Nefilim (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:36:23 UTC

According to Vitali Kremez and Michael Gillespie, this ransomware shares much code with Nemty 2.5. A difference is removal of the RaaS component, which was switched to email communications for payments. Uses AES-128, which is then protected RSA2048.

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 2021-10-05 · Trend Micro · Byron Gelera, Fyodor Yarochkin, Janus Agcaoili, Nikko Tamana
Ransomware as a Service: Enabler of Widespread Attacks
Cerber Conti DarkSide Gandcrab Locky Nefilim REvil Ryuk 2021-07-14 · Intel 471 · Intel 471
How cybercriminals create turbulence for the transportation industry
Mount Locker Nefilim 2021-06-28 · Trend Micro · Trend Micro
Nefilim Ransomware Attack Through a MITRE Att&ck Lens
Nefilim 2021-06-08 · Trend Micro · David Sancho, Feike Hacquebord, Fernando Mercês, Ian Kenefick, Mayra Fuentes, Robert McArdle, Stephen Hilt, Vladimir Kropotov
Modern Ransomware’s Double Extortion Tactics and How to Protect Enterprises Against Them
Nefilim 2021-05-25 · Kaspersky · Fedor Sinitsyn, Yanis Zinchenko
Evolution of JSWorm ransomware
Nefilim Nemty 2021-05-12 · Qualys · Bajrang Mane
Nefilim Ransomware
Nefilim 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 2021-04-25 · Vulnerability.ch Blog · Corsin Camichel
Ransomware and Data Leak Site Publication Time Analysis
Avaddon Babuk Clop Conti DarkSide DoppelPaymer Mespinoza Nefilim REvil 2021-02-28 · 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 2021-02-25 · Intezer · Intezer

Year of the Gopher A 2020 Go Malware Round-Up

NiuB WellMail elf.wellmess ArdaMax AsyncRAT CyberGate DarkComet Glupteba Nanocore RAT Nefilim NjRAT Quasar RAT WellMess Zebrocy 2021-02-23 · Trend Micro · Byron Gelera, Janus Agcaoili

An Analysis of the Nefilim Ransomware

Nefilim 2021-01-26 · SophosLabs Uncut · Bill Kearney, David Anderson, Michael Heller, Peter Mackenzie, Sergio Bestulic

Nefilim Ransomware Attack Uses “Ghost” Credentials

Nefilim 2021-01-01 · Secureworks · SecureWorks

Threat Profile: GOLD MANSARD

Nefilim Nemty GOLD MANSARD 2020-12-28 · Bleeping Computer · Lawrence Abrams

Home appliance giant Whirlpool hit in Nefilim ransomware attack

Nefilim 2020-12-16 · Accenture · Paul Mansfield

Tracking and combatting an evolving danger: Ransomware extortion

DarkSide Egregor Maze Nefilim RagnarLocker REvil Ryuk SunCrypt 2020-12-10 · US-CERT · FBI, MS-ISAC, US-CERT

Alert (AA20-345A): Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data

PerlBot Shlayer Agent Tesla Cerber Dridex Ghost RAT Kovter Maze MedusaLocker Nanocore RAT Nefilim REvil Ryuk Zeus 2020-12-03 · PICUS Security · Süleyman Özarslan

How to Beat Nefilim Ransomware Attacks

Nefilim 2020-10-23 · Hornetsecurity · Hornetsecurity Security Lab

Leakware-Ransomware-Hybrid Attacks

Avaddon Clop Conti DarkSide DoppelPaymer Mailto Maze Mespinoza Nefilim RagnarLocker REvil Sekhmet SunCrypt 2020-08-25 · 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 2020-07-15 · 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 2020-06-16 · New Zealand CERT · New Zealand CERT

Active ransomware campaign leveraging remote access technologies

Nefilim 2020-05-04 · SentinelOne · Jim Walter

Meet NEMTY Successor, Nefilim/Nephilim Ransomware

Nefilim Nemty 2020-03-24 · Bleeping Computer · Lawrence Abrams

Three More Ransomware Families Create Sites to Leak Stolen Data

Clop DoppelPaymer Maze Nefilim Nemty REvil 2020-03-23 · Trend Micro · Trend Micro

Nefilim Ransomware Threatens to Expose Stolen Data

Nefilim 2020-03-17 · Bleeping Computer · Lawrence Abrams

New Nefilim Ransomware Threatens to Release Victims' Data

Nefilim 2020-03-14 · ID Ransomware · Andrew Ivanov

Nefilim Ransomware

Nefilim 2020-01-01 · Blackberry · Blackberry Research

State of Ransomware

Maze MedusaLocker Nefilim Phobos REvil Ryuk STOP

▶ [TLP:WHITE] win_nefilim_auto (20251219 | Detects win.nefilim.)
