DATASHEET

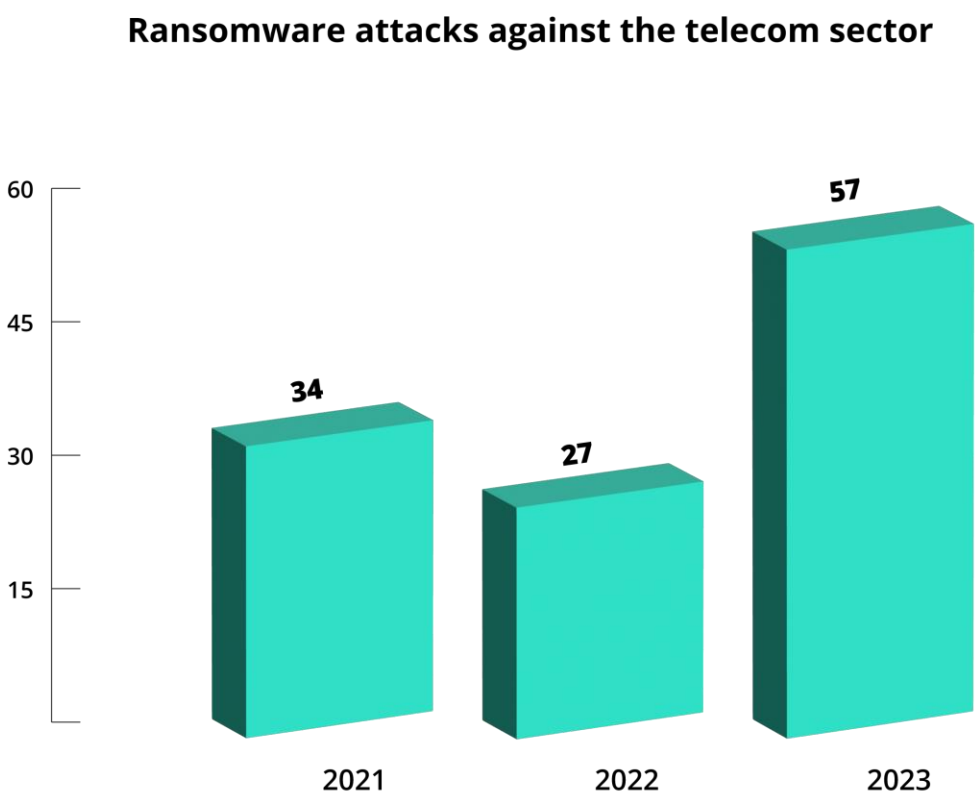
電気通信業界を狙うサイバー犯罪の脅威

あらゆるモノやサービスが急速にインターネットにつながるようになった現在、電気通信業界はサイバー犯罪者にとって理想的な標的となっています。インターネットサービスプロバイダー（ISP）や電話、携帯、人工衛星を扱う企業をはじめ、様々なビジネスが同業界に関与しているがゆえに、多数の組織や顧客に影響を及ぼすような大規模攻撃を実行できる機会が生まれているのです。電気通信業界に混乱が生じた場合は、社会や経済にも重大な影響が及び、例えば2023年11月半ばにオーストラリアの電気通信事業者「Optus」社で大規模なサービス障害が発生した際には、同国の人口約40%に影響が生じました。また同社では2022年にもデータ侵害が発生しており、この時のインシデントでは顧客1万人もの機密情報が流出する事態となりました。本データシートでは、電気通信業界を狙う持続的脅威について解説します。

