アンラボ・セキュリティレター

Press Ahn

2017.10　Vol.46

生活密着型セキュリティ脅威 Top3

日常生活に密着したセキュリティ脅威の特徴とその事例

生活密着型セキュリティ脅威 Top3

2017年は WannaCryptor や Petya などの強力なランサムウェアが世界で猛威を振るった。だがこれらの脅威以外にもけして見過ごせない生活密着型脅威が続々と出現している。

生活密着型脅威その1.フィッシング

フィッシングとは?

「フィッシング(Phishing)」とは、デバイスに保管されたユーザーのアカウント情報、住民番号(日本のマイナンバー)、口座番号、カード番号などの重要な個人情報を偽装メールアドレスや悪意ある Webページを利用して奪取するサイバー攻撃手法を意味する。攻撃者はユーザーに個人情報を入力させるため、有名なオンラインサービスのメールアドレスや正常なオンラインサービスそっくりの URLと画面を使用してくる。そして収集した使用者情報から同じアカウントを使用すると予想される他のオンラインサービスにログインしてみたり、迷惑メールやギャンブルサイトの会員登録など、各種不正サービスに悪用することが多い。このように流出された個人情報が悪用される可能性が高い点から、けして見過ごせない脅威といえる。

ターゲットシステム	PC、モバイルなどデバイス全般
主な動作	Webサービスのアカウント情報やその他の個人情報の収集
その他の特徴	収集した情報を使って他のサイバー犯罪に悪用
被害予防策	主要サービスにログインする際、変わったことがないか確認
推奨するアンラボソリューション	V3(フィッシングサイト遮断可能)

[表1] フィッシングの特徴と対策

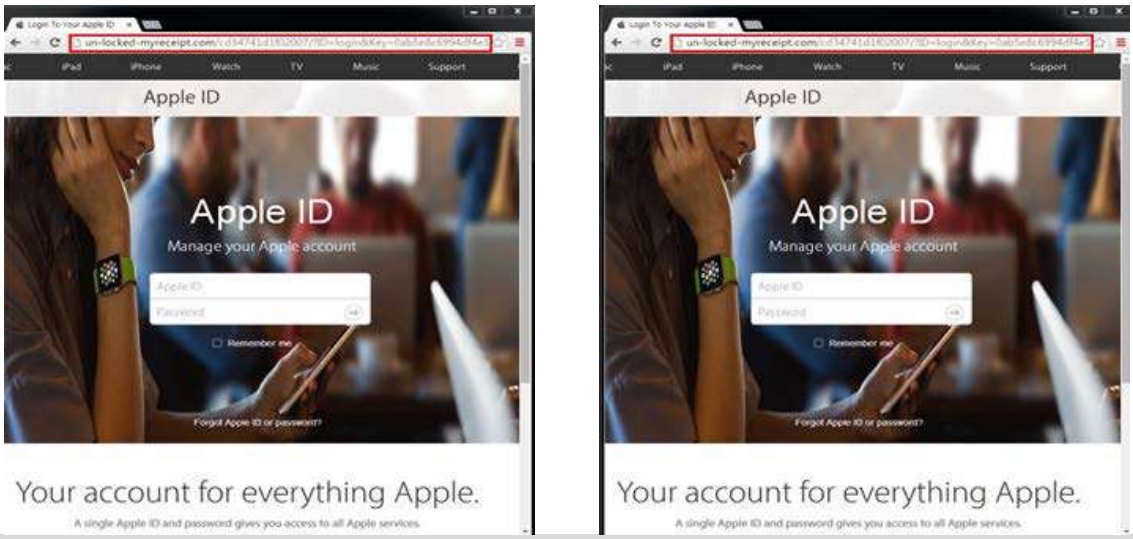
■ フィッシング攻撃ケース ①:アップルサービスを模したフィッシングメール

[図1] アップルからの警告メールに偽装したフィッシング

攻撃者はアップル(Apple.com)のお知らせメールそっくりのメールを送りつけ、アップルアカウントが 24時間以内に非アクティブになると警告してユーザーがフィッシングページに接続するように誘導した。

アップルのメールは通常 apple.comドメインを使用する。フィッシングメールにリンクされた URLをクリックすると、アップルの公式ホームページを模して製作されたフィッシングサイトに接続する。

