~2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024

Created by Cyber Intelligence Group

MBSD Know your enemy. Defense leadership.

History of ransomware group connections and transitions Rev.2.12

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/

Rebrand — Relationship

Confirmed Exposure Activities★ (incl. base prep.)

★ Fill Leak site is online in last 2 weeks

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

No Exposure Activities (or not confirmed)

Others

- ShadowSyndigate (Relationship appears across multiple groups, including possibility of IAB, affiliates, and others)
- Five Families (consists from ThreatSec, GhostSec, Stormous, Blackforums, and SiegedSec)
- Commonly used as a Precursor Malware -1 (QBOT)
- It is pointed out that there are common affiliates across groups -1 (Wazawaka and others)

DEFRAY777 → RANSOM EXX

Confirmed cooperative activities with OSINT Corp. MEDUSA

AKO → THUNDER X → RANZY LOCKER

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

PWNDLOCKER → PROLOCK

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

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.

The actors are reportedly similar within those ransomware.

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

CHACHA → MAZE → EGREGOR

SEKHMET

EGREGOR : It is considered as a variant of SEKHMET.

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

SUNCRYPT

RAGNAR LOCKER

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

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

VASA LOCKER (BABY)

Leak site was taken down on Oct. 19, 2023. Multiple countries cooperated and dismantled the group.

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

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

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.

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.

Sold on hacker forums since 2017. Multiple variants exist. HERMES

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

RYUK (Involvement : GRIM SPIDER)

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

JSWORM → NEMTY → NEFILIM → KARMA

ASTRO (ASTRA) : It is pointed out that there are relationship within affiliates.

MOUNT LOCKER → QUANTUM

ASTRO (ASTRA) XING

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

DAGON

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

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

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

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

WHITERABBIT MARIO

WHITERABBIT, MARIO : Cooperation with BIANLIAN was confirmed in ransomware attacks.

(Involvement: FIN8)

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.

CLOAK

GOOD DAY : Relationship is pointed out because the CLOAK's leak site URL appears in the ransom note.

GOOD DAY

ATOMSILO

LOCKFILE

ROOK

PANDORA

CATB (CATB99,BAXTOY)

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

X00IXS

X00IXS : It is pointed out that the content of the postings on the leak site is very similar to ROOK.

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.

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

BIANLIAN

BABUK

PAYLOAD.BIN

DARK ANGELS → DUNGHILL

DAIXIN

RA GROUP

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.)

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 is pointed out that Farnetwork, which is suspected to be related to JSWORM, is behind the scene.

Takedown in January 2023.In Nov., arrested attackers who used LOCKERGOGA, MEGACORTEX, and DHARMA in addition to HIVE.

NOKOYAWA → NEVADA

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.

PLAY

HIVE

HUNTERS INTERNATIONAL : The attack group is pointed out rebranding of HIVE ransomware because of its source code similarities, but they denied.

HUNTERS INTERNATIONAL

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

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

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

Extortion group with confirmed ties to ransomware attack groups.

DONUT

Possibly associated with ransomware group's initial access broker.

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

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

MONTI

It is pointed out that the presence of a common developer with BABUK.

NB65

SILENT RANSOM GROUP

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

The decryption key and source code were released in the hacker forum on February 2023.
The leak site was found on Nov. 2023.

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

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

AVOSLOCKER

PUTIN TEAM SCARECROW BLUESKY MEOW

Presumed variant of the leaked CONTI source code.

RANSOMED.VC : Cooperative relationship with EVEREST is pointed out.

BLACKBYTE : Similarities to EVEREST have been observed.

EVEREST

STORMOUS

RANSOMED.VC : They expressed STORMOUS as a partner.

SIEGEDSEC

Announced dissolution in Oct. 2023. Then they hinted resuming activities under a new name in Dec.

RANSOMED.VC → RAZNATOVIC

RANSOMCORP

Though the specific activity start date was uncertain, the leak site was found in 2023.

RANSOMCORP : Some indicated there may be a relationship with RANSOMED.VC.

SIEGEDSEC : A connection to the operational base of RANSOMED.VC is pointed out.

The leak site was launched in Dec. 2023. Soon after, it was taken down by the hacktivist group "D7BBUK".

BLACKBYTE : It could be the extortion department of CONTI.

DIAVOL : Similarities to CONTI have been observed.

DIAVOL : Possibly using common infrastructure with KARAKURT.

DIAVOL BLACKBYTE

(Involvement : HECAMEDE)

While some question the claims of ransomware usage, samples written by PHP are confirmed. Also confirmed they expressed RANSOMED.VC as a partner.

KARAKURT

TOMMYLEAKS SCHOOLBOYS

They are possibly a same group.

