AsyncRAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 13:09:51 UTC

AsyncRAT

VTCollection

AsyncRAT is a Remote Access Tool (RAT) designed to remotely monitor and control other computers through a secure encrypted connection. It is an open source remote administration tool, however, it could also be used maliciously because it provides functionality such as keylogger, remote desktop control, and many other functions that may cause harm to the victim's computer. In addition, AsyncRAT can be delivered via various methods such as spear-phishing, malvertising, exploit kit and other techniques.

References

2026-01-29 · Censys ·
AsyncRAT C2 Activity at Internet Scale
AsyncRAT

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

2025-09-18 · Hunt.io · Hunt.io
Tracking AsyncRAT via Trojanized ScreenConnect and Open Directories
AsyncRAT

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

2025-06-12 · Check Point Research · Check Point
From Trust to Threat: Hijacked Discord Invites Used for Multi-Stage Malware Delivery
AsyncRAT Skuld

2025-06-05 · Hunt.io · Hunt.io
Abusing Paste.ee to Deploy XWorm and AsyncRAT Across Global C2 Infrastructure
AsyncRAT XWorm

2025-04-23 · Medium b.magnezi · 0xMrMagnezi
AsyncRAT Malware Analysis
AsyncRAT

2025-04-22 · AhnLab · ASEC
Distribution of PebbleDash Malware in March 2025
AsyncRAT PEBBLEDASH

2025-03-26 · ThreatMon · Aziz Kaplan, ThreatMon, ThreatMon Malware Research Team
Raton / Silly - Remote Access Trojan | Technical Malware Analysis Report
AsyncRAT

2025-03-18 · WeLiveSecurity · Dominik Breitenbacher
Operation AkaiRyū: MirrorFace invites Europe to Expo 2025 and revives ANEL backdoor
Anel AsyncRAT

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

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

2025-02-12 · Red Canary · Phil Hagen, Tony Lambert
Defying tunneling: A Wicked approach to detecting malicious network traffic
AsyncRAT DCRat NjRAT XWorm

2025-02-12 · cyber.wtf blog · Hendrik Eckardt, Leonard Rapp
Unpacking Pyarmor v8+ scripts
AsyncRAT DCRat 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

2025-01-03 · Nimantha Deshappriya

RATs on the island (Remote Access Trojans in Sri Lanka's Cybersecurity Landscape)

AsyncRAT Quasar RAT Remcos

2024-11-21 · Rapid7 · Anna Širokova

A Bag of RATs: VenomRAT vs. AsyncRAT

AsyncRAT Venom RAT

2024-11-18 · Proofpoint · Proofpoint Threat Research Team, Selena Larson, Tommy Madjar

Security Brief: ClickFix Social Engineering Technique Floods Threat Landscape

AsyncRAT Brute Ratel C4 DanaBot DarkGate Latrodectus Lumma Stealer NetSupportManager RAT XWorm