だが、[図2]のように本物と比べてみると見た目はそっくりではあるが URLとセキュリティプロトコルが微妙に違うことが分かる。



[図2] フィッシングサイト(左)と公式サイト(右)

[図3] 個人情報が流出された後で正常サイトに接続

ユーザーがフィッシングサイトに IDとパスワードを入力すると、アカウント確認のために追加情報入力が必要であるというメッセージが表示され、問題を解決(Unlock)するために金融情報及び個人情報を入力するように誘導する。
ガイドに従って▲カード情報 (カード番号、CVV番号、有効期間)、▲個人情報(名前、国籍、住所、郵便番号、生年月日、電話番号)などの情報を入力すると、クレジットカードに関するセキュリティコード(Secure Code)の入力フォームがアクティブになる。入力プロセスが終了したら正常なアップルサイトにリダイレクトされるため、ユーザーは正常なサービスを利用したと思うしかない。

■ フィッシング攻撃ケース ②： Googleドライブに偽装したフィッシングメール

[図4] PDFファイルに偽装

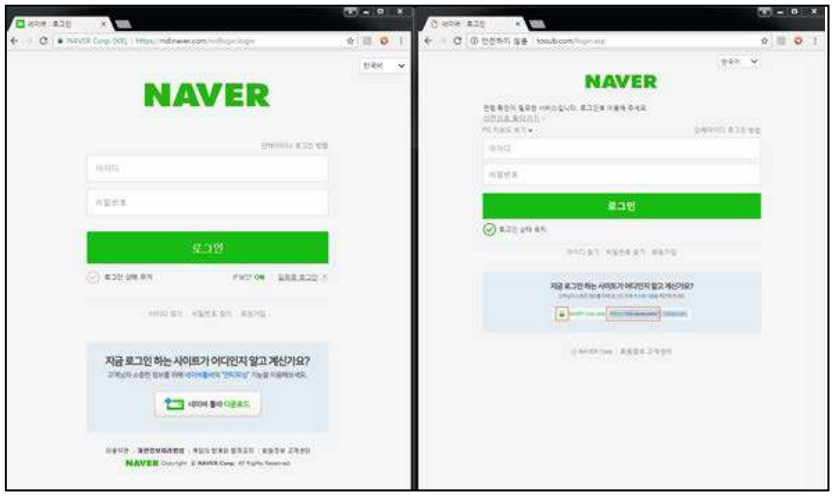
攻撃者はメールで送付したドキュメントにフィッシングページの URLを挿入し、ユーザーのクリックを誘導した。
[図4]の「DOWNLOAD」リンクをクリックすると、[図5]の Google Driveログイン画面に移動する。
Google Driveは写真や文書などを保存する無料クラウドサービスであり、Google Docsは Google Driveが提供する文書作成ツールだ。

添付ファイルを開くためにアカウント情報を入力して「ログイン」ボタンをクリックすると、攻撃者が事前に設定した特定のサーバーに入力した情報を送信する。その後、正常なGoogle Docsに再アクセスするように処置し、ユーザーに正常なサービスを利用したと思い込ませる。
メールアカウントで Gmailを選択した場合、メールアカウントを復元するための電話番号またはサブのメールアドレス情報を追加で要求する。ユーザーが入力した追加情報は攻撃者に送信される。

