KASPERSKY lab

Kaspersky Lab の
高度なアンチフィッシング技術

ID データは、個人をデジタル形式で表示したものであり、その持ち主にとって価値があるのと同様に、他人にとっても価値があります。サイバー犯罪者の中には、個人の信頼性を確認するユーザーの認証情報を探し求め、それを詐欺師に転売したり、自分自身で使おうとする者がいます。ID データのよくある使い道として、ユーザーの銀行口座から金銭を盗む、ユーザーのソーシャルネットワーク上の連絡リストから友人にマルウェアを送りつけるなどが挙げられます。フィッシングは、認証情報を盗むためにもっとも使われている方法の一つです。

ほとんどのフィッシング攻撃が、被害者がよく利用する Web ページのコピーを作成する方法で行われます。コピーされたページは元のサイトとよく似たドメインに設置され、さまざまな手段でユーザーをそのページに誘導し、認証情報を入力させようとします。

ユーザーを偽サイトに誘導するため、犯罪者はソーシャルエンジニアリングや心理テクニックを積極的に使用します。例えば、嘘の機密情報やセンセーショナルな情報、巨額賞金の提供、あるいは公的機関からの架空の罰金などの制裁措置までも装って、ユーザーの興味を引き起こそうとします（通常はメールやソーシャルネットワーキングサイトのメッセージ、あるいは Skype などのインスタントメッセージを使用します）。

犯罪者たちは、数多くの手段を使って認証情報を盗む行動を隠蔽します。中には、偽サイトと正規のサイトとを識別するのがほとんど不可能なケースもあります。URL を隠す通常の方法（パーセントエンコーディングの値で非予約文字を置換え、URL の転送、あるいは通常の名前の代わりに短いエイリアスサービスまたは IP アドレスを使用）とは別に、ブラウザ特有の視覚的なおとりを使います。つまり、ブラウザのスクリプト言語を使用し、正規の Web アドレスを表すグラフィックを偽の Web アドレスと一緒にアドレスバーの上に配置します。また、この方法で SSL ロック、つまり HTTPS の暗号化接続のサインの模倣もできます。

Kaspersky Security Network (*)の統計によると、2015 年上半期だけで、Kaspersky Lab のアンチフィッシングシステムは、Kaspersky Lab ユーザーのコンピューター上で 8,000 万回呼び出されました。

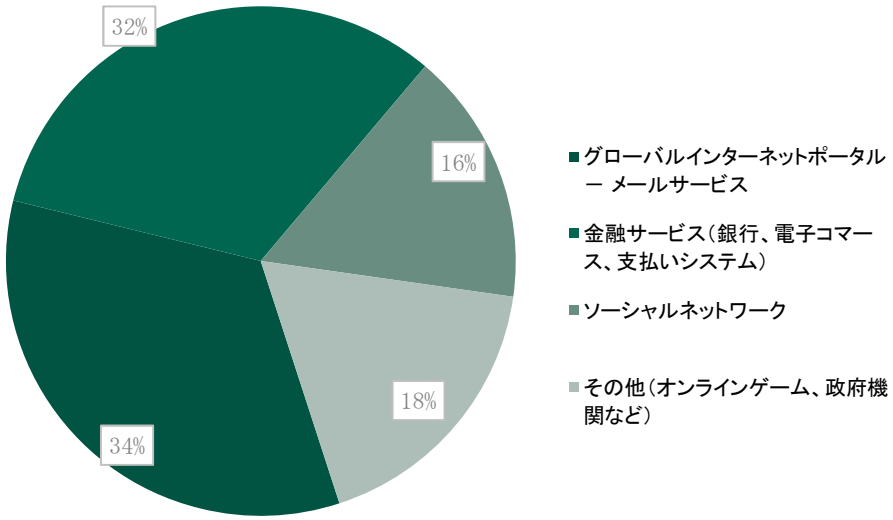

図 1. 2015 年上半期のフィッシング攻撃の標的

Kaspersky Lab のアンチフィッシング技術の仕組み

Kaspersky Lab のソリューションに実装されているアンチフィッシングモジュールは、次の 3 つの検知方法を組み合わせることによって、フィッシングスキームに対する効果的な保護を提供します。

- ユーザーのデバイス上で、ローカルアンチフィッシングデータベースによってサイトをチェック
- Kaspersky Security Network 上のクラウドデータベースによってサイトをチェック
- ヒューリスティック分析（上記のデータベースにまだ取り上げられていないフィッシング Web ページも認識）

