KELA DATASHEET

金融業界を狙う
サイバー犯罪の脅威

2023年、金融業界はサイバー脅威から特に標的とされる業界の1つとなりました。金融機関が世界経済の中枢部分を担う一方で、サイバー犯罪者は高度な技術を用いて機密データを侵害し、重要な金融業務を混乱に陥れようと企んでいます。本データシートでは、データ窃取やランサムウェア攻撃、ネットワークアクセスの販売、内部脅威、DDoS攻撃など、金融業界を脅かすサイバー犯罪について調査した結果を詳述します。

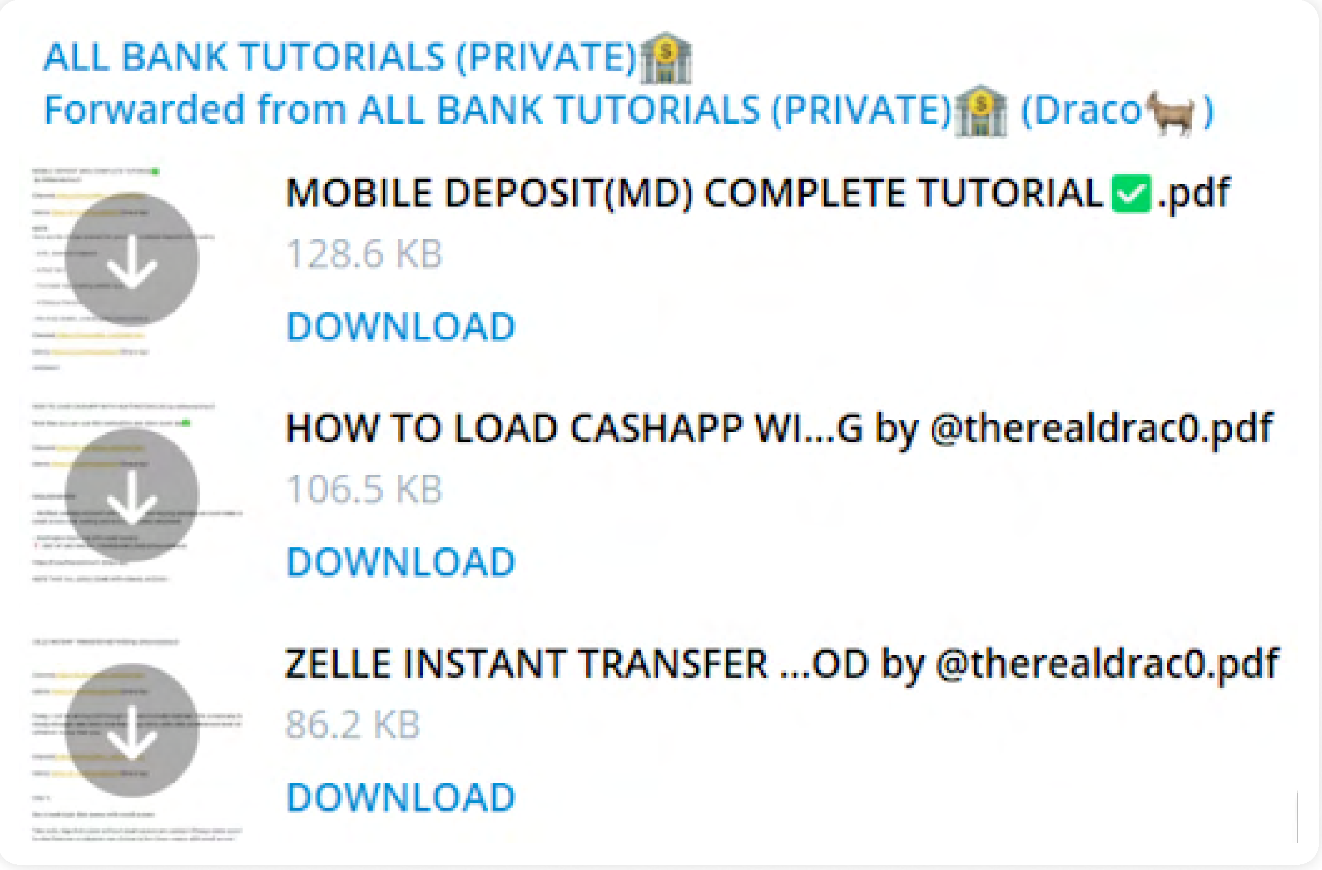
内部脅威

KELAが観察したところ、銀行詐欺にはいくつか明確なパターンが見られました。銀行詐欺の実行犯には多くの共通点があり、彼らは似たような手口を使っています。また大抵の場合、彼らは銀行内で自らの犯行を支援してくれる内部協力者を擁しています。内部協力者は銀行内のシステムや手順に関する知識を悪用し、企業秘密や知的財産、顧客データなどを窃取したり、金融詐欺に関与しています。以前KELAが某金融機関の内部脅威を調査した事例では、以下の計画が明らかとなりました。

1. 実行犯は某銀行支店の行員と知り合いであった。そしてこの行員は自分が勤める銀行の顧客、すなわち今後標的となりうる人物の情報にアクセスできる立場にあり、実行犯の依頼に基づいて標的の情報を送っていた。
2. 実行犯は、「金銭を窃取するスキルを持ったハッカーグループを探している」とのメッセージを某サイバー犯罪フォーラムに投稿していた。
3. この計画ではSIMスワップを行い、内部協力者が被害者の口座から電信送金を実行し、他銀行にある別の口座に資金を移す予定であった。

銀行データの販売

よくある銀行詐欺の戦術としては、銀行の顧客を標的としたフィッシングやソーシャルエンジニアリング、クレジットカードのスキミング、カードのクラッキング、名義貸しなどが挙げられます。いまやメッセージングプラットフォーム「Telegram」上では、銀行詐欺の手順を解説したチュートリアルが多数出回っており、初心者レベルのサイバー犯罪者でも銀行詐欺を実行できるようになっています。またその結果、詐欺行為で窃取された様々な情報がサイバー犯罪コミュニティで売買されています。具体例を挙げると、アンダーグラウンドには「Omerta」や「Brian’s Club」、「Yale Lodge」などのクレジットカードマーケットがあり、そこではサイバー犯罪者が不正に入手したクレジットカード情報とCVV/CVV2情報がセットで販売されています。さらにTelegramチャンネルでは、（窃取された）使用可能な正規の小切手や、偽の小切手が詐欺スキームの一部として多数流通しています。



