Created by Cyber Intelligence Group

# ランサムウェア／攻撃グループの変遷と繋がり

# MBSD RANSOMWARE MAP Rev. 2.20

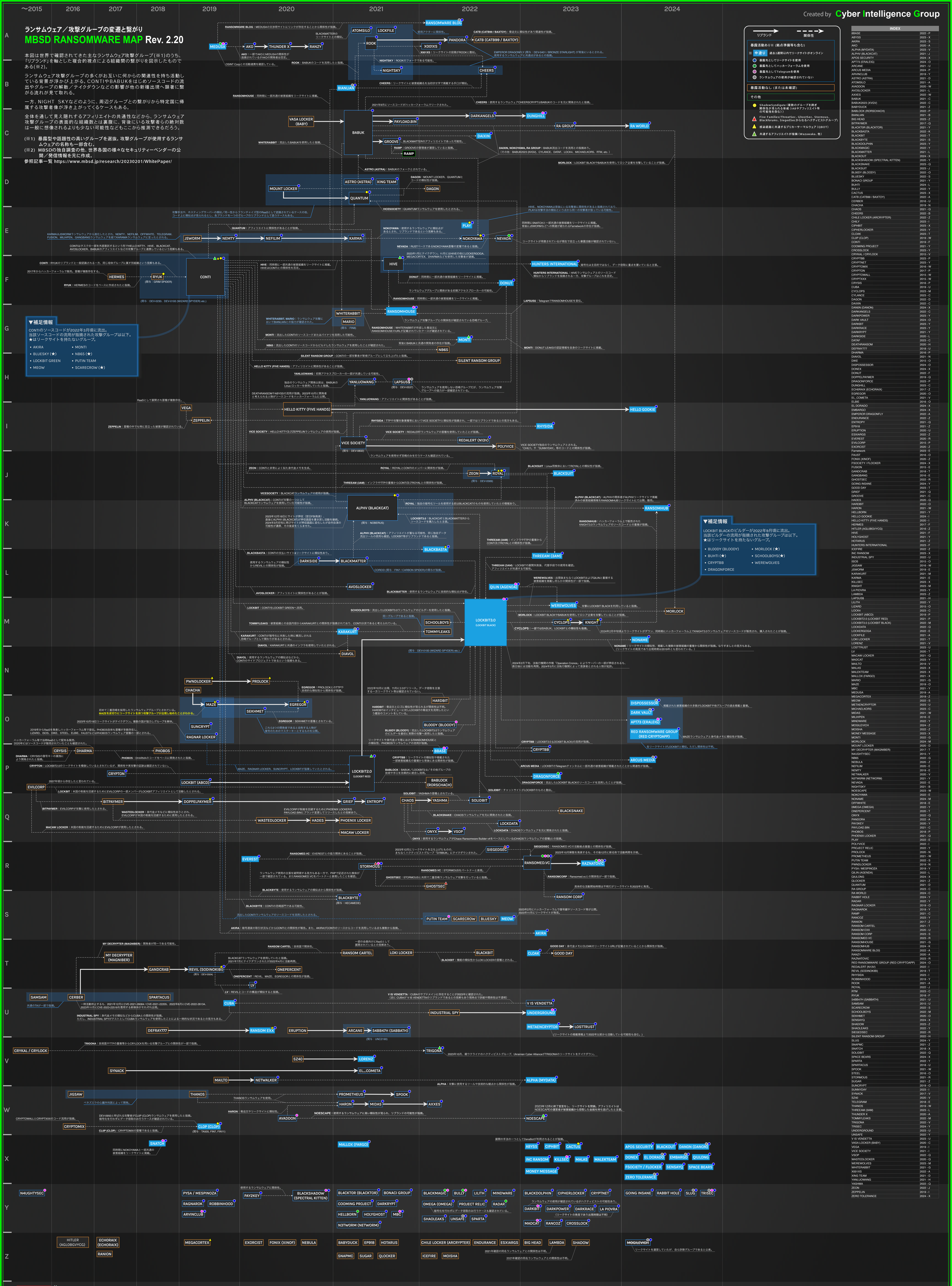
本図は世界で確認されてきた主なランサムウェア攻撃グループ(※1)のうち、「リブランド」を軸とした複合的視点による組織間の繋がりを図示したものである(※2)。

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顔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 https://www.mbsd.jp/research/20230201/WhitePaper/





M|B|S|D. Know your enemy. Defense leadership.
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 | SD21-102F-2406

Created by Cyber Intelligence Group
© 2024 Mitsui Bussan Secure Directions, Inc. All rights reserved. ／ 本図の内容は 2024 年 6 月 10 日時点の情報です。

本コンテンツの最新バージョン (PDF) は
右の QR コードから無料ダウンロード可能
https://www.mbsd.jp/research/20230201/whitepaper/