote Access Tool” used on Windows platforms, and has been used to hack into some of the most sensitive computer networks on Earth. Below is a list of Gh0st RAT capabilities. Gh0st RAT can: • Take full control of the remote screen on the infected bot. • Provide real time as well as offline keystroke logging. • Provide live feed of webcam, microphone of infected host. • Download remote binaries on the infected remote host. • Take control of remote shutdown and reboot of host. • Disable infected computer remote pointer and keyboard input. • Enter into shell of remote infected host with full control. • Provide a list of all the active processes. • Clear all existing SSDT of all existing hooks.
Information	<https://resources.infosecinstitute.com/gh0st-rat-complete-malware-analysis-part-1/> <https://labs.bitdefender.com/2018/02/operation-pzchao-a-possible-return-of-the-iron-tiger-apt/> <http://download01.norman.no/documents/ThemanyfacesofGh0stRat.pdf> <https://www.proofpoint.com/us/threat-insight/post/north-korea-bitten-bitcoin-bug-financially-motivated-campaigns-reveal-new> <https://www.proofpoint.com/sites/default/files/pfpt-us-wp-north-korea-bitten-by-

	bitcoin-bug.pdf> <http://www.malware-traffic-analysis.net/2018/01/04/index.html> <https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2018/april/decoding-network-data-from-a-gh0st-rat-variant/> <http://www.hexblog.com/?p=1248> <https://blog.cylance.com/the-ghost-dragon> <https://www.intezer.com/blog-chinaz-relations/> <https://cofense.com/blog/open-source-gh0st-rat-still-haunting-inboxes-15-years-after-release/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0032/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.ghost_rat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:Gh0st%20RAT> <https://otx.alienvault.com/browse/pulses?q=tag:PCRat>

Last change to this tool card: 26 April 2023

Download this tool card in JSON format

All groups using tool Gh0st RAT

Changed	Name	Country	Observed	
APT groups				
	Anchor Panda, APT 14		2012	
	APT 17, Deputy Dog, Elderwood, Sneaky Panda		2009-Jun 2024	
	APT 18, Dynamite Panda, Wekby		2009-May 2016	
	APT 31, Judgment Panda, Zirconium		2016-Mar 2024	
	APT 41		2012-Jul 2025	
	Axiom, Group 72		2008-2008/2014	
	Bronze Butler, Tick, RedBaldNight, Stalker Panda		2006-Apr 2021	
	Dust Storm		2010	
	Earth Berberoka		2022	

	Emissary Panda, APT 27, LuckyMouse, Bronze Union		2010-Aug 2023	
	GhostNet, Snooping Dragon		2009-2010	●
	Kimsuky, Velvet Chollima		2012-Aug 2025	●
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	●
	Leviathan, APT 40, TEMP.Periscope		2013-Jul 2021	●
	Mikroceen		2017-Mar 2021	
	Nitro, Covert Grove		2011-Jul 2014	
	Operation Diplomatic Specter		2022	
	PassCV		2016	
	PittyTiger, Pitty Panda		2011-2014	
	RedAlpha		2015-2021	
	Roaming Tiger		2014-Aug 2015	
	Space Pirates		2017-Nov 2024	
	Stone Panda, APT 10, menuPass		2006-Mar 2025	●
	TA459		2017-Apr 2022	
	Wicked Spider, APT 22		2018	

25 groups listed (25 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=c4684682-855e-4968-abaa-f930a6e4efcb