ISFB (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:54:42 UTC

2006 Gozi v1.0, Gozi CRM, CRM, Papras
2010 Gozi v2.0, Gozi ISFB, ISFB, Pandemyia(*)

In September 2010, the source code of a particular Gozi CRM dll version was leaked. This led to two main branches: one became known as Gozi Prinimalka, which was merge with Pony and became Vawtrak/Neverquest.

The other branch became known as Gozi ISFB, or ISFB in short. Webinject functionality was added to this version.

There is one panel which often was used in combination with ISFB: IAP. The panel's login page comes with the title 'Login - IAP'. The body contains 'AUTHORIZATION', 'Name:', 'Password:' and a single button 'Sign in' in a minimal design. Often, the panel is directly accessible by entering the C2 IP address in a browser. But there are ISFB versions which are not directly using IAP. The bot accesses a gate, which is called the 'Dreambot' gate. See win.dreambot for further information.

ISFB often was protected by Rovnix. This led to a further complication in the naming scheme - many companies started to call ISFB Rovnix. Because the signatures started to look for Rovnix, other trojans protected by Rovnix (in particular ReactorBot and Rerdom) sometimes got wrongly labelled.

In April 2016 a combination of Gozi ISFB and Nymaim was detected. This breed became known as GozNym. The merge uses a shellcode-like version of Gozi ISFB, that needs Nymaim to run. The C2 communication is performed by Nymaim.

See win.gozi for additional historical information.

2025-12-16 · R3dy's Blog ·
Gozi Gozi Gozi - String Decryption
Gozi ISFB 2023-10-13 · Twitter (@JAMESWT_MHT) · JamesWT
Tweets on Wikiloader delivering ISFB
ISFB WikiLoader 2023-10-12 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update Q3 2023
FluBot AsyncRAT Ave Maria Cobalt Strike DCRat Havoc IcedID ISFB Nanocore RAT NjRAT QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Stealc Tofsee Vidar 2023-07-31 · Proofpoint · Kelsey Merriman, Pim Trouerbach
Out of the Sandbox: WikiLoader Digs Sophisticated Evasion
ISFB WikiLoader 2023-07-18 · Kostas TS · Kostas
Ursnif VS Italy: Il PDF del Destino
Gozi ISFB Snifula 2023-07-11 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q2 2023

Hydra AsyncRAT Aurora Stealer Ave Maria BumbleBee Cobalt Strike DCRat Havoc IcedID ISFB NjRAT QakBot Quasar RAT RecordBreaker RedLine Stealer Remcos Rhadamanthys Sliver Tofsee 2023-05-10 · Bridewell · Bridewell

Hunting for Ursnif

ISFB Royal Ransom 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 2023-03-30 · eSentire · eSentire Threat Response Unit (TRU)

eSentire Threat Intelligence Malware Analysis: BatLoader

BATLOADER Cobalt Strike ISFB SystemBC Vidar 2023-03-19 · 0xToxin Labs · @0xToxin

Gozi - Italian ShellCode Dance

Gozi ISFB 2023-03-09 · eSentire · eSentire Threat Response Unit (TRU)

BatLoader Continues to Abuse Google Search Ads to Deliver Vidar Stealer and Ursnif

BATLOADER ISFB Vidar 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 2023-02-08 · NTT Security · Ryu Hiyoshi

SteelClover Attacks Distributing Malware Via Google Ads Increased

BATLOADER ISFB RedLine Stealer 2023-01-09 · The DFIR Report · The DFIR Report

Unwrapping Ursnifs Gifts

ISFB 2022-10-24 · Medium CSIS Techblog · Benoît Ancel

Chapter 1 — From Gozi to ISFB: The history of a mythical malware family.

