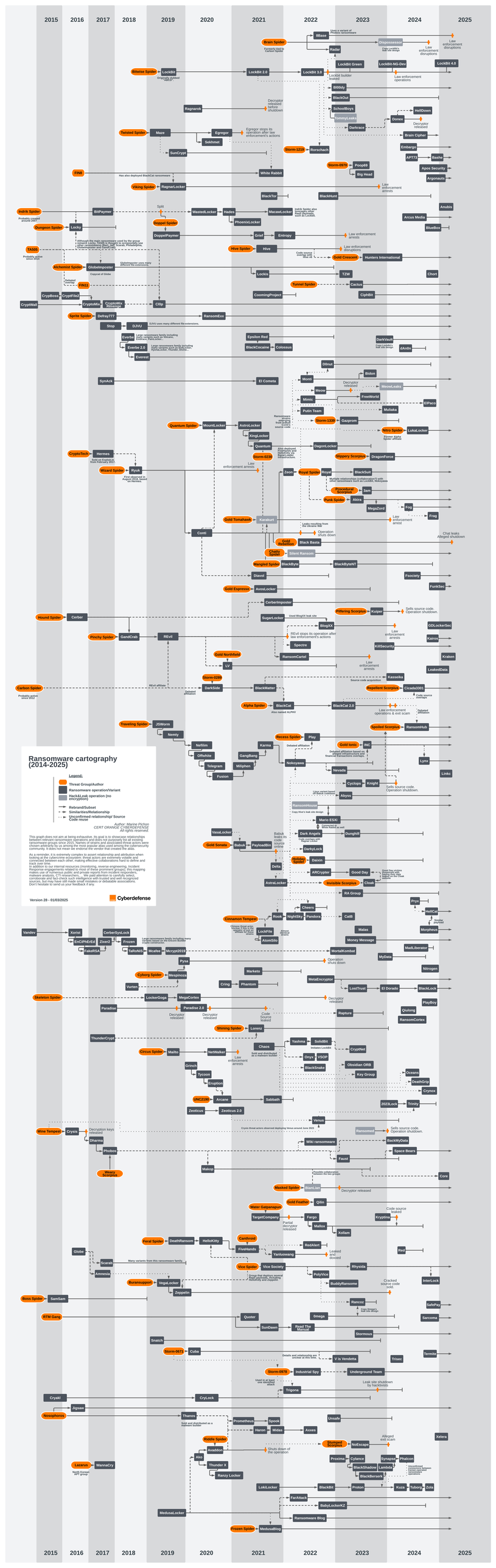
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
Ransomware cartography (2014-2025)
Legend:
Threat Group/Author
Ransomware operation/Variant
Hack&Leak operation (no encryption)
Rebrand/Subset
Similarities/Relationship
Unconfirmed relationship/ Source Code reuse
Author: Marine Pichon
CERT ORANGE CYBERDEFENSE
All rights reserved
This graph does not aim at being exhaustive. Its goal is to showcase relationships between ransomware groups and to show how it has evolved since the emergence of ransomware groups since 2015. Names of actors and associated threat actors were chosen arbitrarily by us among the most popular atlas 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 to prove.
In addition to our internal resources (monitoring, reverse engineering, Incident Response engagements related to most of these prominent groups), this mapping was made using a lot of OSINT: ransomware victim lists, malware analysis, CTI researchers... We paid attention to carefully select, corroborate and fact-check such intelligence with trusted and well recognized sources, in order to avoid misleading interpretations or debatable associations. Don't hesitate to send us your feedback if any.
Version 28 - 01/03/2025
Cyberdefense
Brain Spider
Brain Cipher
Used a variant of Phobos ransomware
Data Leaders Sub site dropp
Law enforcement disruptions
Law enforcement operations
Bitwise Spider
LockBit
Originally dubbed ABCD
LockBit 2.0
LockBit 3.0
LockBit Green
LockBit-NG-Dev
LockBit 4.0
LockBit builder leaked
Ragnarok
Decryptor released before shutdown
Twisted Spider
Maze
Egregor
Egregor stops its operation after law enforcement's actions
Sekhmet
SunCrypt
Storm-1810
Rorschach
Storm-0570
Pooplo69
Big Head
Donex
Decryptor released
HellDown
Darkrace
Embargo
APT73
Bashe
Apos Security
Argonauts
FIN8
Has also deployed BlackCat ransomware
White Rabbit
Viking Spider
RagnarLocker
Law enforcement arrests
BlackTor
BlackHunt
Indrik Spider
Probably coupled around 2017
BitPaymer
Split
WastedLocker
Hades
MacawLocker
Indrik Spider also leverages other RaaS like Dridex, PsyLoc & LockBit.
