

Maze (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:26:58 UTC

Maze Ransomware encrypts files and makes them inaccessible while adding a custom extension containing part of the ID of the victim. The ransom note is placed inside a text file and an htm file. There are a few different extensions appended to files which are randomly generated.

Actors are known to exfiltrate the data from the network for further extortion. It spreads mainly using email spam and various exploit kits (Spelevo, Fallout).

The code of Maze ransomware is highly complicated and obfuscated, which helps to evade security solutions using signature-based detections.

2024-05-01 · [Natto Thoughts](#) ·

Ransom-War: Russian Extortion Operations as Hybrid Warfare, Part One

[Clop Conti Maze TrickBot](#) 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](#) 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](#) 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](#) 2022-05-05 ·

[Intel 471](#) · [Intel 471](#)

Cybercrime loves company: Conti cooperated with other ransomware gangs

[LockBit Maze RagnarLocker Ryuk](#) 2022-03-31 · [Trellix](#) · [Jambul Tolgonov](#), [John Fokker](#)

Conti Leaks: Examining the Panama Papers of Ransomware

[LockBit Amadey Buer Conti IcedID LockBit Mailto Maze PhotoLoader Ryuk TrickBot](#) 2022-03-23 · [splunk](#) · [Shannon](#)

[Davis](#)

Gone in 52 Seconds...and 42 Minutes: A Comparative Analysis of Ransomware Encryption Speed

[Avaddon Babuk BlackMatter Conti DarkSide LockBit Maze Mespinoza REvil Ryuk](#) 2022-03-17 · [Sophos](#) · [Tilly](#)

[Travers](#)

The Ransomware Threat Intelligence Center

[ATOMSILO](#) [Avaddon](#) [AvosLocker](#) [BlackKingdom](#) [Ransomware](#) [BlackMatter](#) [Conti](#) [Cring](#) [DarkSide](#) [dearcy](#) [Dharma](#) [Egregor](#) [Entropy](#) [Epsilon](#) [Red](#) [Gandcrab](#) [Karma](#) [LockBit](#) [LockFile](#) [Mailto](#) [Maze](#) [Nefilim](#) [RagnarLocker](#) [Ragnarok](#) [REvil](#) [RobinHood](#) [Ryuk](#) [SamSam](#) [Snatch](#) [WannaCryptor](#) [WastedLocker](#) 2022-02-23 · [splunk](#) · [Shannon Davis](#), [SURGe](#)

An Empirically Comparative Analysis of Ransomware Binaries

[Avaddon](#) [Babuk](#) [BlackMatter](#) [Conti](#) [DarkSide](#) [LockBit](#) [Maze](#) [Mespinoza](#) [REvil](#) [Ryuk](#) 2022-02-09 · [Bleeping Computer](#) · [Lawrence Abrams](#)

Ransomware dev releases Egregor, Maze master decryption keys

[Egregor](#) [Maze](#) [Sekhmet](#) 2022-02-09 · [Security Affairs](#) · [Pierluigi Paganini](#)

Master decryption keys for Maze, Egregor, and Sekhmet ransomware leaked online

[Egregor](#) [m0yv](#) [Maze](#) [Sekhmet](#) 2021-11-03 · [CERT-FR](#) · [ANSSI](#)

Identification of a new cybercriminal group: Lockean

[DoppelPaymer](#) [Egregor](#) [Maze](#) [PwndLocker](#) [REvil](#) 2021-10-26 · [ANSSI](#)

Identification of a new cyber criminal group: Lockean

[Cobalt Strike](#) [DoppelPaymer](#) [Egregor](#) [Maze](#) [PwndLocker](#) [QakBot](#) [REvil](#) 2021-08-15 · [Symantec](#) · [Threat Hunter Team](#)

The Ransomware Threat

[Babuk](#) [BlackMatter](#) [DarkSide](#) [Avaddon](#) [Babuk](#) [BADHATCH](#) [BazarBackdoor](#) [BlackMatter](#) [Clon](#) [Cobalt Strike](#) [Conti](#) [DarkSide](#) [DoppelPaymer](#) [Egregor](#) [Emotet](#) [FiveHands](#) [FriedEx](#) [Hades](#) [IcedID](#) [LockBit](#) [Maze](#) [MegaCortex](#) [MimiKatz](#) [QakBot](#) [RagnarLocker](#) [REvil](#) [Ryuk](#) [TrickBot](#) [WastedLocker](#) 2021-08-10 · [Bleeping Computer](#) · [Sergiu Gatlan](#)