2024-10-16 · ThreatMon · Aziz Kaplan, ThreatMon, ThreatMon Malware Research Team

X-ZIGZAG Technical Malware Analysis Report

AsyncRAT X-ZIGZAG

2024-07-17 · Huntress Labs · Alden Schmidt, Greg Linares, Matt Anderson

Fake Browser Updates Lead to BOINC Volunteer Computing Software

FAKEUPDATES MintsLoader AsyncRAT

2024-07-16 · Sentinel LABS · Jim Walter

NullBulge | Threat Actor Masquerades as Hacktivist Group Rebelling Against AI

AsyncRAT LockBit XWorm Nullbulge

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

2024-04-20 · Axel's IT Security Research · Axel Mahr

New Robust Technique for Reliably Identifying AsyncRAT/DcRAT/VenomRAT Servers

AsyncRAT DCRat Venom RAT

2024-04-13 · cyber5w · cyber5w, M4lcode

Analysis of malicious Microsoft office macros

AsyncRAT Ave Maria

2024-04-11 · Github (jeFF0Falltrades) · Jeff Archer

Rat King Configuration Parser

AsyncRAT DCRat Quasar RAT Venom RAT

2024-02-09 · Censys · Censys, Embee_research

A Beginners Guide to Tracking Malware Infrastructure

AsyncRAT BianLian Cobalt Strike QakBot

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

2024-01-09 · Recorded Future · Insikt Group

2023 Adversary Infrastructure Report

AsyncRAT Cobalt Strike Emotet PlugX ShadowPad

2024-01-05 · AlienLabs · Fernando Martinez

AsyncRAT loader: Obfuscation, DGAs, decoys and Govno

MintsLoader AsyncRAT

2023-12-13 · cocomelonc · cocomelonc

Malware in the wild book

AsyncRAT Babuk BlackCat BlackLotus Carbanak HelloKitty Paradise Stealc WinDealer

2023-12-12 · Check Point Research · Check Point

November 2023’s Most Wanted Malware: New AsyncRAT Campaign Discovered while FakeUpdates Re-Entered the Top Ten after Brief Hiatus

FAKEUPDATES AsyncRAT

2023-12-02 · openhunting.io · openhunting.io

Threat Hunting Malware Infrastructure

VBREVSHELL AsyncRAT

2023-11-01 · Twitter (@embee_research) · Embee_research

Malware Unpacking With Memory Dumps - Intermediate Methods (Pe-Sieve, Process Hacker, Hxd and Pe-bear)

AsyncRAT

2023-10-30 · Twitter (@embee_research) · Embee_research
Unpacking .NET Malware With Process Hacker and Dnspy
AsyncRAT

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

2023-07-20 · Gatewatcher · Gatewatcher
zip-files-make-it-bigger-to-avoid-edr-detection
AsyncRAT

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

2023-05-19 · cocomelonc · cocomelonc
Malware source code investigation: AsyncRAT
AsyncRAT

2023-05-09 · Huntress Labs · Matthew Brennan
Advanced Cyberchef Tips - AsyncRAT Loader
AsyncRAT

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

2023-04-08 · kienmanowar Blog · m4n0w4r, Tran Trung Kien
[QuickNote] Uncovering Suspected Malware Distributed By Individuals from Vietnam
AsyncRAT DCRat WorldWind

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

2023-03-27 · splunk · Splunk Threat Research Team

AsyncRAT Crusade: Detections and Defense

AsyncRAT

2023-03-15 · Lab52 · Lab52

APT-C-36: from NjRAT to LimeRAT

AsyncRAT NjRAT

2023-03-01 · Zscaler · Meghraj Nandanwar, Shatak Jain

OneNote: A Growing Threat for Malware Distribution

AsyncRAT Cobalt Strike IcedID QakBot RedLine Stealer

2023-02-27 · Blackberry · BlackBerry Research & Intelligence Team

Blind Eagle Deploys Fake UUE Files and Fsociety to Target Colombia's Judiciary, Financial, Public, and Law Enforcement Entities

AsyncRAT APT-C-36

2023-02-11 · @0xToxin

AsyncRAT OneNote Dropper

AsyncRAT

2023-02-08 · Huntress Labs · Michael Elford

AsyncRAT: Analysing the Three Stages of Execution

AsyncRAT

2023-01-04 · cocomelonc

Malware development tricks: part 26. Mutex. C++ example.

AsyncRAT Conti HelloKitty

2022-12-06 · · 360 Threat Intelligence Center · 360 Beacon Lab

Analysis of suspected APT-C-56 (Transparent Tribe) attacks against terrorism

AhMyth Meterpreter SpyNote AsyncRAT

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

2022-09-06 · Check Point · Check Point Research

DangerousSavanna: Two-year long campaign targets financial institutions in French-speaking Africa

AsyncRAT Meterpreter PoshC2 DangerousSavanna

2022-08-29 · · 360 netlab · wanghao

PureCrypter Loader continues to be active and has spread to more than 10 other families

404 Keylogger Agent Tesla AsyncRAT Formbook RedLine Stealer

2022-08-29 · Netskope · Gustavo Palazolo

AsyncRAT: Using Fully Undetected Downloader

AsyncRAT

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 · Secureworks · Counter Threat Unit ResearchTeam