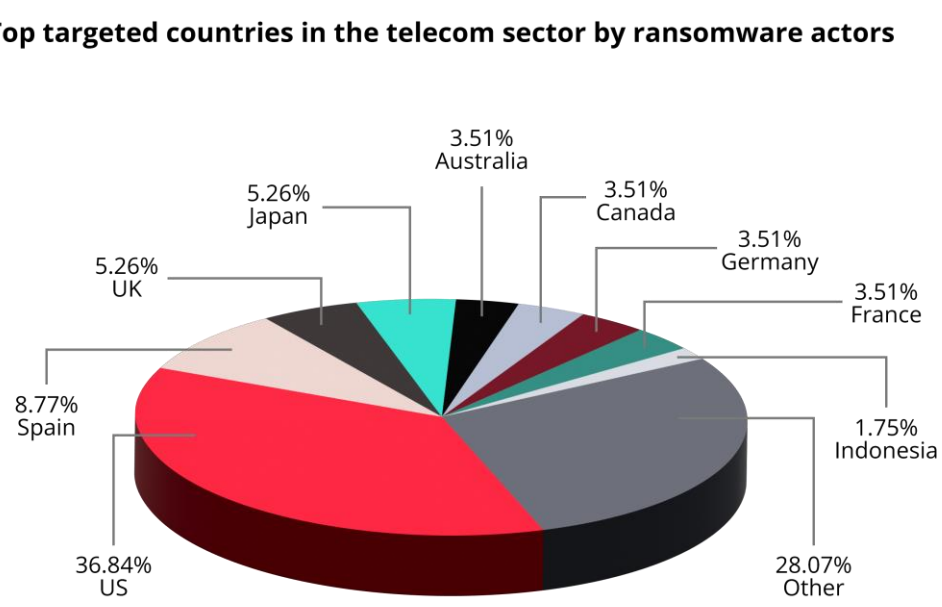
マルウェアを使った攻撃

脅威アクターは、電気通信業界を標的とする活動で様々なマルウェアを使用しています。電気通信ネットワークを狙った攻撃で最も頻繁に使用されているのが、脆弱なデバイスをスキャンするボットネット型マルウェアであり、多岐にわたるIoTボットネット（IoT機器で構成されたボットネット）が戦術に取り入れられています。また研究者からは、通信ネットワークを標的にしたIoTボットネットのトラフィックが、2023年は2022年の5倍に増加したとの報告が寄せられています。

ランサムウェアグループも電気通信業界を標的に活動し、データを暗号化するマルウェアを展開したり、情報を窃取しています。KELAが、電気通信業界を標的としたランサムウェア攻撃やデータリーク攻撃、それら攻撃を受けた組織を分析した結果、2023年が終わっていない現時点（本稿執筆時点）でも今年の被害組織数は約60近くに上っており、すでに2022年の2倍を超えていることが判明しました。つまり、ランサムウェアグループやデータリークグループは、2023年も持続的脅威として電気通信業界を脅かしているということです。また被害組織を国別に分類したところ、1位は米国、その後にスペイン、英国、日本が続きました。



