NetWire RC (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:10:16 UTC

NetWire RC

aka: NetWeird, NetWire, Recam

Actor(s): APT33

VTCollection URLhaus

Netwire is a RAT, its functionality seems focused on password stealing and keylogging, but includes remote control capabilities as well.

Keylog files are stored on the infected machine in an obfuscated form. The algorithm is:

for i in range(0,num_read):
buffer[i] = ((buffer[i]-0x24)^0x9D)&0xFF

References

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

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

2023-03-10 · The Register · Jessica Lyons Hardcastle
FBI and international cops catch a NetWire RAT
NetWire RC

2023-01-30 · Checkpoint · Arie Olshtein
Following the Scent of TrickGate: 6-Year-Old Packer Used to Deploy the Most Wanted Malware
Agent Tesla Azorult Buer Cerber Cobalt Strike Emotet Formbook HawkEye Keylogger Loki Password Stealer (PWS) Maze NetWire RC Remcos REvil TrickBot

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

2022-12-18 · ZAYOTEM · Enes Şakir Çolak

NetWire Technical Analysis Report

NetWire RC

2022-11-06 · LMNTRIX · LMNTRIX

Analysis Of Netwire RAT

NetWire RC

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

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

Threat Actors Prey on Eager Travelers

AsyncRAT NetWire RC Quasar RAT

2022-02-18 · YouTube (John Hammond) · John Hammond

Uncovering NETWIRE Malware - Discovery & Deobfuscation

NetWire RC

2022-02-15 · BleepingComputer · Ionut Ilascu

Unskilled hacker linked to years of attacks on aviation, transport sectors

AsyncRAT Houdini NetWire RC Parallax RAT

2022-02-15 · Threat Post · Elizabeth Montalbano

TA2541: APT Has Been Shooting RATs at Aviation for Years

AsyncRAT Houdini NetWire RC Parallax RAT

2022-02-09 · SentinelOne · Juan Andrés Guerrero-Saade, Tom Hegel

Modified Elephant APT and a Decade of Fabricating Evidence

DarkComet Incubator NetWire RC

2022-02-09 · Sentinel LABS · Tom Hegel

ModifiedElephant APT and a Decade of Fabricating Evidence

DarkComet Incubator NetWire RC ModifiedElephant

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

2021-10-01 · HP · HP Wolf Security
Threat Insights Report Q3 - 2021
STRRAT CloudEyE NetWire RC Remcos TrickBot Vjw0rm

2021-09-23 · Talos · Asheer Malhotra, Justin Thattil, Vanja Svajcer
Operation “Armor Piercer:” Targeted attacks in the Indian subcontinent using commercial RATs
Ave Maria NetWire RC

2021-09-16 · Blackberry · The BlackBerry Research & Intelligence Team
Threat Thursday: NetWire RAT is Coming Down the Line
NetWire RC

2021-09-01 · · 360 Threat Intelligence Center · Advanced Threat Institute
APT-C-56 (Transparent Tribe) Latest Attack Analysis and Associated Suspected Gorgon Group Attack Analysis Alert
Crimson RAT NetWire RC

2021-08-05 · · Twitter (@BaoshengbinCumt) · 2ero
Attacks on NCGSA, MOITT, MOD, NSCP and SCO in Pakistan
NetWire RC

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

2021-06-10 · ZAYOTEM · Fatma Helin Çakmak, Fatma Nur Gözüküçük, Hakan Soysal, Halil Filik, Yasin Mersin
NetWire Technical Analysis Report
NetWire RC

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

2021-04-21 · Talos · Vanja Svajcer
A year of Fajan evolution and Bloomberg themed campaigns
MASS Logger Nanocore RAT NetWire RC Revenge RAT XpertRAT

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

2021-03-18 · Cybereason · Daniel Frank
Cybereason Exposes Campaign Targeting US Taxpayers with NetWire and Remcos Malware
NetWire RC Remcos

2021-02-08 · Arsenal Consulting · Arsenal Consulting
National Investigation Agency VS Sudhir Pralhad Dhawale & others Report 1
NetWire RC

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

2020-11-18 · G Data · G-Data
Business as usual: Criminal Activities in Times of a Global Pandemic
Agent Tesla Nanocore RAT NetWire RC Remcos

2020-09-22 · vmware · Omar Elgebaly, Takahiro Haruyama
Detecting Threats in Real-time With Active C2 Information
Agent.BTZ Cobalt Strike Dacls NetWire RC PoshC2 Winnti

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

2020-07-14 · SophosLabs Uncut · Markel Picado, Sean Gallagher
RATicate upgrades “RATs as a Service” attacks with commercial “crypter”
LokiBot BetaBot CloudEyE NetWire RC

2020-06-15 · Amnesty International · Amnesty International
India: Human Rights Defenders Targeted by a Coordinated Spyware Operation
NetWire RC

2020-05-21 · Malwarebytes · Malwarebytes Labs
Cybercrime tactics and techniques
Ave Maria Azorult DanaBot Loki Password Stealer (PWS) NetWire RC

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

2020-05-06 · Yoroi · Davide Testa, Luca Mella, Luigi Martire

New Cyber Operation Targets Italy: Digging Into the Netwire Attack Chain

NetWire RC

2020-04-03 · Palo Alto Networks Unit 42 · Brad Duncan

GuLoader: Malspam Campaign Installing NetWire RAT

CloudEyE NetWire RC

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

2020-03-05 · · VinCSS · Dang Dinh Phuong

[RE011] Unpack crypter của malware Netwire bằng x64dbg

NetWire RC

2020-01-01 · Secureworks · SecureWorks

COBALT TRINITY

POWERTON pupy Imminent Monitor RAT Koadic Nanocore RAT NetWire RC PoshC2 APT33

2019-11-20 · vmware · Takahiro Haruyama

Active C2 Discovery Using Protocol Emulation Part1 (HYDSEVEN NetWire)

NetWire RC

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

2019-09-26 · 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

2019-09-12 · Avast · Adolf Středa, Luigino Camastra

The tangle of WiryJMPer's obfuscation

NetWire RC

2019-05-08 · Dr.Web · Dr.Web

A new threat for macOS spreads as WhatsApp

NetWire RC

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

2019-01-30 · Samip Pokharel
Analysis of NetWiredRC trojan
NetWire RC

2017-12-06 · Cisco · Christopher Marczewski, Holger Unterbrink
Recam Redux - DeConfusing ConfuserEx
NetWire RC

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

2016-11-28 · Secureworks · Incident Reponse Team
NetWire RAT Steals Payment Card Data
NetWire RC

2014-11-26 · CIRCL · CIRCL
TR-23 Analysis - NetWiredRC malware
NetWire RC

2014-08-04 · Palo Alto Networks Unit 42 · Phil Da Silva, Rob Downs, Ryan Olson
New Release: Decrypting NetWire C2 Traffic
NetWire RC

Yara Rules

▶ [TLP:WHITE] win_netwire_auto (20251219 | Detects win.netwire.)	
▶ [TLP:WHITE] win_netwire_w0 (20170517 | NetWiredRC)	
▶ [TLP:WHITE] win_netwire_w1 (20170517 | No description)	

Download all Yara Rules