ALL BANK TUTORIALS (PRIVATE)🏦
Forwarded from ALL BANK TUTORIALS (PRIVATE)🏦 (Draco🐐)

MOBILE DEPOSIT(MD) COMPLETE TUTORIAL ✅.pdf
128.6 KB
DOWNLOAD

HOW TO LOAD CASHAPP WI...G by @therealdrac0.pdf
106.5 KB
DOWNLOAD

ZELLE INSTANT TRANSFER ...OD by @therealdrac0.pdf
86.2 KB
DOWNLOAD

Telegramで流通していた銀行詐欺のチュートリアル

データベースのダンプ

サイバー犯罪者が金融機関を標的とする理由は、金銭や財務データを窃取することに留まりません。金融機関が保有している顧客データを窃取し、後に別の攻撃で悪用しようと企んでいる場合もあります。その一例として、インドに拠点を置く「The Kurla NagrikSahakari Bank」の事例が挙げられます。2023年11月、某脅威アクターが同行の顧客7万6,890人の機密情報を含んだデータベースを、サイバー犯罪フォーラムでリークしました。このデータベースには、顧客の年齢や生年月日、カーストの階級、学歴や職歴、電子メールアドレスなどの情報が含まれていました。このように広範な情報を網羅したデータセットは、サイバー犯罪者によって様々な攻撃に悪用される場合があります。例えば、顧客の詳細な個人情報をもとに説得力のある偽メッセージを作成して、フィッシング攻撃を実行することが可能となります。またサイバー犯罪者は、個人情報を悪用して成りすましや不正な金融取引、その他の不正行為を実行することができるため、データの流出が、成りすまし犯罪や金融詐欺を助長する可能性があります。

11-06-2023, 11:18 AM (This post was last modified: 11-06-2023, 11:29 AM by Fireflies.) #1

Hello all users of the breachforums community, today I will share the databases of www.knsbl.com website

