Egregor (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:47:14 UTC

According to Heimdal, Egregor ransomware infection happens via a loader, then, in the victim’s firewall, it enables the Remote Desktop Protocol. After this part, the malware is free to move inside the victim’s network, identifying and disabling all the antivirus software it can find. The next step is the encryption of the data and the insertion of a ransom note named “RECOVER-FILES.txt” in all the compromised folders.

2024-02-15 · Bleeping Computer ·
Zeus, IcedID malware gangs leader pleads guilty, faces 40 years in prison
Egregor IcedID Maze Zeus 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 2022-05-01 · BushidoToken · BushidoToken
Gamer Cheater Hacker Spy
Egregor HelloKitty NetfilterRootkit RagnarLocker Winnti 2022-03-17 · Sophos · Tilly Travers
The Ransomware Threat Intelligence Center
ATOMSILO Avaddon AvosLocker BlackKingdom Ransomware BlackMatter Conti Cring DarkSide dearcry Dharma Egregor Entropy Epsilon Red Gandcrab Karma LockBit LockFile Mailto Maze Nefilim RagnarLocker Ragnarok REvil RobinHood Ryuk SamSam Snatch WannaCryptor WastedLocker 2022-02-09 · Security Affairs · Pierluigi Paganini
Master decryption keys for Maze, Egregor, and Sekhmet ransomware leaked online
Egregor m0yv Maze Sekhmet 2022-02-09 · Bleeping Computer · Lawrence Abrams
Ransomware dev releases Egregor, Maze master decryption keys
Egregor 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 2021-10-22 · HUNT & HACKETT · Krijn de Mik
Advanced IP Scanner: the preferred scanner in the A(P)T toolbox
Conti DarkSide Dharma Egregor Hades REvil Ryuk 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 2021-08-10 · 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 2021-08-04 · CrowdStrike · CrowdStrike Intelligence Team, CrowdStrike IR, Falcon

OverWatch Team

PROPHET SPIDER Exploits Oracle WebLogic to Facilitate Ransomware Activity

Cobalt Strike Egregor Mount Locker Prophet Spider 2021-07-27 · Bleeping Computer · Lawrence Abrams

LockBit ransomware now encrypts Windows domains using group policies

Egregor LockBit 2021-07-21 · IBM · Allison Wikoff, Chris Caridi

This Chat is Being Recorded: Egregor Ransomware Negotiations Uncovered

Egregor 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 · 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 Clop Conti Cuba DarkSide DoppelPaymer Egregor Hades LockBit Mailto Maze MedusaLocker Mespinoza Mount Locker Nefilim Nemty Pay2Key PwndLocker RagnarLocker Ragnarok RansomEXX REvil Sekhmet SunCrypt ThunderX 2021-04-26 · CoveWare · CoveWare

Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound

Avaddon Clop Conti DarkSide Egregor LockBit Mailto Phobos REvil Ryuk SunCrypt 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 2021-03-26 · Trend Micro · Trend Micro

Alleged Members of Egregor Ransomware Cartel Arrested

Egregor QakBot 2021-03-24 · Cisco · Caitlin Huey, David Liebenberg

Quarterly Report: Incident Response trends from Winter 2020-21

Egregor REvil WastedLocker 2021-03-16 · The Record · Catalin Cimpanu

France’s lead cybercrime investigator on the Egregor arrests, cybercrime

Egregor 2021-03-02 · ANSSI · ANSSI

EGREGOR RANSOMWARE

Egregor 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 2021-02-25 · 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 Winnti Zloader Evilnum OUTLAW SPIDER RIDDLE SPIDER SOLAR SPIDER VIKING SPIDER 2021-02-17 · Intel 471 · Intel 471

Egregor operation takes huge hit after police raids

Egregor 2021-02-17 · Security Service of Ukraine · Security Service of Ukraine

SBU blocks activity of transnational hacking group

Egregor 2021-02-15 · Emsisoft · EmsiSoft Malware Lab

Ransomware Profile: Egregor

Egregor 2021-02-11 · Morphisec · Morphisec

An Analysis of the Egregor Ransomware

Egregor 2021-02-04 · Chainanalysis · Chainalysis Team

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

DoppelPaymer Egregor Maze SunCrypt 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 2021-01-18 · Arete · Adam Brown, Harold Rodriguez

Egregor: The Ghost of Soviet Bears Past Haunts On

Egregor 2021-01-06 · FBI · FBI

PIN Number 20210106-001: Egregor Ransomware Targets Businesses Worldwide, Attempting to Extort Businesses by Publicly Releasing Exfiltrated Data

Egregor QakBot 2021-01-04 · Bleeping Computer · Sergiu Gatlan

TransLink confirms ransomware data theft, still restoring systems

Egregor 2020-12-16 · Accenture · Paul Mansfield

Tracking and combatting an evolving danger: Ransomware extortion

DarkSide Egregor Maze Nefilim RagnarLocker REvil Ryuk SunCrypt 2020-12-15 · Malwarebytes · Pieter Arntz

