Conti (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:48:04 UTC

Conti is an extremely damaging ransomware due to the speed with which it encrypts data and spreads to other systems. It was first observed in 2020 and it is thought to be led by a Russia-based cybercrime group that goes under the Wizard Spider pseudonym. In early May 2022, the US government announced a reward of up to $10 million for information on the Conti ransomware gang.

2025-05-23 · Shadow Banker ·
Shadow Banker Makes Glorious Return, Interviews Guy Exposing Conti Command & Control
Conti Conti 2025-01-17 · Google Cloud Security · Office of the CISO
Threat Horizons - H1 2025 Threat Horizons Report
FAKEUPDATES Conti Hades LockBit Phoenix Locker RansomHub TRIPLESTRENGTH 2024-06-05 · S-RM · David Broom, Gavin Hull
Exmatter malware levels up: S-RM observes new variant with simultaneous remote code execution and data targeting
BlackCat BlackMatter Conti ExMatter LockBit REvil Ryuk 2024-05-01 · Natto Thoughts · Natto Team
Ransom-War: Russian Extortion Operations as Hybrid Warfare, Part One
Clop Conti Maze TrickBot 2024-04-10 · 0ffset Blog · Daniel Bunce
Resolving Stack Strings with Capstone Disassembler & Unicorn in Python
Conti 2023-10-03 · Luca Mella
Lighting the Exfiltration Infrastructure of a LockBit Affiliate (and more)
LockBit LockBit Conti LockBit 2023-09-12 · · ANSSI · ANSSI
FIN12: A Cybercriminal Group with Multiple Ransomware
BlackCat Cobalt Strike Conti Hive MimiKatz Nokoyawa Ransomware PLAY Royal Ransom Ryuk SystemBC
2023-09-07 · Department of Justice · Office of Public Affairs
Multiple Foreign Nationals Charged in Connection with Trickbot Malware and Conti Ransomware Conspiracies
Conti Conti TrickBot 2023-07-26 · Arctic Wolf · Akshay Suthar, Connor Belfiore, Steven Campbell
Conti and Akira: Chained Together
Akira Conti 2023-06-27 · SecurityIntelligence · Charlotte Hammond, Ole Villadsen
The Trickbot/Conti Crypters: Where Are They Now?
Black Basta Conti Mount Locker PhotoLoader Royal Ransom SystemBC TrickBot 2023-06-17 · Github (EmissarySpider) · EmissarySpider
ransomware-descendants
Babuk Conti LockBit 2023-06-08 · VMRay · Patrick Staubmann
Busy Bees - The Transformation of BumbleBee
BumbleBee Cobalt Strike Conti Meterpreter Sliver 2023-03-10 · Medium walmartglobaltech · Jason Reaves, Joshua Platt
From Royal With Love
Cobalt Strike Conti PLAY Royal Ransom Somnia 2023-02-10 · cocomelonc · cocomelonc

Malware analysis: part 8. Yara rule example for MurmurHash2. MurmurHash2 in Conti ransomware

Conti 2023-02-01 · Security Affairs · Pierluigi Paganini

New LockBit Green ransomware variant borrows code from Conti ransomware

Conti LockBit 2023-01-04 · cocomelonc

Malware development tricks: part 26. Mutex. C++ example.

AsyncRAT Conti HelloKitty 2022-12-06 · EuRepoC · Camille Borrett, Kerstin Zettl-Schabath, Lena Rottinger

Conti/Wizard Spider

BazarBackdoor Cobalt Strike Conti Emotet IcedID Ryuk TrickBot WIZARD SPIDER 2022-11-21 · Palo Alto Networks Unit 42 · Kristopher Russo

Threat Assessment: Luna Moth Callback Phishing Campaign

BazarBackdoor Conti Luna Moth 2022-09-20 · vmware · Dana Behling

Threat Report: Illuminating Volume Shadow Deletion

Conti HelloKitty 2022-09-07 · Blackberry · Anuj Soni, Ryan Chapman

The Curious Case of “Monti” Ransomware: A Real-World Doppelganger

Conti MimiKatz Veeam Dumper 2022-09-07 · Intel 471 · Intel 471

Conti vs. Monti: A Reinvention or Just a Simple Rebranding?

