Created by Cyber Intelligence Group

Know your enemy. Defense leadership.®

History of ransomware group connections and transitions

Rev.2.09

This chart shows the connections between the major ransomware attack groups (*1) confirmed around the world, from multiple perspectives centered on "rebranding" (*2).

This reveals the background of many ransomware attack groups having some connections with each other. The influence of CONTI, BABUK source code leakage, group break up / takedown, etc. leads to the emergence of other new groups. On the other hand, in some cases, such as NIGHT SKY, the image of an attacker who belongs to a specific country emerges from the connection with groups around.

From the similarity of affiliates, it is possible that the absolute number of attackers may be smaller than generally reported.

(*1) Selected double extortion groups, related groups, and hot topic groups.
(*2) This chart is created by MBSD's own research and information published by various security vendors around the world.
Here is a list of references. https://www.mbsd.jp/research/20230201/WhitePaper/

~2015 2016 2017 2018 2019 2020 2021 2022 2023

A B C D E F G H I J

DEFRAY777 → RANSOM EXX

Confirmed cooperative activities with OSINT Corp. MEDUSA

AKO : Relationship between AKO and MEDUSA is pointed out sometimes, but AKO developer denied.

AKO → THUNDER X → RANZY LOCKER

EGREGOR : Relationship with PROLOCK is pointed out based on TTP and technical similarities.

PWNDLOCKER → PROLOCK

The actors are reportedly similar within those ransomware.

MAZE : It is believed to be the first ransomware group to employ double extortion.
It can be seen that attack groups with leak sites began to emerge starting with MAZE.

Their leak site is similar to BLACKMATTER's leak site.

CHACHA → MAZE → EGREGOR

SEKHMET

EGREGOR : It is considered as a variant of SEKHMET.

A person claiming to be the developer of these three, released a master key for decryption.

RAGNAR LOCKER

SUNCRYPT

MAZE, RAGNAR LOCKER, SUNCRYPT, and LOCKBIT were reportedly collaborating.

ROOK : It is pointed out they used BABUK's code.

ONYX : This ransomware reportedly developed based on CHAOS Ransomware Builder v4 (variant of CHAOS ransomware).

ONYX → VSOP

LOCKDATA : It is reportedly developed based on CHAOS ransomware.

LOCKDATA

BLACKSNAKE : It is reportedly developed based on CHAOS ransomware.

BLACKSNAKE

CHAOS → YASHMA → SOLIDBIT

The chat site is very similar to that of LOCKBIT.

SOLIDBIT : It is considered as a variant of YASHMA.

ATOMSILO

LOCKFILE

PANDORA → CATB (CATB99,BAXTOY)

CATB : Ransom notes are similar and relevance of the groups are pointed out.

ROOK → X00IXS

X001XS : It is pointed out that the content of the postings on the leak site is very similar to ROOK.

EMPEROR DRAGONFLY (involves DEV-0401 / BRONZE STARLIGHT) is reportedly behind this. It has been pointed out that there are similarities with those ransomware.

NIGHT SKY

NIGHT SKY : Possibly a fork of ROOK.

The method of posting the name of the victim organization in hidden letters on the leak site is similar.

CHEERS

CHEERS : It is pointed out that the CHEERSCRYPT ransomware was developed based on BABUK's code.

BIANLIAN

VASA LOCKER (BABY)

BABUK

PAYLOAD.BIN

DARK ANGELS → DUNGHILL

DAIXIN

RA GROUP

BABUK : Source code was leaked on a hacker forum in September 2021.

WHITERABBIT (MARIO) : It is pointed out that this group used the leaked BABUK.

ASTRO LOCKER : Considered to be a variant of BABUK.

GROOVE → RAMP

RAMP : It is pointed out that it is operated by the administrator of GROOVE.

GROOVE : Possibly ran by BLACKMATTER affiliates.

DAIXIN, NOKOYAWA, RA GROUP : It is pointed out that they used leaked BABUK's code. (Other; BABUK2023 (XVGV), CYLANCE, DATAF, LOCK4, MICHAELKORS, RTM, etc.)