Crytek confirms Egregor ransomware attack, customer data theft

[Egregor](#) [Maze](#) 2021-08-05 · [KrebsOnSecurity](#) · [Brian Krebs](#)

Ransomware Gangs and the Name Game Distraction

[DarkSide](#) [RansomEXX](#) [Babuk](#) [Cerber](#) [Conti](#) [DarkSide](#) [DoppelPaymer](#) [Egregor](#) [FriedEx](#) [Gandcrab](#) [Hermes](#) [Maze](#) [RansomEXX](#) [REvil](#) [Ryuk](#) [Sekhmet](#) 2021-07-09 · [The Record](#) · [Catalin Cimpanu](#)

Ransomwhere project wants to create a database of past ransomware payments

[Egregor](#) [Mailto](#) [Maze](#) [REvil](#) 2021-07-01 · [DomainTools](#) · [Chad Anderson](#)

The Most Prolific Ransomware Families: A Defenders Guide

[REvil](#) [Conti](#) [Egregor](#) [Maze](#) [REvil](#) 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](#) 2021-05-18 · [The Record](#) · [Catalin Cimpanu](#)

Darkside gang estimated to have made over \$90 million from ransomware attacks

[DarkSide](#) [DarkSide](#) [Mailto](#) [Maze](#) [REvil](#) [Ryuk](#) 2021-05-18 · [Bleeping Computer](#) · [Ionut Ilascu](#)

DarkSide ransomware made \$90 million in just nine months

[DarkSide](#) [DarkSide](#) [Egregor](#) [Gandcrab](#) [Mailto](#) [Maze](#) [REvil](#) [Ryuk](#) 2021-05-10 · [DarkTracer](#) · [DarkTracer](#)

Intelligence Report on Ransomware Gangs on the DarkWeb: List of victim organizations attacked by ransomware gangs released on the DarkWeb

[RansomEXX](#) [Avaddon](#) [Babuk](#) [Clon](#) [Conti](#) [Cuba](#) [DarkSide](#) [DoppelPaymer](#) [Egregor](#) [Hades](#) [LockBit](#) [Mailto](#) [Maze](#) [MedusaLocker](#) [Mespinoza](#) [Mount Locker](#) [Nefilim](#) [Nemty](#) [Pay2Key](#) [PwndLocker](#) [RagnarLocker](#) [Ragnarok](#) [RansomEXX](#) [REvil](#) [Sekhmet](#) [SunCrypt](#) [ThunderX](#) 2021-05-07 · [Bleeping Computer](#) · [Lawrence Abrams](#)

Data leak marketplaces aim to take over the extortion economy

[Babuk](#) [Maze](#) 2021-05-06 · [Cyborg Security](#) · [Brandon Denker](#)

Ransomware: Hunting for Inhibiting System Backup or Recovery

[Avaddon Conti DarkSide LockBit Mailto Maze Mespinoza Nemty PwndLocker RagnarLocker RansomEXX REvil Ryuk Snatch ThunderX](#) 2021-04-27 · [CrowdStrike](#) · [Eben Kaplan](#), [Josh Dalman](#), [Kamil Janton](#)

Ransomware Preparedness: A Call to Action

[Dharma GlobeImposter Maze Phobos CIRCUS SPIDER TRAVELING SPIDER](#) 2021-04-07 · [ANALYST1](#) · [Jon DiMaggio](#)

Ransom Mafia Analysis of the World's First Ransomware Cartel

[Conti Egregor LockBit Maze RagnarLocker Ryuk SunCrypt TA2101 VIKING SPIDER](#) 2021-04-07 · [ANALYST1](#) · [Jon DiMaggio](#)

Ransom Mafia - Analysis of the World's First Ransomware Cartel

[Conti Egregor LockBit Maze RagnarLocker SunCrypt VIKING SPIDER](#) 2021-03-17 · [Palo Alto Networks Unit 42](#) · [Unit42](#)

