PwC's Cyber Intelligence

日本企業のビジネス環境を織り込んだサイバー攻撃
古典的テクニックでありながらもすり抜けてしまうのはなぜか

サイバー攻撃では情報量や対象範囲の広さの差から攻撃者が有利な状況であり、CISO（Chief Information Security Officer）などのセキュリティ担当責任者は、より積極的なサイバー攻撃への防御戦略を策定しなければなりません。PwC's Cyber Intelligenceでは、今後のリスク要因の特定を支援するため、スレットインテリジェンスとその背景にある攻撃者の動向を解説します。

狙われ続ける人間の脆弱性

この10年ほど、マルウェアを用いた情報漏えいやランサムウェアによる被害の多くは、メール添付ファイルの閲覧や不審なWebサイトへのアクセスなど、ユーザーによる受動的なアクションが攻撃の起点となっています。

特にマルウェア感染の9割が、一般企業が業務で利用するメールに起因するという統計が複数確認されています。※1 日々、セキュリティ技術が進歩し、その導入も進んでいる中であっても、このトレンドは継続していくことが予想されます。個々のセキュリティ対策製品の性能が向上しても、それらを組み合わせて有効なセキュリティ対策にすること、また、その対策を有効に活用できることは別の問題だからです。

信頼と関心で「ユーザー自身を操作」する攻撃者

2020年6月、北朝鮮が関与していると言われる攻撃者グループであるLazarus Groupが、新型コロナウイルス感染症（COVID-19）に便乗した大規模なフィッシングメール攻撃を、日本を含む6か国に対して計画していたことが報告されました。※2 こうした時勢に応じた攻撃は、過去に東日本大震災などでも確認されています。

昨今では、こうした出所が不確かなメールはスパムフィルタに弾かれてしまうことが多く、高度なセキュリティ対策を実施している企業や組織では、メールによる添付ファイルの受信さえ制限しています。しかし、そのような環境でも、比較的容易に攻撃を成功させることができる余地は残ります。ちなみに、送信ドメイン認証の仕組みであるSPF／DKIM／DMARCといった技術の導入は、DNS（Domain Name System）設定による不具合への不安などから、JPドメイン名における送信ドメイン認証技術の設定率は低いものとなっています。※3

このような不特定多数に配信されるスパムとは異なり、攻撃者が特定のユーザー（担当者）に添付ファイルを開かせるために必要なことは、まず、本文を読んでもらうことです。一般的な企業・組織の採用・顧客対応といった部門では、送信元が不特定であっても業務上、メールを読むことは避けられません。そのため、攻撃者がこうした窓口の担当者にマルウェアを送り込もうとすることは、必定と言えます。

当然、担当者も攻撃を疑う可能性があります。攻撃者はそうした場合に備えて、事前にSNSなどを交流サイトを通じて、実在する人物になりすまして担当者の信頼を得ようとします。また、メールのやり取りでも、ソーシャル・エンジニアリングの手法が発揮されます。1通目のメールでは、編集ができない形式のファイルを意図的に文字化けした状態で送り、「文字化けして見えない」という返信を担当者から引き出した後、「文字化けしない方法が分からないため元のドキュメントファイルを送ります。パスワードは別送します」といった日本の組織特有の暗号化ZIP添付メールの慣習（後述）のように、マルウェアを添付したメールを送信し、添付ファイルを開くように誘導します。こうした攻撃は、主にAPT（Advanced Persistent Threat）の初期フェーズで行われており、目にする機会は限られています。

pwc

別の事例として、メールに添付されたドキュメントに、図1のようなメッセージが1行だけ記載されているといったものも紹介します。

図1：ドキュメントに記載されたメッセージ

This document was created using cyber version, please click options in the security warning above and Enable Content to view.

