Avast

Press Release

Avast PR 事務局
2024 年 6 月

アバスト 、2024 年第 1 四半期脅威レポートを発表

YouTube がサイバー犯罪の新たな主戦場になり始めている
サポート詐欺も前四半期から 153%の増加

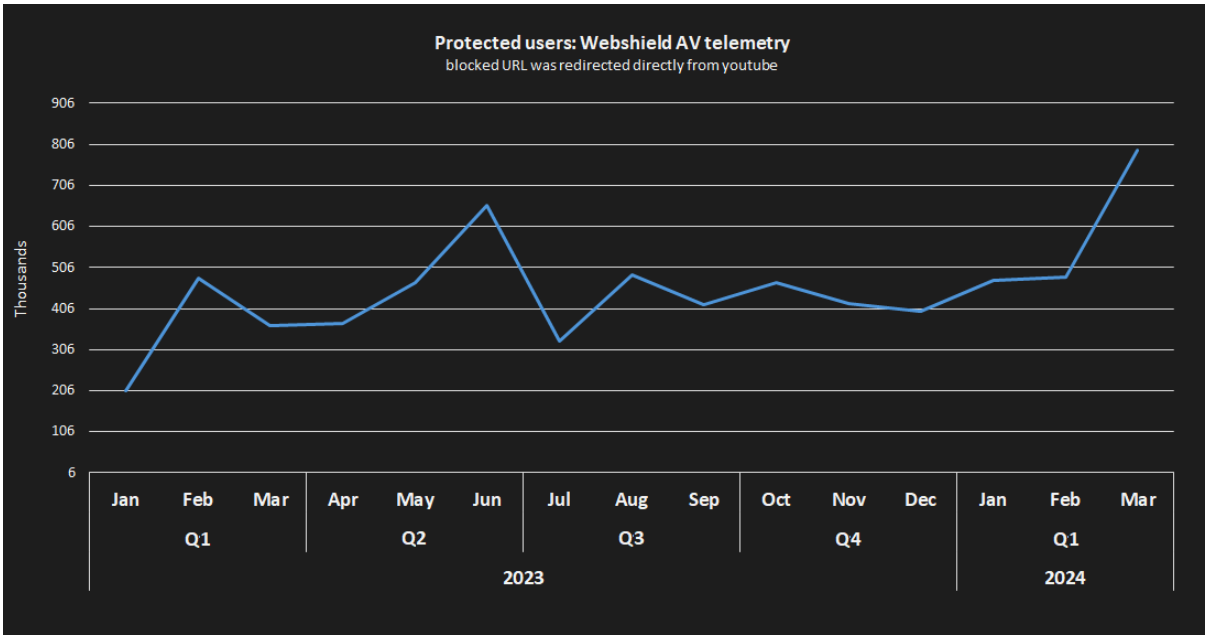
デジタルセキュリティおよびプライバシー製品のグローバルリーダーで、Gen 傘下のアバストは、2024 年第 1 四半期の脅威レポートを発表しました。レポートによると、YouTube を介したサイバー犯罪が活発になってきたことが明らかになりました。また、日本は引き続きサポート詐欺において世界トップクラスの被害件数を記録し、全四半期から 153%も増加したことが分かりました。

レポートの主なトピックは以下をご覧ください。

YouTube がフィッシング、不正広告、仮想通貨詐欺の新たな戦場に

25 億人のユーザーを抱える YouTube が不正広告の重要なターゲットとして、詐欺師から注目されつつあります。自動化された広告システムとユーザー生成コンテンツの組み合わせは、サイバー犯罪者が従来セキュリティ対策を回避するための手法となっており、YouTube がフィッシングやマルウェアを展開するための強力な媒体となりつつあります。またその中にある脅威としては、Lumma や Redline のような認証情報を盗むもの、フィッシングや詐欺のランディングページ、正規のソフトウェアやアップデートを装った悪意のあるソフトウェアなどが存在しています。さらに、YouTube はトラフィック配信システム（TDS）への導線としても機能し、ユーザーを悪意のあるサイトへの誘導や、偽の景品から投資詐欺など、さまざまな詐欺の足がかりとなっています。