Conti 2022-08-22 · Microsoft · Microsoft

Extortion Economics - Ransomware’s new business model

BlackCat Conti Hive REvil AgendaCrypt Black Basta BlackCat Brute Ratel C4 Cobalt Strike Conti Hive Mount Locker Nokoyawa Ransomware REvil Ryuk 2022-08-10 · Avast Decoded · Threat Research Team

Avast Q2/2022 Threat Report: Farewell to Conti, Zloader, and Maldocs; Hello Resurrection of Raccoon Stealer, and more Ransomware Attacks

Conti Raccoon RecordBreaker Zloader Caramel Tsunami 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 2022-08-02 · Recorded Future · Insikt Group

Initial Access Brokers Are Key to Rise in Ransomware Attacks

Azorult BlackMatter Conti Mars Stealer Raccoon RedLine Stealer Taurus Stealer Vidar 2022-07-20 · Kaspersky · Dmitry Galov, Jornt van der Wiel, Marc Rivero López, Sergey Lozhkin

Luna and Black Basta — new ransomware for Windows, Linux and ESXi

Black Basta Conti 2022-06-23 · Kaspersky · Danila Nasonov, Natalya Shornikova, Nikita Nazarov, Vasily Davydov, Vladislav Burtsev

The hateful eight: Kaspersky’s guide to modern ransomware groups’ TTPs (Download Form)

BlackByte BlackCat Clop Conti Hive LockBit Mespinoza RagnarLocker 2022-06-23 · Trellix · Christiaan Beek

The Sound of Malware

Conti VHD Ransomware 2022-06-15 · ThreatStop · Ofir Ashman

First Conti, then Hive: Costa Rica gets hit with ransomware again

Conti Hive Conti Hive 2022-06-15 · AttackIQ · AttackIQ Adversary Research Team, Jackson Wells

Attack Graph Emulating the Conti Ransomware Team’s Behaviors

BazarBackdoor Conti TrickBot 2022-06-02 · Eclypsium · Eclypsium

Conti Targets Critical Firmware

Conti HermeticWiper TrickBot WhisperGate 2022-05-24 · The Hacker News · Florian Goutin

Malware Analysis: Trickbot

Cobalt Strike Conti Ryuk TrickBot 2022-05-23 · Trend Micro · Matsugaya Shingo

LockBit, Conti, and BlackCat Lead Pack Amid Rise in Active RaaS and Extortion Groups: Ransomware in Q1 2022

BlackCat Conti LockBit 2022-05-23 · Trend Micro · Trend Micro Research

LockBit, Conti, and BlackCat Lead Pack Amid Rise in Active RaaS and Extortion Groups: Ransomware in Q1 2022 (PDF)

BlackCat Conti LockBit 2022-05-20 · AdvIntel · Marley Smith, Vitali Kremez, Yelisey Boguslavskiy

DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape

AvosLocker Black Basta BlackByte BlackCat Conti HelloKitty Hive 2022-05-18 · PRODAFT Threat Intelligence · PRODAFT

Wizard Spider In-Depth Analysis

Cobalt Strike Conti WIZARD SPIDER 2022-05-17 · Advanced Intelligence · Vitali Kremez, Yelisey Boguslavskiy

Hydra with Three Heads: BlackByte & The Future of Ransomware Subsidiary Groups

BlackByte Conti 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 · YouTube (The Vertex Project) · Ryan Hallbeck

Contileaks: Identifying, Extracting, & Modeling Bitcoin Addresses

Conti 2022-05-03 · Cisco · JAIME FILSON, Kendall McKay, Paul Eubanks.

Conti and Hive ransomware operations: Leveraging victim chats for insights

Conti Hive 2022-05-03 · Talos Intelligence · JON MUNSHAW

Conti and Hive ransomware operations: What we learned from these groups' victim chats

Conti Hive 2022-05-02 · Cisco Talos · JAIME FILSON, Kendall McKay, Paul Eubanks

Conti and Hive ransomware operations: Leveraging victim chats for insights

Cobalt Strike Conti Hive 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 · PWC · PWC UK

Cyber Threats 2021: A Year in Retrospect (Annex)

Cobalt Strike Conti PlugX RokRAT Inception Framework Red Menshen 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 2022-04-21 · Secureworks · Counter Threat Unit ResearchTeam

GOLD ULRICK Continues Conti Operations Despite Public Disclosures

Conti Conti 2022-04-20 · Bleeping Computer · Bill Toulas

Microsoft Exchange servers hacked to deploy Hive ransomware

Babuk BlackByte Conti Hive LockFile 2022-04-18 · Trellix · Alexandre Mundo, Jambul Tologonov, Marc Elias

