アンラボ・セキュリティレター

Press Ahn

2014.8　Vol.08

2014 年下半期セキュリティ脅威予測

アナリストが語る 2014 年セキュリティ動向

2014 年下半期セキュリティ脅威予測

上半期は個人情報流出、Windows XPサービス終了、スピアフィッシング、スミッシングなどの脅威が問題として浮上しました。

アンラボのASEC（AhnLab Security Emergency response Center）では、引き続き2014年上半期のセキュリティ動向と下半期のセキュリティ脅威予測を発表しました。

2014 年上半期のセキュリティ動向

ハイブリッド

マルウェア作成はもはやプラットフォームを選びません。今までPCマルウェアの作成者はPCのみを対象に、モバイルマルウェアの作成者はモバイルプラットフォームのみを対象にマルウェアを作成しました。しかし2014年の上半期に発見された一部のマルウェアは、PCを最初に感染させた後で携帯電話にマルウェアを感染させる機能を持っていました。このマルウェアは、感染PCにモバイルを接続させると有害アプリをインストールさせる仕組みになっていました。その他、ルータの脆弱性を攻撃してルータに設定されたDNS情報を改ざんする手法も確認されています。

かつてはPCのhostsファイルを改ざんし、有名サイトにアクセスするとフィッシングサイトへのリンクを誘導する方法がメジャーなものでした。最近はルータの脆弱性を利用し、DNS設定を改ざんされたルータに接続するPCと携帯電話の両方に影響を与える方法も登場しています。

POSシステム

2013年末、米国の大手流通会社のPOS（Point-of-Sales）システムがハッキングされ、7,000万人以上の個人情報が流出しました。この事件以降も米国のデパート、レストランなどのPOSシステムのハッキングにより、クレジットカード情報の流出は持続的に発生しています。

韓国でもPOS端末をハッキングして流出した情報をもとに、149枚の偽造カードを作成した犯人グループが検挙されたことがあります。ここではPOSシステムの提供業者のサーバーをハッキングして通常ファイルをマルウェアにすりかえる手法が用いられました。

IoT

モノのインターネット（Internet of Things、IoT）のセキュリティ問題が注目されつつあります。通常Linuxで動作するインターネット・ルータを感染させるワームが登場したのです。仮想貨幣ビットコインが流行し、一部のマルウェアはビットコイン採掘の機能を含んでいるものもあります。韓国でも無線インターネットルータのDNSアドレスを改ざんしてマルウェアの配布に利用したり、冷暖房管理のための機器がDDoS攻撃に使用されたケースもありました。この分野のほとんどはまだセキュリティ機能が存在しないため、根本的な解決が困難な状態です。

サーバーセキュリティ脆弱性

上半期にはサーバーセキュリティの深刻な脆弱性が多数報告されました。

第一には心臓出血という意味を持つ「ハートブリード（HeartBleed）」がありました。その名の通り非常に致命的なこの脆弱性（CVE-2014-0160）は、SSL/TLSを採用したOpenSSLライブラリ上の問題で、メモリ上の機密データがそのまま無防備に公開される可能性があります。上半期だけでもすでに6件ものOpenSSLライブラリの脆弱性が発見されました。Web、メール、メッセンジャーおよびVPN（Vritual Private Network）など広範囲に使用されたセキュリティのためのライブラリが、むしろユーザーとセキュリティ関係者の心臓を凍らせた事件でもありました。

第二は、Apache Webサーバーを攻撃するApache Struts（アパッチ・ストラッツ）セキュリティを迂回する脆弱性（CVE-2014-0094）がありました。Java EE Webアプリケーション開発のためにインストールされるStrutsフレームワーク上の脆弱性で、正常なサービスの運営を妨害し攻撃者が任意のコードを実行させることができます。このフレームワーク上の脆弱性もまた数回に渡って発表されており、上半期にはクライアントシステムを攻撃する手法が主流だった中、深刻なサーバ脆弱性が発生したことによりセキュリティのために適用したシールドも間違って使用する場合、より大きな脅威になりえると警鐘を鳴らしました。