当社のリアルタイムスキャンでは、ユーザーがコンテンツ閲覧する際に YouTube からリダイレクトされる HTTP リクエストを毎日数千件もブロックしています。



-2023 年に YouTube で詐欺の脅威から保護されたユニークユーザーは約 400 万人
-2024 年第 1 四半期だけでは、月間約 50 万人のユニークユーザーを保護

＜本件に関するお問い合わせ先
Avast PR 事務局（株式会社プラチナム内） 担当：石間、杉原、加藤、宮下
TEL：03-5572-6071（PR 事務局）／Mail：norton-pr@vectorinc.co.jp

また近年の傾向として、YouTube 上で DeepFake 動画が増加しています。これらの動画は、人物などを模倣し、視聴者を誤解させ、偽情報を広める重大なリスクを伴います。第 1 四半期には、5,000 万人以上の登録者を持つ YouTube アカウントが、仮想通貨詐欺の DeepFake 動画を拡散するために乗っ取られたことを確認できました。

YouTube を悪用して脅威を広める方法は数多くあり、以下その一部を紹介します：

1. クリエイターを狙ったフィッシングキャンペーン：YouTube クリエイターに対して、コラボの提案をする不正メールを送信します。このメールを信じて連絡がとれると、コラボに必要なソフトウェアと装ってマルウェアへのリンクを送り、Cookie 盗難やアカウント情報を盗まれます。

2. 悪意のある動画説明文：詐欺師は、ゲームや効率化ツール、ウイルス対策プログラムなど、正規のソフトウェアのダウンロードを装い、悪意のあるリンクを含む説明付きの動画をアップロードすることにより、ユーザーを騙してマルウェアのダウンロードを促します。

3. チャンネル乗っ取りによる脅威の拡散：フィッシングやマルウェアによって YouTube のチャンネルをコントロールすることで、詐欺師がそのチャンネルを利用し、視聴者からの初回入金を必要とする暗号通貨詐欺など、様々な詐欺脅威を広めます。

4. ソフトウェア・ブランドと合法的に見えるドメインの悪用：信頼できる企業を模倣したウェブサイトを作成し、違法なソフトウェアのダウンロードを促します。

5. ビデオコンテンツによるソーシャルエンジニアリング：チュートリアルビデオやクラックされたソフトウェアのオファー投稿をし、有益なツールを装ってマルウェアをダウンロードするようユーザーを誘導します。この手口は、有料のサービスやソフトウェアに無料でアクセスしようとするユーザーを狙い、YouTube の検索や推薦のアルゴリズムを活用して、潜在的な被害者を狙います。

ランサムウェアのリスク比率が前四半期の 2 倍以上に上昇

ランサムウェアとは、恐喝を行うマルウェアの一種です。最も一般的なパターンは、被害者の PC 上の文書、写真、ビデオ、データベース、その他のファイルを暗号化するものです。これらのファイルが、まず復号化しなければ使用できなくなり、ファイルを復号化するために、攻撃者は「ランサム」と呼ばれる金銭を要求します。

ランサムウェアの猛威をふるっている 1 つが LockBit で、その暗号化と攻撃は引き続き続いています。LockBit への注目は依然高く、今年の 2 月 19 日には、10 カ国の法執行機関による共同作戦「クロノス作戦」が発表されたことで注目されました。また、この作戦の成果として FBI は LockBit のインフラへの侵入に成功し、約 1000 の秘密暗号鍵を確保し、公開復号化装置を公開しました。

