IcedID (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:43:30 UTC

According to Proofpoint, IcedID (aka BokBot) is a malware originally classified as a banking malware and was first observed in 2017. It also acts as a loader for other malware, including ransomware. The well-known IcedID version consists of an initial loader which contacts a Loader C2 server, downloads the standard DLL Loader, which then delivers the standard IcedID Bot. IcedID is developed and operated by the actor named LUNAR SPIDER.

As previously published, historically there has been just one version of IcedID that has remained constant since 2017.
* In November 2022, Proofpoint researchers observed the first new variant of IcedID Proofpoint dubbed 'IcedID Lite' distributed as a follow-on payload in a TA542 Emotet campaign. It was dropped by the Emotet malware soon after the actor returned to the e-crime landscape after a nearly four-month break.
* The IcedID Lite Loader observed in November 2022 contains a static URL to download a 'Bot Pack' file with a static name (botpack.dat) which results in the IcedID Lite DLL Loader, and then delivers the Forked version of IcedID Bot, leaving out the webinjects and backconnect functionality that would typically be used for banking fraud.
* Starting in February 2023, Proofpoint observed the new Forked variant of IcedID. This variant was distributed by TA581 and one unattributed threat activity cluster which acted as initial access facilitators. The campaigns used a variety of email attachments such as Microsoft OneNote attachments and somewhat rare to see .URL attachments, which led to the Forked variant of IcedID.

2025-12-10 · Netresec ·
Latrodectus BackConnect
IcedID Keyhole Latrodectus 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 2024-07-02 · Sekoia · Quentin Bourgue
Exposing FakeBat loader: distribution methods and adversary infrastructure
BlackCat Royal Ransom EugenLoader Carbanak Cobalt Strike DICELOADER Gozi IcedID Lumma Stealer NetSupportManager RAT Pikabot RedLine Stealer SectopRAT Sliver SmokeLoader Vidar 2024-05-30 · Europol · Europol
Largest ever operation against botnets hits dropper malware ecosystem
BumbleBee IcedID SmokeLoader SystemBC TrickBot 2024-05-16 · Elastic · Daniel Stepanic, Samir Bousseaden
Spring Cleaning with LATRODECTUS: A Potential Replacement for ICEDID
IcedID Latrodectus 2024-04-29 · The DFIR Report · The DFIR Report
From IcedID to Dagon Locker Ransomware in 29 Days
IcedID Mount Locker 2024-04-08 · 0x0d4y · 0x0d4y

IcedID – Technical Analysis of an IcedID Lightweight x64 DLL

IcedID 2024-04-04 · Proofpoint · Proofpoint Threat Research Team, Team Cymru, TEAM CYMRU S2 THREAT RESEARCH

Latrodectus: This Spider Bytes Like Ice

IcedID Latrodectus 2024-04-01 · The DFIR Report · The DFIR Report

From OneNote to RansomNote: An Ice Cold Intrusion

Cobalt Strike IcedID Nokoyawa Ransomware PhotoLoader 2024-03-17 · Technical Evolution · Simon

Carving the IcedId - Part 3

IcedID 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 2024-02-15 · Department of Justice · Office of Public Affairs

Foreign National Pleads Guilty to Role in Cybercrime Schemes Involving Tens of Millions of Dollars in Losses

Egregor IcedID Maze Zeus 2024-02-15 · Bleeping Computer · Sergiu Gatlan

Zeus, IcedID malware gangs leader pleads guilty, faces 40 years in prison

Egregor IcedID Maze Zeus 2024-01-16 · Medium walmartglobaltech · Jason Reaves, Jonathan Mccay, Joshua Platt

Keyhole Analysis

IcedID Keyhole 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 2024-01-09 · 0x0d4y · 0x0d4y

IcedID – Technical Malware Analysis [Second Stage]

IcedID PhotoLoader 2023-10-12 · Netresec · Erik Hjelmvik

Forensic Timeline of an IcedID Infection

Cobalt Strike IcedID IcedID Downloader 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 2023-08-28 · The DFIR Report · The DFIR Report

HTML Smuggling Leads to Domain Wide Ransomware

Cobalt Strike IcedID Nokoyawa Ransomware 2023-07-28 · Team Cymru · S2 Research Team

Inside the IcedID BackConnect Protocol (Part 2)

IcedID 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 2023-06-10 · The DFIR Report · The DFIR Report