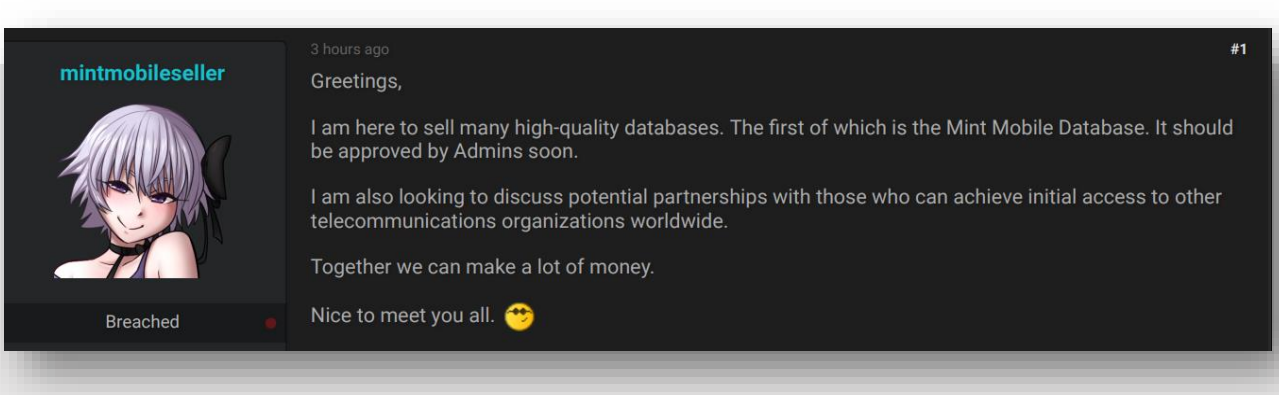
電気通信業界で発生したランサムウェア攻撃の件数（2021～2023年）



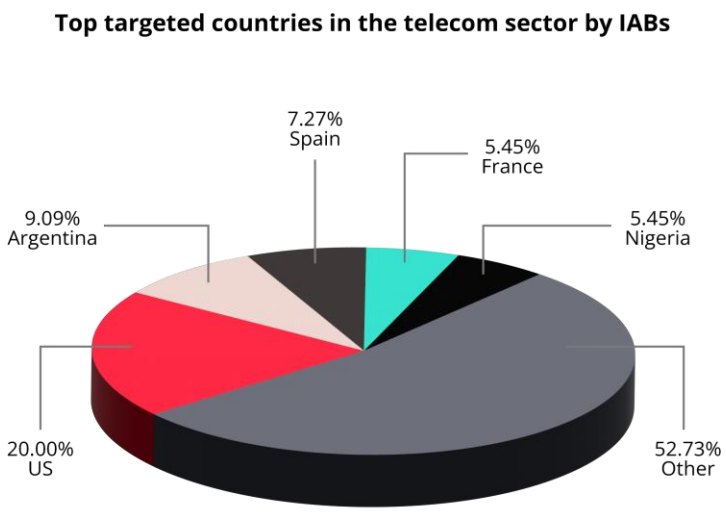
2023年に電気通信業界を標的にしたランサムウェアグループを分析したところ、攻撃件数上位はLockBit、Clop、Alphvとなりました。またこの3グループは、電気通信業界のみならず全ての業界において、2023年の攻撃件数上位にランクインしました。

ネットワークアクセスの販売

初期アクセスブローカー（IAB）は、侵害先となるネットワークのアクセスを攻撃者に提供している脅威アクターであり、ランサムウェア・アズ・ア・サービス（RaaS）のサプライチェーンで重要な役割を果たしています。一般的に、電気通信会社は顧客企業の社内データや他社のネットワークにアクセスすることができるため、脅威アクターにとっては電気通信会社を侵害することで、その後の活動チャンスを大幅に広げることが可能となります。我々の調査では、2023年に入って売り出された電気通信会社のネットワークアクセスは約55件に上ることが判明しています。また同業界は、2023年に初期アクセスブローカーが標的にした業界のトップ10にもランクインしています。



