

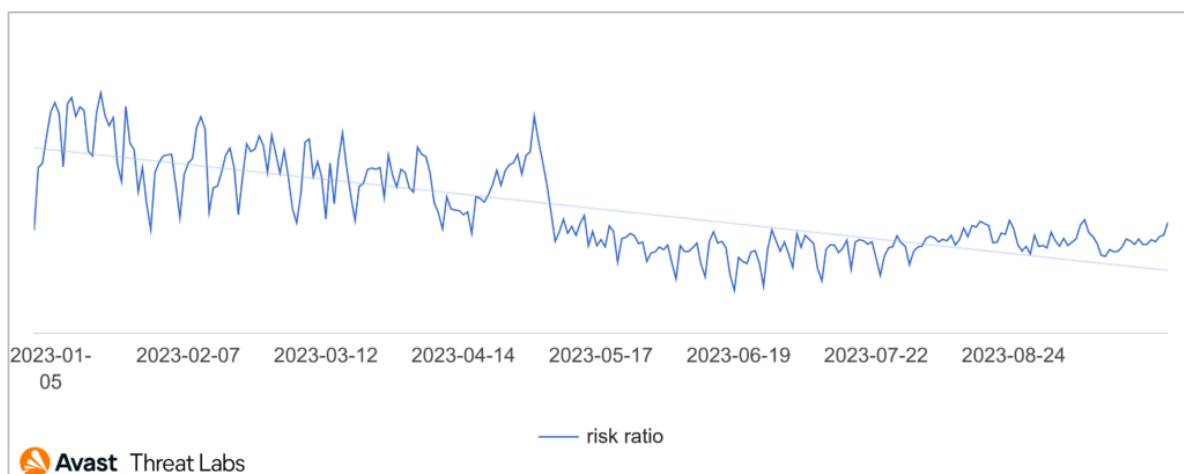
アバスト、2023 第 3 四半期脅威レポートを発表

日本のサポート詐欺のリスクは世界 2 位
SpyNote を使用した詐欺のターゲットとなっていることも明らかに

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、2023 年第 3 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、日本のインターネットユーザーがサポート詐欺に遭遇するリスクは世界的に減少傾向であるなか、リスク比率において、日本はドイツに次いで世界 2 位となりました。また詐欺攻撃も前四半期と同様に世界的に増加傾向であり、日本のリスク比率も 19%上昇していることが分かりました。さらに、メッセージ、写真、位置情報、ログイン情報などの個人情報を抽出する目的で使用されるスパイウェアは、「Spymax」が引き続き世界的に猛威を振るい、新たに「SpyNote」というものも登場しました。また SpyNote/Spymax の別バージョンが、日本ユーザーをターゲットとして公共料金や水道料金の未払いの支払いを要求する、偽 SMS メッセージとして使用されたことが分かりました。

日本のサポート詐欺に遭遇するリスクは、世界で 2 位に

サポート詐欺の脅威としては、正規のテクニカルサポート担当者を装った詐欺師が被害者のデバイスへリモートでアクセスし、クレジットカードや銀行口座の詳細などの機密の個人情報を取得しようとするのが挙げられます。これらの詐欺は被害者の信用を得るために信用詐欺の手口を使い、多くの場合、不必要なサービスの料金を支払ったり、高価なギフトカードを購入したりするよう促します。被害にあわないためには、テクニカルサポートサービスを提供すると主張する人物が、本当にその立場にあるのかを注意深く確認することが重要です。