These groups are recognized as franchise-type RaaS, because attack methods and hosting servers are similar or identical. In some cases, these groups are considered as a rebranded group due to code similarities.

KARMA is said to have started from JSWORM, and evolved through NEMTY, NEFILIM, OFFWHITE, TELEGRAM, FUSION, MILIHPEN, and GANGBANG ransomware.

MOUNT LOCKER

ASTRO (ASTRA)

XING

QUANTUM

DAGON : Code similarities with MOUNT LOCKER and QUANTUM have been pointed out.

DAGON

NOKOYAWA : It is similar to KARMA, and some says it is a rebranded group.

At the same timing, some of the same victims by SNATCH were posted on the leak site.

It has been pointed out that CONTI is collaborating with affiliates of HELLO KITTY, HIVE, BLACKCAT, AVOSLOCKER, and BABUK attack groups, by outsourcing some of its tasks.

CONTI : While it is generally recognized as a rebrand of RYUK, some consider it is a separate organization belonging to the same parent group.

JSWORM → NEMTY → NEFILIM → KARMA

HERMES → RYUK → CONTI

(Involvement : GRIM SPIDER)

(Involvement : DEV-0230、DEV-0193 (WIZARD SPYDER) etc.)

Sold on hacker forums since 2017. Multiple variants exist.

RYUK : It is pointed out that it was created based on the HERMES's code.

QUANTUM : It is pointed out that there are relationship within affiliates.

HIVE : At the same timing, same victims were posted on both leak sites. But HIVE denied any connection to CONTI.

At the same timing, same victims were posted on both leak sites.

Takedown in January 2023.

HIVE

PLAY

NOKOYAWA → NEVADA

At the same timing, same victims were posted on both leak sites.

DONUT

NEVADA : It is pointed out that a variant of RUST-based NOKOYAWA subspecies.

Leak site exists, but no exposure activity has been confirmed at this moment.

Possibly associated with HIVE's initial access broker.

It is pointed out attackers behind HIVE and NOKOYAWA are related each other. PLAY may be ran by the same attackers due to similar attack methods.

RANSOMHOUSE

Extortion group with confirmed ties to ransomware attack groups.

At the same timing, same victims were posted on both leak sites.

WHITERABBIT (MARIO)

(Involvement: FIN8)

RANSOMHOUSE : A case has been confirmed in which the URL of RANSOMHOUSE was included in a threatening letter created by WHITERABBIT.

AVOSLOCKER : It is pointed out that there are relationship within affiliates.

NB65 : Confirmed this ransomware was built from the leaked CONTI source code.

MONTI : May have used leaked CONTI source code or binaries.

NB65

MONTI

MONTI : MONTI posted DONUT LEAKS credentials on the leak site.

SILENT RANSOM GROUP : It is pointed out that some CONTI attackers launched it as a new group.

SILENT RANSOM GROUP

LAPSUS$: This group promotes RANSOMHOUSE on Telegram.

Presumed variant of the leaked CONTI source code.

PUTIN TEAM SCARECROW BLUESKY MEOW

BLACKBYTE : It could be the extortion department of CONTI.

DIAVOL : Similarities to CONTI have been observed.

EVEREST

BLACKBYTE : Similarities to EVEREST have been observed.

BLACKBYTE

(Involvement : HECAMEDE)

VICE SOCIETY : Reportedly used QUANTUM ransomware.

The decryption key and source code were released in the hacker forum on February 2023.

DIAVOL : Possibly using common infrastructure with KARAKURT.

DIAVOL

KARAKURT : It is said to be an extortion group when CONTI failed to encrypt.

KARAKURT

TOMMYLEAKS

SCHOOLBOYS

TOMMYLEAKS : Conversation with the victims points out a relationship with KARAKURT, and it is believed to be a branch of CONTI.

They are possibly a same group.

SCHOOLBOYS : It is reportedly used the leaked LOCKBIT3.0 ransomware builder.

They do not use ransomware, but confirmed some cooperation with other groups.

LAPSUS$

(Involvement : DEV-0537)

Possibly some IAB (Initial Access Broker) are the same.

HELLO KITTY (FIVE HANDS) : It is pointed out that there are relationship within affiliates.

