FAKEUPDATES (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-02 11:02:09 UTC

FAKEUPDATES

aka: FakeUpdate, GhoLoader, SocGholish

Actor(s): GOLD PRELUDE

FAKEUPDATES is a downloader written in JavaScript that communicates via HTTP. Supported payload types include executables and JavaScript. It writes the payloads to disk prior to launching them. FAKEUPDATES has led to further compromise via additional malware families that include CHTHONIC, DRIDEX, EMPIRE, KOADIC, DOPPELPAYMER, and AZORULT.

FAKEUPDATES has been heavily used by UNC1543, a financially motivated group.

References

2025-11-25 · Arctic Wolf ·
Russian RomCom Utilizing SocGholish to Deliver Mythic Agent to U.S. Companies Supporting Ukraine
FAKEUPDATES

2025-08-06 · Silent Push · Silent Push
Unmasking SocGholish: Silent Push Untangles the Malware Web Behind the “Pioneer of Fake Updates” and Its Operator, TA569
FAKEUPDATES MintsLoader Parrot TDS Parrot TDS WebShell Raspberry Robin

2025-04-29 · Recorded Future · Insikt Group
Uncovering MintsLoader With Recorded Future Malware Intelligence Hunting
FAKEUPDATES MintsLoader GhostWeaver Stealc TAG-124

2025-04-29 · LinkedIn (Ethical Hackers Academy) · Ethical Hackers Academy
RansomHub Ransomware Deploys Malware to Breach Corporate Networks
FAKEUPDATES RansomHub

2025-03-14 · Trend Micro · Adam O'Connor, Ian Kenefick, Jack Walsh, Laura Medina, Lucas Silva
SocGholish’s Intrusion Techniques Facilitate Distribution of RansomHub Ransomware
FAKEUPDATES RansomHub

2025-02-28 · KrebsOnSecurity · Brian Krebs

Notorious Malware, Spam Host “Prospero” Moves to Kaspersky Lab

FAKEUPDATES GootLoader

2025-02-18 · Proofpoint · Proofpoint Threat Research Team

An Update on Fake Updates: Two New Actors, and New Mac Malware

Marcher FAKEUPDATES FrigidStealer Lumma Stealer

2025-02-15 · Medium TRAC Labs · TRAC Labs

Don’t Ghost the SocGholish: GhostWeaver Backdoor

FAKEUPDATES GhostWeaver

2025-02-13 · Intel 471 · Intel 471

Threat hunting case study: SocGholish

FAKEUPDATES

2025-01-17 · Google Cloud Security · Office of the CISO

Threat Horizons - H1 2025 Threat Horizons Report

FAKEUPDATES Conti Hades LockBit Phoenix Locker RansomHub TRIPLESTRENGTH

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

2024-12-16 · Morphisec · Morphisec Labs, Nadav Lorber

CoinLurker: The Stealer Powering the Next Generation of Fake Updates

ClearFake FAKEUPDATES

2024-12-15 · Malwarebytes · Jérôme Segura

Malicious ad distributes SocGholish malware to Kaiser Permanente employees

FAKEUPDATES

2024-11-21 · Intrinsec · CTI Intrinsec, Intrinsec

PROSPERO & Proton66: Uncovering the links between bulletproof networks

Coper SpyNote FAKEUPDATES GootLoader EugenLoader

2024-11-20 · Intrinsec · Equipe CTI

PROSPERO & Proton66: Tracing Uncovering the links between bulletproof networks

Coper SpyNote FAKEUPDATES GootLoader EugenLoader IcedID Matanbuchus Nokoyawa Ransomware Pikabot

2024-09-30 · X (@GenThreatLabs) · Gen Threat Labs

Tweet on FAKEUPDATES pushing WARMCOOKIE backdoor via compromised websites targeting France

FAKEUPDATES WarmCookie

2024-07-17 · Huntress Labs · Alden Schmidt, Greg Linares, Matt Anderson
Fake Browser Updates Lead to BOINC Volunteer Computing Software
FAKEUPDATES MintsLoader AsyncRAT

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

2024-04-30 · Intrinsec · Intrinsec
Matanbuchus & Co: Code Emulation and Cybercrime Infrastructure Discovery
FAKEUPDATES Matanbuchus

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

2023-12-12 · Check Point Research · Check Point
November 2023’s Most Wanted Malware: New AsyncRAT Campaign Discovered while FakeUpdates Re-Entered the Top Ten after Brief Hiatus
FAKEUPDATES AsyncRAT

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

2023-02-26 · Proofpoint · Andrew Northern
TA569: SocGholish and Beyond
FAKEUPDATES RedLine Stealer solarmarker

2022-11-07 · SentinelOne · Aleksandar Milenkoski
SocGholish Diversifies and Expands Its Malware Staging Infrastructure to Counter Defenders
FAKEUPDATES

