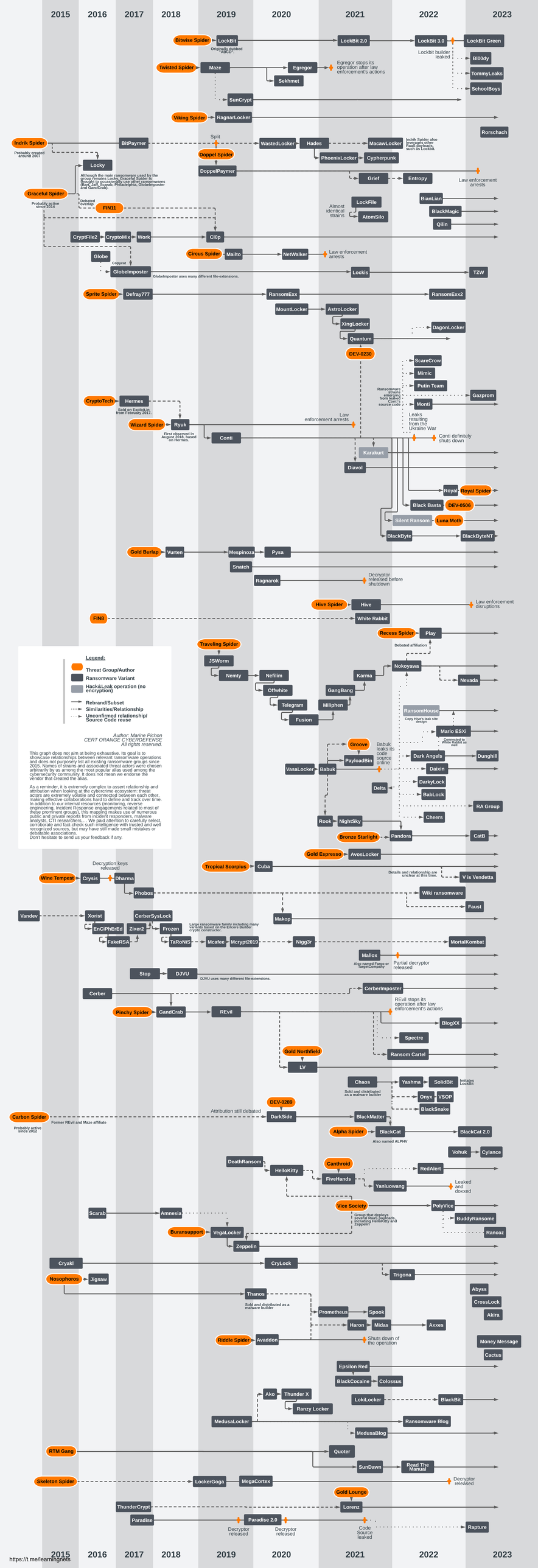
2015
2016
2017
2018
2019
2020
2021
2022
2023
Bitwise Spider
LockBit
Originally dubbed "ABCD".
LockBit 2.0
LockBit 3.0
LockBit Green
Lockbit builder leaked
Bl00dy
TommyLeaks
SchoolBoys
Twisted Spider
Maze
Egregor
Egregor stops its operation after law enforcement's actions
Sekhmet
SunCrypt
Viking Spider
RagnarLocker
Rorschach
Indrik Spider
Probably created around 2007
BitPaymer
Split
Doppel Spider
WastedLocker
Hades
MacawLocker
Indrik Spider also leverages other Hades payloads, such as Locksin.
PhoenixLocker
Cypherpunk
Locky
DoppelPaymer
Grief
Entropy
Law enforcement arrests
Although the main ransomware used by the group remains Locky, Graceful Spider is thought to occasionally use other ransomwares (Bart, Jaff, Scarab, Philadelphia, Globeimposter and GandCrab).
Graceful Spider
Probably active since 2014
Debated overlap
FIN11
Almost identical strains
LockFile
AtomSilo
BianLian
BlackMagic
Qilin
CryptFile2
CryptoMix
Work
Clop
Globe
Copycat
Circus Spider
Mailto
NetWalker
Law enforcement arrests
GlobeImposter
GlobeImposter uses many different file-extensions.
