Clop (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:11:34 UTC

Clop is a ransomware which uses the .clop extension after having encrypted the victim's files. Another unique characteristic belonging with Clop is in the string: "Dont Worry C|0P" included into the ransom notes. It is a variant of CryptoMix ransomware, but it additionally attempts to disable Windows Defender and to remove the Microsoft Security Essentials in order to avoid user space detection.

2025-07-31 · Intrinsec ·
Shadow syndicate infrastructure illumination
AMOS BlackCat Cactus Cicada3301 Clop LockBit PLAY RansomHub Royal Ransom Silence 2024-05-01 · Natto Thoughts · Natto Team
Ransom-War: Russian Extortion Operations as Hybrid Warfare, Part One
Clop Conti Maze TrickBot 2023-07-26 · Talos · Nicole Hoffman
Incident Response trends Q2 2023: Data theft extortion rises, while healthcare is still most-targeted vertical
BianLian Clop LockBit Royal Ransom LockBit 8Base BianLian Clop LockBit Money Message Royal Ransom 2023-06-23 · Fourcore · Jones Martin
Clop Ransomware: History, Timeline, And Adversary Simulation
Clop 2023-05-23 · loginsoft · Saharsh Agrawal
Taming the Storm: Understanding and Mitigating the Consequences of CVE-2023-27350
Clop LockBit Silence 2022-12-08 · Cisco Talos · Tiago Pereira
Breaking the silence - Recent Truebot activity
Clop Cobalt Strike FlawedGrace Raspberry Robin Silence Teleport 2022-10-27 · Microsoft · Microsoft Threat Intelligence
Raspberry Robin worm part of larger ecosystem facilitating pre-ransomware activity
FAKEUPDATES BumbleBee Clop Fauppod Raspberry Robin Roshtyak Silence DEV-0950 Mustard Tempest 2022-10-27 · Bleeping Computer · Sergiu Gatlan
Microsoft links Raspberry Robin worm to Clop ransomware attacks
Clop Raspberry Robin 2022-09-06 · PRODAFT · PRODAFT
TA505 Group’s TeslaGun In-Depth Analysis
Clop ServHelper 2022-07-26 · Mandiant · Daniel Kapellmann Zafra, Jay Christiansen, Keith Lunden, Ken Proska, Thibault van Geluwe de Berlaere
Mandiant Red Team Emulates FIN11 Tactics To Control Operational Technology Servers
Clop Industroyer MimiKatz Triton 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
Conti Hive BlackByte BlackCat Clop LockBit Mespinoza Ragnarok 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 2022-05-28 · Bleeping Computer · Sergiu Gatlan

Clop ransomware gang is back, hits 21 victims in a single month

Clop 2022-02-22 · Trend Micro · Trend Micro Research

Ransomware Spotlight: Clop

Clop 2021-11-16 · Trend Micro · Trend Micro

Global Operations Lead to Arrests of Alleged Members of GandCrab/REvil and Cl0p Cartels

REvil Clop Gandcrab REvil 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 2021-08-15 · 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 2021-06-30 · Advanced Intelligence · AdvIntel Security & Development Team, Brandon Rudisel, Yelisey Boguslavskiy

Ransomware-&-CVE: Industry Insights Into Exclusive High-Value Target Adversarial Datasets

BlackKingdom Ransomware Clop dearcry Hades REvil 2021-06-25 · KrCert · Dongwook Kim, Kayoung Kim, Seulgi Lee, Taewoo Lee

Attack patterns in AD environment

Clop 2021-06-24 · Binance · Binance

Binance Helps Take Down Cybercriminal Ring Laundering $500M in Ransomware Attacks

Clop 2021-06-16 · KrebsOnSecurity · Brian Krebs

Ukrainian Police Nab Six Tied to CLOP Ransomware

Clop 2021-06-16 · · Національної поліції України · Національна поліція України

Cyberpolice exposes hacker group in spreading encryption virus and causing half a billion dollars in damage to foreign companies

Clop Cobalt Strike FlawedAmmyy 2021-06-16 · · Youtube (Національна поліція України) · Національна поліція України

Кіберполіція викрила хакерське угруповання у розповсюдженні вірусу-шифрувальника (Clop operators)

Clop 2021-06-16 · The Record · Catalin Cimpanu

Ukrainian police arrest Clop ransomware members, seize server infrastructure

Clop 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 2021-05-10 · 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 2021-05-03 · splunk · Splunk Threat Research Team

Clop Ransomware Detection: Threat Research Release, April 2021

Clop 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 2021-04-14 · Vice · Lorenzo Franceschi-Bicchierai

Meet The Ransomware Gang Behind One of the Biggest Supply Chain Hacks Ever

Clop 2021-04-13 · splunk · Splunk Threat Research Team

Detecting Clop Ransomware

Clop 2021-04-13 · Palo Alto Networks Unit 42 · Doel Santos

Threat Assessment: Clop Ransomware

Clop 2021-03-26 · Bleeping Computer · Lawrence Abrams

Ransomware gang urges victims' customers to demand a ransom payment

Clop 2021-03-11 · Flashpoint · Flashpoint

CL0P and REvil Escalate Their Ransomware Tactics

Clop REvil 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 2021-02-23 · 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 2021-02-22 · FireEye · Andrew Moore, Genevieve Stark, Isif Ibrahima, Kimberly Goody, Van Ta

Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion

DEWMODE Clop 2021-02-15 · Medium s2wlab · Sojun Ryu

Operation SyncTrek

AbaddonPOS Azorult Clop DoppelDridex DoppelPaymer Dridex PwndLocker 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 2021-01-05 · AhnLab · AhnLab ASEC Analysis Team

[Threat Analysis] CLOP Ransomware that Attacked Korean Distribution Giant

Clop 2020-12-15 · Twitter (@darb0ng) · Minhee Lee

Tweet on Symrise group hit by Clop Ransomware

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

Ransomware gang says they stole 2 million credit cards from E-Land

Clop 2020-12-02 · · AhnLab · AhnLab ASEC Analysis Team

CLOP Ransomware Report

Clop 2020-11-23 · S2W LAB Inc. · TALON

[S2W LAB] Analysis of Clop Ransomware suspiciously related to the Recent Incident

Clop 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 2020-11-16 · Fox-IT · Anne Postma, Antonis Terefos, Tera0017

TA505: A Brief History Of Their Time

Clop Get2 SDBbot TA505 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 2020-10-20 · · Bundesamt für Sicherheit in der Informationstechnik · BSI

Die Lage der IT-Sicherheit in Deutschland 2020

Clop Emotet REvil Ryuk TrickBot 2020-10-08 · ZDNet · Catalin Cimpanu

German tech giant Software AG down after ransomware attack

Clop 2020-10-06 · Telekom · Thomas Barabosch

Eager Beaver: A Short Overview of the Restless Threat Actor TA505

Clop Get2 SDBbot TA505 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 · 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 2020-08-20 · CERT-FR · CERT-FR

Development of the Activity of the TA505 Cybercriminal Group

AndroMut Bart Clop Dridex FlawedAmmyy FlawedGrace Get2 Locky Marap QuantLoader SDBbot ServHelper tRat TrickBot 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 2020-07-07 · Hornetsecurity · Hornetsecurity Security Lab

Clop, Clop! It’s a TA505 HTML malspam analysis

Clop Get2 2020-06-22 · · CERT-FR · CERT-FR

Évolution De Lactivité du Groupe Cybercriminel TA505

Amadey AndroMut Bart Clop Dridex FlawedGrace Gandcrab Get2 GlobeImposter Jaff Locky Marap Philadephia Ransom QuantLoader Scarab Ransomware SDBbot ServHelper Silence tRat TrickBot 2020-06-22 · BleepingComputer · Lawrence Abrams

Indiabulls Group hit by CLOP Ransomware, gets 24h leak deadline

Clop 2020-06-16 · Telekom · Thomas Barabosch

TA505 returns with a new bag of tricks

Clop Get2 SDBbot TA505 2020-03-26 · Telekom · Thomas Barabosch

TA505's Box of Chocolate - On Hidden Gems packed with the TA505 Packer

Amadey Azorult Clop FlawedGrace Get2 SDBbot Silence TinyMet TA505 2020-03-24 · Bleeping Computer · Lawrence Abrams

Three More Ransomware Families Create Sites to Leak Stolen Data

Clop DoppelPaymer Maze Nefilim Nemty REvil 2020-03-04 · 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 2020-03-04 · SentinelOne · Jason Reaves

Breaking TA505’s Crypter with an SMT Solver

Clop CryptoMix MINEBRIDGE 2020-02-28 · Financial Security Institute · Financial Security Institute

Profiling of TA505 Threat Group That Continues to Attack the Financial Sector

Amadey Clop FlawedAmmyy Rapid Ransom SDBbot TinyMet 2020-02-20 · ZDNet · Catalin Cimpanu

Croatia's largest petrol station chain impacted by cyber-attack

Clop 2020-02-07 · Bleeping Computer · Sergiu Gatlan

TA505 Hackers Behind Maastricht University Ransomware Attack

Clop 2020-01-29 · ANSSI · ANSSI

État de la menace rançongiciel

Clop Dharma FriedEx Gandcrab LockerGoga Maze MegaCortex REvil RobinHood Ryuk SamSam 2020-01-14 · Telekom · Thomas Barabosch

Inside of CL0P’s ransomware operation

Clop Get2 SDBbot 2020-01-13 · Github (Tera0017) · Tera0017

TAFOF Unpacker

Clop Get2 Silence 2020-01-07 · Github (albertzsigovits) · Albert Zsigovits

Clop ransomware Notes

Clop 2020-01-07 · Github (albertzsigovits) · Albert Zsigovits

Clop ransomware Notes

Clop 2020-01-01 · Secureworks · SecureWorks

GOLD TAHOE

Clop FlawedAmmyy FlawedGrace Get2 SDBbot ServHelper TA505 2019-11-22 · · CERT-FR · CERT-FR

RAPPORT MENACES ET INCIDENTS DU CERT-FR

Clop 2019-11-19 · · ACTU · Rédaction Normandie

Une rançon après la cyberattaque au CHU de Rouen ? Ce que réclament les pirates

Clop 2019-08-01 · McAfee · Alexandre Mundo, Marc Rivero López

Clop Ransomware

Clop 2019-03-28 · Carbon Black · CB TAU Threat Intelligence

CryptoMix Clop Ransomware Disables Startup Repair, Removes & Edits Shadow Volume Copies

Clop 2019-03-05 · Bleeping Computer · Lawrence Abrams

CryptoMix Clop Ransomware Says It's Targeting Networks, Not Computers

Clop 2019-02-02 · Medium Sebdraven · Sébastien Larinier

Unpacking Clop

Clop

▶ [TLP:WHITE] win_clop_auto (20251219 | Detects win.clop.)
