2023
年世界モバイル脅威レポート

エグゼクティブサマリー

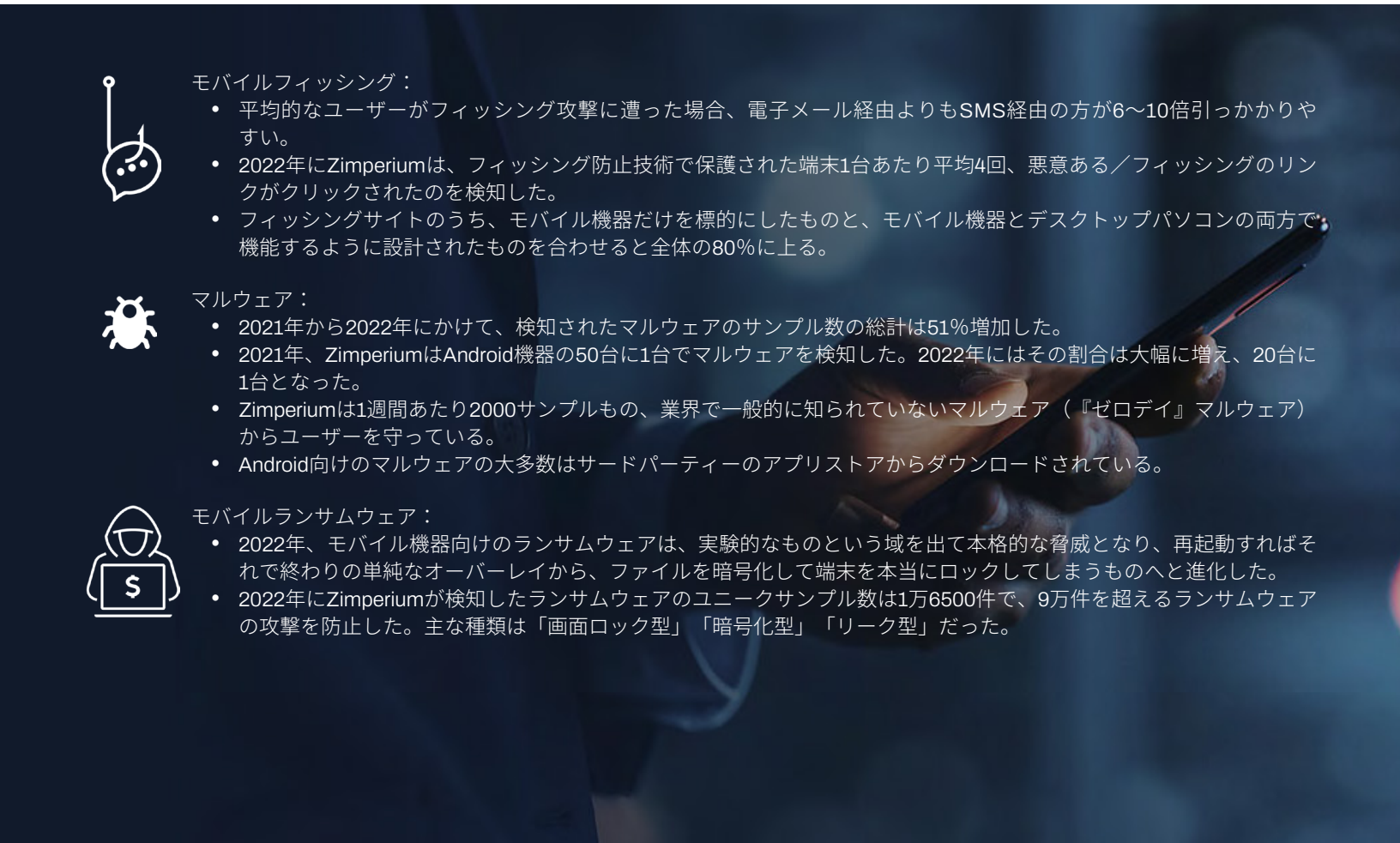
ZIMPERIUM®

業務そして商取引の軸足は、モバイルファーストへと移りつつあります。近年ではモバイル機器の利用が世界中で進み、日常生活とは切っても切れないものになりつつあります。モバイル機器は、コミュニケーションを取ったり道を調べたり、写真を撮ったり、情報を得たりするのに日々使われています。仕事においても欠かせないものとなっており、これまでノートパソコンやデスクトップパソコンからアクセスしていたデータに、最近ではモバイル機器からアクセスするようになっています。私たちの日常生活の欠かせない一部になっているのは、モバイル機器だけではありません。モバイルアプリも買い物や銀行利用などさまざまなことを行うエコシステムになっています。また、モバイルアプリは自動車やエンターテイメントシステム、ホームセキュリティシステム、医療機器、ヘルストラッカーと情報をやりとりしたり操作する際の仲介手段にもなってきています。

この大転換期に乗り遅れまいと、世界中の企業がモバイル活用企業へと変貌しつつあります。そうした企業が掲げるモバイル活用の取り組みは、収益性や生産性、競争力の向上に欠かせません。そうした取り組みは、企業にも従業員にも消費者にも利益をもたらしています。いくつか例を挙げると、さまざまなデバイスを使ったリモートワークやモバイルバンキング、遠隔医療、モバイル機器からのネットショッピングなど――。

ただし問題もあります。そうした大切な取り組みの核であるアプリやデバイスの重要性を、犯罪者集団はよく分かっている。攻撃する理由には事欠かないわけだ。攻撃する側が戦略に磨きをかけて最大限の利益を得ようとする中で、脅威は量的に増えているばかりか高度化もしているのが現状です。機器、ネットワーク、フィッシング、アプリへの攻撃を組み合わせ、犯罪者たちはモバイル活用の取り組みの根幹を危機にさらしています。その結果、先進的な組織は従来型の手法を新しいモバイル世界に向けて応用するだけでは不十分だと認識し、モバイルファーストのセキュリティ対策を取るようになっています。

