報道関係者各位

2013 年 10 月 16 日

2013 年、日本で急増するセキュリティ脅威

2013 年 1 月からのこの 9 ヶ月間、エフセキュアが検知した日本でのセキュリティ脅威は急増しています。

日本におけるセキュリティ脅威は、年末へ向けて急増しています。既に年初からの 9 ヶ月間で、エフセキュアが検知した件数は 2 倍に達しています。

猛威を奮うマルウェア

今日、最も多く検知されているマルウェアはバックドアを仕掛ける「トロイの木馬」型の Bandook です。Bandook は Windows 2000, XP, 2003, Vista, 7 を含む Windows NT ファミリーに感染します。このマルウェアは感染したコンピュータをリモートでアクセス可能にし、画面キャプチャーやキーボード入力のログの詐取といった悪意のある機能を備えています。

また過去に Conficker として知られていた Downadup の二つのファミリーが二位と三位を占めています。これらのファミリーが出現してから既に 5 年を経ていますが、日本での Windows XP, 2000, 2003 が引き続き数多く利用されているため、引き続き大きな脅威となっているといえます。

続く Java エクスプロイト

2013 年 3 月および 6 月のレポートで報じておりますが、日本では Java エクスプロイトの Majava ファミリーが、検知されたエクスプロイトのトップ五位を占めております。さらに Java Runtime Environment (JRE) の脆弱性 CVE-2013-1493 と CVE-2013-2471 を悪用する、他の二つのエクスプロイトにも注意が必要です。

マルチ・レイヤーでの防御の必要性

シグネチャーが作成されていない所謂ゼロデイ攻撃を引き起こす未知の脅威に対しては、エフセキュアの振る舞い型エンジンである DeepGuard が有効です。数多く検知された「トロイの木馬」のひとつである Bandook も DeepGuard によって阻止されました。今後攻撃はさらに高度化すると予測されるため、DeepGuard のように未知の脅威を阻止する振る舞い型の防御が必要となります。

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/