BumbleBee (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:59:07 UTC

BumbleBee

aka: COLDTRAIN, SHELLSTING, Shindig

Actor(s): EXOTIC LILY, GOLD CABIN, TA578, TA579

VTCollection

This malware is delivered by an ISO file, with an DLL inside with a custom loader. Because of the unique user-agent "bumblebee" this malware was dubbed BUMBLEBEE. At the time of Analysis by Google's Threat Analysis Group (TAG) BumbleBee was observed to fetch Cobalt Strike Payloads.

References

2025-08-05 · The DFIR Report ·
From Bing Search to Ransomware: Bumblebee and AdaptixC2 Deliver Akira
AdaptixC2 Akira BumbleBee

2025-07-29 · Lumu · Antonio Gomez
Advisory Alert: BumbleBee Malware in the Spotlight
BumbleBee

2025-07-14 · Spamhaus · Spamhaus Malware Labs
Spamhaus Botnet Threat Update January to June 2025
Coper FluBot Hook Joker Mirai AsyncRAT BianLian BumbleBee Chaos Cobalt Strike DanaBot DCRat Havoc Latrodectus NjRAT Quasar RAT RedLine Stealer Remcos Rhadamanthys Sliver ValleyRAT WarmCookie XWorm

2025-06-17 · DARKReading · James Shank
Operation Endgame: Do Takedowns and Arrests Matter?
BumbleBee Emotet Pikabot SmokeLoader TrickBot

2025-05-19 · cyjax · Joe Wrieden
A Sting on Bing: Bumblebee delivered through Bing SEO poisoning campaign
BumbleBee

2024-10-18 · Netskope · Leandro Froes
New Bumblebee Loader Infection Chain Signals Possible Resurgence
BumbleBee

2024-05-30 · Europol · Europol
Largest ever operation against botnets hits dropper malware ecosystem
BumbleBee IcedID SmokeLoader SystemBC TrickBot

2024-02-13 · Proofpoint · Axel F, Selena Larson
Bumblebee Buzzes Back in Black
BumbleBee

2023-10-04 · Twitter (@Intrisec) · CTI Intrinsec
Tweet about new Bumblebee campaign leveraging CVE-2023-38831
BumbleBee

2023-09-15 · Johannes Bader's Blog · Johannes Bader
The DGA of BumbleBee
BumbleBee

2023-09-11 · Twitter (@Artilllerie) · @Artilllerie
Tweet on BumbleBee sample containing a DGA
BumbleBee

2023-09-07 · Twitter (@Intrisec) · CTI Intrinsec
Tweets on Bumblebee campaign spreading via Html smuggling downloading RAR archive with European Central Bank PDF lure and folder containing Bumblebee EXE payload.
BumbleBee

2023-09-01 · VMRay · Emre Güler
Understanding BumbleBee: BumbleBee’s malware configuration and clusters
BumbleBee

2023-08-18 · VMRay · Emre Güler
Understanding BumbleBee: The malicious behavior of BumbleBee
BumbleBee

2023-08-09 · VMRay · Emre Güler
Understanding BumbleBee: The delivery of Bumblee
BumbleBee

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

2023-06-22 · DeepInstinct · Deep Instinct Threat Lab, Mark Vaitzman, Shaul Vilkomir-Preisman
PindOS: New JavaScript Dropper Delivering Bumblebee and IcedID
PindOS BumbleBee PhotoLoader

2023-06-08 · VMRay · Patrick Staubmann
Busy Bees - The Transformation of BumbleBee
BumbleBee Cobalt Strike Conti Meterpreter Sliver

2023-04-20 · Secureworks · Counter Threat Unit ResearchTeam
Bumblebee Malware Distributed Via Trojanized Installer Downloads
BumbleBee Cobalt Strike

2023-04-18 · Twitter (@threatinsight) · Threat Insight
Tweet on TA581 using Keitaro TDS URL to download a .MSI file to deliver BumbleBee malware
BumbleBee

2023-04-16 · Botconf · Suweera De Souza
Tracking Bumblebee’s Development
BumbleBee

2023-04-16 · YouTube (botconf eu) · Crowdstrike Technical Analysis Cell (TAC), Suweera De Souza
Tracking Bumblebee’s Development
BumbleBee

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

2023-04-11 · SEC Consult · Angelo Violetti
BumbleBee hunting with a Velociraptor
BumbleBee