電気通信会社の初期アクセスを探しているアクターの投稿

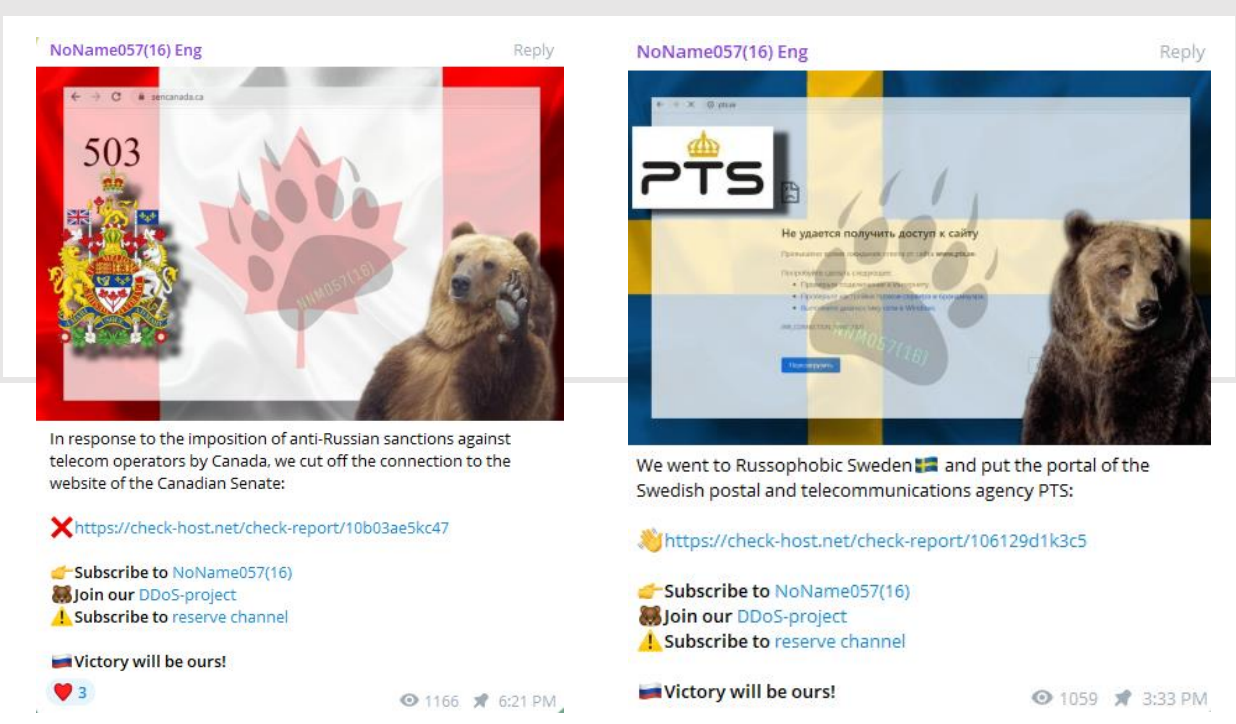


初期アクセスブローカーが売りに出した電気通信業界のネットワークアクセス

（国別の割合、2023年1～10月）

DDoS攻撃

DDoS（分散型サービス拒否）攻撃も電気通信業界にとって重大な脅威であり、攻撃を受けた場合は会社の評判が損なわれたり、経済的損失を被る可能性があります。DDoS攻撃はネットワークのリソースを過剰に消費させ、サービスを一時的または無期限に使用不可能にするため、通信インフラの信頼性を担保する上で大きな問題となります。DDoS攻撃の中には、イデオロギー的な動機で活動しているハクティビストグループによって行われているものもあり、彼らは特定の国や企業を標的にDDoS攻撃を実行しています。例えば親ロシア派ハクティビスト「NoName057（16）」は、主にウクライナを支持している国々の電気通信会社を標的に、複数回にわたってDDoSキャンペーンを展開しています。



電気通信会社を標的としたDDoS攻撃の犯行声明

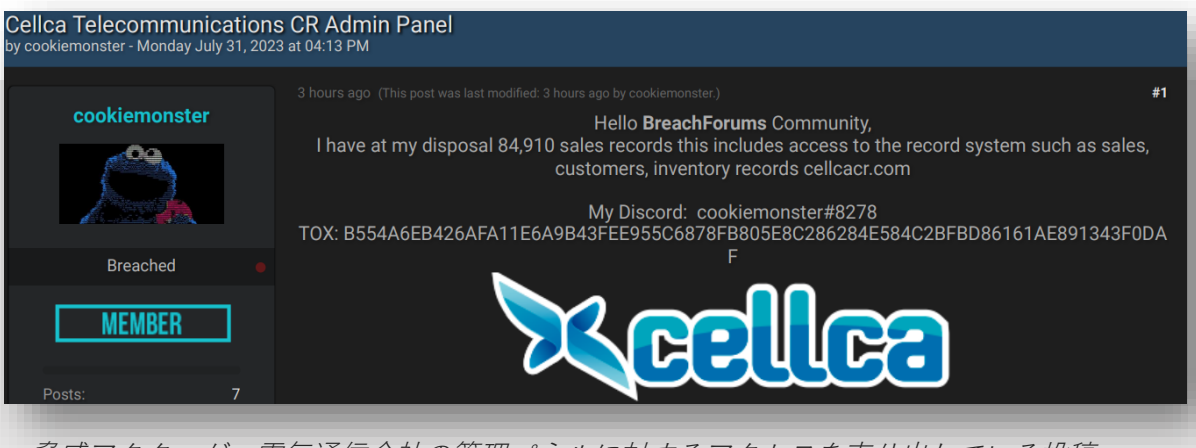
（NoNameの投稿：2023年6～7月）

またKELAが観察したところ、イスラエル・ハマス間の衝突を発端としたサイバー攻撃でも電気通信会社が重要な標的と見なされ、多数のDDoSキャンペーンが展開されていました。そしてその結果、DDoS攻撃を受けた電気通信会社の一部は、衝突による紛争の最中にサービスの停止を余儀なくされました。これらのDDoS攻撃には、イスラエルを標的としたものもあればハマスを標的としたものもあり、またいずれか一方を支持している国々も攻撃の標的となりました。