Conti Group Targets ESXi Hypervisors With its Linux Variant

Conti Conti 2022-04-17 · BushidoToken Blog · BushidoToken

Lessons from the Conti Leaks

BazarBackdoor Conti Emotet IcedID Ryuk TrickBot 2022-04-15 · Arctic Wolf · Arctic Wolf

The Karakurt Web: Threat Intel and Blockchain Analysis Reveals Extension of Conti Business Model

Conti Diavol Ryuk TrickBot 2022-04-15 · Bleeping Computer · Ionut Ilascu

Karakurt revealed as data extortion arm of Conti cybercrime syndicate

Anchor BazarBackdoor Conti TrickBot 2022-04-12 · ConnectWise · ConnectWise CRU

Threat Profile: Conti

Conti 2022-04-11 · cocomelonc

Conti ransomware source code investigation - part 2

Conti 2022-04-09 · Bleeping Computer · Lawrence Abrams

Hackers use Conti's leaked ransomware to attack Russian companies

Conti 2022-04-08 · ReversingLabs · Paul Roberts

ConversingLabs Ep. 2: Conti pivots as ransomware as a service struggles

Conti Emotet TrickBot 2022-04-06 · TRM Labs · TRM Labs

TRM Analysis Corroborates Suspected Ties Between Conti and Ryuk Ransomware Groups and Wizard Spider

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

Stolen Images Campaign Ends in Conti Ransomware

Conti IcedID 2022-04-02 · Github (cocomelonc) · cocomelonc

Malware development tricks. Find kernel32.dll base: asm style. C++ example.

Conti 2022-03-31 · nccgroup · Alex Jessop, Nikolaos Pantazopoulos, RIFT: Research and Intelligence Fusion Team, Simon Biggs

Conti-nuation: methods and techniques observed in operations post the leaks

Cobalt Strike Conti QakBot 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 2022-03-27 · cocomelonc

Conti ransomware source code investigation - part 1

Conti 2022-03-25 · Zscaler · Brett Stone-Gross

Conti Ransomware Attacks Persist With an Updated Version Despite Leaks

Conti 2022-03-23 · Intel 471 · Intel 471

Conti puts the ‘organized’ in organized crime

Conti 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 2022-03-23 · 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 2022-03-22 · ThreatStop · Ofir Ashman

Conti ransomware leaks - what happens when hackers support Russia

Conti 2022-03-21 · Threat Post · Lisa Vaas

Conti Ransomware V. 3, Including Decryptor, Leaked

Cobalt Strike Conti 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 2022-03-18 · eSentire · eSentire Threat Response Unit (TRU)

Analysis of Leaked Conti Intrusion Procedures by eSentire's Threat Response Unit (TRU)

Conti Conti 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 2022-03-17 · 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 2022-03-17 · Google · Benoit Sevens, Vladislav Stolyarov

Exposing initial access broker with ties to Conti

BazarBackdoor BumbleBee Conti EXOTIC LILY 2022-03-16 · Dragos · Josh Hanrahan

Suspected Conti Ransomware Activity in the Auto Manufacturing Sector

Conti Emotet 2022-03-16 · Symantec · Symantec Threat Hunter Team

The Ransomware Threat Landscape: What to Expect in 2022

AvosLocker BlackCat BlackMatter Conti DarkSide DoppelPaymer Emotet Hive Karma Mespinoza Nemty Squirrelwaffle VegaLocker WastedLocker Yanluowang Zeppelin 2022-03-15 · Prevailion · Matt Stafford, Sherman Smith

What Wicked Webs We Un-weave

Cobalt Strike Conti 2022-03-10 · Check Point Research

Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Tech Start-Up… Sort Of

Conti 2022-03-09 · Bleeping Computer · Ionut Ilascu

CISA updates Conti ransomware alert with nearly 100 domain names

BazarBackdoor Cobalt Strike Conti TrickBot 2022-03-08 · Github (whichbuffer) · Arda Büyükkaya

Conti-Ransomware-IOC

Conti 2022-03-08 · The Record · Dina Temple-Raston

Inside Conti leaks: The Panama Papers of ransomware

Conti 2022-03-08 · Yoroi · Carmelo Ragusa, Luca Mella, Luigi Martire

Conti Ransomware source code: a well-designed COTS ransomware

Conti 2022-03-08 · · MBSD · MBSD

ContiLeaks

Conti 2022-03-07 · CyberScoop · Suzanne Smalley

Ransomware gang Conti has already bounced back from damage caused by chat leaks, experts say

