Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:01:47 UTC

Tool: 9002 RAT

Names	9002 RAT McRAT MdmBot Homux Hydraq HidraQ HOMEUNIX Aurora Roarur
Category	Malware
Type	Backdoor, Info stealer
Description	9002 RAT is a Remote Access Tool typically observed to be used by an APT to control a victim's machine. It has been spread over via zero day exploits (e.g. targeting Internet Explorer) as well as via email attachments. The infection chain starts by opening a .LNK (an OLE packager shell object) that executes a Powershell command.
Information	<https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html> <https://www.arbornetworks.com/blog/asert/wp-content/uploads/2016/01/ASERT-Threat-Intelligence-Brief-2015-08-Uncovering-the-Seven-Point-Dagger.pdf> <https://community.hpe.com/t5/Security-Research/9002-RAT-a-second-building-on-the-left/ba-p/6894315> <http://researchcenter.paloaltonetworks.com/2016/07/unit-42-attack-delivers-9002-trojan-through-google-drive/> <https://www.fireeye.com/blog/threat-research/2013/05/ready-for-summer-the-sunshop-campaign.html> <https://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/> <https://www.proofpoint.com/us/threat-insight/post/operation-rat-cook-chinese-apt-actors-use-fake-game-thrones-leaks-lures> <https://www.fireeye.com/blog/threat-research/2013/02/lady-boyle-comes-to-town-

	with-a-new-exploit.html> <https://blog.trendmicro.com/trendlabs-security-intelligence/supply-chain-attack-operation-red-signature-targets-south-korean-organizations/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0203/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.9002>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:9002>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool 9002 RAT

Changed	Name	Country	Observed	
APT groups				
	APT 17, Deputy Dog, Elderwood, Sneaky Panda		2009-Jun 2024	
	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	
	Mustang Panda, Bronze President		2012-Jun 2025	
	Nightshade Panda, APT 9, Group 27		2013-Sep 2016	
	Operation Red Signature		2018	
	Space Pirates		2017-Nov 2024	

9 groups listed (9 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f3993a74-3133-4926-aeab-2b93ef6ed81d