Gozi ISFB Snifula 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 · Group-IB · Albert Priego

We see you, Gozi Hunting the latest TTPs used for delivering the Trojan

ISFB 2022-06-07 · McAfee · Jyothi Naveen, Kiran Raj

Phishing Campaigns featuring Ursnif Trojan on the Rise

ISFB 2022-05-19 · IBM · Charlotte Hammond, Golo Mühr, Ole Villadsen

ITG23 Crypters Highlight Cooperation Between Cybercriminal Groups

IcedID ISFB Mount Locker WIZARD SPIDER 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 2022-05-08 · Qualys · Amit Gadhave

Ursnif Malware Banks on News Events for Phishing Attacks

ISFB 2022-04-14 · Avast Decoded · Vladimir Martyanov

Zloader 2: The Silent Night

ISFB Raccoon Zloader 2022-01-11 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

Signed DLL campaigns as a service

BATLOADER Cobalt Strike ISFB Zloader 2021-10-25 · Cleafy · Cleafy

Digital banking fraud: how the Gozi malware works

ISFB 2021-09-29 · Proofpoint · Proofpoint Staff, Selena Larson

TA544 Targets Italian Organizations with Ursnif Malware

ISFB 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 2021-07-30 · HP · Patrick Schläpfer

Detecting TA551 domains

Valak Dridex IcedID ISFB QakBot 2021-06-30 · The Record · Catalin Cimpanu

Gozi malware gang member arrested in Colombia

Gozi ISFB 2021-06-23 · IBM · Itzik Chimino

Ursnif Leverages Cerberus to Automate Fraudulent Bank Transfers in Italy

ISFB 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 2021-05-10 · Mal-Eats · mal_eats

Overview of Campo, a new attack campaign targeting Japan

AnchorDNS BazarBackdoor Cobalt Strike ISFB Phobos TrickBot Zloader 2021-05-04 · NCC Group · fumik0, NCC RIFT

RM3 – Curiosities of the wildest banking malware

ISFB RM3 2021-05-04 · Fox-IT · Fox IT, fumik0, the RIFT Team

RM3 – Curiosities of the wildest banking malware

ISFB 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 2021-04-06 · Intel 471 · Intel 471

EtterSilent: the underground's new favorite maldoc builder

BazarBackdoor ISFB QakBot TrickBot 2021-02-03 · ZDNet · Charlie Osborne

Ursnif Trojan has targeted over 100 Italian banks

ISFB Snifula 2021-01-12 · Fortinet · Xiaopeng Zhang

New Variant of Ursnif Continuously Targeting Italy

ISFB 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 2021-01-08 · 0xC0DECAFE · Thomas Barabosch

The malware analyst's guide to aPLib decompression

ISFB Rovnix 2020-11-27 · malware.love · Robert Giczewski

Having fun with a Ursnif VBS dropper

ISFB Snifula 2020-11-26 · Cybereason · Cybereason Nocturnus, Lior Rochberger

Cybereason vs. Egregor Ransomware

Cobalt Strike Egregor IcedID ISFB QakBot 2020-10-29 · CERT-FR · CERT-FR

LE MALWARE-AS-A-SERVICE EMOTET

Dridex Emotet ISFB QakBot 2020-10-15 · Department of Justice · Department of Justice

Officials Announce International Operation Targeting Transnational Criminal Organization QQAAZZ that Provided Money Laundering Services to High-Level Cybercriminals

Dridex ISFB TrickBot 2020-09-02 · Cisco Talos · Edmund Brumaghin, Holger Unterbrink

Salfram: Robbing the place without removing your name tag

Ave Maria ISFB SmokeLoader Zloader 2020-08-28 · Checkpoint · Check Point Research

Gozi: The Malware with a Thousand Faces

DreamBot ISFB LOLSnif SaiGon 2020-08-01 · · TG Soft · TG Soft

TG Soft Cyber - Threat Report

DarkComet Darktrack RAT Emotet ISFB 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 2020-07-29 · ESET Research · welivesecurity

THREAT REPORT Q2 2020

DEFENSOR ID HiddenAd Bundlore Pirrit Agent.BTZ Cerber ClipBanker CROSSWALK Cryptowall CTB Locker DanaBot Dharma Formbook Gandcrab Grandoreiro Houdini ISFB LockBit Locky Mailto Maze Microcin Nemty NjRAT Phobos PlugX Pony REvil Socelars STOP Tinba TrickBot WannaCryptor 2020-07-23 · Darktrace · Max Heinemeyer

The resurgence of the Ursnif banking trojan

ISFB Snifula 2020-07-22 · SentinelOne · Jason Reaves, Joshua Platt

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

ISFB Maze TrickBot Zloader 2020-07-18 · Hornetsecurity · Hornetsecurity Security Lab