詐欺・不正行為

電気通信業界を標的とした詐欺・不正行為には、サブスクリプション詐欺からなりすまし、SIMカードのスワッピングにいたるまで様々な種類があります。我々が監視しているサイバー犯罪ソースでも詐欺・不正行為が話題に上っており、一部事例としては以下が挙げられます。

- SIMスワッピングサービス：サイバー犯罪者が個人の電話番号を不正に乗っ取る手口です。サイバー犯罪ソースでは、このサービスを提供するアクターと購入するアクターの両方が存在します。
- 窃取したe-SIMの販売：このサービスを利用することで、他者が登録したデジタルSIMカードを使用し、不正行為を行うことが可能となります。
- VoIP通話のスプーフィング（なりすまし）サービスの販売：これらのツールまたはプラットフォームを使用することで、電話に表示される発信元ID情報を偽装することが可能となります。
- **電気通信会社の管理パネルに対するアクセスの販売**：このアクセスを使用することで、eSIMをアクティベートしたり、企業や顧客のデータに不正アクセスすることが可能となります。また、その他の不正行為にも利用される可能性があります。
- **電話番号の大量買い取り**：脅威アクターは、詐欺行為に悪用（外部からの入電を自らの電話番号に転送して身元の追跡を困難にするなど）するために、電話番号の買い取り広告を投稿しています。



脅威アクターが、電気通信会社の管理パネルに対するアクセスを売り出している投稿

我々のビジネスに利用できる日本の電話番号を探している。かかってきた電話を我々の
番号に転送するために、大量の電話番号が必要なんだ。選択肢としては、
SIPやSkypeのアカウント、SIMカードなどを考えている。

もし日本の電話番号を売ってくれるなら、サービスと価格を提示してくれ。
平日1日あたり5件の電話番号を手に入れたい。提供してくれる電話番号の
電気通信事業者名を記載してくれれば、その中で最適なものを我々が選ぶ。

双方にとって取引のセキュリティと信頼性が確保されるよう、
売買はフォーラムのエスクローサービスを通じて行いたい。

我々の予算は電話番号1件につき100米ドル。

質問や提案があれば、以下に連絡してくれ。

Telegram：@RaspberryPi_xss

脅威アクターが、日本の電話番号の大量買い取りを申し出ている投稿
（以下は日本語参考訳）

電気通信業界を標的とするAPTグループ

国家の支援を受けた脅威アクターも、偵察や監視、通信、諜報活動目的で電気通信インフラを標的にしている可能性があります。またそういった活動の中には、政府や軍、企業の機密通信の傍受も含まれていると思われます。我々の調査では2023年当初から、電気通信会社を標的としたAPTキャンペーンが複数件確認されています。

- 中国の国家支援を受けた「APT41」が、スパイウェア「WyrmSpy」と「DragonEgg」を使用して、知的財産の窃取を目的とするキャンペーンや携帯端末を標的とするキャンペーンを実行。