LAPSUS$: This group promotes RANSOMHOUSE on Telegram.

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

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

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

ZEON : Generates a ransom note very similar to CONTI.

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.

It is pointed out that the relationship between Royal and Conti.

ZEON ROYAL

(Involvement : DEV-0569)

BLACKSUIT

Reuse of DeathRansom and ABYSS is pointed out. An individual believed to be the developer released the source code on a hacker forum in Oct. 2023.

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

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

YANLUOWANG

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

BLACKSUIT : Pointed out similarities with ROYAL in Linux sample.

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

HELLO KITTY (FIVE HANDS)

There are also confirmed cases of extortion without using ransomware.

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

VICE SOCIETY

(Involvement : DEV-0832)

REDALERT (N13V)

POLYVICE

VICESOCIETY : Reportedly used QUANTUM ransomware.

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

VEGA → ZEPPELIN

There are multiple variants deployed as RaaS.

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

ALPHV (BLACKCAT)

(Involvement : NOBERUS)

The website was taken down by FBI on Dec. 19, 2023, followed by officially announcement. But, it was immediately rewritten by AlphV stating activities will continue.

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

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

ZEPPELIN : Among variants, outstanding damages have been confirmed.

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

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.

Ralationship with REVIL is pointed out due to similarity of the ransomware.

DARKSIDE → BLACKMATTER

There are technical similarities in those ransomware.

BLACK BASTA

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

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

EVILCORP

It is said to have existed since around 2007.

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)

THREEAM : Confirmed usage after LOCKBIT exploit failure. Affiliates maybe belong both.

THREEAM

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

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

BADLOCK (RORSCHACH)

WEREWOLVES

Soon after WEREWOLVES appeared, they posted victims overlapping with LOCKBIT and QILIN, hinting some connections.

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.

BITPAYMER → DOPPELPAYMER → GRIEF → ENTROPY

QILIN (AGENDA)

BLOODY

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

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.

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

LV

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.

ONEPERCENT → ERUPTION → ARCANE → SABBATH

(Involvement : UNC2190)

GANDCRAB → REVIL (SODINOKIBI)

(Involvement : DEV-0504)

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

RANSOM CARTEL : Technical relationship is pointed out.

RANSOM CARTEL

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

HARDBIT

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

SAMSAM CERBER SPARTACUS

It is pointed out that there are common TA.

They temporarily suspended its activities, but new specimens appeared, exploiting CVE-2021-26084 / CVE-2021-22205 in Dec. 2021, CVE-2022-26134 in Jun. 2022, and CVE-2023-22518 in Nov. 2023.

AVADDON → HARON → HARON → MIDAS → AXXES

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

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

NOESCAPE

Termination was declared and closed leak site in Dec. 2023. Affiliates claimed NOESCAPE operators absconded with money stolen from victims.

JIGSAW THANOS

Using THANOS ransomware.

PROMETHEUS → SPOOK

They were developed by a Venezuelan cardiac surgeon.

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

It is pointed out similarities with BABUK and LOCKBIT.

CYCLOPS → KNIGHT

CRYSIS → DHARMA → PHOBOS

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

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.

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

8BASE

CRYPTBB : Connection is pointed out due to the similarity of leak site and the duplication of victim list.

CRYPTBB

Diversion of LOCKBIT3.0 (LOCKBIT BLACK) is pointed out.

CRYKAL / CRYLOCK

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

TRIGONA

Ukrainian Cyber Alliance (pro-Ukrainian hacktivist group) took down TRIGONA's leak site in Oct. 2023.

CUBA

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

SHADOW

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

N4UGHTYSEC

HITLER (AGL0BGVYCG)

ECHORAIX RANION SNATCH

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

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

PAY2KEY → BLACKSHADOW (SPECTRAL KITTEN)

PYSA / MESPINOZA

RAGNAROK ROBBINHOOD

ARVINCLUB

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

CRYPTOMIX

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

CLOP

(Involvement : TA505, FIN7, FIN11)

MAILTO → NETWALKER

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

NEBULA FONIX (XINOF) EXORCIST

MALLOX (FARGO) NETWORM (N3TW0RM)

BL4CKTOR COOMING PROJECT MBC

HELLBORN HOTARUS EP918 DARKRYPT

SUGAR QLOCKER SNAPMC BABYDUCK

BONACI GROUP HOLYGHOST

MINDWARE BLACKMAGIC RADAR BULLY

LILITH SHAOLEAKS OMEGA UNSAFE SPARTA

ENDURANCE PROJECT RELIC ICEFIRE MOISHA

CHILE LOCKER (ARCRYPTER) ESXIARGS

It is pointed out that DanaBot is used as a deployment method is.

