【プレスリリース】

マカフィー株式会社
2021 年 6 月 30 日

※当資料は米国時間 2021 年 6 月 28 日に、米国で発表されたプレスリリースの抄訳です。

マカフィー、モバイル脅威レポート最新版を公開
ロックダウン中の 1 年で、銀行、請求、新型コロナワクチンを狙った
モバイルマルウェアが急増

ハッカーはパンデミックを悪用し、無防備な消費者を標的に

ニュースハイライト：

- 2021 年はマルウェアによる偽情報やステルス攻撃の年になると予測
- マカフィーが検出したモバイルマルウェアの総数は、2020 年末（第 4 四半期）時点で 4,300 万件、このうち 300 万件超が新規検出
- 「トロイの木馬」がパンデミック関連のマルウェア全体の 90%を占め、一般ユーザーの最大の脅威の 1 つに
- ハッカーはモバイルマルウェア「Etinu」によりユーザーに気付かれる事なく、SMS メッセージを読み取り、プレミアムサービスのサブスクリプション認証に必要な情報を抽出。検出・削除されるまでに 70 万超のダウンロードが行われたと報告

デバイスからクラウドまでを保護するサイバーセキュリティ企業である米国マカフィー（McAfee Corp、本社：米国カリフォルニア州、Nasdaq：MCFE）の Advanced Threats Research チームは、「モバイル脅威レポート 2021」（英語）を発表しました。本レポートにおいて、ハッカーが偽アプリ、トロイの木馬、詐欺メッセージを悪用して一般ユーザーを狙っていることが明らかになりました。昨年、一般ユーザーが直面した最もアクティブなモバイル脅威は「隠しアプリ」でした。1 年間のロックダウン（都市封鎖）と、オンライン、デバイス使用時間の急増という機に乗じて、ハッカーたちは多くのアプローチを通じて利益を得ています。マカフィーは最新の調査結果に基づき、世界の大部分で COVID-19 への懸念が続き、ワクチンへの需要が高い中、ハッカーが偽アプリ、テキストメッセージ、ソーシャルメディアへの招待を使っていかに人々の恐怖心につけこんでいるかを明らかにしています。

マカフィーのコンシューマービジネスグループ シニアバイスプレジデントのジュディス・ビターリ（Judith Bitterli）は、次のように述べています。「パンデミックは消費者の生活様式を変えました。ハッカーはこれに適応し、一般ユーザーを狙った多種多様な攻撃方法へとシフトしました。多くの人々がこれまでになくオンラインを利用するようになる中、私たちは、一般ユーザーのデジタル習慣に改めて目を向け、本人とその友人や家族にとって大切なもの、つまり個人情報を保護するために、できること

は全て行うつもりです。依然として世界に蔓延しているモバイル脅威は、ハッカーが一段と高度な方法を取り入れ、今後も継続していくことでしょう。私たちは、一般ユーザーの個人のデバイスだけでなく、より大切な個人データも保護することを目指しています。」

この 1 年間、ワクチンの供給スピードは世界各地において異なり、ハッカーに多くの機会をもたらす結果となっています。マカフィーATR のリサーチャーは、ハッカーが偽のワクチン接種予約や登録画面の広告内にマルウェアや悪意あるリンクを潜ませていることを発見しました。これらは、偽の広告を表示しているデバイス上にマルウェアをダウンロードする危険性があるだけでなく、デバイスへのアクセス機能を稼働させ、ハッカーがデバイスを完全に制御して銀行口座情報や認証情報を盗み出してしまうおそれがあります。調査によると、懸念すべきことにこれらのサイバー攻撃のいくつかは、ワクチンが正式に承認される前の昨年 11 月に早くも開始され、新型コロナとの戦いで各国でのワクチン接種プログラムが進む中、なお続いています。

マカフィーのチーフサイエンティスト兼フェローのラージ・サマニ（Raj Samani）は、次のように述べています。「パンデミックはモバイルデバイスへの依存度を高めただけでなく、悪意ある攻撃者が一般ユーザーをだまして個人情報を盗み取る新たな方法の開発を後押ししたことも判明しました。こうした高度なマルウェアや詐欺に加えて、新たな手口による請求詐欺も復活していることが明らかになりました。一般ユーザーは慌ただしく日常の活動を続けているため、個人データの保護についてよく理解し、積極的に取り組むことが重要です。」

モバイル脅威のトレンドは、以下の通りです。

- **新型コロナ関連マルウェア：**McAfee COVID-19 ダッシュボード（英語）によると、パンデミック関連マルウェアの 90%以上がトロイの木馬の形式でした。マカフィーのリサーチャーは最も初期のワクチン詐欺攻撃キャンペーンの一部として、インドの一般ユーザーを標的とした SMS ワームの痕跡を発見しました。SMS メッセージや WhatsApp メッセージは共に、ユーザーにワクチンアプリをダウンロードするように促し、ダウンロードされると、SMS や WhatsApp を介してユーザーの連絡先リスト全員に対してマルウェアが送信しました。この攻撃キャンペーンで使われたマルウェアは、昨年 7 月にインドで TikTok アプリが禁止された際に関係していたものと同じファミリーです。

- **気付かれずに商品を購入させる請求詐欺マルウェア：**マカフィーのリサーチャーは、Etinu と呼ばれるモバイルマルウェアに関する新しい情報を得ました。主に南西アジアと中東のユーザーを狙った Etinu は Google Play を介して配布され、検出・削除されるまでに 70 万回超ダウンロードされました。この請求詐欺アプリが Google Play ストア経由でインストールされると、マルウェアは通知リスナー機能を使用して着信 SMS メッセージを盗み出します。その後、プレミアムサービスとサブスクリプションへのサインアップと購入ができるようになり、ユーザーのアカウントに請求されます。

- **ハッカーは、世界中の数百の金融機関を標的とするバンキング型トロイの木馬を使用：**マカフィー モバイルセキュリティは、バンキング型トロイの木馬の活動が 2020 年第 3 四半期から第 4 四半期の間に 141%増加したことを確認しました。ほとんどのバンキング型トロイの木馬は、Google のスクリーニングプロセスを回避するため、フィッシング SMS メッセージなどのメカニズムを介して配布されています。マカフィーは調査中に、一般的なバンキング型トロイの木馬である Brazilian Remote Access Tool Android（BRATA） を発見しました。これは、Google Play ストアに繰り返し登場し、何千ものユーザーをだましてダウンロードさせていました。

マカフィーについて

マカフィーはデバイスからクラウドまでを保護するサイバーセキュリティ企業です。業界、製品、組織、そして個人の垣根を越えて共に力を合わせることで実現するより安全な世界を目指し、マカフィーは企業、そして個人向けのセキュリティ ソリューションを提供しています。
詳細は https://www.mcafee.com/enterprise/ja-jp/home.html をご覧ください。

＜本情報のお問い合わせ＞

マカフィー株式会社（ https://www.mcafee.com/enterprise/ja-jp/home.html ）
広報担当 戸田
Tel: 070-2680-0731
hiromi_toda@mcafee.com