報道関係者各位

2013 年 10 月 1 日

2013 年上半期、Java エクスプロイトが急増、

Android マルウェアはアプリストア外にも出現

（2013 年 9 月 24 日ヘルシンキ発 － フィンランド本社発表資料抄訳）

エフセキュアが公開した最新の脅威レポートでは、オンラインセキュリティのホットな話題が網羅されています。

エクスプロイトベースの攻撃、特に Java を狙った攻撃が増加の傾向を辿っており、またモバイルの脅威が複雑化し続けていることが、2013 年上半期の特徴となっています。2013 年上半期には、デジタルセキュリティの世界において興味深い事実が明らかになりました。本日公開されたエフセキュアの 2013 年上半期脅威レポートによれば、当期にエフセキュアが検出した脅威のトップ 10 のうちのおよそ 60%近くがエクスプロイトだったのです。

エクスプロイト：もっとも一般的な攻撃ベクトル

エフセキュアラボのセキュリティアドバイザー、**ショーン・サリヴァン**は、エフセキュアが高い割合でエクスプロイトを検出していることは良いことだと指摘し、「当社が検出した脅威トップ 10 の大部分がペイロードへの対応ではなくエクスプロイトのブロックであるという事実から、マルウェア自体をマシンに入り込ませないようにしているという点では成功しているということです」と語っています。

米国のユーザは脆弱性に関連する攻撃を受けることが多く、1000 人あたり 78 人のユーザがエクスプロイトに遭遇しています。これに続くのはドイツおよびベルギーで、1000 人あたり 60 人がエクスプロイトに遭遇しています。Java を標的にしたエクスプロイトは、エクスプロイト全体の中でももっとも多いもので、検出された脅威トップ 10 のほぼ半数を占め、前年下半期の 3 分の 1 から上昇しています。

エクスプロイトはプログラムですが、感染した USB ドライブや e メールと同様に、マルウェアをマシンに運び込むための 1 つの媒体にすぎません。通常、悪意のある Web サイトや感染した Web サイトを経由した攻撃では、コンピュータにインストールされたアプリケーションのコードの不備を悪用してコンピュータにアクセスし、ユーザを監視したり、パスワードやその他の機密データを盗んだり、サイバー犯罪者にマシンの制御を認めたりするマルウェアを感染させます。

モバイルマルウェア：アプリストアの枠を超えて

2013 年上半期には、Android マルウェアの 358 の新しいファミリーおよび亜種がエフセキュアラボによって検出されました。これにより、当ラボがこれまでに検出した驚異の合計数は、ほぼ 2 倍の 794 になりました。これに続くのは Symbian で、16 の新しいファミリーおよび亜種が発見されました。その他のモバイルプラットフォームでは新しいファミリーや亜種は発見されませんでした。

Android マルウェアも、アプリストアだけで配布されるものではなくなりました。2013 年上半期は、感染しているサイトを訪問している間に、悪意のある広告やドライブバイダウンロードによって配布されることがありました。悪意のある広告または悪意のある製品にユーザを導く広告は、広範囲に

及ぶことも手伝って、モバイルマルウェアの配布に利用されることが多くなっています。また、モバイルではまだパソコンほど複雑でないとはいえ、ドライブバイダウンロードが今後も攻撃ベクトルとなることが見込まれています。モバイルドライブバイでは、アプリケーションのインストールを確認するメッセージを使用していますが、これらを回避するオプションがあるため、パソコンのドライブバイよりも見破りやすいものだといえます。

Android のトロイの木馬である Stels は、ボットネットの構築から、バンキングにおけるトロイの木馬としての mTANs（モバイル取引認証番号）の窃取まで、複数の目的を果たすものです。Stels は、配布手段としてスパムなど、Windows マルウェアで一般的な方法を使用します。これは、Android マルウェアが、高度に発展した Windows の脅威のレベルにさらに近づいていることを証明しています。

APT の脅威、Bitcoin マイニング、Mac マルウェア

APT の脅威は、組織や産業界のデータセキュリティに対する脅威として頻繁に話題に上るようになっています。エフセキュアラボは、APT の攻撃者が狙うターゲットの大まかな全体像をまとめました。対象とした APT 攻撃で使用された 100 の文書の研究に関する詳細や、莫大な利益を生む Bitcoin マイニング、および Mac マルウェア、フィッシングなどの最新情報については、2013 年上半期脅威レポートの完全版をご覧ください。

2013 年上半期脅威レポート（英語）：http://www.f-secure.com/en/web/labs_global/

注記 ： エフセキュアラボでは、ユニークサンプル数よりもマルウェアのファミリーおよび亜種の数に重点を置いています。サイバー犯罪者は、マルウェアが検出されるのを避けるために、自動でマルウェアコードにわずかな変化をつけており、これが、基本的には同じマルウェアのファミリーおよび亜種である新しいマルウェアのサンプルとなっています。そのため、サンプルではなくファミリーおよび亜種を数えることで、より現実に即した脅威の数を把握できます。

エフセキュア株式会社 会社概要

http://www.f-secure.co.jp/

エフセキュア ー かけがえのないものを守る

エフセキュアは、お客様が重要なアクティビティに専念できるよう、コンピュータでもスマートフォンでも、オンラインでの保護と安全をお約束します。また、バックアップを提供するとともに、重要なファイルの共有も可能にします。エフセキュアのサービスは、200 以上の通信事業者を通じて世界で提供されており、数百万のホームユーザ、ビジネスユーザから信頼を受けています。1988 年創業のエフセキュアは、NASDAQ OMX Helsinki Ltd に上場しています。

エフセキュア株式会社は、エフセキュア社 100%出資の現地法人として設立され、以降、増収を続けながら順調に企業規模を拡大しており、2009 年 5 月に日本法人設立満 10 周年を迎えました。

会 社 名:	エフセキュア株式会社
カントリーマネージャ:	アリエン・ヴァン・ブロックランド
所 在 地:	〒107-0052 東京都港区赤坂 2-11-7 ATT 新館 6F
設 立:	1999 年 5 月
事業内容:	セキュリティ関連製品・サービスの販売およびサポート

本件に関するお問合せ先
エフセキュア株式会社
マーケティング部
Tel: 03-5545-8942 Fax: 03-5545-8945
Email: japan@f-secure.co.jp
〒107-0052 東京都港区赤坂 2-11-7 ATT 新館 6F
URL: http://www.f-secure.co.jp/
Blog: http://blog.f-secure.jp/