報道関係者各位

2015 年 5 月 12 日

エフセキュア、CozyDuke と社会的地位のある標的を狙う諜報活動との関連を指摘

（2015 年 4 月 30 日ヘルシンキ発 ー フィンランド本社発表資料抄訳）

エフセキュアラボが最新のホワイトペーパーで、CozyDuke が現在も継続する、政府およびその他大規模組織を狙った一連の持続的標的型攻撃（APT）に関与していることを強調。

エフセキュアラボは、マルウェアに関する新しい分析で、政府およびその他大規模組織が直面する継続的な脅威として、CozyDuke を挙げています。CozyDuke は、標的のセキュリティを低下させ、情報を盗むために、いくつかの戦術とマルウェアを組み合わせて利用する持続的標的型攻撃（APT）のツールキットです。エフセキュアの今回の分析では、社会的地位のある標的を狙う多くの攻撃に関与するその他の APT と、この CozyDuke を関連付けています。

分析によると、CozyDuke は、コマンドアンドコントロールのリソースを有名な MiniDuke および OnionDuke APT と共有しています。エフセキュアラボでは、ロシアの TOR 出口ノードを使用する人々に対する悪意のある攻撃、NATO および多数の欧州の政府機関に対する標的型攻撃など、社会的地位のある標的を狙う攻撃がこれらの APT プラットフォームに起因すると考えました*。CozyDuke は、このような他のプラットフォームとほぼ同じインフラストラクチャを利用し、OnionDuke が利用するのと類似した暗号化アルゴリズムを含んだコンポーネントを採り入れ、同じテクノロジーを異なる作戦に転用しています。

「これらの脅威はすべて互いに関連し、リソースを共有していますが、特定の標的に対してより効果が上がるよう、少しだけ方法を変えて作成されています」とエフセキュアのセキュリティ・アドバイザーである**ショーン・サリバン**は述べています。「CozyDuke が興味深いのは、多様な標的に対して利用されていることです。その標的の多くは、依然として欧米の政府や機関ですが、アジアを拠点とする標的に対しても利用されていることがわかっています。このことは注目すべき観察結果です。」

CozyDuke とそれに関連する脅威は、ロシアが起源であると考えられています**。攻撃者は、組織の従業員に、気をそらすおとりファイル（PDF やビデオなど）を添付した電子メールを送信し、その従業員をだまして添付ファイルを開くなどの操作をさせて、組織に足場をつくります。CozyDuke は、気づかれずにその足場を利用してシステムに感染します。攻撃者は、CozyDuke と互換性のある多様なペイロードを利用して、さまざまなタスクを実行できます。これにより、パスワードやその他の機密情報の収集、リモートでのコマンドの実行、または秘密の通信の傍受を行うことができます。

サリバンは、攻撃者の本当の正体と動機が何であるのかを確実に結論づける十分な証拠はないとしながらも、OnionDuke と MiniDuke に起因する攻撃を行っているのは同じ人物であることに、確信を強めています。「CozyDuke が実際に現れたのは 2011 年以降のことですが、常に拡大を続けている脅威です。現在も変化し続けています。」このことは、これらのツールの改良に時間と金を投資し

ている 1 つまたは複数のグループが存在することを示唆しています。よって、現在彼らが何を目的にしているのかを知ることに、私たちは焦点を当てる必要があります。」

このホワイトペーパーでは、CozyDuke が感染する前に、サイバーセキュリティソフトウェアの有無を確認していることも指摘しています。ソフトウェアの種類によっては、CozyDuke が攻撃を中止する場合があります。エフセキュアで脅威に関する情報のアナリストを務める Artturi Lehtiö が執筆したホワイトペーパーは、エフセキュアの Web サイトから無料でダウンロードできます。

*出典: https://www.f-secure.com/weblog/archives/00002764.html

**出典：https://www.f-secure.com/weblog/archives/00002780.html

詳細情報：

CozyDuke マルウェアの分析: https://www.f-secure.com/documents/996508/1030745/CozyDuke

2014 年下半期脅威レポート: https://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2014

エフセキュア株式会社 会社概要

http://www.f-secure.com

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、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
代表取締役社長:	イングヴァー フロイランド
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
〒102-0072 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.com
Blog: http://blog.f-secure.jp