Quasar RAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:31:18 UTC

Quasar RAT

aka: CinaRAT, QuasarRAT, Yggdrasil

Actor(s): APT33, Dropping Elephant, Stone Panda, The Gorgon Group

VTCollection URLhaus

Quasar RAT is a malware family written in .NET which is used by a variety of attackers. The malware is fully functional and open source, and is often packed to make analysis of the source more difficult.

References

2026-01-13 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update July to December 2025
Coper FluBot Joker Aisuru Mirai AsyncRAT BianLian Cobalt Strike DCRat Havoc Latrodectus PureLogs Stealer Quasar RAT Remcos Rhadamanthys Sliver ValleyRAT Venom RAT Vidar XWorm

2025-12-18 · Acronis · Acronis Security
Acronis TRU Alliance {Hunt.io}: Hunting DPRK threats - New Global Lazarus & Kimsuky campaigns
BADCALL POOLRAT Quasar RAT

2025-11-10 · Genians · Genians
State-Sponsored Remote Wipe Tactics Targeting Android Devices
Quasar RAT Remcos

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

2025-06-24 · Bridewell · Bridewell
2025 Cyber Threat Intelligence Report
AsyncRAT Brute Ratel C4 Cobalt Strike Fog Ghost RAT Lumma Stealer Meduza Stealer Quasar RAT RedLine Stealer Sliver

2025-04-17 · Proofpoint · Greg Lesnewich, Josh Miller, Mark Kelly, Saher Naumaan
Around the World in 90 Days: State-Sponsored Actors Try ClickFix
Quasar RAT UNK_RemoteRogue

2025-03-13 · Securonix · Den Iyzvyk, Tim Peck
Analyzing OBSCURE#BAT Threat Actors Lure Victims into Executing Malicious Batch Scripts to Deploy Stealthy Rootkits
Quasar RAT r77

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

2025-03-04 · · Genians · Genians
Analysis of Kimsuky Group association with emergency martial arts-themed APT attack
Quasar RAT

2025-02-24 · Kaspersky Labs · Georgy Kucherin, João Godinho
The GitVenom campaign: cryptocurrency theft using GitHub
AsyncRAT Quasar RAT

2025-02-04 · Team Cymru · S2 Research Team
Tracing the Path From SmartApeSG to NetSupport RAT
SmartApeSG NetSupportManager RAT Quasar RAT

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

2025-01-03 · Nimantha Deshappriya
RATs on the island (Remote Access Trojans in Sri Lanka's Cybersecurity Landscape)
AsyncRAT Quasar RAT Remcos

2024-12-12 · Elastic · Daniel Stepanic, Elastic Security Labs, Jia Yu Chan, Salim Bitam, Seth Goodwin
Under the SADBRIDGE with GOSAR: QUASAR Gets a Golang Rewrite
Gosar Quasar RAT SADBRIDGE

2024-09-05 · Zscaler · Gaetano Pellegrino
BlindEagle Targets Colombian Insurance Sector with BlotchyQuasar
Quasar RAT

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

2024-04-11 · Github (jeFF0Falltrades) · Jeff Archer
Rat King Configuration Parser
AsyncRAT DCRat Quasar RAT Venom RAT

2024-01-25 · JSAC 2024 · Masafumi Takeda, Tomoya Furukawa
Threat Intelligence of Abused Public Post-Exploitation Frameworks
AsyncRAT DCRat Empire Downloader GRUNT Havoc Koadic Merlin PoshC2 Quasar RAT Sliver

2024-01-15 · DFIR.ch · Stephan Berger
Hunting AsyncRAT & QuasarRAT
AsyncRAT Quasar RAT

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

2024-01-08 · YouTube (Embee Research) · Embee_research
Malware Analysis - Powershell decoding and .NET C2 Extraction (Quasar RAT)
Quasar RAT

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

2023-09-08 · Gi7w0rm
Uncovering DDGroup — A long-time threat actor
AsyncRAT Ave Maria BitRAT DBatLoader NetWire RC Quasar RAT XWorm

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

2023-06-08 · Twitter (@embee_research) · Embee_research
Practical Queries for Identifying Malware Infrastructure: An informal page for storing Censys/Shodan queries
Amadey AsyncRAT Cobalt Strike QakBot Quasar RAT Sliver solarmarker

2023-05-15 · embeeresearch · Embee_research
Quasar Rat Analysis - Identification of 64 Quasar Servers Using Shodan and Censys
Quasar RAT

2023-04-23 · ESET Research · Alexandre Côté Cyr, Matthieu Faou
TA410: APT10's distant cousin
FlowCloud Lookback PlugX Quasar RAT Tendyron Witchetty

2023-04-13 · OALabs · Sergei Frankoff
Quasar Chaos: Open Source Ransomware Meets Open Source RAT
Chaos Quasar RAT

