History of ransomware group connections and transitions

MBSD RANSOMWARE MAP Rev. 2.20

Created by Cyber Intelligence Group

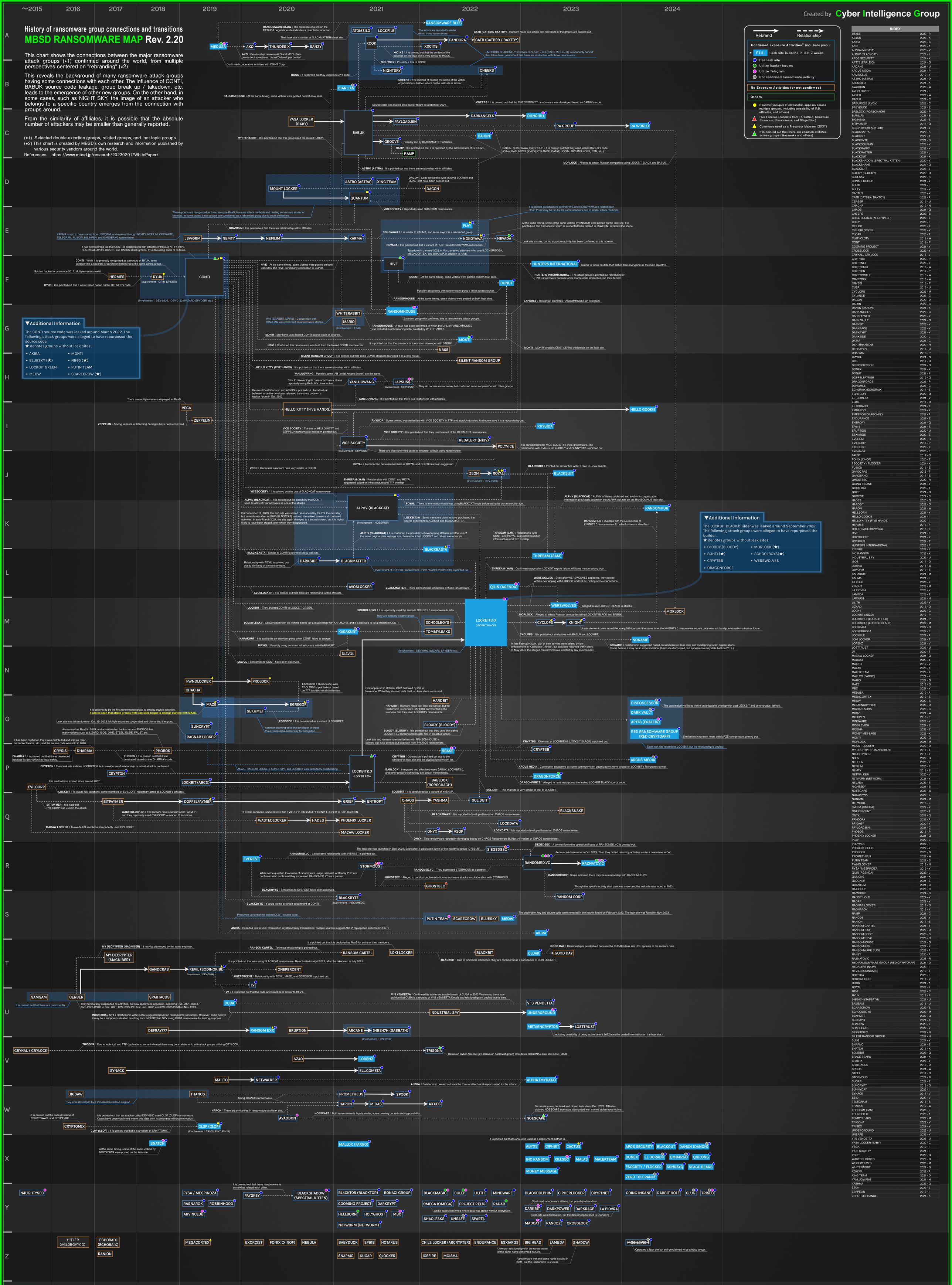
This chart shows the connections between the major ransomware attack groups (⋆1) confirmed around the world, from multiple perspectives centered on "rebranding" (⋆2).

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.

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



▼Additional Information

The CONTI source code was leaked around March 2022. The following attack groups were alleged to have repurposed the source code.
★ denotes groups without leak sites.

- AKIRA
- BLUESKY (★)
- LOCKBIT GREEN
- MEOW
- MONTI
- NB65 (★)
- PUTIN TEAM
- SCARECROW (★)

▼Additional Information

The LOCKBIT BLACK builder was leaked around September 2022. The following attack groups were alleged to have repurposed the builder.
★ denotes groups without leak sites.

- BLOODY (BLOODY)
- BUHTI (★)
- CRYPTBB
- DRAGONFORCE
- MORLOCK (★)
- SCHOOLBOYS(★)
- WEREWOLVES

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 | SD22-102F- 2406

Created by Cyber Intelligence Group

© 2024 Mitsui Bussan Secure Directions, Inc. All rights reserved. ／ Contents shown in this sheet are as of June 10, 2024.

The latest version of this content (PDF) is available for free download. Scan the QR code.
https://www.mbsd.jp/research/20230201/whitepaper/