On November 6, 2023 The Kurla Nagrik Sahakari Bank Ltd https://www.knsbl.com/ experienced a data breach. The leak resulted in the disclosure of data including 76890 data containing users

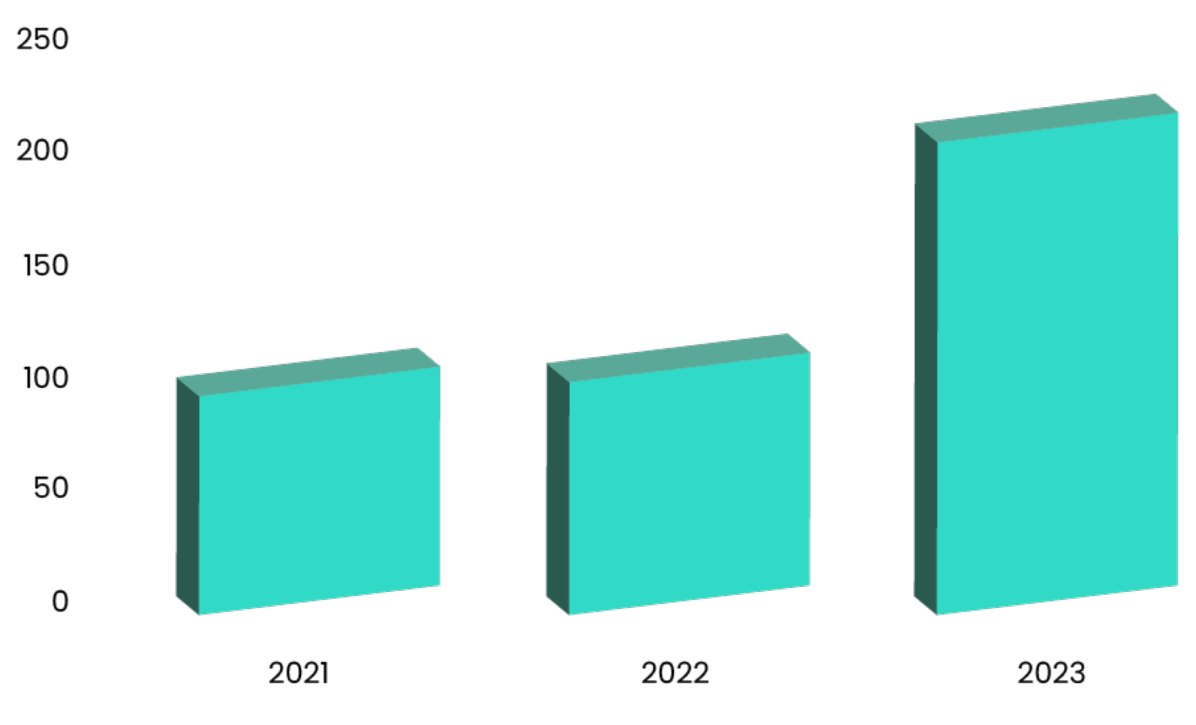
```
| profile4        | varchar(100) |
| profile5        | varchar(100) |
| profile6        | varchar(100) |
| religion        | varchar(111) |
| resumefile      | varchar(100) |
| specialise      | varchar(100) |
| stdcode         | varchar(10)  |
| surname         | varchar(51)  |
| title           | varchar(6)   |
```

