報道関係者各位
プレスリリース

2015 年 11 月 16 日
株式会社 FFRI

ソニー銀行が FFRI の標的型攻撃対策ソフト「FFR yarai」を採用
～未知の脅威を検知するソリューションとして OA 系システム全端末に導入～

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、標的型攻撃対策ソフト「FFR yarai」がソニー銀行株式会社（本社：東京都千代田区、代表取締役社長：伊藤裕、以下：ソニー銀行）に採用されたことを 2015 年 11 月 16 日にご報告いたします。

ソニー銀行は、個人に特化したオンラインバンキングサービスを展開するインターネット銀行です。金融商品・サービスの拡充とともに、お客様の大切な資産を守るためにセキュリティ対策にも注力しています。

ソニー銀行ではパターンマッチング型のウイルス対策やURLフィルタリングの導入、端末のシンクライアント化の実施をしていましたが、これらの対策では対応できない脅威を検知するためのソリューションを検討していました。また、ネットワークレイヤーにはプログラムの振る舞いから脅威を検知するサンドボックスを既に導入していましたが、より強固なセキュリティ対策を実現すべく、ネットワークとは異なる防御レイヤー（エンドポイント）に対して、異なる検知ロジックを持つ振る舞い検知製品の導入を検討していました。

そこでセキュリティコンサルティング企業とともに外資系ベンダー製品を含め、製品の評価を実施し検討したところ、機能とコストのバランスの優位性から「FFR yarai」が、インターネット接続可能な OA 系システム全端末に採用されました。採用につながる大きなポイントとなったのは、他社製品と組み合わせて使っても運用負荷が重くならないことや、製品バージョンアップの頻度が年 1～2 回と低いことなど運用上のメリットが多い点でした。また、国内に研究開発体制があることや、国内で発生した問題に対してのレスポンスの速さなどの FFRI のサポート体制も高く評価されました。

「FFR yarai」は、官公庁や重要インフラ企業での導入実績が豊富な標的型攻撃対策ソフトです。FFRI が独自に開発した「プログレッシブ・ヒューリスティック技術」※1 により、日本年金機構を狙ったマルウェア「Emdivi」（2015 年 6 月）やバンキングマルウェア「SHIFU」（2015 年 10 月）も検知・防御できることが確認されています。

※1 パターンファイルに全く依存せず、マルウェアの構造や振る舞いを見て、マルウェアに特徴的な「悪意」を分析することにより検知・防御する技術。パターンマッチング技術では防御が難しい新種や改造されたマルウェアであっても、マルウェアに共通する「悪意」を検知して防御することが可能。

ソニー銀行では社内向け・顧客向けシステムを問わず、自社を取り巻く IT 環境とサイバーセキュリティ動向を見定め、継続的なセキュリティ対策強化を検討していくとのことです。

FFRI は攻撃者の思考を先読みし、サイバーセキュリティ上の未知の脅威に対抗するプロアクティブな研究開発体制を構築しております。今後も研究開発の知見とノウハウを活かし、企業の経営戦略に合致した製品やサービスを提供し、健全な IT 社会の発展に貢献してまいります。

製品名称

FFR yarai

http://www.ffri.jp/products/yarai/index.htm

FFR yarai 防御実績ページ（防御した攻撃・マルウェアー覧）

http://www.ffri.jp/products/yarai/defense_achievements.htm

関連ページ

ソニー銀行様　FFR yarai 導入事例

http://www.ffri.jp/assets/files/products/exp/yarai_SonyBank.pdf

【FFR yarai のプログレッシブ・ヒューリスティック技術】

■ZDPエンジン	メールやWebページ閲覧時の攻撃など、既知・未知の脆弱性を狙ったウイルス攻撃を防御。 独自の「API-NX」技術(特許第4572259号)で、任意コード実行型脆弱性の攻撃を防御。
■Static分析エンジン	プログラムを動作させることなく分析。「PE構造分析」「リンカー分析」「パッカー分析」「想定オペレーション分析」など 多数の分析手法「N-Static分析」で検知。
■Sandboxエンジン	仮想CPU、仮想メモリ、仮想Windowsサブシステムなどで構成される仮想環境上でプログラムを実行。 独自の「U-Sandbox検知ロジック」で命令の組み合わせに基づいて検知。
■HIPSエンジン	実行中プログラムの動作を監視。他プログラムへの侵入、異常なネットワークアクセス、 キーロガーやバックドア的な動作などの挙動を、独自の「DHIPSロジック」で検知。
■機械学習エンジン	FFRIが収集したマルウェアに関するビッグデータを元に実行中のプログラムを監視。 ビッグデータ上の振る舞い特性を抽出し、機械学習で分析した特徴により端末上の悪意ある挙動を検知。

■ソニー銀行株式会社について

個人のお客様を対象に資産運用を中心とした金融商品・サービスを提供するインターネット銀行です。「フェアである」ことを企業理念に掲げ、お客様目線のより良いサービスを追求しています。

■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、IT 社会に貢献すべく設立されました。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：「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 2015【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
経営管理本部　PR 担当
TEL：03-6277-1811
E-Mail：pr@ffri.jp　URL：http://www.ffri.jp