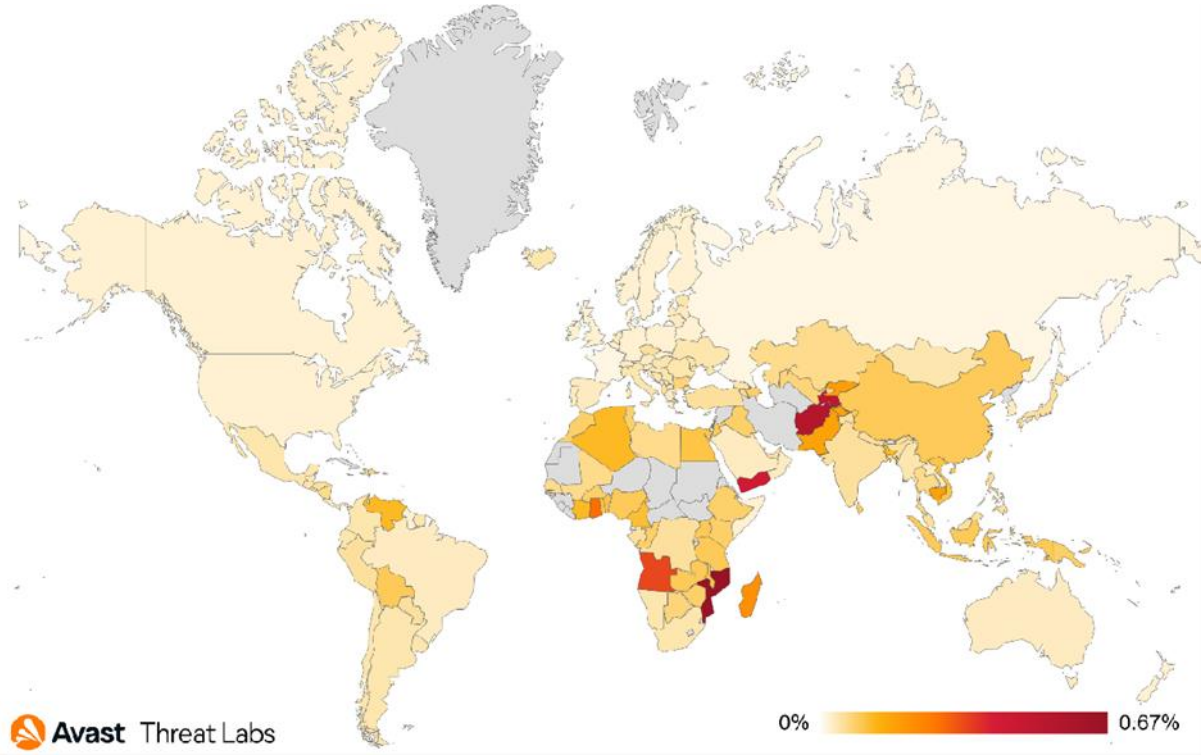
当社のユーザーベースで最も多くブロックされているランサムウェアは以下になります。

LockBit、Akira、BlackCat のような有名な脅威とは対照的に、以下のランサムウェアについてメディアで目にすることはほとんどありません。理由としては、これらの種類のランサムウェアは大企業を攻撃して、身代金として数百万ドルを要求するのではなく、個人または中小企業に焦点を当て、数千ドル単位の身代金を要求するためです。

- WannaCry (21%)
- Enigma (12%)
- STOP (12%)
- Mallox (aka TargetCompany) (3%)
- DarkSide (2%)
- Cryptonite (1%)