脅威アクターがTheKurla NagrikSahakariBankのデータベースを公開した投稿

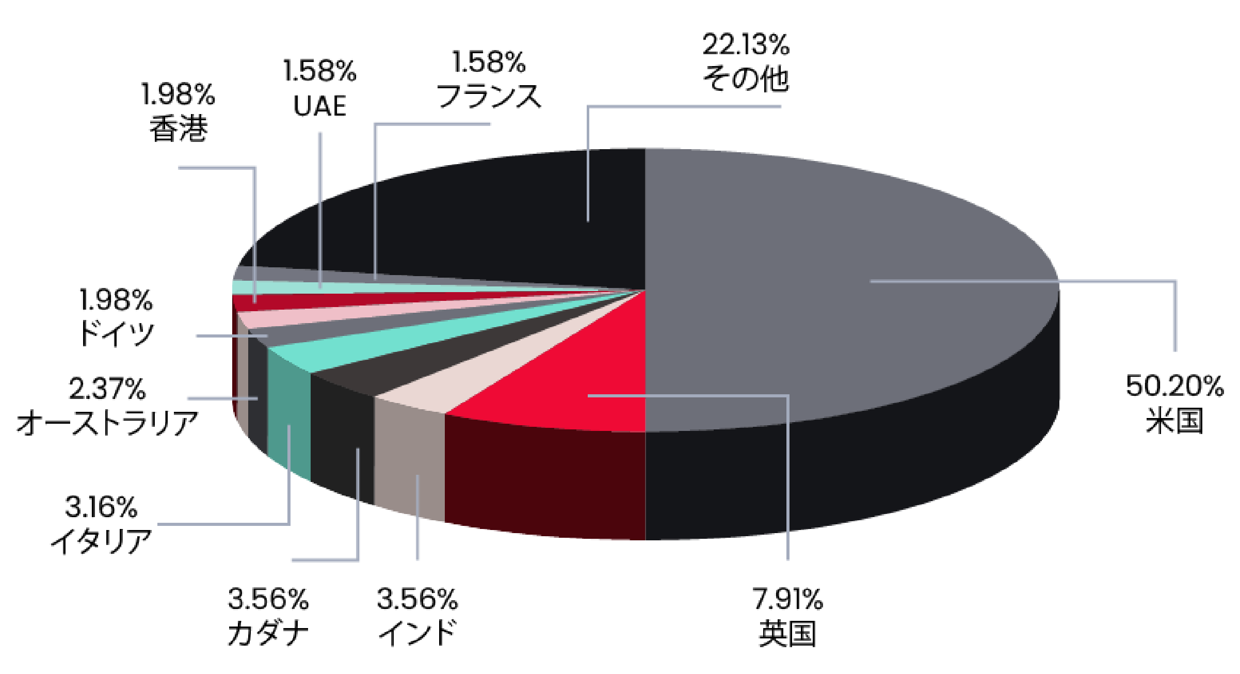
ランサムウェア攻撃

2023年、金融業界では250件以上のランサムウェア攻撃が発生しており、ランサムウェアグループやデータリークグループによって「標的にされた業界」のトップ10にランクインしています。金融業界の被害組織を国別にみると、**「標的にされた国」の1位は米国**であり、同業界で発生したランサムウェア攻撃およびデータリーク攻撃の約50%を占めました。米国に続き「標的にされた国」は、**2位が英国、3位がインド、4位がカナダ、5位がイタリア**となっています。また、金融業界を標的にしたランサムウェア攻撃を犯行グループ別に分類すると、**1位は「Clop」、2位は「LockBit」、3位は「Alphv」、4位は「8Base」、5位は「Black Basta」**となりました。