IcedID Brings ScreenConnect and CSharp Streamer to ALPHV Ransomware Deployment

BlackCat Cobalt Strike IcedID 2023-05-30 · Palo Alto Networks Unit 42 · Brad Duncan

Cold as Ice: Answers to Unit 42 Wireshark Quiz for IcedID

IcedID PhotoLoader 2023-05-22 · The DFIR Report · The DFIR Report

IcedID Macro Ends in Nokoyawa Ransomware

IcedID Nokoyawa Ransomware PhotoLoader 2023-05-21 · Github (0xThiebaut) · Maxime Thiebaut

PCAPeek

IcedID QakBot 2023-05-04 · Elastic · Cyril François

Unpacking ICEDID

IcedID PhotoLoader 2023-05-03 · Palo Alto Networks Unit 42 · Bob Jung, Daniel Raygoza, Mark Lim

Teasing the Secrets From Threat Actors: Malware Configuration Parsing at Scale

IcedID PhotoLoader 2023-05-03 · unpac.me · Sean Wilson

UnpacMe Weekly: New Version of IcedId Loader

IcedID PhotoLoader 2023-05-02 · loginsoft · System-41

IcedID Malware: Traversing Through its Various Incarnations

IcedID 2023-04-28 · DISCARDED Podcast · Joe Wise, Pim Trouerbach

Beyond Banking: IcedID Gets Forked

IcedID PhotoLoader 2023-04-21 · Sophos · Colin Cowie, Paul Jaramillo

IcedID: Defrosting a Recent Campaign Illustrating evolving tactics and shared infrastructure

IcedID PhotoLoader 2023-04-12 · SANS ISC · Brad Duncan

Recent IcedID (Bokbot) activity

IcedID 2023-04-12 · InfoSec Handlers Diary Blog · Brad Duncan

Recent IcedID (Bokbot) activity

IcedID PhotoLoader 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 · Twitter (@Unit42_Intel) · Unit42

Tweet on change of IcedID backconnect traffic port from 8080 to 443

IcedID 2023-04-03 · The DFIR Report · The DFIR Report

Malicious ISO File Leads to Domain Wide Ransomware

Cobalt Strike IcedID Mount Locker 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 2023-03-27 · Proofpoint · Joe Wise, Kelsey Merriman, Pim Trouerbach

Fork in the Ice: The New Era of IcedID

IcedID PHOTOFORK PHOTOLITE PhotoLoader 2023-03-20 · NVISO Labs · Maxime Thiebaut

IcedID's VNC Backdoors: Dark Cat, Anubis & Keyhole

IcedID 2023-03-17 · Elastic · Cyril François, Daniel Stepanic

Thawing the permafrost of ICEDID Summary

IcedID PhotoLoader 2023-03-01 · Zscaler · Meghraj Nandanwar, Shatak Jain

OneNote: A Growing Threat for Malware Distribution

AsyncRAT Cobalt Strike IcedID QakBot RedLine Stealer 2023-02-28 · Intel 471 · Intel 471

Malvertising Surges to Distribute Malware

EugenLoader BATLOADER IcedID 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 2023-02-24 · Team Cymru · Team Cymru

Desde Chile con Malware (From Chile with Malware)

IcedID PhotoLoader 2023-02-15 · Netresec · Erik Hjelmvik

How to Identify IcedID Network Traffic

IcedID 2023-01-20 · Blackberry · BlackBerry Research & Intelligence Team

Emotet Returns With New Methods of Evasion

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

Emotet returns and deploys loaders

BumbleBee Emotet IcedID PHOTOLITE 2022-12-23 · Trendmicro · Ian Kenefick

IcedID Botnet Distributors Abuse Google PPC to Distribute Malware

IcedID 2022-12-21 · Team Cymru · S2 Research Team

Inside the IcedID BackConnect Protocol

IcedID 2022-12-18 · ZAYOTEM · Berkay DOĞAN, Dilara BEHAR, Rabia EKŞİ, Zafer Yiğithan DERECİ

IcedID Technical Analysis Report

IcedID 2022-12-15 · ISC · Brad Duncan

Google ads lead to fake software pages pushing IcedID (Bokbot)

IcedID 2022-12-06 · EuRepoC · Camille Borrett, Kerstin Zettl-Schabath, Lena Rottinger

