なりすましメールの被害に遭ったトップ企業リスト（2017年上半期）を公開

ゼロデイ脆弱性の減少に伴い、エクスプロイトキットに代わりEメールを媒介する攻撃が再浮上
クラウド活用でのファイル交換、クライアントの推奨設定など、IT管理者へのヒントを提供

エクスプロイトキットの減少に伴い、マルウェア、不正行為、詐欺を拡散させるための攻撃の媒介手段として、迷惑メールが再浮上しています。そして、迷惑メール送信者が受信者をだますために使用するトリックの1つが、実在する企業になりすます方法です。エフセキュア本社（フィンランド）のエフセキュア研究所であるF-Secure Labsは、2017年上半期に迷惑メールにより偽装されたトップ企業のリストを公開しました。
このリストには、Apple、Amazon、Microsoftのような巨大企業が含まれており、組織が大きくなればなるほど、ブランド名を迷惑メールのおとりとして使う攻撃者にとって、より魅力的になるのです。
エフセキュアのセキュリティ研究所においてセキュリティ・アドバイザーを務めるSean Sullivan（ショーン・サリバン）は、「これらの企業は、さまざまな関係者が非常に多いため、迷惑メールのこれらの企業へのなりすましが最も成功しているのです」と述べています。

大手IT企業以外でなりすまされた企業は、オンラインデート（Match.com）や金融（PayPal）などの特定の業種に分類されます。USPSやFedExのような配送サービスも、このリストの上位ですが、この業種では荷物の配送通知がおとりとして使用されています。ドイツでは、GiropayとEbayが、なりすましによく使われているブランドであり、北欧では、Nordea Bank、Ikeaが頻繁に悪用されています。

「迷惑メールに関して言えば、ソーシャルエンジニアリングの悪用がこれまで以上に簡単になっています。昨今は、電子商取引が極めて一般的なので、単純に“ご注文は配信できませんでした”と表示するだけでよいのです。膨大な数の迷惑メール受信者は、実際に注文して配信されるのを待っているということが保証されているのです。これでは、セキュリティ意識向上の訓練を重ねるより、セレンディピティ（偶然に発見する能力）を鍛える方が早いかもしれません。」とショーン・サリバンは述べています。

なりすましの電子メールは、添付ファイルとしてマルウェアを送り込んだり、バンキング型トロイの木馬やキーロガーなどの他の種類のランサムウェアを送り込んだりする可能性があります。それらのメールには、正規の製品を販売するかのごとく記載されているかもしれませんが、実際にはクレジットカードの詳細情報やその他の個人情報を収集することを目論んでいます。アカウントの認証情報を盗むように作成されたフィッシングメールの可能性もあります。

エクスプロイトキットは、侵害されたWebサイトや、悪意のあるWebサイトに潜んで、訪問者のブラウザやシステムに存在する脆弱性を悪用するマルウェア感染のベクタとして利用され、市場で猛威を振るってきました。ソフトウェアの脆弱性がより迅速に修正され、ゼロデイ脆弱性が従来よりも少なくなっているため、エクスプロイトキット使用の減少が見られます。犯罪者が市場原

理に適応するにつれて、悪意のあるEメールの量が増えています。

◆ 迷惑メールによる感染を防ぐヒント

迷惑メールは攻撃の媒介手段として減速していないことから、ショーン・サリバンは、IT管理者に向けて迷惑メールによる感染を防ぐために次のヒントを提供しています。

・ ユーザは、本当にzipファイルを受信できる必要がありますか?
クラウドサービスを使うことで、ユーザは大量の文書に安全にリンクすることができます。ゲートウェイでzipファイルをブロックするか、グループポリシーを使用して、安全でないファイルタイプに設定することを検討してください。
・ ユーザのマシン上で何かを実際に実行するものからjscriptを分離してください。
・ 電子メールで受信したOfficeファイルからマクロスクリプトを無効にしてください。

◆ 2017年上半期 迷惑メールで偽装されたトップ企業リスト

1. USPS
2. Amazon
3. FedEx
4. Apple
5. PayPal
6. Walgreens
7. Microsoft
8. Eharmony
9. Lyft
10. Facebook
11. Bank of America
12. Match.com

※エフセキュア研究所が公開している「Threat Intelligence」でさらに詳細な情報をご覧いただけます
「Don’t be fooled: these companies are the most-spoofed in spam」
https://business.f-secure.com/top-companies-spoofed-in-spam

■エフセキュアについて

https://www.f-secure.com/ja_JP/
エフセキュアは、無作為攻撃型ランサムウェア感染から高度なサイバー攻撃まで、あらゆる脅威から企業や個人ユーザーを守る、数十年に及ぶ経験を持つサイバーセキュリティのリーディングカンパニーです。その包括的な一連のサービスと数多くの受賞歴を誇る製品は、セキュリティを革新する特許技術と、洗練された脅威対策の知見を駆使して、数多くの企業や人々を保護します。エフセキュアは、他のどの企業をも凌ぐ多数のセキュリティエキスパートを擁しており、ヨーロッパのサイバー犯罪現場の調査にも参加しています。エフセキュアの製品は、200以上のオペレータや数千社のパートナーによって世界中で販売されています。

エフセキュアは、1988年に創業し、NASDAQ OMX Helsinki Ltd.に上場しています。日本法人であるエフセキュア株式会社は、エフセキュア社100%出資の現地法人として1999年に設立され、以降、増収を続けながら順調に企業規模を拡大しています。

Generated by ぷれりりプレスリリース
https://www.prerele.com