Gandcrab (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:47:39 UTC

GandCrab was a Ransomware-as-a-Service (RaaS) emerged in January 28, 2018, managed by a criminal organization known to be confident and vocal, while running a rapidly evolving ransomware campaign. Through their aggressive, albeit unusual, marketing strategies and constant recruitment of affiliates, they were able to globally distribute a high volume of their malware.

In a surprising announcement on May 31, 2019, the GandCrab's operators posted on a dark web forum, announced the end of a little more than a year of ransomware operations, citing staggering profit figures. However, If there's one thing that sets these threat actors apart from other groups, it is that they are unpredictable; so there is always the possibility that they might re-surface in one form or another.

2022-11-08 · AhnLab · ASEC
LockBit 3.0 Being Distributed via Amadey Bot
Amadey Gandcrab LockBit 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 2021-11-16 · Trend Micro · Trend Micro
Global Operations Lead to Arrests of Alleged Members of GandCrab/REvil and Cl0p Cartels
REvil Clop Gandcrab REvil 2021-10-05 · 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 2021-08-05 · 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 2021-07-16 · Malwarebytes Labs · Jérôme Segura
Vidar and GandCrab: stealer and ransomware combo observed in the wild
Gandcrab Vidar 2021-07-06 · paloalto Networks Unit 42 · John Martineau
Understanding REvil: The Ransomware Gang Behind the Kaseya Attack
Gandcrab REvil 2021-07-06 · CrowdStrike · Adam Meyers
The Evolution of PINCHY SPIDER from GandCrab to REvil
Gandcrab REvil 2021-06-02 · TEAMT5 · TeamT5
Introducing The Most Profitable Ransomware REvil
Gandcrab REvil 2021-05-18 · Bleeping Computer · Ionut Ilascu
DarkSide ransomware made $90 million in just nine months
DarkSide DarkSide Egregor Gandcrab Mailto Maze REvil Ryuk 2021-03-17 · Palo Alto Networks Unit 42 · Unit42
Ransomware Threat Report 2021

RansomEXX Dharma DoppelPaymer Gandcrab Mailto Maze Phobos RansomEXX REvil Ryuk WastedLocker

2021-01-01 · Secureworks · SecureWorks

Threat Profile: GOLD GARDEN

Gandcrab GOLD GARDEN 2020-09-24 · CrowdStrike · CrowdStrike Intelligence Team

Double Trouble: Ransomware with Data Leak Extortion, Part 1

DoppelPaymer Gandcrab LockBit Maze MedusaLocker RagnarLocker SamSam OUTLAW SPIDER

OVERLORD SPIDER 2020-08-21 · Vimeo (RiskIQ) · Josh Burgess, Steve Ginty

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

Gandcrab REvil 2020-08-03 · Bitdefender · Filip Truta

Belarus Authorities Arrest GandCrab Ransomware Operator

Gandcrab 2020-07-31 · BleepingComputer · Ionut Ilascu

GandCrab ransomware operator arrested in Belarus

Gandcrab 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 2020-07-17 · CERT-FR ·

CERT-FR

The Malware Dridex: Origins and Uses

Andromeda CryptoLocker Cutwail DoppelPaymer Dridex Emotet FriedEx Gameover P2P Gandcrab ISFB

Murofet Necurs Predator The Thief Zeus 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 2020-06-22 · · CERT-FR · CERT-FR

Évolution De Lactivité du Groupe Cybercriminel TA505

Amadey AndroMut Bart Clop Dridex FlawedGrace Gandcrab Get2 GlobeImposter Jaff Locky Marap Philadephia

Ransom QuantLoader Scarab Ransomware SDBbot ServHelper Silence tRat TrickBot 2020-05-21 · Intel 471 · Intel

471

A brief history of TA505

AndroMut Bart Dridex FlawedAmmyy FlawedGrace Gandcrab Get2 GlobeImposter Jaff Kegotip Locky Necurs

Philadephia Ransom Pony QuantLoader Rockloader SDBbot ServHelper Shifu Snatch TrickBot 2020-03-31 · Intel

471 · Intel 471

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

Gandcrab 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 2020-02-25 · 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 2020-01-29 · ANSSI · ANSSI

État de la menace rançongiciel

Clop Dharma FriedEx Gandcrab LockerGoga Maze MegaCortex REvil RobinHood Ryuk SamSam 2020-01-20 · Virus Bulletin · AhnLab Security Analysis Team

Behind the scenes of GandCrab's operation

Gandcrab 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 2020-01-10 · CSIS · CSIS

Threat Matrix H1 2019

Gustuff magecart Emotet Gandcrab Ramnit TrickBot 2020-01-01 · Secureworks · SecureWorks

GOLD GARDEN

Gandcrab 2019-11-01 · Virus Bulletin · Alexandre Mundo Alguacil, John Fokker

VB2019 paper: Different ways to cook a crab: GandCrab ransomware-as-a-service (RaaS) analysed in depth

Gandcrab 2019-10-02 · McAfee · McAfee Labs

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

Gandcrab REvil 2019-07-08 · KrebsOnSecurity · Brian Krebs

Who's Behind the GandCrab Ransomware?

