アンラボ・セキュリティレター

Press Ahn

2017.9　Vol.45

不正アプリの高度化、最新の手法と対策

THREAT ANALYSIS MALICIOUS APPS

不正アプリの高度化、最新の手法と対策

最近、韓国ではボイスフィッシングと偽の金融機関アプリを組み合わせた融資詐欺事件が発生した。海外ではアイコンを隠したまま端末にインストールされた悪質なアプリが、ユーザーの金融アプリとウーバー(Uber)など予約関連アプリの使用情報、通話履歴、メッセージ情報を奪取し、通話内容まで録音していたことが発覚した。これまでは文字メッセージを利用して不正アプリのインストールを誘導する手法が多かったが、直近は Web やフィッシングサイトを利用したり、ボイスフィッシングと組み合わせてインストールを誘導するものまで登場した。さらにアイコンやショートカットを非表示にして、ユーザーがアプリのインストール状況を把握できないようにするなどますます攻撃手法が高度化している。今回のコラムは不正アプリがインストールされたときの症状やこれらのアプリを確認する方法について説明した。

ケース 1)

不動産費用などで追加融資を悩んでいたAさん。なぜかタイミングよく有名なキャピタル会社から融資案内の電話がかかってきた。先方は Aさんのクレジット照会のためスマートフォンにアプリをインストールするように案内した。Aさんがアプリインストール後、案内通りまた電話がかかってきたが、その時の発信者情報には有名な銀行名と代表番号が表示されていた。話を聞いたところ、利子を前納すると貸出が可能であるという。通話終了後、腑に落ちなかった Aさんは警察に連絡して先ほどの電話番号の照会に当たってみたが、警察でも問題なしと太鼓判を押された。やっと安心できた Aさんは前納分の利子に相当する金額を送金した。ところが数日後、Aさんはキャピタル会社ではなく警察から連絡を受けた。実は Aさんがインストールしたアプリは不正アプリであり、インストール後にかかってきた銀行からの電話も、確認を取った警察も、すべては不正アプリからボイスフィッシング組織に接続するように仕向けられたものだった。

ケース 2)

通勤中にモバイルゲームを楽しむ Bさんは、最近サービスを開始したゲームアプリをダウンロードするかどうか迷っていた。そしてよくアクセスするコミュニティサイトをのぞいて見ると、そのゲームアプリのファイルを共有するという書き込みがあった。Google Play Storeでは有料配信されるアプリだったが、ネットからダウンロードすると無料でプレーできるらしい。Bさんは迷わずファイルをダウンロードして端末にインストールし、すぐにゲームをプレーした。だが数日経ってからいくつもの広告バナーが表示され始めた。広告を表示しないようにするには『指紋やPINコードでログインせよ』とガイドされ、入力してみたらさらに別のアプリを追加インストールしろという。その時点でやっと「おかしい」と気づいた。

「モバイルマルウェア」と呼ばれる悪質なアプリは大きく2つのタイプに分かれる。一つ目は正常なアプリや有名なアプリを装って悪意ある機能を実行するタイプだ。名前やアイコン画像などを巧みに偽装してユーザーを騙す。次にゲームやユーティリティなどユーザーが必要とする機能を提供するが、広告表示などユーザーが不要とする機能も実行して不快感を与えるタイプがある。双方ともに大なり小なりのダメージを与えるという点で悪質な不正アプリとしてみることができる。

これらの不正アプリはサードパーティ(Third-Party)ストアだけでなく正常なアプリストアでも配信されている。最近の調査によるとGoogleのPlay Storeとサードパーティのアプリストアに1,000個以上の不正アプリが存在することが分かった。韓国ではGoogle Playや検察庁を詐称したアプリをはじめ、大手銀行や有名キャピタルを詐称する不正アプリが増加している。特にオリジナルの銀行アプリアイコンが変更されると、不正アプリもこれに合わせてアイコンを変更するなどオンタイムで高度化された動きを見せている。

悪質な不正アプリのインストール誘導手法が高度化

ユーザーが悪質なアプリをインストールするように誘導する手法も、より多様化した。代表的なものとして前述した「ケース1)」のように融資業者を装ったボイスフィッシングと連携して不正アプリのインストールを誘導する手法がある。この手法でインストールされたアプリは、[図1]のように有名な銀行の貸出サービスに関する画面を表示する。この画面に表示された相談窓口の電話番号と金融監督院の苦情相談電話番号は、実際の電話番号と同じである。しかしナンバーの部分をタップして電話をかけると、攻撃者があらかじめ仕掛けておいた番号に接続される。もしユーザーが直接入力して電話をかけるとしても、強制的に着信先を切り替えるため攻撃者が操作しておいた番号に接続する。その際、画面にはユーザーが入力した電話番号が表示されるため偽者だと疑いにくいのである。

