Remcos (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:17:57 UTC

Remcos

aka: RemcosRAT, Remvio, Socmer

Actor(s): APT33, The Gorgon Group, UAC-0050

VTCollection URLhaus

Remcos (acronym of Remote Control & Surveillance Software) is a commercial Remote Access Tool to remotely control computers.

Remcos is advertised as legitimate software which can be used for surveillance and penetration testing purposes, but has been used in numerous hacking campaigns.
Remcos, once installed, opens a backdoor on the computer, granting full access to the remote user.
Remcos is developed by the cybersecurity company BreakingSecurity.

References

2026-03-04 · EG-FinCirt ·
Remcos RAT Operations: How Attackers Gain and Maintain Control
Remcos

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

2026-01-12 · Securonix · Aaron Beardslee, Akshay Gaikwad, Shikha Sangwan
SHADOW#REACTOR – Text-Only Staging, .NET Reactor, and In-Memory Remcos RAT Deployment
Remcos

2025-12-19 · cyble · Cyble
Stealth in Layers: Unmasking the Loader used in Targeted Email Campaigns
DCRat Katz Stealer PhantomVAI PureLogs Stealer Remcos XWorm

2025-11-26 · Intrinsec · CTI Intrinsec, David Sardinha
Trouble in the air: A spree of campaigns targeting the aerospace industry in Russia
DarkWatchman CloudEyE Formbook PhantomCore Remcos

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

2025-10-15 · Kaspersky · Noushin Shabab, Ye Jin
Mysterious Elephant: a growing threat
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

2025-06-02 · Aryaka Networks · bikash dash, varadharajan krishnasamy
Remcos on the Wire: Analyzing Network Artifacts and C2 Command Structures
Remcos

2025-04-03 · Microsoft · Microsoft Threat Intelligence
Threat actors leverage tax season to deploy tax-themed phishing campaigns
Brute Ratel C4 CloudEyE Latrodectus Remcos Storm-0249

2025-03-28 · Intrinsec · David Sardinha
From espionage to PsyOps: Tracking operations and bulletproof providers of UACs in 2025
sLoad NetSupportManager RAT Remcos SmokeLoader

2025-03-28 · Cisco Talos · Guilherme Venere
Gamaredon campaign abuses LNK files to distribute Remcos backdoor
Remcos

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

2025-03-10 · Check Point Research · Check Point Research
Blind Eagle: …And Justice for All
Remcos

2025-02-21 · SonicWall · SonicWall
Remcos RAT Targets Europe: New AMSI and ETW Evasion Tactics Uncovered
Remcos

2025-01-30 · Recorded Future · Insikt Group
TAG-124's Multi-Layered TDS Infrastructure and Extensive User Base
Rhysida KongTuke MintsLoader Broomstick Remcos Rhysida WarmCookie

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

2024-11-08 · Fortinet · Xiaopeng Zhang
New Campaign Uses Remcos RAT to Exploit Victims
Remcos

2024-07-29 · loginsoft · Saharsh Agrawal
Blue Screen Mayhem: When CrowdStrike's Glitch Became Threat Actor's Playground
Daolpu HijackLoader Remcos

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

2024-06-06 · Medium b.magnezi · 0xMrMagnezi
Remcos RAT Analysis
Remcos

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

2024-05-10 · Elastic · Cyril François, Samir Bousseaden
Dissecting REMCOS RAT: An in- depth analysis of a widespread 2024 malware, Part Four
Remcos

2024-05-03 · Elastic · Cyril François, Samir Bousseaden
Dissecting REMCOS RAT: An in- depth analysis of a widespread 2024 malware, Part Three
Remcos

2024-04-30 · Elastic · Cyril François, Samir Bousseaden
Dissecting REMCOS RAT: An in- depth analysis of a widespread 2024 malware, Part Two
Remcos

2024-04-24 · Elastic · Cyril François, Samir Bousseaden
Dissecting REMCOS RAT: An in- depth analysis of a widespread 2024 malware, Part One
Remcos

2024-04-15 · Positive Technologies · Aleksandr Badaev, Kseniya Naumova
SteganoAmor campaign: TA558 mass-attacking companies and public institutions all around the world
LokiBot 404 Keylogger Agent Tesla CloudEyE Formbook Remcos XWorm

