Zloader (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:40:15 UTC

This family describes the (initially small) loader, which downloads Zeus OpenSSL.

In June 2016, a new loader was dubbed DEloader by Fortinet. It has some functions borrowed from Zeus 2.0.8.9 (e.g. the versioning, nrv2b, binstorage-labels), but more importantly, it downloaded a Zeus-like banking trojan (-> Zeus OpenSSL). Furthermore, the loader shared its versioning with the Zeus OpenSSL it downloaded.
The initial samples from May 2016 were small (17920 bytes). At some point, visualEncrypt/Decrypt was added, e.g. in v1.11.0.0 (September 2016) with size 27648 bytes. In January 2017 with v1.15.0.0, obfuscation was added, which blew the size up to roughly 80k, and the loader became known as Zloader aka Terdot. These changes may be related to the Moskalvzapoe Distribution Network, which started the distribution of it at the same time.

Please note that IBM X-Force decided to call win.zloader/win.zeus_openssl "Zeus Sphinx", after mentioning it as "a new version of Zeus Sphinx" in their initial post in August 2016. Malpedia thus lists the alias "Zeus XSphinx" for win.zeus_openssl - the X to refer to IBM X-Force.

2024-12-10 · Zscaler · ThreatLabZ research team
Inside Zloader’s Latest Trick: DNS Tunneling
GhostSocks Zloader 2024-12-04 · Rapid7 · Tyler McGraw
Black Basta Ransomware Campaign Drops Zbot, DarkGate, and Custom Malware
Black Basta Cobalt Strike DarkGate SystemBC Zloader 2024-07-29 · Mandiant · Ashley Pearson, Jake Nicastro, Joseph Pisano, Josh Murchie, Joshua Shilko, Raymond Leong
UNC4393 Goes Gently into the SILENTNIGHT
Black Basta QakBot sRDI SystemBC Zloader UNC3973 UNC4393 2024-04-29 · Zscaler · Santiago Vicente
Zloader Learns Old Tricks
Zloader 2024-02-14 · K7 Security · Sudeep Waingankar
Zloader Strikes Back
Zloader 2024-01-19 · Zscaler · Ismael Garcia Perez, Santiago Vicente
Zloader: No Longer Silent in the Night
Zloader 2023-07-29 · Medium walmartglobaltech · Jason Reaves, Joshua Platt
Unknown powershell backdoor with ties to new Zloader
Zloader 2023-03-30 · United States District Court (Eastern District of New York) · Fortra, HEALTH-ISAC, Microsoft
Cracked Cobalt Strike (1:23-cv-02447)
Black Basta BlackCat LockBit RagnarLocker LockBit Black Basta BlackCat Cobalt Strike Cuba Emotet LockBit Mount Locker PLAY QakBot RagnarLocker Royal Ransom Zloader 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 2022-08-10 · Avast Decoded · Threat Research Team

Avast Q2/2022 Threat Report: Farewell to Conti, Zloader, and Maldocs; Hello Resurrection of Raccoon Stealer, and more Ransomware Attacks

Conti Raccoon RecordBreaker Zloader Caramel Tsunami 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 2022-06-24 · Palo Alto Networks Unit 42 · Mark Lim, Riley Porter

There Is More Than One Way to Sleep: Dive Deep Into the Implementations of API Hammering by Various Malware Families

BazarBackdoor Zloader 2022-06-02 · Youtube (AhmedS Kasmani) · AhmedS Kasmani

Zloader Malware Analysis - 1. Unpacking First stage.

Zloader 2022-04-25 · VinCSS · m4n0w4r, Tran Trung Kien

[RE026] A Deep Dive into Zloader - the Silent Night

Zloader 2022-04-25 · Cybereason · Aleksandar Milenkoski, Loïc Castel, Yonatan Gidnian

THREAT ANALYSIS REPORT: SocGholish and Zloader – From Fake Updates and Installers to Owning Your Systems

FAKEUPDATES Zloader 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 2022-04-14 · Avast Decoded · Vladimir Martyanov

Zloader 2: The Silent Night

ISFB Raccoon Zloader 2022-04-13 · UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA · UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA

Court order for taking down Zloader Infrastructure

Zloader 2022-04-13 · Microsoft · Amy Hogan-Burney

Notorious cybercrime gang’s botnet disrupted

Ryuk Zloader 2022-04-13 · Microsoft · Microsoft 365 Defender Threat Intelligence Team

Dismantling ZLoader: How malicious ads led to disabled security tools and ransomware

BlackMatter Cobalt Strike DarkSide Ryuk Zloader 2022-04-13 · ESET Research · Jean-Ian Boutin, Tomáš Procházka

ESET takes part in global operation to disrupt Zloader botnets

Cobalt Strike Zloader 2022-03-14 · CrowdStrike · Falcon OverWatch Team

Falcon OverWatch Threat Hunting Uncovers Ongoing NIGHT SPIDER Zloader Campaign

Zloader 2022-01-19 · Sophos · Colin Cowie, Mat Gangwer, Sophos MTR Team, Stan Andic

