BlackMatter (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:42:44 UTC

BlackMatter

VTCollection

According to PCrisk, BlackMatter is a piece of malicious software categorized as ransomware. It operates by encrypting data for the purpose of making ransom demands for the decryption tools. In other words, files affected by BlackMatter are rendered inaccessible, and victims are asked to pay - to recover access to their data.

During the encryption process, files are appended with an extension consisting of a random character string. For example, a file initially named "1.jpg" would appear as something similar to "1.jpg.k5RO9fVOl". After this process is complete, the ransomware changes the desktop wallpaper and created a ransom note - "[random_string].README.txt" (e.g., k5RO9fVOl.README.txt).

References

2025-03-13 · Forescout ·
New Ransomware Operator Exploits Fortinet Vulnerability Duo
BlackMatter LockBit Mora_001

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

2022-09-22 · Broadcom · Symantec Threat Hunter Team
Noberus Ransomware: Darkside and BlackMatter Successor Continues to Evolve its Tactics
BlackCat BlackMatter DarkSide

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

2022-07-25 · Trend Micro · Byron Gelera, Ieriz Nicolle Gonzalez, Ivan Nicole Chavez, Katherine Casona, Nathaniel Gregory Ragasa, Nathaniel Morales

LockBit Ransomware Group Augments Its Latest Variant, LockBit 3.0, With BlackMatter Capabilities
BlackMatter LockBit

2022-07-13 · · GLIMPS · GLIMPS
Lockbit 3.0
BlackMatter DarkSide LockBit

2022-05-09 · Microsoft Security · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center
Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself
Griffon BazarBackdoor BlackCat BlackMatter Blister Gozi LockBit Pandora Rook SystemBC 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

2022-04-27 · · ANSSI · ANSSI
LE GROUPE CYBERCRIMINEL FIN7
Bateleur BELLHOP Griffon SQLRat POWERSOURCE Andromeda BABYMETAL BlackCat BlackMatter BOOSTWRITE Carbanak Cobalt Strike DNSMessenger Dridex DRIFTPIN Gameover P2P MimiKatz Murofet Qadars Ranbyus SocksBot

2022-04-13 · Microsoft · Microsoft 365 Defender Threat Intelligence Team
Dismantling ZLoader: How malicious ads led to disabled security tools and ransomware
BlackMatter Cobalt Strike DarkSide Ryuk Zloader

2022-04-08 · The Hacker News · Ravie Lakshmanan
Researchers Connect BlackCat Ransomware with Past BlackMatter Malware Activity
BlackCat BlackMatter BlackCat BlackMatter

2022-03-24 · SentinelOne · Antonio Cocomazzi
Ransomware Encryption Internals: A Behavioral Characterization
Babuk Babuk BlackMatter

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

2022-03-22 · The Register · Jeff Burt
This is a BlackCat you don't want crossing your path
BlackCat BlackMatter

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 · Cisco · Caitlin Huey, Tiago Pereira

From BlackMatter to BlackCat: Analyzing two attacks from one affiliate

BlackCat BlackMatter BlackCat BlackMatter

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

2022-03-01 · VirusTotal · VirusTotal

VirusTotal's 2021 Malware Trends Report

Anubis AsyncRAT BlackMatter Cobalt Strike DanaBot Dridex Khonsari MimiKatz Mirai Nanocore RAT Orcus RAT

2022-02-23 · splunk · Shannon Davis, SURGe

An Empirically Comparative Analysis of Ransomware Binaries

Avaddon Babuk BlackMatter Conti DarkSide LockBit Maze Mespinoza REvil Ryuk

2022-01-19 · Blackberry · The BlackBerry Research & Intelligence Team

Kraken the Code on Prometheus

Prometheus Backdoor BlackMatter Cerber Cobalt Strike DCRat Ficker Stealer QakBot REvil Ryuk

2022-01-19 · Mandiant · Adrian Sanchez Hernandez, Ervin James Ocampo, Paul Tarter

One Source to Rule Them All: Chasing AVADDON Ransomware

BlackMatter Avaddon BlackMatter MedusaLocker SystemBC ThunderX

2021-12-10 · Medium s2wlab · S2W TALON

BlackCat: New Rust based ransomware borrowing BlackMatter’s configuration

BlackCat BlackMatter

2021-11-24 · Google · Google Cybersecurity Action Team, Google Threat Analysis Group

Threat Horizons Cloud Threat Intelligence November 2021. Issue 1

BlackMatter

2021-11-04 · CrowdStrike · Eric Loui, Josh Reynolds

CARBON SPIDER Embraces Big Game Hunting, Part 2

BlackMatter Griffon BlackMatter DarkSide HiddenTear JSSLoader

2021-11-03 · The Record · Catalin Cimpanu

BlackMatter ransomware says its shutting down due to pressure from local authorities

BlackMatter

2021-11-03 · Group-IB · Andrey Zhdanov
The Darker Things BlackMatter and their victims
BlackMatter DarkSide BlackMatter DarkSide

2021-11-03 · Bleeping Computer · Lawrence Abrams
BlackMatter ransomware moves victims to LockBit after shutdown
BlackMatter BlackMatter LockBit

