REvil (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:41:51 UTC

REvil Beta
MD5: bed6fc04aeb785815744706239a1f243
SHA1: 3d0649b5f76dbbff9f86b926afbd18ae028946bf
SHA256: 3641b09bf6eae22579d4fd5aae420476a134f5948966944189a70afd8032cb45
* Privilege escalation via CVE-2018-8453 (64-bit only)
* Rerun with RunAs to elevate privileges
* Implements a requirement that if "exp" is set, privilege escalation must be successful for full execution to occur
* Implements target whitelisting using GetKetboardLayoutList
* Contains debug console logging functionality
* Defines the REvil registry root key as SOFTWARE\!test
* Includes two variable placeholders in the ransom note: UID & KEY
* Terminates processes specified in the "prc" configuration key prior to encryption
* Deletes shadow copies and disables recovery
* Wipes contents of folders specified in the "wfld" configuration key prior to encryption
* Encrypts all non-whitelisted files on fixed drives
* Encrypts all non-whitelisted files on network mapped drives if it is running with System-level privileges or can impersonate the security context of explorer.exe
* Partially implements a background image setting to display a basic "Image text" message
* Sends encrypted system data to a C2 domain via an HTTPS POST request (URI path building is not implemented.)

REvil 1.00
MD5: 65aa793c000762174b2f86077bdafaea
SHA1: 95a21e764ad0c98ea3d034d293aee5511e7c8457
SHA256: f0c60f62ef9ffc044d0b4aeb8cc26b971236f24a2611cb1be09ff4845c3841bc
* Adds 32-bit implementation of CVE-2018-8453 exploit
* Removes console debug logging
* Changes the REvil registry root key to SOFTWARE\recfg
* Removes the System/Impersonation success requirement for encrypting network mapped drives
* Adds a "wipe" key to the configuration for optional folder wiping
* Fully implements the background image setting and leverages values defined in the "img" configuration key
* Adds an EXT variable placeholder to the ransom note to support UID, KEY, and EXT
* Implements URI path building so encrypted system data is sent to a C2 pseudo-random URL
* Fixes the function that returns the victim's username so the correct value is placed in the stats JSON data
---

REvil 1.01

MD5: 2abff29b4d87f30f011874b6e98959e9

SHA1: 9d1b61b1cba411ee6d4664ba2561fa59cdb0732c

SHA256: a88e2857a2f3922b44247316642f08ba8665185297e3cd958bbd22a83f380feb

* Removes the exp/privilege escalation requirement for full execution and encrypts data regardless of privilege level

* Makes encryption of network mapped drives optional by adding the "-nolan" argument

---

REvil 1.02

MD5: 4af953b20f3a1f165e7cf31d6156c035

SHA1: b859de5ffcb90e4ca8e304d81a4f81e8785bb299

SHA256: 89d80016ff4c6600e8dd8cfad1fa6912af4d21c5457b4e9866d1796939b48dc4

* Enhances whitelisting validation by adding inspection of GetUserDefaultUILanguage and GetSystemDefaultUILanguage

* Partially implements "lock file" logic by generating a lock filename based on the first four bytes of the Base64-decoded pk key, appending a .lock file extension, and adding the filename to the list of whitelisted files in the REvil configuration (It does not appear that this value is referenced after it is created and stored in memory. There is no evidence that a lock file is dropped to disk.)

* Enhances folder whitelisting logic that take special considerations if the folder is associated with "program files" directories

* Hard-codes whitelisting of all direct content within the Program Files or Program Files x86 directories

* Hard-codes whitelisting of "sql" subfolders within program files

* Encrypts program files sub-folders that does not contain "sql" in the path

* Compares other folders to the list of whitelisted folders specified in the REvil configuration to determine if they are whitelisted

* Encodes stored strings used for URI building within the binary and decodes them in memory right before use

* Introduces a REvil registry root key "sub_key" registry value containing the attacker's public key

---

REvil 1.03

MD5: 3cae02306a95564b1fff4ea45a7dfc00

SHA1: 0ce2cae5287a64138d273007b34933362901783d

SHA256: 78fa32f179224c46ae81252c841e75ee4e80b57e6b026d0a05bb07d34ec37bbf

* Removes lock file logic that was partially implemented in 1.02

* Leverages WMI to continuously monitor for and kill newly launched processes whose names are listed in the prc configuration key (Previous versions performed this action once.)

* Encodes stored shellcode

* Adds the -path argument:

* Does not wipe folders (even if wipe == true)

* Does not set desktop background

* Does not contact the C2 server (even if net == true)

* Encrypts files in the specified folder and drops the ransom note

* Changes the REvil registry root key to SOFTWARE\QtProject\OrganizationDefaults

* Changes registry key values from --> to:
* sub_key --> pvg
* pk_key --> sxsP
* sk_key --> BDDC8
* 0_key --> f7gVD7
* rnd_ext --> Xu7Nnkd
* stat --> sMMnxpgk

REvil 1.04
MD5: 6e3efb83299d800edf1624ecbc0665e7
SHA1: 0bd22f204c5373f1a22d9a02c59f69f354a2cc0d
SHA256: 2ca64feaaf5ab6cf96677fbc2bc0e1995b3bc93472d7af884139aa757240e3f6
* Leverages PowerShell and WMI to delete shadow copies if the victim's operating system is newer than Windows XP (For Windows XP or older, it uses the original command that was executed in all previous REvil versions.)
* Removes the folder wipe capability
* Changes the REvil registry root key to SOFTWARE\GitForWindows
* Changes registry key values from --> to:
* pvg --> QPM
* sxsP --> cMtS
* BDDC8 --> WGg7j
* f7gVD7 --> zbhs8h
* Xu7Nnkd --> H85TP10
* sMMnxpgk --> GCZg2PXD

REvil v1.05
MD5: cfefcc2edc5c54c74b76e7d1d29e69b2
SHA1: 7423c57db390def08154b77e2b5e043d92d320c7
SHA256: e430479d1ca03a1bc5414e28f6cdbb301939c4c95547492cdbe27b0a123344ea
* Add new 'arn' configuration key that contains a boolean true/false value that controls whether or not to implement persistence.
* Implements persistence functionality via registry Run key. Data for value is set to the full path and filename of the currently running executable. The executable is never moved into any 'working directory' such as %AppData% or %TEMP% as part of the persistence setup. The Reg Value used is the hardcoded value of 'lNOWZyAWVv' :
* SOFTWARE\Microsoft\Windows\CurrentVersion\Run\lNOWZyAWVv
* Before exiting, REvil sets up its malicious executable to be deleted upon reboot by issuing a call to MoveFileExW and setting the destination to NULL and the flags to 4 (MOVEFILE_DELAY_UNTIL_REBOOT). This breaks persistence however as the target executable specified in the Run key will no longer exist once this is done.
* Changes registry key values from --> to:
* QPM --> tgE
* cMtS --> 8K09