HELLO KITTY (FIVE HANDS)

It is pointed out that there is a relationship with affiliates.

YANLUOWANG

YANLUOWANG : Prior to developing its own ransomware, it was reportedly using BABUK's Linux locker.

It is pointed out the relationship between Royal and Conti.

ZEON → ROYAL

(Involvement : DEV-0569)

BLACKSUIT

ROYAL : There is information that it was using BLACKCAT's tools before using its own encryption tool.

ZEON : Generates a ransom note very similar to CONTI.

VICE SOCIETY : The use of HELLO KITTY and ZEPPELIN ransomware has been pointed out.

There are also confirmed cases of extortion without using ransomware.

VICE SOCIETY

(Involvement : DEV-0832)

POLYVICE

REDALERT (N13V)

POLYVICE : It is considered to be VICE SOCIETY's own ransomware. The relationship with codes such as CHILY and SUNNYDAY is pointed out.

There are multiple variants deployed as RaaS.

VEGA → ZEPPELIN

ZEPPELIN : Among variants, outstanding damages have been confirmed.

VICESOCIETY : It is pointed out the use of BLACKCAT ransomware.

ALPHV (BLACKCAT) : It is pointed out the possibility that CONTI used BLACKCAT ransomware as one of the attacks.

ALPHV (BLACKCAT)

Involvement : NOBERUS

ALPHV (BLACKCAT) : It is confirmed the possibility of overlapping affiliates and the use of the same original data leakage tool. Pointed out that LOCKBIT and others are rebrands.

VICE SOCIETY : It is pointed out that they used variant of the REDALERT ransomware.

There are technical similarities in those ransomware.

BLACK BASTA : Similar to CONTI's payment site & leak site.

DARKSIDE → BLACKMATTER

Involvement of COREID (Involvement : FIN7 / CARBON SPIDER) is pointed out.

BLACK BASTA

LOCKBIT3.0 : Some members claim to have purchased the source code from BLACKCAT and BLACKMATTER.

It is pointed out the code diversion of CRYPTOWALL and CRYPTXXX.

CRYPTOMIX

It is pointed out that it is a variant of CRYPTOMIX.

It is pointed out that an attacker called DEV-0950 used CLOP ransomware.

CLOP

(Involvement : TA505, FIN7)

It is said to have existed since around 2007.

EVILCORP

LOCKBIT : To evade US sactions, some members of EVILCORP reportedly acted as LOCKBIT's affiliates.

LOCKBIT (ABCD)

MACAW LOCKER : To evade US sactions, it reportedly used EVILCORP.

LOCKBIT2.0 (LOCKBIT RED)

MACAW LOCKER

LOCKBIT : They diverted CONTI to LOCKBIT GREEN.

LOCKBIT3.0 (LOCKBIT BLACK)

BITPAYMER : It is said that EVILCORP was used in the attack.

CRYPTON

CRYPTON : Their leak site imitates LOCKBIT2.0, but no evidence of relationship or actual attack is confirmed.

BADLOCK : Integrated and effectively used BABUK, LOCKBIT2.0, and other group's technology and attack methodology.

BADLOCK (RORSCHACH)

BITPAYMER → DOPPELPAYMER → GRIEF → ENTROPY

WASTEDLOCKER : The ransom note is similar to BITPAYMER, and they reportedly used EVILCORP to evade US sactions.

WASTEDLOCKER → HADES → PHOENIX LOCKER

To evade sactions, some believe that EVILCORP rebranded PHOENIX LOCKER to PAYLOAD.BIN.

HARDBIT : Ransom notes and logo are similar, but the relationship is unknown. HARDBIT commented in the interview that they used LOCKBIT's ransom note.

BLOODY : It is pointed out that they used the leaked LOCKBIT 3.0 ransomware builder first in an actual attack.

BLOODY

HARDBIT

First appeared in October 2022, followed by 2.0 in November. While they claimed data theft, no leak site is confirmed.

LV : It is pointed out that the code and structure is similar to REVIL.

LV

ONEPERCENT

ERUPTION → ARCANE → SABBATH

(Involvement : UNC2190)

MY DECRYPTER (MAGNIBER) : It may be developed by the same engineer.