ドキュメントの本文には“This Document was created using older version, please click options in the security warning above and Enable Content to view”という記載がされており、閲覧ソフトウェアの設定を変更してドキュメントのマクロ機能の有効化を誘うものとなっています。このようなマクロを有効にしないと閲覧できないドキュメントを作成して送ることは、通常だと考え難い行為でしょう。しかし、「見ることができない」と思うと、つい見たくなる心理が働かないとは言い切れません。

また、こうした添付メールの暗号化対策として、企業や組織がドキュメントを自己解凍アーカイブに埋め込み、送信するといった対策製品を導入しているケースもあります。こうした環境では、標的となる担当者の関心とは無関係に、添付ファイルを閲覧するために操作が必要と認知され、上記のような設定変更の誘導に対して心理的抵抗が低くなる可能性があります。

さらに、攻撃者は攻撃対象となる国の商習慣にも敏感です。日本では特に、添付ファイルをメールで送る際はパスワード付き圧縮ファイルとして送り、その後パスワードを別送する、という商習慣があります。これは、プライバシーマーク制度の導入に伴い、認証取得の審査項目として、個人情報を含む添付ファイルをメール送信する際の対策が求められるようになったことが要因として考えられます。

このパスワード付き圧縮ファイルを作成するためには、パスワード付き圧縮ファイルを生成できるソフトウェアが必要です。しかし、このパスワードを用いた暗号化機能がオペレーティングシステムの標準機能でサポートされていない場合、日本語に対応したフリーソフトウェアのサードパーティ製ファイルアーカイバを利用するケースが多く見受けられます。攻撃者は、このファイルアーカイバの脆弱性や、サポートするアーカイブ形式が増えることを利用する、といったことも行います。

他にも、APT攻撃と言われている、標的を定めた無差別でない攻撃で利用されている、RTF（Rich Text Format）フォーマットに多数のオブジェクトを埋め込むことができる仕様を用いた攻撃手法があります。 ※4 これらの攻撃では、主にオフィススイートのコンポーネントを狙います。オペレーティングシステムが最新であっても、既存業務やシステムとの相互運用性を考慮し、業務端末に1世代または2世代古いオフィススイートがインストールされている・利用されている場合に、こうした攻撃の影響を受ける可能性があります。この脆弱性を悪用して起こる数式エディタへの攻撃は、90%以上が日本に集中しているとの報告もあります。例えば、COM（Common Object Model）コンポーネントとして独立したプロセスで実行されるため、アンチウィルスソフトウェアなどのエンドポイント対策製品による監視から漏れることがあり、攻撃者に好んで利用されています。

図2：オフィススイートの脆弱性の例

オフィススイートで利用するソフトウェアコンポーネントの処理に存在する脆弱性
ワードプロセッシングソフトウェアに対するリモートからコード実行の脆弱性
外部URLから取得したリソースの処理に起因する脆弱性
数式エディタに関する脆弱性
数式エディタの脆弱性に対する修正漏れ

※1 F-Secure BLOG, 2018年11月12日, 'Failed delivery spam and other naughty things to watch out for this holiday season'
※2 COINPOST,「北朝鮮ハッカー集団ラザルス、コロナ給付金を装ったフィッシング詐欺を計画」
※3 IIJ Engineers Blog,「世界と日本のメール送信ドメイン認証」
※4 Virus Bulletin, 'Attribution is in the object: using RTF object dimensions to track APT phishing weaponizers' [Michael, VB2019]
※5 Cisco Japan Blog,「テンプレート インジェクションを利用した重要インフラへの攻撃」
※6 LAC,「攻撃者グループmenuPassとマルウェア『Poison Ivy、PlugX、ChChes』の関連性」[JPCERT/CC, 2017]

他にも昨今、ドキュメントのテンプレートをネットワーク上から取得し、テンプレート内に同梱されているマクロを悪用した攻撃が確認されています。※5 攻撃者は、まずネットワーク上に攻撃用のマクロを含んだ文書テンプレートを事前に設置します。次に、当該ドキュメントテンプレートへの参照を含んだ、特別に細工した攻撃用ドキュメントを作成し、標的に添付ファイルとしてメールで送信します。本文などによりだまされた特定のユーザー（担当者）が当該ドキュメントファイルを開くと、オフィススイートの仕様により、自動的に参照先であるドキュメントテンプレートが取得され、同梱されたマクロが実行されます。この攻撃では、標的がメールで受信した攻撃用ドキュメントファイル自体にはマクロが含まれておらず、従来のアンチウィルスソフトウェアなどで当該ドキュメントファイルを検査するだけではマルウェアとして検知できない恐れがあります。