Conti/Wizard Spider

BazarBackdoor Cobalt Strike Conti Emotet IcedID Ryuk TrickBot WIZARD SPIDER 2022-11-14 · Twitter (@embee_research) · Matthew

Twitter thread on Yara Signatures for Qakbot Encryption Routines

IcedID QakBot 2022-10-31 · Elastic · Andrew Pease, Daniel Stepanic, Derek Ditch, Seth Goodwin

ICEDIDs network infrastructure is alive and well

IcedID 2022-10-12 · Netresec · Erik Hjelmvik

IcedID BackConnect Protocol

IcedID 2022-10-07 · Team Cymru · S2 Research Team

A Visualizza into Recent IcedID Campaigns: Reconstructing Threat Actor Metrics with Pure Signal™ Recon

IcedID PhotoLoader 2022-09-07 · Google · Google Threat Analysis Group, Pierre-Marc Bureau

Initial access broker repurposing techniques in targeted attacks against Ukraine

AnchorMail Cobalt Strike IcedID 2022-09-01 · Medium michaelkoczwara · Michael Koczwara

Hunting C2/Adversaries Infrastructure with Shodan and Censys

Brute Ratel C4 Cobalt Strike Deimos GRUNT IcedID Merlin Meterpreter Nighthawk PoshC2 Sliver 2022-08-12 · SANS ISC · Brad Duncan

Monster Libra (TA551/Shathak) pushes IcedID (Bokbot) with Dark VNC and Cobalt Strike

Cobalt Strike DarkVNC IcedID 2022-08-04 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

IcedID leverages PrivateLoader

IcedID PrivateLoader 2022-07-27 · SANS ISC · Brad Duncan

IcedID (Bokbot) with Dark VNC and Cobalt Strike

DarkVNC IcedID 2022-07-18 · Palo Alto Networks Unit 42 · Unit 42

Monster Libra

Valak IcedID GOLD CABIN 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 2022-06-24 · Soc Investigation · BalaGanesh

IcedID Banking Trojan returns with new TTPS – Detection & Response

IcedID 2022-06-21 · McAfee · Lakshya Mathur

Rise of LNK (Shortcut files) Malware

BazarBackdoor Emotet IcedID QakBot 2022-05-30 · Matthieu Walter

Automatically Unpacking IcedID Stage 1 with Angr

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

ITG23 Crypters Highlight Cooperation Between Cybercriminal Groups

IcedID ISFB Mount Locker WIZARD SPIDER 2022-05-17 · Trend Micro · Trend Micro Research

Ransomware Spotlight: RansomEXX

LaZagne Cobalt Strike IcedID MimiKatz PyXie RansomEXX TrickBot 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 2022-05-11 · InfoSec Handlers Diary Blog · Brad Duncan

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

BumbleBee Cobalt Strike IcedID PhotoLoader 2022-05-09 · Cybereason · Lior Rochberger

Cybereason vs. Quantum Locker Ransomware

IcedID Mount Locker 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 2022-05-04 · Twitter (@felixw3000) · Felix

Twitter Thread with info on infection chain with IcedId, Cobalt Strike, and Hidden VNC.

Cobalt Strike IcedID PhotoLoader 2022-04-28 · Symantec · Karthikeyan C Kasiviswanathan, Vishal Kamble

Ransomware: How Attackers are Breaching Corporate Networks

AvosLocker Conti Emotet Hive IcedID PhotoLoader QakBot TrickBot 2022-04-26 · Intel 471 · Intel 471

Conti and Emotet: A constantly destructive duo

Cobalt Strike Conti Emotet IcedID QakBot TrickBot 2022-04-25 · The DFIR Report · The DFIR Report

Quantum Ransomware

Cobalt Strike IcedID 2022-04-17 · BushidoToken Blog · BushidoToken

Lessons from the Conti Leaks

BazarBackdoor Conti Emotet IcedID Ryuk TrickBot 2022-04-14 · Bleeping Computer · Bill Toulas

Hackers target Ukrainian govt with IcedID malware, Zimbra exploits

IcedID 2022-04-14 · · Cert-UA · Cert-UA

Cyberattack on Ukrainian state organizations using IcedID malware (CERT-UA#4464)

IcedID 2022-04-04 · The DFIR Report · @0xtornado, @MettalicHack, @yatinwad, @_pete_0

