アンラボ・セキュリティレター

Press Ahn

2023.12　Vol.120

スミッシング攻撃の深層解析、被害者の心理を掘り下げる悪意のあるアプリの進化

スミッシング攻撃の深層解析、被害者の心理を掘り下げる悪意のあるアプリの進化

スミッシング（Smishing）攻撃は過去 1次元的に攻撃対象をだました方式から、様々な攻撃手法を活用して被害者の心理を掘り下げる形に進化した。特に、攻撃者が制作する悪意のあるアプリは簡単に判断しにくいほど巧妙に設計されており、さらに注意が必要である。

アンラボは最近、韓国国内で起きたモバイルスミッシングと悪意のあるアプリの攻撃手法を詳細に分析したレポートを発行した。レポートの主な内容を紹介する。

1. 概要

スマートフォンが大衆化され広く普及し、これを狙った攻撃がますます増加している。Android 端末の場合、外部からダウンロードしたアプリを簡単なプロセスを経てインストールできる。これにより端末に悪意のあるアプリがインストールされる可能性がさらに高まる。

最近のニュースでは、悪意のあるアプリのインストールだけで被害者の資金が流出したという事例が報告され続けている。これは、悪意のあるアプリが二要素認証をバイパスする手法を使用して発生している。二要素認証とは、ユーザーがアクセスしようとするサービスにログインする際、既に登録されている電話番号にセキュリティコードを送信し、セキュリティコードを入力すると本人認証が完了しサービスログインが正常に行われる認証方式である。認証が簡単であるというメリットでインターネットバンキングの利用口座の変更や様々なグローバルサービスを通じて広く使用されているが、悪意のあるアプリによって認証コードが公開されて悪用される可能性がある。

今回のレポートでは、韓国で配布中のスミッシングメッセージのタイプを分類し、各タイプ別の事例をまとめる。そして、被害者が実際にダウンロードする悪意のあるアプリの配布サイトのタイプを分類し、各サイト固有の特徴について説明する。ボイスフィッシング攻撃時、Google Play ストアに存在するリモートコントロールアプリ、金融資産照会アプリについて各アプリの特徴と共に、配布サイトアドレスを隠すために使用される短縮 URL の説明と最近 3ヶ月間の攻撃時に活用した短縮 URL アドレスのリストを紹介する。続いて、インフォスティーラー（情報窃取）、Kaishi（銀行＆アンチウィルス偽装）、インフォスティーラー（モムケム・フィッシング - アダルトライブチャットのフィッシング