セキュリティ製品にとって苦手なファイル形式

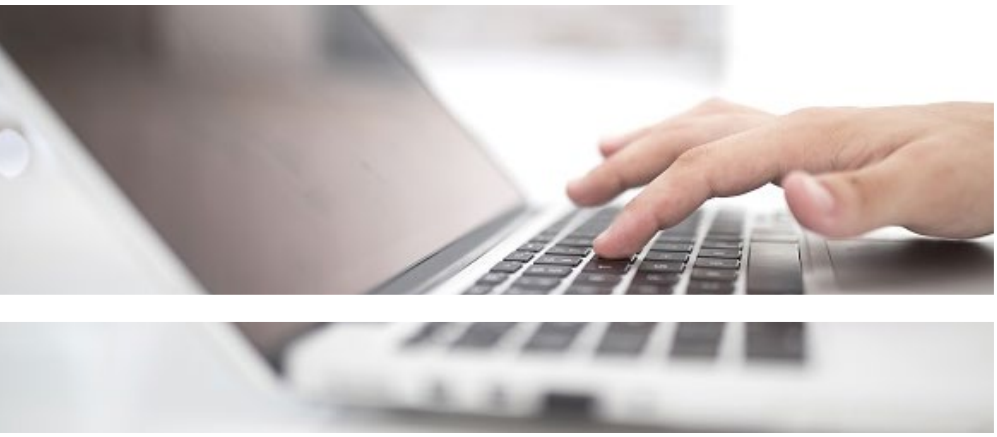
ここまで攻撃側の巧妙な手口を解説してきましたが、防御側の技術も日々、進化しています。最新のオペレーティングシステムでは、サードパーティのアンチウィルスソフトウェアを支援するための機能が提供されており、ドキュメントに同梱されたマクロを実行する直前に検査するといった機能も提供されています。アンチウィルスソフトウェアも、従来のようなウイルス定義ファイルに依存したパターンマッチングに留まらず、機械学習やディープラーニング（深層学習）といった技術の実用化が進んでいます。また、メールの添付ファイルをメールサーバー上あるいはネットワーク上に設置したサンドボックス製品で検査するといった対策ソリューションも隆盛を極めています。

しかし、古今東西、攻撃側が優位であるという原則を覆すには至っていません。例えば、2016年ごろから、ショートカットリンク（.lnk）を用いて、ユーザーにマルウェア起動を促す攻撃が盛んに行われています。※6

ショートカットリンクの利用は、攻撃者にとって以下の利点があります。

- 標的の業務端末にインストールされているアプリケーションのアイコンを使って、アイコンを偽装することができる。
- コマンドラインインターフェイス経由ではなく、オペレーティングシステム標準シェル経由での実行となる。そのため、例えばWebアクセス用の正規コンポーネントへのショートカットにインターネットURLを引数に指定し実行することで、エンドポイント対策製品による検知を回避することが期待される。
- ファイル自体の情報量が少なく、またアンチウィルスソフトウェアなどで検知される可能性が低い。

こうした攻撃は、サンドボックス製品などによる検査が最善策となりますが、パスワード付き圧縮ファイルで暗号化されていた場合、チェックをすり抜ける可能性があります。



セキュリティ投資を無駄なく有効に割り当てるためには

特筆すべきは、攻撃者が、日本で広く利用されているパスワード付き圧縮ファイルでの添付ファイルのやり取りなどの商習慣を把握し、人間心理を巧みに突いて攻撃してきていることです。セキュリティ対策を導入していても、商習慣やビジネスルールによってその機能が十分に活用されていない場合、攻撃者はそうした事情を織り込んで攻撃を行ってきます。そのため企業や組織は、セキュリティ対策製品を導入するだけでなく、その効果を最大化するためのビジネスルールの見直しも併せて実施することが求められます。特に、昨今の急速な在宅勤務（リモートワーク）の導入・普及により、リモートでの業務環境と既存のビジネスルールに不整合が生じている可能性が考えられます。

どのような対策を導入しても、人間による運用は切り離すことができません。操作ログの取得と保存といった、事前にインシデント発生時のトレーサビリティを確保することも重要となります。

執筆者

名和　利男

PwC Japan グループ
サイバーセキュリティ
最高技術顧問

林　和洋

PwCコンサルティング
合同会社
パートナー

岩井　博樹

PwC Japan グループ
スレットインテリジェンス
アドバイザー

村上　純一

PwCコンサルティング
合同会社
ディレクター

PwC Cyber Security & Privacy

https://www.pwc.com/jp/ja/services/digital-trust.html