報道関係者各位

2014 年 7 月 24 日

エフセキュア、SNS とデジタル通貨を悪用したマルウェア ’Lecpetex’ に関するホワイトペーパーをリリース

エフセキュアは、Facebook のメッセージ機能を悪用して不正なビットコイン・マイニングのためのボットネット感染を引き起こすマルウェア Lecpetex に関するホワイトペーパーをリリースいたしました。

Facebook、Twitter、Skype などのソーシャル・ネットワーク・プラットフォームを悪用したマルウェアは目新しいものではありません。より深刻なのは、マルウェアがワームとして自らを拡散し、感染したユーザのマシンからのデータ収集に重点を置くようになったことです。一方、ビットコインマイニングは、ユーザが自分のマシンで現金を生み出す方法として人気になっており、また犯罪者にもしばしば悪用されるようになっています。このため、ソーシャルネットワーキングとデジタル通貨という 2 つの傾向を結びつけたマルウェアが出現することは、避けられない事態でした。感染したマシンはボットネットとして悪用されます。エフセキュアでは Facebook との共同による取り組みで発見したマルウェア Lecpetex について、注意を喚起するホワイトペーパーをリリースしました。

Lecpetex は、ソーシャルエンジニアリングの手法で拡散されます。これは、Facebook のメッセンジャーサービス経由で送信されるメッセージに添付された ZIP ファイル形式の実行可能プログラムとして配布されるということです。ユーザが添付ファイルをクリックしやすくするよう、メッセージには「lol」、「hahaha」、「OMG」など、古典的な仕掛けのテキストが使用されます。

メッセージに添付された ZIP ファイルをクリックすると、Java 実行可能ファイル（JAR）プログラムが解凍されます。JAR ファイルを起動すると、事前定義された Dropbox ファイル共有リンクから fbgen.dat という名前のダイナミックリンクライブラリ（DLL）ファイルを探し、ダウンロードします。このプロセスの間、何らかのアクションが発生したことをユーザに示す兆候はありません。JAR ファイルをクリックした後、すべてがバックグラウンドにおいてサイレントモードで実行されます。

ファイルが見つかりダウンロードが完了すると、JAR ファイルは実行中にダイアログボックスが表示されないよう「/s」キーを使用して DLL のサイレント登録を指定し、「regsvr32.exe」を実行します。マルウェアはその起動場所を隠すため、レジストリエディタで無視される 255 文字を超えるキー名を使って偽のレジストリエントリを追加します。次に DLL は、explorer.exe インスタンスに、ビットコインマイニングのアクティビティを書き込ます。

Lecpetex は、ユーザのファイルの内容に対する好奇心を悪用して、マルウェア自体をダウンロードおよびインストールさせる、古典的なソーシャルエンジニアリング攻撃手法を使用して拡散されます。このため、ユーザ行動の標準的な予防措置が効果的です。

- 知らない相手から送信された添付ファイルはクリックしない。
- メッセージは一見すると友人から送付されたように見えるが、その内容が普段と違うように感じる場合、添付ファイルをクリックしない。他の手段を使ってその友人に連絡を取り、アカウントが侵害されている可能性があることを伝える。
- 添付ファイルをクリックすると実行可能ファイルが表示される場合、これを実行する前に、信頼できるアンチウイルスプログラムを使用してスキャンする。

エフセキュアのセキュリティ製品は、以下を検出することでマルウェアのさまざまなコンポーネントを特定します。

- Trojan-Downloader:Java/Lecpetex.C
- Trojan.Win32/Lecpetex.A!Mem

ホワイトペーパーの詳細はこちらでご覧いただけます（英語）：

http://www.f-secure.com/static/doc/labs_global/Whitepapers/lecpetex_whitepaper.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、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/