BlackMatter (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 20:25:28 UTC

There is no description at this point.

2022-09-28 · vmware ·
ESXi-Targeting Ransomware: The Threats That Are After Your Virtual Machines (Part 1)
Avoslocker Babuk Black Basta BlackCat BlackMatter Conti DarkSide HelloKitty Hive LockBit Luna RansomEXX RedAlert Ransomware REvil 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 2022-04-08 · The Hacker News · Ravie Lakshmanan
Researchers Connect BlackCat Ransomware with Past BlackMatter Malware Activity
BlackCat BlackMatter BlackCat BlackMatter 2022-03-17 · Cisco · Caitlin Huey, Tiago Pereira
From BlackMatter to BlackCat: Analyzing two attacks from one affiliate
BlackCat BlackMatter BlackCat BlackMatter 2022-02-09 · vmware · VMWare
Exposing Malware in Linux-Based Multi-Cloud Environments
ACBackdoor BlackMatter DarkSide Erebus HelloKitty Kinsing PLEAD QNAPCrypt RansomEXX REvil Sysrv-hello TeamTNT Vermilion Strike Cobalt Strike 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 2021-11-18 · Cisco · Josh Pyorre
BlackMatter, LockBit, and THOR
BlackMatter LockBit PlugX 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 · 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 2021-10-22 · Bleeping Computer · Ionut Ilascu
DarkSide ransomware rushes to cash out $7 million in Bitcoin
BlackMatter DarkSide BlackMatter DarkSide 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 · Twitter (@GelosSnake) · Omri Segev Moyal

Tweet on List of wallets used by Darkside/Blackmatter Operator to split out the money

BlackMatter DarkSide BlackMatter DarkSide 2021-10-18 · 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 2021-09-14 · 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 2021-09-02 · 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 2021-08-15 · 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 · Twitter (@VK_intel) · Vitali Kremez

Tweet on Linux variant of BlackMatter

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

Linux version of BlackMatter ransomware targets VMware ESXi servers

BlackMatter

There is no Yara-Signature yet.
