2025 年 8 月 14 日

報道関係者各位

三井物産セキュアディレクション株式会社

世界中で 1 億ドル以上を恐喝したとされる
ランサムウェア集団「Black Basta」の実態を明らかに

～ MBSD が 20 万件の内部チャットログを徹底分析したレポート
「Behind Black Basta」(全 284 ページ)を無料公開 ～

三井物産セキュアディレクション株式会社（本社：東京都中央区、代表取締役社長：鈴木大山）のサイバーインテリジェンスグループ（CIG）は、2025 年 2 月に流出した国際的ランサムウェア攻撃グループ「Black Basta」の内部チャット約 20 万件を分析したレポート「Behind Black Basta」（全 284 ページ）を、2025 年 8 月 14 日に無料で公開いたします。

本レポートは、2023 年 9 月から 2024 年 9 月までの 1 年間にわたり記録された、約 134 万行・約 4,600 万文字に及ぶチャットログを対象に、グループの組織構造、技術的戦術、人間関係、倫理観といった側面を多角的に分析したものです。攻撃の準備段階から実行後の振り返り、さらには日常的な会話に至るまで、これらのチャットは犯罪組織の内情を克明に映し出しており、従来の脅威インテリジェンスでは捉えきれなかった実態を浮かび上がらせています。

レポート本編では、チャットログ全体の統計分析に始まり、IP アドレス・ドメイン情報、生成 AI の悪用手法、恐喝の台本共有、内部の階層構造、生活実態や倫理観まで、全 9 章＋付録という構成で、技術・組織・人間という三層の観点から多角的に Black Basta の実態を描き出しています。

Black Basta の技術力や組織運営の巧妙さに加え、メンバー間の心理的なやりとりや倫理的葛藤なども記録されており、単なる攻撃手法の解明にとどまらず、サイバー犯罪の“人間的側面”にまで踏み込んだ稀有な資料となっています。警察や捜査機関の動向に対する強い警戒、他グループの摘発から学ぶ姿勢など、国際的な法執行とのせめぎ合いも多く観察されており、グローバルに展開されるサイバー犯罪の構造的理解にも資する内容です。

なお、Black Basta に関する分析としては、本レポートは情報量・網羅性・分析の深度において極めて詳細な内容であり、サイバーセキュリティに関わる幅広い関係者の皆様にご活用いただけるものとなっています。

【主な分析ポイント】

- 秩序だった組織運営と物理的な拠点の存在
  チャットログから、Black Basta がリーダーを中心とした厳格なヒエラルキーと役割分担に基づいて活動していたことが判明。共同生活やオフィスといった物理的拠点の存在も明らかにされました。

- 人間的な側面と倫理的葛藤
  メンバー間のプライベートな相談や、医療機関への攻撃に対する戸惑いなど、犯罪組織でありながらも人間としての感情が垣間見える会話が多数記録されていました。

- 高度な攻撃技術と生成 AI の悪用
  ゼロデイ脆弱性や Microsoft Teams を悪用したフィッシング、生成 AI による自然言語生成の悪用など、技術的にも極めて高度な戦術が確認されています。

- 恐喝のプロセスとブランディング
  被害組織に対して事前に財務状況を調査し、台本を用いて身代金交渉を行うなど、脅迫に関する手法も洗練されており、被害組織に対して事前に財務状況を調査し、台本を用いて身代金交渉を行うなど、脅迫のプロセスにも計画性があり、まるで一般的な「営業活動」のような手法が用いられている実態が浮かび上がりました。

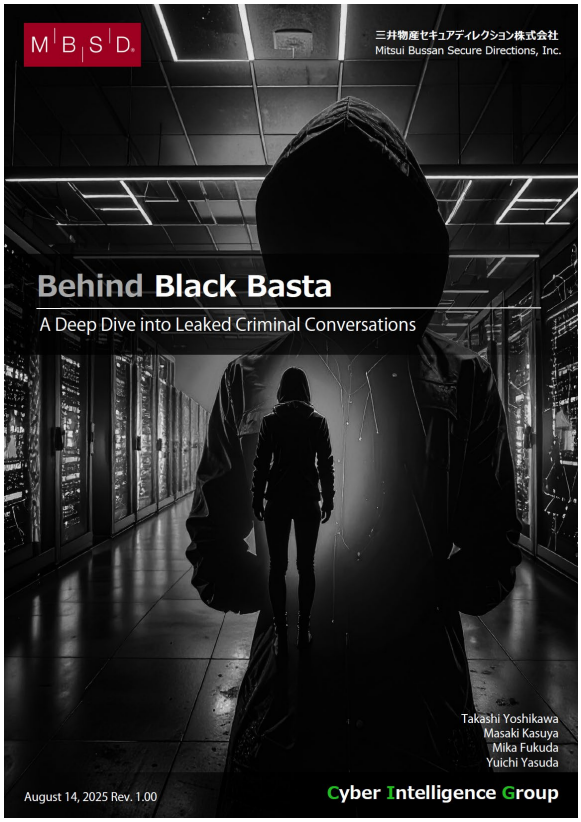
- 日本企業も標的に
  流出したチャットには日本企業に関する言及も含まれており、公表されていない事例が多数存在する可能性が示唆されています。

- 他グループとの連携と摘発への警戒
  他の攻撃グループとの繋がりを示唆する様子や、捜査機関の摘発事例から学習し、警戒態勢を強化する様子が確認されました。サイバー犯罪の背後にある流動的かつ戦略的な連携構造が明らかになっています。

【レポート公開情報】

- 公開日：2025 年 8 月 14 日
- 公開先：https://www.mbsd.jp/report
- 形式：PDF (A4 サイズ、284 ページ)

【表紙デザイン】



三井物産セキュアディレクション（MBSD）について

2001 年にサイバーセキュリティの専門会社として設立、ペネトレーションテスト/TLPT/レッドチーム、Web アプリケーション/ネットワーク脆弱性診断等の各種診断サービス、マルウェア解析、統合ログ監視/Managed XDR サービス等の高度なセキュリティ技術サービス、コンサルティングサービス等を提供し、日本有数の高度セキュリティ技術人材が多数在籍する企業です。

サイバーインテリジェンスグループ（CIG）について

MBSD の社内組織であり、マルウェア解析、ランサムウェアグループの活動実態調査、脅威インテリジェンスの収集・分析、国内外メディア・業界団体への情報提供などを担うインテリジェンスグループです。

＜本件に関するお問い合わせ先＞

三井物産セキュアディレクション株式会社
https://www.mbsd.jp/contact/