2023-03-29 · Krakz · Pierre Le Bourhis
BumbleBee notes
BumbleBee

2023-03-28 · Cerbero · Erik Pistelli
Reversing Complex PowerShell Malware
BumbleBee

2023-03-04 · 0xToxin Labs · @0xToxin
Bumblebee DocuSign Campaign
BumbleBee

2023-02-03 · Mandiant · Genevieve Stark, Kimberly Goody
Float Like a Butterfly Sting Like a Bee

BazarBackdoor BumbleBee Cobalt Strike

2023-01-19 · Cisco · Guilherme Venere

Following the LNK metadata trail

BumbleBee PhotoLoader QakBot

2023-01-09 · Intrinsec · CTI Intrinsec, Intrinsec

Emotet returns and deploys loaders

BumbleBee Emotet IcedID PHOTOLITE

2022-11-16 · Proofpoint · Axel F, Pim Trouerbach

A Comprehensive Look at Emotet Virus' Fall 2022 Return

BumbleBee Emotet PHOTOLITE

2022-11-10 · Intezer · Nicole Fishbein

How LNK Files Are Abused by Threat Actors

BumbleBee Emotet Mount Locker QakBot

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

2022-10-27 · 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

2022-10-13 · Spamhaus · Spamhaus Malware Labs

Spamhaus Botnet Threat Update Q3 2022

FluBot Arkei Stealer AsyncRAT Ave Maria BumbleBee Cobalt Strike DCRat Dridex Emotet Loki Password Stealer (PWS) Nanocore RAT NetWire RC NjRAT QakBot RecordBreaker RedLine Stealer Remcos Socelars Tofsee Vjw0rm

2022-10-06 · Twitter (@ESETresearch) · ESET Research

Tweet on Bumblebee being modularized like trickbot

BumbleBee

2022-10-03 · Check Point · Marc Salinas Fernandez

Bumblebee: increasing its capacity and evolving its TTPs

BumbleBee Cobalt Strike Meterpreter Sliver Vidar

2022-09-26 · The DFIR Report · The DFIR Report

BumbleBee: Round Two

BumbleBee Cobalt Strike Meterpreter

2022-09-07 · cyble · Cyble

Bumblebee Returns With New Infection Technique

BumbleBee Cobalt Strike

2022-09-05 · Infinitum IT · Arda Büyükkaya
Bumblebee Loader Malware Analysis
BumbleBee

2022-08-24 · Microsoft · Microsoft Security Experts
Looking for the ‘Sliver’ lining: Hunting for emerging command-and-control frameworks
BumbleBee Sliver

2022-08-24 · Deep instinct · Deep Instinct Threat Lab
The Dark Side of Bumblebee Malware Loader
BumbleBee

2022-08-18 · IBM · Charlotte Hammond, Ole Villadsen
From Ramnit To Bumblebee (via NeverQuest): Similarities and Code Overlap Shed Light On Relationships Between Malware Developers
BumbleBee Karius Ramnit TrickBot Vawtrak

2022-08-17 · Cybereason · Cybereason Global SOC Team
Bumblebee Loader – The High Road to Enterprise Domain Control
BumbleBee Cobalt Strike

2022-08-10 · · Weixin · Red Raindrop Team
Operation(верность) mercenary: a torrent of steel trapped in the plains of Eastern Europe
BumbleBee Cobalt Strike

2022-08-08 · The DFIR Report · The DFIR Report
BumbleBee Roasts Its Way to Domain Admin
BumbleBee Cobalt Strike

2022-08-04 · Cloudsek · Aastha Mittal, Anandeshwar Unnikrishnan
Technical Analysis of Bumblebee Malware Loader
BumbleBee

2022-08-03 · Palo Alto Networks Unit 42 · Brad Duncan
Flight of the Bumblebee: Email Lures and File Sharing Services Lead to Malware
BazarBackdoor BumbleBee Cobalt Strike Conti

2022-07-17 · Resecurity · Resecurity
Shortcut-Based (LNK) Attacks Delivering Malicious Code On The Rise
AsyncRAT BumbleBee Emotet IcedID QakBot

2022-07-07 · IBM · Charlotte Hammond, Kat Weinberger, Ole Villadsen
Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine
AnchorMail BumbleBee Cobalt Strike IcedID Meterpreter