* WGg7j --> xMtNc
* zbhs8h --> CTgE4a
* H85TP10 --> oE5bZg0
* GCZg2PXD --> DC408Qp4

REvil v1.06
MD5: 65ff37973426c09b9ff95f354e62959e
SHA1: b53bc09cfbd292af7b3609734a99d101bd24d77e
SHA256: 0e37d9d0a7441a98119eb1361a0605042c4db0e8369b54ba26e6ba08d9b62f1e
* Updated string decoding function to break existing yara rules. Likely the result of the blog posted by us.
* Modified handling of network file encryption. Now explicitly passes every possible "Scope" constant to the WNetOpenEnum function when looking for files to encrypt. It also changed the 'Resource Type" from RESOURCETYPE_DISK to RESOURCETYPE_ANY which will now include things like mapped printers.
* Persistence registry value changed from 'lNOWZyAWVv' to 'sNpEShi30R'
* Changes registry key values from --> to:
* tgE --> 73g
* 8K09 --> vTGj
* xMtNc --> Q7PZe
* CTgE4a --> BuCrIp
* oE5bZg0 --> lcZd7OY
* DC408Qp4 --> sLF86MWC

REvil v1.07
MD5: ea4cae3d6d8150215a4d90593a4c30f2
SHA1: 8dcbcbefaedf5675b170af3fd44db93ad864894e
SHA256: 6a2bd52a5d68a7250d1de481dcce91a32f54824c1c540f0a040d05f757220cd3
TBD

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 2023-04-18 · Mandiant · Mandiant
M-Trends 2023
QUIETEXIT AppleJeus Black Basta BlackCat CaddyWiper Cobalt Strike Dharma HermeticWiper Hive INDUSTROYER2 Ladon LockBit Meterpreter PartyTicket PlugX QakBot REvil Royal Ransom SystemBC WhisperGate 2023-02-02 · cocomelonc · cocomelonc
Malware analysis: part 7. Yara rule example for CRC32. CRC32 in REvil ransomware
REvil 2023-01-30 · Checkpoint · Arie Olshtein
Following the Scent of TrickGate: 6-Year-Old Packer Used to Deploy the Most Wanted Malware
Agent Tesla Azorult Buer Cerber Cobalt Strike Emotet Formbook HawkEye Keylogger Loki Password Stealer (PWS) Maze NetWire RC Remcos REvil TrickBot 2022-08-22 · Microsoft · Microsoft
Extortion Economics - Ransomware’s new business model
BlackCat Conti Hive REvil AgendaCrypt Black Basta BlackCat Brute Ratel C4 Cobalt Strike Conti Hive Mount

Locker Nokoyawa Ransomware REvil Ryuk 2022-07-27 · Trend Micro · Buddy Tancio, Jed Valderama

Gootkit Loader’s Updated Tactics and Fileless Delivery of Cobalt Strike

Cobalt Strike GootKit Kronos REvil SunCrypt 2022-06-13 · SecurityScorecard · Vlad Pasca

A Detailed Analysis Of The Last Version Of REvil Ransomware (Download PDF)

REvil 2022-05-09 · Secureworks · Counter Threat Unit ResearchTeam

REvil Development Adds Confidence About GOLD SOUTHFIELD Reemergence

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 2022-05-01 · Bleeping Computer · Lawrence Abrams

REvil ransomware returns: New malware sample confirms gang is back

REvil 2022-05-01 · Github (k-vitali) · Vitali Kremez

REvil Reborn Ransom Config

REvil 2022-04-20 · Bleeping Computer · Ionut Ilascu

REvil's TOR sites come alive to redirect to new ransomware operation

REvil 2022-04-12 · ConnectWise · ConnectWise CRU

Threat Profile: REvil

REvil 2022-04-04 · Bankinfo Security · Jeremy Kirk

The Ransomware Files, Episode 6: Kaseya and REvil

REvil 2022-03-24 · United States Senate · U.S. Senate Committee on Homeland Security & Governmental Affairs

America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies

REvil 2022-03-24 · United States Senate · U.S. Senate Committee on Homeland Security & Governmental Affairs

New Portman Report Demonstrates Threat Ransomware Presents to the United States

REvil 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 2022-03-17 · 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 · Trend Micro · Trend Micro Research

Navigating New Frontiers Trend Micro 2021 Annual Cybersecurity Report

REvil BazarBackdoor Buer IcedID QakBot REvil 2022-03-16 · Red Canary · Brian Donohue, Laura Brosnan

Uncompromised: When REvil comes knocking

REvil 2022-03-09 · Department of Justice · Office of Public Affairs

Sodinokibi/REvil Ransomware Defendant Extradited to United States and Arraigned in Texas

REvil 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 · Darktrace · Oakley Cox

Staying ahead of REvil's Ransomware-as-a-Service business model

REvil REvil 2022-01-27 · ANALYST1 · Jon DiMaggio

A History of Revil

REvil REvil 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 2022-01-14 · Advanced Intelligence · Yelisey Boguslavskiy

Storm in "Safe Haven": Takeaways from Russian Authorities Takedown of REvil

REvil REvil 2022-01-14 · FSB · FSB

Unlawful Activities of Members of an Organized Criminal Community were suppressed

REvil REvil 2021-12-20 · Trend Micro · Trend Micro Research

Ransomware Spotlight: REvil

REvil REvil 2021-11-17 · BBC · Joe Tidy

Evil Corp: 'My hunt for the world's most wanted hackers'

REvil REvil 2021-11-16 · Trend Micro · Trend Micro

Global Operations Lead to Arrests of Alleged Members of GandCrab/REvil and Cl0p Cartels

REvil Clop Gandcrab REvil 2021-11-16 · IronNet · IronNet Threat Research, Joey Fitzpatrick, Morgan Demboski, Peter Rydzynski

How IronNet's Behavioral Analytics Detect REvil and Conti Ransomware

Cobalt Strike Conti IcedID REvil 2021-11-10 · Blackberry · Codi Starks, Ryan Chapman

REvil Under the Microscope

GootKit REvil 2021-11-10 · · RT on the Russian · Aleksey Polyakov, Alena Goinskaya, Ekaterina Suslova, Elizaveta Koroleva

"He does not get in touch": what is known about Barnaul, wanted by the FBI on charges of cybercrime

