CloudEyE (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:10:53 UTC

CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.

2025-11-26 · Intrinsec ·
Trouble in the air: A spree of campaigns targeting the aerospace industry in Russia
DarkWatchman CloudEyE Formbook PhantomCore 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 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 2024-03-11 · CyberInt · Adi Bleih
GuLoader Downloaded: A Look at the Latest Iteration
CloudEyE 2024-02-09 · YouTube (Embee Research) · Embee_research
Guloader Decoding With Cyberchef
CloudEyE 2023-12-06 · Elastic · Daniel Stepanic
Getting gooey with GULOADER: deobfuscating the downloader
CloudEyE 2023-09-29 · Intrinsec · CTI Intrinsec, Intrinsec
Ongoing threats targeting the energy industry
Agent Tesla CloudEyE 2023-09-19 · Checkpoint · Alexey Bukhteyev, Arie Olshtein
Unveiling the Shadows: The Dark Alliance between GuLoader and Remcos
CloudEyE Remcos 2023-08-10 · AhnLab · AhnLab ASEC Analysis Team
GuLoader Malware Disguised as Tax Invoices and Shipping Statements (Detected by MDS Products)
CloudEyE 2023-07-28 · YouTube (SANS Cyber Defense) · Stef Rand
Drop It Like It's Qbot: Separating malicious droppers, loaders, and crypters from their payloads
CloudEyE QakBot 2023-07-28 · Red Canary · Stef Rand
Drop It Like It's Qbot: Separating malicious droppers, loaders, and crypters from their payloads
CloudEyE QakBot 2023-07-23 · irfan_eternal · Muhammed Irfan V A
Guloader Deobfuscation using Ghidra
CloudEyE 2023-07-08 · Gi7w0rm
CloudEyE — From .lnk to Shellcode
CloudEyE Remcos 2023-06-29 · Morphisec · Arnold Osipov
GuLoader Campaign Targets Law Firms in the US
CloudEyE 2023-06-29 · MalwareBookReports · muzi
GuLoader: Navigating a Maze of Intricacy
CloudEyE 2023-05-22 · Check Point · Alexey Bukhteyev, Arie Olshtein

Cloud-based Malware Delivery: The Evolution of GuLoader

CloudEyE 2023-05-17 · ANY.RUN · ANY.RUN

Deobfuscating the Latest GuLoader: Automating Analysis with Ghidra Scripting

CloudEyE 2023-04-13 · Microsoft · Microsoft Threat Intelligence

Threat actors strive to cause Tax Day headaches

CloudEyE Remcos 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 2023-03-11 · Zainware labs · ZainWare

Analyzing GuLoader

CloudEyE 2023-01-05 · Symantec · Threat Hunter Team

Bluebottle: Campaign Hits Banks in French-speaking Countries in Africa

CloudEyE Cobalt Strike MimiKatz NetWire RC POORTRY Quasar RAT BlueBottle 2022-12-19 · CrowdStrike · Donato Onofri, Sarang Sonawane

Malware Analysis: GuLoader Dissection Reveals New Anti-Analysis Techniques and Code Injection Redundancy

CloudEyE 2022-10-12 · Spamhaus · Raashid Bhat

Dissecting the new shellcode-based variant of GuLoader (CloudEyE)

CloudEyE 2022-09-12 · VMRay · Pascal Brackmann

The evolution of GuLoader

CloudEyE 2022-08-29 · InQuest · David Ledbetter

Office Files, RTF files, Shellcode and more shenanigans

CloudEyE 2022-07-21 · · Cert-AgID · Cert-AgID

Tecniche per semplificare l'analisi del malware GuLoader

CloudEyE 2022-07-12 · Fortinet · James Slaughter

Spoofed Saudi Purchase Order Drops GuLoader – Part 2

CloudEyE 2022-06-02 · Mandiant · Mandiant

TRENDING EVIL Q2 2022

CloudEyE Cobalt Strike CryptBot Emotet IsaacWiper QakBot 2022-04-12 · HP · Patrick Schläpfer

Malware Campaigns Targeting African Banking Sector

CloudEyE Remcos 2022-03-30 · Securonix · Den Iyzvyk, Oleg Kolesnikov, Tim Peck

New TACTICAL#OCTOPUS Attack Campaign Targets US Entities with Malware Bundled in Tax-Themed Documents

CloudEyE 2022-01-27 · forensicitguy · Tony Lambert

GuLoader Executing Shellcode Using Callback Functions

CloudEyE 2021-11-23 · HP · Patrick Schläpfer

RATDispenser: Stealthy JavaScript Loader Dispensing RATs into the Wild

AdWind Ratty STRRAT CloudEyE Formbook Houdini Panda Stealer Remcos 2021-10-01 · HP · HP Wolf Security

Threat Insights Report Q3 - 2021

STRRAT CloudEyE NetWire RC Remcos TrickBot Vjw0rm 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 2021-08-23 · YouTube (DuMp-GuY TrIcKsTeR) · Jiří Vinopal

[2] Lokibot analyzing - spoofing GULoader and LokiBot C2 [part2] - INetSim + BurpSuite

