Created by Cyber Intelligence Group

MBSD Know your enemy. Defense leadership.

ランサムウェア／攻撃グループの変遷と繋がり Rev.2.11

本図は世界で確認されてきた主なランサムウェア攻撃グループ(※1)のうち、「リブランド」を軸とした複合的視点による組織間の繋がりを図示したものである(※2)。

ランサムウェア攻撃グループの多くがお互いに何からの関連性を持ち活動している背景が浮かび上がる。CONTIやBABUKをはじめソースコードの流出やグループの解散／テイクダウンなどの影響が他の新種出現へ顕著に繋がる流れが見て取れる。一方、NIGHT SKYなどのように、周辺グループとの繋がりから特定国に帰属する攻撃者像が浮き上がってくるケースもある。

全体を通して見え隠れするアフィリエイトの共通性などから、ランサムウェア攻撃グループの表面的な組織数とは裏腹に、背後にいる攻撃者らの絶対数は一般に想像されるよりも少ない可能性などもここから推測できるだろう。

(※1) 暴露型や話題性の高いグループを選抜。攻撃グループが使用するランサムウェアの名称も一部含む。
(※2) MBSDの独自調査の他、世界各国の様々なセキュリティーベンダーの公開／発信情報を元に作成。
参照記事一覧はこちらに掲載：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
OSINT Corpとの活動連携を確認している。
MEDUSA
AKO：一部でAKOとMEDUSAの関係性が指摘されているがAKOの開発者は否定。
AKO → THUNDER X → RANZY LOCKER
EGREGOR：PROLOCKとのTTPや技術的な類似性から関係性が指摘。
PWNDLOCKER → PROLOCK
MAZE：初めて二重恐喝を採用したランサムウェアグループとされている。
MAZEを皮切りにリークサイトを持つ攻撃グループが出現し始めたことがわかる。
CHACHA → MAZE → EGREGOR
SEKHMET
EGREGOR：SEKHMETの亜種とされている。
RAGNAR LOCKER
これら3つの開発者であると自称する人物が復号のためのマスターキーとするものを公開。
SUNCRYPT
MAZE、RAGNAR LOCKER、SUNCRYPT、LOCKBITが協業していたとされる。
VASA LOCKER (BABY)
BABUK：2021年9月にソースコードがハッカーフォーラムでリークされた。
WHITERABBIT (MARIO)：流出したBABUKを使用したと指摘。
ASTRO LOCKER：BABUKのフォークとされている。
攻撃手法や、ホスティングサーバーの類似／同一性からフランチャイズ型のRaaSとして認識されているケースの他、コード上に類似点が見られるとし、各ブランドを一つのグループのリブランドとして扱うケースもある。
KARMAはJSWORMランサムウェアから進化したとされ、NEMTY、NEFILIM、OFFWHITE、TELEGRAM、FUSION、MILIHPEN、GANGBANGランサムウェアを経てKARAMAランサムウェアに至ったとされる。
CONTIはタスクの一部を外部委託するという形でHELLO KITTY、HIVE、BLACKCAT、AVOSLOCKER、BABUKのアフィリエイトなどの攻撃グループと連携しているという見解もある。
CONTI：RYUKのリブランドと一般認識される一方、同じ母体グループに属す別組織という見解もある。
HERMES
2017年からハッカーフォーラムで販売。亜種が複数存在する。
RYUK：HERMESのコードをベースに作成されたと指摘。
RYUK (関与：GRIM SPIDER)
(関与：DEV-0230、DEV-0193 (WIZARD SPYDER) etc.)
JSWORM → NEMTY → NEFILIM → KARMA
CONTI
MOUNT LOCKER → QUANTUM
QUANTUM：アフィリエイトに関係性があることが指摘。
HIVE：HIVE同時期に一部共通の被害組織をリークサイトに掲載。HIVEはCONTIとの関係性を否定。
ONYX：使用するランサムウェアがChaos Ransomware Builder v4をベースにしている(CHAOSランサムウェアの亜種)との指摘。
ONYX → VSOP
LOCKDATA：CHAOSランサムウェアを元に開発されたと指摘。
LOCKDATA
BLACKSNAKE：CHAOSランサムウェアを元に開発されたと指摘。
BLACKSNAKE
CHAOS → YASHMA → SOLIDBIT
チャットサイトがLOCKBITのものと酷似している。
SOLIDBIT：YASHMAの亜種とされている。
使用アクターに関係性。
ATOMSILO
LOCKFILE
BLACKMATTERのリークサイトとの類似。
PANDORA → CATB (CATB99,BAXTOY)
CATB：骨迅文に類似性があり関連性が指摘。
CLOAK
GOOD DAY：身代金メモにCLOAKのリークサイトURLが記載されていることから関係性が指摘。
GOOD DAY
ROOK：BABUKのコードを流用したと指摘。
ROOK
X001XS
X001XS：リークサイトの投稿がROOKと酷似。
NIGHT SKY
NIGHT SKY：ROOKのフォークである可能性。
CHEERS
EMPEROR DRAGONFLY (関与：DEV-0401 / BRONZE STARLIGHT) が背後にいるとされる。使用するランサムウェアに共通点があるとの指摘。
リークサイトに被害組織名を当初伏せ字で掲載する手口が類似。
CHEERS：使用するランサムウェアCHEERSCRYPTはBABUKのコードを元に開発されたと指摘。
BIANLIAN
BABUK
PAYLOAD.BIN
DARK ANGELS → DUNGHILL
DAIXIN
RA GROUP
DAIXIN, NOKOYAWA, RA GROUP：BABUK流出コードを流用との指摘あり。(その他：BABUK2023 (XVGV)、CYLANCE、DATAF、LOCK4、MICHAELKORS、RTM, etc.)
GROOVE → RAMP
RAMP：GROOVEの管理者が運営していると指摘。
GROOVE：BLACKMATTERのアフィリエイトであった可能性。
DAGON：MOUNT LOCKER、QUANTUMとコードの類似性が指摘。
ASTRO (ASTRA)
XING
DAGON
NOKOYAWA：使用するランサムウェアに類似点があるとされ、リブランドであるという見解もある。
同時期にSNATCHと一部共通の被害組織をリークサイトに掲載。
NEVADA：RUSTベースであるNOKOYAWA亜種の変種であると指摘。
NOKOYAWA
NEVADA
リークサイトが用意されているが現在で目立った暴露活動が確認されていない。
PLAY
2023年1月にテイクダウン。
HIVE
同時期に一部共通の被害組織をリークサイトに掲載。
同時期に一部共通の被害組織をリークサイトに掲載。
DONUT
ランサムウェアグループと関係がある初期アクセスブローカーの可能性。
HIVE、NOKOYAWAは背後にいる攻撃者に関係性があると指摘されており、PLAYは攻撃手法の類似という点から同一の攻撃者が扱っている可能性。
RANSOMHOUSE
ランサムウェア攻撃グループとの関係性が確認されている恐喝グループ。
RANSOMHOUSE：WHITERABBITが作成した骨迅文にRANSOMHOUSEのURLが記載されていたケースが確認されている。
同時期に一部共通の被害組織をリークサイトに掲載。
WHITERABBIT (MARIO)
(関与：FIN8)
AVOSLOCKER：アフィリエイトに関係性があることが指摘。
NB65：流出したCONTIのソースコードからビルドしたランサムウェアを使用したことが確認された。
NB65 → MONTI
MONTI：流出したCONTIのソースコードまたはバイナリを流用した可能性。
MONTI：DONUT LEAKSの認証情報を自身のリークサイトに掲載。
LAPSUSS：TelegramでRANSOMHOUSEを宣伝。
VICESOCIETY：QUANTUMランサムウェアを使用したとされる。
2023年2月にハッカーフォーラムで復号鍵やソースコード等が公開。
SILENT RANSOM GROUP：CONTIの一部攻撃者が新規グループとして立ち上げたと指摘。
SILENT RANSOM GROUP
BLACKBYTE：CONTIの恐喝部門である可能性。
流出したCONTIランサムウェアのソースコードを流用したとされる。
PUTIN TEAM
SCARECROW
BLUESKY
MEOW
DIAVOL：使用するランサムウェアにCONTIとの類似点が確認されている。
EVEREST
BLACKBYTE：使用するランサムウェアの類似点から関係性が指摘。
BLACKBYTE (関与：HECAMEDE)
EVERESTとの協力関係にあることが指摘。STORMOUSがパートナーと表現。
RANSOMED.VC
DIAVOL：KARAKURTと共通のインフラを使用していたとされる。
DIAVOL
KARAKURT：CONTIが暗号化に失敗した時に横流しされる恐喝グループとして関わりがあるとされる。
KARAKURT
TOMMYLEAKS
SCHOOLBOYS
TOMMYLEAKS：被害組織との会話内容からKARAKURTとの関係性が指摘されており、CONTI分派であると考えられている。
同一グループであると指摘。
SCHOOLBOYS：流出したLOCKBIT3.0ランサムウェアのビルダーを使用したと指摘。
(リークサイトの掲載情報より2022年以前から活動していると可能性も含む。)
ランサムウェアを使用しない恐喝グループだが、ランサムウェア攻撃グループへの協力が一部確認されている。
LAPSUS$ (関与：DEV-0537)
初期アクセスブローカーの一部が共通している可能性。
HELLO KITTY (FIVE HANDS)：アフィリエイトに関係性があることが指摘。
HELLO KITTY (FIVE HANDS)
YANLUOWANG
YANLUOWANG：独自のランサムウェア開発以前は、BABUKの Linux ロッカーを使用していたと指摘。
アフィリエイトに関係性があることが指摘。
ZEON：CONTIと非常によく似た身代金メモを生成。
ZEON → ROYAL (関与：DEV-0569)
RoyalとContiの関係性も一部で指摘。
METAENCRYPTOR → LOSTTRUST
BLACKSUIT
ランサムウェアを使用せず恐喝のみを行うケースも確認されている。
VICE SOCIETY：HELLO KITTY及びZEPPELINランサムウェアの使用が指摘。
VICE SOCIETY (関与：DEV-0832)
POLYVICE
BLACKSUIT：Linux用検体においてROYALとの類似性が指摘。
RaaSとして展開され亜種が複数存在。
VEGA → ZEPPELIN
ZEPPELIN：亜種の中でも特に目立った被害が確認されている。
VICESOCIETY：BLACKCATランサムウェアの使用が指摘。
VICE SOCIETY：REDALERTランサムウェアの亜種を使用していたことが指摘。
REDALERT (N13V)
ALPHV (BLACKCAT)：CONTIが攻撃の一つとしてBLACKCATランサムウェアを使用していた可能性が指摘。
ALPHV (BLACKCAT) (関与：NOBERUS)
ALPHV (BLACKCAT)：アフィリエイトが重なる可能性、同じ独自データ流出ツールの使用も確認。LOCKBIT等がリブランドであると指摘。
ROYAL：独自の暗号化ツールを使用する前はBLACKCATのものを使用していたとの情報あり。
BLACK BASTA：CONTIの支払いサイト&リークサイトに類似性あり。
使用するランサムウェアの類似性からREVILとの関係性が指摘。
DARKSIDE → BLACKMATTER
使用するランサムウェアに技術的な類似点が存在。
COREID (関与:FIN7 / CARBON SPIDER)の関与が指摘。
BLACK BASTA
LOCKBITの展開失敗後、代替手段での使用を確認。アフィリエイトが共通する可能性。
VICE SOCIETYは背後にいるとされる。「CHILY」や「SUNNYDAY」等のコードとの関係性が指摘。
LOCKBIT3.0：BLACKCATとBLACKMATTERからソースコードを購入したと主張。
CRYPTOWALLとCRYPTXXXのコード流用が指摘。
CRYPTOMIX
CRYPTOMIXの亜種であると指摘。
DEV-0950と呼ばれる攻撃者がCLOPランサムウェアを使用したと指摘。
CLOP (関与：TA505, FIN7, FIN11)
2007年頃から存在したと言われている。
EVILCORP
LOCKBIT：米国の制裁を回避するためにEVILCORPの一部メンバーがLOCKBITアフィリエイトとして活動したとされる。
LOCKBIT (ABCD)
MACAW LOCKER：米国の制裁を回避するためにEVILCORPが使用したとされる。
LOCKBIT2.0 (LOCKBIT RED)
MACAW LOCKER
LOCKBIT：CONTIをLOCKBIT GREENへ流用。
LOCKBIT3.0 (LOCKBIT BLACK)
BIG HEAD
CIPHERLOCKER
AKIRA
MONEY MESSAGE
CACTUS
BITPAYMER：EVILCORPが攻撃に使用したとされる。
CRYPTON
CRYPTON：LOCKBIT2.0のリークサイトを模倣しているとされているが、関係性や実攻撃の証跡は確認されていない。
BADLOCK：BABUK／LOCKBIT2.0／その他グループの技術や手口を効果的に統合し流用。
BADLOCK (RORSCHACH)
THREEAM
DARK POWER
DARKRACE
BITPAYMER
DOPPELPAYMER
GRIEF → ENTROPY
EVILCORPが制裁を回避するためにPHOENIX LOACKERをPAYLOAD.BINにブランド変更してリリースしたとの見解あり。
WASTEDLOCKER：身代金メモなどに類似性ありとされ、EVILCORPが米国の制裁を回避するために使用したとされる。
WASTEDLOCKER → HADES → PHOENIX LOCKER
BLOODY：流出したLOCKBIT3.0ランサムウェアのビルダーを最初に実際の攻撃へ使用したと指摘。
BLOODY
HARDBIT
HARDBIT：骨迅文とロゴに類似性が見られるが関係性は不明。HARDBITはインタビューに対しLOCKBITの骨迅文を流用したという趣旨のコメントをしている。
10月に出現、11月に2.0がリリース。データ窃取を主張する一方リークサイト等は確認されていない。
MY DECRYPTER (MAGNIBER)：開発者が同一である可能性。
MY DECRYPTER (MAGNIBER)
LV：REVILとコードの構造が類似すると指摘。
LV
ONEPERCENT
ERUPTION
ARCANE → SABBATH (関与：UNC2190)
BLACKCATランサムウェアを使用していたと指摘。2021年7月にテイクダウンされたが2022年4月に活動再開。
CERBER
GANDCRAB
REVIL (SODINOKIBI) (関与：DEV-0504)
ONEPERCENT：REVIL、MAZE、EGREGORとの関係性が指摘。
技術面で関係性。
RANSOM CARTEL
LOCKBIT3.0 (LOCKBIT BLACK)の流用が指摘。
CRYPTBB
CRYPTBB：リークサイトの類似性や掲載された一部被害組織名の重複から背後にある関係性が指摘。
8BASE
リークサイトや身代金メモ等におけるRANSOMHOUSEとの類似性、PHOBOSランサムウェアの流用が指摘。
DHARMA：CRYSISの復号キーの漏洩により開発されたと指摘。
SYNACK
EL_COMETA
TTPや攻撃対象業種等においてVICE SOCIETYと類似性が指摘され、一部ではリブランドであるとの見方もある。
CRYSIS → DHARMA → PHOBOS
ハッカーフォーラム等で当時RaaSとして配布&販売、2020年にはソースコードが販売されていたことも確認された。
PHOBOS：DHARMAのコードをベースに開発されたと指摘。
2019年からRaaSを発表しハッカーフォーラム等で宣伝。PHOBOS自体も亜種が多数存在し、LIZARD、ISOS、DIKE、STEEL、ELBIEなどはPHOBOSランサムウェア亜種の一部とされる。
AVADDON
骨迅文やリークサイトに類似性。
HARON → MIDAS → AXXES
(リークサイトの発見であり出現時期は不明)
LA PIOVRA
RHYSIDA
INC RANSOM
NOESCAPE
MALAS
CRYPTNET
JIGSAW
THANOS
THANOSランサムウェアを使用。
使用するランサムウェアに高い類似性が見られ、リブランドの可能性が指摘。
PROMETHEUS → SPOOK
ESXIARGS
一部ではBABUK、LOCKBITとの類似性も指摘。
CYCLOPS → KNIGHT
CIPHBIT
ペネズエラの心臓外科医によって開発。
MAILTO → NETWALKER
BLACKBIT
2021年確認の同名ランサムウェアとの関係性は不明。
SHADOW
BLACKDOLPHIN
RANCOZ
一部の会員向けにRaaSとして展開されているとの見解あり。
LOKI LOCKER
BLACKBIT：機能の類似性からLOKI LOCKERの亜種とされる。
HOLYGHOST
V IS VENDETTA：CUBAのサブドメインに存在することが2023年に確認された。(逆に CUBAが V IS VENDETTAのリブランドであるとの見解もあり現時点で詳細や関係性は不透明)
V IS VENDETTA
TRIGONA：技術面やTTPの重複等からCRYLOCKを用いる攻撃グループとの関係性が一部で指摘。
TRIGONA
ランサムウェアの使用が確認されているがハクティビストの可能性あり。
ABYSS
DARKBIT
CRYKAL / CRYLOCK
N4UGHTYSEC
HITLER (AGL0BGVYCG)
ECHORAIX
RANION
SNATCH
同時期にNOKOYAWAと一部共通の被害組織をリークサイトに掲載。
PYSA / MESPINOZA
CUBA
RAGNAROK
ROBBINHOOD
ARVINCLUB
使用するランサムウェアに関係性。
PAY2KEY
BLACKSHADOW (SPECTRAL KITTEN)
NEBULA
FONIX (XINOF)
EXORCIST
SZ40
LORENZ
BONACI GROUP
STORMOUS
ランサムウェア使用の主張を疑問視する見方もある一方で、PHPで記述された検体が一部で確認されている。また.RANSOMED.VCをパートナーと表現したことを確認。
MALLOX (FARGO)
NETWORM (N3TWORM)
BLACKMAGIC
RADAR
BULLY
SPARTA
BL4CKTOR
COOMING PROJECT
MBC
LILITH
SHAOLEAKS
OMEGA
MINDWARE
UNSAFE
HELLBORN
HOTARUS
EP918
DARKRYPT
QILIN (AGENDA)
PROJECT RELIC
ICEFIRE
MOISHA
SUGAR
QLOCKER
SNAPMC
BABYDUCK
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
BL4CKTOR	2021 - J
BLACK BASTA	2022 - G
BLACKBIT	2022 - I
BLACKBYTE	2021 - E
BLACKDOLPHIN	2023 - I
BLACKMAGIC	2022 - J
BLACKMATTER	2021 - G
BLACKSHADOW (SPECTRAL KITTEN)	2020 - J
BLACKSNAKE	2023 - A
BLACKSUIT	2023 - F
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
CIPHBIT	2023 - I
CIPHERLOCKER	2023 - G
CLOAK	2023 - A
CLOP	2019 - G
CONTI	2019 - D
COOMING PROJECT	2021 - J
CRYKAL / CRYLOCK	2015 - J
CRYPTBB	2023 - H
CRYPTNET	2023 - I
CRYPTOMIX	2016 - G
CRYPTON	2017 - G
CRYPTOWALL	2016 - G
CRYPTXXX	2016 - G
CRYSIS	2016 - H
CUBA	2019 - J
CYCLOPS	2023 - I
CYLANCE	2023 - C
DAGON	2022 - C
DAIXIN	2022 - C
DARK ANGELS	2022 - B
DARKBIT	2023 - J
DARK POWER	2023 - G
DARKRACE	2023 - G
DARKRYPT	2021 - J
DARKSIDE	2020 - G
DATAF	2023 - C
DEFRAY777	2018 - A
DHARMA	2016 - H
DIAVOL	2021 - E
DIKE	2020 - 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
GOOD DAY	2023 - B
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 - I
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
LOSTTRUST	2023 - F
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 - F
MICHAELKORS	2023 - C
MIDAS	2021 - H
MILIHPEN	2017 - C
MINDWARE	2022 - J
MOISHA	2022 - J
MONTI	2022 - E
MONEY MESSAGE	2023 - G
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 (N3TWORM)	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 - H
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
RANCOZ	2023 - I
RANSOM CARTEL	2021 - H
RANION	2017 - J
RANSOMED.VC	2023 - E
RANSOM EXX	2020 - A
RANSOMHOUSE	2021 - D
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	2023 - J
SNATCH	2018 - J
SOLIDBIT	2022 - A
SPARTA	2022 - J
SPOOK	2021 - I
STEEL	2020 - H
STORMOUS	2021 - J
SUGAR	2021 - J
SUNCRYPT	2019 - B
SUNNYDAY	2023 - F
SYNACK	2017 - H
SZ40	2020 - J
TELEGRAM	2019 - C
THANOS	2019 - I
THREEAM	2023 - G
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

リブランド → / 関係性 - - →

暴露活動あり※ (拠点準備等も含む)

※ 中塗り 過去2週間以内でリークサイトがオンライン

- 暴露先としてリークサイトを使用
- 暴露先としてハッカーフォーラムを使用
- 暴露先としてTelegramを使用
- ランサムウェアの使用が確認されていない

暴露活動なし (または未確認)

その他

- ShadowSyndigate (複数のグループを跨ぎ関係性が見られる脅威 (IABやアフィリエイト等の可能性を含む))

© 2023 Mitsui Bussan Secure Directions, Inc. All rights reserved. ／ 本図の内容は2023年10月4日現在のものです。

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

SD21-102C - 2310