Anubis
Arcus Media
Dungeon Spider
Locky
Doppel Spider
PhoenixLocker
DoppelPaymer
Grief
Entropy
Law enforcement arrests
BlueBox
TA505
Probably active since 2014
Alchemist Spider
GlobeImposter
Copycat of Globe
Globeimposter uses many different file-extensions.
Hive Spider
Hive
Code source leaked around Hive v5
Law enforcement disruptions
Gold Crescent
Hunters International
Debated Similar
FIN11
Lockis
TZW
Chort
CrypBoss
CrypFiles
Tunnel Spider
Cactus
CryptNet
CryptoMix
CryptoMix (Revenge)
Citip
CoomingProject
CiphBit
Sprite Spider
Defray777
RansomExx
Stop
DJVU
DJVU uses many different file-extensions.
EverSe
Large ransomware family including Stop/Djvu, Phobos, Dharma, Emotet, TrickBot.
Epsilon Red
BlackCocaine
Cofossus
DarkVault
Copy Locker's Sub site dropp
dAnOn
Everbe 2.0
Large ransomware family including many variants such as EvilLocker, Globe/Locker, Phoenix, Dharma...
Everest
DOnut
SynAck
El Comista
Montl
Bidon
Decryptor released
MeowLeaks
Meow
FreeWorld
Mimic
ElPaco
Putin Team
Mullaka
Ransomware groups from Dubai (Laptrinh) source code
Quantum Spider
MountLocker
AstroLocker
Storm-1339
Gazprom
XingLocker
Nitro Spider
LukaLocker
Former Alpha Spider affiliate
Quantum
Also deployed Phobos and HelloKitty via Malware-as-a-service
DagonLocker
CryptoTech
Hermes
Sent on Exploit from February 2017
Storm-0233
Snappy Scorpius
DragonForce
Law enforcement arrests
Wizard Spider
Ryuk
Was observed in August 2018, linked on Hermes.
Zeon
Royal Spider
Royal
BlackSuit
Multiple relationships (collaboration?) with other ransomware such as LockBit, Babuyaga
Procedural Scorpius
3am
Punk Spider
Akira
MegaZord
Fog
Gold Tomahawk
Karakurt
Law enforcement arrest
Frag
Leaks resulting from the Ukraine War
Conti
Operation shuts down
Chat leaks/ Alleged shutdown
Gold Ransom
Black Basta
Chaty Spider
Silent Ransom
Mangled Spider
BlackByte
BlackByteNT
Diavol
Fsociety
Gold Expresso
AvosLocker
FunkSec
CerberImposter
Hound Spider
Cerber
Pillering Scorpius
Kuiper
Sells source code. Operation shutdown.
SugarLocker
Used BlogXX leak site
BlogXX
GDLockerSec
Pinchy Spider
GandCrab
REvil
REvil stops its operation after law enforcement's actions
Spectre
Kairos
KillSecurity
Gold Northfield
LV
RansomCartel
Law enforcement arrests
Kraken
Storm-0289
Kasseika
Source code analysis
LeakedData
Carbon Spider
Probably active since 2012
REvil affiliate
DarkSide
Debated affiliation
BlackMatter
Repellent Scorpius
Cicada3301
Code source analysis
Alpha Spider
BlackCat
Also named ALPHV
BlackCat 2.0
Law enforcement operations & exit scam
Debated affiliation
Spoiled Scorpius
RansomHub
Traveling Spider
JSWorm
Nemty
Nefilim
Offshite
Telegram
Fusion
Karma
GangBang
Milihpen
Recess Spider
Play
Debated affiliation
Gold Ionic
INC
Detailed affiliation based on financial transactions and financial transactions overlaps
Nokoyawa
Lynx
Linkc
Nevada
Cyclops
Knight
Sells source code. Operation shutdown.
