Formbook (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:14:17 UTC

Formbook

aka: win.xloader

Actor(s): SWEED, Cobalt

VTCollection URLhaus

FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.

References

2026-01-13 · SecurityLiterate ·
Deceiving the Deceivers: A Review of Deception Pro
Formbook

2025-11-26 · Intrinsec · CTI Intrinsec, David Sardinha
Trouble in the air: A spree of campaigns targeting the aerospace industry in Russia
DarkWatchman CloudEyE Formbook PhantomCore Remcos

2025-05-27 · Fortinet · Xiaopeng Zhang
Infostealer Malware FormBook Spread via Phishing Campaign – Part II
Formbook

2025-04-22 · Fortinet · Xiaopeng Zhang
Infostealer Malware FormBook Spread via Phishing Campaign – Part I
Formbook

2024-12-11 · Sublime · Sublime Security
Xloader deep dive: Link-based malware delivery via SharePoint impersonation
Xloader Formbook

2024-11-13 · TEHTRIS · TEHTRIS
Cracking Formbook malware: Blind deobfuscation and quick response techniques
Formbook

2024-06-15 · Medium b.magnezi · 0xMrMagnezi
Malware Analysis FormBook
Formbook

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

2024-03-01 · Logpoint · Nischal khadgi
A Comprehensive Overview on Stealer Malware Families
Agent Tesla Formbook RedLine Stealer Remcos Vidar

2024-02-28 · Security Intelligence · Golo Mühr, Ole Villadsen
X-Force data reveals top spam trends, campaigns and senior superlatives in 2023
404 Keylogger Agent Tesla Black Basta DarkGate Formbook IcedID Loki Password Stealer (PWS) Pikabot QakBot Remcos

2024-01-24 · Medium shaddy43 · Shayan Ahmed Khan
Layers of Deception: Analyzing the Complex Stages of XLoader 4.3 Malware Evolution
Xloader Formbook

2023-07-06 · kienmanowar Blog · m4n0w4r, Tran Trung Kien
[QuickNote] Examining Formbook Campaign via Phishing Emails
Formbook

2023-06-30 · Github (itaymigdal) · Itay Migdal
Formbook unpacking
Formbook

2023-06-05 · Malware Traffic Analysis · Brad Duncan
30 DAYS OF FORMBOOK: DAY 1, MONDAY 2023-06-05
Formbook

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

2023-03-30 · Zscaler · Brett Stone-Gross, Javier Vicente, Nikolaos Pantazopoulos
Technical Analysis of Xloader's Code Obfuscation in Version 4.3
Formbook

2023-03-30 · loginsoft · Saharsh Agrawal
From Innocence to Malice: The OneNote Malware Campaign Uncovered
Agent Tesla AsyncRAT DOUBLEBACK Emotet Formbook IcedID NetWire RC QakBot Quasar RAT RedLine Stealer XWorm

2023-03-16 · Trend Micro · Cedric Pernet, Jaromír Hořejší, Loseway Lu
IPFS: A New Data Frontier or a New Cybercriminal Hideout?
Agent Tesla Formbook RedLine Stealer Remcos

2023-02-28 · ANY.RUN · ANY.RUN
XLoader/FormBook: Encryption Analysis and Malware Decryption
Formbook

2023-01-30 · Checkpoint · Arie Olshtein
Following the Scent of TrickGate: 6-Year-Old Packer Used to Deploy the Most Wanted Malware
Agent Tesla Azorult Buer Cerber Cobalt Strike Emotet Formbook HawkEye Keylogger Loki Password Stealer (PWS) Maze NetWire RC Remcos REvil TrickBot

2023-01-24 · Trellix · Daksh Kapur, John Fokker, Robert Venal, Tomer Shloman
Cyberattacks Targeting Ukraine Increase 20-fold at End of 2022 Fueled by Russia-linked Gamaredon Activity
Andromeda Formbook Houdini Remcos

2022-12-08 · Trustwave · Diana Lopera, Phil Hay, Rodel Mendrez
Trojanized OneNote Document Leads to Formbook Malware
Formbook

2022-11-21 · Malwarebytes · Malwarebytes
2022-11-21 Threat Intel Report
404 Keylogger Agent Tesla Formbook Hive Remcos

2022-10-05 · Fortinet · Xiaopeng Zhang
Excel Document Delivers Multiple Malware by Exploiting CVE-2017-11882 – Part II
Formbook RedLine Stealer

2022-09-19 · Fortinet · Xiaopeng Zhang
Excel Document Delivers Multiple Malware By Exploiting CVE-2017-11882 – Part I
Formbook RedLine Stealer

