「疑わしくないメール」にも疑いの目を　猛威を振るうマルウェア「Emotet」に注意

https://www.itmedia.co.jp/news/articles/1912/23/news014.html

複数のセキュリティ企業や組織が11月以降、マルウェア「Emotet」について注意を呼び掛けている。Emotetの流行は、もはや「怪しいメールに注意する」という対策だけでは通用しなくなりつつあることを示している。

2019年12月23日 07時00分 更新

[高橋睦美, ITmedia]

一概には言えませんが、私は「先ほどメールを送ったので、確認をお願いします」と電話がかかってくると、「二度手間にすぎず、メールで連絡が完結するほうがいいじゃないか」と思ってしまうタイプです。インターネットの品質が文字通りベストエフォートで、ゲートウェイ間で遅延が発生する可能性があった時代ならともかく、今どきはほとんどロストや遅延もなくメールが届きます。ですから、わざわざメールを送ったことを別途電話で確認するなんてばかばかしいと思っていました。

けれども今後、セキュリティ上の理由から、メールを送ったことを電話やメッセンジャーなど他の手段で確認するプロセスが必要になるかもしれません。そんな懸念を抱かせるのが、11月以降に複数のセキュリティ企業や組織が注意を呼び掛けているマルウェア「Emotet」や、日本企業でも被害が報じられているビジネスメール詐欺（BEC：Business Email Compromise）の存在です。

これまで、マルウェア感染を防ぐ基本的な対策の1つとして「疑わしいメールの添付ファイルは開かない、リンクはクリックしない」ことが大切だといわれてきました。確かに、見るからにぎこちない日本語で書かれたメール、仕事のメールなのに個人のアドレスから送られてくるメール、あるいは表示とリンク先が異なるURLのように、一呼吸おけば怪しいと判断できるメールならばクリックするべきではありません。

しかしEmotetの流行は、もはや「怪しいメールに注意する」だけでは通用しなくなりつつあることを示しているように思います。実在する知り合いのメールアドレスから届くこれまでのやりとりをなぞったメール、つまり怪しくないメール経由で感染してしまうからです。だからこそ、これほど急速に、雪だるま式に感染が広がっているのでしょう。

JPCERT/CCによると、メールに添付されたWord形式の添付ファイルを開き、「コンテンツの有効化」を実行すると、Emotetに感染した事例が確認されているという（＝画像はJPCERT/CCのWebサイトより）

盗み取ったメールの再利用で感染拡大

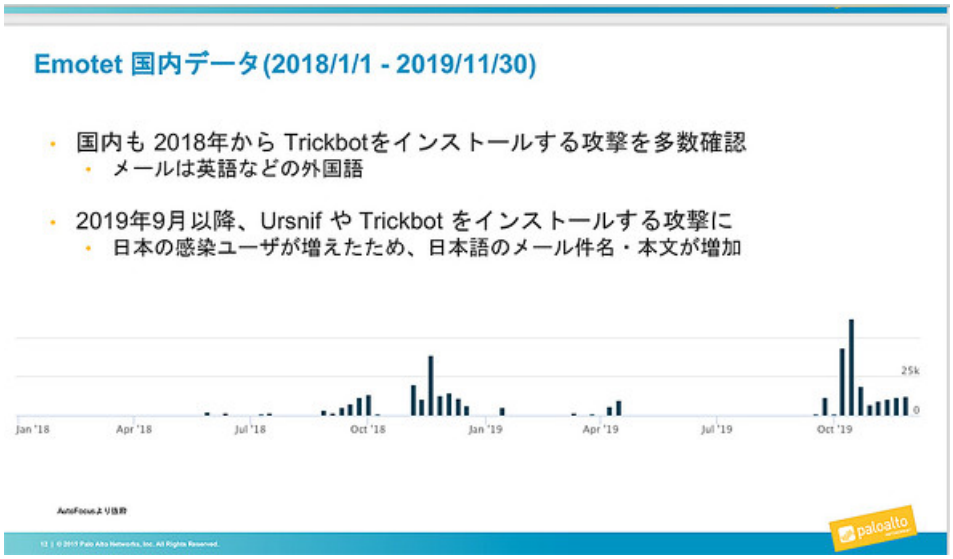
ITmediaでもたびたび報じている通り、Emotetはメール経由で感染するマルウェアです。今、日本国内で主に流行している手法はWord形式の添付ファイルによるものです。添付ファイルを開き、さらに「コンテンツの有効化」を実行してしまうと感染してしまい、端末内のID／パスワードといった認証情報の他、メールアカウントとそのパスワード、メール本文やアドレス帳の情報などを盗み取られてしまいます。

