Babuk (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 03:23:31 UTC

Babuk Ransomware is a sophisticated ransomware compiled for several platforms. Windows and ARM for Linux are the most used compiled versions, but ESX and a 32bit old PE executable were observed over time. as well It uses an Elliptic Curve Algorithm (Montgomery Algorithm) to build the encryption keys.

2024-11-22 · Medium (@lcam) · Luca Mella
How to target European SME with Ransomware? Through Zyxel!
HellDown Babuk 2024-01-09 · Avast Decoded · Threat Research Team
Avast Updates Babuk Ransomware Decryptor in Cooperation with Cisco Talos and Dutch Police
Babuk 2023-12-22 · PRODAFT · PRODAFT
Smoke and Mirrors: Understanding The Workings of Wazawaka
Conti Monti Babuk Hive LockBit RagnarLocker Trigona 2023-12-13 · cocomelonc · cocomelonc
Malware in the wild book
AsyncRAT Babuk BlackCat BlackLotus Carbanak HelloKitty Paradise Stealc WinDealer 2023-06-17 · Github (EmissarySpider) · EmissarySpider
ransomware-descendants
Babuk Conti LockBit 2023-06-15 · Github (cocomelonc) · cocomelonc
Malware analysis report: Babuk ransomware
Babuk 2023-05-16 · KrebsOnSecurity · Brian Krebs
Russian Hacker “Wazawaka” Indicted for Ransomware
Babuk Hive LockBit LockBit Babuk Hive LockBit 2022-12-07 · Morphisec · Morphisec Labs
New Babuk Ransomware Found in Major Attack
Babuk 2022-08-24 · Trend Micro · Hitomi Kimura, Ryan Soliven
Ransomware Actor Abuses Genshin Impact Anti-Cheat Driver to Kill Antivirus
Babuk 2022-08-24 · Trend Micro · Hitomi Kimura, Ryan Soliven
Ransomware Actor Abuses Genshin Impact Anti-Cheat Driver to Kill Antivirus (IoCs)
Babuk 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 2022-05-06 · cyble · Cyble Research Labs
Rebranded Babuk Ransomware In Action: DarkAngels Ransomware Performs Targeted Attack
Babuk 2022-04-20 · Bleeping Computer · Bill Toulas
Microsoft Exchange servers hacked to deploy Hive ransomware
Babuk BlackByte Conti Hive LockFile 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 2022-02-23 · splunk · Shannon Davis, SURGe

An Empirically Comparative Analysis of Ransomware Binaries

Avaddon Babuk BlackMatter Conti DarkSide LockBit Maze Mespinoza REvil Ryuk 2022-02-14 · KrebsOnSecurity · Brian Krebs

Wazawaka Goes Waka Waka

Babuk 2021-11-03 · Cisco Talos · Caitlin Huey, Chetan Raghuprasad, Vanja Svajcer

Microsoft Exchange vulnerabilities exploited once again for ransomware, this time with Babuk

Babuk CHINACHOPPER 2021-10-26 · Github (vc0RExor) · Aaron Jornet

Babuk Ransomware

Babuk 2021-10-18 · McAfee · Thibault Seret

Is There Really Such a Thing as a Low-Paid Ransomware Operator?

Babuk 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 2021-10-01 · ZeroFox · Stephan Simon

Babuk Ransomware Variant Delta Plus Used in Live Attacks After Source Code Leaked

Babuk 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 2021-09-09 · Advanced Intelligence · Anastasia Sentsova, Yelisey Boguslavskiy

Groove VS Babuk; Groove Ransom Manifesto & RAMP Underground Platform Secret Inner Workings

Babuk Babuk 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 · 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 2021-09-01 · 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 2021-08-05 · 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 2021-07-28 · KELA · Victoria Kivilevich

New Russian-Speaking Forum – A New Place for RaaS?

Babuk 2021-07-28 · McAfee · Noël Keijzer, Thibault Seret

Babuk: Moving to VM and *nix Systems Before Stepping Away

Babuk 2021-07-05 · Lab52 · Th3spis

Quick review of Babuk ransomware builder

Babuk 2021-07-04 · Marco Ramilli's Blog · Marco Ramilli

Babuk Ransomware: The Builder

Babuk Babuk 2021-07-01 · BleepingComputer · Ionut Ilascu

Babuk ransomware is back, uses new version on corporate networks

Babuk 2021-06-30 · BleepingComputer · Lawrence Abrams

Leaked Babuk Locker ransomware builder used in new attacks

Babuk 2021-06-27 · Twitter (@GossiTheDog) · Kevin Beaumont

Tweet on babuk ransomware builder

Babuk 2021-06-27 · The Record · Catalin Cimpanu

Builder for Babuk Locker ransomware leaked online

Babuk 2021-06-10 · McAfee · ATR Operational Intelligence Team

Are Virtual Machines the New Gold for Cyber Criminals?

Babuk DarkSide 2021-06-06 · Bleeping Computer · Lawrence Abrams

New Evil Corp ransomware mimics PayloadBin gang to evade US sanctions

Babuk FriedEx PayloadBIN WastedLocker 2021-06-03 · Medium s2wlab · Denise Dasom Kim, Hyunmin Suh, Jungyeon Lim, YH Jeong

W1 Jun | EN | Story of the week: Ransomware on the Darkweb

DarkSide Babuk DarkSide 2021-05-31 · DataBreaches.net · Dissent

Babuk re-organizes as Payload Bin, offers its first leak

Babuk HelloKitty 2021-05-25 · Medium s2wlab · Denise Dasom Kim, Hyunmin Suh, Jungyeon Lim

W4 May | EN | Story of the week: Ransomware on the Darkweb

Babuk REvil 2021-05-12 · Kaspersky · Dmitry Galov, Ivan Kwiatkowski, Leonid Bezvershenko

Ransomware world in 2021: who, how and why

Babuk 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 2021-05-07 · Bleeping Computer · Lawrence Abrams

Data leak marketplaces aim to take over the extortion economy

Babuk Maze 2021-04-29 · · Sekurak.pl · Sekurak

Udało nam się zrealizować wywiad z grupą ransomware (Babuk), która zaszyfrowała policję metropolitarną w Waszyngtonie

Babuk 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 2021-02-24 · McAfee · Alexandre Mundo, John Fokker, Thibault Seret, Thomas Roccia

Technical Analysis of Babuk Ransomware

Babuk 2021-02-08 · Medium Sebdraven · sebdraven

Babuk is distributed packed

Babuk 2021-02-05 · Trend Micro · Don Ovid Ladores, Junestherry Salvador, Llalum Victoria, Monte de Jesus, Nikko Tamana, Raphael Centeno

New in Ransomware: Seth-Locker, Babuk Locker, Maoloa, TeslaCrypt, and CobraLocker

Babuk TeslaCrypt 2021-02-02 · Bleeping Computer · Lawrence Abrams

Babyk Ransomware won't hit charities, unless they support LGBT, BLM

Babuk 2021-01-26 · Medium s2wlab · Hyunmin Suh

W4 Jan | EN | Story of the week: Ransomware on the Darkweb

Avaddon Babuk LockBit 2021-01-16 · Chuongdong blog · Chuong Dong

Babuk Ransomware v3

Babuk 2021-01-05 · Twitter (@Sebdraven) · Sébastien Larinier

Tweet on link between Babuk and Vasa locker

Babuk 2021-01-03 · Chuongdong blog · Chuong Dong

Babuk Ransomware

Babuk 2021-01-01 · Sogeti · Sogeti

Babuk ransomware

Babuk

▶ [TLP:WHITE] win_babuk_auto (20251219 | Detects win.babuk.)