Linux variant based on Black cuckoo
Abyss
RansomHouse
Copy Hive's leak site design
Mario EsXi
Mario Ransom as well
VasaLocker
Babuk leaks its source code online
Dark Angels
Code overlaps with Pegasus Locker
Dunghill
Gold Sonata
Babuk
PayloadBin
DarkyLock
Hunter Spider
Daixin
Delta
ARCrypter
Good Day
Good Day uncites victims since July 2023 but they are still active on the Russian website
AstraLocker
Invisible Scorpius
Cloak
RA Group
Cheers
Pryx
Cinnamon Tempest
Rook
NightSky
Pandora
CatB
HellCat
Sensitive payload
Morpheus
Vandey
Xorist
CerberSysLock
LockFile
Attempt to rebrand
Malas
Money Message
EnCIPHERed
Frozen
Zxxer2
FakeRSA
TaRoNiG
Mcafee
Mcrypt2019
Large ransomware family including many variants such as Xorist, Frozen, Encipher Builder, crypto constructor.
MortalKombat
MadLiberator
AtomSilo
MyData
Operation shuts down
Pysa
Nitrogen
Cyborg Spider
Mespinoza
Marketo
Vurten
Cring
Phantom
MetaEncryptor
LostTrust
El Dorado
BlackLock
Skeleton Spider
LockerGoga
MegaCortex
Decryptor released
PlayBoy
Paradise
Paradise 2.0
Decryptor released
Decryptor released
Code Source leaked
Rapture
Qilong
RansomCortex
Shining Spider
Lorenz
ThunderCryptor
Yashma
SolidBit
Imitates LockBit
Chaos
Sold and distributed as a malware builder
CryptNet
Circus Spider
Mailto
NetWalker
Law enforcement arrests
Onyx
VSOP
Obsidian ORB
Grinch
BlackSnake
Tycoon
Key Group
Ocean
Eruption
DeathGrip
Cryptos
UNC2198
Arcane
Sabbath
2023Lock
Trinity
Zeotious
Zeotious 2.0
Venus
Wine Tempest
Crysis
Decryption keys released
Dharma
Crysis threat actors observed deploying Venus around June 2023
Ransomed
Sells source code. Operation shutdown.
Wiki ransomware
BackMyData
Phobos
Space Bears
Faust
Weary Scorpius
Makop
Possible collaboration between the two groups
Core
Masked Spider
Iranian
Decryptor released
Gold Feather
Qilin
Water Gasparagin
TargetCompany
Fargo
Code source leaked
Krystina
Partial decryptor released
Mallox
Xollam
Globe
Feral Spider
DeathRansom
HelloKitty
Cantroll
FiveHands
Yanluowang
RedAlert
Leaked and doxxed
Reef
Scarab
Many variants from this ransomware family.
Amnesia
Vice Spider
Vice Society
Rhysida
Group that deploys several Ransomware, including HelloKitty and Zeppelin
PolyVice
Buransupport
VegaLocker
BuddyRansome
InterLock
Cracked source code sold.
Ross Spider
SamSam
Zeppelin
Rancoz
Code Dragon's Sub site dropp
SafePay
RTM Gang
Quoter
Omega
Sarcoma
SunDawn
Royal The Mariner
Stormous
Snatch
Storm-0671
Cuba
Details and relationship are unclear at this time
V is Vendetta
Trisec
Termite
Storm-0978
Industrial Spy
Underground Team
Used in a large one identified attack
Trigona
Leak site shutdown by hacktivists
Cryakl
CryLock
Jigsaw
Noscophoros
Thanos
Sold and distributed as a malware builder
Prometheus
Spook
Haron
Midas
Axxes
Unsafe
Ridelle Spider
Avaddon
Shuts down of the operation
Shompen Scorpius
NoEscape
Alleged exit scam
Xelera
Akio
Thunder X
Ranzy Locker
Proxima
Cylance
Lynxpro
Phalcon
BlackShadow
Lambda
BlackBerserk
Unconfirmed relation between Lambda and Lynxpro operations
Lazarus
North Korean APT group
WannaCry
LokiLocker
BlackBit
Proton
Koza
Tuborg
Zola
FarAttack
BabyLockerKZ
MedusaLocker
Ransomware Blog
Frozen Spider
MedusaBlog
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025