Firefox Send sends Ursnif malware

ISFB 2020-07-17 · CERT-FR · CERT-FR

The Malware Dridex: Origins and Uses

Andromeda CryptoLocker Cutwail DoppelPaymer Dridex Emotet FriedEx Gameover P2P Gandcrab ISFB Murofet Necurs Predator The Thief Zeus 2020-07-01 · · TG Soft · TG Soft

Cyber-Threat Report on the cyber attacks of June 2020 in Italy

Avaddon ISFB 2020-07-01 · Cisco Talos · Edmund Brumaghin, Mariano Graziano, Nick Biasini

Threat Spotlight: Valak Slithers Its Way Into Manufacturing and Transportation Networks

Valak IcedID ISFB MyKings Spreader 2020-06-24 · Morphisec · Arnold Osipov

Obfuscated VBScript Drops Zloader, Ursnif, Qakbot, Dridex

Dridex ISFB QakBot Zloader 2020-06-23 · NCC Group · Michael Sandee, Nikolaos Pantazopoulos, Stefano Antenucci

WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group

Cobalt Strike ISFB WastedLocker 2020-06-17 · Youtube (Red Canary) · Adam Pennington, David Kaplan, Erika Noerenberg,

Matt Graeber

ATT&CK® Deep Dive: Process Injection

ISFB Ramnit TrickBot 2020-06-02 · Morphisec · Arnold Osipov

Ursnif/Gozi Delivery - Excel Macro 4.0 Utilization Uptick & OCR Bypass

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

Evolution of Excel 4.0 Macro Weaponization

Agent Tesla DanaBot ISFB TrickBot Zloader 2020-05-07 · Github (mlodic) · Matteo Lodi

Ursnif beacon decryptor

Gozi ISFB 2020-03-30 · Intezer · Michael Kajiloti

Fantastic payloads and where we find them

Dridex Emotet ISFB TrickBot 2020-03-18 · Proofpoint · Axel F, Sam Scholten

Coronavirus Threat Landscape Update

Agent Tesla Get2 ISFB Remcos 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 2020-03-03 · PWC UK · PWC UK

Cyber Threats 2019:A Year in Retrospect

KevDroid MESSAGETAP magecart AndroMut Cobalt Strike CobInt Crimson RAT DNSpionage Dridex Dtrack Emotet FlawedAmmyy FlawedGrace FriedEx Gandcrab Get2 GlobeImposter Grateful POS ISFB Kazuar LockerGoga Nokki QakBot Ramnit REvil Rifdoor RokRAT Ryuk shadowhammer ShadowPad Shifu Skipper StoneDrill Stuxnet TrickBot Winnti ZeroCleare APT41 MUSTANG PANDA Sea Turtle 2020-01-23 · SANS ISC InfoSec Forums · Brad Duncan

German language malspam pushes Ursnif

ISFB 2020-01-22 · Thomas Barabosch

The malware analyst’s guide to PE timestamps

Azorult Gozi IcedID ISFB LOLSnif SUNBURST TEARDROP 2020-01-17 · Ken Sajo, Yasuhiro Takeda, Yusuke Niwa

Battle Against Ursnif Malspam Campaign targeting Japan

Cutwail ISFB TrickBot UrlZone 2019-12-24 · Sophos · SophosLabs Threat Research

Gozi V3: tracked by their own stealth

ISFB 2019-12-23 · Palo Alto Networks Unit 42 · Brad Duncan

Wireshark Tutorial: Examining Ursnif Infections

ISFB 2019-12-07 · Secureworks · Keith Jarvis, Kevin O’Reilly

End-to-end Botnet Monitoring... Botconf 2019

Emotet ISFB QakBot 2019-08-07 · Fortinet · Xiaopeng Zhang

New Ursnif Variant Spreading by Word Document

ISFB 2019-07-11 · Proofpoint · Proofpoint Threat Insight Team

Threat Actor Profile: TA544 targets geographies from Italy to Japan with a range of malware