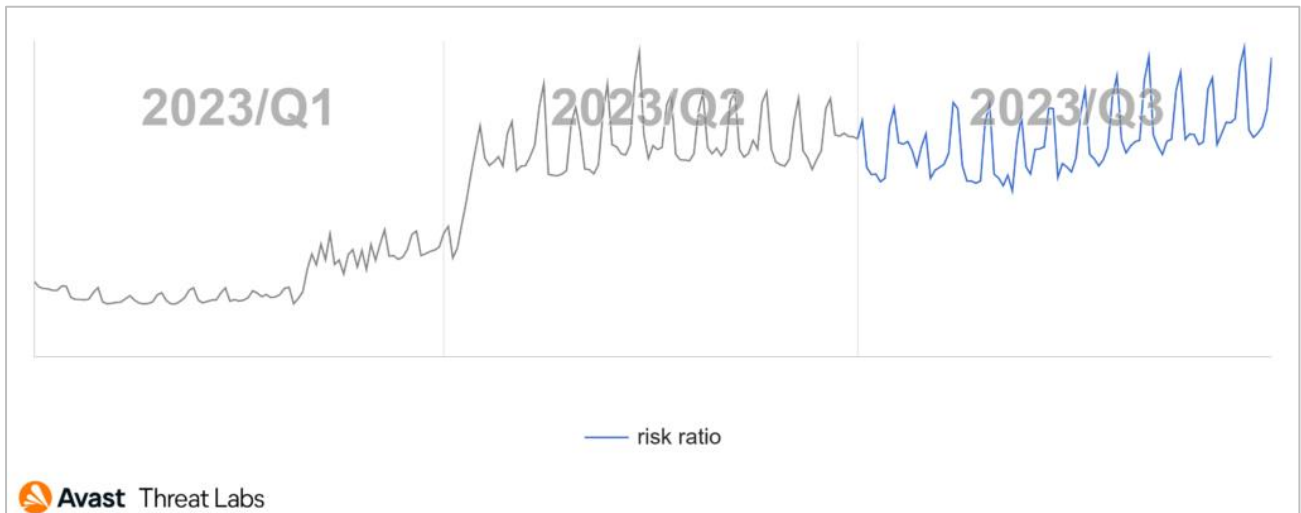


レポートによると上記全体のグラフでは世界的には大きな変化はなく、むしろ第 2 四半期からは減少傾向となっています。一方で全体的な減少傾向にもかかわらず、各国間の検出率に関しては顕著な変化

が観察され、前四半期と比較すると、主に、ドイツ、日本、アメリカ、スイス、カナダでサポート詐欺の被害が多く、日本はドイツに次いで世界で 2 番目に高い結果となりました。

詐欺被害に遭遇するリスクが 19%も上昇

ユーザーをだまして攻撃者に個人情報や金銭譲渡を目的とした詐欺の増加が確認されています。2023 年第 2 四半期に見られた詐欺脅威の大幅な増加は、第 3 四半期でも引き続き見られました。以下のグラフからもわかるように、8 月中旬からも同様に詐欺脅威の増加傾向が確認されました。



詐欺に遭遇するリスクは著しく高まっており、最も影響を受けた国は、日本 (+19%)、ギリシャ (+17%)、米国 (+14%)、オーストリア (+13%)、ドイツ (+12%) でした。

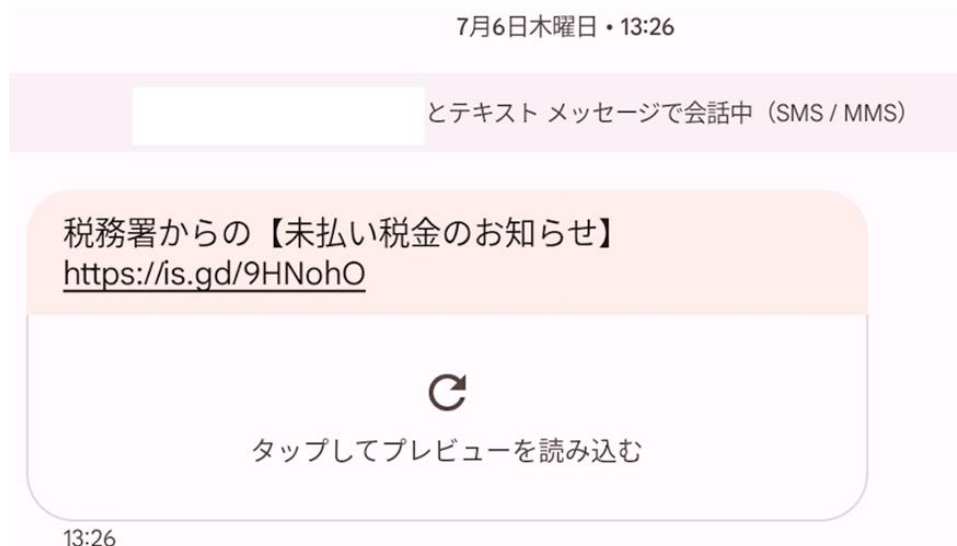
一例として暗号通貨詐欺があり、この詐欺が拡散されるプラットフォームとしてソーシャルメディアが世界的にターゲットとなっています。暗号通貨詐欺は、イーロン・マスク、ミスター・ビースト、ドナルド・トランプなどの有名な人物のディープフェイク動画で始まることが多く、プラットフォームにサインアップし、アカウントを確認するために少額の手数料だけ支払えば、多額のビットコインが手に入ると謳っています。しかし、実際はビットコインが手に入らない上に、プラットフォームに送金された資金が詐欺師によって盗まれ、取り返しはつきません。