ABYSS AKIRA BLACKDOLPHIN RANCOZ

INC RANSOM DARKRACE BIG HEAD DARKBIT

Confirmed ransomware attacks, but possibly a hacktivist.

MONEY MESSAGE CIPHERLOCKER DARK POWER

CACTUS METAENCRYPTOR → LOSTTRUST

(Including possibility of being active before 2022 from the posted information on the leak site.)

DRAGON FORCE CIPHBIT CRYPTNET MALAS

LA PIOVRA RHYSIDA

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

SYNACK → EL_COMETA

MEGACORTEX

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

LOKI LOCKER → BLACKBIT

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

SZ40 → LORENZ

GHOSTSEC

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

Ransomware with the same name existed in 2021, but the relationship is unclear.

LAMBDA MADCAT MALEKTEAM

INDEX (0–9, A - K)	
8BASE	2022 - I
ABYSS	2023 - K
AKIRA	2023 - K
AKO	2020 - A
ALPHV (BLACKCAT)	2021 - F
ARCANE	2021 - H
ARVINCLUB	2019 - K
ASTRO (ASTRA)	2021 - C
ATOMSILO	2021 - A
AVADDON	2020 - I
AVOSLOCKER	2021 - D
AXXES	2022 - I
BABUK	2021 - B
BABUK2023 (XVGV)	2022 - C
BABYDUCK	2021 - K
BADLOCK (RORSCHACH)	2022 - G
BIANLIAN	2021 - B
BIG HEAD	2023 - K
BITPAYMER	2017 - H
BL4CKTOR	2021 - K
BLACK BASTA	2022 - G
BLACKBIT	2022 - L
BLACKBYTE	2021 - E
BLACKDOLPHIN	2023 - K
BLACKMAGIC	2022 - K
BLACKMATTER	2021 - G
BLACKSHADOW (SPECTRAL KITTEN)	2020 - J
BLACKSNAKE	2023 - A
BLACKSUIT	2023 - F
BLOODY	2022 - H
BLUESKY	2022 - E
BONACI GROUP	2021 - K
BULLY	2022 - K
CACTUS	2023 - K
CATB (CATB99,BAXTOY)	2022 - A
CERBER	2016 - I
CHACHA	2019 - B
CHAOS	2021 - A
CHEERS	2022 - B
CHILE LOCKER (ARCRYPTER)	2022 - K
CHILY	2023 - G
CIPHBIT	2023 - L
CIPHERLOCKER	2023 - K
CLOAK	2023 - A
CLOP	2019 - K
CONTI	2019 - D
COOMING PROJECT	2021 - K
CRYKAL / CRYLOCK	2015 - J
CRYPTBB	2023 - I
CRYPTNET	2023 - L
CRYPTOMIX	2016 - K
CRYPTON	2017 - H
CRYPTOWALL	2017 - K
CRYPTXXX	2017 - K
CRYSIS	2016 - I
CUBA	2019 - J
CYCLOPS	2023 - I
CYLANCE	2023 - C
DAGON	2022 - C
DAIXIN	2021 - H
DARK ANGELS	2022 - B
DARKBIT	2023 - K
DARK POWER	2023 - K
DARKRACE	2023 - K
DARKRYPT	2021 - K
DARKSIDE	2020 - G
DATAF	2023 - C
DEFRAY777	2018 - A
DEATHRANSOM	2018 - F
DHARMA	2016 - I
DIAVOL	2021 - E
DIKE	2019 - I
DONUT	2022 - D
DORPELPAYMER	2019 - H
DRAGON FORCE	2023 - L
DUNGHILL	2023 - B
ECH0RAIX	2017 - J
EGREGOR	2020 - B
EL_COMETA	2021 - L
ELBIE	2019 - I
ENDURANCE	2022 - K
ENTROPY	2021 - H
EP918	2021 - K
ERUPTION	2020 - H
ESXIARGS	2022 - K
EVEREST	2020 - E
EVILCORP	2015 - G
EXORCIST	2020 - K
FONIX (XINOF)	2020 - K
FUSION	2017 - C
GANDCRAB	2018 - H
GANGBANG	2018 - C
GHOSTSEC	2022 - L
GOOD DAY	2023 - B
GRIEF	2021 - H
GROOVE	2021 - C
HADES	2020 - H
HARDBIT	2022 - H
HARON	2021 - I
HELLBORN	2021 - K
HELLO KITTY (FIVE HANDS)	2020 - F
HERMES	2017 - D
HITLER (AGL0BGVYCG)	2016 - J
HIVE	2021 - D
HOLYGHOST	2021 - K
HOTARUS	2021 - K
HUNTERS INTERNATIONAL	2023 - D
ICEFIRE	2022 - K
INC RANSOM	2023 - K
ISOS	2019 - I
JIGSAW	2016 - I
JSWORM	2019 - D
KARAKURT	2021 - E
KARMA	2021 - D
KNIGHT	2023 - I

INDEX (L - Z)	
LAMBDA	2023 - L
LA PIOVRA	2023 - L
LAPSUS$	2021 - F
LILITH	2022 - K
LIZARD	2019 - I
LOCK4	2023 - C
LOCKBIT (ABCD)	2019 - G
LOCKBIT2.0 (LOCKBIT RED)	2021 - G
LOCKBIT3.0 (LOCKBIT BLACK)	2022 - G
LOCKDATA	2022 - A
LOCKERGOGA	2022 - C
LOCKFILE	2021 - B
LOKI LOCKER	2021 - L
LORENZ	2022 - C
LV	2020 - H
MACAW LOCKER	2021 - G
MADCAT	2023 - L
MAILTO	2019 - K
MALAS	2023 - L
MALEKTEAM	2023 - L
MALLOX (FARGO)	2021 - K
MARIO	2021 - D
MAZE	2019 - B
MBC	2021 - K
MEGACORTEX	2019 - E
MEOW	2022 - E
METAENCRYPTOR	2023 - K
MICHAELKORS	2023 - C
MIDAS	2021 - I
MILIHPEN	2018 - C
MINDWARE	2022 - K
MOISHA	2022 - K
MONEY MESSAGE	2023 - K
MOUNT LOCKER	2020 - C
MY DECRYPTER (MAGNIBER)	2017 - H
N4UGHTYSEC	2015 - J
NB65	2022 - D
NEBULA	2020 - K
NEFILIM	2020 - D
NEMTY	2019 - D
NETWALKER	2020 - K
NETWORM (N3TW0RM)	2021 - K
NEVADA	2022 - D
NIGHT SKY	2021 - B
NOESCAPE	2023 - I
NOKOYAWA	2022 - D
ONYX	2022 - A
OMEGA	2022 - K
ONEPERCENT	2020 - H
P0PEYE	2022 - A
PANDORA	2019 - G
PAYLOAD.BIN	2021 - B
PAY2KEY	2020 - A
PHOBOS	2018 - I
PHOENIX LOCKER	2020 - A
PLAY	2022 - D
POLYVICE	2022 - F
PROJECT RELIC	2022 - K
PROLOCK	2020 - A
PROMETHEUS	2021 - I
PUTIN TEAM	2022 - E
PWNDLOCKER	2019 - A
PYSA / MESPINOZA	2019 - K
QILIN (AGENDA)	2022 - H
QLOCKER	2021 - K
QUANTUM	2021 - C
RADAR	2022 - K
RAGNAR LOCKER	2019 - B
RAGNAROK	2019 - H
RA GROUP	2023 - C
RAMP	2021 - C
RANCOZ	2023 - K
RANSOM EXX	2020 - A
RANSOMHOUSE	2021 - D
RANSOMED.VC	2023 - E
RANZY LOCKER	2020 - A
RAZNATOVIC	2023 - E
REDALERT (N13V)	2021 - D
REVIL (SODINOKIBI)	2019 - H
RHYSIDA	2023 - L
ROBBINHOOD	2020 - A
ROOK	2021 - B
ROYAL	2022 - F
RTM	2021 - C
RYUK	2018 - D
SABBATH	2021 - H
SAMSAM	2015 - I
SCARECROW	2022 - E
SCHOOLBOYS	2022 - E
SEKHMET	2020 - B
SHADOW	2023 - J
SHAOLEAKS	2022 - K
SIEGEDSEC	2022 - E
SILENT RANSOM GROUP	2022 - E
SNAPMC	2021 - K
SNATCH	2018 - J
SOLIDBIT	2022 - A
SPARTA	2022 - K
SPARTACUS	2018 - I
SPOOK	2021 - I
STEEL	2019 - I
STORMOUS	2021 - E
SUGAR	2021 - K
SUNCRYPT	2019 - B
SUNNYDAY	2023 - G
SYNACK	2017 - L
SZ40	2020 - L
TELEGRAM	2017 - C
THANOS	2019 - I
THREEAM	2023 - G
THUNDER X	2020 - A
TOMMYLEAKS	2022 - E
TRIGONA	2022 - J
UNSAFE	2022 - K
VASA LOCKER (BABY)	2020 - B
VEGA	2019 - F
V IS VENDETTA	2023 - J
VICE SOCIETY	2021 - F
VSOP	2022 - A
WASTEDLOCKER	2020 - H
WEREWOLVES	2023 - H
WHITERABBIT	2021 - D
X00IXS	2022 - B
XING	2021 - C
YANLUOWANG	2021 - F
YASHMA	2022 - A

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

SD22-103D - 2312