Zloader Installs Remote Access Backdoors and Delivers Cobalt Strike

Cobalt Strike Zloader 2022-01-11 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

Signed DLL campaigns as a service

BATLOADER Cobalt Strike ISFB Zloader 2022-01-05 · Check Point · Golan Cohen

Can You Trust a File’s Digital Signature? New Zloader Campaign exploits Microsoft’s Signature Verification putting users at risk

Zloader 2021-11-03 · Team Cymru · tcblogposts

Webinject Panel Administration: A Vantage Point into Multiple Threat Actor Campaigns - A Case Study on the Value of Threat Reconnaisance

DoppelDridex IcedID QakBot Zloader 2021-10-19 · Cisco · Artsiom Holub

STRRAT, ZLoader, and HoneyGain

STRRAT Zloader 2021-10-18 · Ali Aqeel

ZLoader Reversing

Zloader 2021-09-29 · Trend Micro · Trend Micro

Zloader Campaigns at a Glance

Zloader 2021-09-29 · Trend Micro · Trend Micro

Zloader Campaigns at a Glance (IOCs)

Zloader 2021-09-13 · SentinelOne · Antonio Cocomazzi, Antonio Pirozzi

Hide and Seek | New Zloader Infection Chain Comes With Improved Stealth and Evasion Mechanisms

Zloader 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 2021-07-08 · McAfee · Kiran Raj, Kishan N.

Zloader With a New Infection Technique

Zloader 2021-06-23 · K7 Security · Lokesh J

Java Plug-Ins Delivering Zloader

Zloader 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 2021-05-14 · GuidePoint Security · Drew Schmitt

From ZLoader to DarkSide: A Ransomware Story

DarkSide Cobalt Strike Zloader 2021-05-11 · Mal-Eats · mal_eats

Campo, a New Attack Campaign Targeting Japan

AnchorDNS BazarBackdoor campoloader Cobalt Strike Phobos Snifula TrickBot Zloader 2021-05-10 · Mal-Eats · mal_eats

Overview of Campo, a new attack campaign targeting Japan

AnchorDNS BazarBackdoor Cobalt Strike ISFB Phobos TrickBot Zloader 2021-04-21 · PhishLabs · Jessica Ellis

ZLoader Dominates Email Payloads in Q1

Zloader 2021-04-19 · Cybleinc · cybleinc

ZLoader Returns Through Spelevo Exploit Kit & Phishing Campaign

Zloader 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 2021-03-29 · Hornetsecurity · Hornetsecurity Security Lab

Zloader email campaign using MHTML to download and decrypt XLS

Zloader 2021-03-23 · Quick Heal · Anjali Raut

Zloader: Entailing Different Office Files

Zloader 2021-03-17 · HP · HP Bromium

Threat Insights Report Q4-2020

Agent Tesla BitRAT ComodoSec Dridex Emotet Ficker Stealer Formbook Zloader 2021-03-10 · · NTT Security · Hiroki Hada

日本を標的としたPseudoGateキャンペーンによるSpelevo Exploit Kitを用いた攻撃について

Zloader 2021-03-05 · Forcepoint · Kurt Natvig, Robert Neumann

Advancements in Invoicing - A highly sophisticated way to distribute ZLoader

Zloader 2021-03-01 · Group-IB · Oleg Skulkin, Roman Rezvukhin, Semyon Rogachev

Ransomware Uncovered 2020/2021

RansomEXX BazarBackdoor Buer Clop Conti DoppelPaymer Dridex Egregor IcedID Maze PwndLocker QakBot RansomEXX REvil Ryuk SDBbot TrickBot Zloader 2021-02-23 · PhishLabs · Jessica Ellis

Surge in ZLoader Attacks Observed

Zloader 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 2021-02-02 · · 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 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 2020-11-20 · ZDNet · Catalin Cimpanu

The malware that usually installs ransomware and you need to remove right away

Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DoppelPaymer Dridex Egregor Emotet FriedEx MegaCortex Phorpiex PwndLocker QakBot Ryuk SDBbot TrickBot Zloader 2020-11-18 · Sophos · Sophos

SOPHOS 2021 THREAT REPORT Navigating cybersecurity in an uncertain world

Agent Tesla Dridex TrickBot Zloader 2020-11-16 · Malwarebytes · Threat Intelligence Team

Malsmoke operators abandon exploit kits in favor of social engineering scheme

Zloader Malsmoke 2020-11-09 · Bleeping Computer · Ionut Ilascu

Fake Microsoft Teams updates lead to Cobalt Strike deployment

Cobalt Strike DoppelPaymer NjRAT Predator The Thief Zloader 2020-11-06 · · LAC WATCH · Ishikawa, Matsumoto,

