NjRAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:43:56 UTC

NjRAT

aka: Bladabindi, Lime-Worm

Actor(s): AQUATIC PANDA, Earth Lusca, Operation C-Major, The Gorgon Group

URLhaus

RedPacket Security describes NJRat as "a remote access trojan (RAT) has capabilities to log keystrokes, access the victim's camera, steal credentials stored in browsers, open a reverse shell, upload/download files, view the victim's desktop, perform process, file, and registry manipulations, and capabilities to let the attacker update, uninstall, restart, close, disconnect the RAT and rename its campaign ID. Through the Command & Control (CnC) server software, the attacker has capabilities to create and configure the malware to spread through USB drives."

It is supposedly popular with actors in the Middle East. Similar to other RATs, many leaked builders may be backdoored.

References

2026-02-02 · Netresec ·
njRAT runs MassLogger
MASS Logger NjRAT

2025-08-26 · Recorded Future · Insikt Group
TAG-144’s Persistent Grip on South American Organizations
AsyncRAT BitRAT DCRat LimeRAT NjRAT PureCrypter Quasar RAT Remcos

2025-07-14 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update January to June 2025
Coper FluBot Hook Joker Mirai AsyncRAT BianLian BumbleBee Chaos Cobalt Strike DanaBot DCRat Havoc Latrodectus NjRAT Quasar RAT RedLine Stealer Remcos Rhadamanthys Sliver ValleyRAT WarmCookie XWorm

2025-04-28 · Netresec · Erik Hjelmvik
Decoding njRAT traffic with NetworkMiner

NjRAT

2025-03-11 · The Hacker News · Ravie Lakshmanan

Blind Eagle Hacks Colombian Institutions Using NTLM Flaw, RATs and GitHub-Based Attacks

AsyncRAT NjRAT Quasar RAT Remcos

2025-02-12 · Red Canary · Phil Hagen, Tony Lambert

Defying tunneling: A Wicked approach to detecting malicious network traffic

AsyncRAT DCRat NjRAT XWorm

2025-01-10 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update July to December 2024

Coper FluBot Hook Mirai FAKEUPDATES AsyncRAT BianLian Brute Ratel C4 Cobalt Strike DanaBot DCRat Havoc Latrodectus NjRAT Quasar RAT RedLine Stealer Remcos Rhadamanthys Sliver Stealc

2024-08-09 · BreachNova · Osama Ellahi

Full analysis on NJRAT

NjRAT

2024-07-09 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update January to June 2024

Coper FluBot Hook Bashlite Mirai FAKEUPDATES AsyncRAT BianLian Cobalt Strike DCRat Havoc NjRAT QakBot Quasar RAT RedLine Stealer Remcos Rhadamanthys RisePro Sliver

2024-05-14 · Check Point Research · Antonis Terefos, Tera0017

Foxit PDF “Flawed Design” Exploitation

Rafel RAT Agent Tesla AsyncRAT DCRat DONOT Nanocore RAT NjRAT Pony Remcos Venom RAT XWorm

2024-03-19 · Medium b.magnezi · 0xMrMagnezi

Malware Analysis NjRat

NjRAT

2024-01-12 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q4 2023

FluBot Hook FAKEUPDATES AsyncRAT BianLian Cobalt Strike DCRat Havoc IcedID Lumma Stealer Meterpreter NjRAT Pikabot QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver

2023-11-22 · Twitter (@embee_research) · Embee_research

Practical Queries for Malware Infrastructure - Part 3 (Advanced Examples)

BianLian Xtreme RAT NjRAT QakBot RedLine Stealer Remcos

2023-11-21 · Medium infoSec Write-ups · JustAnother-Engineer

Unmasking NJRat: A Deep Dive into a Notorious Remote Access Trojan Part1

NjRAT

2023-10-21 · Infosec Writeups · Osama Ellahi
Malware analysis NJ RAT 0.7NC & 0.6.4
NjRAT