REvil REvil 2021-11-08 · Europol · Europol

Five Affiliates to Sodinokibi/REvil Unplugged

REvil 2021-11-08 · · DIICOT (Romanian Directorate for Investigating Organized Crime and Terrorism) · DIICOT (Romanian Directorate for Investigating Organized Crime and Terrorism)

Press release 2 08.11.2021

REvil REvil 2021-11-08 · U.S. Department of the Treasury · U.S. Department of the Treasury

Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange (Yaroslav Vasinskyi & Yevgeniy Polyanin)

REvil REvil 2021-11-08 · U.S. Department of the Treasury · U.S. Department of the Treasury

Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

REvil REvil 2021-11-08 · Department of Justice · Department of Justice

Indictment of Yevgeniy Polyanin, one off the REvil affliates

REvil REvil 2021-11-08 · Department of Justice · Department of Justice

Ukrainian Arrested and Charged with Ransomware Attack on Kaseya

REvil REvil 2021-11-08 · FBI · FBI

WANTED poster for Yevhgyeniy Polyanin (REvil affiliate)

REvil REvil 2021-11-08 · The Record · Catalin Cimpanu

US arrests and charges Ukrainian man for Kaseya ransomware attack

REvil REvil 2021-11-08 · KrebsOnSecurity · Brian Krebs

REvil Ransom Arrest, $6M Seizure, and $10M Reward

REvil REvil 2021-11-08 · Department of Justice · Department of Justice

Indictment of Yaroslav Vasinskyi (REvil affiliate)

REvil REvil 2021-11-03 · CERT-FR · ANSSI

Identification of a new cybercriminal group: Lockean

DoppelPaymer Egregor Maze PwndLocker REvil 2021-10-28 · · BR.DE · Hakan Tanriverdi, Maximilian Zierer

Mutmaßlicher Ransomware-Millionär identifiziert

REvil REvil 2021-10-26 · ANSSI

Identification of a new cyber criminal group: Lockean

Cobalt Strike DoppelPaymer Egregor Maze PwndLocker QakBot REvil 2021-10-25 · KELA · Victoria Kivilevich

Will the REvil Story Finally be Over?

REvil REvil 2021-10-22 · Reuters · Christopher Bing, Joseph Menn

EXCLUSIVE Governments turn tables on ransomware gang REvil by pushing it offline

REvil REvil 2021-10-22 · Darkowl · Darkowl

“Page Not Found”: REvil Darknet Services Offline After Attack Last Weekend

REvil REvil 2021-10-22 · HUNT & HACKETT · Krijn de Mik

Advanced IP Scanner: the preferred scanner in the A(P)T toolbox

Conti DarkSide Dharma Egregor Hades REvil Ryuk 2021-10-18 · Flashpoint · Flashpoint

REvil Disappears Again: ‘Something Is Rotten in the State of Ransomware’

REvil REvil 2021-10-17 · Bleeping Computer · Lawrence Abrams

REvil ransomware shuts down again after Tor sites were hijacked

REvil REvil 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 2021-10-11 · Accenture · Accenture Cyber Threat Intelligence

Moving Left of the Ransomware Boom

REvil Cobalt Strike MimiKatz RagnarLocker REvil 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 2021-09-29 · Flashpoint · Flashpoint

Russian hacker Q&A: An Interview With REvil-Affiliated Ransomware Contractor

REvil REvil 2021-09-28 · Flashpoint · Flashpoint

REvil’s “Cryptobackdoor” Con: Ransomware Group’s Tactics Roil Affiliates, Sparking a Fallout

REvil 2021-09-23 · Bleeping Computer · Ionut Ilascu

REVil ransomware devs added a backdoor to cheat affiliates

REvil 2021-09-22 · Secureworks · Counter Threat Unit ResearchTeam

REvil Ransomware Reemerges After Shutdown; Universal Decryptor Released

REvil REvil 2021-09-21 · Washington Post · Ellen Nakashima, Rachel Lerman

FBI held back ransomware decryption key from businesses to run operation targeting hackers

REvil 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 2021-09-07 · Bleeping Computer · Lawrence Abrams

REvil ransomware's servers mysteriously come back online

REvil 2021-09-03 · IBM · Andrew Gorecki, Camille Singleton, John Dwyer

Dissecting Sodinokibi Ransomware Attacks: Bringing Incident Response and Intelligence Together in the Fight

Valak QakBot REvil 2021-08-30 · CrowdStrike · Eric Loui, Josh Reynolds

CARBON SPIDER Embraces Big Game Hunting, Part 1

Bateleur Griffon Carbanak DarkSide JSSLoader PILLOWMINT REvil 2021-08-25 · GoggleHeadedHacker Blog · Jacob Pimental

Reverse Engineering Crypto Functions: RC4 and Salsa20

REvil 2021-08-20 · · TEAMT5 · TeamT5

See REvil again?! See how hackers use the same encryption ransomware program REvil to annihilate the attack evidence

REvil 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 2021-08-11 · BleepingComputer · Lawrence Abrams

Kaseya's universal REvil decryption key leaked on a hacking forum

REvil 2021-08-10 · Flashpoint · Flashpoint

REvil Master Key for Kaseya Attack Posted to XSS

REvil 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 2021-08-04 · Trend Micro · Janus Agcaoili, Jessie Prevost, Joelson Soares, Ryan Maglaque

Supply Chain Attacks from a Managed Detection and Response Perspective

REvil 2021-08-02 · The Record · Dmitry Smilyanets

An interview with BlackMatter: A new ransomware group that’s learning from the mistakes of DarkSide and REvil

DarkSide LockBit REvil 2021-07-31 · Bleeping Computer · Lawrence Abrams

BlackMatter ransomware gang rises from the ashes of DarkSide, REvil

DarkSide REvil 2021-07-28 · Digital Shadows · Photon Research Team

REvil: Analysis of Competing Hypotheses

REvil REvil 2021-07-27 · Recorded Future · Insikt Group®

BlackMatter Ransomware Emerges As Successor to DarkSide, REvil

DarkSide LockBit REvil 2021-07-27 · Youtube (SANS Institute) · John Hammond, Katie Nickels

SANS Threat Analysis Rundown - Kaseya VSA attack

REvil 2021-07-27 · Flashpoint · Flashpoint

Chatter Indicates BlackMatter as REvil Successor

REvil 2021-07-27 · Twitter (@fwosar) · Fabian Wosar

Tweet on new REvil variant

REvil 2021-07-25 · Youtube (AhmedS Kasmani) · AhmedS Kasmani

Analysis of Malware from Kaseya/Revil Supply Chain attack.