Takagen

分析レポート：Emotetの裏で動くバンキングマルウェア「Zloader」に注意

Emotet Zloader 2020-11-05 · Twitter (@ffforward) · TheAnalyst

Tweet on Zloader infection leads to Cobaltstrike Installation and deployment of RYUK

Cobalt Strike Ryuk Zloader 2020-10-28 · SophosLabs Uncut · Anand Ajjan, Bill Kearny, Brett Cove, Elida Leite, Gabor Szappanos, Peter Mackenzie, Sean Gallagher, Syed Shahram

Hacks for sale: inside the Buer Loader malware-as-a-service

Buer Ryuk Zloader 2020-10-21 · · Alyac · Alyac

ZLoader 악성코드, 사업 정지 경고로 위장해 유포중

Zloader 2020-10-07 · CrowdStrike · The Falcon Complete Team

Duck Hunting with Falcon Complete: Analyzing a Fowl Banking Trojan, Part 2

QakBot Zloader 2020-09-24 · Click All the Things! Blog · Jamie Arndt

zLoader XLM Update: Macro code and behavior change

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

Salfram: Robbing the place without removing your name tag

Ave Maria ISFB SmokeLoader Zloader 2020-08-19 · SecurityLiterate · Kyle Cucci

Chantay’s Resume: Investigating a CV-Themed ZLoader Malware

Zloader 2020-08-14 · Twitter (@VK_intel) · Vitali Kremez

Tweet on Zloader infection leading to Cobaltstrike Installation

Cobalt Strike Zloader 2020-07-30 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q2 2020

AdWind Agent Tesla Arkei Stealer AsyncRAT Ave Maria Azorult DanaBot Emotet IcedID ISFB KPOT Stealer Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT Pony Raccoon RedLine Stealer Remcos Zloader 2020-07-22 · SentinelOne · Jason Reaves, Joshua Platt

Enter the Maze: Demystifying an Affiliate Involved in Maze (SNOW)

ISFB Maze TrickBot Zloader 2020-06-24 · Morphisec · Arnold Osipov

Obfuscated VBScript Drops Zloader, Ursnif, Qakbot, Dridex

Dridex ISFB QakBot Zloader 2020-06-19 · Click All the Things! Blog · Jamie

zloader: VBA, R1C1 References, and Other Tomfoolery

Zloader 2020-06-19 · Yet Another Security Blog · Michael Weber

Further Evasion in the Forgotten Corners of MS-XLS

Zloader 2020-06-11 · Nullteilerfrei Blog · Lars Wallenborn

API Hashing in the Zloader malware

Zloader 2020-06-02 · Lastline Labs · James Haughom, Stefano Ortolani

Evolution of Excel 4.0 Macro Weaponization

Agent Tesla DanaBot ISFB TrickBot Zloader 2020-05-24 · Nullteilerfrei Blog · Lars Wallenborn

Zloader String Obfuscation

Zloader 2020-05-21 · Malwarebytes · hasherezade, prsecurity

The “Silent Night” Zloader/Zbot

Zloader 2020-05-20 · Proofpoint · Dennis Schwarz, Matthew Mesa, Proofpoint Threat Research Team

ZLoader Loads Again: New ZLoader Variant Returns

Zloader 2020-05-12 · Yet Another Security Blog · Michael Weber

Evading Detection with Excel 4.0 Macros and the BIFF8 XLS Format

Zloader 2020-04-26 · Johannes Bader's Blog · Johannes Bader

The DGA of Zloader

Zloader 2020-04-07 · Youtube (DissectMalware) · Malwrologist

Malware Analysis in Action - Episode 2

Zloader 2020-03-30 · Bleeping Computer · Sergiu Gatlan

Banking Malware Spreading via COVID-19 Relief Payment Phishing

Zloader 2020-03-30 · IBM · Amir Gandler, Limor Kessem

Zeus Sphinx Trojan Awakens Amidst Coronavirus Spam Frenzy

Zeus OpenSSL Zloader 2020-03-13 · Comae · Matt Suiche

Yet Another Active Email Campaign With Malicious Excel Files Identified

Zloader 2018-09-06 · int 0xcc blog · Raashid Bhat

Dissecting DEloader malware with obfuscation

Zloader 2017-06-15 · Limor Kessem

Zeus Sphinx Pushes Empty Configuration Files — What Has the Sphinx Got Cooking?

Zloader 2017-01-26 · SecurityIntelligence · Limor Kessem

Around the World With Zeus Sphinx: From Canada to Australia and Back

Zloader 2017-01-26 · Malwarebytes · Malwarebytes Labs

Zbot with legitimate applications on board

Zloader 2016-09-22 · Forcepoint · Nicholas Griffin

Zeus Delivered by DELoader to Defraud Customers of Canadian Banks

Zloader 2016-06-21 · Fortinet · Floser Bacurio, Roland Dela Paz

The Curious Case of an Unknown Trojan Targeting German-Speaking Users

Zloader

▶ [TLP:WHITE] win_zloader_auto (20251219 | Detects win.zloader.)