2023-10-12 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update Q3 2023
FluBot AsyncRAT Ave Maria Cobalt Strike DCRat Havoc IcedID ISFB Nanocore RAT NjRAT QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Stealc Tofsee Vidar

2023-07-11 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update Q2 2023
Hydra AsyncRAT Aurora Stealer Ave Maria BumbleBee Cobalt Strike DCRat Havoc IcedID ISFB NjRAT QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Tofsee

2023-04-12 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update Q1 2023
FluBot Amadey AsyncRAT Aurora Ave Maria BumbleBee Cobalt Strike DCRat Emotet IcedID ISFB NjRAT QakBot RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Tofsee Vidar

2023-04-10 · Check Point · Check Point
March 2023's Most Wanted Malware: New Emotet Campaign Bypasses Microsoft Blocks to Distribute Malicious OneNote Files
Agent Tesla CloudEyE Emotet Formbook Nanocore RAT NjRAT QakBot Remcos Tofsee

2023-03-15 · Lab52 · Lab52
APT-C-36: from NjRAT to LimeRAT
AsyncRAT NjRAT

2023-01-17 · Trend Micro · Aliakbar Zahravi, Peter Girnus
Earth Bogle: Campaigns Target the Middle East with Geopolitical Lures
NjRAT

2022-12-24 · di.sclosu.re · di.sclosu.re
njRAT malware spreading through Discord CDN and Facebook Ads
NjRAT

2022-10-13 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update Q3 2022
FluBot Arkei Stealer AsyncRAT Ave Maria BumbleBee Cobalt Strike DCRat Dridex Emotet Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT QakBot RecordBreaker RedLine Stealer Remcos Socelars Tofsee Vjw0rm

2022-08-18 · Proofpoint · Joe Wise, Proofpoint Threat Research Team, Selena Larson
Reservations Requested: TA558 Targets Hospitality and Travel
AsyncRAT Loda NjRAT Ozone RAT Revenge RAT Vjw0rm

2022-08-17 · · 360 · 360 Threat Intelligence Center
Kasablanka organizes attacks against political groups and non-profit organizations in the Middle East
SpyNote Loda Nanocore RAT NjRAT

2022-08-12 · Brandefense · Brandefense
Mythic Leopard APT Group
Crimson RAT DarkComet NjRAT Oblique RAT Peppy RAT

2022-05-12 · Morphisec · Hido Cohen
New SYK Crypter Distributed Via Discord
AsyncRAT Ave Maria Nanocore RAT NjRAT Quasar RAT RedLine Stealer

2022-05-09 · Blackberry · The BlackBerry Research & Intelligence Team
Dirty Deeds Done Dirt Cheap: Russian RAT Offers Backdoor Bargains
DCRat NjRAT

2022-03-23 · · EcuCert · EcuCert
APT-C-36 Advanced Persistent Threat Campaign Could be present in Ecuador
NjRAT APT-C-36

2022-03-09 · Lab52 · Lab52
Very very lazy Lazyscripter's scripts: double compromise in a single obfuscation
NjRAT

2022-02-08 · Intel 471 · Intel 471
PrivateLoader: The first step in many malware schemes
Dridex Kronos LockBit Nanocore RAT NjRAT PrivateLoader Quasar RAT RedLine Stealer Remcos SmokeLoader STOP Tofsee TrickBot Vidar

2022-02-03 · forensicitguy · Tony Lambert
njRAT Installed from a MSI
NjRAT

2022-01-12 · Cyber And Ramen blog · Mike R
Analysis of njRAT PowerPoint Macros
NjRAT

2021-11-30 · CYBER GEEKS All Things Infosec · CyberMasterV
Just another analysis of the njRAT malware – A step-by-step approach
NjRAT

2021-11-29 · Trend Micro · Jaromír Hořejší
Campaign Abusing Legitimate Remote Administrator Tools Uses Fake Cryptocurrency Websites
AsyncRAT Azorult Nanocore RAT NjRAT RedLine Stealer Remcos