2022-07-07 · Fortinet · Erin Lin
Notable Droppers Emerge in Recent Threat Campaigns

BumbleBee Emotet PhotoLoader QakBot

2022-06-28 · Symantec · Threat Hunter Team, Vishal Kamble

Bumblebee: New Loader Rapidly Assuming Central Position in Cyber-crime Ecosystem

BumbleBee

2022-06-14 · RiskIQ · Jordan Herman

RiskIQ: Identifying BumbleBee Command and Control Servers

BumbleBee

2022-06-13 · Sekoia · Pierre Le Bourhis, Quentin Bourgue, Threat & Detection Research Team

BumbleBee: a new trendy loader for Initial Access Brokers

BumbleBee

2022-06-07 · cyble · Cyble

Bumblebee Loader on The Rise

BumbleBee Cobalt Strike

2022-05-25 · Logpoint · Logpoint

Buzz of the Bumblebee – A new malicious loader

BumbleBee

2022-05-25 · Team Cymru · S2 Research Team

Bablosoft; Lowering the Barrier of Entry for Malicious Actors

BlackGuard BumbleBee RedLine Stealer

2022-05-19 · InfoSec Handlers Diary Blog · Brad Duncan

Bumblebee Malware from TransferXL URLs

BumbleBee Cobalt Strike

2022-05-19 · InfoSec Handlers Diary Blog · Brad Duncan

Bumblebee Malware from TransferXL URLs

BumbleBee Cobalt Strike

2022-05-12 · Intel 471 · Intel 471

What malware to look for if you want to prevent a ransomware attack

Conti BumbleBee Cobalt Strike IcedID Sliver

2022-05-12 · OALabs · Sergei Frankoff

Taking a look at Bumblebee loader

BumbleBee

2022-05-11 · InfoSec Handlers Diary Blog · Brad Duncan

TA578 using thread-hijacked emails to push ISO files for Bumblebee malware

BumbleBee Cobalt Strike IcedID PhotoLoader

2022-05-11 · SANS ISC · Brad Duncan
TA578 using thread-hijacked emails to push ISO files for Bumblebee malware
BumbleBee

2022-05-08 · Threat hunting with hints of incident response · Jouni Mikkola
Bzz.. Bzz.. Bumblebee loader
BumbleBee

2022-04-29 · NCC Group · Mike Stokkel, Nikolaos Pantazopoulos, Nikolaos Totosis
Adventures in the land of BumbleBee – a new malicious loader
BazarBackdoor BumbleBee Conti

2022-04-28 · Proofpoint · Kelsey Merriman, Pim Trouerbach
This isn't Optimus Prime's Bumblebee but it's Still Transforming
BumbleBee TA578 TA579

2022-04-28 · Bleeping Computer · Ionut Ilascu
New Bumblebee malware replaces Conti's BazarLoader in cyberattacks
BumbleBee

2022-04-27 · Medium elis531989 · Eli Salem
The chronicles of Bumblebee: The Hook, the Bee, and the Trickbot connection
BumbleBee TrickBot

2022-04-14 · Cynet · Max Malyutin
Orion Threat Alert: Flight of the BumbleBee
BumbleBee Cobalt Strike

2022-03-17 · Google · Benoit Sevens, Vladislav Stolyarov
Exposing initial access broker with ties to Conti
BazarBackdoor BumbleBee Conti EXOTIC LILY

2022-03-17 · Google · Benoit Sevens, Google Threat Analysis Group, Vladislav Stolyarov
Exposing initial access broker with ties to Conti
BazarBackdoor BumbleBee Cobalt Strike Conti

2022-01-01 · aspirets · Michael Lamb
Bumblebee Malware Loader: Threat Analysis
BumbleBee

2021-09-10 · Gigamon · Joe Slowik
Rendering Threats: A Network Perspective
BumbleBee Cobalt Strike

2021-09-09 · Trend Micro · Trend Micro

Remote Code Execution 0-Day (CVE-2021-40444) Hits Windows, Triggered Via Office Docs

BumbleBee Cobalt Strike

Yara Rules

▶ [TLP:WHITE] win_bumblebee_auto (20251219 | Detects win.bumblebee.)	
▶ [TLP:WHITE] win_bumblebee_w0 (20220330 | BumbleBee / win.bumblebee)	

Download all Yara Rules

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