[図5] Google Docsに偽装したフィッシングページ

■ フィッシング攻撃ケース ③：コミュニティの書き込みによるフィッシング

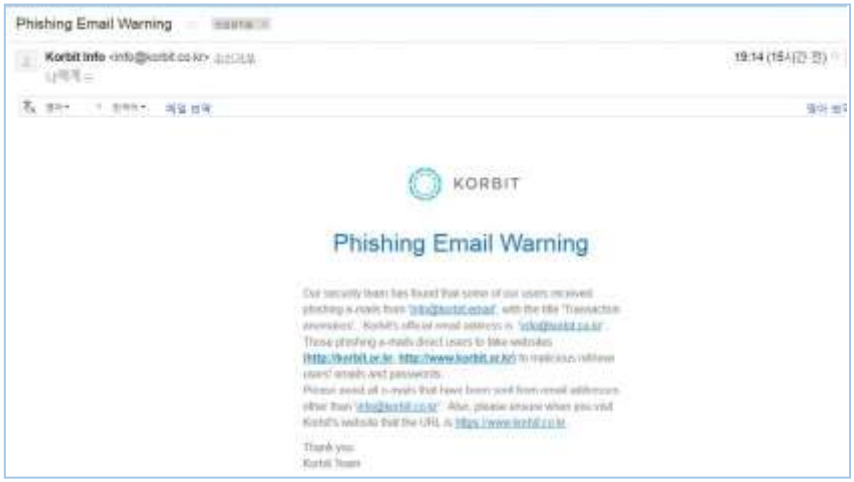
攻撃者は有名コミュニティの掲示板に、興味をそそらせるタイトルの書き込みをアップして会員のクリックを誘導し、フィッシングページにアクセスさせていた。内容にある URLをクリックすると、まず動画プレーヤーに偽装したページに移動する。次に動画プレーヤーアイコンをクリックすると、大手ポータルサイトに偽装したページを表示してアカウント情報の入力を誘導した。フィッシングページから流出されたアカウント情報は、攻撃者に送信されて書き込みの内容と無関係な動画が再生される。



[図6] 韓国の大手ポータルサイトの正常なログインページ(左)とフィッシングページ(右)

■ フィッシング攻撃ケース ④：仮想通貨取引所の案内メッセージに偽装したフィッシング

攻撃者は仮想通貨取引所のログイン・決済完了のお知らせに偽装して取り引きに必要な個人情報を奪取した。正常な仮想通貨取引所の案内フォーマットをそっくりに模したため、正常かどうか見分けることはほとんど不可能だった。攻撃者は「開始する」、「実行する」ボタンのクリックを誘導したり、画面に見える URLと実際に遷移する URLを別々にして、フィッシングサイトに IDとパスワードを入力させた。この件に関して仮想通貨取り引きサイト側も注意喚起のメッセージを出したが、今後も似たような攻撃は続くと予想されている。



[図7] 仮想通貨取り引き所のセキュリティ注意喚起のお知らせ

生活密着型脅威その2.ファーミング

ファーミングとは?

「ファーミング(Pharming)」とは、フィッシング(Phishing)と耕作(Farming)の合成語で、ユーザーが正確なサイトアドレスを入力してもマルウェアによって改ざんされたホスト(hosts)ファイルやDNSアドレスを参照し、攻撃者が作成した偽サイトにアクセスしてオンライン金融取り引きに関する個人情報を奪取するサイバー攻撃手法を意味する。ブラウザの「お気に入り」や「ショートカット」を利用したり、直接アドレスを入力する過程で悪意あるサイトに接続するため、ほとんどのユーザーはマルウェア感染の有無を認識できない。しかも偽サイトは最新のホームページ内容をそのままコピーしたり、オリジナル画面をそのまま再現することが多く、疑うことすら難しい。ポータルサービスのアカウント情報やオンライン金融サービスに関する様々な個人情報まで流出され、個人情報の売買に留まらず金銭的被害までも引き起こしかねない。

診断名	Trojan/Win32.Banki、Dropper/Win32.Banki など
タイプ	バンキ(オンライン金融に関するユーザーの情報収集を目的とする)
ターゲットシステム(OS)	Windows
主な動作	オンライン金融サービスのアカウント、公認認証書1、クレジットカード番号、暗号コードの収集
その他の特徴	直接的な金融被害の誘発
被害予防策	- AhnLab V3を最新バージョンにアップデートして、リアルタイムスキャンを有効 - 過剰な個人情報入力を誘導する場合は疑ってみること
アンラボソリューション	V3、MDS(マルウェア診断・駆除)

[表2] ファーミングの特徴と対策

■ ファーミング攻撃ケース ①：正常なユーティリティのアップデートサーバーを利用してマルウェア配布

正常なユーティリティプログラムのアップデートプロセスを悪用するケースが発見された。悪意あるファイルは正常なアップデートパスから配布され、実行後に追加ファイルを作成して Windows起動時に自動実行されるようにレジストリに登録されていた。この時に作成された [ランダム文字列].exeファイルは、定期的に C&Cに接続して追加ファイルをダウンロードする。ダウンロードされた追加ファイルが動作して PCの物理アドレスを攻撃者に送信した。