Stolen Images Campaign Ends in Conti Ransomware

Conti IcedID 2022-03-31 · Trellix · Jambul Tologonov, John Fokker

Conti Leaks: Examining the Panama Papers of Ransomware

LockBit Amadey Buer Conti IcedID LockBit Mailto Maze PhotoLoader Ryuk TrickBot 2022-03-29 · Threat Post · Elizabeth Montalbano

Exchange Servers Speared in IcedID Phishing Campaign

IcedID 2022-03-28 · Bleeping Computer · Bill Toulas

Microsoft Exchange targeted for IcedID reply-chain hijacking attacks

IcedID 2022-03-28 · Fortinet · Fred Gutierrez, James Slaughter, Val Saengphaibul

Spoofed Invoice Used to Drop IcedID

IcedID 2022-03-28 · Intezer · Joakim Kennedy, Ryan Robinson

New Conversation Hijacking Campaign Delivering IcedID

IcedID PhotoLoader 2022-03-23 · Secureworks · Counter Threat Unit ResearchTeam

Threat Intelligence Executive Report Volume 2022, Number 2

Conti Emotet IcedID TrickBot 2022-03-23 · Secureworks · Counter Threat Unit ResearchTeam

GOLD ULRICK Leaks Reveal Organizational Structure and Relationships

Conti Emotet IcedID TrickBot 2022-03-21 · eSentire · eSentire Threat Response Unit (TRU)

Conti Affiliate Exposed: New Domain Names, IP Addresses and Email Addresses Uncovered

HelloKitty BazarBackdoor Cobalt Strike Conti FiveHands HelloKitty IcedID 2022-03-17 · Github (eln0ty) · Abdallah Elnoty

IcedID Analysis

IcedID 2022-03-17 · Trend Micro · Trend Micro Research

Navigating New Frontiers Trend Micro 2021 Annual Cybersecurity Report

REvil BazarBackdoor Buer IcedID QakBot REvil 2022-03-09 · nikpx · xors

BokBot Technical Analysis

IcedID 2022-02-22 · eSentire · eSentire Threat Response Unit (TRU)

IcedID to Cobalt Strike In Under 20 Minutes

Cobalt Strike IcedID PhotoLoader 2022-02-10 · Cybereason · Cybereason Global SOC Team

Threat Analysis Report: All Paths Lead to Cobalt Strike - IcedID, Emotet and QBot

Cobalt Strike Emotet IcedID QakBot 2022-01-18 · Recorded Future · Insikt Group®

2021 Adversary Infrastructure Report

BazarBackdoor Cobalt Strike Dridex IcedID QakBot TrickBot 2022-01-01 · forensicitguy · Tony Lambert

Analyzing an IcedID Loader Document

IcedID 2021-12-16 · InfoSec Handlers Diary Blog · Brad Duncan

How the "Contact Forms" campaign tricks people

IcedID 2021-12-03 · SANS ISC InfoSec Forums · Brad Duncan

TA551 (Shathak) pushes IcedID (Bokbot)

IcedID 2021-11-16 · IronNet · IronNet Threat Research, Joey Fitzpatrick, Morgan Demboski, Peter Rydzynski

How IronNet's Behavioral Analytics Detect REvil and Conti Ransomware

Cobalt Strike Conti IcedID REvil 2021-11-12 · Recorded Future · Insikt Group®

The Business of Fraud: Botnet Malware Dissemination

Mozi Dridex IcedID QakBot TrickBot 2021-11-04 · splunk · Splunk Threat Research Team

Detecting IcedID... Could It Be A Trickbot Copycat?

IcedID 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 2021-10-18 · The DFIR Report · The DFIR Report

IcedID to XingLocker Ransomware in 24 hours

Cobalt Strike IcedID Mount Locker 2021-10-15 · Trend Micro · Fernando Mercês

Ransomware Operators Found Using New "Franchise" Business Model

Glupteba IcedID Mount Locker 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 2021-08-15 · Symantec · Threat Hunter Team

The Ransomware Threat

Babuk BlackMatter DarkSide Avaddon Babuk BADHATCH BazarBackdoor BlackMatter Clop Cobalt Strike Conti DarkSide DoppelPaymer Egregor Emotet FiveHands FriedEx Hades IcedID LockBit Maze MegaCortex MimiKatz QakBot RagnarLocker REvil Ryuk TrickBot WastedLocker 2021-08-05 · Group-IB · Nikita Rostovcev, Viktor Okorokov

