SmokeLoader (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:34:41 UTC

The SmokeLoader family is a generic backdoor with a range of capabilities which depend on the modules included in any given build of the malware. The malware is delivered in a variety of ways and is broadly associated with criminal activity. The malware frequently tries to hide its C2 activity by generating requests to legitimate sites such as microsoft.com, bing.com, adobe.com, and others. Typically the actual Download returns an HTTP 404 but still contains data in the Response Body.

2025-09-15 · Zscalar · ThreatLabZ research team
SmokeLoader Rises From the Ashes
SmokeLoader 2025-06-17 · DARKReading · James Shank
Operation Endgame: Do Takedowns and Arrests Matter?
BumbleBee Emotet Pikabot SmokeLoader TrickBot 2025-04-09 · Europol · Europol
Operation Endgame follow-up leads to five detentions and interrogations as well as server takedowns
SmokeLoader 2025-03-28 · Intrinsec · David Sardinha
From espionage to PsyOps: Tracking operations and bulletproof providers of UACs in 2025
sLoad NetSupportManager RAT Remcos SmokeLoader 2025-02-06 · Hunt.io · Hunt.io
SmokeLoader Malware Found in Open Directories Targeting Ukraine’s Auto & Banking Industries
SmokeLoader 2025-02-04 · Trend Micro · Peter Girnus
CVE-2025-0411: Ukrainian Organizations Targeted in Zero-Day Campaign and Homoglyph Attacks
SmokeLoader 2024-12-02 · FortiGuard Labs · Pei Han Liao
SmokeLoader Attack Targets Companies in Taiwan
SmokeLoader 2024-11-07 · Perception Point · Arthur Vaiselbuh
Evasive ZIP Concatenation: Trojan Targets Windows Users
SmokeLoader 2024-10-17 · Loader Insight Agency · LIA
Correlating Vidar Stealer Build IDs Based on Loader Tasks
Lumma Stealer SmokeLoader Vidar 2024-07-02 · Sekoia · Quentin Bourgue
Exposing FakeBat loader: distribution methods and adversary infrastructure
BlackCat Royal Ransom EugenLoader Carbanak Cobalt Strike DICELOADER Gozi IcedID Lumma Stealer NetSupportManager RAT Pikabot RedLine Stealer SectopRAT Sliver SmokeLoader Vidar 2024-06-11 · Zscaler · ThreatLabZ research team
A Brief History of SmokeLoader, Part 1
SmokeLoader 2024-05-30 · Europol · Europol
Largest ever operation against botnets hits dropper malware ecosystem
BumbleBee IcedID SmokeLoader SystemBC TrickBot 2024-03-05 · CIP · paloalto Networks: Unit42, State Service of Special Communication and Information Protection of Ukraine (CIP)
Semi-Annual Chronicles of UAC-0006 Operations
SmokeLoader 2024-03-01 · farghlymal github.io · Aziz Farghly

Taking a deep dive into SmokeLoader

SmokeLoader 2024-02-28 · Spamhaus · Spamhaus Malware Labs

Toot about SmokeLoader dropping Xehook Stealer

SmokeLoader 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 2024-01-06 · irfan_eternal · Muhammed Irfan V A

Understanding Internals of SmokeLoader

SmokeLoader 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 2023-10-24 · National Security and Defense Council of Ukraine · Organization of the National Security and Defense Council of Ukraine

The Surge in SmokeLoader Attacks on Ukrainian Institutions

SmokeLoader 2023-10-12 · Cluster25 · Cluster25 Threat Intel Team

CVE-2023-38831 Exploited by Pro-Russia Hacking Groups in RU-UA Conflict Zone for Credential Harvesting Operations

Agent Tesla Crimson RAT Nanocore RAT SmokeLoader 2023-09-28 · HarfangLab · Claudio Teixeira

Loader Galore - TaskLoader at the start of a Pay-per-Install Infection Chain

CustomerLoader Fabookie LgoogLoader SmokeLoader 2023-08-23 · Logpoint · Anish Bogati, Nischal khadgi

Defending Against 8base: Uncovering Their Arsenal and Crafting Responses

8Base Phobos SmokeLoader SystemBC 2023-07-17 · Acronis · Acronis Security

8Base ransomware stays unseen for a year

8Base Phobos SmokeLoader 2023-06-28 · vmware · Bria Beathley, Dana Behling, Deborah Snyder, Fae Carlisle