REvil 2021-07-22 · Bleeping Computer · Lawrence Abrams

Kaseya obtains universal decryptor for REvil ransomware victims

REvil 2021-07-20 · Huntress Labs · John Hammond

Security Researchers' Hunt to Discover Origins of the Kaseya VSA Mass Ransomware Incident

REvil 2021-07-19 · Elliptic · Elliptic

REvil Revealed - Tracking a Ransomware Negotiation and Payment

REvil REvil 2021-07-15 · YouTube (DuMp-GuY TrIcKsTeR) · Jiří Vinopal

Fast API resolving of REvil Ransomware related to Kaseya attack

REvil 2021-07-14 · Advanced Intelligence · AdvIntel Security & Development Team, Yelisey Boguslavskiy

REvil Vanishes From Underground - Infrastructure Down

REvil 2021-07-13 · Bleeping Computer · Lawrence Abrams

REvil ransomware gang's web sites mysteriously shut down

REvil 2021-07-13 · Threat Post · Lisa Vaas

Ransomware Giant REvil's Sites Disappear

REvil REvil 2021-07-09 · The Record · Catalin Cimpanu

Ransomwhere project wants to create a database of past ransomware payments

Egregor Mailto Maze REvil 2021-07-09 · Twitter (@SophosLabs) · SophosLabs

Tweet on speed at which Kaseya REvil attack was conducted

REvil 2021-07-09 · cyjax · william thomas

REvil-ution – A Persistent Ransomware Operation

REvil 2021-07-08 · Gigamon · Joe Slowik

Observations and Recommendations from the Ongoing REvil-Kaseya Incident

REvil 2021-07-08 · KELA · Victoria Kivilevich

Ransomware Gangs are Starting to Look Like Ocean's 11

REvil 2021-07-08 · Sekoia · sekoia

Kaseya: Another Massive Heist by REvil

REvil 2021-07-07 · Trustwave · Nikita Kazymirskyi, Rodel Mendrez

Diving Deeper Into the Kaseya VSA Attack: REvil Returns and Other Hackers Are Riding Their Coattails

Cobalt Strike REvil 2021-07-07 · Elastic · Jamie Butler

Elastic Security prevents 100% of REvil ransomware samples

REvil 2021-07-07 · CrowdStrike · Karan Sood, Liviu Arsene

How CrowdStrike Falcon Stops REvil Ransomware Used in the Kaseya Attack

REvil 2021-07-07 · Netskope · Gustavo Palazolo

Netskope Threat Coverage: REvil

REvil 2021-07-07 · Twitter (@resecurity_com) · Resecurity

Tweet REvil attack chain used against Kaseya

REvil 2021-07-06 · paloalto Networks Unit 42 · John Martineau

Understanding REvil: The Ransomware Gang Behind the Kaseya Attack

Gandcrab REvil 2021-07-06 · Cybereason · Tom Fakterman

Cybereason vs. REvil Ransomware: The Kaseya Chronicles

REvil 2021-07-06 · CrowdStrike · Adam Meyers

The Evolution of PINCHY SPIDER from GandCrab to REvil

Gandcrab REvil 2021-07-06 · TRUESEC · Alexander Andersson

How the Kaseya VSA Zero Day Exploit Worked

REvil 2021-07-06 · splunk · Splunk Threat Research Team

REvil Ransomware Threat Research Update and Detections

REvil 2021-07-06 · Twitter (@_alex_il_) · Alex Ilgayev

Tweet on REvil ransomware actor using vulnerable defender executable in its infection flow in early may before Kaseya attack

REvil 2021-07-06 · Zscaler · Zscaler

Kaseya Supply Chain Ransomware Attack - Technical Analysis of the REvil Payload

REvil 2021-07-05 · Kaspersky · Kaspersky

REvil ransomware attack against MSPs and its clients around the world

REvil 2021-07-05 · · S2W LAB Inc. · S2W LAB INTELLIGENCE TEAM

Kaseya supply chain attack delivers mass ransomware

REvil 2021-07-05 · Morphisec · Morphisec

Real-Time Prevention of the Kaseya VSA Supply Chain REvil Ransomware Attack

REvil 2021-07-05 · splunk · Ryan Kovar

Kaseya, Sera. What REvil Shall Encrypt, Shall Encrypt

REvil 2021-07-05 · Twitter (@SophosLabs) · SophosLabs

Tweet with a REvil ransomware execution demo

REvil 2021-07-05 · Twitter (@R3MRUM) · R3MRUM

Twitter thread with additional context on C2 domains found in REvil configuration

REvil 2021-07-04 · CISA · US-CERT

CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack

REvil REvil 2021-07-04 · TRUESEC · Fabio Viggiani

Kaseya supply chain attack targeting MSPs to deliver REvil ransomware

REvil 2021-07-04 · Twitter (@svch0st) · Zach

Tweet on #Kaseya detection tool for detecting REvil

REvil 2021-07-04 · Sophos · Anand Ajjan, Mark Loman, Sean Gallagher

Independence Day: REvil uses supply chain exploit to attack hundreds of businesses

REvil 2021-07-03 · Kaseya · Kaseya

Kaseya VSA Detection Tool

REvil 2021-07-03 · Cybleinc · cybleinc

Uncensored Interview with REvil / Sodinokibi Ransomware Operators

REvil REvil 2021-07-03 · Kaseya · Kaseya

Updates Regarding VSA Security Incident

REvil 2021-07-03 · Symantec · Threat Hunter Team

Kaseya Ransomware Supply Chain Attack: What You Need To Know

REvil 2021-07-03 · Palo Alto Networks Unit 42 · Unit 42

Threat Brief: Kaseya VSA Ransomware Attack

REvil 2021-07-03 · Twitter (@LloydLabs) · Lloyd

Twitter Thread on Revil sideloading DLL used in Kaseya attack

REvil 2021-07-03 · Medium Doublepulsar · Kevin Beaumont

Kaseya supply chain attack delivers mass ransomware event to US companies

REvil 2021-07-03 · Twitter (@fwosar) · Fabian Wosar

Twitter thread on REvil's cryptographic scheme

REvil 2021-07-02 · The Record · Catalin Cimpanu

REvil ransomware gang executes supply chain attack via malicious Kaseya update

REvil 2021-07-02 · Twitter (@SyscallE) · SeAccessCheck

Tweet on Revil dropper used in Kaseya attack

REvil 2021-07-02 · Github (fwosar) · Fabian Wosar

REvil configuration dump used in Kaseya attack

REvil 2021-07-02 · Twitter (@VK_intel) · Vitali Kremez

Tweet on Revil ransomware analysis used in Kaseya attack

REvil 2021-07-02 · Huntress Labs · Huntress Labs

Crticial Ransomware Incident in Progress

REvil 2021-07-02 · · Velzart · Niels den Hild

Ransomware attack

REvil 2021-07-02 · Bleeping Computer · Lawrence Abrams

REvil ransomware hits 1,000+ companies in MSP supply-chain attack

REvil 2021-07-01 · AT&T Cybersecurity · Fernando Martinez, Ofer Caspi

REvil’s new Linux version

REvil REvil 2021-07-01 · DomainTools · Chad Anderson

The Most Prolific Ransomware Families: A Defenders Guide

REvil Conti Egregor Maze REvil 2021-06-30 · Advanced Intelligence · AdvIntel Security & Development Team, Brandon Rudisel, Yelisey Boguslavskiy