Conti 2022-03-03 · Trend Micro · Trend Micro Research

IOC Resource for Russia-Ukraine Conflict-Related Cyberattacks

ClipBanker Conti HermeticWiper PartyTicket WhisperGate 2022-03-03 · Trend Micro · Trend Micro Research

Cyberattacks are Prominent in the Russia-Ukraine Conflict

BazarBackdoor Cobalt Strike Conti Emotet WhisperGate 2022-03-02 · CyberArk · CyberArk Labs

Conti Group Leaked!

TeamTNT Conti TrickBot 2022-03-02 · · elDiario · Carlos del Castillo

Cybercrime bosses warn that they will "fight back" if Russia is hacked

Conti Ryuk 2022-03-02 · Cluster25 · Cluster25

Conti's Source Code: Deep-Dive Into

Conti 2022-03-02 · Threatpost · Lisa Vaas

Conti Ransomware Decryptor, TrickBot Source Code Leaked

Conti TrickBot 2022-03-02 · KrebsOnSecurity · Brian Krebs

Conti Ransomware Group Diaries, Part II: The Office

Conti Emotet Ryuk TrickBot 2022-03-02 · Youtube (OALabs) · Sean Wilson, Sergei Frankoff

Botleggers Exposed - Analysis of The Conti Leaks Malware

Conti 2022-03-01 · Medium whickey000 · Wade Hickey

How I Cracked CONTI Ransomware Group’s Leaked Source Code ZIP File

Conti 2022-03-01 · Twitter (@TheDFIRReport) · The DFIR Report

Twitter thread with highlights from conti leaks

Conti 2022-03-01 · VX-Underground

Leaks: Conti / Trickbot

Conti TrickBot 2022-03-01 · Bleeping Computer · Lawrence Abrams

Conti Ransomware source code leaked by Ukrainian researcher

Conti 2022-03-01 · Arctic Wolf · Arctic Wolf

Conti Ransomware: An Analysis of Key Findings

Conti 2022-02-28 · Github (TheParmak) · TheParmak

conti-leaks-englished

Conti 2022-02-28 · Medium arnozobec · Arnaud Zobec

Analyzing conti-leaks without speaking russian — only methodology

Conti 2022-02-28 · Sophos · Sean Gallagher

Conti and Karma actors attack healthcare provider at same time through ProxyShell exploits

Conti Karma 2022-02-27 · The Record · Catalin Cimpanu

Conti ransomware gang chats leaked by pro-Ukraine member

Conti LockBit 2022-02-27 · Bleeping Computer · Lawrence Abrams

Conti ransomware's internal chats leaked after siding with Russia

Conti 2022-02-25 · · Red Hot Cyber · Red Hot Cyber

Il ransomware Conti si schiera a favore della Russia.

Conti 2022-02-23 · AdvIntel · Vitali Kremez, Yelisey Boguslavskiy

24 Hours From Log4Shell to Local Admin: Deep-Dive Into Conti Gang Attack on Fortune 500 (DFIR)

Cobalt Strike Conti 2022-02-23 · splunk · Shannon Davis, SURGe

An Empirically Comparative Analysis of Ransomware Binaries

Avaddon Babuk BlackMatter Conti DarkSide LockBit Maze Mespinoza REvil Ryuk 2022-02-22 · Bankinfo Security · Matthew J. Schwartz

Cybercrime Moves: Conti Ransomware Absorbs TrickBot Malware

Conti TrickBot 2022-02-22 · Sophos · Chester Wisniewski

Cyberthreats during Russian-Ukrainian tensions: what can we learn from history to be prepared?

Conti 2022-02-20 · Security Affairs · Pierluigi Paganini

The Conti ransomware group takes over TrickBot malware operation and plans to replace it with BazarBackdoor

malware.