Prometheus TDS The key to success for Campo Loader, Hancitor, IcedID, and QBot

Prometheus Backdoor Buer campoloader Hancitor IcedID QakBot 2021-08-05 · The Record · Catalin Cimpanu

Meet Prometheus, the secret TDS behind some of today’s malware campaigns

Buer campoloader IcedID QakBot 2021-07-30 · HP · Patrick Schläpfer

Detecting TA551 domains

Valak Dridex IcedID ISFB QakBot 2021-07-26 · vmware · Pavankumar Chaudhari, Quentin Fois

Hunting IcedID and unpacking automation with Qiling

IcedID 2021-07-23 · Github (Lastline-Inc) · Pavankumar Chaudhari, Quentin Fois

YARA rules, IOCs and Scripts for extracting IcedID C2s

IcedID 2021-07-19 · The DFIR Report · The DFIR Report

IcedID and Cobalt Strike vs Antivirus

Cobalt Strike IcedID 2021-07-14 · Cerium Networks · Blumira

Threat of the Month: IcedID Malware

IcedID 2021-07-08 · vmware · Pavankumar Chaudhari, Quentin Fois

IcedID: Analysis and Detection

IcedID 2021-06-30 · Cynet · Max Malyutin

Shelob Moonlight – Spinning a Larger Web From IcedID to CONTI, a Trojan and Ransomware collaboration

Conti IcedID 2021-06-24 · Kaspersky · Anton Kuzmenko

Malicious spam campaigns delivering banking Trojans

IcedID QakBot 2021-06-24 · SentinelOne · Marco Figueroa

Evasive Maneuvers | Massive IcedID Campaign Aims For Stealth with Benign Macros

IcedID 2021-06-20 · The DFIR Report · The DFIR Report

From Word to Lateral Movement in 1 Hour

Cobalt Strike IcedID 2021-06-16 · Proofpoint · Daniel Blackford, Garrett M. Graff, Selena Larson

The First Step: Initial Access Leads to Ransomware

BazarBackdoor Egregor IcedID Maze QakBot REvil Ryuk TrickBot WastedLocker TA570 TA575 TA577 2021-05-29 · Youtube (AhmedS Kasmani) · AhmedS Kasmani

Analysis of ICEID Malware Installer DLL

IcedID 2021-05-26 · Check Point · Alex Ilgayev

Melting Ice – Tracking IcedID Servers with a few simple steps

IcedID 2021-05-19 · Team Cymru · Andy Kraus, Josh Hopkins, Nick Byers

Tracking BokBot Infrastructure Mapping a Vast and Currently Active BokBot Network

IcedID 2021-05-18 · RECON INFOSEC · Andrew Cook

An Encounter With TA551/Shathak

IcedID 2021-05-17 · Telekom · Thomas Barabosch

Let’s set ice on fire: Hunting and detecting IcedID infections

IcedID 2021-05-17 · Github (telekom-security) · Deutsche Telekom Security GmbH

icedid_analysis

IcedID 2021-05-12 · The DFIR Report

Conti Ransomware

Cobalt Strike Conti IcedID 2021-05-10 · MALWATION · malwation

IcedID Malware Technical Analysis Report

IcedID 2021-04-19 · Netresec · Erik Hjelmvik

Analysing a malware PCAP with IcedID and Cobalt Strike traffic

Cobalt Strike IcedID 2021-04-17 · YouTube (Worcester DEFCON Group) · Joel Snape, Nettitude

Inside IcedID: Anatomy Of An Infostealer

IcedID 2021-04-13 · Silent Push · Martijn Grooten

Malicious infrastructure as a service

IcedID PhotoLoader QakBot 2021-04-12 · Trend Micro · Don Ovid Ladores, Frankylnn Uy, Junestherry Salvador, Lala Manly, Raphael Centeno

A Spike in BazarCall and IcedID Activity Detected in March

BazarBackdoor IcedID 2021-04-11 · 4rchibld · 4rchibld

IcedID on my neck I’m the coolest

IcedID 2021-04-10 · Youtube (AhmedS Kasmani) · AhmedS Kasmani

Malware Analysis: IcedID Banking Trojan JavaScript Dropper

IcedID 2021-04-09 · Microsoft · Emily Hacker, Justin Carroll, Microsoft 365 Defender Threat Intelligence Team