Lockis
TZW
Sprite Spider
Defray777
RansomExx
RansomExx2
MountLocker
AstroLocker
XingLocker
Quantum
DagonLocker
DEV-0230
ScareCrow
Mimic
Putin Team
Ransomware citizens emerging from leaked Conti's source code
Gazprom
Monti
CryptoTech
Hermes
Sold on Exploit.in from February 2017.
Wizard Spider
Ryuk
First observed in August 2018, based on Hermes.
Law enforcement arrests
Leaks resulting from the Ukraine War
Conti
Conti definitely shuts down
Karakurt
Diavol
Royal
Royal Spider
Black Basta
DEV-0506
Silent Ransom
Luna Moth
BlackByte
BlackByteNT
Gold Burlap
Vurten
Mespinoza
Pysa
Snatch
Ragnarok
Decryptor released before shutdown
Hive Spider
Hive
Law enforcement disruptions
FIN8
White Rabbit
Recess Spider
Play
Debated affiliation
Traveling Spider
JSWorm
Nemty
Nefilim
Offwhite
Telegram
Fusion
Karma
GangBang
Miliphen
Nokoyawa
Nevada
RansomHouse
Copy Hive's leak site design
Mario ESXi
Connected to White Rabbit as well
Groove
Babuk leaks its code source online
PayloadBin
VasaLocker
Babuk
Dark Angels
Dunghill
Daixin
DarkyLock
Delta
BabLock
RA Group
Cheers
Rook
NightSky
Bronze Starlight
Pandora
CatB
Gold Espresso
AvosLocker
Tropical Scorpius
Cuba
Decryption keys released
Wine Tempest
Crysis
Dharma
Details and relationship are unclear at this time.
V is Vendetta
Phobos
Wiki ransomware
Faust
Vandev
Xorist
CerberSysLock
EnCiPHeREd
Zixer2
Frozen
Large ransomware family including many variants based on the Encore Builder crypto constructor.
FakeRSA
TaRoNiS
Mcafee
Mcrypt2019
Makop
Nigg3r
MortalKombat
Mallox
Also named Fargo or TargetCompany
Partial decryptor released
Stop
DJVU
DJVU uses many different file-extensions.
Legend:
Threat Group/Author
Ransomware 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 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.
Cerber
CerberImposter
Pinchy Spider
GandCrab
REvil
REvil stops its operation after law enforcement's actions
BlogXX
Spectre
Gold Northfield
Ransom Cartel
LV
Chaos
Sold and distributed as a malware builder
Yashma
SolidBit
Imitates LockBit
Onyx
VSOP
BlackSnake
Carbon Spider
Former REvil and Maze affiliate
Probably active since 2012
Attribution still debated
DEV-0289
DarkSide
BlackMatter
Alpha Spider
BlackCat
Also named ALPHV
BlackCat 2.0
Vohuk
Cylance
DeathRansom
HelloKitty
Canthroid
FiveHands
RedAlert
Yanluowang
Leaked and doxxed
Scarab
Amnesia
Vice Society
Group that deploys several RaaS payloads, including HelloKitty and Zeppelin
PolyVice
BuddyRansome
Buransupport
VegaLocker
Rancoz
Zeppelin
Cryakl
CryLock
Trigona
Nosophoros
Jigsaw
Thanos
Sold and distributed as a malware builder
Abyss
CrossLock
Akira
Prometheus
Spook
Haron
Midas
Axxes
Riddle Spider
Avaddon
Shuts down of the operation
Money Message
Cactus
Epsilon Red
BlackCocaine
Colossus
Ako
Thunder X
Ranzy Locker
LokiLocker
BlackBit
MedusaLocker
Ransomware Blog
MedusaBlog
RTM Gang
Quoter
SunDawn
Read The Manual
Skeleton Spider
LockerGoga
MegaCortex
Decryptor released
Gold Lounge
ThunderCrypt
Lorenz
Paradise
Paradise 2.0
Decryptor released
Decryptor released
Code Source leaked
Rapture
https://t.me/learningnets