2024-03-26 · K7 Security · Vigneshwaran P
Unknown TTPs of Remcos RAT
Remcos

2024-03-01 · Logpoint · Nischal khadgi
A Comprehensive Overview on Stealer Malware Families
Agent Tesla Formbook RedLine Stealer Remcos Vidar

2024-02-28 · Security Intelligence · Golo Mühr, Ole Villadsen
X-Force data reveals top spam trends, campaigns and senior superlatives in 2023
404 Keylogger Agent Tesla Black Basta DarkGate Formbook IcedID Loki Password Stealer (PWS) Pikabot QakBot Remcos

2024-02-21 · Medium b.magnezi · 0xMrMagnezi
Malware Analysis — Remcos RAT
Remcos

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

2024-01-03 · Uptycs · Karthickkumar Kathiresan, Shilpesh Trivedi
Ukraine Targeted by UAC-0050 Using Remcos RAT Pipe Method for Evasion
Remcos

2023-12-07 · · Cert-UA · Cert-UA
UAC-0050 mass cyberattack using RemcosRAT/MeduzaStealer against Ukraine and Poland (CERT-UA#8218)
Meduza Stealer Remcos

2023-11-23 · Infosec Writeups · Osama Ellahi
Malware analysis Remcos RAT- 4.9.2 Pro

Remcos

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

2023-11-14 · SOC Prime · Veronika Telychko

Remcos RAT Detection: UAC-0050 Hackers Launch Phishing Attacks Impersonating the Security Service of Ukraine

Remcos UAC-0050

2023-10-27 · Twitter (@embee_research) · Embee_research

Remcos Downloader Analysis - Manual Deobfuscation of Visual Basic and Powershell

Remcos

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

2023-09-19 · Checkpoint · Alexey Bukhteyev, Arie Olshtein

Unveiling the Shadows: The Dark Alliance between GuLoader and Remcos

CloudEyE Remcos

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

2023-07-08 · Gi7w0rm

CloudEyE — From .lnk to Shellcode

CloudEyE Remcos

2023-05-16 · CyberRaiju · Jai Minton

Remcos RAT - Malware Analysis Lab

Remcos

2023-04-13 · Microsoft · Microsoft Threat Intelligence

Threat actors strive to cause Tax Day headaches

CloudEyE Remcos

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

2023-03-27 · Zscaler · Meghraj Nandanwar, Satyam Singh
DBatLoader: Actively Distributing Malwares Targeting European Businesses
DBatLoader Remcos

2023-03-16 · Trend Micro · Cedric Pernet, Jaromír Hořejší, Loseway Lu
IPFS: A New Data Frontier or a New Cybercriminal Hideout?
Agent Tesla Formbook RedLine Stealer Remcos

2023-02-22 · SOC Prime · Daryna Olyniychuk
New Phishing Attack Detection Attributed to the UAC-0050 and UAC-0096 Groups Spreading Remcos Spyware
Remcos UAC-0050

2023-02-21 · · Cert-UA · Cert-UA
Cyber attack of the group UAC-0050 (UAC-0096) using the Remcos program (CERT-UA#6011)
Remcos UAC-0050

2023-02-06 · · Cert-UA · Cert-UA
UAC-0050 cyber attack against the state bodies of Ukraine using the program for remote control and surveillance Remcos (CERT-UA#5926)
Remcos UAC-0050

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

2023-01-24 · Trellix · Daksh Kapur, John Fokker, Robert Venal, Tomer Shloman
Cyberattacks Targeting Ukraine Increase 20-fold at End of 2022 Fueled by Russia-linked Gamaredon Activity
Andromeda Formbook Houdini Remcos

2022-11-21 · Malwarebytes · Malwarebytes
2022-11-21 Threat Intel Report
404 Keylogger Agent Tesla Formbook Hive Remcos

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

2022-09-22 · Morphisec · Morphisec Labs
Watch Out For The New NFT-001
Eternity Stealer Remcos

2022-08-29 · Soc Investigation · BalaGanesh
Remcos RAT New TTPS - Detection & Response
Remcos