Ransomware Threat Report 2021

[RansomEXX Dharma DoppelPaymer Gandcrab Mailto Maze Phobos RansomEXX REvil Ryuk WastedLocker](#) 2021-03-02 · [CERT-FR](#) · [CERT-FR](#)

The Egregor Ransomware

[Egregor Maze Sekhmet](#) 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](#) 2021-02-28 · [PWC UK](#) · [PWC UK](#)

Cyber Threats 2020: A Year in Retrospect

[elf.wellmess FlowerPower PowGoop 8.t Dropper Agent.BTZ Agent Tesla Appleseed Ave Maria Bankshot BazarBackdoor BLINDINGCAN Chinox Conti Cotx RAT Crimson RAT DUSTMAN Emotet FriedEx FunnyDream Hakbit Mailto Maze METALJACK Nefilim Oblique RAT Pay2Key PlugX QakBot REvil Ryuk StoneDrill StrongPity SUNBURST SUPERNOVA TrickBot TurlaRPC Turla SilentMoon WastedLocker WellMess Winni ZeroCleare APT10 APT23 APT27 APT31 APT41 BlackTech BRONZE EDGEWOOD Inception Framework MUSTANG PANDA Red Charon Red Nue Sea Turtle Tonto Team](#) 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](#) 2021-02-23 · [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 Winni Zloader Evilnum OUTLAW SPIDER RIDDLE SPIDER SOLAR SPIDER VIKING SPIDER](#) 2021-02-11 · [CTILEAGUE](#) · [CTILEAGUE](#)

CTIL Darknet Report – 2021

[Conti Mailto Maze REvil Ryuk](#) 2021-02-04 · [Chainanalysis](#) · [Chainalysis Team](#)

Blockchain Analysis Shows Connections Between Four of 2020's Biggest Ransomware Strains

[DoppelPaymer Egregor Maze SunCrypt](#) 2021-01-01 · [Talos](#) · [Talos Incident Response](#)

Evicting Maze

[Cobalt Strike Maze](#) 2021-01-01 · [Secureworks](#) · [SecureWorks](#)

Threat Profile: GOLD VILLAGE

[Maze TA2101](#) 2020-12-16 · [Accenture](#) · [Paul Mansfield](#)

Tracking and combatting an evolving danger: Ransomware extortion

[DarkSide Egrogor Maze Nefilim RagnarLocker REvil Ryuk SunCrypt](#) 2020-12-14 · [Medium Killbit](#) · [killbit](#)

Applying the Diamond Model to Cognizant (MSP) vs. Maze Ransomware

[Maze](#) 2020-12-10 · [US-CERT](#) · [FBI](#), [MS-ISAC](#), [US-CERT](#)

Alert (AA20-345A): Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data

[PerlBot Shlayer Agent Tesla Cerber Dridex Ghost RAT Kovter Maze MedusaLocker Nanocore RAT Nefilim](#)

[REvil Ryuk Zeus](#) 2020-12-09 · [Cisco](#) · [Caitlin Huey](#), [David Liebenberg](#)

Quarterly Report: Incident Response trends from Fall 2020

[Cobalt Strike IcedID Maze RansomEXX Ryuk](#) 2020-12-08 · [Sophos](#) · [Anand Aijan](#), [Bill Kearney](#), [Gabor Szappanos](#), [Mark](#)

[Loman](#), [Peter Mackenzie](#), [Sean Gallagher](#), [Sergio Bestulic](#), [Syed Shahram](#)

Egrogor ransomware: Maze's heir apparent

[Egrogor Maze](#) 2020-12-07 · [Minerva Labs](#) · [Tom Roter](#)

Egrogor Ransomware - An In-Depth Analysis

[Egrogor Maze Sekhmet](#) 2020-12-01 · [Trend Micro](#) · [Ryan Flores](#)

The Impact of Modern Ransomware on Manufacturing Networks

[Maze Petya REvil](#) 2020-11-18 · [KELA](#) · [Victoria Kivilevich](#)

Zooming into Darknet Threats Targeting Japanese Organizations

[Conti DoppelPaymer Egrogor LockBit Maze REvil Snake](#) 2020-11-16 · [Intel 471](#) · [Intel 471](#)