その他にも、マルバタイジングの活動が夏季休暇を終え、人々が学校や職場に戻った 9 月に急増しました。サイバー犯罪者は、ポップアップ・メッセージやプッシュ通知で有名企業のロゴを悪用し、デバイスがウイルスに感染していると通知します。そして、これらのポップアップからフィッシングサイトへ誘導し、ウイルス対策サービスの提供を装ってクレジットカード情報の入力を求めるものとなっています。プッシュ通知は特にモバイルで効果的で、不在連絡や新しいテキストメッセージ通知などシステム通知を装い、騙すことが多く見られます。

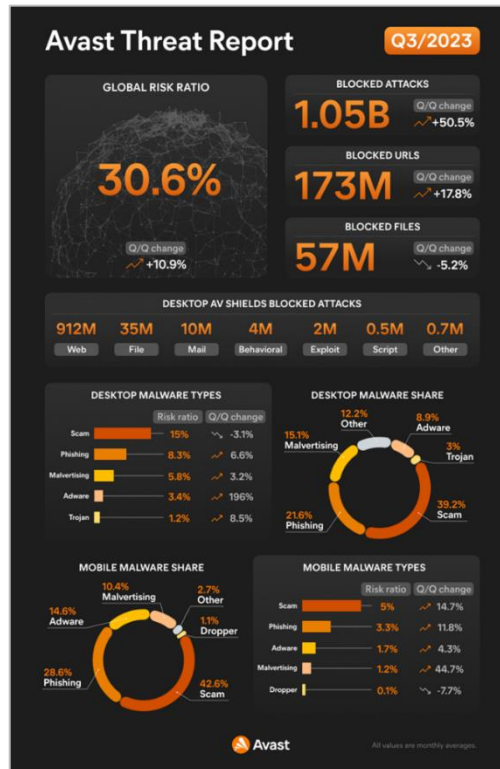
日本がターゲットとなったスパイウェアに注意

スパイウェアは、被害者を監視するために、メッセージ、写真、位置情報、ログイン詳細などの個人情報情報を抽出し、疑いを抱かぬ罪なき人々の情報を抜き取ってしまいます。偽の広告、フィッシングメッセージ、人気のあるアプリケーションの改変を通じ、ユーザー情報の拡散および収集します。特定の国家が支援する商用スパイウェアはますます蔓延しており、個人をターゲットにしたゼロデイエクスプロイトの使用が第 3 四半期で確認されました。

今四半期はスパイウェアの存在感が若干低下しており、Spymax がスパイウェアの中でトップの座を維持し、SexInfoSteal と FaceStealer が僅差で続いています。この四半期にスパイウェアとして新たに追加されたものには、人気の高いメッセージング・アプリケーションをトロイの木馬に感染させたものがいくつかあり、SpyNote も再登場しました。



また SpyNote/Spymax の別のバージョンのものが、日本のユーザーをターゲットとした短いキャンペーンの一環として使用され、公共料金や水道料金の未払いに関する偽の SMS メッセージが送信されました。緊急性を装うこれらのメッセージは、被害者を一連のフィッシングサイトに誘導し、デバイスに SpyNote をダウンロードさせます。その後マルウェアがインストールされると、ユーザーは設定を開きいてアクセシビリティサービスを有効にするよう指示されます。その際マルウェアが同時にインストールされデバイス上に脅威自身を隠すことができるようになります。潜ませることが可能になってしまいます。その後、被害者の個人データを監視している間にながらし、デバイス上の認証アプリにアクセスし、ソーシャルメディアの資格情報を盗んでいたことが確認されました。



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-q3-2023-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。