スミッシング高度化

スミッシング・アプリはSMS（ショート・メッセージ・サービス）に含まれるURLの形式で配布されます。初期はSMSに含まれたURLにアクセスするとアプリがダウンロードされるシンプルな形態でしたが、接続したクライアントがモバイル端末の場合のみ有害なアプリをダウンロードするように進化しました。特にフィッシングサイトを制作してユーザーを騙す手法も登場し、キャプチャコード（CAPTCHA）を導入したケースもありました。

配布方法と機能的な面でも多くの変化があり、初期のスミッシングはC&Cサーバーのアドレス（URLまたはIP）が内部にハードコーディングされてHTTPを介してのみコマンドを受信しましたが、最新のスミッシングはSNSのコメント、SMS、XMPP（インスタントメッセンジャー（IM）の国際標準規格）など多様な方法でC&Cサーバーからコマンドが転送されるように進化しています。

モバイルバンキング

2014年までに発見された韓国のスミッシング・マルウェアは、携帯電話の認証方式を使用する小額決済やモバイルバンキングを攻撃対象とする二つのタイプで発見されました。しかし2014年初頭から最近までは決済を狙ったマルウェアはもはや発見されていません。小額決済に利用される携帯電話の認証プロセスが強化されたことによって、マルウェア作成者らはモバイルバンキングのほうに攻撃を集中させるようになったものと見られます。

最近発見されたオンラインバンキングの情報を奪取する有害アプリは、偽の銀行アプリをダウンロードするためのダウンローダーとダウンロードされる偽の銀行アプリで構成されています。この偽の銀行アプリは、アイコンと画面構成まで実際の銀行アプリと非常に類似し、ユーザーが入力した口座番号、パスワード、セキュリティカードなど金融取引に必要な情報と端末に保存された認証書情報を奪取します。

スパイアプリ

上半期にも2~3年前と同様、不特定多数を対象に個人情報を流出するスミッシング手法が着実に増加し、主に宅配便、交通指導取締り、登記などの内容を装って配布されました。しかし最近では、特定の対象の通話内容、文字、写真、インターネットの検索履歴、GPS情報などをリアルタイムに覗き見る「スパイアプリ」が急増しています。

スパイアプリは市販のアプリであるため、開発元のHPでインストール方法や機能の詳細を確認することができます。アプリを利用するには通常月額で3万~10万ウォンを決済すれば購入者が登録したメールからダウンロードすることができます。アプリの配布は、特定の被害者のスマートフォンに直接インストールしたり、文字、メール、メッセージなどにURLのリンクを送ってインストールを誘導する方法が用いられます。

スパイアプリは子どもの保護対策や配偶者の浮気対策など対象を監視することが容易であるため、今後も継続的に増加すると予想されます。

2014 年下半期のセキュリティ予想

スミッシングの増加と高度化

オンラインバンキングを使用した金融取引や決済のために必要な個人情報などを奪取するスミッシング手法は、今後ますます巧妙になるでしょう。一般ユーザーが疑いを持たずに有害アプリをインストールするよう引っ掛けやすい口説き文句を使ったり、正常なサービスと区別がつかないほど精巧な形態のフィッシングサイトを利用する可能性も大きいです。セキュリティ製品の診断を回避するための多様な試みも持続的に発生するはずです。

また、すでに有害アプリに感染されたユーザーの端末に保存されたアドレス帳から多くの情報が流出し、これを活用したスミッシングもさらに増加すると予想されます。

ハイブリッドマルウェアの増加

スマートフォンユーザーは充電やデータ交換などのためにPCと頻繁に接続しますが、これを悪用して重要データを流出したり追加でマルウェアをインストールする有害なハイブリッドマルウェアや有害アプリが増加すると思われます。特にスマートフォンは個人情報、金融取引に必要な各種情報、企業情報、プライバシー情報など金銭的に利用価値の高いデータが多く保存され、PCが感染されることで接続したスマートフォンまで感染させ、より効果的に重要な情報を流出するケースが増加すると思われます。