MY DECRYPTER (MAGNIBER)

It is pointed out that was using BLACKCAT ransomware. Re-activated in April 2022, after the takedown in July 2021.

CERBER → GANDCRAB → REVIL (SODINOKIBI)

(Involvement : DEV-0504)

ONEPERCENT : Relationship with REVIL, MAZE, and EGREGOR is pointed out.

RANSOM CARTEL

Technical relationship is pointed out.

8BASE

Leak site and ransom note similarities with RANSOMHOUSE is pointed out. Also pointed out diversion from PHOBOS ransomware.

DHARMA : It is pointed out that it was developed because its decryption key was leaked.

SYNACK → EL_COMETA

CRYSIS → DHARMA → PHOBOS

It has been confirmed that it was distributed and sold as RaaS on hacker forums, etc., and the source code was sold in 2020.

PHOBOS : It is pointed out that it was developed based on the DHARMA's code.

Announced as RaaS in 2019, and advertised on hacker forums. PHOBOS has many variants such as LIZARD, ISOS, DIKE, STEEL, ELBIE, etc.

HARON : There are similarities in ransom note and leak site.

AVADDON → HARON → MIDAS → AXXES

(Leak site was discovered, but the date of appearance is unknown)

Some pointed out similarities with VICE SOCIETY in TTP and attack industries. And some says it is a rebranded group.

LA PIOVRA RHYSIDA INC RANSOM

NOESCAPE MALAS

CYCLOPS → KNIGHT

SHADOW

Unknown relationship with the ransomware of the same name confirmed in 2021.

Using THANOS ransomware.

Both ransomware is highly similar, some pointing out re-branding possibility.

JIGSAW THANOS

They were developed by a Venezuelan cardiac surgeon.

PROMETHEUS → SPOOK

MAILTO → NETWALKER

LOKI LOCKER

It is pointed out that it is deployed as RaaS for some of their members.

BLACKBIT : Due to functional similarities, they are considered as a subspecies of LOKI LOCKER.

ESXIARGS

BLACKBIT

It is pointed out similarities with BABUK and LOCKBIT.

V IS VENDETTA : Confirmed its existence in sub-domain of CUBA in 2023. Vice-versa, there is an opinion that CUBA is a rebrand of V IS VENDETTA. Details and relationship are unclear at this time.

V IS VENDETTA

TRIGONA : Due to technical and TTP duplications, some indicated there may be a relationship with attack groups utilizing CRYLOCK.

TRIGONA

DARKBIT

Confirmed ransomware attacks, but possibly a hacktivist.

ABYSS

CRYKAL / CRYLOCK

N4UGHTYSEC

HITLER (AGL0BGVYCG)

ECHORAIX RANION SNATCH

At the same timing, some of the same victims by NOKOYAWA were posted on the leak site.

PYSA / MESPINOZA CUBA

RAGNAROK ROBBINHOOD

ARVINCLUB

It is pointed out that these ransomware is somewhat related each other.

PAY2KEY

BLACKSHADOW (SPECTRAL KITTEN)

NEBULA FONIX (XINOF) EXORCIST

SZ40

LORENZ BONACI GROUP HOLYGHOST

MALLOX (FARGO) NETWORM (N3TWORM)

BL4CKTOR COOMING PROJECT MBC

HELLBORN HOTARUS EP918 DARKRYPT

SUGAR QLOCKER SNAPMC BABYDUCK

While some question the claims of ransomware usage, samples written by PHP are confirmed.