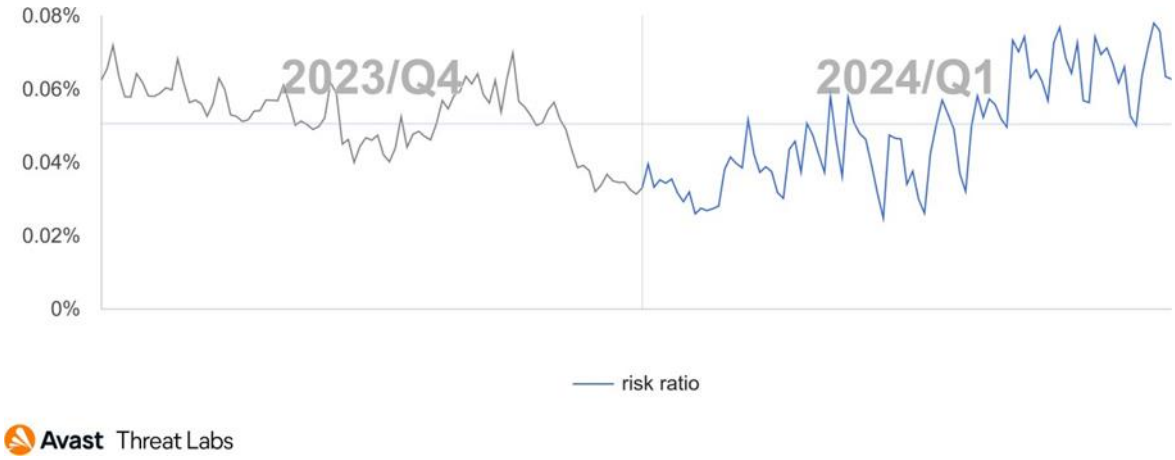
当社のユーザーベースにおけるランサムウェアの全体的なリスク比率は、前四半期と比較して増加傾向にあることが分かりました。国別のランサムウェアリスク比率は以下の地図に示されています。

特に日本、ブルガリア、チェコ、ハンガリーで大幅に増加していることがみられ、リスク比率は前四半期と比較すると 2 倍以上に増加していることがわかりました。



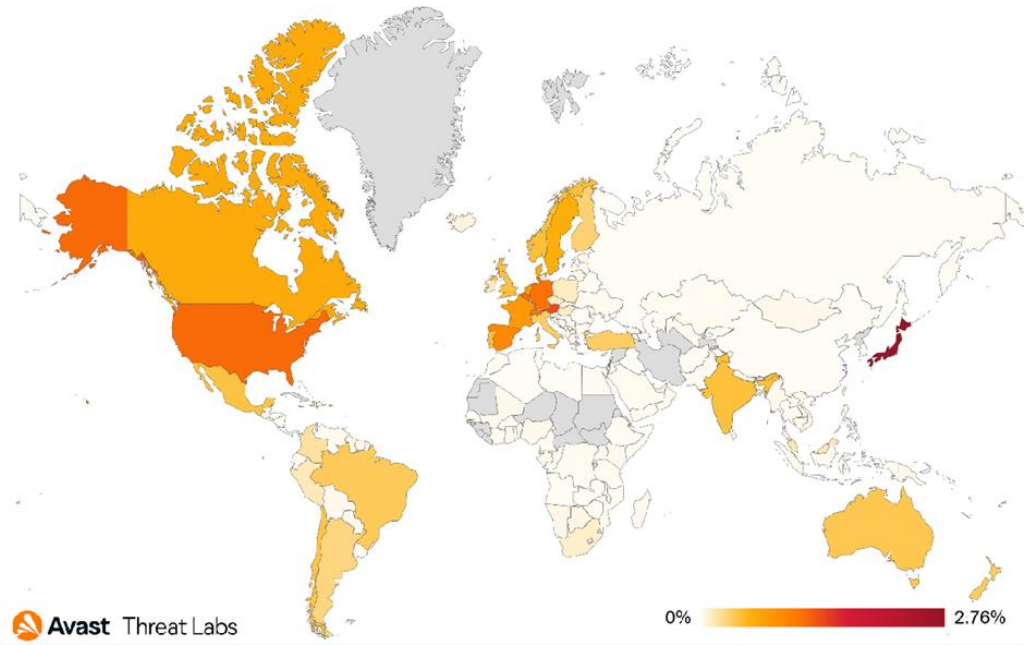
サポート詐欺、日本は 153%増加

サポート詐欺は、正規のサポート担当者を装った詐欺師が、被害者のデバイスにリモートアクセスしたり、クレジットカードや銀行口座の詳細情報などの重要な個人情報を取得しようとしたりするものです。2023 年を通して、サポート詐欺に関する活動は継続的に減少していましたが、今年の第 1 四半期では、サポート詐欺が増加傾向となりました。