Ransomware-&-CVE: Industry Insights Into Exclusive High-Value Target Adversarial Datasets

BlackKingdom Ransomware Clop dearcry Hades REvil 2021-06-30 · Sophos · Tilly Travers

MTR in Real Time: Hand-to-hand combat with REvil ransomware chasing a $2.5 million pay day

REvil 2021-06-30 · Group-IB · Oleg Skulkin

REvil Twins Deep Dive into Prolific RaaS Affiliates' TTPs

Cobalt Strike REvil 2021-06-30 · Sophos SecOps · Tilly Travers

What to expect when you’ve been hit with REvil ransomware

REvil 2021-06-28 · Twitter (@AdamTheAnalyst) · AdamTheAnalyst

Tweet on suspected REvil exfiltration (over RClone FTP) server

REvil REvil 2021-06-23 · · Medium s2wlab · Sojun Ryu

Deep analysis of REvil Ransomware

REvil 2021-06-22 · Secureworks · Counter Threat Unit ResearchTeam

LV Ransomware

REvil 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-

15 · Trend Micro · Byron Gelera, Earle Earnshaw, Janus Agcaoili, Miguel Ang, Nikko Tamana

Ransomware Double Extortion and Beyond: REvil, Clop, and Conti

Clop Conti REvil 2021-06-11 · SophosLabs Uncut · Anand Ajjan, Andrew Brandt, Hajnalka Kope, Mark Loman, Peter Mackenzie

Relentless REvil, revealed: RaaS as variable as the criminals who use it

REvil 2021-06-10 · HUNT & HACKETT · Krijn de Mik

REvil: the usage of legitimate remote admin tooling

REvil 2021-06-09 · Palo Alto Networks Unit 42 · Doel Santos

Prometheus Ransomware Gang: A Group of REvil?

Hakbit Prometheus REvil 2021-06-08 · Advanced Intelligence · Vitali Kremez, Yelisey Boguslavskiy

From QBot...with REvil Ransomware: Initial Attack Exposure of JBS

QakBot REvil 2021-06-02 · Bleeping Computer · Lawrence Abrams

FBI: REvil cybergang behind the JBS ransomware attack

REvil 2021-06-02 · TEAMT5 · TeamT5

Introducing The Most Profitable Ransomware REvil

Gandcrab REvil 2021-06-02 · CrowdStrike · Heather Smith, Josh Dalman

Under Attack: Protecting Against Conti, DarkSide, REvil and Other Ransomware

DarkSide Conti DarkSide REvil 2021-05-28 · Twitter (@Jacob_Pimental) · Jacob Pimental

Tweet on REvil ver 2.07

REvil 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 2021-05-20 · Digital Shadows · Stefano De Blasi

Ransomware-as-a-Service, Rogue Affiliates, and What’s Next

DarkSide DarkSide REvil 2021-05-20 · CrowdStrike · joshua fraser

Response When Minutes Matter: When Good Tools Are Used for (R)Evil

REvil 2021-05-18 · The Record · Catalin Cimpanu

Darkside gang estimated to have made over $90 million from ransomware attacks

DarkSide DarkSide Mailto Maze REvil Ryuk 2021-05-18 · Bleeping Computer · Ionut Ilascu

DarkSide ransomware made $90 million in just nine months

DarkSide DarkSide Egregor Gandcrab Mailto Maze REvil Ryuk 2021-05-14 · The Record · Catalin Cimpanu

Darkside ransomware gang says it lost control of its servers & money a day after Biden threat

DarkSide Avaddon REvil 2021-05-13 · Bleeping Computer · Lawrence Abrams

Popular Russian hacking forum XSS bans all ransomware topics

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

Ransomware world in 2021: who, how and why

Babuk REvil 2021-05-11 · Flashpoint · Flashpoint

DarkSide Ransomware Links to REvil Group Difficult to Dismiss

DarkSide 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 2021-05-08 · Twitter (@Jacob_Pimental) · Jacob Pimental

Tweet on CyberChef recipe to extract Revil Ransomware configuration

REvil 2021-05-06 · Blackberry · BlackBerry Research and Intelligence team

Threat Thursday: Dr. REvil Ransomware Strikes Again, Employs Double Extortion Tactics

REvil 2021-05-06 · Cyborg Security · Brandon Denker

Ransomware: Hunting for Inhibiting System Backup or Recovery

Avaddon Conti DarkSide LockBit Mailto Maze Mespinoza Nemty PwndLocker RagnarLocker RansomEXX REvil Ryuk Snatch ThunderX 2021-05-02 · GoggleHeadedHacker Blog · Jacob Pimental

Sodinokibi Ransomware Analysis

REvil 2021-04-28 · IBM · Limor Kessem

The Sodinokibi Chronicles: A (R)Evil Cybercrime Gang Disrupts Organizations for Trade Secrets and Cash

REvil 2021-04-26 · CoveWare · CoveWare

Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound

Avaddon Clop Conti DarkSide Egregor LockBit Mailto Phobos REvil Ryuk SunCrypt 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 2021-04-23 · CNBC · Eamon Javers

Axis of REvil: What we know about the hacker collective taunting Apple

REvil 2021-04-20 · Bleeping Computer · Sergiu Gatlan

REvil gang tries to extort Apple, threatens to sell stolen blueprints

REvil 2021-03-29 · The DFIR Report · The DFIR Report

Sodinokibi (aka REvil) Ransomware

Cobalt Strike IcedID REvil 2021-03-24 · Cisco · Caitlin Huey, David Liebenberg

Quarterly Report: Incident Response trends from Winter 2020-21

Egregor REvil WastedLocker 2021-03-24 · Twitter (@VK_intel) · Vitali Kremez

Tweet on REvil ransomware

REvil 2021-03-19 · Bleeping Computer · Lawrence Abrams

REvil ransomware has a new ‘Windows Safe Mode’ encryption mode

REvil 2021-03-17 · Palo Alto Networks Unit 42 · Unit42

Ransomware Threat Report 2021

RansomEXX Dharma DoppelPaymer Gandcrab Mailto Maze Phobos RansomEXX REvil Ryuk WastedLocker