2021-11-11 · Microsoft · Microsoft 365 Defender Threat Intelligence Team
HTML smuggling surges: Highly evasive loader technique increasingly used in banking malware, targeted

attacks
AsyncRAT Mekotio NjRAT

2021-10-26 · Kaspersky · Kaspersky Lab ICS CERT
APT attacks on industrial organizations in H1 2021
8.t Dropper AllaKore AsyncRAT GoldMax LimeRAT NjRAT NoxPlayer Raindrop ReverseRAT ShadowPad Zebrocy

2021-10-15 · ESET Research · ESET Research
Tweet on a malicious campaign targeting governmental and education entities in Colombia using multiple stages to drop AsyncRAT or njRAT Keylogger on their victims
AsyncRAT NjRAT

2021-09-20 · Trend Micro · Aliakbar Zahravi, William Gamazo Sanchez
Water Basilisk Uses New HCrypt Variant to Flood Victims with RAT Payloads
Ave Maria BitRAT LimeRAT Nanocore RAT NjRAT Quasar RAT

2021-09-16 · Cisco · Tiago Pereira, Vitor Ventura
Operation Layover: How we tracked an attack on the aviation industry to five years of compromise
AsyncRAT Houdini NjRAT

2021-09-13 · Trend Micro · Daniel Lunghi, Jaromír Hořejší
APT-C-36 Updates Its Spam Campaign Against South American Entities With Commodity RATs (IOCs)
AsyncRAT Ave Maria BitRAT Imminent Monitor RAT LimeRAT NjRAT Remcos

2021-09-13 · Trend Micro · Daniel Lunghi, Jaromír Hořejší
APT-C-36 Updates Its Spam Campaign Against South American Entities With Commodity RATs
AsyncRAT Ave Maria BitRAT Imminent Monitor RAT LimeRAT NjRAT Remcos

2021-08-19 · Talos · Asheer Malhotra, Vanja Svajcer, Vitor Ventura
Malicious Campaign Targets Latin America: The seller, The operator and a curious link
AsyncRAT NjRAT

2021-07-30 · Menlo Security · MENLO Security
ISOMorph Infection: In-Depth Analysis of a New HTML Smuggling Campaign
AsyncRAT NjRAT

2021-07-12 · Cipher Tech Solutions · Claire Zaboeva, Dan Dash, Melissa Frydrych
RoboSki and Global Recovery: Automation to Combat Evolving Obfuscation
404 Keylogger Agent Tesla AsyncRAT Ave Maria Azorult BitRAT Formbook HawkEye Keylogger Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT Quasar RAT RedLine Stealer Remcos

2021-07-12 · IBM · Claire Zaboeva, Dan Dash, Melissa Frydrych
RoboSki and Global Recovery: Automation to Combat Evolving Obfuscation
404 Keylogger Agent Tesla AsyncRAT Ave Maria Azorult BitRAT Formbook HawkEye Keylogger Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT Quasar RAT RedLine Stealer Remcos

2021-07-09 · Seqrite · Chaitanya Haritash, Nihar Deshpande, Shayak Tarafdar
Seqrite uncovers second wave of Operation SideCopy targeting Indian critical infrastructure PSUs
NjRAT ReverseRAT

2021-07-07 · Talos · Asheer Malhotra, Justin Thattil
InSideCopy: How this APT continues to evolve its arsenal (Network IOCs)
AllaKore Lilith NjRAT

2021-07-07 · Talos · Asheer Malhotra, Justin Thattil
InSideCopy: How this APT continues to evolve its arsenal (IOCs)
AllaKore Lilith NjRAT

2021-07-07 · Talos · Asheer Malhotra, Justin Thattil
InSideCopy: How this APT continues to evolve its arsenal
AllaKore Lilith NjRAT

2021-07-07 · Talos Intelligence · Asheer Malhotra, Justin Thattil
InSideCopy: How this APT continues to evolve its arsenal
AllaKore NjRAT SideCopy