Investigating a unique “form” of email delivery for IcedID malware

IcedID 2021-04-09 · aaqeel01 · Ali Aqeel

IcedID Analysis

IcedID 2021-04-07 · Uptycs · Abhijit Mohanta, Ashwin Vamshi

IcedID campaign spotted being spiced with Excel 4 Macros

IcedID 2021-04-07 · Minerva · Minerva Labs

IcedID - A New Threat In Office Attachments

IcedID 2021-04-01 · Reversing Labs · Robert Simmons

Code Reuse Across Packers and DLL Loaders

IcedID SystemBC 2021-03-31 · Red Canary · Red Canary

2021 Threat Detection Report

Shlayer Andromeda Cobalt Strike Dridex Emotet IcedID MimiKatz QakBot TrickBot 2021-03-31 · Silent Push · Martijn Grooten

IcedID Command and Control Infrastructure

IcedID PhotoLoader 2021-03-29 · The DFIR Report · The DFIR Report

Sodinokibi (aka REvil) Ransomware

Cobalt Strike IcedID REvil 2021-03-12 · Binary Defense · James Quinn

IcedID GZIPLOADER Analysis

IcedID 2021-03-04 · F5 · Dor Nizar, Roy Moshailov

IcedID Banking Trojan Uses COVID-19 Pandemic to Lure New Victims

IcedID 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 2021-02-26 · CrowdStrike · Eric Loui, Sergei Frankoff

Hypervisor Jackpotting: CARBON SPIDER and SPRITE SPIDER Target ESXi Servers With Ransomware to Maximize Impact

DarkSide RansomEXX Griffon Carbanak Cobalt Strike DarkSide IcedID MimiKatz PyXie RansomEXX REvil 2021-02-25 · FireEye · Brendan McKeague, Bryce Abdo, Van Ta

So Unchill: Melting UNC2198 ICEDID to Ransomware Operations

MOUSEISLAND Cobalt Strike Egregor IcedID Maze SystemBC 2021-02-25 · Mandiant · Brendan McKeague, Bryce Abdo, Van Ta

So Unchill: Melting UNC2198 ICEDID to Ransomware Operations

IcedID TA2101 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 2021-02-03 · Mimecast, Nettitude

TA551/Shathak Threat Research

IcedID 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 2021-01-19 · Medium elis531989 · Eli Salem

Funtastic Packers And Where To Find Them

Get2 IcedID QakBot 2021-01-19 · Palo Alto Networks Unit 42 · Brad Duncan

Wireshark Tutorial: Examining Emotet Infection Traffic

Emotet GootKit IcedID QakBot TrickBot 2021-01-18 · tccontre Blog · tcontre

Extracting Shellcode in ICEID .PNG Steganography

IcedID 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 2021-01-07 · Palo Alto Networks Unit 42 · Brad Duncan

TA551: Email Attack Campaign Switches from Valak to IcedID

IcedID 2021-01-01 · AWAKE · Awake Security

Breaking the Ice: Detecting IcedID and Cobalt Strike Beacon with Network Detection and Response (NDR)

Cobalt Strike IcedID PhotoLoader 2020-12-10 · · NRI SECURE · NeoSOC

マルウェア「IcedID」の検知傾向と感染に至るプロセスを徹底解説

IcedID 2020-12-09 · Cisco · Caitlin Huey, David Liebenberg

Quarterly Report: Incident Response trends from Fall 2020

Cobalt Strike IcedID Maze RansomEXX Ryuk 2020-12-09 · Microsoft · Microsoft 365 Defender Research Team

EDR in block mode stops IcedID cold

IcedID 2020-12-02 · CyberInt · Cyberint Research

IcedID Stealer Man-in-the-browser Banking Trojan

IcedID 2020-11-26 · Cybereason · Cybereason Nocturnus, Lior Rochberger

Cybereason vs. Egregor Ransomware

Cobalt Strike Egregor IcedID ISFB QakBot 2020-09-29 · Microsoft · Microsoft

Microsoft Digital Defense Report

Emotet IcedID Mailto Maze QakBot REvil RobinHood TrickBot 2020-08-16 · kienmanowar Blog · m4n0w4r