[図1] 有名な某銀行の貸出サービスアプリそっくりの不正アプリ

5月には PCからインターネットを利用するユーザーを狙って「有害サイト遮断案内ページ」を装ったサイトとQRコードを利用し、不正アプリのインストールを誘導するケースも確認された。

[図2]のように本物のサイトとそっくりのページを展開して「トラフィック遮断プログラムをインストールしてください」という警告メッセージを表示する。また、あたかも「モバイル向けセキュリティアプリ」を案内するように偽装したメッセージとともに QRコードを公開してスマートフォンに不正アプリをインストールするように誘導した。ひとたびインストールされた不正アプリは、端末に保存された銀行とローン会社の電話番号リストをダウンロードし、ユーザーがそのリストに存在する銀行やメーカーに電話をかけると強制的に着信転換されて攻撃者が仕掛けた番号に繋がってしまう。

[図2] 偽装サイトを利用した不正アプリのインストール誘導

悪質な不正アプリによる主な症状

次に不正アプリがインストールされた場合に見られる症状をまとめた。

1.小額決済を悪用した不正課金

2013年以降、韓国では携帯電話の小額決済のホールを利用したモバイルマルウェアによる被害が多発している。多くのユーザーが自動振り込みで通信料を支払うため被害にあったことを認知するまで数ヶ月かかってしまうことが多く、さらに機種変更時に一定期間様々な付加サービスがついて小額決済内訳に注意を払わないユーザーが多いのだ。

小額決済を悪用した不正アプリは、主にメッセージを利用したフィッシング(スミッシング)やルーター改ざん、脆弱サイトを通じて拡散される。Chromや宅配などのアイコンを偽装してインストールされ、削除されるまで持続的に被害を与える。ユーザーは普段から通信料の請求書に変わったことはないかチェックすることが大事だ。特にオンライン請求書を利用する場合はさらなる注意が必要だ。

2.メッセージ(SMS)送信の異常

不正アプリは、攻撃者のコマンドを受信したり認証情報を奪取するため、メッセージ(SMS)を利用する場合が多い。メッセージに含まれた認証情報を横取りして攻撃者に送信したり、特定の情報を奪取したりする。ユーザーがメッセージを送信しても送信ボックスに保存されていなかったり、相手が受信できなかった場合は不正アプリがインストールされた可能性がある。特定の人からメッセージを続けて受信できなかったら特に疑わしい。

3.初回実行時に広告表示または任意にダウンロードしたアプリのインストール誘導

端末のロック画面を解除する際に広告通知が表示されたり、画面全体に広告が表示されることがある。どのアプリのせいか把握できずもどかしいが、これは不正アプリがインストールされている可能性が高い。アプリを起動せずに広告が表示されたり、アプリのインストールページに移動する場合は不正アプリを疑うことができる。このタイプの中には、インストールしてから一定のプロセス終了後に動作を開始するケースもある。またパッケージマネージャを使用してユーザーが気づかないうちにダウンロードされたアプリのインストールを要求する場合、不正アプリを疑ってみる必要がある。

4. データー使用量の異常な増加

ユーザーの同意なしにインストールされるアプリは、保管中の情報を外部に送信したり外部から別のファイルをダウンロードすることもある。ほとんどの不正アプリは Wi-Fiに接続されなくても悪質な機能を実行するため、通常のアプリに比べてデーター消費量が多いほうだ。理由なく普段に比べてデーター量が急増した場合、不正アプリのインストールを疑うことができる。

5.度々発生するプログラムクラッシュ・アプリ実行不可

普段よく使っていたアプリが正常に実行されなかったり、スマートフォンのロック画面解除時にアプリが異常終了する場合、不正アプリのインストールが疑われる。不正アプリ作成者は、さまざまな環境でテストするほどのことはないため、特定の端末では正常に動作しないことがある。また多くの不正アプリはユーザーがロック画面を解除するときに動作するため、このタイミングで異常なアプリ終了が発生することもある。

悪質な不正アプリをチェックする方法

上記のような症状が現れたとき、不正アプリの有無をチェックする方法がある。

1.アプリ毎のデーター使用量をチェックする

広告表示のようにユーザーに不快感をもたらす不正アプリは、広告データーの受信やアプリダウンロードのために大量のデーターを使用する。Android 端末は設定メニューからモバイルデーターの使用量とアプリ別の使用量を確認することができる。データーを多く使用中のアプリの中で知らないアイコンが見えたら疑ってみるべきだ。

