Rhadamanthys (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-02 11:08:15 UTC

According to PCrisk, Rhadamanthys is a stealer-type malware, and as its name implies - it is designed to extract data from infected machines.

At the time of writing, this malware is spread through malicious websites mirroring those of genuine software such as AnyDesk, Zoom, Notepad++, and others. Rhadamanthys is downloaded alongside the real program, thus diminishing immediate user suspicion. These sites were promoted through Google ads, which superseded the legitimate search results on the Google search engine.

2026-03-10 · Check Point Research ·
Iranian MOIS Actors & the Cyber Crime Connection
Qilin Tsundere CASTLELOADER Rhadamanthys 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 2025-12-10 · SpyCloud · SpyCloud Labs Research Team
Analyzing the Impact of the Operation Endgame Takedown on Rhadamanthys & the MaaS Ecosystem
Rhadamanthys 2025-11-13 · Politie NL · Politie NL
Again criminal infrastructure dismantled in international ransomware operation
Rhadamanthys Venom RAT 2025-10-01 · Checkpoint · hasherezade
Rhadamanthys 0.9.x – walk through the updates
Rhadamanthys 2025-08-08 · AhnLab · AhnLab ASEC Analysis Team
Distribution of SmartLoader Malware via Github Repository Disguised as a Legitimate Project
Rhadamanthys SmartLoader 2025-07-31 · Twitter (@Threatlabz) · Zscaler
Tweet about new variant with BEEF instead of !RHA as config magic bytes
Rhadamanthys 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 · VMRay · Albert Zsigovits, VMRay
Rhadamanthys slips through in large installer files
Rhadamanthys 2025-05-22 · Elastic · Daniel Stepanic
De-obfuscating ALCATRAZ
DOUBLELOADER Rhadamanthys 2025-03-28 · Trend Micro · Ahmed Mohamed Ibrahim, Aliakbar Zahravi
A Deep Dive into Water Gamayun’s Arsenal and Infrastructure
DarkWisp SilentPrism Kematian Stealer Rhadamanthys Stealc Water Gamayun 2025-03-14 · Twitter (@CERTCyberdef) · Alexandre Matousek, Marine PICHON

Tweet on Emmenhtal v3

Emmenhtal Lumma Stealer Rhadamanthys 2025-03-06 · Outpost24 · KrakenLabs

Unveiling EncryptHub: Analysis of a multi-stage malware campaign

Rhadamanthys 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 2025-01-04 · revdiaries.com · heapoverflow

"Solara" Roblox Executor Malware

Rhadamanthys 2024-11-06 · Check Point Research · Check Point Research

CopyRh(ight)adamantys Campaign: Rhadamantys Exploits Intellectual Property Infringement Baits

Rhadamanthys 2024-10-23 · Cisco Talos · Edmund Brumaghin, Holger Unterbrink, Jordyn Dunk, Nicole Hoffman

Highlighting TA866/Asylum Ambuscade Activity Since 2021

WasabiSeed Cobalt Strike csharp-streamer RAT Resident Rhadamanthys WarmCookie 2024-10-17 · Sekoia · Quentin Bourgue, Sekoia TDR

ClickFix tactic: The Phantom Meet

Rhadamanthys Stealc 2024-09-26 · Recorded Future · Insikt Group

Rhadamanthys Stealer Adds Innovative AI Feature in Version 0.7.0

Rhadamanthys 2024-07-25 · Symantec · Symantec

Growing Number of Threats Leveraging AI

Broomstick DBatLoader NetSupportManager RAT Rhadamanthys 2024-07-24 · Check Point Research · Antonis Terefos

Stargazers Ghost Network

Atlantida Lumma Stealer RedLine Stealer Rhadamanthys RisePro Stargazer Goblin 2024-07-14 · Medium b.magnezi · 0xMrMagnezi

Malware Analysis - Rhadamanthys

Rhadamanthys 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 2024-06-17 · Recorded Future · Insikt Group

The Travels of “markopolo”: Self-Proclaimed Meeting Software Vortax Spreads Infostealers, Unveils Expansive Network of Malicious macOS Applications

AMOS Rhadamanthys Stealc Markopolo 2024-04-10 · Proofpoint · Selena Larson, Tommy Madjar

Security Brief: TA547 Targets German Organizations with Rhadamanthys Stealer

Rhadamanthys 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 2023-12-14 · Checkpoint · hasherezade

Rhadamanthys v0.5.0 – A Deep Dive into the Stealer’s Components

Rhadamanthys 2023-10-27 · Elastic · Joe Desimone, Salim Bitam

GHOSTPULSE haunts victims using defense evasion bag o' tricks

HijackLoader Lumma Stealer NetSupportManager RAT Rhadamanthys SectopRAT Vidar 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 2023-10-03 · Outpost24 · David Catalan

Rhadamanthys malware analysis: How infostealers use VMs to avoid analysis

Rhadamanthys 2023-09-25 · EchoCTI · Bilal BAKARTEPE, bixploit

Rhdamanthys Technical Analysis Report

Rhadamanthys 2023-08-31 · Checkpoint · hasherezade

From Hidden Bee to Rhadamanthys - The Evolution of Custom Executable Formats

Hidden Bee Rhadamanthys 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 2023-06-15 · eSentire · RussianPanda

eSentire Threat Intelligence Malware Analysis: Resident Campaign

Cobalt Strike Resident Rhadamanthys WarmCookie 2023-05-16 · Secureworks · Counter Threat Unit ResearchTeam

The Growing Threat from Infostealers

Graphiron GraphSteel Raccoon RedLine Stealer Rhadamanthys Taurus Stealer Vidar 2023-04-19 · Google · Billy Leonard, Google Threat Analysis Group

Ukraine remains Russia’s biggest cyber focus in 2023

Rhadamanthys 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 2023-03-27 · Check Point Research · Checkpoint Research

Rhadamanthys: The “Everything Bagel” Infostealer

Rhadamanthys 2023-02-21 · Zscaler · Nikolaos Pantazopoulos, Sarthak Misraa

Technical Analysis of Rhadamanthys Obfuscation Techniques

Rhadamanthys 2023-01-16 · Medium elis531989 · Eli Salem

Dancing With Shellcodes: Analyzing Rhadamanthys Stealer

Rhadamanthys 2023-01-12 · Cybleinc · Cyble

Rhadamanthys: New Stealer Spreading Through Google Ads

Rhadamanthys 2023-01-03 · Malware Traffic Analysis · Brad Duncan

2023-01-03 (TUESDAY) - GOOGLE AD --> FAKE NOTPAD++ PAGE --> RHADAMANTHYS STEALER

Rhadamanthys 2022-12-05 · Accenture · Paul Mansfield, Thomas Willkan

Popularity spikes for information stealer malware on the dark web

MetaStealer Rhadamanthys 2022-10-06 · ThreatMon · ThreatMon Malware Research Team

Rhadamanthys Stealer Analysis

Rhadamanthys

▶ [TLP:WHITE] win_rhadamanthys_auto (20251219 | Detects win.rhadamanthys.)
