報道関係者各位
プレスリリース

2015 年 6 月 11 日
株式会社 FFRI

FFR yarai が日本年金機構を狙うマルウェア「Emdivi」を検知・防御
～パターンファイルに依存せず、最新のマルウェア動向研究の知見を活かして～

サイバーセキュリティ領域において国内で独自の研究開発活動を展開している株式会社 FFRI（本社：東京都渋谷区、代表取締役社長：鵜飼裕司、以下 FFRI）は、2015 年 6 月 11 日、標的型攻撃対策ソフトウェア「FFR yarai」および個人 PC 向けセキュリティソフト「FFRI プロアクティブ セキュリティ」が日本年金機構を狙う遠隔操作型マルウェア「Emdivi」をリアルタイムに検知・防御が可能であったことをご報告いたします。

「パターンマッチング方式」の既存のアンチウイルス製品では防御困難な標的型攻撃

2015 年 6 月 1 日、日本年金機構より基礎年金番号を含む個人情報、約 125 万件の流出が発表されました。報道によると、悪意の第三者により職員宛てに送信されたマルウェアが添付された電子メールを開封した結果、マルウェアに感染し、情報の窃取に至ったとされています。

近年、こうした情報搾取等の明確な目的の下、特定組織を狙った標的型攻撃が増加しております。標的型攻撃においては、ほとんどの場合新種のマルウェアが利用されますが、こうしたマルウェアは一般に流布していないため事前にパターンを用意することが困難であり、現在広く普及している「パターンマッチング方式」のアンチウイルス製品では、防御することが極めて困難です。今回の日本年金機構を狙った攻撃もこうした標的型攻撃の一種であり、職員端末に導入されていたアンチウイルス製品では防御できなかったことが報道されています。

日本年金機構を狙うマルウェア「Emdivi」 vs. FFR yarai

本件で悪用されたマルウェアは、「Emdivi」と呼ばれる種類のマルウェアであることが報道されています。FFRI は、日本年金機構を対象とした標的型攻撃で使用されたと見られるマルウェアの検体をセキュリティ業界関係ルートで入手し、当社製品で検知・防御できるか否かの確認を実施いたしました。その結果、メール添付されたと見られる検体は、下記の 2 製品で検知・防御できることを確認いたしました。

・FFR yarai Version 2.5.1192 (2014 年 8 月 22 日リリース)～同 Version 2.6.1294 (2015 年 6 月 4 日リリース) ※1

・FFRI プロアクティブ セキュリティ Version 1.0.217 (2015 年 4 月 24 日リリース)

※1 本製品リリースは、事前に計画された製品ロードマップに基づくものであり、今回の事件への対応とは関係ありません。

当社製品はパターンファイルを一切使用しておりませんが、FFRI のエンジニアが最新のマルウェアの動向を研究し、その知見を反映したプログレッシブ・ヒューリスティック技術を搭載しているため、マルウェアの構造や振る舞いを見て攻撃を検知・防御することが可能です。本製品が導入されていた環境下においては、メール添付されていたファイルを仮に実行していたとしても被害が発生していないものと思われます。

FFRI は、今後も独自の調査・分析を行い、脅威を先読みすることで真に価値のある対策を社会に提供できるよう日々精進していく所存です。

◎法人向け
【製品名称】
FFR yarai
http://www.ffri.jp/products/yarai/index.htm
【FFR yarai の防御実績】 これまでに防御した攻撃・マルウェア一覧
http://www.ffri.jp/products/yarai/defense_achievements.htm

◎個人・SOHO 向け
【製品名称】
FFRI プロアクティブ セキュリティ
http://www.ffri.jp/online_shop/proactive/index.htm

■標的型攻撃対策ソフトウェア「FFR yarai」とは

FFR yarai シリーズは、従来のセキュリティ対策で用いられているシグニチャやパターンファイルなどに依存せず、標的型攻撃で利用される攻撃の特徴を 5 つのヒューリスティックエンジンにより、様々な角度から分析し、未知の脅威に対して高い精度で攻撃を検知・防御します。純国産の技術で開発した製品で、厳格なセキュリティ対策が求められる官公庁や重要インフラ企業、金融機関での採用実績が多数あります。

韓国の放送局や銀行などがシステムダウンした韓国サイバー攻撃（2013 年 3 月）、ソニー・ピクチャーズエンターテイメント社に対する一連のサイバー攻撃に関連するシステム破壊型マルウェア（2014 年 12 月）、Adobe Flash Player の脆弱性（2015 年 1 月）、ハードディスクのファームウエアの書き換えを行う HDD

ファームウェア感染マルウェア（2015 年 2 月）、ネットバンキングユーザーを狙ったバンキングマルウェア（2015 年 3 月）等、これまでに防御した攻撃・マルウェアを防御実績として FFRI ホームページにて公開しています。

■株式会社 FFRI について

当社は 2007 年、日本において世界トップレベルのセキュリティリサーチチームを作り、コンピュータ社会の健全な運営に寄与するために設立されました。現在では日々進化しているサイバー攻撃技術を独自の視点で分析し、日本国内で対策技術の研究開発に取り組んでいます。研究内容は国際的なセキュリティカンファレンスで継続的に発表し、海外でも高い評価を受けておりますが、これらの研究から得られた知見やノウハウを製品やサービスとしてお客様にご提供しています。主力製品となる、「FFR yarai」はミック経済研究所調べ※2 によるエンドポイント型標的型攻撃対策分野における出荷金額において No.1 を獲得しております。

※2 出典：ミック経済研究所「情報セキュリティソリューション市場の現状と将来展望 2014【外部攻撃防御型ソリューション編】」

本件に関するお問い合わせ先
写真・資料等がご入用の場合もお問い合わせください。

株式会社 FFRI
経営企画部　PR 担当
TEL：03-6277-1811
E-Mail：pr@ffri.jp　URL：http://www.ffri.jp