【プレスリリース】

マカフィー株式会社
2020 年 3 月 12 日

※当資料は、米国時間 2020 年 3 月 4 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、最新のモバイル脅威レポートを公開
2020 年は「隠しアプリ」によるモバイルステルス攻撃の年に

モバイルの「隠しアプリ」と独自の配信方法で一般ユーザーを標的にするハッカーが出現

ニュースハイライト：

- 2020 年は「隠しアプリ」によるモバイルステルス攻撃の年と予測
- 隠しモバイルアプリが、2019 年のモバイルに対する悪意ある脅威全体のおよそ 50%に
- 偽のセキュリティ警告で被害者をだまし、危険な設定を有効にさせ、望まない自動アクションを実行するモバイルマルウェアファミリー「LeifAccess」

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 LLC、本社：米国カリフォルニア）は、「モバイル脅威レポート 2020」を発表しました。本レポートにおいて、ハッカーがモバイルの隠しアプリ、サードパーティーのログイン機能、偽のゲーム動画を使用して、一般ユーザーを標的にしていることが明らかになりました。昨年、ハッカーはバックドアや仮想通貨マイニングなど、多岐にわたる方法で一般ユーザーを標的にしていました。最新の調査結果に基づき、マカフィーは、ハッカーが攻撃を隠す手法を拡大し、特定および駆除がますます困難になっていることを明らかにするとともに、2020 年は「隠しアプリ」によるモバイルステルス攻撃の年になると予測しています。

マカフィーは、一般ユーザーが直面する最も危険なモバイルの脅威は「隠しアプリ」であり、2019 年では悪意あるアクティビティ全体の 50%近くに及んだと明らかにしました。2018 年から 30%増加しています。2030 年までに、一人当たりのネットワークに接続しているデバイスの所有数が 15 台になると予測される中、ハッカーは一般ユーザーが最も時間を費やすチャネル、すなわちデバイスを通じて彼らを狙っています。隠しアプリは、サードパーティーのログインサービスを使用したり、望まない広告を配信するなどさまざまな方法で、疑いを持たない一般ユーザーにつけこんできます。

マカフィーのコンシューマービジネス担当エグゼクティブバイスプレジデントのテリー・ヒックス（Terry Hicks）は次のように述べています。「一般ユーザーは、今まで以上にインターネットにつながっています。セキュリティの現状と将来のリスクを考慮すると、一般ユーザーにとってより大切なもの、つまり個人データ、家族、友人を保護するためにできるあらゆることにしっかりと取り組んでいきたいと考えています。水面下でデータを盗んでいくモバイル脅威が台頭してくる中、一般ユーザーにとって最も価値ある資産とデータの保護強化に引き続き注力していきます。」

「モバイル脅威レポート 2020」は、モバイルの脅威トレンドとして、以下を強調しています。

- **ゲーム人気に便乗して一般ユーザーを騙すハッカー：**ハッカーは人気のゲーマー向けチャットアプリのリンクを介して悪意あるアプリを配信したり、偽アプリへのリンクを含む独自コンテンツのチート動画を配信するなど、ゲーム人気を利用しています。これらのアプリは、本物のアプリによく似たアイコンで本物になりすまし、望まない広告を配信してユーザーデータを収集します。マカフィーのリサーチャーは、FaceApp、Spotify、Call of Duty などの人気アプリにはすべて、疑いを持たない一般ユーザー、特に若者を狙おうとする偽のバージョンがあることを明らかにしました。

- **サードパーティーのサインオン機能を使用してアプリのランキングシステムを操作する新たなモバイルマルウェアが出現：**マカフィーのリサーチャーは、「LeifAccess（別称 Shopper）」と呼ばれるモバイルマルウェアファミリーに関する新たな情報を明らかにしました。このマルウェアは、Android のアクセシビリティー機能を利用して、アカウントの作成、アプリのダウンロード、被害者のデバイスに設定された名前とメールによるレビューの投稿を行います。マカフィーのリサーチャーは、「LeifAccess」をベースとする不正アプリがソーシャルメディア、ゲーミングプラットフォーム、詐欺的広告、およびゲーマー向けチャットアプリを介して配信されていることを確認しました。偽の警告を発し、ユーザーにアクセシビリティー機能を有効化させることでマルウェアのあらゆる機能を有効にします。

- **正規の交通アプリを介して機密データを盗む独自のアプローチ：**マカフィーのリサーチャーは、韓国の交通アプリが機密ファイルをアップロードする「MalBus」と呼ばれる偽のライブラリやプラグインにより不正アクセスされたことを明らかにしました。この攻撃は、オリジナルの開発者の Google Play アカウントをハッキングすることで、韓国の正規の交通アプリに潜んでいました。この交通アプリは 5 年以上にわたり、韓国の地域ごとのバス停の場所、路線図、時刻表など幅広い情報を提供していました。「MalBus」は、ハッカーが評判の高い人気アプリの正規開発者のアカウントを狙うという、既存の攻撃手法とは異なります。

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。「一般ユーザーのデジタル世界をリモートコントロールするデバイスから、貴重なリソースと大切なデータを水面下で盗む、隠しアプリが非常に増えています。これまで以上に一般ユーザーにとって必要なことは、新たな脅威を認識するとともに、正規のアプリストアを利用したり、レビューを注意深く読むなど、自身を守るために取るべき手段を講じることです。」

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/ja-jp/ 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/ja-jp/ ）
広報担当 戸田
東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 20 階
Tel: 070-2680-0731 Fax: 03-5428-1480
hiromi_toda@mcafee.com