2021-03-16 · The Record · Dmitry Smilyanets

‘I scrounged through the trash heaps… now I’m a millionaire:’ An interview with REvil’s Unknown

REvil 2021-03-11 · Flashpoint · Flashpoint

CL0P and REvil Escalate Their Ransomware Tactics

Clop REvil 2021-03-01 · Techtarget · Rob Wright

Ransomware negotiations: An inside look at the process

REvil 2021-03-01 · Group-IB · Oleg Skulkin, Roman Rezvukhin, Semyon Rogachev

Ransomware Uncovered 2020/2021

RansomEXX BazarBackdoor Buer Clop Conti DoppelPaymer Dridex Egregor IcedID Maze PwndLocker QakBot RansomEXX REvil Ryuk SDBbot TrickBot Zloader 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 2021-02-26 · CrowdStrike · Eric Loui, Sergei Frankoff

Hypervisor Jackpotting: CARBON SPIDER and SPRITE SPIDER Target ESXi Servers With Ransomware to Maximize Impact

DarkSide RansomEXX Griffon Carbanak Cobalt Strike DarkSide IcedID MimiKatz PyXie RansomEXX REvil 2021-02-24 · IBM · IBM SECURITY X-FORCE

X-Force Threat Intelligence Index 2021

Emotet QakBot Ramnit REvil TrickBot 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 2021-02-11 · CTI LEAGUE · CTI LEAGUE

CTIL Darknet Report – 2021

Conti Mailto Maze REvil Ryuk 2021-02-02 · · CRONUP · Germán Fernández

De ataque con Malware a incidente de Ransomware

Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DanaBot Dharma Dridex Egregor Emotet Empire Downloader FriedEx GootKit IcedID MegaCortex Nemty Phorpiex PwndLocker PyXie QakBot RansomEXX REvil Ryuk SDBbot SmokeLoader TrickBot Zloader 2021-02-01 · AhnLab · ASEC Analysis Team

BlueCrab ransomware, CobaltStrike hacking tool installed in corporate environment

Cobalt Strike REvil 2021-01-28 · · AhnLab · ASEC Analysis Team

BlueCrab ransomware constantly trying to bypass detection

Cobalt Strike REvil 2021-01-26 · Trend Micro · Trend Micro Research

Examining a Sodinokibi Attack

REvil 2021-01-21 · InfoSec Handlers Diary Blog · Xavier Mertens

Powershell Dropping a REvil Ransomware

REvil 2021-01-04 · KELA · Almog Zoosman, Victoria Kivilevich

Darknet Threat Actors Are Not Playing Games with the Gaming Industry

REvil 2021-01-01 · Secureworks · SecureWorks

Threat Profile: GOLD SOUTHFIELD

REvil GOLD SOUTHFIELD 2021-01-01 · Acronis · Alexander Koshelev, Ravikant Tiwari

Taking Deep Dive into Sodinokibi Ransomware

REvil 2020-12-16 · Accenture · Paul Mansfield

Tracking and combatting an evolving danger: Ransomware extortion

DarkSide Egregor Maze Nefilim RagnarLocker REvil Ryuk SunCrypt 2020-12-16 · Dragos · Camille Singleton, IBM SECURITY X-FORCE, Selena Larson

Assessing Ransomware and Extortion Activities Impacting Industrial Organizations: Ransomware in ICS Environments

REvil 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 2020-12-09 · FireEye · Mitchell Clarke, Tom Hall

It's not FINished The Evolving Maturity in Ransomware Operations (SLIDES)

Cobalt Strike DoppelPaymer QakBot REvil 2020-12-03 · KELA · Victoria Kivilevich

Easy Way In? 5 Ransomware Victims Had Their Pulse Secure VPN Credentials Leaked

REvil 2020-12-01 · Trend Micro · Ryan Flores

The Impact of Modern Ransomware on Manufacturing Networks

Maze Petya REvil 2020-11-30 · Malwarebytes · hasherezade, Jérôme Segura

German users targeted with Gootkit banker or REvil ransomware

GootKit REvil 2020-11-30 · FireEye · Mitchell Clarke, Tom Hall

It's not FINished The Evolving Maturity in Ransomware Operations

Cobalt Strike DoppelPaymer MimiKatz QakBot REvil 2020-11-18 · Bleeping Computer · Lawrence Abrams

REvil ransomware hits Managed.com hosting provider, 500K ransom

REvil 2020-11-18 · KELA · Victoria Kivilevich

Zooming into Darknet Threats Targeting Japanese Organizations

Conti DoppelPaymer Egregor LockBit Maze REvil Snake 2020-11-16 · Intel 471 · Intel 471

Ransomware-as-a-service: The pandemic within a pandemic

Avaddon Clop Conti DoppelPaymer Egregor Hakbit Mailto Maze Mespinoza RagnarLocker REvil Ryuk SunCrypt ThunderX 2020-11-10 · AP News · Ashish Gahlot

Threat Hunting for REvil Ransomware

REvil 2020-11-04 · ZDNet · Catalin Cimpanu

REvil ransomware gang 'acquires' KPOT malware

KPOT Stealer REvil 2020-10-29 · Bleeping Computer · Ionut Ilascu

REvil ransomware gang claims over $100 million profit in a year

REvil 2020-10-28 · Intel 471 · Intel 471

Alleged REvil member spills details on group’s ransomware operations

REvil 2020-10-26 · Checkpoint · Eyal Itkin, Itay Cohen

Exploit Developer Spotlight: The Story of PlayBit

Dyre Maze PyLocky Ramnit REvil 2020-10-23 · Hornetsecurity · Hornetsecurity Security Lab

Leakware-Ransomware-Hybrid Attacks

Avaddon Clop Conti DarkSide DoppelPaymer Mailto Maze Mespinoza Nefilim RagnarLocker REvil Sekhmet SunCrypt 2020-10-20 · · Bundesamt für Sicherheit in der Informationstechnik · BSI

Die Lage der IT-Sicherheit in Deutschland 2020

Clop Emotet REvil Ryuk TrickBot 2020-10-06 · CrowdStrike · The Crowdstrike Intel Team

Double Trouble: Ransomware with Data Leak Extortion, Part 2

Maze MedusaLocker REvil VIKING SPIDER 2020-10-01 · KELA · Victoria Kivilevich

To Attack or Not to Attack: Targeting the Healthcare Sector in the Underground Ecosystem

