
2015
2016
2017
2018
2019
2020
2021
2022
2023
Bitwise Spider
LockBit
Originally dubbed "ABCD"
LockBit 2.0
LockBit 3.0
LockBit Green
Lockbit builder leaked
Boss Spider
SamSam
BlOOdy
TommyLeaks
SchoolBoys
Darkrace
Ragnarok
Decryptor released before shutdown
Lazarus
North Korean APT group
WannaCry
Circus Spider
Mailto
NetWalker
Law enforcement arrests
Brain Spider
Radar
Twisted Spider
Maze
Egregor
Egregor stops its operation after law enforcement's actions
Sekhmet
Rorschach
SunCrypt
Split
Indrik Spider
Probably created around 2007
BitPayment
WastedLocker
Hades
MacawLocker
Indrik Spider also leverages other RaaS payloads such as LockBit.
Doppel Spider
PhoenixLocker
Cyberpunk
Locky
DoppelPaymer
Although the main ransomware used by the group remains Locky, Graceful Spider is thought to occasionally use other ransomware (Bart, Jaff, Scarab, Philadelphia, GlobeImposter and GandCrab).
Grief
Entropy
Law enforcement arrests
Graceful Spider
Probably active since 2014
Debated overlap
FIN11
LockFile
Almost identical strains
AtomSilo
BianLian
Qilin
CryptFile2
CryptoMix
Work
Cl0p
Hive Spider
Hive
Law enforcement disruptions
Globe
Copycat
GlobeImposter
GlobeImposter uses many different file-extensions.
Lockis
TZW
Sprite Spider
Defray777
RansomExx
RansomExx2
ARCrypter
MountLocker
AstroLocker
XingLocker
DagonLocker
Quantum
Storm-0230
ScareCrow
Mimic
Ransomware strains emerging from leaked Conti's source code
Putin Team
Monti
Storm-1339
Gazprom
CryptoTech
Hermes
Sold on Exploit.in from February 2017.
Leaks resulting from the Ukraine War
Wizard Spider
Ryuk
Law enforcement arrests
First observed in August 2018, based on Hermes.
Conti
Operation shuts down
Karakurt
Diavol
Royal Spider
Royal
BlackSuit
Akira
Storm-0506
Black Basta
Luna Moth
Silent Ransom
Mangled Spider
BlackByte
BlackByteNT
Gold Burlap
Vurten
Mespinoza
Pysa
Snatch
FIN8
White Rabbit
Viking Spider
RagnarLocker
Recess Spider
Play
Debated affiliation
Traveling Spider
JSWorm
Nemty
Nefilim
Karma
Nokoyawa
Offwhite
GangBang
Nevada
Telegram
Milihpen
RansomHouse
Copy Khonsari's leak site design
Fusion
8Base
Legend:
Threat Group/Author
Ransomware operation
Hack&Leak operation (no encryption)
Rebrand/Subset
Similarities/Relationship
Unconfirmed relationship/ Source Code reuse
Author: Marine Pichon
CERT ORANGE CYBERDEFENSE
All rights reserved.
This graph does not aim at being exhaustive. Its goal is to showcase relationships between relevant ransomware operations and does not purposely list all existing ransomware groups since 2015. Names of strains and associated threat actors were chosen arbitrarily by us among the most popular alias used among the cybersecurity community. It does not mean we endorse the vendor that created the alias.
As a reminder, it is extremely complex to assert relationship and attribution when looking at the cybercrime ecosystem: threat actors are extremely volatile and connected between each other, making effective collaborations hard to define and track over time. In addition to our internal resources (monitoring, reverse engineering, Incident Response engagements related to most of these prominent groups), this mapping makes use of numerous public and private reports from incident responders, malware analysts, CTI researchers,… We paid attention to carefully select, corroborate and fact-check such intelligence with trusted and well recognized sources, but may have still made small mistakes or debatable associations.
Don't hesitate to send us your feedback if any.
Version 24 - 04/08/2023
Mario ESXi
Connected to White Rabbit as well
Groove
Babuk leaks its code source online
Dark Angels
Dunghill
PayloadBin
VasaLocker
Babuk
Daixin
Delta
DarkyLock
BabLock
Cheers
RA Group
Cyclops
Knight
Rook
NightSky
Bronze Starlight
Pandora
CatB
SynAck
El Cometa
Vohuk
Cylance
Gold Espresso
AvosLocker
Storm-0289
Attribution still debated
Carbon Spider
Probably active since 2012
Former REvil and Maze affiliate
DarkSide
BlackMatter
Alpha Spider
BlackCat
BlackCat 2.0
Also named ALPHV
CerberImposter
Cerber
Pinchy Spider
GandCrab
REvil
REvil stops its operation after law enforcement's actions
BlogXX
Spectre
Ransom Cartel
Gold Northfield
LV
Chaos
Yashma
SolidBit
Imitates LockBit
Sold and distributed as a malware builder
Onyx
VSOP
BlackSnake
Everbe
Large ransomware family including many variants such as Volcano, Embrace, PainLocker...
Everbe 2.0
Large ransomware family including many variants such as EvilLocker, HyenaLocker, Thunder, Unrew...
Obsidian ORB
Everest
Skeleton Spider
LockerGoga
MegaCortex
Decryptor released
Stop
DJVU
DJVU uses many different file-extensions.
Zeoticus
Zeoticus 2.0
Venus
Crysis threat actors observed deploying Venus around June 2022
Wine Tempest
Crysis
Dharma
Decryption keys released
Phobos
Wiki ransomware
Faust
Vandev
Xorist
CerberSysLock
Makop
EnCiPhErEd
Zixer2
Frozen
Large ransomware family including many variants based on the Encore Builder crypto constructor.
FakeRSA
TaRoNiS
Mcafee
Mcrypt2019
Nigg3r
MortalKombat
TargetCompany
Partial decryptor released
Fargo
Mallox
Xollam
DeathRansom
Cantroid
HelloKitty
RedAlert
FiveHands
Yanluowang
Leaked and doxxed
Vice Society
PolyVice
Group that deploys several ransom payloads, including HelloKitty and Zeppelin
BuddyRansome
Rancoz
Scarab
Amnesia
Rhysida
Buransupport
VegaLocker
Zeppelin
Storm-0671
Cuba
Details and relationships are unclear at this time.
V is Vendetta
Storm-0978
Industrial Spy
Underground Team
Used in at least one identified attack
Trigona
Cryakl
CryLock
LokiLocker
BlackBit
Nosophoros
Jigsaw
Thanos
Sold and distributed as a malware builder
Prometheus
Spook
Haron
Midas
Axxes
Riddle Spider
Avaddon
Shuts down of the operation
Ako
Thunder X
NoEscape
Ranzy Locker
MedusaLocker
Ransomware Blog
MedusaBlog
RTM Gang
Quoter
SunDawn
Read The Manual
Storm-0970
Poop69
Big Head
Gold Lounge
ThunderCrypt
Lorenz
Paradise
Paradise 2.0
Decryptor released
Decryptor released
Code Source leaked
Rapture
Epsilon Red
BlackCocaine
Colossus
Abyss
CrossLock
Money Message
Cactus
MalasLocker
CryptNet
2015
2016
2017
2018
2019
2020
2021
2022
2023