Conti TrickBot 2022-02-18 · Bleeping Computer · Ionut Ilascu

Conti ransomware gang takes over TrickBot malware operation

Conti TrickBot 2022-02-14 · Cyware

Ransomware Becomes Deadlier, Conti Makes the Most Money

Conti 2022-02-09 · Dragos · Anna Skelton

Dragos ICS/OT Ransomware Analysis: Q4 2021

LockBit Conti LockBit 2022-02-04 · Bleeping Computer · Sergiu Gatlan

HHS: Conti ransomware encrypted 80% of Ireland's HSE IT systems

Conti 2022-01-27 · BleepingComputer · Sergiu Gatlan

Taiwanese Apple and Tesla contractor hit by Conti ransomware

Conti 2022-01-27 · CoveWare

Ransomware as a Service Innovation Curve

Conti LockBit 2022-01-24 · CyCraft · CyCraft AI

The Road to Ransomware Resilience, Part 2: Behavior Analysis

Conti Prometheus WastedLocker 2022-01-01 · Silent Push · Silent Push

Consequences- The Conti Leaks and future problems

Cobalt Strike Conti 2022-01-01 · Symposium on Electronic Crime Research · Benjamin Brown, Damon McCoy, Ian W. Gray, Jack Cable, Vlad Cuiujuclu

Money Over Morals: A Business Analysis of Conti Ransomware

Conti Conti 2021-12-23 · Symantec · Siddhesh Chandrayan

Log4j Vulnerabilities: Attack Insights

Tsunami Conti Dridex Khonsari Orcus RAT TellYouThePass 2021-12-17 · Advanced Intelligence · Vitali Kremez, Yelisey Boguslavskiy

Ransomware Advisory: Log4Shell Exploitation for Initial Access & Lateral Movement

Conti 2021-12-13 · The DFIR Report · The DFIR Report

Diavol Ransomware

BazarBackdoor Conti Diavol 2021-12-08 · Darktrace · Justin Fier

The double extortion business: Conti Ransomware Gang finds new avenues of negotiation

Conti 2021-12-03 · HSE · HSE

Conti cyber attack on the HSE

Conti 2021-12-01 · Trend Micro · Trend Micro

Ransomware Spotlight: Conti

Conti 2021-11-29 · The DFIR Report · The DFIR Report

CONTInuing the Bazar Ransomware Story

BazarBackdoor Cobalt Strike Conti 2021-11-18 · Elliptic · Elliptic Intel

Conti Ransomware Nets at Least $25.5 Million in Four Months

Conti 2021-11-18 · PRODAFT Threat Intelligence · PRODAFT

Conti Ransomware Group In-Depth Analysis

Conti 2021-11-18 · Red Canary · The Red Canary Team

Intelligence Insights: November 2021

Andromeda Conti LockBit QakBot Squirrelwaffle 2021-11-18 · Qualys · Ghanshyam More

Conti Ransomware

Conti 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 2021-11-15 · TRUESEC · Fabio Viggiani

ProxyShell, QBot, and Conti Ransomware Combined in a Series of Cyberattacks

Cobalt Strike Conti QakBot 2021-11-10 · AT&T · Josh Gomez

Stories from the SOC - Powershell, Proxyshell, Conti TTPs OH MY!

Cobalt Strike Conti 2021-11-09 · Cybereason · Aleksandar Milenkoski, Eli Salem

THREAT ANALYSIS REPORT: From Shatak Emails to the Conti Ransomware

Cobalt Strike Conti 2021-11-07 · Marco Ramilli's Blog · Marco Ramilli

CONTI Ransomware: Cheat Sheet

Conti 2021-11-02 · Intel 471 · Intel 471

Cybercrime underground flush with shipping companies’ credentials

Cobalt Strike Conti 2021-11-02 · unh4ck · Cyb3rSn0rlax

Detecting CONTI CobaltStrike Lateral Movement Techniques - Part 2

Cobalt Strike Conti 2021-10-26 · unh4ck · Hamza OUADIA

Detecting CONTI CobaltStrike Lateral Movement Techniques - Part 1

Cobalt Strike Conti 2021-10-25 · KrebsOnSecurity · Brian Krebs

Conti Ransom Gang Starts Selling Access to Victims

Conti 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 2021-10-05 · Trend Micro · Byron Gelera, Fyodor Yarochkin, Janus Agcaoili, Nikko Tamana

Ransomware as a Service: Enabler of Widespread Attacks

Cerber Conti DarkSide Gandcrab Locky Nefilim REvil Ryuk 2021-10-04 · The DFIR Report · The DFIR Report

BazarLoader and the Conti Leaks

BazarBackdoor Cobalt Strike Conti 2021-09-29 · Advanced Intelligence · Vitali Kremez, Yelisey Boguslavskiy

