Press Release

ノートン 広報部
2023 年 3 月 6 日

PDF を介した新たなマルウェア攻撃を発見

信頼できるファイル形式の PDF がサイバー犯罪者にとっては魅力的な媒体
PC・スマートフォンの両方で被害にあうリスクあり

消費者向けサイバーセーフティブランド「ノートン™」は、サイバー犯罪者が様々なシステムやネットワークを侵害する高度なマルウェア攻撃が急増していることを報告します。特に懸念される手段としては、ドキュメントの共有とコラボレーションに広く使用されている形式である PDF ファイルを介したマルウェアの脅威が拡大しています。

PDF ファイルを用いた手法が注目されている要因

ノートンと同じ Gen 傘下である Avast が公開した 2023 年第 4 四半期脅威レポート※1 でも、この PDF ファイル形式を活用したマルウェアの脅威について報告しています。

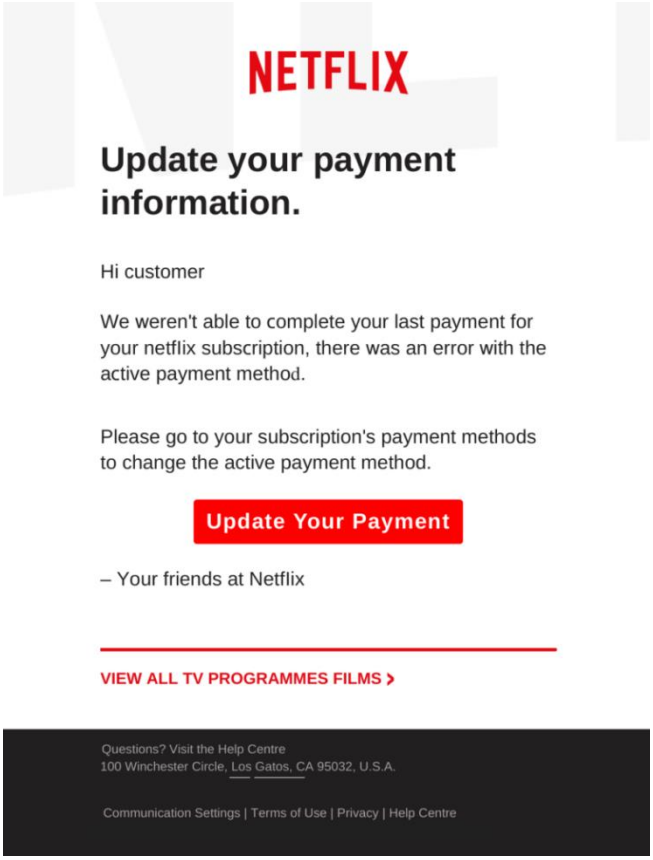
PDF ファイルはプラットフォームに依存せず、さまざまなデバイスでも一貫した形式であるためドキュメントを共有するための媒体として多くの人に使用されています。しかし、この特徴によりマルウェアを配信しようとするサイバー犯罪者にとっては魅力的な手法となっています。さらに、PDF の添付ファイルはスパムゲートウェイによってデフォルトで信頼度が高く許可されることが多いため、被害にあう危険性が非常に高いです。また、PDF ファイルは PC とモバイルの両デバイスでも開くことができることも、サイバー犯罪者にとっては魅力的な手法となっています。さらに、ウイルス対策のスキャンを掻い潜るために、偽 URL を使用し始めており、 リンク短縮サービスなどのサービスを通じて URL 偽装も行われています。

※1：アバスト 2023 年第 4 四半期脅威レポート（https://decoded.avast.io/threatresearch/avast-q4-2023-threat-report/）

PDF と親和性が高く、最近使用されているマルウェア攻撃のパターンと手法

マルウェア攻撃には様々な種類があります。1 つ の例として、Amazon や金融機関などの有名な企業を装い、「アカウントがブロックされた」、「24 時間以内に情報の更新を行わないと、アカウントに永久にアクセスできなくなります。」といったユーザーを急かすような文言のメッセージが送られます。以下は Netflix を装った一例です。支払いにおける問題を説明し、金融情報等の個人情報の詳細を