- APTグループ「Lancefly」が、バックドア「Merdoor」を使用して南及び東南アジアの電気通信組織を攻撃。

- ロシアの国家支援を受けたAPTグループ「Winter Vivern」が、マルウェア「Aperitif」を使用して欧州の政府組織や電気通信サービス企業を攻撃。

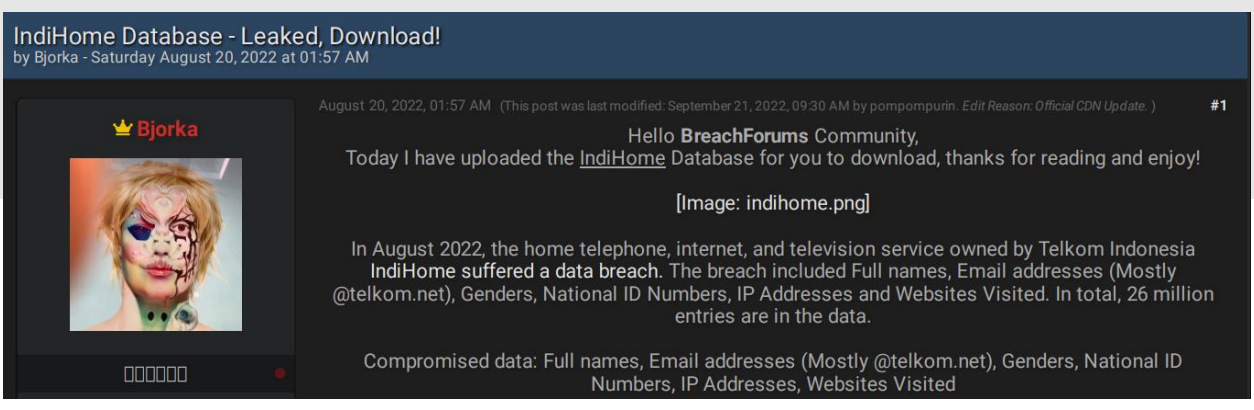
- 中国の国家を受けたAPTグループ「Gallium」が、「Mimikatz」をカスタイマイズした亜種「mim221」を使用して、中東の電気通信会社を標的としたキャンペーンを実行。

- APTグループ「Sandman」が、プラットフォーム「LuaJIT」を悪用してバックドアを配備し、中東や西欧、南アジア亜大陸の電気通信会社を攻撃。

データベースのダンプ

脅威アクターは、電気通信会社が保有しているデータにも高い関心を持っています。その理由として、電気通信会社のデータにはサードパーティに関する重要な情報や、今後の攻撃に悪用可能な情報が含まれている可能性があることが挙げられます。また電気通信会社でデータ侵害が発生した場合、連絡先情報の詳細や社会保障番号、さらには数百万人もの顧客のクレジットカード情報などのレコードが流出する可能性があります。脅威アクターの中には電気通信会社に特化して活動している者もおり、例えば「IntelBroker」は、これまでに電気通信会社（AT&T社やCharter Communications社、Verizon Wireless社、Comcast社、US Cellular社）のデータベースを複数件売りに出しています。

その他に電気通信業界で発生した大規模なデータ侵害の一例として、2022年8月に脅威アクター「Bjorka」が、インドネシアのインターネットサービスプロバイダー「IndiHome」社のデータベースを侵害・公開したインシデントが挙げられます。このインシデントにより、IndiHome社のサービスを利用する顧客の氏名や電子メールアドレス、ID番号、キーワード、IPアドレス、住所、ブラウザの種類、性別などの情報を含んだレコード約2,670万件が流出する事態となりました* 。



Bjorkaがインドネシアの電気通信企業のデータベースを公開した投稿

推奨される対策

- **サイバー犯罪ソースの監視**：自組織のネットワークやデジタル資産を保護する取り組みにおいては、アンダーグラウンドのサイバー犯罪ソースを監視することが重要となります。潜在的な脅威を認識し、リスクを低減するためには、サイバー犯罪者の活動やTTP（技術・戦術・手順）、新たに使用しているツールなどの情報に加え、違法なサービスやデータ侵害などの投稿を把握しておく必要があります。

- **サプライチェーンの保護**：電気通信会社は、サプライチェーン攻撃の一環で標的となる可能性があります。そのため、ベンダーやパートナーなどのサードパーティに関するセキュリティ対策を事前に策定し、順守を徹底することが重要となります。

- **DDoS攻撃に対する防御**：対DDoS攻撃ソリューションを導入し、サービスの停止につながりうる大規模攻撃からネットワークを保護します。また、DDoS攻撃の影響を緩和・低減できる設備能力を常時維持しておきます。

- **バックアップの取得・障害時の復旧**：重要なデータのバックアップを定期的にとり、障害発生時の復旧計画を事前に策定しておきます。これにより、サイバー攻撃が発生しても速やかにシステムを復旧することが可能となります。

脅威アクター「Bjorka」のプロファイルは、KELAのプラットフォームでご覧いただけます