DCRat (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:22:20 UTC

DCRat

aka: DarkCrystal RAT

DCRat is a typical RAT that has been around since at least June 2019.

References

2026-01-14 · Trellix ·
Hiding in Plain Sight: Deconstructing the Multi-Actor DLL Sideloading Campaign abusing ahost.exe
DCRat

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

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

2025-12-16 · Zscaler · Gaetano Pellegrino
BlindEagle Targets Colombian Government Agency with Caminho and DCRAT
DCRat PhantomVAI

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

2025-06-03 · IBM X-Force · Melissa Frydrych
IBM X-Force Threat Analysis: DCRat presence growing in Latin America
DCRat PhantomVAI

2025-03-11 · Kaspersky Labs · AMR
DCRat backdoor returns
DCRat

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

2025-02-11 · EclecticIQ · Arda Büyükkaya
Sandworm APT Targets Ukrainian Users with Trojanized Microsoft KMS Activation Tools in Cyber Espionage Campaigns
Kalambur BACKORDER DCRat

2025-02-11 · CyberSecurityNews · Do Son
Sandworm APT Exploits Trojanized KMS Tools to Target Ukrainian Users in Cyber Espionage Campaign
DCRat

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

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

2024-06-04 · · Cert-UA · Cert-UA
UAC-0200: Targeted cyberattacks using DarkCrystal RAT and Signal as a trusted distribution vehicle (CERT-UA#9918)
DCRat

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

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

2024-03-11 · SOCRadar · SOCRadar
Acuity Federal Contractor Breach, Okta Customers Leak, DCRat Exploit and Access Sales
DCRat CyberNiggers

2024-02-01 · · Infinitum IT · Kerime Gencay
DcRat Technical Analysis Report (Paywall)
DCRat

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

2024-01-12 · 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

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

2023-09-04 · Github (muha2xmad) · Muhammad Hasan Ali
A deep dive into DCRAT/DarkCrystalRAT malware
DCRat

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

2023-04-12 · 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

2023-04-08 · Twitter (@embee_research) · Embee_research
Dcrat - Manual De-obfuscation of .NET Malware
DCRat

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

2022-09-19 · Recorded Future · Insikt Group®
Russia-Nexus UAC-0113 Emulating Telecommunication Providers in Ukraine
Ave Maria Colibri Loader DCRat

2022-09-15 · Sekoia · Threat & Detection Research Team
PrivateLoader: the loader of the prevalent ruzki PPI service
Agent Tesla Coinminer DanaBot DCRat Eternity Stealer Glupteba Mars Stealer NetSupportManager RAT Nymaim Nymaim2 Phoenix Keylogger PrivateLoader Raccoon RedLine Stealer SmokeLoader Socelars STOP Vidar YTStealer

2022-08-30 · Cisco · Vanja Svajcer
ModernLoader delivers multiple stealers, cryptominers and RATs
Coinminer DCRat ModernLoader RedLine Stealer SapphireMiner SystemBC

2022-08-18 · Trustwave · Pawel Knapczyk
Overview of the Cyber Weapons Used in the Ukraine - Russia War
AcidRain CaddyWiper Cobalt Strike CredoMap DCRat DoubleZero GraphSteel GrimPlant HermeticWiper INDUSTROYER2 InvisiMole IsaacWiper PartyTicket

2022-08-18 · Trustwave · Pawel Knapczyk
Overview of the Cyber Weapons Used in the Ukraine - Russia War
AcidRain CaddyWiper Cobalt Strike CredoMap DCRat DoubleZero GraphSteel GrimPlant HermeticWiper INDUSTROYER2 InvisiMole IsaacWiper PartyTicket

2022-06-24 · · Cert-UA · Cert-UA

Cyberattack against Ukrainian telecommunications operators using DarkCrystal RAT malware (CERT-UA # 4874)

DCRat Sandworm

2022-06-10 · · Cert-UA · Cert-UA

Massive cyberattack on Media Organizations of Ukraine using crescentImp malware (CERT-UA#4797)

DCRat

2022-05-09 · Blackberry · The BlackBerry Research & Intelligence Team

Dirty Deeds Done Dirt Cheap: Russian RAT Offers Backdoor Bargains

DCRat NjRAT

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

2022-04-16 · forensicitguy · Tony Lambert

Snip3 Crypter used with DCRat via VBScript

DCRat

2022-03-02 · RiskIQ · Jennifer Grob

RiskIQ: Malware Linked to Upwork Post Seeking Content Writer for a "Newly Developed Application" Deploys DCRat

DCRat

2022-02-17 · Zscaler · Aditya Sharma, Stuti Chaturvedi

FreeCryptoScam - A New Cryptocurrency Scam That Leads to Installation of Backdoors and Stealers

DCRat

2022-01-19 · Blackberry · The BlackBerry Research & Intelligence Team

Kraken the Code on Prometheus

Prometheus Backdoor BlackMatter Cerber Cobalt Strike DCRat Ficker Stealer QakBot REvil Ryuk

2021-10-19 · Cisco Talos · Asheer Malhotra

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

DCRat Quasar RAT

2021-10-12 · Infoblox · Avinash Shende

Malspam Campaign Delivers Dark Crystal RAT (dcRAT)

DCRat

2021-09-22 · YouTube (John Hammond) · John Hammond

Snip3 Crypter/RAT Loader - DcRat MALWARE ANALYSIS

DCRat

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

2020-05-12 · FireEye · Jacob Thompson

Analyzing Dark Crystal RAT, a C# backdoor

DCRat

2019-10-02 · tcontre

DCRAT malware Evades SandBox that use Fake Internet by using the Google public DNS IP address

DCRat

Yara Rules

▶ [TLP:WHITE] win_dcrat_w0 (20200227 | DCRat payload)

Download all Yara Rules

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