金融業界を標的としたランサムウェア攻撃の件数



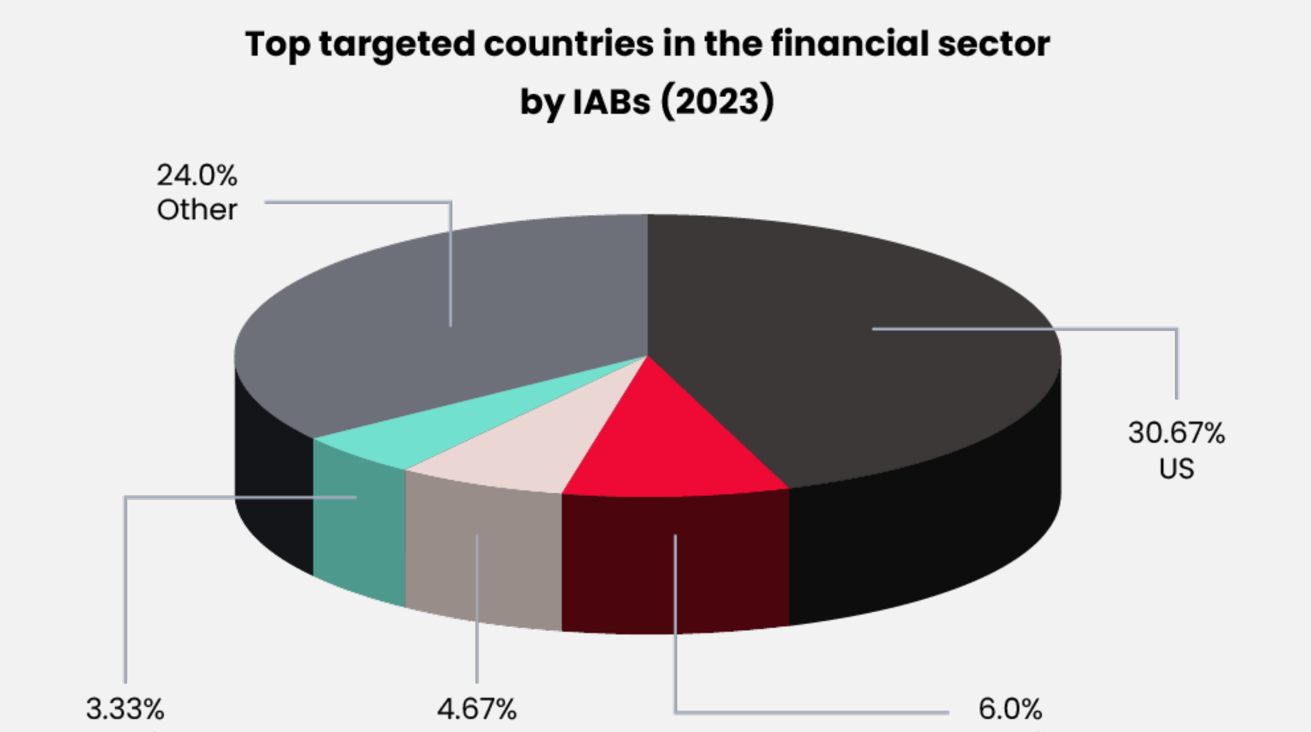
ランサムウェア攻撃を受けた金融業界組織の国別データ（2023年）



ネットワークアクセスの販売

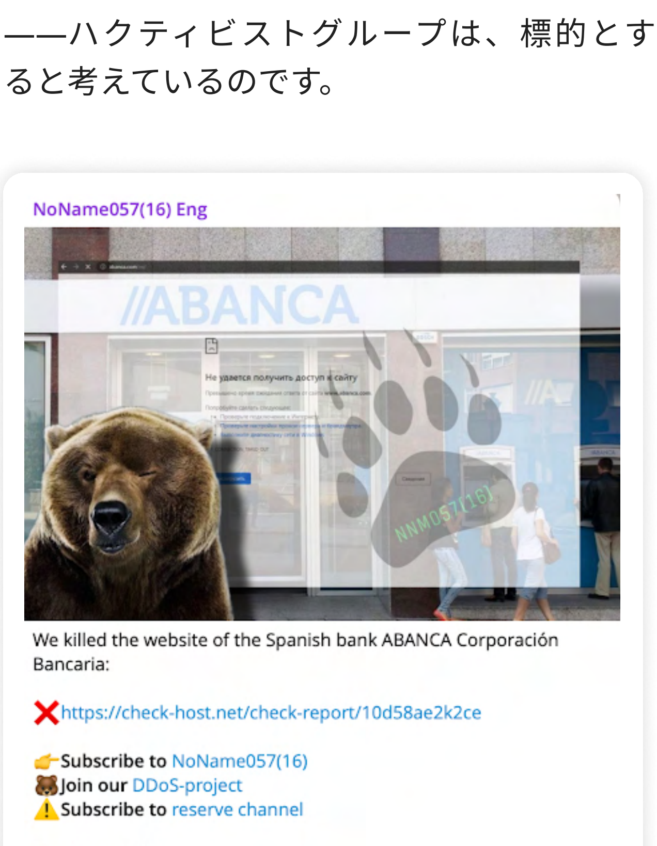
初期アクセスは、ランサムウェア・アズ・ア・サービス（RaaS）のサプライチェーンにおける重要なアイテムであり、その売買において中心的役割を果たしているのが初期アクセスブローカーです。KELAが調査したところ、2023年に売り出された金融機関関連のネットワークアクセスは80件を超えました。またそれらを国別に分類した結果、**初期アクセスブローカーが標的にした国の1位は米国**（全アクセスの31%）、**2位はブラジル、3位はアルゼンチン、4位は英国**となりました。

Top targeted countries in the financial sector by IABs (2023)