2023-03-30 · loginsoft · Saharsh Agrawal
From Innocence to Malice: The OneNote Malware Campaign Uncovered
Agent Tesla AsyncRAT DOUBLEBACK Emotet Formbook IcedID NetWire RC QakBot Quasar RAT RedLine Stealer XWorm

2023-02-24 · Zscaler · Avinash Kumar, Niraj Shivtarkar
Snip3 Crypter Reveals New TTPs Over Time
DCRat Quasar RAT

2023-01-05 · Symantec · Threat Hunter Team
Bluebottle: Campaign Hits Banks in French-speaking Countries in Africa
CloudEyE Cobalt Strike MimiKatz NetWire RC POORTRY Quasar RAT BlueBottle

2022-09-13 · Symantec · Threat Hunter Team
New Wave of Espionage Activity Targets Asian Governments
MimiKatz PlugX Quasar RAT ShadowPad Trochilus RAT

2022-08-18 · Sophos · Sean Gallagher
Cookie stealing: the new perimeter bypass
Cobalt Strike Meterpreter MimiKatz Phoenix Keylogger Quasar RAT

2022-07-29 · Qualys · Viren Chaudhari
New Qualys Research Report: Evolution of Quasar RAT
Quasar RAT

2022-07-27 · Qualys · Viren Chaudhari
Stealthy Quasar Evolving to Lead the RAT Race
Quasar RAT

2022-07-13 · Weixin · Antiy CERT
Confucius: The Angler Hidden Under CloudFlare
Quasar RAT

2022-06-23 · Secureworks · Counter Threat Unit ResearchTeam
BRONZE STARLIGHT Ransomware Operations Use HUI Loader

ATOMSILO Cobalt Strike HUI Loader LockFile NightSky Pandora PlugX Quasar RAT Rook SodaMaster BRONZE STARLIGHT

2022-06-02 · FortiGuard Labs · Fred Gutierrez, Gergely Revay, James Slaughter, Shunichi Imano

Threat Actors Prey on Eager Travelers

AsyncRAT NetWire RC Quasar RAT

2022-05-19 · Blackberry · The BlackBerry Research & Intelligence Team

.NET Stubs: Sowing the Seeds of Discord

Agent Tesla Quasar RAT WhisperGate

2022-05-19 · Blackberry · The BlackBerry Research & Intelligence Team

.NET Stubs: Sowing the Seeds of Discord (PureCrypter)

Aberebot AbstractEmu AdoBot 404 Keylogger Agent Tesla Amadey AsyncRAT Ave Maria BitRAT BluStealer Formbook LimeRAT Loki Password Stealer (PWS) Nanocore RAT Orcus RAT Quasar RAT Raccoon RedLine Stealer WhisperGate

2022-05-16 · JPCERT/CC · Shusei Tomonaga

Analysis of HUI Loader

HUI Loader PlugX Poison Ivy Quasar RAT

2022-05-12 · Morphisec · Hido Cohen

New SYK Crypter Distributed Via Discord

AsyncRAT Ave Maria Nanocore RAT NjRAT Quasar RAT RedLine Stealer

2022-04-27 · Trendmicro · Daniel Lunghi, Jaromír Hořejší

Operation Gambling Puppet

reptile oRAT AsyncRAT Cobalt Strike DCRat Ghost RAT PlugX Quasar RAT Trochilus RAT Earth Berberoka

2022-04-27 · Trendmicro · Trendmicro

IOCs for Earth Berberoka - Windows

AsyncRAT Cobalt Strike PlugX Quasar RAT Earth Berberoka

2022-04-27 · Trend Micro · Daniel Lunghi, Jaromír Hořejší

New APT Group Earth Berberoka Targets Gambling Websites With Old and New Malware

HelloBot AsyncRAT Ghost RAT HelloBot PlugX Quasar RAT Earth Berberoka

2022-03-24 · Lab52 · freyit

Another cyber espionage campaign in the Russia-Ukrainian ongoing cyber attacks

Quasar RAT

2022-03-05 · Bleeping Computer · Lawrence Abrams

Malware now using NVIDIA's stolen code signing certificates

Quasar RAT

2022-02-22 · CyCraft Technology Corp

China Implicated in Prolonged Supply Chain Attack Targeting Taiwan Financial Sector

Quasar RAT

2022-02-21 · The Record · Catalin Cimpanu

Chinese hackers linked to months-long attack on Taiwanese financial sector

Quasar RAT

2022-02-21 · · CyCraft · CyCraft AI

An in-depth analysis of the Operation Cache Panda organized supply chain attack on Taiwan's financial industry