詐欺)、SMSstealer (二要素認証バイパス) など 、悪意のあるアプリの特徴と悪意のあるアプリの種類、実行画面、主な機能を説明する。

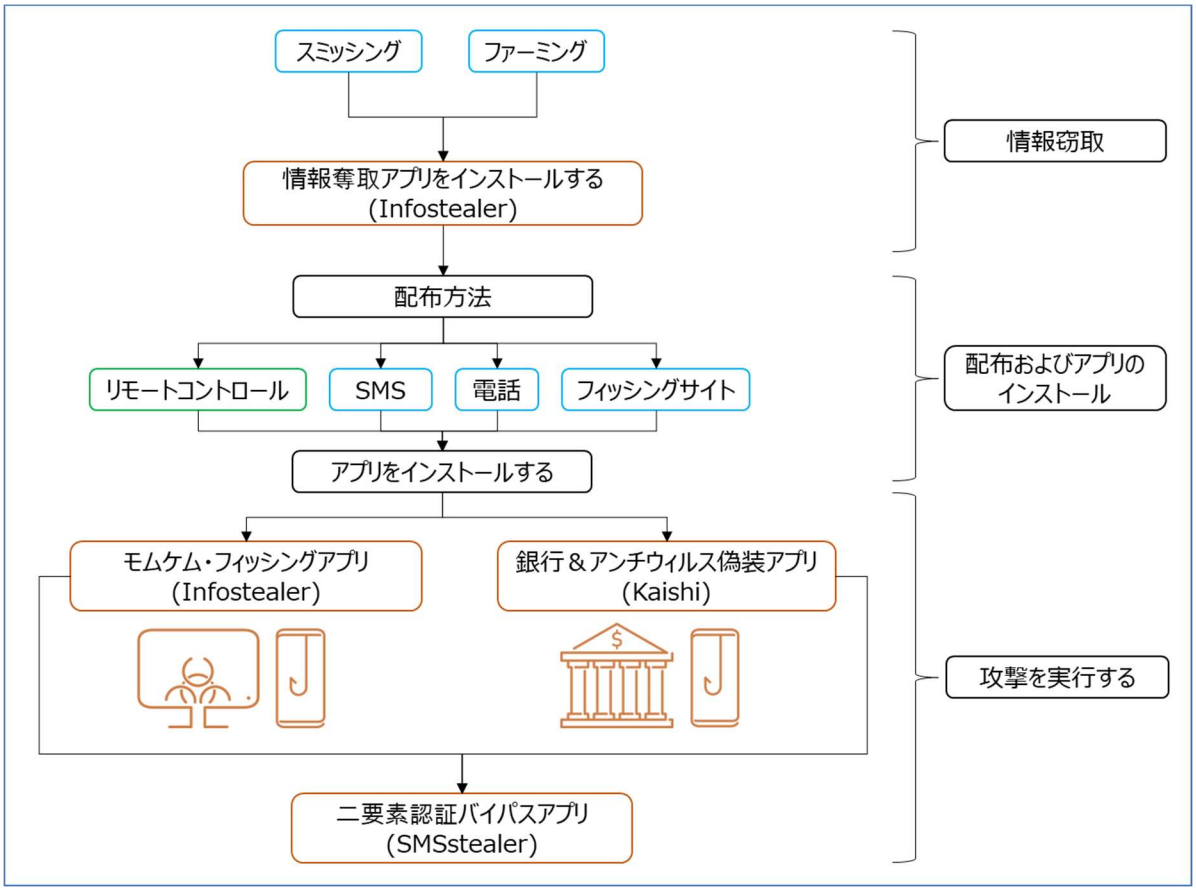
また、各アプリの関係を通じて悪意のあるアプリがインストールされ、ユーザーの制約なしに資産が流出されるシナリオについて紹介する。

2. 攻撃シナリオ

配布者はターゲットに設定する被害者を物色するための事前作業として、スミッシングまたはファーミング攻撃を通じて悪意のあるコンテンツを無差別に配布する。配布された SMS に含まれるアドレスにアクセスし、情報を窃取するアプリ (以下インフォスティーラー) をインストールして実行すると、個人情報 (連絡先、メッセージなど) のような敏感な情報が配布者の C2 サーバーに転送される。

情報窃取が成功すると、配布者は感染したユーザーだけでなく知人にもスミッシング SMS の送信を通じてフィッシングサイト (悪意のあるアプリの配布サイト) へのアクセスを誘導する。あるいは「犯罪行為に関わる」、「海外決済」など、被害者に不安感を与えることができる言葉で被害者を惑わし、リモートコントロールアプリのインストールを誘導した後、「端末スキャン」などの名目で銀行＆アンチウィルス偽装アプリ (以下 Kaishi) をインストールして実行する。このほか、アダルトチャットやマッチングアプリを装い、より多くの情報を見せるという名目でモムケム・フィッシングアプリ (以下インフォスティーラー) をインストールするよう誘惑する。

配布者の目的は被害者の資金を窃取することで、二要素認証プロセスをバイパスするためにメッセージを傍受する悪意のあるアプリ (SMSstealer) を追加インストールするよう誘導する。これは、インフォスティーラーと Kaishi をインストールした被害者端末から認証コードを窃取して資金を盗む方式に進化している。攻撃者が活用する攻撃手法と悪意のあるアプリ情報および攻撃シナリオをまとめると [図 1] の通りである。



[図 1] 攻撃シナリオ

[図 1] で青色で表示された部分は攻撃手法であり、各手法の説明は次の通りである。

- **スミッシング**: メッセージを通じてフィッシングサイトにアクセスを誘導し、マルウェアを配布する攻撃手法である。
- **ファーミング**: 正常サイトのドメインアドレス (DNS) を窃取してユーザーが正常サイトにアクセスしたかのように勘違いさせ、個人情報を窃取する攻撃手法である。
- **フィッシング**: 不特定多数が偽のホームページにアクセスするようにし、個人情報を窃取する攻撃手法である。

[図 1] で緑色で表示された部分は攻撃時に活用される正常なアプリで、攻撃に活用される手法は次の通りである。

- **リモートコントロール**: 攻撃者がリモートコントロールアプリがインストールされた被害者端末を操作する。リモートコントロールを通じてアプリのインストール、端末監視などの行為を行う。