■ ファーミング攻撃ケース ②：不要なプログラム(PUP)によるマルウェア配布

セットアッププロセスの中で提携するサービスプログラムを一緒にインストールすることがあるが、その時に脆弱なプログラムを通じて不要なプログラムやマルウェアが配布されることがある。また ActiveXの形でインストールされる不要なプログラムのプロセスから、マルウェアを配布することもあった。

不要なプログラムのアップデートファイルが実行されると、アップデートサーバーに接続してアップデートファイルの有無を確認する。アップデートファイルが存在する場合はダウンロード・実行するが、この時にダウンロードされるファイルの改ざん有無を確認するスキャン機能は存在しない。攻撃者はこれを利用して、特定の時間にアップデートファイルをマルウェアにすり替えて配布した。

マルウェアの構造は、不要なプログラム(PUP)ファイルを作成する動作コードと、悪意ある動作を行うコードが結合された形になっていた。

1 韓国でオンライン金融取引をする際に必要な電子証明書

■ ファーミング攻撃ケース ③：脆弱なサイトからマルウェアを配布(Drive By Download)

脆弱なサイトや広告目的に作成されたホームページは、攻撃者にとって恰好の餌食になる。攻撃者は自分の位置を隠した状態で持続的に攻撃することが可能で、広告ページの露出頻度によって不特定多数を対象にマルウェアを拡散・配布できる。だが脆弱なサイトや広告目的のホームページに対する注意喚起は数年前から情報セキュリティレポートなどで登場していたため、攻撃者は時間を特定してマルウェアを配布するようになった。今は正常に見える広告目的のホームページでも、ある瞬間改ざんされてマルウェアを配布するようになる。感染したユーザーを悪意あるサイトに接続させて、個人情報の流出・金銭的な被害を与えるケースが発見されている。

生活密着型脅威その3.正常なファイルに偽装したマルウェア

マルウェアが正常ファイルになりすますのはユーザーを騙すためであり、手法そのものは進化しているものの、基本的に人を騙すことから大きく逸脱していない。攻撃者は Windowsの正常なファイル名をそのまま使用したり、誰もが信頼する応用プログラム名とアイコンを使って自分を偽装する。文書ファイルになりすましてユーザーのクリックを誘導するケースが多く、請求書になりすますケースも出てきた。
これらのマルウェアはユーザーの個人情報を収集して、ユーザーがアクセスするインフラに存在する様々な資料を収集したり、PCやサーバーを乗っ取って攻撃者の思惑通りに活用したりする。乗っ取ったインフラが用済みになったら攻撃に使用したマルウェアを削除して静かに消える場合もあるが場合によっては PCを使い物にならないくらい毀損する場合もある。

診断名	PDF/Phishing, Trojan/Win32.Delpiloader, Trojan/Win32.Bladabindi など
タイプ	トロイの木馬(Trojan、情報収集・流出を目的とする)
ターゲットシステム(OS)	Windows
主な動作	使用者情報の収集・流出、感染 PCを掌握
その他の特徴	攻撃者の意図通りに動くゾンビ PCにして他の攻撃に悪用する
被害予防策	- AhnLab V3を最新バージョンにアップデートして、リアルタイムスキャンを有効 - 文書ファイルや新規インストールファイルは信頼できる出処から入手・使用すること
推奨するアンラボソリューション	V3、MDS(マルウェア診断・駆除)

[表3] なりすまし攻撃の特徴と対策

■ なりすまし攻撃ケース ①：正常なユーティリティになりすましたマルウェア

これまで攻撃者は「PCユーザー」にとって有名なユーティリティや動画ファイルに偽装させたマルウェアを使用することが多かった。最近発見されたバックドア(Backdoor)マルウェアも、韓国の有名な圧縮プログラムに偽装していた。また Adobe Frashアップデートプログラムになりすました「setup.exe」でランサムウェアが配布されたこともあった。この件ではファイル名が setup.exeでも、ファイルのアイコンが存在しなかった点と、ファイル名が Flash_updateでも著作権の説明が「Firefox and Mozila」になっていた点にユーザーが気づけば感染を回避できただろう。だが通常の使用環境の中でユーザーが setup.exeファイルに疑いを持つことはあまりないため、ランサムウェアに感染するケースが多い。