モバイル・ランサムウェアの脅威

モバイル・ランサムウェアは、感染したスマートフォンのSDカード内のすべてのデータを暗号化します。非常にハイレベルの暗号化アルゴリズムを使用するため、事実上マルウェアの作成者だけが知る復号化キー以外に解除する方法はありません。一度感染すると、写真、動画、音楽、映画、ドキュメント、アプリのデータファイルが暗号化されて使用不可になります。悪意あるアプリの作成者はこれらのデータを人質にした後、ユーザーに金銭的な要求をしてきます。最初に発見されたモバイル・ランサムウェアは、ウクライナのユーザーを狙って作成されました。韓国のようにスマートフォンとモバイルバンキングが発達した環境では、モバイル・ランサムウェアはより致命的です。ランサムウェアに感染した状態で、モバイルバンキングを利用して送金するために入力した銀行アカウントを奪取されるなど、さらに大きな被害を被る可能性があります。今後、韓国のモバイルユーザーをターゲットにしたモバイル・ランサムウェアと銀行アカウントを奪取する有害アプリが結合された新たな脅威が発生する可能性もあります。

電子金融詐欺手口の多様化

攻撃者はユーザーの預金を奪取するため、金融情報を奪取しようとします。このため、マルウェア作成者は今までフィッシング、メモリハッキング、hostsまたはhosts.icsファイルの改ざんおよびルータDNS設定の変更、スミッシングなど多様な方法を使ってきました。今後マルウェアの拡散方法において今よりもさらにユーザーが認知し難い方法（正常プログラムの更新ファイル改ざんなど）を使用してくる可能性が高いです。しかし電子金融詐欺の手法そのものは今までと大差はないと思われるため、hosts ファイルの改ざんが最も多く使用されるでしょう。

APTの多様化

興味を惹くメールで特定のターゲットを攻撃するスピアフィッシングは下半期も続くと思われます。このような社会工学的手法は今年のアジア競技大会や国際問題などを装って悪用される可能性もあります。ハッキングされたWebサイトにアクセスすることで、ゼロデイ脆弱性を介してマルウェアを感染させる水飲み場型攻撃（Watering Hole）も懸念されます。

最近発見されたOpenSSL脆弱性のハートブリード（HeartBleed）のように、オープンソースの脆弱性を利用した攻撃手法もあります。攻撃対象も金融機関や一般企業に拡大されつつあり、企業の経済的損失や機密流出などに常時備える必要があります。

IoTセキュリティの問題

モノのインターネットが増加し、この分野におけるセキュリティ問題も注目され始めています。現況ではモノのインターネットの標準化作業を進めていますが、もしセキュリティ面で脆弱なプラットフォームが標準として選定される場合、今後大きな災害となる可能性もあります。今すぐに発生することはないと思われますが、モノのインターネットのセキュリティ問題は、今後市場拡大が予想されているだけに要注意です。

開発元とコンテンツ配信ネットワーク業者をハッキング

今年の下半期には、開発元とコンテンツ配信ネットワーク（CDN）業者へのハッキング試みが増加すると予想されます。ほとんどのユーザーは開発元から配信するソフトウェアを信頼していますが、中にはセキュリティが脆弱な会社も存在します。

またCDN業者をハッキングし、アップロードされたファイルをマルウェアにすりかえる場合は、開発元がセキュリティを徹底してもマルウェアがユーザーに配布されることになります。よって開発元とともにコンテンツ配信ネットワーク業者もセキュリティ強化が必要です。

国家間のサイバー紛争激化

近年いくつかの主要国では特定の国がサイバー諜報活動と攻撃を仕掛けていると主張し、具体的な証拠を提示することもありました。米国政府は、自国でサイバースパイ活動を行ったとして中国人を起訴して容疑者を検挙したこともあります。これを受けて中国政府は米国のOSやセキュリティ製品の使用中止を検討しています。今後このような国家間のサイバー紛争はさらに続くものと思われます。

http://www.ahnlab.co.jp

http://global.ahnlab.com

http://www.ahnlab.com

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

〒101-002 東京都千代田区外神田4-14-1 秋葉原ＵＤＸ ８階北 | Tel：03-5209-8610 (代)