Ransomware-as-a-service: The pandemic within a pandemic

[Avaddon Clop Conti DoppelPaymer Egrogor Hakbit Mailto Maze Mespinoza RagnarLocker REvil Ryuk](#)

[SunCrypt ThunderX](#) 2020-11-11 · [Kaspersky Labs](#) · [Dmitry Bestuzhev](#), [Fedor Sinityn](#)

Targeted ransomware: it's not just about encrypting your data! Part 1 - "Old and New Friends"

[Egrogor Maze RagnarLocker](#) 2020-11-06 · [Telsy](#) · [Telsy Research Team](#)

Malware Analysis Report: Trying not to walk in the dark woods. A way out of the Maze

[Maze](#) 2020-10-29 · [Bleeping Computer](#) · [Lawrence Abrams](#)

Maze ransomware is shutting down its cybercrime operation

[Egrogor Maze](#) 2020-10-28 · [Bitdefender](#) · [Ruben Andrei Condor](#)

A Decade of WMI Abuse – an Overview of Techniques in Modern Malware

[sLoad Emotet Maze](#) 2020-10-26 · [Checkpoint](#) · [Eyal Itkin](#), [Itay Cohen](#)

Exploit Developer Spotlight: The Story of PlayBit

[Dyre Maze PyLocky Ramnit REvil](#) 2020-10-23 · [Hometsecurity](#) · [Hometsecurity Security Lab](#)

Leakware-Ransomware-Hybrid Attacks

[Avaddon Clop Conti DarkSide DoppelPaymer Mailto Maze Mespinoza Nefilim RagnarLocker REvil Sekhmet](#)

[SunCrypt](#) 2020-10-21 · [Kaspersky Labs](#) · [Fedor Sinityn](#), [Nikita Galimov](#), [Vladimir Kuskov](#)

Life of Maze ransomware

[Maze](#) 2020-10-06 · [CrowdStrike](#) · [The CrowdStrike Intel Team](#)

Double Trouble: Ransomware with Data Leak Extortion, Part 2

[Maze MedusaLocker REvil VIKING SPIDER](#) 2020-10-01 · [KELA](#) · [Victoria Kivilevich](#)

To Attack or Not to Attack: Targeting the Healthcare Sector in the Underground Ecosystem

[Conti DoppelPaymer Mailto Maze REvil Ryuk SunCrypt](#) 2020-09-29 · [Microsoft](#) · [Microsoft](#)

Microsoft Digital Defense Report

[Emotet IcedID Mailto Maze QakBot REvil RobinHood TrickBot](#) 2020-09-25 · [CrowdStrike](#) · [The CrowdStrike Intel Team](#)

Double Trouble: Ransomware with Data Leak Extortion, Part 1

[DoppelPaymer FriedEx LockBit Maze MedusaLocker RagnarLocker REvil RobinHood SamSam WastedLocker](#)

[MIMIC SPIDER PIZZO SPIDER TA2101 VIKING SPIDER](#) 2020-09-25 · [StateScoop](#) · [Benjamin Freed](#)

Baltimore ransomware attack was early attempt at data extortion, new report shows

[Maze RobinHood OUTLAW SPIDER](#) 2020-09-24 · [CrowdStrike](#) · [CrowdStrike Intelligence Team](#)

Double Trouble: Ransomware with Data Leak Extortion, Part 1

[DoppelPaymer Gandcrab LockBit Maze MedusaLocker RagnarLocker SamSam OUTLAW SPIDER](#)

[OVERLORD SPIDER](#) 2020-09-22 · [Sophos SecOps](#) · [Greg Iddon](#)

MTR Casebook: Blocking a \$15 million Maze ransomware attack

[Maze](#) 2020-09-17 · [Bleeping Computer](#) · [Lawrence Abrams](#)

Maze ransomware now encrypts via virtual machines to evade detection

[Maze](#) 2020-09-17 · [SophosLabs Uncut](#) · [Andrew Brandt](#), [Peter Mackenzie](#)

Maze attackers adopt Ragnar Locker virtual machine technique

[Maze](#) 2020-09-01 · [Cisco Talos](#) · [Caitlin Huey](#), [David Liebenberg](#)

