報道関係者各位

2013 年 2 月 14 日

エフセキュアは 2012 年をエクスプロイト・キットの年と評価

（2013 年 2 月 5 日ヘルシンキ発 ― フィンランド本社発表資料抄訳）

今日オンラインテクノロジーや携帯電話をより安全に且つ信頼して利用できる環境の推進は非常に重要です。強固なパスワードの重要性に加え、コモディティ化が進みプロ化したマルウェア「業界」からの脅威の増大について、エフセキュアの最新の脅威レポートが解説しています。

エフセキュアラボの最新レポート「Threat Report H2 2012」によると、エクスプロイトの闇ビジネスが拡大していること、モバイルを対象にするマルウェアは Android と Symbian 向けが大半を占めていること、そしてボットネットは改変されて再度蔓延していることが指摘されています。2 月 5 日の「Safer Internet Day」に合わせてリリースされたレポートの中では、パスワードの問題に加え、脅威に対抗する方法が提示されています。

「今日のマルウェアの世界はコモディティ化され、そしてプロ化されています」と主席研究員の**ミッコ・ヒッポネン**は述べています。「特に昨年後半には、脆弱性の悪用をより標準化したものや、自動化したエクスプロイト・キットの増加が見られました。」

エクスプロイト・キットと古いソフトウェアの脆弱性

2012 年はソフトウェアの脆弱性を悪用したユーザーの機器へのアクセスが最も顕著な手法になりました。昨年後半はエクスプロイト関連の検出が全体の 28%を占め、そのうちの 68%が Java の脆弱性に関連したものでした。

エクスプロイト検出の大半は 4 つの脆弱性（Windows が 2 つ、Java が 2 つ）に関連したものであり、そのほとんどが今日の顕著なエクスプロイト・キットである BlackHole や Cool Exploit を含む脆弱性を悪用するものによって起こされたものでした。これら全ての脆弱性は過去 2 年間にすでに報告されたもので、ベンダーによってソフトウェア更新の重要性の喚起とともにパッチも提供されていました。

「マルウェアシステムにおける犯罪者たちは、各々がそれぞれ小さな部分を担当し、それがチェーンとなってつながっていきます」とエフセキュアのセキュリティアドバイザーの**ショーン・サリヴァン**は述べています。「エクスプロイトは最初のつながりにすぎず、犯罪者たちはそこからドアを開けて入り込みます。」

増加するモバイルマルウェア:サンプル、あるいはファミリーや亜種?

2012 年に検出された新しくユニークなモバイルマルウェアの亜種のうち、Android を対象としたマルウェアは 79%（238）を占めており、この数字はモバイル市場におけるプラットフォームとしての占有度合が高いためと言われています。Symbian は次に大きなシェアで、検出された亜種の 19%を占めています。

レポートによって数十から数十万と数は異なりますが、Android 向けのマルウェアサンプルが 2012 年に増加したと声高に主張したセキュリティベンダーがありました。サンプル検出数は増えていますが、エフセキュアラボでは単に検出数だけを注視しているわけではありません。「サンプルはマルウェアパッケージの周辺部にすぎないからです」とサリヴァンは述べています。

内部は従来と同じマルウェアファミリーですが、いろいろな方法で偽装することが可能です。我々はむしろファミリーと亜種の数を注視しています。」マルウェアサンプルの増加は製作側がコモディティ化と自動化を進めている現れであって、必ずしもマルウェアファミリーが増えたわけではないとサリヴァンは指摘しています。

「エフセキュアはセキュリティの位置づけをより包括的に捉えており、ひとつのデータだけに頼ることはできません。」とサリヴァンは述べています。「ひとつのデータでセキュリティの分析を行うことは馬鹿げたことか、誇大マーケティングだと考えます。」

ボットネット、銀行関連のトロイの木馬とパスワードの問題

被害を受けた様々な分野で対策が進んだためボットネットは活発ではない状態が近年は続いていましたが、新しいパッケージングや従来とは異なる手法を使って 2012 年に再び現れました。”rent-a-botnet”スキームのような新しいビジネスモデルが拡大していますが、そこではサイバー上の犯罪者たちが感染したコンピュータのネットワーク全体を借りて攻撃に悪用しています。ZeroAccess は最も早いスピードで増えているボットネットであり、グローバルでは数百万台ものコンピュータが 2012 年に感染してアメリカとヨーロッパでは 140,000 あまりのユニークな IP アドレスが影響を受けました。Botnet Zeus は感染が拡大している銀行関連のトロイの木馬で、アメリカ、イタリア、ドイツが最も被害を受けた国です。

レポートではパスワードが「機能していないことはみんな知っている」と指摘しています。強固なパスワードは記憶するのが難しく、アカウント毎に異なるパスワードを使うなど面倒を強いられています。ソーシャルエンジニアリングの秀でたテクニックを使えば強固なパスワードでさえリセットすることができます。より良いソリューションが登場するまでは、安全なパスワード管理方法をレポートで提供していきます。

MAC 向けマルウェア、産業スパイ、Web 上のマルウェアを含む最新の脅威に関しての詳細は、エフセキュアの Threat Report H2 2012 を参照ください。

Threat Report H2 2012 の詳細情報：

http://www.f-secure.com/en/web/labs_global/whitepapers/reports

強固なパスワードを覚えておくには？：

http://safeandsavvy.f-secure.com/2013/01/21/how-do-i-remember-strong-passwords/

Threat Report H2 2012 に関するブログ：

http://blog.f-secure.jp/archives/50693330.html

エフセキュア株式会社 会社概要

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

エフセキュアは、IT 先進国フィンランドで 1988 年に設立されて以来、23 年にわたりセキュリティ製品に取り組んでいる業界の先駆者で、世界規模でセキュリティサービスを提供しています。1999 年にOMX ヘルシンキ証券取引所に上場し、以来、順調に成長を続けている株式公開企業のひとつです。

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/