8Base Ransomware: A Heavy Hitting Player

8Base Phobos SmokeLoader SystemBC 2023-06-24 · Twitter (@embee_research) · Embee_research

SmokeLoader - Malware Analysis and Decoding With Procmon

SmokeLoader 2023-02-27 · PRODAFT Threat Intelligence · PRODAFT

RIG Exploit Kit: In-Depth Analysis

Dridex IcedID ISFB PureCrypter Raccoon RecordBreaker RedLine Stealer Royal Ransom Silence SmokeLoader Zloader 2022-11-19 · Malwarology · Robert Simmons

Malicious Packer pkr_ce1a

SmokeLoader Vidar 2022-11-17 · Trellix · Trelix

Trellix Insights: SmokeLoader Exploits Old Vulnerabilities to Drop zgRAT

SmokeLoader zgRAT 2022-10-07 · YouTube (BSides Portland) · Pim Trouerbach

SmokeLoader - The Pandora's box of Tricks

SmokeLoader 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 2022-09-26 · Kaspersky · Artem Ushkov, Haim Zigel, Oleg Kupreev

NullMixer: oodles of Trojans in a single dropper

ColdStealer DanaBot GCleaner Nullmixer PrivateLoader PseudoManuscrypt RedLine Stealer SmokeLoader Vidar 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 2022-08-31 · BitSight · André Tavares

Tracking PrivateLoader: Malware Distribution Service

PrivateLoader RedLine Stealer SmokeLoader 2022-08-30 · Github (vc0RExor) · vc0RExor

SmokeLoader - Quick-Analysis

SmokeLoader 2022-08-25 · OALabs · Sergei Frankoff

SmokeLoader Triage Taking a look how Smoke Loader works

SmokeLoader 2022-08-08 · Fortinet · James Slaughter

Life After Death - SmokeLoader Continues to Haunt Using Old Vulnerabilities

SmokeLoader zgRAT 2022-08-08 · Medium CSIS Techblog · Benoît Ancel

An inside view of domain anonymization as-a-service — the BraZZZerSFF infrastructure

Riltok magecart Anubis Azorult BetaBot Buer CoalaBot CryptBot DiamondFox DreamBot GCleaner ISFB Loki Password Stealer (PWS) MedusaLocker MeguminTrojan Nemty PsiX RedLine Stealer SmokeLoader STOP TinyNuke Vidar Zloader 2022-07-29 · Blackberry · BlackBerry Research & Intelligence Team

SmokeLoader Malware Used to Augment Amadey Infostealer

Amadey SmokeLoader 2022-07-27 · Darktrace · Sam Lister, Shuh Chin Goh

PrivateLoader: Network-Based Indicators of Compromise

PrivateLoader SmokeLoader 2022-07-21 · AhnLab · ASEC

Amadey Bot Being Distributed Through SmokeLoader

Amadey SmokeLoader 2022-06-21 · SonicWall · SonicWall

HTML Application Files are being used to distribute Smoke Loader Malware

SmokeLoader 2022-04-20 · CISA · CISA

Alert (AA22-110A): Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

VPNFilter BlackEnergy DanaBot DoppelDridex Emotet EternalPetya GoldMax Industroyer Sality SmokeLoader TrickBot Triton Zloader Killnet 2022-04-20 · CISA · Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), CISA, FBI, Government Communications Security Bureau, National Crime Agency (NCA), NCSC UK, NSA

AA22-110A Joint CSA: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

VPNFilter BlackEnergy DanaBot DoppelDridex Emotet EternalPetya GoldMax Industroyer Sality SmokeLoader TrickBot Triton Zloader 2022-04-12 · AhnLab · ASEC Analysis Team

SystemBC Being Used by Various Attackers

Emotet SmokeLoader SystemBC 2022-02-18 · Bleeping Computer · Sergiu Gatlan

New Golang botnet empties Windows users' cryptocurrency wallets

Anubis Loader SmokeLoader 2022-02-17 · Blackberry · BlackBerry Research & Intelligence Team

Threat Thursday: Arkei Infostealer Expands Reach Using SmokeLoader to Target Crypto Wallets and MFA

Arkei Stealer SmokeLoader 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 2022-01-01 · Silent Push · Silent Push

Privacy tools (not) for you

SmokeLoader 2021-06-17 · Suvaditya Sur

Analysis of SmokeLoader

SmokeLoader 2021-06-10 · ZAYOTEM · Buğra KÖSE, Çağlar YÜN, Esmanur ALİCAN, Fatih YILMAZ, İrem ALKAŞİ