■ なりすまし攻撃ケース ②：文書ファイルになりすましたマルウェア

マルウェア作成者は悪意あるファイルを履歴書に偽装して人事担当者がファイルを展開するように誘導した。文書ファイルに偽装したファイルは実行する際に自動で圧縮が解除される形になっていた。

[図8] 履歴書や料金請求書に偽装した悪意あるファイル

同マルウェアを実行すると、正常なPDF形式の履歴書が追加の悪意あるファイルと一緒に生成され、ユーザー側から悪意あるファイルだと判断しにくい。ちなみに履歴書と同じフォルダーに作成された悪意あるファイルは隠しファイルになっており、エクスプローラーメニューの [整理]-[フォルダーオプション]-[表示]から「保護されたオペレーティングシステムファイルを表示しない(推奨)」項目をオフにしないと表示すらされないのだ。同マルウェアは偽の証明書に署名されていたため、署名情報をよく見ると証明書が有効でないことがわかる。これは攻撃者と持続的に通信して感染対象の内部情報収集・流出及び追加コマンドを遂行するようになっていた。

また他のケースとして料金請求書に偽装した攻撃ケースもあった。2017年4月に発見された同マルウェアは、料金請求書の文書アイコンを使っていたが実際は *.exe拡張子の実行プログラムだった。ファイルを実行するとまず空のワード文書が現われるが、同ファイルは悪意ある行為をしない正常なファイルであるため、ユーザーの疑いを避けられた。同マルウェアの場合はユーザーのキーボード入力内容を別のデータファイルに保存して、ブラウザー閲覧履歴、お気に入り、ショートカット情報及び登録されたアカウント情報、有名なメッセンジャープログラムの使用者情報を奪取した。

■ なりすまし攻撃ケース ③：動画ファイルになりすましたマルウェア

ユーザー同士オンラインでファイルを共有する「トレント(Torrent)」サービスがある。トレントは相互ファイルを送信するプロトコルを意味すると同時にこれを利用する応用プログラムの名前でもある。トレントを利用するとファイルをインターネット上に分散、保存、共有して多数の接続を使って複数の経路から同時にファイルを呼び出すため、送信速度が速い上に多様な領域のファイルを入手できる。トレントサービスを提供する企業は公開掲示板からダウンロード可能なファイルをアップし、検索結果で出されたサービスは誰でも利用できる。またオンラインのコミュニティ掲示板にはダウンロード回数を増やすために興味を引くタイトルのトレントファイルが添付されることが多い。

そんな中、動画プレーヤーアイコンを使用してファイル名に動画拡張子ファイル「*.mp4」をつけたマルウェアが発見された。同マルウェアを実行すると、まずは本物の動画ファイルを生成して表示するためユーザー側からマルウェアと気付きにくい。ユーザーが動画をプレイしたら、攻撃者はマルウェアを通じて使用者情報を奪取してリモートコマンドを送信する準備を進める。

まとめ

攻撃者は今もIT環境のセキュリティホールを探り、攻撃する準備を進めている。彼らは金銭的な利益を目的として奪取した個人情報をブラックマーケットに販売したり、金融情報を利用してダイレクトに資金を落すことまである。もちろんセキュリティシステムも多様化しているが攻撃者は防御システムを迂回してヒューマンエラーを誘導する手法を駆使してくる。双方の攻防戦はどんどん激化している。

今回のコラムでは、正常なサイトとそっくりの偽サイトに個人情報を入力させる「フィッシング手法」、普段よく見知ったサイトアドレスを通じて攻撃者があらかじめ作っておいた有害なサイトに繋ぐ「ファーミング手法」、正常な応用プログラムや文書ファイルに偽装してユーザーPCに潜入後、重要な個人情報を奪取して消える「なりすまし型マルウェア手法」を紹介した。

これらは身近な生活の中で直面する可能性が高い脅威であり、常に注意しなければならない。個人情報の大切さを忘れず普段から気を配れば、より安全で安心できるIT環境を実現できるだろう。

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)