セキュリティレポート

2023.8

YOU DESERVE THE BEST SECURITY

フィッシングによるインターネットバンキング不正送金被害が急増中!!

警察庁と金融庁は8月8日、

フィッシングによるものとみられるインターネットバンキングに係る不正送金について、注意喚起を発表しました。

増加する被害

両庁では2023年4月に、インターネットバンキングに係る不正送金事犯による

被害急増に関する注意喚起を実施するとともに、被害金融機関と連携し対策を

講じていますが、その後も被害は拡大し続け2023年上半期の被害件数は

8月4日時点で過去最多の2,322件、被害額も約30.0億円となりました。

CHECK POINT

被害の原因

両庁によると、被害の多くはフィッシングによるものとみられ、金融機関（銀行）を装ったフィッシングサイトへ誘導するメールやSMSに記載されたリンクからアクセスした偽サイトに、IDやワンタイムパスワード・乱数表等を入力しないよう注意を呼びかけています。

※ 平成24年から令和４年の数値は確定値、令和５年上半期の数値は、同年８月４日時点における暫定値
※ 金融庁より抜粋

CHECK POINT

身近に出来ること

- **心当たりのないSMS等は開かない**。*金融機関が、ＩＤ・パスワード等をSMS等で問い合わせることはありません。
- インターネットバンキングの利用状況を通知する機能を有効にして、不審な取引（例えば、ログイン、パスワード変更、送金等）に注意する。こまめに口座残高、入出金明細を確認し、**身に覚えのない取引を確認した場合は速やかに金融機関に照会**する。
- 金融機関のウェブサイトへのアクセスに際しては、**SMS等に記載されたURLからアクセスせず**、事前に正しいウェブサイトのURLをブックマーク登録しておき、ブックマークからアクセスする。または、金融機関が提供する公式アプリを利用する。

パソコンやスマートフォン・アプリの設定

- 大量のフィッシングメールが届いている場合は、**迷惑メールフィルターの強度を上げて設定**する。
- 金融機関が推奨する**多要素認証等の認証方式を利用**する。
- 金融機関の公式サイトで**ウイルス対策ソフトが無償で提供されている場合は、導入**を検討する。
- パソコンの**セキュリティ対策ソフトを最新版**にする。

CHECK POINT

フィッシング対策にはクラウドセキュリティ Harmony!!

◆ 以前に比べ「怪しいメール」を判断しづらい
◆ メール経由の標的型攻撃やランサムウェア等の攻撃が増えた
◆ パスワード付き添付ファイルの検査ができない

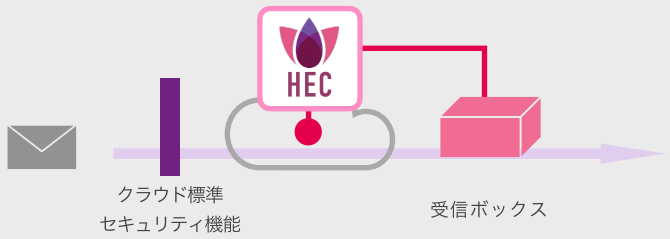
今回の様なフィッシング被害における、メールを経由した攻撃は後を断ちません。
一昔前までは、『怪しいメールを開かない』という声掛けで防いでいましたが、
現在は見分けがつかず巧妙化し、被害も拡大しています。

これらを解決する**『Harmony Email & コラボレーション』**は

◆ 悪質な添付ファイルをブロック
◆ ゼロフィッシング対策
◆ パスワード付きファイルの検査
◆ アノマリー検知

機能を備える、クラウド型アドバンストメールセキュリティとして、
悪意あるメールから企業を守ります!!

Harmony Email & Collaboration



- 攻撃者が迂回できないセキュリティ対策
- クラウド標準セキュリティ機能との併用可
- AI / MLベースのセキュリティ対策
- クラウドサービス内容に組み込まれたAPI型セキュリティ
- 他のAPI型製品では対応できない、受信前のセキュリティ検査が可能

悪質な添付ファイルをブロック

・添付ファイルを無害して提供
・バックグラウンドでファイルをスキャン、悪質な場合はブロックします

ゼロフィッシング

数秒で300以上の指標を分析、フィッシングサイトを判定します

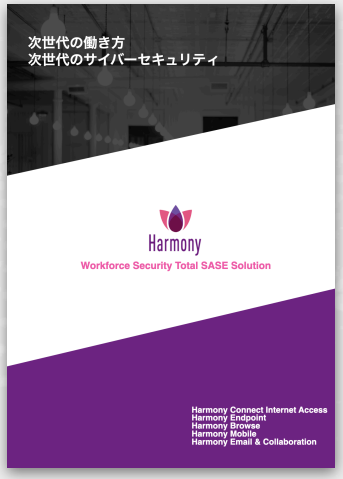
パスワード付きファイル検査機能

今後増加が予想されるパスワード付きZipファイルによる添付マルウェアも検査可能

アノマリー（異常行動）検知機能

普段と違う国からのメールや、不自然なメールの大量送付などによる異常行動を検知します

Harmony
Workforce Security Total SASE Solution



フィッシング対策には

Harmony Mobile
Harmony Browseも

効果を発揮します!!

CHECK POINT

最新マルウェアランキング

国内で活発な上位のマルウェアファミリー

7月はQbotが5月以降3ヶ月連続となる国内・グローバルランキングの首位に立ちました。国内ランキング首位をQbotと分け合ったRemcosはグローバルでも順位を4つ上げ、3位に浮上しています。CPRの調査結果によると、このRemcosの浮上は、脅威アクターが作成した偽のウェブサイトを通じてRAT（リモートアクセス型トロイの木馬）を搭載した悪質なダウンローダーを拡散した結果と見られます。モバイルマルウェアの分野では、モバイルバンキング型トロイの木馬Anubisが順位を上げ、比較的新参のSpinOkから首位を奪い返しました。また、最も攻撃されている業種・業界は引き続き「教育・研究」分野でした。

Qbotの主な特徴

Qbot、別名Qakbotは、2008年に初めて発見されたバンキング型トロイの木馬で、キーストロークの記録、認証情報やブラウザからのクッキー情報の窃取、銀行アカウントアクティビティに対するスパイ、さらに追加的なマルウェアの展開を行うよう設計されています。スパムメールを通じて拡散されることが多く、アンチVM（仮想マシン）、アンチデバッグ、アンチサンドボックスなど複数の手法を用いて解析を妨げ、検知を回避します。2022年以来、最も流行しているトロイの木馬のひとつとして台頭しています。

順位	呼称
1位	**Qbot**
同1位	**Remcos**
2位	**Formbook**
3位	**NanoCore**

CHECK POINT