[図 1] で赤色で表示された部分は攻撃時に使用した悪意のあるアプリで、各アプリの特徴は次の通りである。

- **情報窃取インフォスティーラー悪意のあるアプリ**: 個人情報を窃取する悪意のあるアプリで、主に宅配、ショッピングモールなどに偽装する。
- **モムケム・フィッシングインフォスティーラー悪意のあるアプリ**: 端末および個人情報を窃取してリアルタイム録音と画面録画などの行為を行う悪意のあるアプリで、主に成人向けアプリに偽装する。
- **銀行＆アンチウィルス偽装 Kaishi 悪意のあるアプリ**: 端末および個人情報などを窃取してデフォルトの電話アプリを悪意のあるアプリに変え、電話の状態を監視する。電話番号を監視するリストが存在し、配布者が不要な番号に連絡したり、着信拒否、電話の発信など電話に関連する行為を制御する強制受信と発信の機能を含む。主に銀行アプリに偽装する。
- **二要素認証バイパス SMSstealer 悪意のあるアプリ**: デフォルトの SMS アプリを悪意のあるアプリに変え、端末で送受信されるメッセージの状態を監視する。感染した端末で送受信されるすべてのメッセージを窃取するため、メッセージ履歴が存在せず、すべてのメッセージの内容を流出する。主に宅配、結婚式招待状などのアプリに偽装する。

3. 攻撃手法

攻撃者が悪意のあるアプリを配布し、インストール後に実行するまで使用する攻撃手法と、攻撃時に活用する正常なアプリとサービスについて紹介する。

3.1. スミッシング

スミッシングは被害者の不安な心理を狙って社会的問題、個人生活と密接に関連する内容を配布し、悪意のあるアプリのインストールを誘導する形に進化している。スミッシングメッセージは、主に内容と悪意のある URL リンクが含まれたアドレス形式で配布されており、最近はセキュリティアプリの検知をバイパスするために URL アドレスを除外して攻撃者の電話番号を記入し、被害者に電話するよう誘導する形に進化している。

メッセージの多くは「国外発信」、「Web 発信」などの内容が含まれており、アンチウィルスアプリなどによる検知を避けるために正常な単語内に不要な文字を挿入、浮き書き除去、異常な文字の使用などの手法を使用する。悪意のあるアプリをダウンロードするアドレスの場合、被害者の疑いを避けるために短縮 URL サイトで提供されるサービスを活用する。

3.1.1. 宅配便詐欺

大多数の宅配便タイプのスミッシングメッセージは主に宅配会社を詐称する。詐欺メッセージは「国外発信」、「国際発信」、「請求番号」などの情報から始まり、「道路名不一致による住所変更」、「配送遅延による配送日程の確認」、「未受取宅配便の確認」などの言葉で被害者に不安感を助成する。メッセージに記載されているアドレスにアクセスすると、詐称した会社を装ったフィッシングサイトが表示される。これにより、被害者は疑うことなく、情報を確認するために電話番号と名前、生年月日などの情報を入力した後、悪意のあるアプリをダウンロードしてインストールする。

最近の宅配会社は宅配便の通知を SMS で送信せず、独自に開発したアプリやポータルサイト内の通知サービスを活用しているので、

注意が必要である。宅配便詐欺スミッシングメッセージを受信したら、宅配会社が提供する郵便追跡サービスを通じて直接確認する手続きをして、事前に被害を防止しなければならない。

3.1.2. 公共機関を詐称する

公共機関を詐称するスミッシングメッセージは主に最近の社会的問題または警察および公団などを詐称して配布され、「交通違反」、「罰点報告書」、「過怠金」、「通知書」 などの言葉で被害者に不安感を与える。メッセージに記載されているアドレスにアクセスすると、機関を装ったフィッシングサイトが表示される。これにより被害者は特に疑うことなく、情報を確認するために電話番号と名前、生年月日などの情報を入力した後、悪意のあるアプリをダウンロードしてインストールする。

公共機関の場合、公式アプリストア以外のところではアプリのインストールを誘導しないので、注意が必要である。公共機関を詐称するスミッシングメッセージを受信したら、発信機関の苦情相談室に確認し、事前に被害を防止しなければならない。

