

2014年8月13日

NAS デバイスを狙ったランサムウェアが蔓延

NAS デバイスのファイルを暗号化し、「身代金」を要求するランサムウェア SynoLocker の攻撃が広がっています。

現在、ビジネスユーザでもホームユーザでも広く利用されている NAS デバイスをターゲットとしたマルウェアが広がり始めています。このマルウェア SynoLocker に感染すると、デバイスに格納されているファイルが暗号化されてしまいます。

Synolocker は暗号化に続けて、ユーザに「身代金」についてのメッセージを提示します。このメッセージでは、まず Tor Browser Bundle をダウンロードして、インストールするようにユーザに指示し、次にユーザは Tor ネットワーク上の特定の Web サイトへ誘導されます。この Web サイトでは、ある Bitcoin ウォレットに 0.6 BTC (約 36,000 円相当) の支払いを行うよう指示を受けます。マルウェアの作者らは、送金を受け取った後にユーザにファイルを復旧するための復号キーを提供することを表示しています。

その結果、ユーザが別途バックアップを保持していない限り、NAS デバイ스에格納された任意のファイルが失われるという事態に直面することになります。

マルウェアの作者へ「身代金」を支払ってもファイルが復旧される保証はなく、また悪意ある集団に金銭的利益を与え、さらなる被害へ繋がることになるため、「身代金」の支払いは絶対に行わないように十分な対策が求められます。

- 万一の感染に備えてバックアップを取っておく。感染した場合は、対応方法をメーカーに確認する。
- 攻撃は古い NAS OS の脆弱性を悪用したものが多いため、最新の状態にしておく。

なお、エフセキュアの各セキュリティ製品では SynoLocker を Trojan:Linux/SynoLocker.A として検知し特定します。

Synolocker の詳細はこちらでご覧いただけます：

<http://blog.f-secure.jp/archives/50732483.html>

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/>