2021-07-02 · Cisco · Asheer Malhotra, Justin Thattil
InSideCopy: How this APT continues to evolve its arsenal
AllaKore CetaRAT Lilith NjRAT ReverseRAT

2021-05-05 · Zscaler · Aniruddha Dolas, Manohar Ghule, Mohd Sadique
Catching RATs Over Custom Protocols Analysis of top non-HTTP/S threats
Agent Tesla AsyncRAT Crimson RAT CyberGate Ghost RAT Nanocore RAT NetWire RC NjRAT Quasar RAT Remcos

2021-04-21 · Facebook · David Agranovich, Mike Dvilyanski
Taking Action Against Hackers in Palestine
SpyNote Houdini NjRAT

2021-03-22 · K7 Security · Mary Muthu Francisca
MalSpam Campaigns Download njRAT from Paste Sites
NjRAT

2021-03-21 · Blackberry · Blackberry Research
2021 Threat Report
Bashlite FritzFrog IPStorm Mirai Tsunami elf.wellmess AppleJeus Dacls EvilQuest Manuscrypt Astaroth BazarBackdoor Cerber Cobalt Strike Emotet FinFisher RAT Kwampirs MimiKatz NjRAT Ryuk SmokeLoader TrickBot

2021-02-25 · Intezer · Intezer
Year of the Gopher A 2020 Go Malware Round-Up

NiuB WellMail elf.wellmess ArdaMax AsyncRAT CyberGate DarkComet Glupteba Nanocore RAT Nefilim NjRAT Quasar RAT WellMess Zebrocy

2021-01-11 · ESET Research · Matías Porolli

Operation Spalax: Targeted malware attacks in Colombia

Agent Tesla AsyncRAT NjRAT Remcos

2021-01-05 · · Sangfor · Clairvoyance Safety Laboratory

Attack from Mustang Panda? My rabbit is back!

NjRAT

2020-12-21 · Cisco Talos · JON MUNSHAW

2020: The year in malware

WolfRAT Prometei Poet RAT Agent Tesla Astaroth Ave Maria CRAT Emotet Gozi IndigoDrop JhoneRAT Nanocore RAT NjRAT Oblique RAT SmokeLoader StrongPity WastedLocker Zloader

2020-12-10 · Intel 471 · Intel 471

No pandas, just people: The current state of China’s cybercrime underground

Anubis SpyNote AsyncRAT Cobalt Strike Ghost RAT NjRAT

2020-12-09 · Palo Alto Networks Unit 42 · Chris Navarrete, Haozhe Zhang, Yanhui Jia

njRAT Spreading Through Active Pastebin Command and Control Tunnel

NjRAT

2020-12-01 · sonatype · Ax Sharma

There’s a RAT in my code: new npm malware with Bladabindi trojan spotted

NjRAT

2020-11-09 · Bleeping Computer · Ionut Ilascu

Fake Microsoft Teams updates lead to Cobalt Strike deployment

Cobalt Strike DoppelPaymer NjRAT Predator The Thief Zloader

2020-10-26 · · 360 Core Security · 360

北非狐（APT-C-44）攻击活动揭露

Xtreme RAT Houdini NjRAT Revenge RAT

2020-09-21 · Trend Micro · Raphael Centeno

Cybercriminals Distribute Backdoor With VPN Installer

NjRAT

2020-09-01 · nviso · Bart Parys, Didier Stevens, Dries Boone, Maxime Thiebaut, Michel Coene

Epic Manchego – atypical maldoc delivery brings flurry of infostealers

Azorult NjRAT

2020-08-19 · · AhnLab · AhnLab ASEC 분석팀

국내 유명 웹하드를 통해 유포되는 njRAT 악성코드

NjRAT

2020-07-30 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q2 2020

AdWind Agent Tesla Arkei Stealer AsyncRAT Ave Maria Azorult DanaBot Emotet IcedID ISFB KPOT Stealer Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT Pony Raccoon RedLine Stealer Remcos Zloader