3.1.3. 知人を詐称する

知人を詐称するスミッシングメッセージは 「結婚式の招待状」、「結婚式」、「訃告」、「認証」 などの言葉で被害者の知人が送ったような形で配布される。メッセージにアドレスが含まれている場合は被害者のアクセスを誘導するが、含まれていない場合はメッセージや電話を通じて本人認証を名目に身分証明写真などの個人情報を要求したり、特定のSNSアカウントの追加を誘導する。知人を詐称するスミッシングメッセージを受信したら、知人に直接連絡してメッセージを送信したか確認し、被害を防止しなければならない。

3.1.4. 振り込め詐欺

振り込め詐欺スミッシングは他の詐欺とは異なり、フィッシングサイトアドレスが存在しない。アドレスが記載されていると疑われる可能性があるため、被害者から電話するよう誘導するために主に 「大きな金額が支払われた」 という内容で被害者に不安感を与え、電話するよう誘導する。メッセージ内の電話番号に電話すると実際の顧客センターではなく偽の顧客センターにつながり、被害受付を名目に電話番号、名前、生年月日などの情報を要求する。これは単に個人情報を収集する用途ではなく、該当の SMS を配布した攻撃者が実際に被害者に送ったことを確認するための作業の一部である。

攻撃者は事前に確保した個人情報に基づいてスミッシングメッセージを配布する。被害者から電話か来ると、自分が配布した対象であるかどうか確認し、一致したらリモートコントロールアプリのインストールまたは携帯電話の検査を名目に追加アプリのインストールを誘導する。攻撃者が使用する電話番号は数時間が経過すると無効になり、さらに時間が経過すると正常番号として使用される可能性があるため、単に番号照会の結果でスミッシングであるかどうかを確認するのではなく、疑わしい SMS を削除することが重要である。振り込め詐欺スミッシングメッセージを受信したら、カード会社のカスタマーセンターに連絡して決済の有無を確認し、決済していない場合はメッセージを削除して被害を防止しなければならない。

3.1.5. 金融機関を装う

金融機関を装うスミッシングメッセージは融資、社会的問題などの要素を反映して配布される。以前は新型コロナウイルス感染症対応支援金を装ったメッセージが流行しており、一般的には融資に関する内容が多い。金融機関を装うスミッシングの場合、過去には悪意のあるアプリをダウンロードできるフィッシングサイトへのアクセスを誘導した。

最近は被害者が直接攻撃者に電話するように SMS に電話番号が記載されており、実在の銀行のカスタマーセンターの電話番号と「直通電話番号」、「相談窓口案内」、「着信拒否」 などの内容と偽番号が一緒に記載される。偽の電話番号 (攻撃者) に電話すると、音声で銀行を装うフィッシングサイトアドレスを案内し、被害者がアクセスした後にアプリのインストールをするよう誘導する。金融機関を装うスミッシングメッセージを受信したら、銀行のカスタマーセンターに連絡して被害事実を知らせ、被害の有無を確認しなければならない。

3.1.6. その他

その他のスミッシングの場合、モムケム・フィッシング、社会的問題などの要素に応じて配布される。モムケム・フィッシングの場合、偽の会員

と連絡しながら被害者に「より多くの情報を見るためにはアプリのインストールが必要だ」とし、悪意のあるアプリを直接送ったり、インストールできるサイトに移動させる。この他にも、社会的問題または被害者の不安な部分を悪用してスミッシングメッセージを配布する。不要なメッセージを受信したら、これを削除して事前に被害を防止しなければならない。

3.2. 悪意のあるアプリの配布サイト

悪意のあるアプリの配布サイトの場合、ユーザーが直接アプリをインストールするようにしたり、サイトにアクセスした直後に悪意のある APK がダウンロードされるなど、様々な攻撃形態がある。配布サイトの共通の特徴としては特定の機関または企業を詐称したり、成人サイトなどを装って活性化されていることだ。また、正常なサイトに見せるために、被害者から電話番号、請求書番号などの情報を入力すると目的の情報が確認できるよう設計されている。

ほとんどの配布サイトはモバイル以外の環境（Windows PC など）でアクセスする場合、正常なサイトに移動するように設計されている。攻撃者がサイトを直接開設してアクセスを誘導する形態も存在するが、正常なサイトの機能を悪用して被害者のアクセスを誘導する事例も発見されているため、注意が必要である。