2022-08-29 · · 360 netlab · wanghao
PureCrypter Loader continues to be active and has spread to more than 10 other families
404 Keylogger Agent Tesla AsyncRAT Formbook RedLine Stealer

2022-08-04 · ConnectWise · Stu Gonzalez
Formbook and Remcos Backdoor RAT by ConnectWise CRU
Formbook Remcos

2022-07-25 · · Cert-UA · Cert-UA
Mass distribution of desktops (Formbook, Snake Keylogger) and use of Malware RelicRace/RelicSource as a means of delivery (CERT-UA#5056)
404 Keylogger Formbook RelicRace

2022-07-12 · Cyren · Kervin Alintanahin
Example Analysis of Multi-Component Malware
Emotet Formbook

2022-07-01 · cyble · Cyble
Xloader Returns With New Infection Technique
Formbook

2022-05-19 · Blackberry · The BlackBerry Research & Intelligence Team
.NET Stubs: Sowing the Seeds of Discord (PureCrypter)
Aberebot AbstractEmu AdoBot 404 Keylogger Agent Tesla Amadey AsyncRAT Ave Maria BitRAT BluStealer Formbook LimeRAT Loki Password Stealer (PWS) Nanocore RAT Orcus RAT Quasar RAT Raccoon RedLine Stealer WhisperGate

2022-03-11 · Netskope · Gustavo Palazolo
New Formbook Campaign Delivered Through Phishing Emails
Formbook

2022-03-07 · · LAC WATCH · Cyber Emergency Center
I CAN'T HEAR YOU NOW! INTERNAL BEHAVIOR OF INFORMATION-STEALING MALWARE AND JSOC DETECTION TRENDS
Xloader Agent Tesla Formbook Loki Password Stealer (PWS)

2022-02-28 · AhnLab · ASEC Analysis Team
Change in Distribution Method of Malware Disguised as Estimate (VBS Script)
Formbook

2022-02-11 · forensicitguy · Tony Lambert
XLoader/Formbook Distributed by Encrypted VelvetSweatshop Spreadsheets
Formbook

2022-01-21 · Zscaler · Brett Stone-Gross, Javier Vicente
Analysis of Xloader’s C2 Network Encryption
Xloader Formbook

2022-01-18 · Elastic · Andrew Pease, Daniel Stepanic, Derek Ditch, Seth Goodwin
FORMBOOK Adopts CAB-less Approach
Formbook

2021-11-23 · HP · Patrick Schläpfer
RATDispenser: Stealthy JavaScript Loader Dispensing RATs into the Wild
AdWind Ratty STRRAT CloudEyE Formbook Houdini Panda Stealer Remcos

2021-11-16 · Yoroi · Carmelo Ragusa, Luca Mella, Luigi Martire
Office Documents: May the XLL technique change the threat Landscape in 2022?
Agent Tesla Dridex Formbook

2021-09-30 · Blackberry · The BlackBerry Research & Intelligence Team
Threat Thursday: xLoader Infostealer
Xloader Formbook

2021-09-29 · Trend Micro · Aliakbar Zahravi, Kamlapati Choubey, Peter Girnus, William Gamazo Sanchez
FormBook Adds Latest Office 365 0-Day Vulnerability (CVE-2021-40444) to Its Arsenal
Formbook

2021-07-21 · Quick Heal · Rumana Siddiqui
FormBook Malware Returns: New Variant Uses Steganography and In-Memory Loading of multiple stages to steal data
Formbook

2021-07-12 · Cipher Tech Solutions · Claire Zaboeva, Dan Dash, Melissa Frydrych
RoboSki and Global Recovery: Automation to Combat Evolving Obfuscation
404 Keylogger Agent Tesla AsyncRAT Ave Maria Azorult BitRAT Formbook HawkEye Keylogger Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT Quasar RAT RedLine Stealer Remcos

2021-07-12 · IBM · Claire Zaboeva, Dan Dash, Melissa Frydrych
RoboSki and Global Recovery: Automation to Combat Evolving Obfuscation
404 Keylogger Agent Tesla AsyncRAT Ave Maria Azorult BitRAT Formbook HawkEye Keylogger Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT Quasar RAT RedLine Stealer Remcos

2021-04-22 · Fortinet · Xiaopeng Zhang
Deep Analysis: FormBook New Variant Delivered in Phishing Campaign – Part II
Formbook

2021-04-12 · Fortinet · Xiaopeng Zhang
Deep Analysis: New FormBook Variant Delivered in Phishing Campaign – Part I
Formbook

