報道関係者各位

2014 年 12 月 19 日

エフセキュア、マルウェア・キット Regin に関する ホワイトペーパー公開

エフセキュアは、最新のマルウェア・キット Regin に関して攻撃の前半の技術的な解析を行ったホワイトペーパーを公開しました。

Regin は現在活動中のマルウェア群の中で最も複雑なもののひとつで、洗練された最新の諜報キットとして、世界中の広範な組織を攻撃しています。エフセキュアでは 2009 年にヨーロッパで初めて Regin を検知し、それ以来 Regin の新しいバージョンを解析し続けてきました。最新の Regin の攻撃は非常に複雑で洗練されており、Stuxnet や、Flame、Turla/Snake のようなマルウェアと同一のカテゴリに配しています。

このほどエフセキュアでは、32bit 版および 64bit 版の Rigin それぞれについて、二段階からなる攻撃の前半について技術的な解析を行い、ホワイトペーパーとして公開いたしました。Regin による攻撃の一段目の目的は、モジュールをローディングし、セキュリティ製品による検知を困難にすることによって、二段目の攻撃を可能にすることです。Regin の一段目のターゲットは、Windows NT 4.0 以降の幅広い Windows プラットフォームです。Regin の一段目は、攻撃されたシステムの特定の箇所から暗号化されたコンテンツを検索し、カーネルのメモリー上で展開して、コントロールを奪取します。

なおエフセキュアの製品では、Regin を Rootkit:W32/Regin.A および Backdoor.Regin.A として検知し、防御する実装が成されています。

Regin に関する技術的な情報は、下記エフセキュア・ブログ、および各ホワイトペーパーをご参照ください。

エフセキュア・ブログ：諜報ツールキット Regin

http://blog.f-secure.jp/archives/50738899.html

ホワイトペーパー：Malware Analysis Report W32/Regin, Stage #1（英語）

https://www.f-secure.com/documents/996508/1030745/w32_regin_stage_1.pdf

ホワイトペーパー：Malware Analysis Report W64/Regin, Stage #1（英語）

https://www.f-secure.com/documents/996508/1030745/w64_regin_stage_1.pdf

---

エフセキュア株式会社 会社概要

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

F-Secure – Switch on freedom

エフセキュアは、オンラインセキュリティおよびプライバシー保護を提供するフィンランドの企業です。弊社は、世界中の何百万人もの人々が、監視されることなくインターネットを楽しみ、さまざまなデータを保存や共有する力と、オンラインの脅威からの安全性を提供します。弊社の存在意義は「デジタルフリーダム」のために闘うことです。この動きに参加し、自由のために闘いましょう。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、2014 年 5 月に日本法人設立満 15 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:	〒102-0072 東京都千代田区飯田橋 3-11-14　GS 千代田ビル 5F
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: 03-3556-6301　Fax: 03-3556-6295
Email: japan@f-secure.co.jp
〒102-0082 東京都千代田区飯田橋 3-11-14　GS 千代田ビル 5F
URL: http://www.f-secure.co.jp/
Blog: http://blog.f-secure.jp/