Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:34:31 UTC

Tool: njRAT

Names	njRAT Bladabindi Jorik
Category	Malware
Type	Backdoor, Keylogger, Credential stealer, Info stealer, Downloader, Exfiltration
Description	(Carbon Black) njRAT is a Remote Access Trojan (RAT) that will silently collect and steal sensitive information such as login credentials. It can also perform keylogger monitoring, remote desktop control, installing additional malicious software, and many other malicious activities on the victim's computer. In addition, njRAT is still a malware family that is being actively distributed via various methods such as spear-phishing, malvertising, exploit kits and other techniques. Figure 1 shows a screenshot for the njRAT Panel Menu. Depending on the configuration taken from the attackers in njRAT panel, the features it provided can be used to perform malicious activities such as stealing sensitive data/information, disabling security software, install additional malicious payload to the victim's computer and many more harmful actions. Upon the execution of njRAT, it will connect to the command and control (C&C) server, allowing the attacker to perform malicious activity on the victim's machine. Other than that, it will create copies of itself in the %Temp% folder and rename itself by masquerading as a legitimate binary. In this example it was renamed to 'svhost.exe' which is trying to imitate 'svchost.exe'. Furthermore, it tries to hide its persistence from the user by setting the file attributes as 'Hidden' onto the original and the copy of the binary. Moreover, it will also make a copy of itself in the "%AppData%\Microsoft\Windows\Start Menu" folder and create or modify the registry key for persistence to ensure it will be executed on startup. The following event logs from CB Threat Hunter shown below display the relevant events.

Information	<https://www.carbonblack.com/2019/12/10/threat-analysis-unit-tau-threat-intelligence-notification-njrat/> <http://threatgeek.typepad.com/files/fta-1009---njrat-uncovered-1.pdf> <http://csecybsec.com/download/zlab/20171221_CSE_Bladabindi_Report.pdf> <http://blog.trendmicro.com/trendlabs-security-intelligence/new-rats-emerge-from-leaked-njw0rm-source-code/> <https://blog.fortinet.com/2016/11/30/bladabindi-remains-a-constant-threat-by-using-dynamic-dns-services> <https://researchcenter.paloaltonetworks.com/2018/08/unit42-gorgon-group-slithering-nation-state-cybercrime/> <https://unit42.paloaltonetworks.com/njrat-pastebin-command-and-control/> <https://www.zscaler.com/blogs/research/njrat-pushes-lime-ransomware-and-crypto-wallet-grabbers>
MITRE ATT&CK	<https://attack.mitre.org/software/S0385/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.njrat>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:njRAT>

Last change to this tool card: 20 January 2021

Download this tool card in JSON format

All groups using tool njRAT

Changed	Name	Country	Observed	
APT groups				
	Aggah	[Unknown]	2018-Jun 2022	
	APT 41		2012-Jul 2025	
	Aquatic Panda		2020	
	Blind Eagle		2018-Nov 2024	
	Gorgon Group		2017-Jul 2020	
	Group5		2015	
	LazyScripter	[Unknown]	2018	

	Molerats, Extreme Jackal, Gaza Cybergang	[Gaza]	2012-Jul 2023	
	OilAlpha		2022	
	Operation Comando	[Unknown]	2018	
	Operation Epic Manchego	[Unknown]	2020	
	Operation Layover		2013	
	Operation Spalax	[Unknown]	2020	
	RATicate	[Unknown]	2019	
	RedAlpha		2015-2021	
	RevengeHotels	[Unknown]	2015	
	SideCopy		2019-Mar 2025	
	Sphinx	[Unknown]	2014	
	↳ Subgroup: Goldmouse, APT-C-27		2014	
	↳ Subgroup: Pat Bear, APT-C-37		2015	
	TA558	[Unknown]	2018-Jun 2023	
	Transparent Tribe, APT 36		2013-Mar 2025	

22 groups listed (22 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a442ea06-de48-42e2-beb3-7f2ce7a438b5