更新するように求めています。リンクをクリックすると、金融情報の入力画面が表示され、その情報が



犯罪者に盗まれてしまいます。

また、ほかにも有名な手法として、宝くじなどの当選を装う懸賞の詐欺があります。この手法では賞品が当たり、受け取るために個人情報の送信を求められます。この情報を送信してしまうと、送金手数料として前払いのお金を要求されるケースもあります。

上記で紹介したのはマルウェア攻撃の一例ですが、どれも PDF との親和性が高いため使用されており、ほかにも出会い系詐欺などの単純なものや、フィッシング詐欺まで、様々な脅威で PDF の使用が確認されました。Avast の報告では 1,000 万以上の PDF ベースの攻撃をブロックし、世界中で 400 万以上のユーザーを保護していると発表しました。

PDF を用いたマルウェア攻撃から見るサイバー犯罪の変化

PDF ベースのサイバー脅威の急増から、サイバー犯罪者の戦術の大きな変化が見られます。単純な詐欺から複雑なマルウェア配信までの手法の幅が広くなったことから、サイバー犯罪者のデジタル媒体への適応力の高さだけでなく、この PDF を用いた手法はサイバー犯罪者にとって重要となってきていることがわかります。また、この傾向からはサイバー犯罪者が革新的な手法を反映しているだけでなく、ユーザーの日常的な行動に内在する脆弱性も明らかとなりました。

Avast がこれらの攻撃を阻止することに成功したことから、強固なサイバーセキュリティ対策が非常に効果的であることが分かりました。しかし、この対策には私たちの技術的な防止策だけでなく、ユーザーの意識も重要となってきます。ユーザーは見覚えのない話や通知に対して疑いをもつことや、フィッシングや詐欺の傾向を知ることで新しい脅威に警戒し、疑うことを意識してください。

ノートン製品情報

■パソコン、スマホをオールインワンで守るセキュリティソフト

ノートン™ 360：https://jp.norton.com/360

ノートン 360 デラックスは、パソコン、スマホ、タブレットなどのデバイスと Wi-Fi 通信等をオールインワンで守るセキュリティソフトです。詐欺サイトやウイルスなどサイバー攻撃の脅威を検知し、防御する他、インターネット利用時に通信内容を盗み見されないように暗号化する VPN 機能を搭載。その他、お子様を守るための保護者機能、個人情報流出を検知するダークウェブモニタリング機能、パスワードを安全に管理するパスワードマネージャー機能など、消費者の皆様が、より快適かつ安全にインターネットを利用できるようになる機能を多数搭載しています。

*ノートン 360 スタンダード版には、保護者機能とダークウェブモニタリング機能は搭載していません。

■個人情報の流出を検知し、メールとアプリで通知、被害時に 365 日電話でサポート！

ノートン™ ID アドバイザー：https://jp.norton.com/products/identity-advisor

ノートン™ 公式ストア：https://jp.norton.com/

流出した個人情報は、ダークウェブ等で売買され、不正利用される可能性があります。ノートンはインターネットをパトロールし、お客様の個人情報が流出した場合、メールとアプリでお知らせします。また、SNS アカウントの乗っ取り、フィード内の危険なリンクや不適切コンテンツを警告します。個人情報の不正利用被害にあった場合は、365 日復旧支援スペシャリスト(日本拠点）がトラブル解決をサポートします。関連機関と三者通話を行い、サポートさせていただく場合もございます。

*対象 SNS 等、機能の詳細は HP をご確認ください。

ノートンについて

ノートンは、サイバーセーフティのブランドである、Norton、Avast、LifeLock、Avira、AVG、ReputationDefender、CCleaner を通じて、デジタル化が進んだ世界においてもサイバー犯罪などの危険を心配せず、自由にデジタルを使いこなせる環境、「デジタルフリーダム」の実現に力を注ぐグローバル企業「ジェン (NASDAQ：GEN)」の主要サイバーセーフティブランドです。人々が安全に、プライバシーが保たれ、自信を持ってデジタルライフを送ることができるよう、これからの時代もサポートしてまいります。ジェンは、サイバーセキュリティ(インターネット利用の保護)、プライバシー保護、個人情報対策の分野で受賞歴のある製品とサービスを、150 カ国以上の 5 億人以上のユーザーに提供しています。詳しくは、Norton.com と GenDigital.com をご覧ください。