半径300メートルのIT:

猛威を振るう「Emotet」、いま私たちに何ができるのか

https://www.itmedia.co.jp/enterprise/articles/2009/08/news045.html

活動期と休止期を繰り返すことで知られるマルウェア「Emotet」は現在、日本企業をターゲットに猛攻を仕掛けてきています。2020年夏の活動期には、これまでになかった攻撃のパターンが観測されました。従来の「マクロを仕込んだWordファイル添付」から「パスワード付きzipファイル」に送付手段が変わったのです。日本のビジネスの脆弱性をよく理解した、狡猾な攻撃者がいるようです。

2020年09月08日 07時00分 更新

[宮田健, ITmedia]

日本で「Emotet」が猛威をふるっています。

IPAのツイートによれば、現在のEmotetはメールの添付ファイルやリンク先からダウンロードされるOffice書類の不正なマクロ、不正なPDFファイルなどを使って、感染を拡大している様子。Emotetの活動には周期性があり、JPCERT/CC 分析センターは2020年9月からの大幅な観測数増加を指摘しています。

Emotetは侵入した端末が送受信しているメールの情報を悪用します。あたかも実在する相手からメールが届いたように見えるため不正なファイルを実行しやすくなり、多くの組織で注意喚起が発表されています。つい先日はトレンドマイクロの名前をかたり、アンケートを装った攻撃メールが発見されました。警視庁サイバーセキュリティ対策本部も注意喚起をしています。

併せて読みたい関連記事

- トレンドマイクロのアンケートを偽装した攻撃メールに注意
- JPCERT/CCが注意喚起　マルウェア「Emotet」の新たな手口とは
- セキュリティ的に意味なし　“旧ノーマル”な職場にはびこる習慣、その名も「PPAP」を知っていますか

Emotetがここまで注目される理由

Emotetは活動が活発化するたびに大きな話題になります。組織のシステムを危険にさらし、取引先にも迷惑を掛ける厄介なマルウェアであることに加え、攻撃の手法が日本の組織に特化しているためです。

Emotetは2019年末に観測数が激増した後、年の瀬にかけていったん活動が落ち着いたように見えました。しかし年始の仕事始めと同時にサイバー犯罪者も“仕事始め”を仕掛け、観測数がまた激増したという記録が取れています。週末には減り、週明けに増える――しかも活動の時間帯も日本のビジネスアワーに合わせており、明らかに日本の組織をターゲットにしています。

かつてのEmotetには、明らかに日本語が母国語ではない人の書いた不自然な文章が目立っていました。しかし最近は「請求書の件です」や「ご入金額の通知・ご請求書発行のお願い」「賞与支払届」など、日本のビジネスパーソンならば無視できないような件名のメールが増えています。日本のセキュリティベンダーが「添付ファイルに気を付けよう」と伝えれば「詳細は以下のURLから」とリンクを貼る方法に切り替えるなど、ありとあらゆる面で狡猾です。

そして最近、さらに“進化”したEmotetが発見されました。添付ファイルが不正なマクロを仕込んだWordから「パスワード付きzipファイル」に切り替わったというのです。

マルウェア Emotet の感染拡大および新たな攻撃手法について

もちろんメール本文には、zipファイルを解凍するためのパスワードが記載されています。まさにビジネスシーンでよく見かける「やったつもりセキュリティ」の体裁です。

- セキュリティ的に意味なし　“旧ノーマル”な職場にはびこる習慣、その名も「PPAP」を知っていますか

パスワード付きzipファイルは、攻撃に利用されると非常に悪質なものになります。これまでの「添付ファイル」や「URL」であれば、メールソフトのパターンマッチングやリスト参照といったセキュリティ対策が有効です。しかしパスワード付きzipファ

イルは符号化されているため、メールソフトのセキュリティ機能でスキャンできません。パスワード付きzipファイルの攻撃メールは、これまで投資してきたセキュリティ施策をすり抜けて、あなたの受信箱に届いてしまいます。

