報道関係者各位

不審と報告されるメールの 3 分の 1 が実際にフィッシングメール、エフセキュアが調査結果を発表

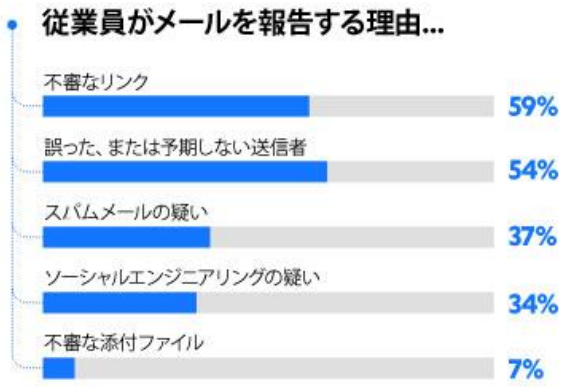
～分析を担当するセキュリティチームの燃え尽き症候群を防ぐには、トリアージの自動化が必要～

2021 年 9 月 9 日
エフセキュア株式会社

先進的サイバー・セキュリティ・テクノロジーのプロバイダである F-Secure (本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、エフセキュア) が実施したフィッシングメールに関する調査によると、企業の従業員がフィッシングの疑いがあるとセキュリティ部門に分析依頼をした電子メールのうち、33%は実際に悪意のあるもの、または非常に疑わしいものであることがわかりました。この調査結果は、2021 年上半期に世界中の企業の従業員から報告されたメール 20 万通を分析したもので、サイバー攻撃を防ぐために報告を挙げるという従業員主導の取り組みの有効性を表しています。

2021 年上半期、エフセキュアの Microsoft Office 365 向け不審メール報告用プラグインを使用している企業の従業員のうち約 3 分の 1 から、合計 20 万通以上のメールが分析対象として報告されました。同期間中、それらのアクティブユーザーは 1 人平均 2.14 通のメールを提出しました。

分析結果 *1 によると、ユーザーがメールを報告する理由として最も多かったのは「不審なリンクが含まれている」であり、59%のユーザーが理由に挙げています。それに続くのが「誤った／予期しない送信者からのものである」の 54%、「スパムの疑いがあると」が 37%でした。更に、34%のユーザーが「ソーシャルエンジニアリングの可能性がある」、7%が「不審な添付ファイル」を報告の理由としています。

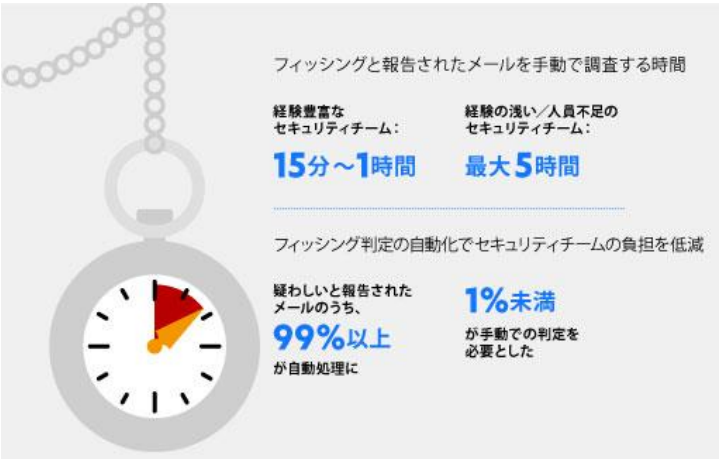


報告されたメールの 99%が自動分析され、そのうち 33%が実際にフィッシングメールであると判定されました。残りの 1%についてはセキュリティ専門家が手作業で分析し、そのうち 63%がフィッシングメールとの判定を受けました。

エフセキュアでコンサルティングディレクターを務める Riaan Naude (リアン・ナウデ) は、不審なメールの報告について、以下のように述べています。
「セキュリティの弱点は人であるという話をよく耳にします。これは非常に皮肉なことで、従業員が企業のセキュリティ防衛の最前線に立っていることの利点を考慮していません。従業員は受信ボックスに入ってくるかなりの数の脅威をキャッチすることができており、不審メールの報告プロセスの簡易化によって、フィッシング対策において目覚ましい成果をもたらすのです。」

電子メールは、サイバー犯罪者がマルウェアを拡散するために使用する最も一般的な手法であり、2020 年には感染ルートの半数以上を占めています [*2]。不審なメールを積極的に報告することは、こうした問題への有効な対応である一方、マイナス面も持っています。Naude は、セキュリティチームのスキルやケースの複雑さに応じて、フィッシング分析には 15 分から 1 時間程度必要だと考えています。

リサーチ会社である Ponemon Institute が 2019 年に実施した調査 [*3] では、調査対象となった企業の 73%において、セキュリティオペレーションセンター (SOC) スタッフが、作業量の増加による燃え尽き症候群により苦痛を感じていると回答しています。それを考慮すると、企業はセキュリティチームが仕事量を適切に管理するためのツールを導入する必要があります。この調査の回答者の 67%が、SOC チームの苦痛を軽減するための最も重要な施策として、ワークフローの自動化を挙げています。



「手作業によるトリアージはセキュリティチームにとって明らかに大きな負担であり、従業員によって不審なメールが報告されると、そのメールが実際に脅威であるかどうかに関わらず、このトリアージプロセスが開始されます。これは明らかに、セキュリティチームの専門家が自分たちが持つ知識やスキルを向上させるうえで、テクノロジーのサポートが必要となる分野の 1 つです。」と Naude は語っています。

フィッシングやその他のセキュリティ上の課題への対応を支援するエフセキュアのソリューションの詳細については、以下のページをご覧ください。
https://www.f-secure.com/jp-ja/business

*1: https://www.f-secure.com/content/dam/press/ja/media-library/reports/202109_Automated_Phishing_Triage_JP.pdf
(調査レポートのインフォグラフィックスをダウンロードいただけます)
*2: https://blog-assets.f-secure.com/wp-content/uploads/2021/03/30120359/attack-landscape-update-h1-2021.pdf
*3: https://www.devo.com/wp-content/uploads/2019/07/2019-Devo-Ponemon-Study-Final.pdf

エフセキュアプレスページ:
https://www.f-secure.com/jp-ja/press

エフセキュアについて

エフセキュアほど現実世界のサイバー脅威についての知見を持つ企業は市場に存在しません。数百名にのぼる業界で最も優れたセキュリティコンサルタント、何百万台ものデバイスに搭載された数多くの受賞歴を誇るソフトウェア、進化し続ける革新的なセキュリティ対策に関する AI テクノロジー、そして「検知と対応」。これらの橋渡しをするのがエフセキュアです。当社は、大手銀行機関、航空会社、そして世界中の多くのエンタープライズから、「世界で最も強力な脅威に打ち勝つ」という私たちのコミットメントに対する信頼を勝ち取っています。グローバルなトップクラスのチャネルパートナー、200 社以上のサービスプロバイダーにより構成されるネットワークと共にエンタープライズクラスのサイバーセキュリティを提供すること、それがエフセキュアの使命です。
エフセキュアは本社をフィンランド・ヘルシンキに、日本法人であるエフセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。詳細は https://www.f-secure.com/en/welcome (英語) および https://www.f-secure.com/ja_JP/ (日本語) をご覧ください。また、Twitter @FSECUREBLOG でも情報の配信をおこなっています。