Quasar RAT

2022-02-11 · blog.rootshell.be · Xavier Mertens

[SANS ISC] CinaRAT Delivered Through HTML ID Attributes

Quasar RAT

2022-02-08 · ASEC · ASEC

Distribution of Kimsuky Group’s xRAT (Quasar RAT) Confirmed

GoldDragon Quasar RAT

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

2022-01-08 · Bleeping Computer · Lawrence Abrams

Trojanized dnSpy app drops malware cocktail on researchers, devs

Quasar RAT

2021-12-14 · Trend Micro · Nick Dai, Ted Lee, Vickie Su

Collecting In the Dark: Tropic Trooper Targets Transportation and Government

ChiserClient Ghost RAT Lilith Quasar RAT xPack APT23

2021-10-19 · Cisco Talos · Asheer Malhotra

Malicious campaign uses a barrage of commodity RATs to target Afghanistan and India

DCRat Quasar RAT

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

2021-09-03 · Trend Micro · Mohamad Mokbel

The State of SSL/TLS Certificate Usage in Malware C&C Communications

AdWind ostap AsyncRAT BazarBackdoor BitRAT Buer Chthonic CloudEyE Cobalt Strike DCRat Dridex FindPOS GootKit Gozi IcedID ISFB Nanocore RAT Orcus RAT PandaBanker Qadars QakBot Quasar RAT Rockloader ServHelper Shifu SManager TorrentLocker TrickBot Vawtrak Zeus Zloader

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

2021-07-12 · 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

2021-05-27 · MinervaLabs · Tom Roter
Trapping A Fat Quasar RAT
Quasar RAT

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

2021-04-27 · Kaspersky · GReAT
APT trends report Q1 2021
PAS Artra Downloader BadNews Bozok DILLJUICE Kazuar Quasar RAT SodaMaster

2021-04-14 · Zscaler · Atinderpal Singh, Rohit Chaturvedi, Tarun Dewan
A look at HydroJiin campaign
NetWire RC Quasar RAT

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

2021-02-23 · CrowdStrike · CrowdStrike
2021 Global Threat Report
RansomEXX Amadey Anchor Avaddon BazarBackdoor Clop Cobalt Strike Conti Cutwail DanaBot DarkSide DoppelPaymer Dridex Egregor Emotet Hakbit IcedID JSOutProx KerrDown LockBit Mailto Maze MedusaLocker Mespinoza Mount Locker NedDnLoader Nemty Pay2Key PlugX Pushdo PwndLocker PyXie QakBot Quasar RAT RagnarLocker Ragnarok RansomEXX REvil Ryuk Sekhmet ShadowPad SmokeLoader Snake SUNBURST SunCrypt TEARDROP TrickBot WastedLocker Winnti Zloader Evilnum OUTLAW SPIDER RIDDLE SPIDER SOLAR SPIDER VIKING SPIDER

2021-02-05 · Morphisec · Nadav Lorber
CinaRAT Resurfaces with New Evasive Tactics and Techniques
Quasar RAT

2021-01-09 · Marco Ramilli's Blog · Marco Ramilli
Command and Control Traffic Patterns
ostap LaZagne Agent Tesla Azorult Buer Cobalt Strike DanaBot DarkComet Dridex Emotet Formbook IcedID ISFB NetWire RC PlugX Quasar RAT SmokeLoader TrickBot

2020-12-28 · · Antiy CERT · Antiy CERT
"Civerids" organization vs. Middle East area attack activity analysis report
Quasar RAT

2020-12-24 · IronNet · Adam Hlavek
China cyber attacks: the current threat landscape
PLEAD TSCookie FlowCloud Lookback PLEAD PlugX Quasar RAT Winnti

2020-12-10 · JPCERT/CC · Kota Kino
Attack Activities by Quasar Family
AsyncRAT Quasar RAT Venom RAT XPCTRA

2020-12-09 · Cybereason · Cybereason Nocturnus
New Malware Arsenal Abusing Cloud Platforms in Middle East Espionage Campaign
DropBook MoleNet Quasar RAT SharpStage Spark

2020-12-09 · Cybereason · Cybereason Nocturnus Team
MOLERATS IN THE CLOUD: New Malware Arsenal Abuses Cloud Platforms in Middle East Espionage Campaign
DropBook JhoneRAT Molerat Loader Pierogi Quasar RAT SharpStage Spark

2020-11-19 · Threatpost · Elizabeth Montalbano
APT Exploits Microsoft Zerologon Bug: Targets Japanese Companies
Quasar RAT Ryuk

2020-11-17 · Symantec · Threat Hunter Team
Japan-Linked Organizations Targeted in Long-Running and Sophisticated Attack Campaign
Quasar RAT

2020-06-22 · MalwareLab.pl · Maciej Kotowicz
VenomRAT - new, hackforums grade, reincarnation of QuassarRAT
Quasar RAT Venom RAT

2020-05-29 · Zscaler · Sudeep Singh
ShellReset RAT Spread Through Macro-Based Documents Using AppLocker Bypass
Quasar RAT