図 2. さまざまな方法を使用してカスペルスキー製品でフィッシングサイトをブロック

データベースによるチェック

Kaspersky Lab では、フィッシングサイトに関するデータベースを常にアップデートしています。このデータベースには、弊社の技術により検知されたフィッシングページだけでなく、多くのパートナーから提供されたあらゆるフィッシングページに関する情報が蓄積されています。有害な URL を含むデータベースは、Kaspersky Lab のソリューションおよびクラウドデータベース（Kaspersky Security Network）へ定期的に送信され、クラウドデータベースにはそれらの完全で正確なコレクションが保存されています。悪意のある URL が新しくコンピューター上で検知されると、検知後 15 ～ 30 秒以内にこの脅威に関する情報がクラウドデータベースから入手できるようになります。さらに、Kaspersky Security Network は、サイトの安全性を決定するための追加基準として、ドメイン名と対応した独自の SSL 証明書ベースを有しています。

ただし、サイバー犯罪者たちが新たに攻撃を開始したばかりで、新しいフィッシングページを目にしたユーザーがわずかしかいない場合、フィッシングのリンクはまだデータベースには存在していません。この場合は、ヒューリスティックモジュールを使用することになります。

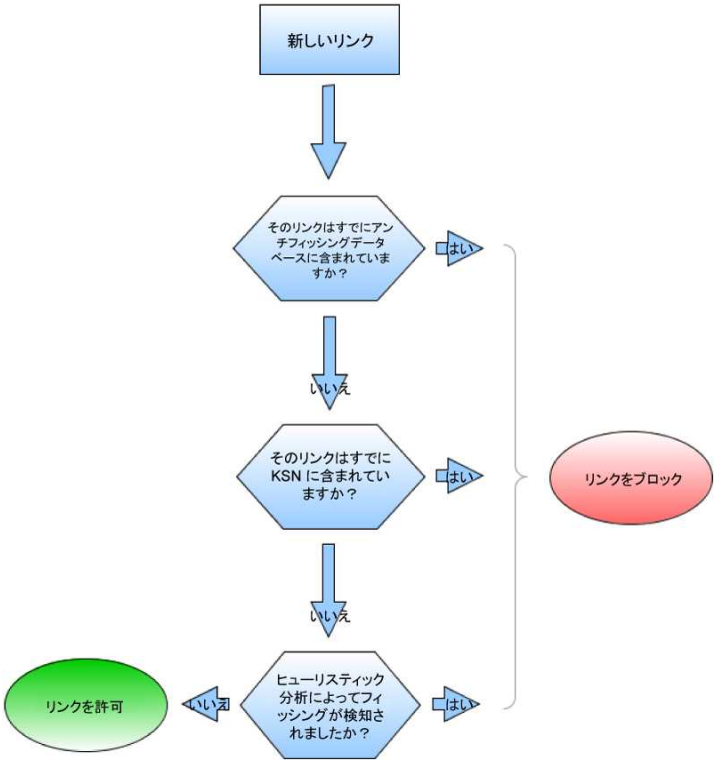

図 3. Web アンチウイルスを使用した、フィッシングページの検出プロセス

ヒューリスティック検知

ヒューリスティックモジュールは、フィッシング攻撃に対するユーザーの最終防御線です。この極めて効果的なシステムにより、たとえユーザーが遭遇したサイトがローカルデータベースやクラウドデータベースに表示されていなくても、Kaspersky Lab はそのサイトがフィッシングサイトかそうでないかについて信頼性の高い判断を下すことができます。Kaspersky Lab の統計によると、フィッシング検知のほぼ 50% がこのシステムによるものです。

ヒューリスティックモジュールは、偽サイトを証明できる既定の属性を探すための単なるチェックマシンではありません（しかし、そのような属性を検出した場合は確実にユーザーに警告します）。最新の高度なフィッシング技術により、サイバー犯罪者たちは「決定的な証拠」を残さずに手口を隠ぺいすることができます。それでも、間接的な兆候が見つかる場合があります。

たとえば、データの Uniform Resource Identifier（URI）方式を使用する方法があります。これは、Web ページにデータを埋め込むための合法的な方法です。ただし、この方法を使用して、合法的なページにフィッシングコンテンツを追加することができます。もう一つの例として、外部のスクリプトコードを使用しようとするクロスサイトスクリプティングがあります。これは、犯罪者の意図の現れである可能性もあれば、単にプログラマーの怠惰の結果（銀行や他の厳格な組織においても珍しいことではありません）である可能性もあります。アンチフィッシングモジュールは、多数のフィッシングの兆候に注目して、それらを他の兆候（ドメイン名、フレームの使用、入力暗号化の使用など多数）と比較し、この間