2021-11-02 · Varonis · Dvir Sason
BlackMatter Ransomware: In-Depth Analysis & Recommendations
BlackMatter

2021-10-22 · Elliptic · Elliptic Intel
DarkSide bitcoins on the move following government cyberattack against REvil ransomware group
BlackMatter DarkSide BlackMatter DarkSide

2021-10-22 · The Record · Catalin Cimpanu
DarkSide ransomware gang moves some of its Bitcoin after REvil got hit by law enforcement
BlackMatter DarkSide BlackMatter DarkSide

2021-10-22 · Bleeping Computer · Ionut Ilascu
DarkSide ransomware rushes to cash out $7 million in Bitcoin
BlackMatter DarkSide BlackMatter DarkSide

2021-10-22 · Twitter (@GelosSnake) · Omri Segev Moyal
Tweet on List of wallets used by Darkside/Blackmatter Operator to split out the money
BlackMatter DarkSide BlackMatter DarkSide

2021-10-20 · Mandiant · Jacob Thompson
Hidden in Plain Sight: Identifying Cryptography in BLACKMATTER Ransomware
BlackMatter

2021-10-18 · CISA · US-CERT
Alert (AA21-291A): BlackMatter Ransomware
BlackMatter BlackMatter

2021-10-14 · YouTube (Uriel Kosayev) · Uriel Kosayev
DarkSide Ransomware Reverse Engineering
BlackMatter DarkSide BlackMatter DarkSide

2021-10-12 · CrowdStrike · CrowdStrike Intelligence Team
ECX: Big Game Hunting on the Rise Following a Notable Reduction in Activity
Babuk BlackMatter DarkSide REvil Avaddon Babuk BlackMatter DarkSide LockBit Mailto REvil

2021-09-23 · Blackberry · The BlackBerry Research & Intelligence Team
Threat Thursday: BlackMatter RaaS - Darker Than DarkSide?
BlackMatter DarkSide BlackMatter DarkSide

2021-09-22 · McAfee · Alexandre Mundo, Marc Elias
BlackMatter Ransomware Analysis; The Dark Side Returns
BlackMatter

2021-09-21 · Nozomi Networks · Nozomi Networks Labs
BlackMatter Ransomware Technical Analysis and Tools from Nozomi Networks Labs
BlackMatter

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

2021-09-10 · S2W LAB Inc. · S2W TALON
Groove x RAMP : The relation between Groove, Babuk, Payload.bin, RAMP, and BlackMatter
Babuk BlackMatter Babuk BlackMatter

2021-09-08 · McAfee · John Fokker, Max Kersten, Thibault Seret
How Groove Gang is Shaking up the Ransomware-as-a-Service Market to Empower Affiliates
Babuk BlackMatter Babuk BlackMatter CTB Locker

2021-09-08 · Medium s2wlab · S2W TALON
Groove’s thoughts on Blackmatter, Babuk, and cheese shortages in the Netherlands
Babuk BlackMatter Babuk BlackMatter

2021-09-08 · Ciper Tech Solutions · Cipher Tech ACCE Team
Rapidly Evolving BlackMatter Ransomware Tactics
BlackMatter

2021-09-06 · KELA · Victoria Kivilevich
The Ideal Ransomware Victim: What Attackers Are Looking For
BlackMatter Cryakl

2021-09-05 · Chuongdong blog · Chuong Dong
BlackMatter Ransomware v2.0
BlackMatter

2021-09-02 · US Department of Health and Human Services · Health Sector Cybersecurity Coordination Center (HC3)
Demystifying BlackMatter
BlackMatter BlackMatter DarkSide

2021-09-01 · Medium s2wlab · Chaewon Moon, Denise Dasom Kim, Jungyeon Lim, S2W LAB INTELLIGENCE TEAM, Sujin Lim, Yeonghyeon Jeong

BlackMatter x Babuk : Using the same web server for sharing leaked files
Babuk BlackMatter Babuk BlackMatter

2021-08-31 · Minerva Labs · Minerva Labs
BlackMatter - The New Star Of Ransomware
BlackMatter

2021-08-23 · Netskope · Gustavo Palazolo
Netskope Threat Coverage: BlackMatter
BlackMatter

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

2021-08-09 · Sophos · Mark Loman
BlackMatter ransomware emerges from the shadow of DarkSide
BlackMatter BlackMatter

2021-08-06 · Group-IB · Andrey Zhdanov
It's alive! The story behind the BlackMatter ransomware strain
BlackMatter DarkSide BlackMatter DarkSide

2021-08-05 · Tesorion · Gijs Rijnders
Analysis of the BlackMatter ransomware
BlackMatter

2021-08-04 · Jan Gruber
Understanding BlackMatter's API Hashing
BlackMatter

2021-08-04 · Recorded Future · Insikt Group®
Protect Against BlackMatter Ransomware Before It’s Offered
BlackMatter DarkSide

Yara Rules

▶ [TLP:WHITE] win_blackmatter_auto (20251219 | Detects win.blackmatter.)

Download all Yara Rules

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.blackmatter