Backup “Removal” Solutions - From Conti Ransomware With Love

Cobalt Strike Conti 2021-09-22 · CISA · US-CERT

Alert (AA21-265A) Conti Ransomware

Cobalt Strike Conti 2021-09-14 · CrowdStrike · CrowdStrike Intelligence Team

Big Game Hunting TTPs Continue to Shift After DarkSide Pipeline Attack

BlackMatter DarkSide REvil Avaddon BlackMatter Clop Conti CryptoLocker DarkSide DoppelPaymer Hades REvil 2021-09-13 · The DFIR Report · The DFIR Report

BazarLoader to Conti Ransomware in 32 Hours

BazarBackdoor Cobalt Strike Conti 2021-09-03 · Sophos · Anand Ajjan, Andrew Ludgate, Gabor Szappanos, Peter Mackenzie, Sean Gallagher, Sergio Bestulic, Syed Zaidi

Conti affiliates use ProxyShell Exchange exploit in ransomware attacks

Cobalt Strike Conti 2021-09-02 · Talos · Azim Khodjibaev, Caitlin Huey, David Liebenberg, Dmytro Korzhevin

Translated: Talos' insights from the recently leaked Conti ransomware playbook

Conti 2021-08-19 · Sekoia · sekoia

An insider insights into Conti operations – Part two

Cobalt Strike Conti 2021-08-17 · Advanced Intelligence · Vitali Kremez, Yelisey Boguslavskiy

Hunting for Corporate Insurance Policies: Indicators of [Ransom] Exfiltration

Cobalt Strike Conti 2021-08-17 · Sekoia · sekoia

An insider insights into Conti operations – Part one

Cobalt Strike Conti 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 2021-08-11 · Advanced Intelligence · Vitali Kremez

Secret "Backdoor" Behind Conti Ransomware Operation: Introducing Atera Agent

Cobalt Strike Conti 2021-08-10 · Youtube (OALabs) · OALabs

Leaked Conti Ransomware Playbook - Red Team Reacts

Conti 2021-08-10 · LIFARS · Vlad Pasca

A Detailed Analysis of The Last Version of Conti Ransomware

Conti 2021-08-06 · Threat Post · Elizabeth Montalbano

Angry Affiliate Leaks Conti Ransomware Gang Playbook

Conti 2021-08-06 · Sophos Naked Security · Paul Ducklin

Conti ransomware affiliate goes rogue, leaks “gang data”

Conti 2021-08-05 · Bleeping Computer · Lawrence Abrams

Angry Conti ransomware affiliate leaks gang's attack playbook

Conti 2021-08-05 · The Record · Catalin Cimpanu

Disgruntled ransomware affiliate leaks the Conti gang’s technical manuals

Conti 2021-08-05 · Twitter (@AltShiftPrtScn) · Peter Mackenzie

Tweet on Conti ransomware affiliates using AnyDesk, Atera, Splashtop, Remote Utilities and ScreenConnect to maintain network access

Conti 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 2021-08-01 · The DFIR Report · The DFIR Report

BazarCall to Conti Ransomware via Trickbot and Cobalt Strike

BazarBackdoor Cobalt Strike Conti TrickBot 2021-07-21 · Twitter (@AltShiftPrtScn) · Peter Mackenzie

Tweet on Conti ransomware actor installing AnyDesk for remote access in victim environment

Conti 2021-07-08 · SentinelOne · Antonio Pirozzi, Idan Weizman

Conti Unpacked: Understanding Ransomware Development as a Response to Detection - A Detailed Technical Analysis

Conti 2021-07-01 · DomainTools · Chad Anderson

The Most Prolific Ransomware Families: A Defenders Guide

REvil Conti Egregor Maze REvil 2021-07-01 · Fortinet · Asaf Rubinfeld, Dor Neemani

Diavol - A New Ransomware Used By Wizard Spider?