スイスのサポート詐欺の活動は 177%増と今期最高の伸びを示し、サポート詐欺のホットスポットである日本も、153%の大幅増加が確認されました。

これらの数字の増加より、各地域におけるサイバーセキュリティ自体の増加傾向が浮き彫りにされ、特にヨーロッパの裕福な国々が顕著な結果をしめしている。

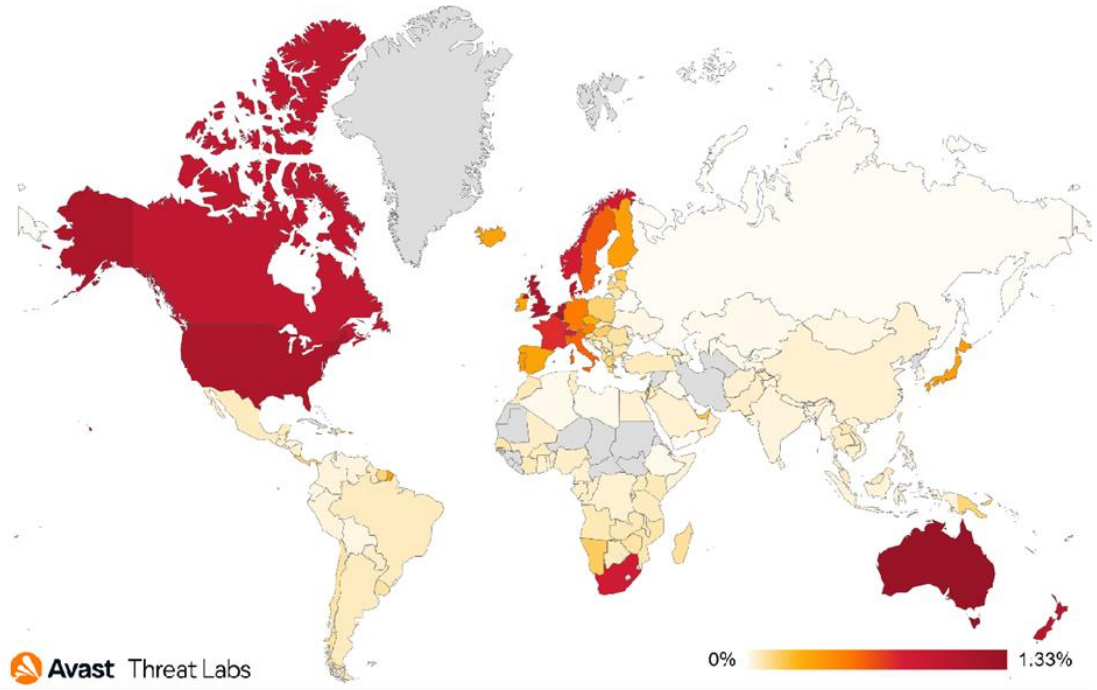


返金と請求書詐欺：iCloud データ削除詐欺

2024 年第 1 四半期に注目を集めた還付金詐欺と請求書詐欺の一つは、トップクラスのサービスを標的にし、そこから他のあまり価値のないサービスへ誘導するものがありました。標的となったアカウントは iCloud で、機密情報を含むユーザー情報を抽出する支払いゲートウェイへの TinyURL リンクが添付されていたことが分かりました。

これを防ぐために、多要素認証を有効にし保護することが重要であり、9to5 Google によると、Google ユーザーの多要素認証を有効にすることで、漏洩したアカウントが 50%減少したことが判明しています。

世界的な広がりを見ると、英語圏が欧州連合（EU）とともに最も影響を受けていることがわかる。前四半期に最も急増した国は、29%増のベルギー、13%増のイギリス、10%増のルクセンブルクである。一方、最も落ち込んだのは 29%減のオーストラリア、15%減のアメリカ、5%減のカナダである。