Zimperium の 2023 年世界モバイル脅威レポートの狙いは、ビジネスにおけるモバイル活用の取り組みの根幹を揺るがす脅威に対する、客観的で事実に基づく視点を提供することであり、モバイルファーストのセキュリティ戦略の指針についてあらましを説明することです。本レポートはモバイルファーストのセキュリティ対策を取っている数百の企業や政府機関で確認された事象や Zimperium zLabs の独自の調査に基づいています。以下ではその中から、脅威が質・量ともに増していることを示すいくつかのデータをご紹介します。



モバイルフィッシング：

- 平均的なユーザーがフィッシング攻撃に遭った場合、電子メール経由よりもSMS経由の方が6〜10倍引っかかりやすい。
- 2022年にZimperiumは、フィッシング防止技術で保護された端末1台あたり平均4回、悪意ある／フィッシングのリンクがクリックされたのを検知した。
- フィッシングサイトのうち、モバイル機器だけを標的にしたものと、モバイル機器とデスクトップパソコンの両方で機能するように設計されたものを合わせると全体の80%に上る。

マルウェア：

- 2021年から2022年にかけて、検知されたマルウェアのサンプル数の総計は51%増加した。
- 2021年、ZimperiumはAndroid機器の50台に1台でマルウェアを検知した。2022年にはその割合は大幅に増え、20台に1台となった。
- Zimperiumは1週間あたり2000サンプルもの、業界で一般的に知られていないマルウェア（『ゼロデイ』マルウェア）からユーザーを守っている。
- Android向けのマルウェアの大多数はサードパーティーのアプリストアからダウンロードされている。

モバイルランサムウェア：

- 2022年、モバイル機器向けのランサムウェアは、実験的なものという域を出て本格的な脅威となり、再起動すればそれで終わりの単純なオーバーレイから、ファイルを暗号化して端末を本当にロックしてしまうものへと進化した。
- 2022年にZimperiumが検知したランサムウェアのユニークサンプル数は1万6500件で、9万件を超えるランサムウェアの攻撃を防止した。主な種類は「画面ロック型」「暗号化型」「リーク型」だった。