Conti DoppelPaymer Mailto Maze REvil Ryuk SunCrypt 2020-09-29 · Microsoft · Microsoft

Microsoft Digital Defense Report

Emotet IcedID Mailto Maze QakBot REvil RobinHood TrickBot 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 2020-09-24 · Kaspersky Labs · Kaspersky Lab ICS CERT

Threat landscape for industrial automation systems - H1 2020

Poet RAT Mailto Milum RagnarLocker REvil Ryuk Snake 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 2020-08-21 · Vimeo (RiskIQ) · Josh Burgess, Steve Ginty

The Evolution of Ransomware & Pinchy Spider's Shot at the Title

Gandcrab REvil 2020-08-21 · RiskIQ · Steve Ginty

Pinchy Spider: Ransomware Infrastructure Connected to Dark Web Marketplace

REvil 2020-08-20 · DomainTools · Chad Anderson

Revealing REvil Ransomware With DomainTools and Maltego

REvil 2020-08-20 · sensecy · cyberthreatinsider

Global Ransomware Attacks in 2020: The Top 4 Vulnerabilities

Clop Maze REvil Ryuk 2020-08-01 · Temple University · CARE

Critical Infrastructure Ransomware Attacks

CryptoLocker Cryptowall DoppelPaymer FriedEx Mailto Maze REvil Ryuk SamSam WannaCryptor 2020-07-31 · PRODAFT Threat Intelligence · PRODAFT

OpBlueRaven: Unveiling Fin7/Carbanak - Part 1 : Tirion

Carbanak REvil FIN7 2020-07-29 · ESET Research · welivesecurity

THREAT REPORT Q2 2020

DEFENSOR ID HiddenAd Bundlore Pirrit Agent.BTZ Cerber ClipBanker CROSSWALK Cryptowall CTB Locker DanaBot Dharma Formbook Gandcrab Grandoreiro Houdini ISFB LockBit Locky Mailto Maze Microcin Nemty NjRAT Phobos PlugX Pony REvil Socelars STOP Tinba TrickBot WannaCryptor 2020-07-29 · AmosSys · Nicolas Guillois

Sodinokibi / REvil Malware Analysis

REvil 2020-07-22 · · TEHTRIS · TEHTRIS

Peut-on neutraliser un ransomware lancé en tant que SYSTEM sur des milliers de machines en même temps?

REvil 2020-07-15 · Advanced Intelligence · Samantha van de Ven, Yelisey Boguslavskiy

Inside REvil Extortionist “Machine”: Predictive Insights

Gandcrab REvil 2020-07-10 · Advanced Intelligence · Advanced Intelligence

The Dark Web of Intrigue: How REvil Used the Underground Ecosystem to Form an Extortion Cartel

Gandcrab REvil 2020-06-30 · AppGate · The Immunity Team

Electric Company Ransomware Attack Calls for $14 Million in Ransom

REvil 2020-06-23 · Symantec · Critical Attack Discovery and Intelligence Team

Sodinokibi: Ransomware Attackers also Scanning for PoS Software, Leveraging Cobalt Strike

Cobalt Strike REvil 2020-06-19 · Panda Security · Aaron Jornet Sales, Javier Muñoz Alcázar, Jorge Barelles Menes, Pablo Cardós Marqués

Sodinokibi Malware report

REvil 2020-06-02 · ZDNet · Catalin Cimpanu

REvil ransomware gang launches auction site to sell stolen data

REvil 2020-06-01 · Arete · Arete Incident Response

Sodinokibi / REvil Ransomware attacks against the Education Sector

REvil 2020-05-26 · DataBreaches.net · Dissent

A former DarkSide listing shows up on REvil's leak site

DarkSide REvil 2020-05-07 · REDTEAM.PL · Adam Ziaja

Sodinokibi / REvil ransomware

Maze MimiKatz REvil 2020-05-04 · Intel 471 · Intel 471 Malware Intelligence team

Changes in REvil ransomware version 2.2

REvil 2020-04-28 · Microsoft · Microsoft Threat Protection Intelligence Team

Ransomware groups continue to target healthcare, critical services; here's how to reduce risk

LockBit Mailto Maze MedusaLocker Paradise RagnarLocker REvil RobinHood 2020-04-11 · Bleeping Computer · Lawrence Abrams

Sodinokibi Ransomware to stop taking Bitcoin to hide money trail

REvil 2020-04-09 · Graham Cluley Blog · Graham Cluley

Travelex paid hackers $2.3 million worth of Bitcoin after ransomware attack

REvil 2020-03-31 · Intel 471 · Intel 471

REvil Ransomware-as-a-Service – An analysis of a ransomware affiliate operation

Gandcrab REvil 2020-03-24 · Bleeping Computer · Lawrence Abrams

Three More Ransomware Families Create Sites to Leak Stolen Data

Clop DoppelPaymer Maze Nefilim Nemty REvil 2020-03-07 · Bleeping Computer · Lawrence Abrams

Ransomware Threatens to Reveal Company's 'Dirty' Secrets

REvil 2020-03-05 · Microsoft · Microsoft Threat Protection Intelligence Team

Human-operated ransomware attacks: A preventable disaster

Dharma DoppelPaymer Dridex EternalPetya Gandcrab Hermes LockerGoga MegaCortex MimiKatz REvil RobinHood Ryuk SamSam TrickBot WannaCryptor PARINACOTA 2020-03-04 · CrowdStrike · CrowdStrike

2020 CrowdStrike Global Threat Report

MESSAGETAP More_eggs 8.t Dropper Anchor BabyShark BadNews Clop Cobalt Strike CobInt Cobra Carbon System Cutwail DanaBot Dharma DoppelDridex DoppelPaymer Dridex Emotet FlawedAmmyy FriedEx Gandcrab Get2 IcedID ISFB KerrDown LightNeuron LockerGoga Maze MECHANICAL Necurs Nokki Outlook Backdoor Phobos Predator The Thief QakBot REvil RobinHood Ryuk SDBbot Skipper SmokeLoader TerraRecon TerraStealer TerraTV TinyLoader TrickBot Vidar Winnti ANTHROPOID SPIDER APT23 APT31 APT39 APT40 BlackTech BuhTrap Charming Kitten CLOCKWORK SPIDER DOPPEL SPIDER FIN7 Gamaredon Group GOBLIN PANDA MONTY SPIDER MUSTANG PANDA NARWHAL SPIDER NOCTURNAL SPIDER PINCHY SPIDER SALTY SPIDER SCULLY SPIDER SMOKY SPIDER Thrip VENOM SPIDER VICEROY TIGER 2020-03-03 · PWC UK · PWC UK