2020-05-14 · Lab52 · Dex
The energy reserves in the Eastern Mediterranean Sea and a malicious campaign of APT10 against Turkey
Cobalt Strike HTran MimiKatz PlugX Quasar RAT

2020-04-27 · 0x00sec · Dan Lisichkin
Master of RATs - How to create your own Tracker
Quasar RAT

2020-02-21 · ADEO DFIR · ADEO DFIR
APT10 Threat Analysis Report
CHINACHOPPER HTran MimiKatz PlugX Quasar RAT

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

2020-01-17 · JPCERT/CC · Takayoshi Shiigi
Looking back on the incidents in 2019
TSCookie NodeRAT Emotet PoshC2 Quasar RAT

2020-01-01 · Secureworks · SecureWorks
ALUMINUM SARATOGA
BlackShades DarkComet Xtreme RAT Poison Ivy Quasar RAT Molerats

2020-01-01 · Secureworks · SecureWorks
BRONZE RIVERSIDE
Anel ChChes Cobalt Strike PlugX Poison Ivy Quasar RAT RedLeaves APT10

2019-11-19 · FireEye · Kelli Vanderlee, Nalani Fraser
Achievement Unlocked: Chinese Cyber Espionage Evolves to Support Higher Level Missions
MESSAGETAP TSCookie ACEHASH CHINACHOPPER Cobalt Strike Derusbi Empire Downloader Ghost RAT HIGHNOON HTran MimiKatz NetWire RC POISONPLUG Poison Ivy pupy Quasar RAT ZXShell

2019-05-24 · Fortinet · Ben Hunter
Uncovering new Activity by APT10
PlugX Quasar RAT

2019-05-20 · Twitter (@struppigel) · Karsten Hahn
Tweet on Yggdrasil / CinaRAT
Quasar RAT

2019-04-16 · FireEye · Ben Read, Chi-en Shen, John Hultquist, Oleg Bondarenko
Spear Phishing Campaign Targets Ukraine Government and Military; Infrastructure Reveals Potential Link to So-Called Luhansk People's Republic
Quasar RAT Vermin

2019-04-01 · · Macnica Networks · Macnica Networks
Trends in Cyber Espionage Targeting Japan 2nd Half of 2018
Anel Cobalt Strike Datper PLEAD Quasar RAT RedLeaves taidoor Zebrocy

2019-03-27 · Symantec · Security Response Attack Investigation Team

Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.

DarkComet Nanocore RAT pupy Quasar RAT Remcos TURNEDUP APT33

2019-03-27 · Symantec · Critical Attack Discovery and Intelligence Team

Elfin: Relentless Espionage Group Targets Multiple Organizations in Saudi Arabia and U.S.

DarkComet MimiKatz Nanocore RAT NetWire RC pupy Quasar RAT Remcos StoneDrill TURNEDUP APT33

2019-02-14 · CISA · CISA

AR18-352A: Quasar Open-Source Remote Administration Tool

Quasar RAT

2018-10-01 · · Macnica Networks · Macnica Networks

Trends in cyber espionage (targeted attacks) targeting Japan | First half of 2018

Anel Cobalt Strike Datper FlawedAmmyy Quasar RAT RedLeaves taidoor Winnti xxmm

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

2018-07-17 · ESET Research · Kaspars Osis

A deep dive down the Vermin RAThole

Quasar RAT Sobaken Vermin

2018-06-07 · Volexity · Matthew Meltzer, Sean Koessel, Steven Adair

Patchwork APT Group Targets US Think Tanks

Quasar RAT Unidentified 047 QUILTED TIGER

2018-03-30 · · 360 Threat Intelligence · Qi Anxin Threat Intelligence Center

Analysis of the latest cyber attack activity of the APT organization against sensitive institutions in China

Quasar RAT

2017-12-11 · Trend Micro · Cedric Pernet, Daniel Lunghi, Jaromír Hořejší

Untangling the Patchwork Cyberespionage Group

Quasar RAT

2017-04-01 · PricewaterhouseCoopers · PricewaterhouseCoopers

Operation Cloud Hopper: Technical Annex

ChChes PlugX Quasar RAT RedLeaves Trochilus RAT

2017-01-30 · Palo Alto Networks Unit 42 · Mashav Sapir, Netanel Rimer, Simon Conant, Taras Malivanchuk, Tomer Bar, Yaron Samuel

Downeks and Quasar RAT Used in Recent Targeted Attacks Against Governments

Quasar RAT

2016-10-20 · Twitter (@malwrhunterteam) · MalwareHunterTeam

Tweet on Quasar RAT

Quasar RAT

Yara Rules

▶ [TLP:WHITE] win_quasar_rat_auto (20180607 | autogenerated rule brought to you by yara-signator)

Download all Yara Rules

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