接的な証拠を基に判断を下します。アンチフィッシングモジュールは、画像にさえも「目をこらし」、そこに何が書かれているかを分析できます。このような属性は一つだけでは必ずしも悪意のあるサイトの証拠にはなりませんが、それらが組み合わさると悪意のあるサイトとなる場合があります。ヒューリスティックシステムの有効性は、これらの兆候とその組み合わせに左右されます。

ヒューリスティックシステムは、既知の最新のフィッシング方法の知識と、検知済みのフィッシングサイトを集めた膨大な Kaspersky Lab データベースに基づいて、これらの兆候を分析して分類するインテリジェントなシステムです。

ヒューリスティックエンジンが、あるサイトがフィッシングサイトである可能性を示してもそれを保証できない場合、データを Kaspersky Lab のクラウドインフラストラクチャに送信します。そこには、独自のより強力なヒューリスティックエンジンによって分析を完了するためのはるかに多くのリソースが含まれています。これにより、ユーザーのコンピューターのリソースを保存し、瞬時のうちに正確な判断を下すことができます。ヒューリスティックモジュールが分析対象のページをフィッシングサイトであると識別した場合、そのページは直ちにブロックされ、ページの情報がすぐに Kaspersky Security Network に送信されて、他のユーザーがそのページを閲覧しないようにします。

危険サイト診断レピュテーションサービス

アンチフィッシングサイトの同じデータベースも、さらにもう一つの技術の機能を強化しています。このデータベースの情報は、他の悪意のあるサイトに関するデータによって補充され、危険サイト診断のレピュテーションサービスによって使用されています。よく知られた検索エンジンの一つを誰かが使用した場合、危険サイト診断によって見つかったリンクかどうかがチェックされ、緑色（信頼できるリンクの場合）または赤色（フィッシングサイトや悪意のあるサイトへ誘導するリンクの場合）の印が付けられます。

図 4. Kaspersky Lab の製品によって赤色マークが付けられた悪意のあるリンク

この技術はフィッシングに対抗する上で欠かせません。ソーシャルネットワーク上の乗っ取ったアカウントのニュースフィードにリンクを配信する、偽のページが人気キーワードの検索結果の上位に表示されるようさまざまな不正 SEO 対策を実施するなど、攻撃者はありとあらゆる手段を使ってリンクに信頼性を持たせようとするからです。この機能は、Windows および Mac OS X でのみ動作します。

Kaspersky Lab のアンチフィッシング技術の利点

- 包括的なアプローチ：リンクが安全だと分類されるまでに、最大で 3 種類の異なるチェックが実行されます。
- 最小限度の応答時間：Kaspersky Lab のアンチフィッシング技術によって、最新のフィッシング攻撃からもユーザーを保護します。
- プロアクティブ保護：Kaspersky Lab のヒューリスティックアンチフィッシングモジュールは、データベースにまだ追加されていないフィッシング Web ページであっても特定できます。
- 早期の警告：危険サイト診断のレピュテーションサービスが、不審なリンクをたどることなく、ブラウザ内のフィッシングリンクを特定します。

カスペルスキー インターネット セキュリティが高度なアンチフィッシング技術によって提供する保護は、特定の脅威に対処するための単なる一連のメカニズムの枠を超えています。サイバー犯罪者が考案した詐欺計画がどれだけ洗練されたものであっても、ユーザーの安全なオンライン体験を実現する、統合されたソリューションです。

(*) Kaspersky Security Network（KSN）：クラウドベースのアンチウイルスネットワーク。ネット上の新しい脅威を即時に検知し、感染源を数分でブロックすることで KSN に接続されたすべてのコンピューターを保護します。

搭載製品

アンチフィッシング技術は、以下の製品に組み込まれています。

個人向け製品

- カスペルスキー インターネット マルチプラットフォーム セキュリティ
- カスペルスキー インターネット セキュリティ
- カスペルスキー インターネット セキュリティ for Mac
- カスペルスキー インターネット セキュリティ for Android
- Kaspersky Safe Browser for iOS

法人向け製品

- Kaspersky Endpoint Security for Business
- Kaspersky Security for Linux Mail Server
- Kaspersky Small Office Security