Threat profile: Egregor ransomware is making a name for itself

Egregor 2020-12-15 · Hornetsecurity · Hornetsecurity Security Lab

QakBot reducing its on disk artifacts

Egregor PwndLocker QakBot 2020-12-14 · Trend Micro · Trend Micro Research

Egregor Ransomware Launches String of High-Profile Attacks to End 2020

Egregor 2020-12-11 · · ANSSI · ANSSI

EGREGOR Ransomware

Egregor 2020-12-08 · Palo Alto Networks Unit 42 · Brittany Barbehenn, Doel Santos, Robert Falcone

Threat Assessment: Egregor Ransomware

Egregor 2020-12-08 · Sophos · Anand Aijan, Bill Kearney, Gabor Szappanos, Mark Loman, Peter Mackenzie, Sean Gallagher, Sergio

Bestulic, Syed Shahram

Egregor ransomware: Maze’s heir apparent

Egregor Maze 2020-12-07 · Minerva Labs · Tom Roter

Egregor Ransomware - An In-Depth Analysis

Egregor Maze Sekhmet 2020-12-04 · Bleeping Computer · Lawrence Abrams

Metro Vancouver's transit system hit by Egregor ransomware

Egregor 2020-12-04 · Bleeping Computer · Lawrence Abrams

Largest global staffing agency Randstad hit by Egregor ransomware

Egregor 2020-12-03 · Bleeping Computer · Lawrence Abrams

Kmart nationwide retailer suffers a ransomware attack

Egregor 2020-12-03 · Recorded Future · Insikt Group®

Egregor Ransomware, Used in a String of High-Profile Attacks, Shows Connections to QakBot

Egregor QakBot 2020-12-02 · Red Canary · twitter (@redcanary)

Tweet on increased #Qbot activity delivering Cobalt Strike & #Egregor ransomware

Cobalt Strike Egregor QakBot 2020-12-01 · Group-IB · Group-IB, Oleg Skulkin, Roman Rezvukhin, Semyon Rogachev

Egregor ransomware: The legacy of Maze lives on

Egregor QakBot 2020-11-26 · Cybereason · Cybereason Nocturnus, Lior Rochberger

Cybereason vs. Egregor Ransomware

Cobalt Strike Egregor IcedID ISFB QakBot 2020-11-25 · SentinelOne · Jim Walter

Egregor RaaS Continues the Chaos with Cobalt Strike and Rclone

Cobalt Strike Egregor 2020-11-20 · Group-IB · Oleg Skulkin, Roman Rezvukhin, Semyon Rogachev

The Locking Egregor

Egregor QakBot 2020-11-20 · ZDNet · Catalin Cimpanu

The malware that usually installs ransomware and you need to remove right away

Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DoppelPaymer Dridex Egregor Emotet FriedEx

MegaCortex Phorpiex PwndLocker QakBot Ryuk SDBbot TrickBot Zloader 2020-11-18 · KELA · Victoria Kivilevich

Zooming into Darknet Threats Targeting Japanese Organizations

Conti DoppelPaymer Egregor LockBit Maze REvil Snake 2020-11-16 · Intel 471 · Intel 471

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

Avaddon Clop Conti DoppelPaymer Egregor Hakbit Mailto Maze Mespinoza RagnarLocker REvil Ryuk

SunCrypt ThunderX 2020-11-14 · Bleeping Computer · Lawrence Abrams

Retail giant Cencosud hit by Egregor Ransomware attack, stores impacted

Egregor 2020-11-12 · Intrinsec · Jean Bichet

Egregor – Prolock: Fraternal Twins ?

Egregor PwndLocker QakBot 2020-11-11 · Kaspersky Labs · Dmitry Bestuzhev, Fedor Sinitsyn

Targeted ransomware: it’s not just about encrypting your data! Part 1 - “Old and New Friends”

Egregor Maze RagnarLocker 2020-10-29 · Bleeping Computer · Lawrence Abrams

Maze ransomware is shutting down its cybercrime operation

Egregor Maze 2020-10-29 · Security Boulevard · Tomas Meskauskas

Egregor: Sekhmet’s Cousin

Egregor 2020-10-20 · Bleeping Computer · Lawrence Abrams

Barnes & Noble hit by Egregor ransomware, strange data leaked

Egregor 2020-10-15 · ZDNet · Catalin Cimpanu

Ubisoft, Crytek data posted on ransomware gang's site

Egregor 2020-10-02 · AppGate · AppGate Labs

Appgate Labs Analyzes New Family Of Ransomware - Egregor

Egregor 2020-09-18 · · ID Ransomware · Andrew Ivanov

Egregor Ransomware

Egregor

There is no Yara-Signature yet.
