Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:50:56 UTC

Tool: QuasarRAT

Names	QuasarRAT Quasar RAT CinaRAT Yggdrasil
Category	Tools
Type	Reconnaissance, Backdoor, Keylogger, Credential stealer, Info stealer, Exfiltration, Tunneling
Description	Quasar is a fast and light-weight remote administration tool coded in C#. The usage ranges from user support through day-to-day administrative work to employee monitoring. Providing high stability and an easy-to-use user interface, Quasar is the perfect remote administration solution for you. Feature: • TCP network stream (IPv4 & IPv6 support) • Fast network serialization (Protocol Buffers) • Compressed (QuickLZ) & Encrypted (TLS) communication • Multi-Threaded • UPnP Support • No-Ip.com Support • Visit Website (hidden & visible) • Show Messagebox • Task Manager • File Manager • Startup Manager • Remote Desktop • Remote Shell • Download & Execute • Upload & Execute • System Information • Computer Commands (Restart, Shutdown, Standby) • Keylogger (Unicode Support)

	• Reverse Proxy (SOCKS5) • Password Recovery (Common Browsers and FTP Clients) • Registry Editor
Information	<https://github.com/quasar/QuasarRAT> <https://threatvector.cylance.com/en_us/home/threat-spotlight-menupass-quasarrat-backdoor.html> <https://researchcenter.paloaltonetworks.com/2018/01/unit42-vermin-quasar-rat-custom-malware-used-ukraine/> <https://www.fireeye.com/blog/threat-research/2019/04/spear-phishing-campaign-targets-ukraine-government.html> <https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/> <https://www.volexity.com/blog/2018/06/07/patchwork-apt-group-targets-us-think-tanks/> <https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-annex-b-final.pdf> <http://researchcenter.paloaltonetworks.com/2017/01/unit42-downeks-and-quasar-rat-used-in-recent-targeted-attacks-against-governments> <https://documents.trendmicro.com/assets/tech-brief-untangling-the-patchwork-cyberespionage-group.pdf> <https://ti.360.net/blog/articles/analysis-of-apt-c-09-target-china/> <https://www.welivesecurity.com/2018/07/17/deep-dive-vermin-rathole/> <https://blogs.jpcert.or.jp/en/2020/12/quasar-family.html> <https://asec.ahnlab.com/en/47283/> <https://www.uptycs.com/blog/quasar-rat> <https://socket.dev/blog/quasar-rat-disguised-as-an-npm-package>
MITRE ATT&CK	<https://attack.mitre.org/software/S0262/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.quasar_rat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:QuasarRat>

Last change to this tool card: 22 February 2025

Download this tool card in JSON format

All groups using tool QuasarRAT

Changed	Name	Country	Observed
APT groups			

	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	
	APT 33, Elfin, Magnallium		2013-Apr 2024	
	Earth Berberoka		2022	
	Gallium		2018-Jun 2022	
	Gorgon Group		2017-Jul 2020	
	LazyScripter	[Unknown]	2018	
	Molerats, Extreme Jackal, Gaza Cybergang	[Gaza]	2012-Jul 2023	
	Patchwork, Dropping Elephant		2013-Jun 2025	
	Stone Panda, APT 10, menuPass		2006-Mar 2025	
	Transparent Tribe, APT 36		2013-Mar 2025	

10 groups listed (10 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=db474214-31e9-4b10-a68b-18bc06b2ddc4