2022-10-27 · Microsoft · Microsoft Threat Intelligence
Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity
FAKEUPDATES BumbleBee Clop Fauppod Raspberry Robin Roshtyak Silence DEV-0950 Mustard Tempest

2022-10-27 · Microsoft · Microsoft Security Threat Intelligence
Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity
FAKEUPDATES BumbleBee Fauppod PhotoLoader Raspberry Robin Roshtyak

2022-08-19 · nccgroup · Ross Inman
Back in Black: Unlocking a LockBit 3.0 Ransomware Attack

FAKEUPDATES Cobalt Strike LockBit

2022-08-16 · SUCURI · Denis Sinegubko

SocGholish: 5+ Years of Massive Website Infections

FAKEUPDATES

2022-07-30 · The Hacker News · Ravie Lakshmanan

Microsoft Links Raspberry Robin USB Worm to Russian Evil Corp Hackers

FAKEUPDATES Raspberry Robin

2022-06-13 · Jorge Testa · Jorge Testa

Killing The Bear - Evil Corp

FAKEUPDATES Babuk Blister DoppelPaymer Dridex Entropy FriedEx Hades Macaw Phoenix Locker WastedLoader WastedLocker

2022-06-08 · Malwarebytes Labs · Threat Intelligence Team

MakeMoney malvertising campaign adds fake update template

FAKEUPDATES

2022-06-02 · Mandiant · Mandiant Intelligence

To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions

FAKEUPDATES Blister Cobalt Strike DoppelPaymer Dridex FriedEx Hades LockBit Macaw MimiKatz Phoenix Locker WastedLocker

2022-05-25 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

SocGholish Campaigns and Initial Access Kit

FAKEUPDATES Blister Cobalt Strike NetSupportManager RAT

2022-05-09 · Microsoft · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC)

Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself

AnchorDNS BlackCat BlackMatter Conti DarkSide HelloKitty Hive LockBit REvil FAKEUPDATES Griffon ATOMSILO BazarBackdoor BlackCat BlackMatter Blister Cobalt Strike Conti DarkSide Emotet FiveHands Gozi HelloKitty Hive IcedID ISFB JSSLoader LockBit LockFile Maze NightSky Pandora Phobos Phoenix Locker PhotoLoader QakBot REvil Rook Ryuk SystemBC TrickBot WastedLocker BRONZE STARLIGHT

2022-05-06 · Twitter (@MsftSecIntel) · Microsoft Security Intelligence

Twitter Thread on initial infeciton of SocGholish/ FAKEUPDATES campaigns lead to BLISTER Loader, CobaltStrike, Lockbit and followed by Hands On Keyboard activity

FAKEUPDATES Blister Cobalt Strike LockBit

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

2022-04-10 · Digital Information World · Hura Anwar
Threatening Redirect Web Service Instills Malicious Campaigns In Over 16,500 Websites
FAKEUPDATES

2022-04-07 · Avast Decoded · Jan Rubín, Pavel Novák
Parrot TDS takes over web servers and threatens millions
FAKEUPDATES Parrot TDS Parrot TDS WebShell NetSupportManager RAT

2022-04-05 · Trend Micro · Abdelrhman Sharshar, Earle Maui Earnshaw, Ian Kenefick, Lucas Silva, Mohamed Fahmy, Ryan Maglaque
Thwarting Loaders: From SocGholish to BLISTER's LockBit Payload
FAKEUPDATES Blister LockBit

2022-04-05 · Trend Micro · Abdelrhman Sharshar, Earle Maui Earnshaw, Ian Kenefick, Lucas Silva, Mohamed Fahmy, Ryan Maglaque
Thwarting Loaders: From SocGholish to BLISTER's LockBit Payload (IoCs)
FAKEUPDATES Blister LockBit

2022-04-04 · · LAC WATCH · Takehiko Takagen
Confirmation of damage to domestic e-commerce sites, actual situation of Web skimming attacks and examples of countermeasures that Rack thinks (Water Pamola)
FAKEUPDATES

2022-03-22 · Red Canary · Red Canary
2022 Threat Detection Report
FAKEUPDATES Silver Sparrow BazarBackdoor Cobalt Strike GootKit Yellow Cockatoo RAT

2022-02-26 · Mandiant · Mandiant
TRENDING EVIL Q1 2022
KEYPLUG FAKEUPDATES GootLoader BazarBackdoor QakBot

2021-07-22 · Expel · Evan Reichard, Kyle Pellett, Ryan Gott, Tyler Fornes
Incident report: Spotting SocGholish WordPress injection
FAKEUPDATES

2020-12-17 · Menlo Security · Krishnan Subramanian
Increase In Attack: SocGholish
FAKEUPDATES

2020-03-16 · Mandiant · Kelli Vanderlee
They Come in the Night: Ransomware Deployment Trends
FAKEUPDATES

2018-04-10 · Malwarebytes Labs · Jérôme Segura
'FakeUpdates' campaign leverages multiple website platforms
FAKEUPDATES

There is no Yara-Signature yet.