Gandcrab 2019-06-24 · Fortinet · Joie Salvio

GandCrab Threat Actors Retire...Maybe

Gandcrab 2019-06-17 · Bitdefender · Bogdan Botezatu

Good riddance, GandCrab! We're still fixing the mess you left behind

Gandcrab 2019-06-03 · SC Magazine · Doug Olenick

GandCrab ransomware operators put in retirement papers

Gandcrab 2019-06-01 · Bleeping Computer · Lawrence Abrams

GandCrab Ransomware Shutting Down After Claiming to Earn $2 Billion

Gandcrab 2019-05-24 · SophosLabs Uncut · Andrew Brandt

Directed attacks against MySQL servers deliver ransomware

Gandcrab 2019-05-08 · Verizon Communications Inc. · Verizon Communications Inc.

2019 Data Breach Investigations Report

BlackEnergy Cobalt Strike DanaBot Gandcrab GreyEnergy Mirai Olympic Destroyer SamSam 2019-03-13 · MyOnlineSecurity · MyOnlineSecurity

Fake CDC Flu Pandemic Warning delivers Gandcrab 5.2 ransomware

Cold$eal Gandcrab 2019-03-06 · CrowdStrike · Bex Hartley, Brendon Feeley, Sergei Frankoff

PINCHY SPIDER Affiliates Adopt “Big Game Hunting” Tactics to Distribute GandCrab Ransomware

Gandcrab Phorpiex PINCHY SPIDER ZOMBIE SPIDER 2019-03-05 · SophosLabs Uncut · Luca Nagy, Suriya Natarajan, Vikas Singh

GandCrab 101: All about the most widely distributed ransomware of the moment

Gandcrab 2019-02-19 · Bitdefender · Bogdan Botezatu

New GandCrab v5.1 Decryptor Available Now

Gandcrab 2019-01-07 · Bleeping Computer · Ionut Ilascu

GandCrab Operators Use Vidar Infostealer as a Forerunner

Gandcrab Vidar 2018-11-08 · TC Contre · tcontre

R.E.: Gandcrab Downloader.. 'There's More To This Than Meets The Eye'

Gandcrab 2018-10-25 · Europol · Europol

Pay No More: universal GandCrab decryption tool released for free on No More Ransom

Gandcrab 2018-10-25 · Bitdefender · Bogdan Botezatu

GandCrab Ransomware decryption tool

Gandcrab 2018-09-18 · Mandiant · Manish Sardiwal, Muhammad Umair, Zain Gardezi

Fallout Exploit Kit Used in Malvertising Campaign to Deliver GandCrab Ransomware

Gandcrab 2018-07-19 · Sensors Tech Forum · Ventsislav Krastev

Killswitch File Now Available for GandCrab v4.1.2 Ransomware

Gandcrab 2018-07-18 · · ASEC · AhnLab ASEC Analysis Team

GandCrab v4.1.2 Encryption Blocking Method (Kill Switch)

Gandcrab 2018-05-09 · Cisco Talos · Christopher Marczewski, Nick Biasini, Nick Lister

Gandcrab Ransomware Walks its Way onto Compromised Sites

Gandcrab 2018-03-07 · InfoSec Handlers Diary Blog · Brad Duncan

Ransomware news: GlobeImposter gets a facelift, GandCrab is still out there

Gandcrab GlobeImposter 2018-02-08 · Bleeping Computer · Lawrence Abrams

GandCrab Ransomware Being Distributed Via Malspam Disguised as Receipts

Gandcrab 2018-01-30 · Malwarebytes · Malwarebytes Labs

GandCrab ransomware distributed by RIG and GrandSoft exploit kits (updated)

Gandcrab 2018-01-29 · Bleeping Computer · Lawrence Abrams

GandCrab Ransomware Distributed by Exploit Kits, Appends GDCB Extension

Gandcrab

▶ [TLP:WHITE] win_gandcrab_auto (20251219 | Detects win.gandcrab.)