DDOS攻撃

DDoS攻撃も、金融業界にとっては重大な脅威となっています。DDoS攻撃で想定される被害としては、オンラインサービスの中断による甚大な経済的損失や評判・信用の失墜が挙げられます。これまでにも多数の脅威アクターが金融業界を標的にDDoS攻撃を実行しており、その中には有料のDDoSサービスを使って特定の標的を攻撃している者もいれば、様々な動機で日和見的に標的を選んで攻撃している者もいます。例えばハクティビストグループは思想的な動機をもとに活動しており、彼らの攻撃の大半は特定の国（とその国の組織）が標的となっています。彼らは抗議行動や異議を表明する手段としてDDoS攻撃を実行し、金融機関を困難な状況に追い込んでいます——ハクティビストグループは、標的とする国で金融機関が重要な役割を果たしていると考えているのです。



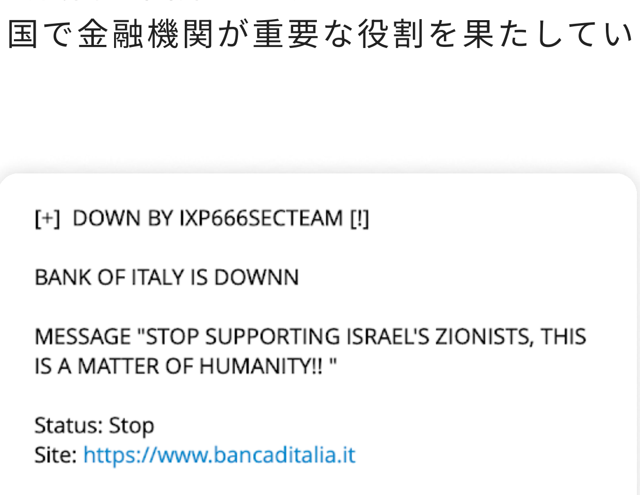
NoName057(16) Eng

We killed the website of the Spanish bank ABANCA Corporación Bancaria:

❌https://check-host.net/check-report/10d58ae2k2ce

👉Subscribe to NoName057(16)
🐻Join our DDoS-project
⚠️Subscribe to reserve channel

🇷🇺Victory will be ours!



[+] DOWN BY IXP666SECTEAM [!]

BANK OF ITALY IS DOWNN

MESSAGE "STOP SUPPORTING ISRAEL'S ZIONISTS, THIS IS A MATTER OF HUMANITY!! "

Status: Stop
Site: https://www.bancaditalia.it

Report: https://check-host.net/check-ping?host=https://www.bancaditalia.it/&csrf_token=e85525fca589413511badd1646ebe2c537421e7d

NoName057(16)がスペインの金融機関をDDoS攻撃の標的に挙げている投稿

推奨される対策＆リスク緩和策

セキュリティ研修：職員を対象に、サイバーセキュリティの基本（フィッシングメールの見分け方や安全性の高いパスワードの作成・管理方法、オンラインで機器や情報を安全に使用する方法など）について学ぶ研修を実施します。

定期的なバックアップ：重要なデータやシステムのバックアップを定期的に取り、オフライン環境で適切に保存して、ランサムウェア攻撃による影響を緩和します。

多要素認証（MFA）：追加のセキュリティ対策として、機密性の高いデータやシステムへのアクセスに多要素認証を実装します。これにより、脅威アクター•が不正入手した資格情報を悪用することが困難になります。

インシデント対応計画：金融業界に即した包括的なインシデント対応計画を策定・更新し、定期的に演習を実施して準備体制を確認します。

セキュリティ監査・評価：第三者の専門家によるセキュリティ監査および評価を定期的に実施し、客観的な評価と脆弱性の特定を行います。

協力体制と情報共有：他の金融機関と協力体制を構築して脅威インテリジェンスを共有し、金融業界に特化したサイバー脅威インテリジェンスコミュニティに参加します。

エンドポイントの保護：ウィルス対策やEDR、行動分析などの機能を有する高度なエンドポイント保護ソリューションを導入し、マルウェアに対する防御を強化します。

サイバー犯罪ソースの監視：サイバー犯罪ソースを監視し、データベースのダンプやアカウント情報、ランサムウェア攻撃に関する投稿、サイバー犯罪の傾向などに関する情報を入手します。