報道関係者各位

2013 年 7 月 10 日

エフセキュア、エクスプロイトとの戦いを進展

（2013 年 6 月 18 日ヘルシンキ発 ー フィンランド本社発表資料抄訳）

今日、非常によくあるマルウェアの感染経路の一つに、オンライン上のエクスプロイトがあります。エフセキュアの新技術により、エクスプロイトをその挙動に基づいて遮断することで、エクスプロイトへの対応範囲を拡大します。

Blackhole、Cool、そしてエクスプロイトによって感染拡大する Citadel のようなボットネット。ユーザのマシンに不正アクセスするための一般的な手法として、ソフトウェアの脆弱性が悪用されるようになっていますが、エフセキュアは事前予防機能を増強することにより、エクスプロイト防御を強化しています。ディープガード 5 は新たに出現する脅威を遮断する、エフセキュアの最新の挙動に基づく解析技術ですが、この公開によりエフセキュアは、悪用の対象となる脆弱性が明らかでなくとも、エクスプロイトの攻撃を検出することを可能にします。

通常、エクスプロイトは悪意のある、または脆弱性のあるウェブサイトを通じて攻撃します。エクスプロイトは、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に存在する欠陥を巧みに利用して、コンピュータに侵入してユーザを監視するマルウェアを感染させたり、パスワードや機密データを盗んだり、マシンを乗っ取ったりさえもします。エフセキュアのセキュリティラボが検出した上位 10 個のマルウェアのうち、70～80%はエクスプロイトです。蔓延拡大の主な原因として、エクスプロイトキットの存在が挙げられます。エクスプロイトキットを使えば、例え技術が未熟であっても簡単にコンピュータに侵入できてしまいます。

「マルウェアは特性を変異させることができますが、常に悪意ある行為をすることに変わりはありません。エクスプロイトによって外観が変化したり、悪用する脆弱性が変わったりする場合もありますが、常にエクスプロイトと同じ挙動を示します。防御方法の代表的なものは悪用されている脆弱性に結びついていますが、我々はその挙動に基づいてエクスプロイトを検出するため、より幅広く対応できます。それは、すべての脆弱性が明らかになっているわけではないからです。」とエフセキュアのシニアアナリスト、**ティモ・ヒルボネン**は述べています。

ディープガード 5 のエクスプロイテーション防御機能により、Web ブラウザ、プラグイン、Microsoft Office、Java といった、悪用されやすいプログラムのプロセスを監視します。また、Microsoft Word や PDF といった、文書形式のファイルを開くためのプログラムも監視します。ディープガードはエクスプロイト攻撃の兆候である怪しい挙動や悪意のある挙動を遮断します。

行動解析：マルチレイヤー保護機能におけるクリティカルレイヤー

エクスプロイト遮断はディープガードに最近追加された機能で、従来のシグネチャスキャンが抱える弱点（分析した上で防御可能にするために、マルウェアのサンプルが必要）に対応します。セキュリティラボがマルウェアサンプルを受け取って保護機能をアップデートしている間に、ユーザがマルウェアに感染してしまうかもしれません。自動マルウェア作成キットにより、マルウェアの新たな亜種が急激に増加していることが、問題を悪化させています。このキットにより、大量の新たな亜種が簡単に増殖されるのです。

「高水準のアンチウイルス技術は、長年指名手配リストに載っている悪者から身を守るだけでは終わらせません。マルウェアを遮断するにはその挙動を理解することが必要です。そこで我々は 2006

年にディープガードの初版を開発いたしました。そして今回の最新版はこれまでの中で、不審な挙動の学習能力に最も優れています。」とエフセキュアのセキュリティアドバイザである**ショーン・サリヴァン**は述べています。

プログラムが実行されると、ディープガードは動作を開始します。そして、悪意のある行為を遅れて行うマルウェアを見つけるため、プログラムの実行中は監視を続けます。ディープガードの行動解析およびエクスプロイト遮断は、エフセキュアのセキュリティレイヤの 2 つを構成します。これにはブラウジング保護、シグネチャスキャン、ファイルレピュテーション、そして感染率検査も含まれます。

ディープガードの貢献により、エフセキュアはドイツのセキュリティソフト第三者評価機関、AV-TEST から贈られる Best Protection 2012 を受賞しました。ゼロデイ攻撃および悪意のあるウェブサイトや電子メールによるマルウェア感染といった、現在の脅威に対して最も効果的な予防策を提供するということで、エフセキュアのホームユーザ向け製品は他の 19 ベンダーの製品に打ち勝ちました。ディープガードの新しいエクスプロイト防御があれば、お客様は今後とも間違いなく最高の保護機能で守られます。ディープガード 5 はすでに公開されているので、最新バージョンをお持ちのエフセキュアのお客様はすでにこの新しい保護機能で守られています。

ディープガードについてさらに詳しい情報は、エフセキュアの最新のホワイトペーパー「エフセキュアディープガード：新たに出現する脅威に対するオンホスト事前予防機能（英語）」を参照ください。

http://safeandsavvy.f-secure.com/2013/06/18/deepguard/

*エフセキュアの社名、ロゴ、製品名は F-Secure Corporation の登録商標です。
*本文中に記載された会社名、製品名は各社の商標または登録商標です。

エフセキュア株式会社 会社概要

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

エフセキュアは、IT 先進国フィンランドで 1988 年に設立されて以来、25 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/