スパイウェア：

- 2022年にZimperiumが検知したスパイウェアのユニークサンプルは3200件に上った。
- スパイウェアに感染した機器の割合が最も高かったのはEMEA（欧州、中東、アフリカ）と北米で、EMEAは35%、北米は25%だった。
- スパイウェアのキット、サービス、ソースコードはダークウェブ上で普通に取引され、シェアされている。GitHubのような大手リポジトリやRedditのようなオンラインコミュニティでもやりとりされている。

脆弱性とその悪用：

- 2022年にセキュリティ侵害が検知されたアンドロイド端末のうち53%は、ユーザーによるroot化だけでなく、外部の攻撃者によってコントロールされていた。セキュリティ侵害が検知されたiOS端末のうち、18%が脅威アクターによって悪用されていた。全体的に見ると、セキュリティ侵害を受けた機器のうち23%が、単に脱獄もしくはroot化されただけでなく悪用もされていた。
    - o レポート公開時点で、セキュリティの侵害が検知されたすべての機器のうち 43%は脱獄も root 化もされていなかった。これは 2022 年の数字と比べ 187%の増加となる。Android の方が多いのは例年通りだが、iOS でもセキュリティが侵害されたすべての機器のうち攻撃者によってコントロールされていたものは 41%で、2022 年から 127%増えていた。
- 2022年にモバイル機器上で活発に悪用されたゼロデイ脆弱性の80%はiOSのものだった。
- 2022年にAndroidのオペレーティングシステムで発見された脆弱性の数は増加し、過去最高の897個のCVEが確認された。深刻度が「Critical」に分類された脆弱性は47個で、2021年と比べて138%の増加だった。
- iOSのオペレーティングシステムで発見された脆弱性の数は2021年の380個から2022年には242個に減少した。このうち27個が深刻度「Critical」に分類されたが、これは2021年と比べて40%少なかった。

アプリのリスク

- iOS向けの全アプリの約2%、Android向けの全アプリの約10%が、安全でないクラウドインスタンスにアクセスしていた。
- 金融サービス業界では、高度化する一方のトロイの木馬による攻撃が続いている。こうしたトロイの木馬は認証情報や金を盗み取るために設計されており、多い場合はすべての金融サービスアプリの50%超を狙った例もある。

2023 年世界モバイル脅威レポートの目的は、情報や分析を集め、まとめ、整頓して提供することにより、世界の企業や組織が十分な情報に基づいてモバイル活用の取り組みを守るための断固とした行動を取れるよう支援することにあります。私たちは組織外からの視点も含むさまざまな視点から意味を引き出すことを狙い、データを集めました。さまざまな角度からモバイル脅威の全容を見られるようにするためです。

- **1 つ目はモバイル機器のアタックサーフェスを調べ、1 年分のモバイル脅威のデータを検討することです。特に注目したのは、具体的にはモバイル機器への脅威や具体的なモバイルアプリの脅威のトレンドです。**
- **続いては、パートナーである Riscure や RSA、SentinelOne や Trellix などのパートナーからの情報も得て、モバイル脅威と現代のモバイルセキュリティ戦略がセキュリティのエコシステム全体に与える影響について調べます。**
- **それから、主要なモバイル攻撃ベクトルや、悪用されたモバイル脆弱性、モバイルフィッシングのトレンド、モバイルマルウェアのトレンドなど、現場から集めたモバイル脅威データに関する要約と、タイムリーな分析を提供します。**

こうした情報や視点が直接的に、これからの 1 年の皆様の組織の戦略や投資の検討材料となれば幸いです。私どもは、さらに安全で、なおかつインターネットとの接続性が高まっていくモバイル活用世界を支えるという責務を果たして参ります。

さらに詳しくお読みになりたい場合、
リポート全文のダウンロードをご希望の場合は以下にアクセスして下さい。
www.zimperium.com/global-mobile-threat-report