以下は、いくつかの悪意のあるアプリの配布サイトのタイプをまとめたものである。

3.2.1. 電話番号の入力

電話番号の入力を誘導するフィッシングサイトの場合、最も一般的な悪意のあるアプリの配布サイトのタイプの1つである。宅配便、健康診断、交通取締りなど様々なタイプで配布されたスミッシングメッセージから電話番号、請求書番号を入力するサイトに移動される。過去には、配布サイトで入力した情報（電話番号、請求書番号など）は検知をしなかったが、最近は攻撃者が配布した対象の電話番号、請求書番号、名前、生年月日などではない場合、実際に悪意のあるアプリをダウンロードできないように進化した。

3.2.2. ボタンをクリックする

ボタンをクリックする配布サイトの場合、ユーザーが直接アプリをインストールできるようにするために、主に「開く」、「ダウンロード」、「公式ストア」などのボタンで表示される。公式ストアボタンをクリックすると、ストアで実際に運営しているように見えるために偽のページに移動される事例も存在する。ボタンをクリックして悪意のあるアプリを配布するサイトの場合、悪意のあるアプリを認証なしに端末にダウンロードする。

3.2.3. 直接ダウンロード

ダウンロードを誘導するタイプの配布サイトの場合、配布者が送ったアドレスにアクセスすると悪意のあるアプリを端末で直接ダウンロードする。被害者はダウンロードの決定権がなく、攻撃者が APK ファイルをリモートコントロールで被害者の端末にダウンロードおよびインストールできる。

3.2.4. リダイレクト

リダイレクトタイプの場合、一部の SNS で許可されているリダイレクト機能を介して正常なサイトアドレスにアクセスすると、悪意のあるアプリの配布サイトに移動される。攻撃者は通常のリンクアドレスが含まれたメッセージを被害者に送信し、被害者がリンクにアクセスすると悪意のあるアプリの配布サイトにリダイレクトされる。通常のサイトアドレスに隠して使用する機能であるため、被害者は該当リンクが悪意のあるリンクであるかの確認が難しく、被害を受ける可能性が高い。

```
<!-- Inside head -->
<meta name="description" content="Redirection Test">
<script type='text/javascript'>
   let new_slug = window.location.pathname;
   let new_root = "[redacted]";
   let new_url = new_root + new_slug;
   console.log(`<link rel=\"canonical\" href=\"" + ${new_url} + "\">`);
</script>
```

```
<script type='text/javascript'>
    window.location = new_url;
</script>
```

[図 2] リダイレクトサイトのタイプ

3.3. 攻撃に活用される正常なアプリとサービス

過去には攻撃者が単にスミッシングメッセージ内のアドレスを通じて、被害者が悪意のあるアプリの配布サイトにアクセスするよう誘導した。しかし、アンチウィルスアプリの検知、スマートフォンユーザーのセキュリティ認識の強化などにより、攻撃が成功しにくくなった。

その中で、攻撃者は攻撃を成功させるために、悪意のあるアプリの配布サイトアドレスを直接送信する従来の手法ではなく、短縮 URL サービスを活用したり、まずは公式ストアの正常なアプリをインストールさせるような手法でユーザーの疑いを避け始めた。そして、攻撃者が直接被害者端末とリモート接続した後、悪意のあるアプリの配布サイトにアクセスし、悪意のあるアプリをダウンロードする手法に進化した。また、資産の現状を簡単に把握するためにサービス中の資産照会アプリを通じて被害者の資産の現状を素早く把握し、窃取する資産の規模を確認することもある。

次に、攻撃者が主に使用するリモートコントロールアプリと金融資産照会アプリの種類と各アプリの特徴について紹介する。

3.3.1. リモートコントロールアプリ

攻撃者は 2つの側面を悪用してリモートコントロールアプリ攻撃を実行する。まず 1つ目は、アプリが公式ストアからダウンロードされるという点である。攻撃者は被害者に公式ストアからリモートコントロールアプリをインストールするように誘導するが、被害者は公式ストアからダウンロードするアプリだけにあまり疑わずリモートコントロールアプリをダウンロードする。

2つ目は、被害者の状況を把握するために直接端末を確認するという名目にリモートコントロールアプリをインストールするよう誘導するということだ。被害者はどうすべきか分からなくなった時、誰かが好意を与え、直接端末を調べてくれるとすると安堵感を感じ、攻撃者の要望に応じてリモートコントロールアプリをインストールする。攻撃者は被害者の端末に直接接続して悪意のあるアプリを簡単にインストールし、金融情報などの個人情報、アンチウィルスプログラムの有無も簡単に確認できる。