2.バッテリー使用量をチェックする

端末の情報を外部に流出する不正アプリは、端末で発生する多数の動作を監視しなければならない。設定メニューからアプリ別バッテリー使用量を確認し、普段あまり使用しないアプリにもかかわらずバッテリー使用量が高いと出た場合、疑ってみる必要がある。

3.デバイス管理者に登録されたアプリをチェックする

不正アプリは削除されたり、より多くの端末機能を利用するため自らデバイス管理者に登録するケースが多い。デバイス管理者に登録されたアプリの中から知らないアプリがあった場合、不正アプリであると疑うことができる。

4.サードパーティアプリ有無をチェックする

ほとんどの不正アプリは公式ストアではなく他の経路を通じてインストールされる。これは「サードパーティアプリ」と呼ばれ、adbコマンドを使用すれば確認できる。「adb shell pm list packages -3」コマンドを実行したときに表示されるパッケージ名の中で、キャリアと端末メーカーに関係のない名前が存在する場合、不正アプリとして疑うことができる。

悪質な不正アプリ、インストール段階から予防すべき

前述のような方法でアプリをチェックして不正アプリを削除すれば、追加の被害は防げる。しかし不正アプリの作成と配布手法が日々高度化され、確かな症状が出ない限りそれと気づくことは難しい状況だ。特に正常なアプリに偽装してインストールされたり、サードパーティのアプリであればさらに区別が難しく、Wi-Fiに接続する場合のみ動作するならばデーター使用量をチェックしても発見が難しい。やはりインストール済みアプリの中から不正アプリを見つけるよりはインストールする前に予防することがはるかに効率的だ。

アンラボの V3 Mobile Securityは OS改ざんをチェックし、ユーザーの同意なしに個人情報にアクセスして情報を流出するアプリを検知する。またインストールアプリに対する事前スキャンや、ユーザーに不快感を与える不要なアプリ(Potentially Unwanted Application、PUA)とファイルとフォルダーを対象に詳細なスキャンを実行できる。リアルタイムスキャンによるインストールやアップデート時にアプリが安全かどうかをスキャンして被害を防止する。

次に安全な端末使用環境のための注意事項をまとめた。

1.提供元不明のアプリをインストールしない

アプリはユーザーが直接インストールする場合がほとんどだ。特にメッセージやチャットアプリなどから、アプリをダウンロードしないように注意すべきだ。

2.端末の OSを任意に変更しない

一部のユーザーは端末をより自由に使用するために「スーパーユーザ権限」を獲得して特定のツールをインストールする。スーパーユーザ権限は端末の制約を解除してくれるが、悪質なアプリが機能することも許可してしまう。ほとんどは suコマンドを実行してスーパーユーザ権限を取得するが、不正アプリがシステムに suコマンドの存在有無を確認し、このコマンドを実行して簡単に権限を格上げできるのだ。

不正アプリがスーパーユーザ権限を取得すれば、権限の許可をベースにするほとんどのセキュリティ機能が無効化する。例えばスーパーユーザ権限を取得した不正アプリは、端末のロックやパスワード領域のように通常のアプリがアクセスできない領域に格納されたファイルまでもアクセス可能となり、パスコードを任意に変更できるようになる。

3. インストールとアップグレードに必要な権限を確認する

通常のアプリはインストール時に必要とする権限とその説明も表示する。この説明の中でアプリの機能と無関係な(例えばSMSや電話アクセスなど)権限を必要とする場合、一度は疑ってみるべきだ。通常はアップグレードを実行する際も元の権限と同じものを必要とする。かつて Googleのプレイストアに登録された開発者アカウントが変更され、アプリをアップグレードする過程で不正アプリが配布された事例があった。Googleプレイからインストールされたアプリは、従来と同じ権限を使用するなら設定に基づいて自動更新されるが、権限の変更があるならばその内容をユーザーに再確認する。正常なマーケットから配布されたアプリをアップグレードする際、既存と異なる過剰な権限を要求する場合はアプリのユーザーレビューや発行元の他アプリのレビュー、インストール数などを確認したほうが良い。

4.モバイル専用セキュリティアプリを使用する

モバイル専用セキュリティ対策プログラムやソフトウェアは、さまざまな技術を使用してアプリの安全性をチェックする。また様々な国のマーケットからアプリ情報を収集・分析し、ユーザーレビューの参照などをもとに不正アプリや偽アプリ、ユーザーに不快感をもたらすアプリを分類する。ユーザー自らアプリのレビューを検索したり、悪質なアプリ有無を診断するよりは簡単かつ迅速に不正アプリを判断できる。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)