2020-07-29 · ESET Research · welivesecurity

THREAT REPORT Q2 2020

DEFENSOR ID HiddenAd Bundlore Pirrit Agent.BTZ Cerber ClipBanker CROSSWALK Cryptowall CTB Locker DanaBot Dharma Formbook Gandcrab Grandoreiro Houdini ISFB LockBit Locky Mailto Maze Microcin Nemty NjRAT Phobos PlugX Pony REvil Socelars STOP Tinba TrickBot WannaCryptor

2020-06-22 · Anurag

njRat Malware Analysis

NjRAT

2020-05-14 · SophosLabs · Markel Picado

RATicate: an attacker’s waves of information-stealing malware

Agent Tesla BetaBot BlackRemote Formbook Loki Password Stealer (PWS) NetWire RC NjRAT Remcos

2020-01-31 · ReversingLabs · Robert Simmons

RATs in the Library: Remote Access Trojans Hide in Plain "Public" Site

CyberGate LimeRAT NjRAT Quasar RAT Revenge RAT

2020-01-01 · Dragos · Joe Slowik

Threat Intelligence and the Limits of Malware Analysis

Exaramel Exaramel Industroyer Lookback NjRAT PlugX

2020-01-01 · Secureworks · SecureWorks

COPPER FIELDSTONE

Crimson RAT DarkComet Luminosity RAT NjRAT Operation C-Major

2019-12-24 · Github (itsKindred) · Derek Kleinhen

Bashar Bachir Infection Chain Analysis

NjRAT

2019-09-26 · Proofpoint · Bryan Campbell, Jeremy Hedges, Proofpoint Threat Insight Team

New WhiteShadow downloader uses Microsoft SQL to retrieve malware

WhiteShadow Agent Tesla Azorult Crimson RAT Formbook Nanocore RAT NetWire RC NjRAT Remcos

2019-09-23 · MITRE · MITRE ATT&CK

APT41

Derusbi MESSAGETAP Winnti ASPXSpy BLACKCOFFEE CHINACHOPPER Cobalt Strike Derusbi Empire Downloader Ghost RAT MimiKatz NjRAT PlugX ShadowPad Winnti ZXShell APT41

2019-08-30 · Github (threatland) · ThreatLand
njRAT builders
NjRAT

2019-08-01 · Kaspersky Labs · GReAT
APT trends report Q2 2019
ZooPark magecart POWERSTATS Chaperone COMpfun EternalPetya FinFisher RAT HawkEye Keylogger HOPLIGHT Microcin NjRAT Olympic Destroyer PLEAD RokRAT Triton Zebrocy

2019-03-25 · · 360 Core Security · zhanghao-ms
Patting the Bear (APT-C-37): Exposure of Continued Attacks Against an Armed Organization
Houdini NjRAT

2018-08-02 · Palo Alto Networks Unit 42 · David Fuertes, Josh Grunzweig, Kyle Wilhoit, Robert Falcone
The Gorgon Group: Slithering Between Nation State and Cybercrime
Loki Password Stealer (PWS) Nanocore RAT NjRAT Quasar RAT Remcos Revenge RAT

2018-07-23 · · 360 Threat Intelligence · Qi Anxin Threat Intelligence Center
Golden Rat Organization-targeted attack in Syria
NjRAT APT-C-27

2016-11-30 · Fortinet · Lilia Elena Gonzalez Medina
Bladabindi Remains A Constant Threat By Using Dynamic DNS Services
NjRAT

2016-10-26 · Unknown · Chris Doman
Moonlight – Targeted attacks in the Middle East
Houdini NjRAT Molerats

2015-01-22 · Trend Micro · Michael Marcos
New RATs Emerge from Leaked Njw0rm Source Code
NjRAT

Yara Rules

▶ [TLP:WHITE] win_njrat_w1 (20170517 | Identify njRat)

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.njrat