2022-08-21 · Perception Point · Igal Lytzki
Behind the Attack: Remcos RAT
Remcos

2022-08-04 · ConnectWise · Stu Gonzalez
Formbook and Remcos Backdoor RAT by ConnectWise CRU
Formbook Remcos

2022-07-20 · Sophos · Colin Cowie, Gabor Szappanos
OODA: X-Ops Takes On Burgeoning SQL Server Attacks
Maoloa Remcos TargetCompany

2022-05-05 · Github (muha2xmad) · Muhammad Hasan Ali
Analysis of MS Word to drop Remcos RAT | VBA extraction and analysis | IoCs
Remcos

2022-04-12 · HP · Patrick Schläpfer
Malware Campaigns Targeting African Banking Sector
CloudEyE Remcos

2022-04-06 · Fortinet · Xiaopeng Zhang
The Latest Remcos RAT Driven By Phishing Campaign
Remcos

2022-03-30 · Morphisec · Hido Cohen
New Wave Of Remcos RAT Phishing Campaign
Remcos

2022-03-25 · Trustwave · Trustwave SpiderLabs
Cyber Attackers Leverage Russia-Ukraine Conflict in Multiple Spam Campaigns
Remcos

2022-03-07 · ASEC · ASEC
Distribution of Remcos RAT Disguised as Tax Invoice
Remcos

2022-03-04 · Bleeping Computer · Bill Toulas
Russia-Ukraine war exploited as lure for malware distribution
Agent Tesla Remcos

2022-03-04 · Bitdefender · Alina Bizga
Bitdefender Labs Sees Increased Malicious and Scam Activity Exploiting the War in Ukraine
Agent Tesla Remcos

2022-02-28 · · ASEC · ASEC
Remcos RAT malware disseminated by pretending to be tax invoices
Remcos

2022-02-18 · SANS ISC · Xavier Mertens
Remcos RAT Delivered Through Double Compressed Archive
Remcos

2022-02-14 · Morphisec · Arnold Osipov, Hido Cohen
Journey of a Crypto Scammer - NFT-001
AsyncRAT BitRAT Remcos

2022-02-08 · Itay Migdal
Remcos Analysis
Remcos

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

2022-01-28 · eSentire · eSentire Threat Response Unit (TRU)
Remcos RAT
Remcos

2022-01-13 · muha2xmad · Muhammad Hasan Ali
Unpacking Remcos malware
Remcos

2022-01-10 · splunk · Splunk Threat Research Team
Detecting Malware Script Loaders using Remcos: Threat Research Release December 2021
Remcos

2022-01-02 · Medium amgedwageh · Amged Wageh
Automating The Analysis Of An AutoIT Script That Wraps A Remcos RAT
Remcos

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

2021-11-23 · HP · Patrick Schläpfer

RATDispenser: Stealthy JavaScript Loader Dispensing RATs into the Wild

AdWind Ratty STRRAT CloudEyE Formbook Houdini Panda Stealer Remcos

2021-11-23 · Morphisec · Arnold Osipov, Hido Cohen

Babadeda Crypter targeting crypto, NFT, and DeFi communities

Babadeda BitRAT LockBit Remcos

2021-11-11 · splunk · Splunk Threat Research Team

FIN7 Tools Resurface in the Field – Splinter or Copycat?

JSSLoader 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

2021-10-06 · ESET Research · Martina López

To the moon and hack: Fake SafeMoon app drops malware to spy on you

Remcos

2021-10-01 · HP · HP Wolf Security

Threat Insights Report Q3 - 2021

STRRAT CloudEyE NetWire RC Remcos TrickBot Vjw0rm

2021-09-15 · Telsy · Telsy

REMCOS and Agent Tesla loaded into memory with Rezer0 loader

Agent Tesla 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

2021-09-13 · 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

2021-08-04 · · ASEC · ASEC

S/W Download Camouflage, Spreading Various Kinds of Malware

Raccoon RedLine Stealer Remcos Vidar

2021-07-27 · Blackberry · BlackBerry Research & Intelligence Team

Old Dogs New Tricks: Attackers Adopt Exotic Programming Languages

elf.wellmess ElectroRAT BazarNimrod Buer Cobalt Strike Remcos Snake TeleBot WellMess Zebrocy