DarkTortilla Malware Analysis

Agent Tesla AsyncRAT Cobalt Strike DarkTortilla Nanocore RAT RedLine Stealer

2022-08-16 · Qualys · Pawan Kumar N

AsyncRAT C2 Framework: Overview, Technical Analysis & Detection

AsyncRAT

2022-07-17 · Resecurity · Resecurity

Shortcut-Based (LNK) Attacks Delivering Malicious Code On The Rise

AsyncRAT BumbleBee Emotet IcedID QakBot

2022-07-15 · HP · Patrick Schläpfer

Stealthy OpenDocument Malware Deployed Against Latin American Hotels

AsyncRAT

2022-07-13 · Trellix · Mohsin Dalla, Sushant Kumar Arya

Targeted Attack on Government Agencies

AsyncRAT LimeRAT

2022-06-08 · Symantec · Karthikeyan C Kasiviswanathan, Yuvaraj Megavarnadu

Attackers Exploit MSDT Follina Bug to Drop RAT, Infostealer

AsyncRAT

2022-06-03 · Avast · Threat Intelligence Team

Outbreak of Follina in Australia

AsyncRAT

2022-06-03 · Avast Decoded · Threat Intelligence Team

Outbreak of Follina in Australia

AsyncRAT APT40

2022-06-02 · FortiGuard Labs · Fred Gutierrez, Gergely Revay, James Slaughter, Shunichi Imano
Threat Actors Prey on Eager Travelers
AsyncRAT NetWire RC Quasar RAT

2022-06-01 · Github (jstnk9) · Jose Luis Sánchez Martínez
Analyzing AsyncRAT distributed in Colombia
AsyncRAT

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

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

2022-05-11 · HP · HP Wolf Security
Threat Insights Report Q1 - 2022
AsyncRAT Emotet Mekotio Vjw0rm

2022-05-06 · Mitchell's Musings · Aiden Mitchell
Attempted AsyncRAT via .vbs
AsyncRAT

2022-05-02 · eSentire · eSentire Threat Response Unit (TRU)
AsyncRAT Activity
AsyncRAT

2022-04-28 · vx-underground · Twitter (@vxunderground)
Tweet on leaked Prynt Stealer source code and similarity to AyncRAT
AsyncRAT Prynt Stealer

2022-04-27 · Zscaler · Brett Stone-Gross, Dennis Schwarz
Targeted attack on Thailand Pass customers delivers AsyncRAT
AsyncRAT

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

2022-04-26 · Trend Micro · Lord Alfred Remorin, Ryan Flores, Stephen Hilt
How Cybercriminals Abuse Cloud Tunneling Services
AsyncRAT Cobalt Strike DarkComet Meterpreter Nanocore RAT

2022-04-19 · RiskIQ · Jennifer Grob
RiskIQ: Legitimate WordPress Site Hosts Malicious Content
AsyncRAT

2022-04-05 · Cisco Talos · Alex Karkins, Edmund Brumaghin
Threat Spotlight: AsyncRAT campaigns feature new version of 3LOSH crypter
AsyncRAT LimeRAT

2022-03-31 · eSentire · eSentire Threat Response Unit (TRU)
Suspected AsyncRAT Delivered via ISO Files Using HTML Smuggling Technique
AsyncRAT

2022-03-12 · Brian Stadnicki
AsyncRAT RCE vulnerability
AsyncRAT

2022-03-01 · VirusTotal · VirusTotal
VirusTotal's 2021 Malware Trends Report
Anubis AsyncRAT BlackMatter Cobalt Strike DanaBot Dridex Khonsari MimiKatz Mirai Nanocore RAT Orcus RAT

2022-02-22 · NCSC Switzerland · NCSC Switzerland
Week 7: Supposed order confirmation delivers malware and new variants in fake extortion emails
AsyncRAT

2022-02-16 · Abdallah Elnoty
Playing with AsyncRAT
AsyncRAT

2022-02-15 · Proofpoint · Joe Wise, Selena Larson
Charting TA2541's Flight
AsyncRAT TA2541

2022-02-15 · Threat Post · Elizabeth Montalbano
TA2541: APT Has Been Shooting RATs at Aviation for Years
AsyncRAT Houdini NetWire RC Parallax RAT

2022-02-15 · BleepingComputer · Ionut Ilascu
Unskilled hacker linked to years of attacks on aviation, transport sectors

AsyncRAT Houdini NetWire RC Parallax RAT

2022-02-14 · Morphisec · Arnold Osipov, Hido Cohen

Journey of a Crypto Scammer - NFT-001

AsyncRAT BitRAT Remcos

2022-02-07 · RiskIQ · RiskIQ

RiskIQ: Malicious Infrastructure Connected to Particular Windows Host Certificates

