Amadey (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:10:25 UTC

Amadey is a botnet that appeared around October 2018 and is being sold for about $500 on Russian-speaking hacking forums. It periodically sends information about the system and installed AV software to its C2 server and polls to receive orders from it. Its main functionality is that it can load other payloads (called "tasks") for all or specifically targeted computers compromised by the malware.

2025-12-08 · Swisscom B2B CSIRT ·
Swisscom B2B CSIRT - TDR Intel Brief: Unmasking Amadey 5
Amadey 2025-08-28 · Intrinsec · David Sardinha
VAIZ, FDN3, TK-NET: A nebula of Ukrainian networks engaged in brute force and password spraying attacks
Amadey 2024-12-11 · Microsoft · Microsoft Threat Intelligence
Frequent freeloader part II: Russian actor Secret Blizzard using tools of other groups to attack Ukraine
Amadey Kazuar Wipbot FlyingYeti 2024-09-09 · LinkedIn (Idan Tarab) · Idan Tarab
APT CoralRaider Expands Arsenal: AmadeyBot, FTP Innovations, and Complex Domain Strategy
Amadey 2024-06-13 · Github (LambdaMamba) · Lena Yu
Implementation of a Config Decryptor for Amadey
Amadey 2024-01-30 · ANY.RUN · Lena (LambdaMamba)
CrackedCantil: A Malware Symphony Breakdown - PrivateLoader, Smoke, Lumma, RedLine, RisePro, Amadey, Stealc, Socks5Systemz, STOP
Amadey CrackedCantil Lumma Stealer PrivateLoader RedLine Stealer RisePro SmokeLoader Socks5 Systemz Stealc STOP 2024-01-25 · JSAC 2024 · Masaki Kasuya
A Study on Long-Term Trends about Amadey C2 Infrastructure
Amadey 2023-12-02 · Medium g0njxa · amadey
Approaching stealers devs : a brief interview with Amadey
Amadey 2023-12-01 · ASEC · ASEC
Kimsuky Group Uses AutoIt to Create Malware (RftRAT, Amadey)
XRat Amadey Appleseed PEBBLEDASH 2023-11-19 · Twitter (@embee_research) · Embee_research
Combining Pivot Points to Identify Malware Infrastructure - Redline, Smokeloader and Cobalt Strike
Amadey Cobalt Strike RedLine Stealer SmokeLoader 2023-11-02 · BitSight · BitSight
Unveiling Socks5Systemz: The Rise of a New Proxy Service via PrivateLoader and Amadey
Amadey PrivateLoader Socks5 Systemz 2023-11-02 · BitSight · BitSight
Unveiling Socks5Systemz: The Rise of a New Proxy Service via PrivateLoader and Amadey
Amadey PrivateLoader Socks5 Systemz 2023-09-04 · VMRay · VMRay Labs Team
Amadey: New encoding with old tricks
Amadey 2023-08-31 · Rapid7 Labs · Evan McCann, Natalie Zargarov, Thomas Elkins, Tyler McGraw
Fake Update Utilizes New IDAT Loader To Execute StealC and Lumma Infostealers
FAKEUPDATES Amadey HijackLoader Lumma Stealer SectopRAT 2023-08-10 · Github (muha2xmad) · Muhammad

Hasan Ali

Amadey configuration extractor

Amadey 2023-08-10 · Github (muha2xmad) · Muhammad Hasan Ali

Amadey string decryptor

Amadey 2023-07-25 · splunk · Splunk Threat Research Team

Amadey Threat Analysis and Detections

Amadey 2023-06-08 · Twitter (@embee_research) · Embee_research

Practical Queries for Identifying Malware Infrastructure: An informal page for storing Censys/Shodan queries

Amadey AsyncRAT Cobalt Strike QakBot Quasar RAT Sliver solarmarker 2023-05-19 · Twitter (@embee_research) · Embee_research

Analysis of Amadey Bot Infrastructure Using Shodan

Amadey 2023-05-01 · Check Point Research · Check Point Research

Chain Reaction: RokRAT's Missing Link

Amadey RokRAT 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 · Twitter (@embee_research) · Matthew

Redline Stealer - Static Analysis and C2 Extraction

Amadey RedLine Stealer 2023-01-27 · cyble · The Cyber Express

Old Bot in New Bottle: Amadey Botnet Back in Action Via Phishing Sites

Amadey 2023-01-25 · cyble · Cyble

The Rise of Amadey Bot: A Growing Concern for Internet Security

Amadey 2022-12-22 · AhnLab · Sanseo

Nitol DDoS Malware Installing Amadey Bot

Amadey Nitol 2022-11-08 · AhnLab · ASEC

LockBit 3.0 Being Distributed via Amadey Bot

Amadey Gandcrab LockBit 2022-10-17 · ASEC · ASEC

Amadey Bot Disguised as a Famous Korean Messenger Program Being Distributed

Amadey 2022-09-29 · Team Cymru · S2 Research Team

Seychelles, Seychelles, on the C(2) Shore: An overview of a bulletproof hosting provider named ELITETEAM.