2021-03-17 · HP · HP Bromium
Threat Insights Report Q4-2020
Agent Tesla BitRAT ComodoSec Dridex Emotet Ficker Stealer Formbook Zloader

2021-03-11 · YouTube (Malware_Analyzing_&_RE_Tips_Tricks) · Jiří Vinopal
Formbook Reversing - Part1 [Formbook .NET loader/injector analyzing, decrypting, unpacking, patching]
Formbook

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

2020-11-19 · SANS ISC InfoSec Forums · Xavier Mertens
PowerShell Dropper Delivering Formbook

Formbook

2020-11-05 · tccontre Blog · tcontre

Interesting FormBook Crypter - unconventional way to store encrypted data

Formbook

2020-10-16 · Hornetsecurity · Hornetsecurity Security Lab

VBA Purging Malspam Campaigns

Agent Tesla Formbook

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

2020-07-22 · S2W LAB Inc. · S2W LAB INTELLIGENCE TEAM

'FormBook Tracker' unveiled on the Dark Web

Formbook

2020-05-31 · Malwarebytes · hasherezade

Revisiting the NSIS-based crypter

Formbook

2020-05-14 · SophosLabs · Markel Picado

RATicate: an attacker’s waves of information-stealing malware

Agent Tesla BetaBot BlackRemote Formbook Loki Password Stealer (PWS) NetWire RC NjRAT Remcos

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

2020-03-24 · Avira · Avira Protection Labs

A new technique to analyze FormBook malware infections

Formbook

2020-01-19 · 360 · kate

BayWorld event, Cyber Attack Against Foreign Trade Industry

Azorult Formbook Nanocore RAT Revenge RAT

2019-12-12 · FireEye · Chi-en Shen, Oleg Bondarenko

Cyber Threat Landscape in Japan – Revealing Threat in the Shadow

Cerberus TSCookie Cobalt Strike Dtrack Emotet Formbook IcedID Icefog IRONHALO Loki Password Stealer (PWS) PandaBanker PLEAD POISONPLUG TrickBot BlackTech

2019-09-26 · Proofpoint · Bryan Campbell, Jeremy Hedges, Proofpoint Threat Insight Team

New WhiteShadow downloader uses Microsoft SQL to retrieve malware

WhiteShadow Agent Tesla Azorult Crimson RAT Formbook Nanocore RAT NetWire RC NjRAT Remcos

2019-07-15 · Cisco Talos · Edmund Brumaghin

SWEED: Exposing years of Agent Tesla campaigns

Agent Tesla Formbook Loki Password Stealer (PWS) SWEED

2019-06-12 · Cyberbit · Hod Gavriel

Formbook Research Hints Large Data Theft Attack Brewing

Formbook

2019-05-02 · Usual Suspect RE · Johann Aydinbas

FormBook - Hiding in plain sight

Formbook

2019-01-01 · Virus Bulletin · Gabriela Nicolao

Inside Formbook infostealer

Formbook

2018-12-05 · Botconf · Rémi Jullian

FORMBOOK In-depth malware analysis

Formbook

2018-11-01 · Peerlyst · Sudhendu

How to Analyse FormBook - A New Malware-as-a-Service

Formbook

2018-10-16 · Peerlyst · Sudhendu

How to understand FormBook - A New Malware-as-a-Service

Formbook

2018-06-22 · InQuest · Aswanda

FormBook stealer: Data theft made easy

Formbook

2018-06-20 · Cisco Talos · Paul Rascagnères, Warren Mercer

My Little FormBook

Formbook

2018-03-29 · Stormshield · Rémi Jullian

In-depth Formbook malware analysis – Obfuscation and process injection

Formbook

2018-01-29 · Vitali Kremez Blog · Vitali Kremez

Let's Learn: Dissecting FormBook Infostealer Malware: Crypter & "RunLib.dll"

Formbook

2017-10-05 · FireEye · Nart Villeneuve, Randi Eitzman, Sandor Nemes, Tyler Dean Significant FormBook Distribution Campaigns Impacting the U.S. and South Korea Formbook
2017-09-20 · NetScout · Dennis Schwarz The Formidable FormBook Form Grabber Formbook
2016-06-01 · Safety First Blog · SL4ID3R Form Grabber 2016 [Crome,FF,Opera,Thunderbird, Outlook IE Safari] Hack the world Formbook

Yara Rules

▶ [TLP:WHITE] win_formbook_auto (20251219 | Detects win.formbook.)	
▶ [TLP:WHITE] win_formbook_w0 (20230118 | No description)	

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook