Created by Cyber Intelligence Group

MBSD Know your enemy. Defense leadership.

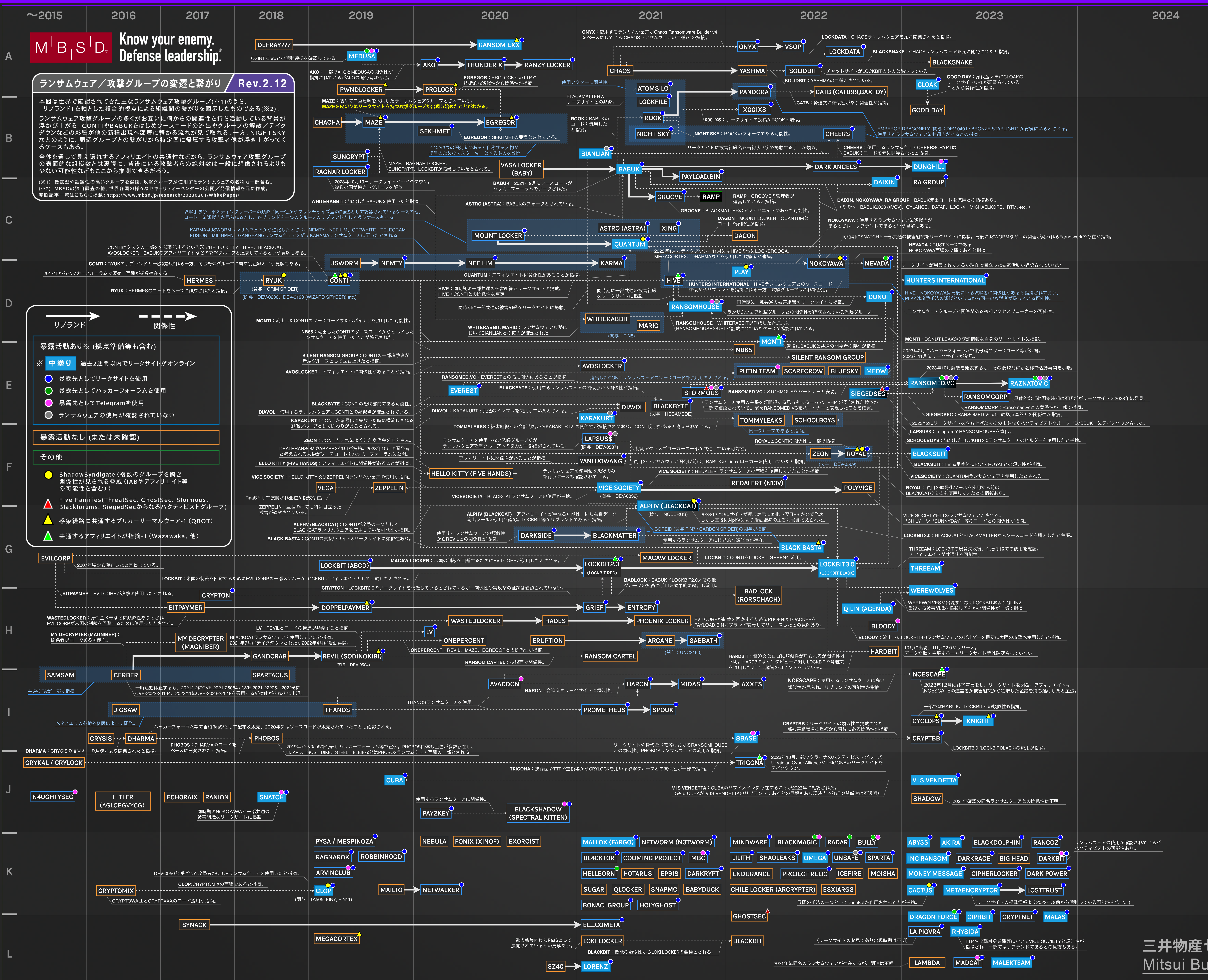
ランサムウェア／攻撃グループの変遷と繋がり Rev.2.12

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らか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/