Cyber Threats 2019:A Year in Retrospect

KevDroid MESSAGETAP magecart AndroMut Cobalt Strike CobInt Crimson RAT DNSpionage Dridex Dtrack

Emotet FlawedAmmyy FlawedGrace FriedEx Gandcrab Get2 GlobeImposter Grateful POS ISFB Kazuar LockerGoga Nokki QakBot Ramnit REvil Rifdoor RokRAT Ryuk shadowhammer ShadowPad Shifu Skipper StoneDrill Stuxnet TrickBot Winnti ZeroCleare APT41 MUSTANG PANDA Sea Turtle 2020-02-29 · Security Affairs · Pierluigi Paganini

Sodinokibi Ransomware gang threatens to disclose data from Kenneth Cole fashion firm

REvil 2020-02-26 · Bleeping Computer · Lawrence Abrams

Sodinokibi Ransomware May Tip NASDAQ on Attacks to Hurt Stock Prices

REvil 2020-02-25 · RSA Conference · Joel DeCapua

Feds Fighting Ransomware: How the FBI Investigates and How You Can Help

FastCash Cerber Defray Dharma FriedEx Gandcrab GlobeImposter Mamba Phobos Rapid Ransom REvil Ryuk SamSam Zeus 2020-02-10 · Malwarebytes · Adam Kujawa, Chris Boyd, David Ruiz, Jérôme Segura, Jovi Umawing, Nathan Collier, Pieter Arntz, Thomas Reed, Wendy Zamora

2020 State of Malware Report

magecart Emotet QakBot REvil Ryuk TrickBot WannaCryptor 2020-02-02 · Nullteilerfrei Blog · Lars Wallenborn

Defeating Sodinokibi/REvil String-Obfuscation in Ghidra

REvil 2020-01-30 · Under The Breach · Under The Breach

Tracking Down REvil's "Lalartu" by utilizing multiple OSINT methods

REvil 2020-01-30 · Digital Shadows · Photon Research Team

Competitions on Russian-language cybercriminal forums: Sharing expertise or threat actor showboating?

REvil 2020-01-29 · ANSSI · ANSSI

État de la menace rançongiciel

Clop Dharma FriedEx Gandcrab LockerGoga Maze MegaCortex REvil RobinHood Ryuk SamSam 2020-01-28 · KPN · KPN

Tracking REvil

REvil 2020-01-26 · Youtube (OALabs) · Sean Wilson, Sergei Frankoff

IDA Pro Automated String Decryption For REvil Ransomware

REvil 2020-01-23 · Bleeping Computer · Sergiu Gatlan

Sodinokibi Ransomware Threatens to Publish Data of Automotive Group

REvil 2020-01-18 · Bleeping Computer · Lawrence Abrams

New Jersey Synagogue Suffers Sodinokibi Ransomware Attack

REvil 2020-01-17 · Secureworks · Keita Yamazaki, Tamada Kiyotaka, You Nakatsuru

Is It Wrong to Try to Find APT Techniques in Ransomware Attack?

Defray Dharma FriedEx Gandcrab GlobeImposter Matrix Ransom MedusaLocker Phobos REvil Ryuk SamSam Scarab Ransomware 2020-01-11 · Bleeping Computer · Lawrence Abrams

Sodinokibi Ransomware Publishes Stolen Data for the First Time

REvil 2020-01-10 · BleepingComputer · Sergiu Gatlan

Sodinokibi Ransomware Hits New York Airport Systems

REvil 2020-01-09 · Bleeping Computer · Lawrence Abrams

Sodinokibi Ransomware Says Travelex Will Pay, One Way or Another

REvil 2020-01-06 · Bleeping Computer · Ionut Ilascu

Sodinokibi Ransomware Hits Travelex, Demands $3 Million

REvil 2020-01-01 · Secureworks · SecureWorks

GOLD SOUTHFIELD

REvil 2020-01-01 · Blackberry · Blackberry Research

State of Ransomware

Maze MedusaLocker Nefilim Phobos REvil Ryuk STOP 2019-12-20 · Trustwave · Rodel Mendrez

Undressing the REvil

REvil 2019-12-18 · Hatching.io · Pete Cowman

Understanding Ransomware Series: Detecting Sodin

REvil 2019-12-12 · Bleeping Computer · Lawrence Abrams

Another Ransomware Will Now Publish Victims' Data If Not Paid

REvil 2019-12-04 · Elastic · David French

Ransomware, interrupted: Sodinokibi and the supply chain

REvil 2019-11-09 · Lars Wallenborn

API-Hashing in the Sodinokibi/Revil Ransomware - Why and How?

REvil 2019-10-20 · McAfee · Christiaan Beek, Jessica Saavedra-Morales, Ryan Sherstobitoff

McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service – Crescendo

REvil 2019-10-02 · McAfee · McAfee Labs

McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service – What The Code Tells Us

Gandcrab REvil 2019-09-24 · Secureworks · CTU Research Team

REvil: The GandCrab Connection

REvil GOLD SOUTHFIELD 2019-09-24 · Secureworks · CTU Research Team

REvil/Sodinokibi Ransomware

REvil GOLD SOUTHFIELD 2019-08-30 · Bleeping Computer · Ionut Ilascu

A Look Inside the Highly Profitable Sodinokibi Ransomware Business

REvil 2019-08-23 · The New York Times · David E. Sanger, Manny Fernandez, Marina Trahan Martinez

Ransomware Attacks Are Testing Resolve of Cities Across America

REvil 2019-08-10 · Dissecting Malware · Marius Genheimer

GermanWiper's big Brother? GandGrab's kid ? Sodinokibi!

REvil 2019-07-15 · KrebsOnSecurity · Brian Krebs

Is ‘REvil’ the New GandCrab Ransomware?

REvil 2019-07-03 · Kaspersky Labs · Artur Pakulov, Fedor Sinitsyn, Orkhan Mamedov

Sodin ransomware exploits Windows vulnerability and processor architecture

REvil 2019-06-24 · VirIT · Federico Girotto, Gianfranco Tonello, Michele Zuin

Ransomware REvil - Sodinokibi: Technical analysis and Threat Intelligence Report

REvil 2019-06-14 · Certego · Matteo Lodi

Malware Tales: Sodinokibi

REvil 2019-05-01 · WatchGuard · WatchGuard

Internet Security Report

REvil RobinHood 2019-04-30 · Cisco Talos · Colin Grady, Jaeson Schultz, Matt Valites, Pierre Cadieux

Sodinokibi ransomware exploits WebLogic Server vulnerability

REvil

▶ [TLP:WHITE] win_revil_auto (20251219 | Detects win.revil.)

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