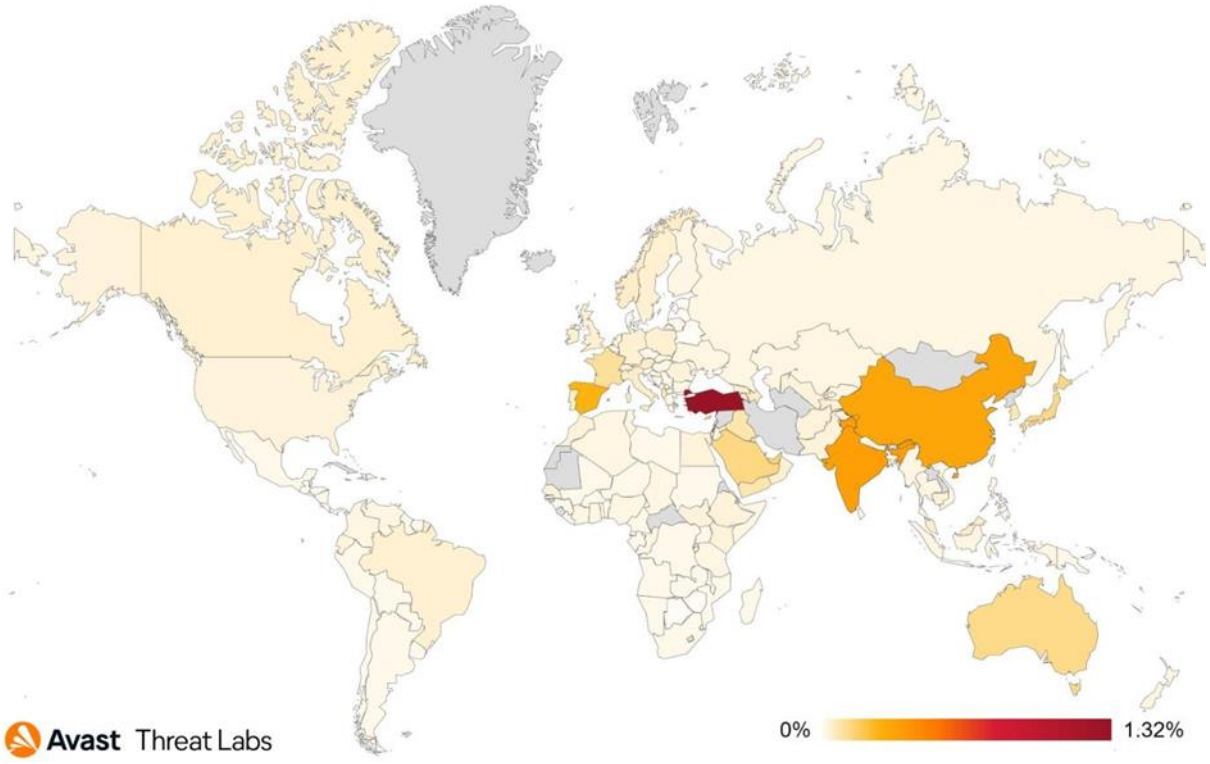
モバイルユーザーを脅かす新しい自動起動バンカー

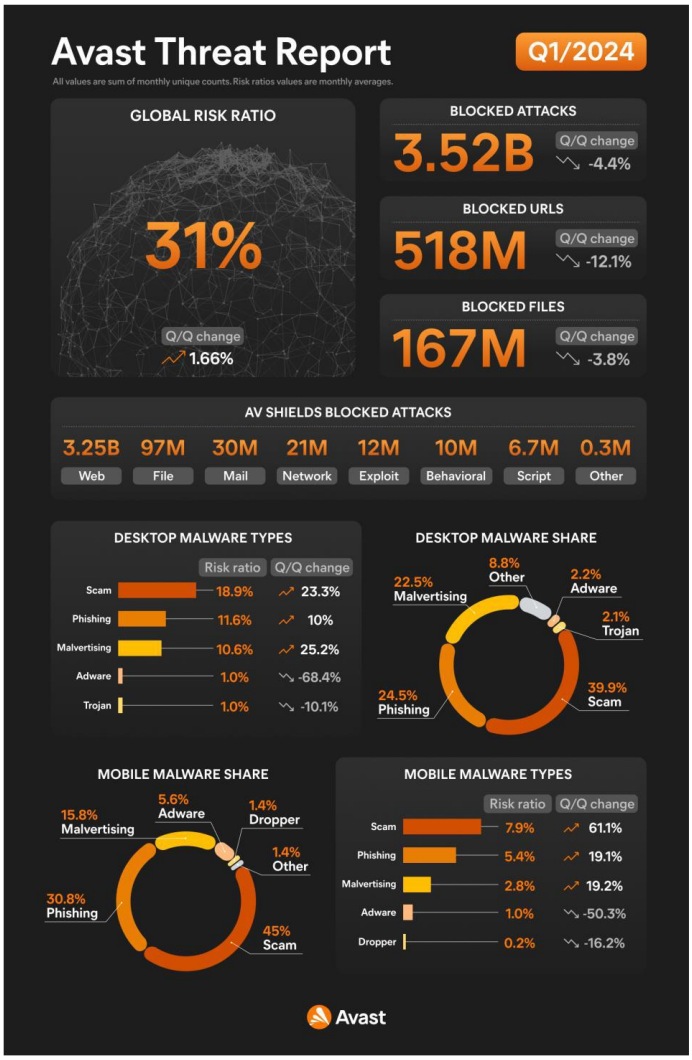
バンカー（Bankers）は洗練されたタイプのモバイルマルウェアで、銀行口座の詳細、暗号通貨ウォレット、インスタントペイメントをターゲットにし、金銭を引き出すことを目的としています。

MoqHao バンカーは、Android に内蔵された Contact Provider サービスを使用することで、インストール後に自動実行する機能を導入しています。また特別なメタデータを持つアプリマニフェストの最初のアクティビティとしてこれを設定することで、アプリがインストールされるとすぐに実行され、ユーザーが初めて実行する前に悪意のあるサービスをトリガーできるようになります。インストールされ、実行されると、MoqHao はユーザーを騙して、銀行の詳細を提供させようとするフィッシングメッセージが表示されます。その後、連絡先の詳細や SMS メッセージを取得し、C&C サーバーに送信されます。　バンカーは国別のフィッシング・メッセージをプリセットしている一方で、この目的のために特別に設定された Pinterest のプロフィール記述から動的にメッセージを読み込むことも可能で、被害者に合わせたメッセージを配信するという非常に巧妙な方法をとっています。

またこのバンカーは、偽のフィッシング SMS メッセージを通じて配信されており、多くの場合は配送サービスを装い、主に日本、 韓国、ドイツ、フランス、インドのユーザーをターゲットにしている。

2024 年第 1 四半期のバンカーのリスク比率は、トルコが最も高い結果となりました。また、RewardSteal バンカーが台頭しているインドでも、リスク比率が顕著に上昇しているのがみられました。そのほかにも韓国、日本、タイ、ベトナムといった国々が、新たなバンカーのターゲットとなっていることが明らかとなりました。





より詳細な情報については、レポート（英語）をご覧ください：
https://decoded.avast.io/threatresearch/avast-q1-2024-threat-report/

Avast について

アバストはデジタルセキュリティとプライバシーのリーダーであり、信頼できる消費者ブランドで、デジタル化が進んだ世界においてもサイバー犯罪などの危険を心配せず、自由にデジタルを使いこなせる環境「デジタルフリーダム」の実現に力を注ぐグローバル企業の Gen（NASDAQ: GEN）のブランドです。アバストは数億人ものユーザーをインターネット上の脅威から守り、モバイル、PC、Mac 向けのセキュリティ製品は、著名な第三者機関である VB100、AV-Comparatives、AV-Test、SE Labs 等によって授賞を受けています。またアバストは Coalition Against Stalkerware、No More Ransom、Internet Watch Foundation のメンバーです。詳しくは Avast.com をご覧ください。