ここからは「あなた」の脆弱（ぜいじゃく）性が攻撃されます。例えばテレワーク中に「Web会議のURLが変更されました」や「交通費支給の変更」といった件名のメールを受け取れば、件名だけで不審に思うのは難しいでしょう。私自身もすべてを見抜くことはできないと思います。最終的にはパスワード付きZIPファイルを全てマルウェア扱いするくらいの対策しか、私たちにできることはありません（クラウドファイル共有を使おう！）。

私たちにできることはあるのか

EmotetはCOVID-19同様、私たちに「ニューノーマル」を突きつけるきっかけになるかもしれません。私たちは、このタイミングでセキュリティのニューノーマルを考えるべきでしょう。ずる賢いマルウェアは、Emotetに限らず今後もたくさん発生するでしょう。それに対抗するには、「知の共有」しかありません。

本来あるべきセキュリティとは、**どんな人であっても守られる仕組み**です。セキュリティに強い者だけが生き残り、弱者はだまされても仕方がないような世界には持続性がありません。ただ、そのような世界が実現するのはもう少し先になりそうです。だからこそ、特に企業にいる組織を守る仲間としてのビジネスパーソンは、いま置かれている危機にほんの少し歩み寄って、学ぶ必要があるのではないかと、私は考えています。

幸いあらゆるセキュリティ機関が、Emotetに限らず有用な情報を広く公開しています。エンジニア目線でのEmotet解説は、エンジニアでなくても理解できるよう工夫されていることも多いので、まずはこれらの記事をぜひ、読んでみてください。私たちのPCが、パズルを解くように攻撃されていることがよく分かるかと思います。

今更ながらEmotetについて調べてみた - SSTエンジニアブログ

最恐のマルウェア“Emotet”を徹底解剖。特徴と今必要な対策を解説します。| wizLanScope

D アラート情報｜サイバーリスク情報提供サービス「D アラート」｜企業・官公庁のお客様｜デジタルアーツ株式会社

特に三井物産セキュアディレクションが公開したEmotetの内部構造は実に興味深い内容です。PCの内部構造をご存じの方やセキュリティ技術者がこれを読んだら、いかにその仕組みが考えられているのかが分かるかと思います。

経営層に近い方であれば、Emotetを分かりやすく語る対談をチェックするのもいいでしょう。**「怪しいと思ったらすぐに連絡、でもメールそのものを添付して転送するな」**など、思わず膝を打つ事前対応が紹介されています。

「Emotetに気を付けよう、だまされないようにしよう」という言葉だけでは、実像を捉えられず「文面の怪しいメールに注意する」といった結論に陥りがちです。フィッシング対策同様、マルウェアも真贋の判定を人任せにするのは良い対策とは思えません。重要なのは「まず敵を知り、知を共有すること」ではないかと思います。

まずは組織を守る一員としてのあなたから。そして、あなたが理解したら、ぜひ家族や知人にもこの話をしてあげてください。あなたが組織を守ることから始め、そして家族や地域を守る――。セキュリティに近道はまだなさそうですが、悲観する前にできることだってきっとあるはずです。

著者紹介：宮田健（みやた・たけし）

元@ITの編集者としてセキュリティ分野を担当。現在はフリーライターとして、ITやエンターテインメント情報を追いかけている。自分の生活を変える新しいデジタルガジェットを求め、趣味と仕事を公私混同しつつ日々試行錯誤中。

2019年2月1日に2冊目の本『Q&Aで考えるセキュリティ入門　「木曜日のフルット」と学ぼう！〈漫画キャラで学ぶ大人のビジネス教養シリーズ〉』（エムディエヌコーポレーション）が発売。スマートフォンやPCにある大切なデータや個人情報を、インターネット上の「悪意ある攻撃」などから守るための基本知識をQ&Aのクイズ形式で楽しく学べる。