Quarterly Report: Incident Response trends in Summer 2020

[Cobalt Strike LockBit Mailto Maze Ryuk](#) 2020-08-25 · [KELA](#) · [Victoria Kivilevich](#)

How Ransomware Gangs Find New Monetization Schemes and Evolve in Marketing

[Avaddon Clop DarkSide DoppelPaymer Mailto Maze MedusaLocker Mespinoza Nefilim RagnarLocker REvil](#)

[Sekhmet](#) 2020-08-20 · [sensecy](#) · [cyberthreatinsider](#)

Global Ransomware Attacks in 2020: The Top 4 Vulnerabilities

[Clop Maze REvil Ryuk](#) 2020-08-13 · [SentinelOne](#) · [SentinelLabs](#)

Case Study: Catching a Human-Operated Maze Ransomware Attack In Action

[Maze](#) 2020-08-04 · [ZDNet](#) · [Catalin Cimpanu](#)

Ransomware gang publishes tens of GBs of internal data from LG and Xerox

[Maze](#) 2020-08-01 · [Temple University](#) · [CARE](#)

Critical Infrastructure Ransomware Attacks

[CryptoLocker Cryptowall DoppelPaymer FriedEx Mailto Maze REvil Ryuk SamSam WannaCryptor](#) 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 · [SentinelOne](#) ·

[Jason Reaves](#), [Joshua Platt](#)

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

[ISFB Maze TrickBot Zloader](#) 2020-07-15 · [Mandiant](#) · [Corey Hildebrandt](#), [Daniel Kapellmann Zafra](#), [Keith Lunden](#), [Ken Proska](#),

[Nathan Brubaker](#)

Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families

[Clop DoppelPaymer LockerGoga Maze MegaCortex Nefilim Snake](#) 2020-06-18 · [Quick Heal](#) · [Preksha Saxena](#)

Maze ransomware continues to be a threat to the consumers

[Maze](#) 2020-06-17 · [Cognizant](#) · [Cognizant](#)

Notice of Data Breach

[Maze](#) 2020-06-16 · [BleepingComputer](#) · [Sergiu Gatlan](#)

Chipmaker MaxLinear reports data breach after Maze Ransomware attack

[Maze](#) 2020-06-04 · [Sophos Naked Security](#) · [Lisa Vaas](#)

Nuclear missile contractor hacked in Maze ransomware attack

[Maze](#) 2020-05-21 · [BrightTALK \(FireEye\)](#) · [Jeremy Kennelly](#), [Kimberly Goody](#)

Navigating MAZE: Analysis of a Rising Ransomware Threat

[Maze](#) 2020-05-12 · [SophosLabs Uncut](#) · [Sophos](#)

Maze ransomware: extorting victims for 1 year and counting

[Maze](#) 2020-05-07 · [FireEye Inc](#) · [Jeremy Kennelly](#), [Joshua Shilko](#), [Kimberly Goody](#)

Navigating the MAZE: Tactics, Techniques and Procedures Associated With MAZE Ransomware Incidents

[Maze](#) 2020-05-07 · [REDTEAM.PL](#) · [Adam Ziaja](#)

Sodinokibi / REvil ransomware

[Maze MimiKatz REvil](#) 2020-05-04 · [Blueliv](#) · [Blueliv Team](#)

Escape from the Maze

[Maze](#) 2020-05-01 · [CrowdStrike](#) · [Shaun Hurley](#)

The Many Paths Through Maze

[Maze](#) 2020-04-28 · [Microsoft](#) · [Microsoft Threat Protection Intelligence Team](#)

Ransomware groups continue to target healthcare, critical services; here's how to reduce risk

[LockBit Mailto Maze MedusaLocker Paradise RagnarLocker REvil RobinHood](#) 2020-04-18 · [Bleeping Computer](#) · [Lawrence Abrams](#)

IT services giant Cognizant suffers Maze Ransomware cyber attack

[Maze](#) 2020-04-18 · [Cognizant](#) · [Cognizant](#)

Cognizant Security Incident Update

[Maze](#) 2020-03-26 · [McAfee](#) · [Alexandre Mundo](#)