AsyncRAT BitRAT Nanocore RAT

2022-01-26 · The Hacker News · Ravie Lakshmanan

Hackers Using New Evasive Technique to Deliver AsyncRAT Malware

AsyncRAT

2022-01-25 · Morphisec · Michael Dereviashkin

New Threat Campaign Identified: AsyncRAT Introduces a New Delivery Technique

AsyncRAT

2022-01-12 · Cisco · Chetan Raghuprasad, Vanja Svajcer

Nanocore, Netwire and AsyncRAT spreading campaign uses public cloud infrastructure

AsyncRAT Nanocore RAT NetWire RC

2021-12-29 · Github (jeFF0Falltrades) · Jeff Archer

AsyncRAT Configuration Parser

AsyncRAT

2021-12-13 · RiskIQ · Jordan Herman

RiskIQ: Connections between Nanocore, Netwire, and AsyncRAT and Vjw0rm dynamic DNS C2 infrastructure

AsyncRAT Nanocore RAT NetWire RC Vjw0rm

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

2021-09-16 · 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
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 (IOCs)
AsyncRAT Ave Maria BitRAT Imminent Monitor RAT LimeRAT NjRAT Remcos

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

2021-08-19 · 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

2021-07-19 · Bitdefender · Bitdefender
Debugging MosaicLoader, One Step at a Time
AsyncRAT Glupteba

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

2021-06-27 · Fortinet · Gayathri Thirugnanasambandam
Spear Phishing Campaign with New Techniques Aimed at Aviation Companies
AsyncRAT

2021-05-14 · Morphisec · Arnold Osipov
AHK RAT Loader Used in Unique Delivery Campaigns
AsyncRAT Houdini Revenge RAT

2021-05-11 · Twitter (@MsftSecIntel) · Microsoft Security Intelligence
Tweet on Snip3 crypter delivering AsyncRAT or AgentTesla
Agent Tesla AsyncRAT

2021-05-07 · Morphisec · Nadav Lorber
Revealing the 'Snip3' Crypter, a Highly Evasive RAT Loader
Agent Tesla AsyncRAT NetWire RC Revenge 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

2021-03-16 · Morphisec · Nadav Lorber
Tracking HCrypt: An Active Crypter as a Service
AsyncRAT LimeRAT Remcos

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

2021-02-19 · K7 Security · Partheeban J
GitHub – Home to AsyncRAT Backdoor
AsyncRAT

2021-01-11 · ESET Research · Matías Porolli
Operation Spalax: Targeted malware attacks in Colombia
Agent Tesla AsyncRAT NjRAT Remcos

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

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

2020-11-03 · Kaspersky Labs · GReAT
APT trends report Q3 2020
WellMail EVILNUM Janicab Poet RAT AsyncRAT Ave Maria Cobalt Strike Crimson RAT CROSSWALK Dtrack LODEINFO MoriAgent Okrum PlugX POISONPLUG Rover ShadowPad SoreFang Winnti

2020-10-19 · Red Sky Alliance · Yury Polozov
Possible Identity of a Kuwaiti Hacker NYANxCAT
AsyncRAT

2020-09-21 · · Qianxin · RedDrip Team
Operation Tibo: A retaliatory targeted attack from the South Asian APT organization "Mo Luo Suo"
AsyncRAT Darktrack RAT

2020-08-26 · Proofpoint · Proofpoint Threat Research Team
Threat Actor Profile: TA2719 Uses Colorful Lures to Deliver RATs in Local Languages
AsyncRAT Nanocore RAT TA2719

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

2019-11-19 · VMWare Carbon Black · VMWare
Threat Analysis Unit (TAU) Threat Intelligence Notification: AsyncRAT
AsyncRAT

2019-01-19 · Github (NYAN-x-CAT) · NYAN-x-CAT
AsyncRAT: Open-Source Remote Administration Tool For Windows C# (RAT)
AsyncRAT

Yara Rules

▶ [TLP:WHITE] win_asyncrat_auto (20201014 | autogenerated rule brought to you by yara-signator)

▶ [TLP:WHITE] win_asyncrat_w0 (20201006 | detect AsyncRat in memory)

Download all Yara Rules

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