2021-07-19 · Malwarebytes · Erika Noerenberg
Remcos RAT delivered via Visual Basic
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

2021-07-12 · 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

2021-05-13 · Anomali · Gage Mele, Tara Gould
Threat Actors Use MSBuild to Deliver RATs Filelessly
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

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

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

2021-02-18 · PTSecurity · PTSecurity
https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/
Poet RAT Gravity RAT Ketrican Okrum OopsIE Remcos RogueRobinNET RokRAT SmokeLoader

2021-01-13 · Bitdefender · Janos Gergo Szeles
Remcos RAT Revisited: A Colombian Coronavirus-Themed Campaign
Remcos

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

2020-12-07 · Proofpoint · Proofpoint Threat Research Team
Commodity .NET Packers use Embedded Images to Hide Payloads
Agent Tesla Loki Password Stealer (PWS) Remcos

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

2020-07-30 · 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

2020-07-13 · Github (1d8) · 1d8
Remcos RAT Macro Dropper Doc
Remcos

2020-06-11 · Talos Intelligence · Joe Marshall, Kendall McKay
Tor2Mine is up to their old tricks — and adds a few new ones
Azorult Remcos

2020-05-20 · Zscaler · Amandeep Kumar, Rohit Chaturvedi
Latest Version of Amadey Introduces Screen Capturing and Pushes the Remcos RAT
Amadey Remcos

2020-05-14 · 360 Total Security · kate
Vendetta - new threat actor from Europe
Nanocore RAT Remcos

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

2020-04-02 · Cisco Talos · Vanja Svajcer
AZORult brings friends to the party
Azorult Remcos

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

2020-03-18 · Proofpoint · Axel F, Sam Scholten
Coronavirus Threat Landscape Update
Agent Tesla Get2 ISFB Remcos

2019-10-21 · Fortinet · Chris Navarrete, Xiaopeng Zhang
New Variant of Remcos RAT Observed In the Wild
Remcos

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

2019-09-07 · Dissecting Malware · Marius Genheimer
Malicious RATatouille
Remcos

2019-08-22 · Youtube (OALabs) · Sergei Frankoff
Remcos RAT Unpacked From VB6 With x64dbg Debugger
Remcos

2019-08-15 · Trend Micro · Aliakbar Zahravi
Analysis: New Remcos RAT Arrives Via Phishing Email
Remcos

2019-07-01 · Talos Intelligence · Holger Unterbrink
RATs and stealers rush through “Heaven’s Gate” with new loader
Agent Tesla HawkEye Keylogger Remcos

2019-06-19 · Check Point · Kobi Eisenkraft, Moshe Hayun
Check Point’s Threat Emulation Stops Large-Scale Phishing Campaign in Germany
Remcos

2019-05-08 · VMRay · Francis Montesino
Get Smart with Enhanced Memory Dumping in VMRay Analyzer 3.0
Remcos

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

2018-08-22 · Cisco Talos · Edmund Brumaghin, Eric Kuhla, Holger Unterbrink, Lilia Gonzalez Medina
Picking Apart Remcos Botnet-In-A-Box
Remcos

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

2018-03-02 · KrabsOnSecurity · Mr. Krabs
Analysing Remcos RAT’s executable

Remcos

2018-03-01 · My Online Security · My Online Security

Fake order spoofed from Finchers ltd Sankyo-Rubber delivers Remcos RAT via ACE attachments

Remcos

2018-01-23 · RiskIQ · Yonathan Klijnsma

Espionage Campaign Leverages Spear Phishing, RATs Against Turkish Defense Contractors

Remcos

2017-12-22 · Malware Traffic Analysis · Brad Duncan

MALSPAM USES CVE-2017-0199 TO DISTRIBUTE REMCOS RAT

Remcos

2017-07-01 · Secrary Blog · lasha

Remcos RAT

Remcos

2017-02-14 · Fortinet · Floser Bacurio, Joie Salvio

REMCOS: A New RAT In The Wild

Remcos

Yara Rules

▶ [TLP:WHITE] win_remcos_auto (20251219 | Detects win.remcos.)

▶ [TLP:WHITE] win_remcos_w0 (20230906 | Detects strings present in remcos rat Samples.)

Download all Yara Rules

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