

2022.6.24

尼崎市全住民の個人情報入りUSBメモリ、カバンごと発見される

業務終了後にデータが入ったUSBメモリを所持したまま居酒屋へ立ち寄って飲食。その後帰路に向かう途中で眠り込み、翌日22日3時ごろ路上で目が冷めたときには、USBメモリが入ったカバンを紛失していた。同日報告を受けた同市では23日に事態を公表。その後も探索作業が進められていた。

「FFRI yarai」に新版、悪意あるOfficeマクロへの対策を強化

FFRIは、セキュリティ対策ソフトの最新版「FFRI yarai Version 3.5.0」をリリースした。

同製品は、複数の検知エンジンを搭載したマルウェア対策製品。最新版では、マルウェアの感染プロセスにおいてたびたび悪用されている「Office」のマクロ機能を用いた攻撃を防ぐ機能「ディープマクロ分析」を追加した。

同機能は、「Officeファイル」からマクロを抽出し、動作させることなく解析して悪意あるファイルを検出するもので、難読化されたマクロについても、難読化の特徴より検出が行えるとしている。

また、「機械学習エンジン」における検出方式を刷新。従来は実行しているプログラムの動作からマルウェアの判別を行っていたが、プログラムを動作させる前にサンドボックス上で仮想的に動作させる方法へ変更。マルウェアが活動する前に検出できるようになった。

さらにマルウェアの活動内容や解析情報をグラフィカルに表示できる機能を追加したほか、ログを外部送信する「Syslog送信機能」の強化なども行っている。

引用文献：<https://www.security-next.com/>



当社で取扱いございます。Emotet対策にお勧めです！
■通常のウィルスソフトではEmotetは防げません！
■ご利用状況によっては今お使いのウィルスソフトとほぼ同額で入れ替え可能です。

GOODO情報セキュリティかわら版

第5号

令和4年7月発行
ゴードービジネスマシン株式会社