報道関係者各位
プレスリリース

2017 年 6 月 20 日

株式会社ＦＦＲＩ

豊島区役所がＦＦＲＩのマルウェア自動解析システム「FFRI yarai analyzer」を採用
～庁舎移転後からメール通信の監視に利用、庁舎内でマルウェアを迅速に解析～

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、マルウェア自動解析システム「FFRI yarai analyzer」が豊島区役所（東京都豊島区、区長：伊藤雅彦、以下 豊島区役所）に採用されたことをご報告いたします。

豊島区役所は、2015 年 5 月に現庁舎へ移転しました。豊島区 政策経営部 情報管理課では現庁舎への移転にあたり、移転の 2～3 年前からは庁舎内のシステムの洗い直しにとどめ、移転のタイミングで実現させたい、新たなセキュリティ対策の計画を推進してきました。

より強固なセキュリティ対策の実現に向けて「土日も開庁している区民の窓口業務をしっかりと守るため、有人での 24 時間 365 日体制は必須」「移転前にできていなかったログ管理や通信をすべて見るフォレンジックがこれからは必要」「今後は未知マルウェア対策としてサンドボックスを利用した製品も利用していくべき」といった情報管理課の要望を踏まえ、有人による 24 時間 365 日体制で統合運用管理サービスの利用を移転後から開始しました。

統合運用管理サービスの一環である「FFRI yarai analyzer」は、パケットキャプチャ製品（トーテックアメニティ社「NetRAPTOR」）との連携や、未知マルウェア検出に優れたエンジンにより仮想環境上で動的解析が可能であるという点で、まさに豊島区が移転前から求めていた、新たなセキュリティ対策の要望を満たすセキュリティ製品として評価されました。

豊島区では現在、FFRI yarai analyzer をメール通信の監視に利用しています。現庁舎への移転以降、何件かのマルウェアの検出がありましたが、統合運用管理サービスのヘルプデスク担当が検出後すぐに庁舎内で FFRI yarai analyzer で解析し、情報管理課に迅速に報告を上げることができました。解析の結果、いずれも幸いなことに事故につながるようなマルウェアではありませんでしたが、仮に今後、深刻なマルウェアが発生した場合でも、外部に依頼することなく、スピーディーに庁舎内で解析できるようになったため、移転前に比べてセキュリティレベルが上がっていると実感できているとのことです。

2015 年の日本年金機構の情報漏洩事故を受け、総務省は各自治体に 2017 年 7 月までに下記 2 点の実施を求めています。

●「自治体情報システム強靭性向上モデル」に基づき、LGWAN(統合行政ネットワーク)接続系とインターネット接続系のネットワーク分離

●市区町村が個々に持っているインターネットの接続口を都道府県レベルに集約し、セキュリティレベルの向上を図る「自治体情報セキュリティクラウド」の実施

豊島区も現在、上記の運用手順の作成にあたっています。

豊島区ではセキュリティ脅威の現状と ICT の進化を合わせて考え、豊島区のセキュリティ対策にはどこが足りないのか、どこを強化すべきか、各製品のすみ分けについても常に考えています。今後は東京都のセキュリティクラウドを利用していくことになるため、都のセキュリティクラウドを利用した場合に、よりセキュリティレベルと効率の上がる FFRI yarai analyzer の利用方法を検討していきたいとのことです。

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

FFRI yarai analyzer

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

関連ページ

豊島区役所様　FFRI yarai analyzer 導入事例

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

【FFRI の独自技術「CODE:F」による多層防御で未知の脅威から防御】



■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。

■豊島区について

都市づくりの基本構想において区の将来像を『未来へ　ひびきあう、人　まち・としま』と掲げ、平和の希求、人権の尊重、住民自治の実現を基本的な理念とし、さまざまな人と共に生き、共に責任を担う協働・協創のまちづくりを推進しています。この将来像を実現するため、豊島区に住み、働き、学び、訪れるすべての人と共に地域づくりを推進していく姿勢として「1.あらゆる主体が参画しながら、まちづくりを実現していく」「2.安心して住み続けられる、心のかよいあうみどりのまちを創造する」「3.魅力と活力にあふれる、にぎわいのあるまちをめざす」「4.伝統・文化と新たな息吹が融合する文化の風薫るまちをめざす」の 4 つの柱を示しています。

■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、「FFRI yarai」はミック経済研究所調べ※1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、ITR 調べ※2による EDR 市場（2015 年度）における売上金額において No.1 を獲得しております。

※1　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 2016【外部攻撃防御型ソリューション編】」

※2　出典：ITR「ITR Market View：情報漏洩対策市場 2016」

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　経営企画部　ＩＲ広報担当
TEL：03-6277-1811
E-Mail：pr@ffri.jp　URL：http://www.ffri.jp

「ＦＦＲＩ」、「FFRI yarai」は、株式会社ＦＦＲＩの登録商標です。

その他すべての社名、製品・サービス名は、各社の商標または登録商標です。

出典資料の引用等、調査会社の著作物を利用する場合は、出典元にお問い合わせください。