SmokeLoader Technical Analysis Report

SmokeLoader 2021-05-26 · DeepInstinct · Ron Ben Yizhak

A Deep Dive into Packing Software CryptOne

Cobalt Strike Dridex Emotet Gozi ISFB Mailto QakBot SmokeLoader WastedLocker Zloader 2021-05-19 · Intel 471 · Intel 471

Look how many cybercriminals love Cobalt Strike

BazarBackdoor Cobalt Strike Hancitor QakBot SmokeLoader SystemBC TrickBot 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 2021-03-21 · Blackberry · Blackberry Research

2021 Threat Report

Bashlite FritzFrog IPStorm Mirai Tsunami elf.wellmess AppleJeus Dacls EvilQuest Manuscrypt Astaroth BazarBackdoor Cerber Cobalt Strike Emotet FinFisher RAT Kwampirs MimiKatz NjRAT Ryuk SmokeLoader TrickBot 2021-03-18 · Proofpoint · Brandon Murphy, Dennis Schwarz, Jack Mott, Proofpoint Threat Research Team

Now You See It, Now You Don’t: CopperStealer Performs Widespread Theft

CopperStealer SmokeLoader 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 2021-02-18 · PTSecurity · PTSecurity

https://www.ptsecurity.com/ww-en/analytics/antisandbox-techniques/

Poet RAT Gravity RAT Ketrican Okrum OopsIE Remcos RogueRobinNET RokRAT SmokeLoader 2021-02-02 · · CRONUP · Germán Fernández

De ataque con Malware a incidente de Ransomware

Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DanaBot Dharma Dridex Egregor Emotet Empire Downloader FriedEx GootKit IcedID MegaCortex Nemty Phorpiex PwndLocker PyXie QakBot RansomEXX REvil Ryuk SDBbot SmokeLoader TrickBot Zloader 2021-02-01 · Microsoft · Microsoft 365 Defender Threat Intelligence Team

What tracking an attacker email infrastructure tells us about persistent cybercriminal operations

Dridex Emotet Makop Ransomware SmokeLoader TrickBot 2021-01-18 · Medium csis-techblog · Benoît Ancel

GCleaner — Garbage Provider Since 2019

Amadey Ficker Stealer Raccoon RedLine Stealer SmokeLoader STOP 2021-01-11 · AhnLab · ASEC Analysis Team

Smoke Loader Learns New Tricks

SmokeLoader 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 2020-12-23 · 0xC0DECAFE · Thomas Barabosch

Detect RC4 in (malicious) binaries

SmokeLoader Zloader 2020-12-21 · Cisco Talos · JON MUNSHAW

2020: The year in malware

WolfRAT Prometei Poet RAT Agent Tesla Astaroth Ave Maria CRAT Emotet Gozi IndigoDrop JhoneRAT Nanocore RAT NjRAT Oblique RAT SmokeLoader StrongPity WastedLocker Zloader 2020-12-17 · Telekom · Thomas Barabosch

Smokeloader is still alive and kickin' – A new way to encrypt CC server URLs

SmokeLoader 2020-09-09 · Malwarebytes · Threat Intelligence Team

Malvertising campaigns come back in full swing

Raccoon SmokeLoader Malsmoke 2020-09-09 · Malwarebytes · Threat Intelligence Team

Malvertising campaigns come back in full swing

Raccoon SmokeLoader 2020-09-02 · Cisco Talos · Edmund Brumaghin, Holger Unterbrink

Salfram: Robbing the place without removing your name tag

Ave Maria ISFB SmokeLoader Zloader 2020-08-27 · Hatching.io · Pete Cowman

Smokeloader Analysis and More Family Detections

SmokeLoader 2020-06-22 · m.alvar.es · Marcos Alvares

Comparative analysis between Bindiff and Diaphora - Patched Smokeloader Study Case

SmokeLoader 2020-06-21 · N1ght-W0lf Blog · Abdallah Elshinbary

Deep Analysis of SmokeLoader

SmokeLoader 2020-06-10 · m.alvar.es · Marcos Alvares

Unpacking Smokeloader and Reconstructing PE Programatically using LIEF

SmokeLoader 2020-05-24 · Malware and Stuff · Andreas Klopsch

Examining Smokeloader's Anti Hooking technique

SmokeLoader 2020-05-24 · Positive Technologies · PT ESC Threat Intelligence

Operation TA505: network infrastructure. Part 3.

