WastedLocker (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:17:33 UTC

WastedLocker is a ransomware detected to be in use since May 2020 by EvilCorp. The ransomware name is derived from the filename that it creates which includes an abbreviation of the victim's name and the string 'wasted'. WastedLocker is protected with a custom crypter, referred to as CryptOne by Fox-IT InTELL. On examination, this crypter turned out to be very basic and was used also by other malware families such as: Netwalker, Gozi ISFB v3, ZLoader and Smokeloader. The crypter mainly contains junk code to increase entropy of the sample and hide the actual code.

2022-07-31 · BushidoToken Blog ·
Space Invaders: Cyber Threats That Are Out Of This World
Poison Ivy Raindrop SUNBURST TEARDROP WastedLocker 2022-06-13 · Jorge Testa · Jorge Testa
Killing The Bear - Evil Corp
FAKEUPDATES Babuk Blister DoppelPaymer Dridex Entropy FriedEx Hades Macaw Phoenix Locker WastedLoader WastedLocker 2022-06-02 · Mandiant · Mandiant Intelligence
To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions
FAKEUPDATES Blister Cobalt Strike DoppelPaymer Dridex FriedEx Hades LockBit Macaw MimiKatz Phoenix Locker WastedLocker 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 2022-03-17 · 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 2022-03-16 · 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 2022-02-23 · Sentinel LABS · Antonio Pirozzi, Antonis Terefos, Idan Weizman
Sanctions Be Damned | From Dridex to Macaw, The Evolution of Evil Corp
Dridex WastedLocker 2022-02-01 · Sentinel LABS · Antonio Pirozzi, Antonis Terefos, Idan Weizman
Sanctions be Damned | From Dridex To Macaw, The Evolution of Evil Corp
Dridex FriedEx Hades Phoenix Locker WastedLocker 2022-01-25 · Seguranca Informatica · Pedro Tavares

WastedLocker malware analysis

WastedLocker 2022-01-24 · CyCraft · CyCraft AI

The Road to Ransomware Resilience, Part 2: Behavior Analysis

Conti Prometheus WastedLocker 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 2021-06-16 · 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 2021-06-06 · Bleeping Computer · Lawrence Abrams

New Evil Corp ransomware mimics PayloadBin gang to evade US sanctions

Babuk FriedEx PayloadBIN WastedLocker 2021-05-26 · DeepInstinct · Ron Ben Yizhak

A Deep Dive into Packing Software CryptOne

Cobalt Strike Dridex Emotet Gozi ISFB Mailto QakBot SmokeLoader WastedLocker Zloader 2021-05-20 · Github (microsoft) · Microsoft

Microsoft 365 Defender Hunting Queries for hunting multiple threat actors' TTPs and malwares

STRRAT OceanLotus BabyShark Elise Revenge RAT WastedLocker Zebrocy 2021-05-18 · Bitdefender · Aron Radu, Bogdan Botezatu, George Mihali, Mihai Neagu, Ștefan Trifescu

New WastedLoader Campaign Delivered Through RIG Exploit Kit

WastedLoader WastedLocker 2021-05-05 · TRUESEC · Mattias Wåhlén

Are The Notorious Cyber Criminals Evil Corp actually Russian Spies?

Cobalt Strike Hades WastedLocker 2021-03-25 · Bleeping Computer · Sergiu Gatlan

Evil Corp switches to Hades ransomware to evade sanctions

Hades WastedLocker 2021-03-25 · Bleeping Computer · Lawrence Abrams

Insurance giant CNA hit by new Phoenix CryptoLocker ransomware

WastedLocker 2021-03-24 · Cisco · Caitlin Huey, David Liebenberg

Quarterly Report: Incident Response trends from Winter 2020-21

Egregor REvil WastedLocker 2021-03-17 · CrowdStrike · Adam Podlosky, Brendon Feeley

INDRIK SPIDER Supersedes WastedLocker with Hades Ransomware to Circumvent OFAC Sanctions

FriedEx WastedLocker 2021-03-17 · Palo Alto Networks Unit 42 · Unit42

Ransomware Threat Report 2021

RansomEXX Dharma DoppelPaymer Gandcrab Mailto Maze Phobos RansomEXX REvil Ryuk WastedLocker 2021-02-28 · 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 2021-02-23 · 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 2021-01-01 · SecureWorks

Threat Profile: GOLD DRAKE

Cobalt Strike Dridex FriedEx Koadic MimiKatz WastedLocker Evil Corp 2020-12-21 · Cisco Talos · JON MUNSHAW

2020: The year in malware

WolfRAT Prometei Poet RAT Agent Tesla Astaroth Ave Maria CRAT Emotet Gozi IndigoDrop JhoneRAT Nanocore RAT NjRAT Oblique RAT SmokeLoader StrongPity WastedLocker Zloader 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 2020-09-25 · 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 2020-08-31 · Symantec · Threat Hunter Team

Sophisticated Groups and Cyber Criminals Set Sights on Lucrative Financial Sector

WastedLocker 2020-08-28 · McAfee · McAfee

MVISION Insights: Wastedlocker Ransomware

WastedLocker 2020-08-16 · · Hatena Blog · 谷川哲司

WastedLocker IoC collection

WastedLocker 2020-08-04 · SophosLabs Uncut · Anand Ajjan, Mark Loman

WastedLocker’s techniques point to a familiar heritage

WastedLocker 2020-07-31 · Kaspersky Labs · Fedor Sinitsyn

WastedLocker: technical analysis

WastedLocker 2020-07-30 · Palo Alto Networks Unit 42 · Adrian McCabe, Alex Hinchliffe, Doel Santos, Robert Falcone

Threat Assessment: WastedLocker Ransomware

WastedLocker 2020-07-28 · Securonix · Oleg Kolesnikov

Detecting WastedLocker Ransomware Using Security Analytics

WastedLocker 2020-07-24 · BleepingComputer · Sergiu Gatlan

Garmin outage caused by confirmed WastedLocker ransomware attack

WastedLocker 2020-07-23 · Sentinel LABS · Jim Walter

WastedLocker Ransomware: Abusing ADS and NTFS File Attributes

WastedLocker 2020-07-10 · Malwarebytes · Pieter Arntz

Threat spotlight: WastedLocker, customized ransomware

WastedLocker 2020-07-06 · Cisco Talos · Arnaud Zobec, Ben Baker, Edmund Brumaghin, JJ Cummings

WastedLocker Goes "Big-Game Hunting" in 2020

WastedLocker 2020-07-01 · Arete · Arete Incident Response

WastedLocker Ransomware Insights

WastedLocker 2020-06-26 · BBC · BBC News

Russian hacker group Evil Corp targets US workers at home

WastedLocker Evil Corp 2020-06-26 · Symantec · Critical Attack Discovery and Intelligence Team

WastedLocker: Symantec Identifies Wave of Attacks Against U.S. Organizations

donut_injector WastedLocker 2020-06-23 · NCC Group · Michael Sandee, Nikolaos Pantazopoulos, Stefano Antenucci

WastedLocker: A New Ransomware Variant Developed By The Evil Corp Group

Cobalt Strike ISFB WastedLocker 2020-05-31 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

WastedLoader or DridexLoader?

Dridex WastedLocker 2020-01-01 · Palo Alto Networks Unit 42 · Unit42

Wastedlocker-ransomware

WastedLocker

▶ [TLP:WHITE] win_wastedlocker_auto (20251219 | Detects win.wastedlocker.)
