Nanocore RAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:41:42 UTC

Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.

2025-02-27 · Medium b.magnezi ·
NanoCore Malware Analysis
Nanocore RAT 2024-09-03 · Twitter (@embee_research) · Embee_research
Advanced Cyberchef Techniques - Defeating Nanocore Obfuscation With Math and Flow Control
Nanocore RAT 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 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 2023-10-12 · Cluster25 · Cluster25 Threat Intel Team
CVE-2023-38831 Exploited by Pro-Russia Hacking Groups in RU-UA Conflict Zone for Credential Harvesting Operations
Agent Tesla Crimson RAT Nanocore RAT SmokeLoader 2023-09-21 · Medium shaddy43 · Shayan Ahmed Khan
Secrets of commercial RATs! NanoCore dissected
Nanocore RAT 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 2023-02-03 · Cloudsek · Deepanjli Paulraj, Pavan Karthick M
Threat Actors Abuse AI-Generated Youtube Videos to Spread Stealer Malware
Alfonso Stealer Bandit Stealer Cameleon Fabookie Lumma Stealer Nanocore RAT Panda Stealer RecordBreaker RedLine Stealer Stealc STOP Vidar zgRAT 2023-01-09 · YouTube (Embee Research) · Embee_research
Malware Analysis - VBS Decoding With Cyberchef (Nanocore Loader)
Nanocore RAT 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 2022-08-30 · Medium the_abjuri5t · John F
NanoCore RAT Hunting Guide
Nanocore RAT 2022-08-17 · Secureworks · Counter Threat Unit ResearchTeam
DarkTortilla Malware Analysis

Agent Tesla AsyncRAT Cobalt Strike DarkTortilla Nanocore RAT RedLine Stealer 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 2022-05-19 · 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 2022-04-26 · Trend Micro · Lord Alfred Remorin, Ryan Flores, Stephen Hilt

How Cybercriminals Abuse Cloud Tunneling Services

AsyncRAT Cobalt Strike DarkComet Meterpreter Nanocore RAT 2022-04-15 · Center for Internet Security · CIS

Top 10 Malware March 2022

Mirai Shlayer Agent Tesla Ghost RAT Nanocore RAT SectopRAT solarmarker Zeus 2022-03-27 · Medium M3H51N · M3H51N

Malware Analysis — NanoCore Rat

Nanocore RAT 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 2022-02-08 · 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 2022-02-07 · RiskIQ · RiskIQ

RiskIQ: Malicious Infrastructure Connected to Particular Windows Host Certificates

AsyncRAT BitRAT Nanocore RAT 2022-01-12 · Cisco · Chetan Raghuprasad, Vanja Svajcer

Nanocore, Netwire and AsyncRAT spreading campaign uses public cloud infrastructure

AsyncRAT Nanocore RAT NetWire RC 2021-12-13 · 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 2021-10-27 · Proofpoint · Joe Wise, Selena Larson

New Threat Actor Spoofs Philippine Government, COVID-19 Health Data in Widespread RAT Campaigns

Nanocore RAT Remcos TA2722 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 · 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 2021-05-05 · 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 · Talos · Vanja Svajcer

A year of Fajan evolution and Bloomberg themed campaigns

MASS Logger Nanocore RAT NetWire RC Revenge RAT XpertRAT 2021-03-11 · Trustwave · Diana Lopera

Image File Trickery Part II: Fake Icon Delivers NanoCore

Nanocore 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 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 · US-CERT · FBI, MS-ISAC, US-CERT

Alert (AA20-345A): Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data

PerlBot Shlayer Agent Tesla Cerber Dridex Ghost RAT Kovter Maze MedusaLocker Nanocore RAT Nefilim REvil Ryuk Zeus 2020-11-18 · G Data · G-Data

Business as usual: Criminal Activities in Times of a Global Pandemic

Agent Tesla Nanocore RAT NetWire RC Remcos 2020-09-18 · Symantec · Threat Hunter Team

Elfin: Latest U.S. Indictments Appear to Target Iranian Espionage Group

Nanocore RAT 2020-09-17 · FBI · FBI

FBI PIN Number 20200917-001: IRGC-Associated Cyber Operations Against US Company Networks

MimiKatz Nanocore RAT 2020-09-10 · Medium mariohenkel · Mario Henkel

Decrypting NanoCore config and dump all plugins

Nanocore 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 2020-06-07 · Zero2Automated Blog · 0verfl0w

Dealing with Obfuscated Macros, Statically - NanoCore

Nanocore RAT 2020-05-26 · CrowdStrike · Guillermo Taibo

Weaponized Disk Image Files: Analysis, Trends and Remediation

Nanocore RAT 2020-05-14 · 360 Total Security · kate

Vendetta - new threat actor from Europe

Nanocore RAT Remcos 2020-04-15 · Zscaler · Sudeep Singh

Multistage FreeDom loader used in Aggah Campaign to spread Nanocore and AZORult

Azorult Nanocore RAT 2020-04-04 · MalwareInDepth · Myrtus 0x0

Nanocore & CypherIT

Nanocore RAT 2020-04-01 · Cisco · Andrea Kaiser, Shyam Sundar Ramaswami

Navigating Cybersecurity During a Pandemic: Latest Malware and Threat Actors

Azorult CloudEyE Formbook KPOT Stealer Metamorfo Nanocore RAT NetWire RC TrickBot 2020-03-20 · Bitdefender · Liviu Arsene

5 Times More Coronavirus-themed Malware Reports during March

ostap HawkEye Keylogger Koadic Loki Password Stealer (PWS) Nanocore RAT Remcos 2020-02-13 · Talos · Edmund Brumaghin, Nick Biasini

Threat actors attempt to capitalize on coronavirus outbreak

Emotet Nanocore RAT Parallax RAT 2020-01-19 · 360 · kate

BayWorld event, Cyber Attack Against Foreign Trade Industry

Azorult Formbook Nanocore RAT Revenge RAT 2020-01-01 · Secureworks · SecureWorks

COBALT TRINITY

POWERTON pupy Imminent Monitor RAT Koadic Nanocore RAT NetWire RC PoshC2 APT33 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 2019-09-19 · NSHC · ThreatRecon Team

Hagga of SectorH01 continues abusing Bitly, Blogger and Pastebin to deliver RevengeRAT and NanoCore

Nanocore RAT Revenge RAT 2019-08-25 · Github (threatland) · ThreatLand

Nanocor Sample

Nanocore RAT 2019-05-05 · GoggleHeadedHacker Blog · Jacob Pimental

Unpacking NanoCore Sample Using AutoIT

Nanocore RAT 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 2019-03-27 · 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 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 2018-02-26 · Bleeping Computer · Catalin Cimpanu

Nanocore RAT Author Gets 33 Months in Prison

Nanocore RAT 2017-09-20 · FireEye · Jacqueline O'Leary, Josiah Kimble, Kelli Vanderlee, Nalani Fraser

Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware

DROPSHOT Nanocore RAT NetWire RC SHAPESHIFT TURNEDUP APT33