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))
▲ Five Families(ThreatSec、GhostSec、Stormous、Blackforums、SiegedSecからなるハクティビストグループ)
▲ 感染経路に共通するプリカーサーマルウェア-1 (QBOT)
▲ 共通するアフィリエイトが指摘-1 (Wazawaka、他)

〜2015　2016　2017　2018　2019　2020　2021　2022　2023　2024

A

DEFRAY777 → RANSOM EXX

OSINT Corpとの活動連携を確認している。 MEDUSA

AKO → THUNDER X → RANZY LOCKER

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。

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。

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。

BLACKMATTERのリークサイトとの類似。

ATOMSILO
LOCKFILE

PANDORA → CATB (CATB99,BAXTOY)

CATB：脅迫文に類似性があり関連性が指摘。

CLOAK → GOOD DAY

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。

B

ROOK：BABUKのコードを流用したと指摘。

ROOK → PANDORA

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。

CHACHA → MAZE → EGREGOR

SEKHMET

EGREGOR：SEKHMETの亜種とされている。

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

RAGNAR LOCKER

MAZE、RAGNAR LOCKER、SUNCRYPT、LOCKBITが協業していたとされる。

2023年10月19日リークサイトがテイクダウン。複数の国が協力しグループを解体。

BIANLIAN

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。

VASA LOCKER (BABY) → BABUK → DARK ANGELS → DUNGHILL

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。

BABUK → PAYLOAD.BIN

DAIXIN
RA GROUP

BABUK → GROOVE

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。

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. ）

C

WHITERABBIT：流出したBABUKを使用したと指摘。

ASTRO (ASTRA)：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。

MOUNT LOCKER → QUANTUM

ASTRO (ASTRA)
XING

DAGON：MOUNT LOCKER、QUANTUMとコードの類似性が指摘。

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。背後にJSWORMなどへの関連が疑われるFarnetworkの存在が指摘。

NEVADA：RUSTベースであるNOKOYAWA亜種の変種であると指摘。

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。

2023年1月にテイクダウン。11月にはHIVEの他にLOCKERGOGA、MEGACORTEX、DHARMAなどを使用した攻撃者が逮捕。

D

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。

JSWORM → NEMTY → NEFILIM → KARMA

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

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。

HERMES　RYUK　CONTI
(関与：GRIM SPIDER)
(関与：DEV-0230、DEV-0193 (WIZARD SPYDER) etc.)

RYUK：HERMESのコードをベースに作成されたと指摘。

QUANTUM：アフィリエイトに関係性があることが指摘。

HIVE

HUNTERS INTERNATIONAL：HIVEランサムウェアとのソースコード類似からリブランドを指摘される一方、攻撃グループはこれを否定。

HUNTERS INTERNATIONAL

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。

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。

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。

RANSOMHOUSE

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。

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。

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。

WHITERABBIT　MARIO
(関与：FIN8)

WHITERABBIT, MARIO：ランサムウェア攻撃においてBIANLIANとの協力が確認された。

RANSOMHOUSE：WHITERABBITが作成した脅迫文にRANSOMHOUSEのURLが記載されていたケースが確認されている。

MONTI　背後にBABUKと共通の開発者の存在が指摘。

MONTI：DONUT LEAKSの認証情報を自身のリークサイトに掲載。

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

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。
2023年11月にリークサイトが発見。

E

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

AVOSLOCKER：アフィリエイトに関係性があることが指摘。

AVOSLOCKER

PUTIN TEAM　SCARECROW　BLUESKY　MEOW

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。

2023年10月解散を発表するも、その後12月に新名称で活動再開を示唆。

RANSOMED.VC：EVERESTとの協力関係にあることが指摘。

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。

STORMOUS

RANSOMED.VC：STORMOUSをパートナーと表現。

SIEGEDSEC

RANSOMED.VC → RAZNATOVIC

RANSOMCORP　具体的な活動開始時期は不明だがリークサイトを2023年に発見。

RANSOMCORP：Ransomed.vcとの関係性が一部で指摘。

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。

SIEGEDSEC：RANSOMED.VCの活動拠点基盤との関係性が指摘。

2023/12にリークサイトを立ち上げたもののまもなくハクティビストグループ「D7BBUK」にテイクダウンされた。

BLACKBYTE：CONTIの恐喝部門である可能性。

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。

DIAVOL：KARAKURTと共通のインフラを使用していたとされる。

DIAVOL

BLACKBYTE
(関与：HECAMEDE)