Ransomware Maze

[Maze](#) 2020-03-26 · [TechCrunch](#) · [Zack Whittaker](#)

Cyber insurer Chubb had data stolen in Maze ransomware attack

[Maze](#) 2020-03-25 · [Bitdefender](#) · [Bitdefender Team](#)

A Technical Look into Maze Ransomware

[Maze](#) 2020-03-24 · [Bleeping Computer](#) · [Lawrence Abrams](#)

Three More Ransomware Families Create Sites to Leak Stolen Data

[Clop DoppelPaymer Maze Nefilim Nemty REvil](#) 2020-03-12 · [Cyberbit](#) · [Dor Neemani](#), [Hod Gavriel](#), [Omer Fishel](#)

Lost in the Maze

[Maze](#) 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 · [Bleeping Computer](#) · [Lawrence Abrams](#)

Ransomware Attackers Use Your Cloud Backups Against You

[DoppelPaymer](#) [Maze](#) 2020-02-20 · [McAfee](#) · [Christiaan Beek](#), [Darren Fitzpatrick](#), [Eamonn Ryan](#)

CSI: Evidence Indicators for Targeted Ransomware Attacks – Part II

[Cobalt Strike](#) [LockerGoga](#) [Maze](#) [MegaCortex](#) 2020-01-30 · [ZATAZ](#) · [Damien Bancal](#)

Cyber attaque à l'encontre des serveurs de Bouygues Construction

[Maze](#) 2020-01-29 · [ANSSI](#) · [ANSSI](#)

État de la menace rançongiciel

[Clop](#) [Dharma](#) [FriedEx](#) [Gandcrab](#) [LockerGoga](#) [Maze](#) [MegaCortex](#) [REvil](#) [RobinHood](#) [Ryuk](#) [SamSam](#) 2020-01-22 ·

[Deloitte](#) · [Deloitte](#)

Project Lurus

[Maze](#) 2020-01-01 · [Secureworks](#) · [SecureWorks](#)

GOLD VILLAGE

[Maze](#) 2020-01-01 · [Blackberry](#) · [Blackberry Research](#)

State of Ransomware

[Maze](#) [MedusaLocker](#) [Nefilim](#) [Phobos](#) [REvil](#) [Ryuk](#) [STOP](#) 2019-12-24 · [Bleeping Computer](#) · [Lawrence Abrams](#)

Maze Ransomware Releases Files Stolen from City of Pensacola

[Maze](#) 2019-12-18 · [Github \(albertzsigovits\)](#) · [Albert Zsigovits](#)

Maze ransomware

[Maze](#) 2019-12-17 · [Cisco](#) · [Dave Liebenberg](#), [JJ Cummings](#)

Incident Response lessons from recent Maze ransomware attacks

[Maze](#) 2019-12-16 · [KrebsOnSecurity](#) · [Brian Krebs](#)

Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up

[Maze](#) 2019-12-11 · [Bleeping Computer](#) · [Lawrence Abrams](#)

Maze Ransomware Behind Pensacola Cyberattack, \$1M Ransom Demand

[Maze](#) 2019-11-21 · [Bleeping Computer](#) · [Lawrence Abrams](#)

Allied Universal Breached by Maze Ransomware, Stolen Data Leaked

[Maze](#) 2019-11-14 · [Proofpoint](#) · [Bryan Campbell](#), [Proofpoint Threat Insight Team](#)

TA2101 plays government imposter to distribute malware to German, Italian, and US organizations

[Maze](#) [TA2101](#) 2019-11-08 · [Twitter \(@certbund\)](#) · [CERT-Bund](#)

Tweet on Spam Mails containing MAZE

[Maze](#) 2019-10-18 · [Bleeping Computer](#) · [Sergiu Gatlan](#)

Maze Ransomware Now Delivered by Spelevo Exploit Kit

[Maze](#) 2019-05-13 · [Amigo A](#)

ChaCha Ransomware

[Maze](#) 2019-01-01 · [CrowdStrike](#) · [CrowdStrike](#)

Twisted Spider

[Maze](#) [TA2101](#)

► [TLP:WHITE] win_maze_auto (20251219 | Detects win.maze.)

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.maze>