STORMOUS BLACKMAGIC RADAR BULLY SPARTA

LILITH SHAOLEAKS OMEGA MINDWARE UNSAFE

QILIN (AGENDA) PROJECT RELIC ICEFIRE MOISHA

ENDURANCE CHILE LOCKER (ARCRYPTER)

INDEX (0–9, A - L)

8BASE	2022 - H
ABYSS	2023 - J
AKIRA	2023 - G
AKO	2020 - A
ALPHV (BLACKCAT)	2021 - F
ARCANE	2021 - H
ARVINCLUB	2019 - J
ASTRO (ASTRA)	2021 - C
ATOMSILO	2021 - A
AVADDON	2020 - H
AVOSLOCKER	2021 - D
AXXES	2022 - H
BABUK	2021 - B
BABUK2023 (XVGV)	2022 - C
BABYDUCK	2021 - J
BADLOCK (RORSCHACH)	2022 - G
BIANLIAN	2021 - B
BIG HEAD	2023 - G
BITPAYMER	2017 - G
BLACKTOR	2021 - J
BLACK BASTA	2022 - G
BLACKBIT	2022 - I
BLACKBYTE	2021 - E
BLACKMAGIC	2022 - J
BLACKMATTER	2021 - G
BLACKSHADOW (SPECTRAL KITTEN)	2020 - J
BLACKSNAKE	2023 - A
BLACKSUIT	2023 - I
BLOODY	2022 - H
BLUESKY	2022 - E
BONACI GROUP	2021 - J
BULLY	2022 - J
CACTUS	2023 - G
CATB (CATB99,BAXTOY)	2022 - A
CERBER	2016 - H
CHACHA	2019 - B
CHAOS	2021 - A
CHEERS	2022 - B
CHILE LOCKER (ARCRYPTER)	2022 - J
CHILY	2023 - F
CIPHERLOCKER	2023 - G
CLOP	2019 - G
CONTI	2019 - D
COOMING PROJECT	2021 - J
CRYKAL / CRYLOCK	2015 - J
CRYPTOMIX	2016 - G
CRYPTON	2017 - G
CRYPTOWALL	2017 - G
CRYPTXXX	2018 - G
CRYSIS	2016 - H
CUBA	2019 - J
CYCLOPS	2023 - I
CYLANCE	2022 - C
DAGON	2022 - C
DAIXIN	2022 - C
DARK ANGELS	2022 - B
DARKBIT	2023 - I
DARK POWER	2023 - G
DARKRACE	2023 - G
DARKRYPT	2021 - J
DARKSIDE	2020 - G
DATAF	2022 - C
DEFRAY777	2018 - A
DHARMA	2016 - H
DIAVOL	2021 - E
DIKE	2019 - H
DONUT	2022 - D
DOPPELPAYMER	2019 - G
DUNGHILL	2023 - B
ECHORAIX	2017 - J
EGREGOR	2020 - B
EL_COMETA	2021 - H
ELBIE	2020 - H
ENDURANCE	2022 - J
ENTROPY	2021 - G
EP918	2021 - J
ERUPTION	2020 - H
ESXIARGS	2022 - I
EVEREST	2020 - E
EVILCORP	2015 - G
EXORCIST	2020 - J
FONIX (XINOF)	2020 - J
FUSION	2017 - C
GANDCRAB	2018 - H
GANGBANG	2017 - C
GRIEF	2021 - G
GROOVE	2021 - C
HADES	2020 - H
HARDBIT	2022 - H
HARON	2021 - H
HELLBORN	2021 - J
HELLO KITTY (FIVE HANDS)	2020 - F
HERMES	2017 - D
HITLER (AGL0BGVYCG)	2016 - J
HIVE	2021 - D
HOLYGHOST	2021 - J
HOTARUS	2021 - J
ICEFIRE	2022 - J
INC RANSOM	2023 - H
ISOS	2019 - H
JIGSAW	2016 - I
JSWORM	2019 - D
KARAKURT	2021 - E
KARMA	2021 - D
KNIGHT	2023 - I
LA PIOVRA	2023 - H
LAPSUS$	2021 - E
LILITH	2022 - J
LIZARD	2019 - H
LOCK4	2023 - C
LOCKBIT (ABCD)	2019 - G
LOCKBIT2.0 (LOCKBIT RED)	2021 - G
LOCKBIT3.0 (LOCKBIT BLACK)	2022 - G
LOCKDATA	2022 - A
LOCKFILE	2021 - B
LOKI LOCKER	2021 - I
LORENZ	2021 - J
LV	2020 - H

INDEX (M - Z)