Conti Diavol 2021-06-30 · Cynet · Max Malyutin

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

Conti IcedID 2021-06-18 · Palo Alto Networks Unit 42 · Richard Hickman

Conti Ransomware Gang: An Overview

Conti 2021-06-15 · Trend Micro · Byron Gelera, Earle Earnshaw, Janus Agcaoili, Miguel Ang, Nikko Tamana

Ransomware Double Extortion and Beyond: REvil, Clop, and Conti

Clop Conti REvil 2021-06-02 · CrowdStrike · Heather Smith, Josh Dalman

Under Attack: Protecting Against Conti, DarkSide, REvil and Other Ransomware

DarkSide Conti DarkSide REvil 2021-05-20 · FBI · FBI

Alert Number CP-000147-MW: Conti Ransomware Attacks Impact Healthcare and First Responder Networks

Conti 2021-05-16 · NCSC Ireland · NCSC Ireland

Ransomware Attack on Health Sector - UPDATE 2021-05-16

Cobalt Strike Conti 2021-05-12 · The DFIR Report

Conti Ransomware

Cobalt Strike Conti IcedID 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 2021-05-06 · 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 2021-04-29 · The Institute for Security and Technology · The Institute for Security and Technology

Combating Ransomware A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force

Conti EternalPetya 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 2021-04-25 · Vulnerability.ch Blog · Corsin Camichel

Ransomware and Data Leak Site Publication Time Analysis

Avaddon Babuk Clop Conti DarkSide DoppelPaymer Mespinoza Nefilim REvil 2021-04-13 · · MBSD · Kei Sugawara, Takashi Yoshikawa

Unraveling the internal structure of the Conti Ransomware

Conti 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 2021-03-01 · 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 Chinoxy 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 Winnti ZeroCleare APT10 APT23 APT27 APT31 APT41 BlackTech BRONZE EDGEWOOD Inception Framework MUSTANG PANDA Red Charon Red Nue Sea Turtle Tonto Team 2021-02-25 · ANSSI · CERT-FR

Ryuk Ransomware

BazarBackdoor Buer Conti Emotet Ryuk TrickBot 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 2021-02-16 · SophosLabs Uncut · Michael Heller

A Conti ransomware attack day-by-day

Conti 2021-02-16 · SophosLabs Uncut · Anand Ajjan, Andrew Brandt

Conti ransomware: Evasive by nature

Conti 2021-02-16 · SophosLabs Uncut · Peter Mackenzie, Tilly Travers

What to expect when you’ve been hit with Conti ransomware

Conti 2021-02-11 · CTI LEAGUE · CTI LEAGUE

CTIL Darknet Report – 2021

Conti Mailto Maze REvil Ryuk 2021-02-04 · ClearSky · ClearSky Research Team

CONTI Modus Operandi and Bitcoin Tracking

Conti Ryuk 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 2021-01-17 · Twitter (@AltShiftPrtScn) · Peter Mackenzie

Tweet on Conti Ransomware group exploiting FortiGate VPNs to drop in CobaltStrike loaders

Cobalt Strike Conti 2021-01-12 · Cybereason · Lior Rochberger

Cybereason vs. Conti Ransomware

BazarBackdoor Conti 2020-12-15 · Medium 0xthreatintel · 0xthreatintel

Reversing Conti Ransomware

Conti 2020-12-15 · Chuongdong blog · Chuong Dong

Conti Ransomware v2

Conti 2020-12-12 · Github (cdong1012) · Chuong Dong

ContiUnpacker: An automatic unpacker for Conti rasnomware

Conti 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 2020-10-23 · Hornetsecurity · Hornetsecurity Security Lab

Leakware-Ransomware-Hybrid Attacks

Avaddon Clop Conti DarkSide DoppelPaymer Mailto Maze Mespinoza Nefilim RagnarLocker REvil Sekhmet SunCrypt 2020-10-16 · CrowdStrike · The Crowdstrike Intel Team

WIZARD SPIDER Update: Resilient, Reactive and Resolute

BazarBackdoor Conti Ryuk TrickBot 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 · PWC UK · Andy Auld

What's behind the increase in ransomware attacks this year?

DarkSide Avaddon Clop Conti DoppelPaymer Dridex Emotet FriedEx Mailto PwndLocker QakBot REvil Ryuk SMAUG SunCrypt TrickBot WastedLocker 2020-08-25 · BleepingComputer · Lawrence Abrams

Ryuk successor Conti Ransomware releases data leak site

Conti 2020-08-18 · Arete · Arete Incident Response

Is Conti the New Ryuk?

Conti Ryuk 2020-07-08 · VMWare Carbon Black · Brian Baskin

TAU Threat Discovery: Conti Ransomware

Conti

- ▶ [TLP:WHITE] win_conti_auto (20251219 | Detects win.conti.)
- ▶ [TLP:WHITE] win_conti_w0 (20220318 | Detect the Conti ransomware (x64))