Manual Unpacking IcedID Write-up

IcedID 2020-08-12 · Juniper · Paul Kimayong

IcedID Campaign Strikes Back

IcedID 2020-08-10 · tccontre Blog · tccontre

Learning From ICEID loader - Including its Steganography Payload Parsing

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

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

Valak IcedID ISFB MyKings Spreader 2020-06-22 · zero2auto · Daniel Bunce

Unpacking Visual Basic Packers – IcedID

IcedID 2020-06-18 · Juniper · Paul Kimayong

COVID-19 and FMLA Campaigns used to install new IcedID banking malware

IcedID 2020-06-17 · Github (f0wl) · Marius Genheimer

deICEr: A Go tool for extracting config from IcedID second stage Loaders

IcedID 2020-05-29 · Group-IB · Ivan Pisarev

IcedID: When ice burns through bank accounts

IcedID 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 2020-02-18 · Sophos Labs · Luca Nagy

Nearly a quarter of malware now communicates using TLS

Dridex IcedID TrickBot 2020-01-22 · Thomas Barabosch

The malware analyst’s guide to PE timestamps

Azorult Gozi IcedID ISFB LOLSnif SUNBURST TEARDROP 2020-01-01 · Secureworks · SecureWorks

GOLD SWATHMORE

GlobeImposter Gozi IcedID TrickBot LUNAR SPIDER 2019-12-18 · Github (psrok1) · Paweł Srokosz

IcedID PNG Extractor

IcedID 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 2019-12-03 · Malwarebytes · Threat Intelligence Team

New version of IcedID Trojan uses steganographic payloads

IcedID 2019-07-09 · Fortinet · Kai Lu

A Deep Dive Into IcedID Malware: Part I - Unpacking, Hooking and Process Injection

IcedID 2019-06-25 · Dawid Golak

IcedID aka #Bokbot Analysis with Ghidra

IcedID 2019-06-16 · Fortinet · Kai Lu

A Deep Dive Into IcedID Malware: Part II - Analysis of the Core IcedID Payload (Parent Process)

IcedID 2019-04-04 · SecurityIntelligence · Limor Kessem, Nir Somech

IcedID Banking Trojan Spruces Up Injection Tactics to Add Stealth

IcedID 2019-03-21 · CrowdStrike · James Scalise, Shaun Hurley

Interception: Dissecting BokBot’s “Man in the Browser”

IcedID 2019-02-15 · CrowdStrike · Bex Hartley, Brendon Feeley

“Sin”-ful SPIDERS: WIZARD SPIDER and LUNAR SPIDER Sharing the Same Web

Dyre IcedID TrickBot Vawtrak LUNAR SPIDER WIZARD SPIDER 2019-02-06 · SecurityIntelligence · Itzik Chimino, Limor Kessem, Ophir Harpaz

IcedID Operators Using ATSEngine Injection Panel to Hit E-Commerce Sites

IcedID 2019-01-03 · CrowdStrike · James Scalise, Shaun Hurley

Digging into BokBot’s Core Module

IcedID 2018-11-09 · Youtube (OALabs) · Sean Wilson, Sergei Frankoff

Reverse Engineering IcedID / Bokbot Malware Part 2

IcedID 2018-10-26 · Youtube (OALabs) · Sergei Frankoff

Unpacking Bokbot / IcedID Malware - Part 1

IcedID 2018-09-07 · Vitali Kremez

Let's Learn: Deeper Dive into "IcedID"/"BokBot" Banking Malware: Part 1

IcedID 2018-08-09 · Fox-IT · Alfred Klason

Bokbot: The (re)birth of a banker

IcedID Vawtrak 2018-04-10 · Cisco Talos · Daphne Galme, Michael Gorelik, Ross Gibb

IcedID Banking Trojan Teams up with Ursnif/Dreambot for Distribution

IcedID 2017-11-14 · Digital Guardian · Chris Brook

IceID Banking Trojan Targeting Banks, Payment Card Providers, E-Commerce Sites

IcedID 2017-11-13 · Intezer · Jay Rosenberg

IcedID Banking Trojan Shares Code with Pony 2.0 Trojan

IcedID IcedID Downloader 2017-11-13 · SecurityIntelligence · Limor Kessem, Maor Wiesen, Tal Darsan, Tomer Agayev

New Banking Trojan IcedID Discovered by IBM X-Force Research

IcedID IcedID Downloader

▶ [TLP:WHITE] win_icedid_auto (20251219 | Detects win.icedid.)

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