MACAW LOCKER	2021 - G
MAILTO	2019 - I
MALAS	2023 - I
MALLOX (FARGO)	2021 - J
MAZE	2019 - B
MBC	2021 - J
MEDUSA	2019 - A
MEOW	2022 - E
METAENCRYPTOR	2023 - G
MICHAELKORS	2023 - C
MIDAS	2021 - H
MILIHPEN	2017 - G
MINDWARE	2022 - J
MOISHA	2022 - J
MONTI	2022 - E
MONEY MESSAGE	2023 - G
MOSES STAFF	2021 - J
MOUNT LOCKER	2020 - C
MY DECRYPTER (MAGNIBER)	2017 - H
N4UGHTYSEC	2015 - J
NB65	2022 - D
NEBULA	2020 - J
NEFILIM	2020 - D
NEMTY	2019 - D
NETWALKER	2020 - I
NETWORM (N3TW0RM)	2021 - J
NEVADA	2022 - D
NIGHT SKY	2021 - B
NOESCAPE	2023 - I
NOKOYAWA	2022 - D
OFFWHITE	2019 - C
ONYX	2022 - A
OMEGA	2022 - J
ONEPERCENT	2020 - I
PANDORA	2022 - A
PAY2KEY	2020 - J
PAYLOAD.BIN	2021 - B
PHOBOS	2018 - H
PHOENIX LOCKER	2021 - H
PLAY	2022 - D
POLYVICE	2022 - F
PROJECT RELIC	2022 - J
PROLOCK	2020 - A
PROMETHEUS	2021 - I
PUTIN TEAM	2022 - E
PWNDLOCKER	2019 - A
PYSA / MESPINOZA	2019 - J
QILIN (AGENDA)	2022 - J
QLOCKER	2021 - J
QUANTUM	2021 - C
RADAR	2022 - J
RAGNAR LOCKER	2019 - B
RAGNAROK	2019 - J
RA GROUP	2023 - C
RAMP	2021 - C
RANSOM CARTEL	2021 - H
RANION	2017 - J
RANSOM EXX	2020 - A
RANZY LOCKER	2020 - A
REDALERT (N13V)	2022 - F
REVIL (SODINOKIBI)	2019 - H
RHYSIDA	2023 - H
ROBBINHOOD	2019 - J
ROOK	2021 - B
ROYAL	2022 - F
RTM	2023 - C
RYUK	2018 - D
SABBATH	2021 - H
SCARECROW	2022 - E
SCHOOLBOYS	2022 - E
SEKHMET	2020 - B
SHADOW	2023 - I
SHAOLEAKS	2022 - J
SILENT RANSOM GROUP	2022 - E
SNAPMC	2021 - J
SNATCH	2018 - J
SOLIDBIT	2022 - A
SPARTA	2021 - I
SPOOK	2021 - I
STEEL	2019 - H
STORMOUS	2022 - J
SUGAR	2021 - J
SUNCRYPT	2019 - B
SUNNYDAY	2023 - F
SYNACK	2017 - H
SZ40	2020 - J
TELEGRAM	2017 - C
THANOS	2019 - I
THUNDER X	2020 - A
TOMMYLEAKS	2022 - E
TRIGONA	2022 - I
UNSAFE	2022 - J
VASA LOCKER (BABY)	2020 - B
VEGA	2019 - F
V IS VENDETTA	2023 - I
VICE SOCIETY	2021 - F
VSOP	2022 - A
WASTEDLOCKER	2020 - H
WHITERABBIT (MARIO)	2021 - D
X001XS	2022 - B
XING	2021 - C
YANLUOWANG	2021 - F
YASHMA	2022 - A
ZEON	2022 - F
ZEPPELIN	2019 - F

Rebrand
Relationship

Confirmed Exposure Activities* (including base preparation)

* Fill Confirmed this is still active

- Has leak site
- Utilize hacker forums
- Utilize Telegram
- Not confirmed ransomware activity

No Exposure Activities* (or not confirmed)

* Fill Confirmed this is still active

Others*

* Fill Confirmed this is still active

三井物産セキュアディレクション株式会社
Mitsui Bussan Secure Directions, Inc.
https://www.mbsd.jp/ | @mbsdnews | Tokyo, JAPAN

SD22-103A - 2308