AndroMut Buhtrap SmokeLoader 2020-03-04 · CrowdStrike · CrowdStrike

2020 CrowdStrike Global Threat Report

MESSAGETAP More_eggs 8.t Dropper Anchor BabyShark BadNews Clop Cobalt Strike CobInt Cobra Carbon System Cutwail DanaBot Dharma DoppelDridex DoppelPaymer Dridex Emotet FlawedAmmyy FriedEx Gandcrab Get2 IcedID ISFB KerrDown LightNeuron LockerGoga Maze MECHANICAL Necurs Nokki Outlook Backdoor Phobos Predator The Thief QakBot REvil RobinHood Ryuk SDBbot Skipper SmokeLoader TerraRecon TerraStealer TerraTV TinyLoader TrickBot Vidar Winnti ANTHROPOID SPIDER APT23 APT31 APT39 APT40 BlackTech BuhTrap Charming Kitten CLOCKWORK SPIDER DOPPEL SPIDER FIN7 Gamaredon Group GOBLIN PANDA MONTY SPIDER MUSTANG PANDA NARWHAL SPIDER NOCTURNAL SPIDER PINCHY SPIDER SALTY SPIDER SCULLY SPIDER SMOKY SPIDER Thrip VENOM SPIDER VICEROY TIGER 2020-02-18 · Github (DanusMinimus) · Dan Lisichkin

Analyzing Modern Malware Techniques Part 4: I'm afraid of no packer(Part 1 of 2)

SmokeLoader 2019-11-21 · SentinelOne · Mario Ciccarelli

Going Deep | A Guide to Reversing Smoke Loader Malware

SmokeLoader 2019-10-31 · m.alvar.es · Marcos Alvares

Dynamic Imports and Working Around Indirect Calls - Smokeloader Study Case

SmokeLoader 2019-08-05 · security.neurolabs · Marcos Alvares

Smokeloader's Hardcoded Domains - Sneaky Third Party Vendor or Cheap Buyer?

SmokeLoader 2019-07-09 · Check Point · Israel Gubi

The 2019 Resurgence of Smokeloader

SmokeLoader 2019-05-02 · Proofpoint · Bryan Campbell, Proofpoint Threat Insight Team

2019: The Return of Retefe

Dok Retefe SmokeLoader 2018-12-19 · Palo Alto Networks Unit 42 · Kaoru Hayashi

Analysis of Smoke Loader in New Tsunami Campaign

SmokeLoader 2018-09-18 · int 0xcc blog · Raashid Bhat

A taste of our own medicine: How SmokeLoader is deceiving configuration extraction by using binary code as bait

SmokeLoader 2018-08-14 · Plug it, play it, burn it, rip it · Alberto Ortega

Anti-Hooking checks of SmokeLoader 2018

SmokeLoader 2018-07-18 · CERT.PL · Michał Praszmo

Dissecting Smoke Loader

SmokeLoader 2018-07-03 · Talos Intelligence · Ben Baker, Holger Unterbrink

Smoking Guns - Smoke Loader learned new tricks

SmokeLoader TrickBot 2018-04-16 · Spamhaus · Spamhaus Malware Labs

Smoke Loader malware improves after Microsoft spoils its Campaign

SmokeLoader 2018-04-04 · Microsoft · Microsoft Defender ATP Research Team

Hunting down Dofoil with Windows Defender ATP

SmokeLoader 2018-01-12 · Malwarebytes · Jérôme Segura

Fake Spectre and Meltdown patch pushes Smoke Loader malware

SmokeLoader 2017-08-24 · Blaze's Security Blog · BartBlaze

Crystal Finance Millennium used to spread malware

Chthonic SmokeLoader 2017-08-04 · PhishLabs · Jason Davison

Smoke Loader Adds Additional Obfuscation Methods to Mitigate Analysis

SmokeLoader 2017-04-03 · Malware Breakdown · Malware Breakdown

Shadow Server Domains Leading to RIG Exploit Kit Dropping Smoke Loader

SmokeLoader 2016-10-17 · Malwarebytes · Jérôme Segura

New-looking Sundown EK drops Smoke Loader, Kronos banker

Kronos SmokeLoader 2016-08-05 · Malwarebytes · Malwarebytes Labs

Smoke Loader – downloader with a smokescreen still alive

SmokeLoader 2014-10-05 · Eternal Todo · Jose Miguel Esparza

Dissecting SmokeLoader (or Yulia's sweet ass proposition)

SmokeLoader

▶ [TLP:WHITE] win_smokeloader_auto (20251219 | Detects win.smokeloader.)