攻撃に多く活用されるリモートコントロールアプリは次の通りである。

3.3.1.1. TeamViewer QuickSupport

TeamViewer QuickSupport の場合、Google の公式ストアで 5000万回ダウンロードされるほど人気の高いリモートコントロールアプリである。インストール後の簡単な利用規約の同意取得手続きを経て、端末制御が可能な固有の ID 情報が割り当てられ、ウェブまたはチームビューアがインストールされた他の端末でもその ID 情報を利用して制御が可能になる。

攻撃者は被害者と電話しながら QuickSupport アプリを Google の公式ストアからインストールするように促し、実行後に得た固有の ID 情報を要求する。ID を介してリモートコントロール環境が設定されると、被害者端末には「遠隔サポートの許可」、「通知ウィンドウと画面内のすべての情報のキャプチャ」ウィンドウが表示され、攻撃者は被害者に許可ボタンをクリックするよう誘導する。リモート接続が正常に行われると、端末内のどの画面部分をクリックするかを表示する機能を通じてリアルタイムで端末画面の状態を確認できる。

3.3.1.2. TeamViewer Host

TeamViewer Host の場合、Google の公式ストアから 500万回以上ダウンロードされたアプリで、他のチームビューアアプリに比べてダウンロード数は少ないが、攻撃者は活発に使用している。上記で紹介した QuickSupport アプリとは異なり、アプリの実行時にデバイスの追加割り当てを名目に TeamViewer アカウントのログインを要求する。攻撃者は自分が使用するアカウントでアプリにログインし、被害者の端末を攻撃者アカウントから信頼できるデバイスとして登録する。ログインが完了すると、攻撃者が使用する端末にインストールされた TeamViewer アプリを介してリモートコントロールを開始する。リモートコントロールの開始時に QuickSupport とは異なり、「遠隔サポートの許可」ウィンドウのみが表示され、これを許可するボタンをクリックするとリモートコントロールを実行する。

3.3.1.3. AnyDesk

AnyDesk の場合、Google の公式ストアから 5000万回以上ダウンロードされ、TeamViewer QuickSupport と同じくらい人気が高いリモートコントロールアプリである。アプリの実行時に端末に応じて追加のプラグインのインストールを要求し、そのプラグインはよりスムーズにリモートコントロールするためにアクセシビリティ権限の許可を要求する。権限が正常に付与されると、使用同意書と端末に接続可能な固有アドレスが表示される。ウェブまたはモバイルからリモートコントロール接続が要求されると、セキュリティ警告ウィンドウが表示され [キャプチャを許可] をクリックするとリモートコントロールを実行する。

3.3.2. 金融資産照会アプリ

攻撃者の最終目的は被害者の資金である。そのため、攻撃者が選定した対象がどの程度の現金を保有しているかを確認する必要がある。過去には被害者が利用している銀行から各銀行に口座情報と保有金額などを一つ一つ尋ねたが、最近は個人資産をより簡単かつ迅速に確認できる資産照会アプリが登場したため、これを活用して被害者の資産情報を確認する。

3.3.3. 短縮 URL

短縮 URL とは、「URL 短縮サービス」と呼ばれ、既存のドメインアドレスを縮小して提供するサービスである。既存のドメインアドレスが長くて複雑であったため、SMS や一部の SNS で文字制限などによりアドレス情報を送信できない場合に主に使用する。スミッシングメッセージの配布者は悪意のあるアプリの配布サイトアドレスを短縮 URL を介して隠し、被害者が短縮 URL アドレスだけではどのリンクであるかを知りにくくする。過去 3ヶ月間に収集されたスミッシングメッセージの配布に使用された短縮 URL リストは [表 7] の通りである。

短縮 URL リスト
me2.do
abit.ly
ko.gl
urlzs.com
snip.ly
dokdo.in
xgo.kr
t.ly
bit.ly
han.gl
zrr.kr
vvd.bz
surl.li
bitly.com
s.id

[表 1] 最近使用された短縮 URL リスト

このように攻撃者は高度化された攻撃手法をもとに被害者の心理を巧妙に悪用し、様々な攻撃を展開している。モバイルスミッシングと悪意のあるアプリによる被害を防ぐためには、まずモバイルアンチウィルスをインストールして最新の状態を維持しなければならない。また、疑わしいウェブサイトへのアクセスを控え、出どころが不明なメッセージは削除する習慣が必要である。

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)