CloudEyE Loki Password Stealer (PWS) 2021-07-07 · YouTube (DuMp-GuY TrIcKsTeR) · Jiří Vinopal

[2] Lokibot analyzing - spoofing GULoader and LokiBot C2 [part1] - Own implementation in Python

CloudEyE Loki Password Stealer (PWS) 2021-07-06 · YouTube (DuMp-GuY TrIcKsTeR) · Jiří Vinopal

[1] Lokibot analyzing - defeating GuLoader with Windbg (Kernel debugging) and Live C2

CloudEyE Loki Password Stealer (PWS) 2021-06-29 · Medium hidocohen · Hido Cohen

GuLoader’s Anti-Analysis Techniques

CloudEyE 2021-04-19 · Medium elis531989 · Eli Salem

Dancing With Shellcodes: Cracking the latest version of Guloader

CloudEyE 2021-04-13 · CERT Polska / NASK · Michał Praszmo

Keeping an eye on CloudEyE (GuLoader) - Reverse engineering the loader

CloudEyE 2021-03-06 · Click All the Things! Blog · Jamie Arndt

oleObject1.bin – OLe10nATive – shellcode

CloudEyE 2021-02-17 · K7 Security · Lokesh J

GuLoader Snowballs via MalSpam Campaigns

CloudEyE 2020-11-18 · VMRay · Mateusz Lukaszewski, Pascal Brackmann, VMRay Labs Team

Malware Analysis Spotlight: AZORult Delivered by GuLoader

Azorult CloudEyE 2020-09-17 · Joe Security's Blog · Joe Security

GuLoader's VM-Exit Instruction Hammering explained

CloudEyE 2020-09-08 · MALWATION · malwation

Malware Config Extraction Diaries #1 – GuLoader

CloudEyE 2020-08-10 · Malwarebytes · Jérôme Segura

SBA phishing scams: from malware to advanced social engineering

CloudEyE 2020-08-05 · Blueliv · Blueliv Labs Team, Carlos Rubio

Playing with GuLoader Anti-VM techniques

CloudEyE 2020-07-14 · SophosLabs Uncut · Markel Picado, Sean Gallagher

RATicate upgrades “RATs as a Service” attacks with commercial “crypter”

LokiBot BetaBot CloudEyE NetWire RC 2020-07-09 · VMRay · Pascal Brackmann

Threat Bulletin: Dissecting GuLoader’s Evasion Techniques

CloudEyE 2020-06-27 · kienmanowar Blog · m4n0w4r

Quick analysis note about GuLoader (or CloudEyE)

CloudEyE 2020-06-25 · CrowdStrike · Umesh Wanve

GuLoader: Peering Into a Shellcode-based Downloader

CloudEyE 2020-06-22 · Proofpoint · Proofpoint Threat Research Team, Sherrod DeGrippo

Hakbit Ransomware Campaign Against Germany, Austria, Switzerland

CloudEyE Hakbit 2020-06-08 · Check Point Research · Check Point Research

GuLoader? No, CloudEyE.

CloudEyE 2020-05-20 · VIPRE · VIPRE Labs

Unloading the GuLoader

CloudEyE 2020-05-08 · Twitter (@sysopfb) · Jason Reaves

Tweet on GuLoader anti analysis techniques

CloudEyE 2020-05-05 · · VinCSS · Dang Dinh Phuong, m4n0w4r

GuLoader AntiVM Techniques

CloudEyE 2020-05-04 · Twitter (@VK_intel) · Vitali Kremez

GuLoader API Loader Algorithm

CloudEyE 2020-04-29 · Twitter (@VK_intel) · Vitali Kremez

Some Insight into GuLoader family

CloudEyE 2020-04-21 · Twitter (@VK_intel) · Vitali Kremez

Tweet on Signed GuLoader

CloudEyE 2020-04-13 · K7 Security · Lokesh J

GuLoader delivers RATs and Spies in Disguise

CloudEyE 2020-04-03 · Palo Alto Networks Unit 42 · Brad Duncan

GuLoader: Malspam Campaign Installing NetWire RAT

CloudEyE NetWire RC 2020-04-02 · Morphisec · Arnold Osipov

GuLoader: The RAT Downloader

CloudEyE 2020-04-01 · Cisco · Andrea Kaiser, Shyam Sundar Ramaswami

Navigating Cybersecurity During a Pandemic: Latest Malware and Threat Actors

Azorult CloudEyE Formbook KPOT Stealer Metamorfo Nanocore RAT NetWire RC TrickBot 2020-03-19 · Twitter (@TheEnergyStory) · Dominik Reichel

Tweet on early GuLoader samples dating back to October 2019

CloudEyE 2020-03-15 · Twitter (@TheEnergyStory) · Dominik Reichel

GuLoader anti analysis/sandbox tricks

CloudEyE

- [TLP:WHITE] win_cloudeye_auto (20251219 | Detects win.cloudeye.)
- [TLP:WHITE] win_cloudeye_w0 (20200204 | Shellcode injector and downloader via RegAsm.exe payload)