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

同一グループであると指摘。

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。

LAPSUS$：TelegramでRANSOMHOUSEを宣伝。

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。

F

ZEON：CONTIと非常によく似た身代金メモを生成。

DEATHRANSOMやABYSSの流用が指摘。2023年10月に開発者と考えられる人物がソースコードをハッカーフォーラムに公開。

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。

ROYALとCONTIの関係性も一部で指摘。

ZEON → ROYAL
(関与：DEV-0569)

ROYAL → BLACKSUIT

BLACKSUIT：Linux用検体においてROYALとの類似性が指摘。

HELLO KITTY (FIVE HANDS)：アフィリエイトに関係性があることが指摘。

アフィリエイトに関係性があることが指摘。

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。

HELLO KITTY (FIVE HANDS)

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：REDALERTランサムウェアの亜種を使用していたことが指摘。

VICESOCIETY：QUANTUMランサムウェアを使用したとされる。

VEGA　ZEPPELIN

RaaSとして展開され亜種が複数存在。

VICE SOCIETY → POLYVICE
(関与：DEV-0832)

REDALERT (N13V)

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。

VICESOCIETY：BLACKCATランサムウェアの使用が指摘。

ZEPPELIN：亜種の中でも特に目立った被害が確認されている。

ALPHV (BLACKCAT)
(関与：NOBERUS)

2023/12 /19にサイトが押収表示に変化し翌日FBIが公式発表。しかし直後にAlphVにより活動継続の主旨に書き換えられた。

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。

VICE SOCIETY独自のランサムウェアとされる。「CHILY」や「SUNNYDAY」等のコードとの関係性が指摘。

COREID (関与:FIN7 / CARBON SPIDER)の関与が指摘。

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。

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。

LOCKBIT3.0：BLACKCATとBLACKMATTERからソースコードを購入したと主張。

BLACK BASTA：CONTIの支払いサイト&リークサイトに類似性あり。

BLACK BASTA

G

THREEAM：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。

EVILCORP

2007年頃から存在したと言われている。

LOCKBIT (ABCD) → LOCKBIT2.0 (LOCKBIT RED) → LOCKBIT3.0 (LOCKBIT BLACK)

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。

MACAW LOCKER

LOCKBIT：CONTIをLOCKBIT GREENへ流用。

THREEAM

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。

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)

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。

BITPAYMER：EVILCORPが攻撃に使用したとされる。

CRYPTON

WEREWOLVES

QILIN (AGENDA)

WEREWOLVESが出現まもなくLOCKBITおよびQILINと重複する被害組織を掲載し何らかの関係性が一部で指摘。

H

BITPAYMER → DOPPELPAYMER → GRIEF → ENTROPY

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

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。

BLOODY

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。

LV：REVILとコードの構造が類似すると指摘。

MY DECRYPTER (MAGNIBER)：開発者が同一である可能性。

MY DECRYPTER (MAGNIBER)

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。

LV

ONEPERCENT

ERUPTION → ARCANE → SABBATH
(関与：UNC2190)

ONEPERCENT：REVIL、MAZE、EGREGORとの関係性が指摘。

CERBER → GANDCRAB → REVIL (SODINOKIBI)
(関与：DEV-0504)

RANSOM CARTEL：技術面で関係性。

RANSOM CARTEL

HARDBIT：脅迫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の脅迫文を流用したという趣旨のコメントをしている。

HARDBIT

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。

I

SAMSAM　CERBER　SPARTACUS

共通のTAが一部で指摘。

一時活動休止するも、2021/12にCVE-2021-26084 / CVE-2021-22205、2022/6にCVE-2022-26134、2023/11にCVE-2023-22518を悪用する新検体がそれぞれ出現。