Amadey Raccoon RedLine Stealer SmokeLoader STOP 2022-07-29 · Blackberry · BlackBerry Research & Intelligence Team

SmokeLoader Malware Used to Augment Amadey Infostealer

Amadey SmokeLoader 2022-07-21 · AhnLab · ASEC

Amadey Bot Being Distributed Through SmokeLoader

Amadey SmokeLoader 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 2022-04-20 · cocomelonc · cocomelonc

Malware development: persistence - part 1. Registry run keys. C++ example.

Agent Tesla Amadey BlackEnergy Cobian RAT COZYDUKE Emotet Empire Downloader Kimsuky 2022-03-31 ·

Trellix · Jambul Tologonov, John Fokker

Conti Leaks: Examining the Panama Papers of Ransomware

LockBit Amadey Buer Conti IcedID LockBit Mailto Maze PhotoLoader Ryuk TrickBot 2021-11-02 · Minerva · Natalie Zargarov

Underminer Exploit Kit: The More You Check The More Evasive You Become

Amadey Oski Stealer RedLine Stealer UnderminerEK 2021-08-12 · Cisco Talos · Vanja Svajcer

Signed MSI files, Raccoon and Amadey are used for installing ServHelper RAT

Amadey Raccoon ServHelper 2021-07-08 · Medium walmartglobaltech · Harold Ogden, Jason Reaves

Amadey stealer plugin adds Mikrotik and Outlook harvesting

Amadey 2021-04-12 · PTSecurity · PTSecurity

PaaS, or how hackers evade antivirus software

Amadey Bunitu Cerber Dridex ISFB KPOT Stealer Mailto Nemty Phobos Pony Predator The Thief QakBot Raccoon RTM SmokeLoader Zloader 2021-03-31 · InfoSec Handlers Diary Blog · Xavier Mertens

Quick Analysis of a Modular InfoStealer

Amadey 2021-02-23 · CrowdStrike · CrowdStrike

2021 Global Threat Report

RansomEXX Amadey Anchor Avaddon BazarBackdoor Clop Cobalt Strike Conti Cutwail DanaBot DarkSide DoppelPaymer Dridex Egregor Emotet Hakbit IcedID JSOutProx KerrDown LockBit Mailto Maze MedusaLocker Mespinoza Mount Locker NedDnLoader Nemty Pay2Key PlugX Pushdo PwndLocker PyXie QakBot Quasar RAT RagnarLocker Ragnarok RansomEXX REvil Ryuk Sekhmet ShadowPad SmokeLoader Snake SUNBURST SunCrypt TEARDROP TrickBot WastedLocker Winnti Zloader Evilnum OUTLAW SPIDER RIDDLE SPIDER SOLAR SPIDER VIKING SPIDER 2021-02-09 · Max Kersten's Blog · Max Kersten

Ghidra script to decrypt strings in Amadey 1.09

Amadey 2021-02-01 · · Microstep Intelligence Bureau · Microstep online research response team

Analysis of the attack activity organized by Konni APT using the topic of North Korean epidemic materials as bait

Amadey 2021-01-18 · Medium csis-techblog · Benoît Ancel

GCleaner — Garbage Provider Since 2019

Amadey Ficker Stealer Raccoon RedLine Stealer SmokeLoader STOP 2020-06-22 · · CERT-FR · CERT-FR

Évolution De Lactivité du Groupe Cybercriminel TA505

Amadey AndroMut Bart Clop Dridex FlawedGrace Gandcrab Get2 GlobeImposter Jaff Locky Marap Philadephia Ransom QuantLoader Scarab Ransomware SDBbot ServHelper Silence tRat TrickBot 2020-05-20 · Zscaler · Amandeep Kumar, Rohit Chaturvedi

Latest Version of Amadey Introduces Screen Capturing and Pushes the Remcos RAT

Amadey Remcos 2020-03-26 · Telekom · Thomas Barabosch

TA505's Box of Chocolate - On Hidden Gems packed with the TA505 Packer

Amadey Azorult Clop FlawedGrace Get2 SDBbot Silence TinyMet TA505 2020-02-28 · Financial Security Institute · Financial Security Institute

Profiling of TA505 Threat Group That Continues to Attack the Financial Sector

Amadey Clop FlawedAmmyy Rapid Ransom SDBbot TinyMet 2020-02-05 · Cybereason · Assaf Dahan, Lior Rochberger

The Hole in the Bucket: Attackers Abuse Bitbucket to Deliver an Arsenal of Malware

Amadey Azorult Predator The Thief STOP Vidar 2020-01-08 · Blackberry · Masaki Kasuya

Threat Spotlight: Amadey Bot Targets Non-Russian Users

Amadey 2019-04-27 · nao_sec · nao_sec

Analyzing Amadey

Amadey 2019-02-13 · KrabsOnSecurity · Mr. Krabs

Analyzing Amadey – a simple native malware

Amadey 2018-11-14 · Twitter (@0xffff0800) · 0xffff0800

Tweet on Amadey C2

Amadey 2018-11-13 · Twitter (@ViriBack) · Dee

Tweet on Amadey Malware

Amadey

▶ [TLP:WHITE] win_amadey_auto (20251219 | Detects win.amadey.)