ISFB PandaBanker UrlZone NARWHAL SPIDER 2019-06-25 · VMRay · Tamas Boczan

Analyzing Ursnif’s Behavior Using a Malware Sandbox

ISFB 2019-06-19 · Proofpoint · Proofpoint Threat Insight Team

URLZone top malware in Japan, while Emotet and LINE Phishing round out the landscape

ISFB UrlZone NARWHAL SPIDER 2019-05-25 · 0ffset Blog · 0verfl0w_

Analyzing ISFB – The Second Loader

ISFB 2019-04-06 · Youtube (hasherezade) · hasherezade

Unpacking ISFB (including the custom 'PX' format)

ISFB 2019-04-05 · Yoroi · Antonio Pirozzi, Davide Testa

Ursnif: The Latest Evolution of the Most Popular Banking Malware

ISFB 2019-03-26 · Yoroi · Davide Testa, Luca Mella, Luigi Martire

The Ursnif Gangs keep Threatening Italy

ISFB 2019-03-13 · 0ffset Blog · 0verfl0w_

Analysing ISFB – The First Loader

ISFB 2019-03-12 · Cybereason · Assaf Dahan, Cybereason Nocturnus

New Ursnif Variant targets Japan packed with new Features

ISFB UrlZone 2019-03-11 · Minerva · Minerva Labs

Attackers Insert Themselves into the Email Conversation to Spread Malware

ISFB 2019-02-07 · Yoroi · Antonio Farina, Antonio Pirozzi, Davide Testa

Ursnif: Long Live the Steganography!

ISFB 2019-01-30 · Cyberbit · Hod Gavriel

New Ursnif Malware Variant – a Stunning Matryoshka (Матрёшка)

ISFB 2019-01-24 · Cisco Talos · John Arneson

Cisco AMP tracks new campaign that delivers Ursnif

ISFB 2019-01-15 · 0ffset Blog · 0verfl0w_

Analyzing COMmunication in Malware

ISFB 2019-01-01 · CSIS · Benoît Ancel, Peter Kruse

Dreambot Business overview 2019

ISFB 2018-12-18 · Trend Micro · Trendmicro

URSNIF, EMOTET, DRIDEX and BitPaymer Gangs Linked by a Similar Loader

Dridex Emotet FriedEx ISFB 2018-05-17 · Fidelis · Threat Research Team

Gozi V3 Technical Update

ISFB 2018-03-19 · hasherezade

Unpacking Ursnif

ISFB 2018-03-06 · Cisco Talos · Adam Weller, Edmund Brumaghin, Holger Unterbrink

Gozi ISFB Remains Active in 2018, Leverages "Dark Cloud" Botnet For Distribution

ISFB 2018-02-07 · Cylance · Threat Research Team

Threat Spotlight: URSNIF Infostealer Malware

ISFB 2018-01-17 · SANS ISC · brad

Reviewing the spam filters: Malspam pushing Gozi-ISFB

ISFB 2018-01-12 · Proofpoint · Proofpoint Staff

Holiday lull? Not so much

Dridex Emotet GlobeImposter ISFB Necurs PandaBanker UrlZone NARWHAL SPIDER 2017-11-28 · FireEye · Abhay Vaish, Sandor Nemes

Newly Observed Ursnif Variant Employs Malicious TLS Callback Technique to Achieve Process Injection

ISFB 2017-07-02 · CERT.PL · Maciej Kotowicz

ISFB: Still Live and Kicking

ISFB 2017-05-29 · Lokalhost.pl · Maciej Kotowicz

Gozi Tree

DreamBot Gozi ISFB Powersniff 2017-04-20 · Malwarebytes · Jérôme Segura

Binary Options malvertising campaign drops ISFB banking Trojan

ISFB 2016-11-01 · Ariel Koren's Blog · Ariel Koren

Ursnif Malware: Deep Technical Dive

ISFB 2016-04-14 · SecurityIntelligence · Limor Kessem, Lior Keshet

Meet GozNym: The Banking Malware Offspring of Gozi ISFB and Nymaim

ISFB Nymaim GozNym 2016-03-23 · Github (gbrindisi) · gbrindisi

Gozi ISFB Sourceccode

ISFB

▶ [TLP:WHITE] win_isfb_auto (20251219 | Detects win.isfb.)