AVADDON

HARON：脅迫文やリークサイトに類似性。

HARON → MIDAS → AXXES

NOESCAPE：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。

NOESCAPE

2023年12月に終了宣言をし、リークサイトを閉鎖。アフィリエイトはNOESCAPEの運営者が被害組織から窃取した金銭を持ち逃げしたと主張。

THANOSランサムウェアを使用。

JIGSAW　THANOS

PROMETHEUS → SPOOK

一部ではBABUK、LOCKBITとの類似性も指摘。

CYCLOPS → KNIGHT

ベネズエラの心臓外科医によって開発。

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。

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。

CRYSIS　DHARMA　PHOBOS　8BASE　CRYPTBB

DHARMA：CRYSISの復号キーの漏洩により開発されたと指摘。

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。

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。

LOCKBIT3.0 (LOCKBIT BLACK)の流用が指摘。

CRYKAL / CRYLOCK　TRIGONA

2023年10月、親ウクライナのハクティビストグループ、Ukrainian Cyber AllianceがTRIGONAのリークサイトをテイクダウン。

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。

J

CUBA

V IS VENDETTA

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）

N4UGHTYSEC　HITLER (AGL0BGVYCG)　ECH0RAIX　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。

使用するランサムウェアに関係性。

PAY2KEY　BLACKSHADOW (SPECTRAL KITTEN)

SHADOW　2021年確認の同名ランサムウェアとの関係性は不明。

K

PYSA / MESPINOZA
RAGNAROK　ROBBINHOOD
ARVINCLUB

NEBULA　FONIX (XINOF)　EXORCIST

MALLOX (FARGO)　NETWORM (N3TW0RM)
BL4CKT0R　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

ABYSS　AKIRA　BLACKDOLPHIN　RANCOZ
INC RANSOM　DARKRACE　BIG HEAD　DARKBIT
MONEY MESSAGE　CIPHERLOCKER　DARK POWER
CACTUS　METAENCRYPTOR → LOSTTRUST

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。

展開の手法の一つとしてDanaBotが利用されることが指摘。

(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可能性も含む。)

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:CRYPTOMIXの亜種であると指摘。

CRYPTOMIX　CLOP
(関与：TA505, FIN7, FIN11)

CRYPTOWALLとCRYPTXXXのコード流用が指摘。

MAILTO → NETWALKER

GHOSTSEC

DRAGON FORCE　CIPHBIT　CRYPTNET　MALAS

L

SYNACK → EL_COMETA

MEGACORTEX

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

BLACKBIT：機能の類似性からLOKI LOCKERの亜種とされる。

LA PIOVRA　(リークサイトの発見であり出現時期は不明)

RHYSIDA

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。

SZ40 → LORENZ

2021年に同名のランサムウェアが存在するが、関連は不明。

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
BL4CKT0R	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	2022 - C
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
DOPPELPAYMER	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	2017 - 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	2018 - 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	2021 - L
LOSTTRUST	2023 - K
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
MEDUSA	2019 - A
MEGACORTEX	2019 - L
MEOW	2022 - E
METAENCRYPTOR	2023 - K
MICHAELKORS	2023 - C
MIDAS	2021 - I
MILIHPEN	2017 - C
MINDWARE	2022 - K
MOISHA	2022 - K
MONTI	2022 - E
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
OFFWHITE	2019 - C
ONYX	2022 - A
OMEGA	2022 - K
ONEPERCENT	2020 - H
PANDORA	2022 - A
PAY2KEY	2020 - J
PAYLOAD.BIN	2021 - B
PHOBOS	2018 - I
PHOENIX LOCKER	2021 - H
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 - K
RA GROUP	2023 - C
RAMP	2021 - C
RANCOZ	2023 - K
RANION	2017 - J
RANSOM CARTEL	2021 - H
RANSOMCORP	2023 - E
RANSOMED.VC	2023 - E
RANSOM EXX	2020 - A
RANSOMHOUSE	2021 - D
RANZY LOCKER	2020 - A
RAZNATOVIC	2023 - E
REDALERT (N13V)	2022 - F
REVIL (SODINOKIBI)	2019 - H
RHYSIDA	2023 - L
ROBBINHOOD	2019 - K
ROOK	2021 - B
ROYAL	2022 - F
RTM	2023 - 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	2019 - 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
X001XS	2022 - B
XING	2021 - C
YANLUOWANG	2021 - F
YASHMA	2022 - A

© 2023 Mitsui Bussan Secure Directions, Inc. All rights reserved. ／ 本図の内容は2023年12月26日現在の情報です。

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 | SD21-102D - 2312