厄介なのはここからです。攻撃者は盗み取ったメールの情報を用い、普段やりとりをしている取引先や顧客にメールを送信して二次被害、三次被害を広げようとします。これは2011年ごろに発生した標的型攻撃でも疑われた手口で、ユーザーが注意を払っても見抜くのはなかなか困難です。

パロアルトネットワークスの林薫氏（日本担当最高セキュリティ責任者）によると、.jpドメインのアドレスを詐称して送られたEmotet付きのメールは、同社が11月に観測しただけで約1万4000通に上ったそうです。名前をかたられた組織は約

300に上り、製造、サービス、飲食など、規模・業種とも多岐にわたっていました。

この中からある製造業の企業について調べてみると、40以上のメールアドレスから630通のメールが送られていたことが判明。林氏は「その大半が個人のアドレスで、Webなどで公開されているものではない。Emotetは盗んだメールアドレスや本文を再利用することで感染率を高めている」と述べ、一種のサプライチェーンリスクだと指摘しました。



Emotetの日本国内での観測データ=パロアルトネットワークス提供

フォーティネット・ジャパンの寺下健一氏（セキュリティストラテジスト）も、「メールのスレッドを盗み出して分析し、未読情報などを基に『より開きやすいメール』を詐称して返信の形で送りつける。それまでの会話が記されているため疑いようがなく、一般的なフィッシングメールよりも成功率が高い」と述べています。

怪しくないメールにも注意を払わざるを得ない状態に

もちろん、受け取ったメールが疑わしくないかどうか「注意する」ことが全く無意味なわけではありません。世の中にはさまざまな攻撃メールが飛び交っており、雑なバラマキ型攻撃メールを見抜くだけでも効果はあります。ですがEmotetのように手の込んだ手法で本物らしく見せるメールが増えてきた今、それ以外の対策はあるのでしょうか。

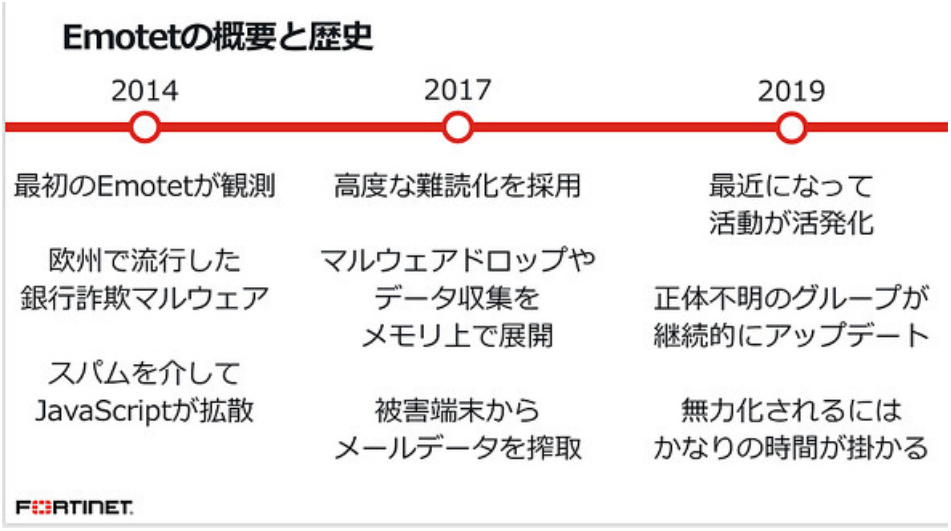
例えば、JPCERTコーディネーションセンターなどがまとめている通り、まずはマクロ自動実行の無効化やパッチの適用、メールセキュリティ製品による水際での検出と監査ログの確認などの対策が推奨されています。

ですが、問題はその対象です。林氏は「怪しくないメールであっても添付ファイルやリンクの取り扱いには注意せざるを得ない」といい、たとえ促されてもマクロを有効化しないよう心掛けることが大事だとしています。同時に資産を棚卸しし、重要なデータやサーバについては最小権限のアクセスに絞るなど、侵入されても影響を最小限にする対策が必要だとしました。寺下氏も「100%侵害を防ぐことはできないという前提の下、緩和策、減災を図ることが必要だ」と述べています。

Emotetに関してはもう1つ注意すべきことがあります。Emotetというマルウェア単体で完結するのではなく、これを介して別のさまざまなマルウェアが送り込まれてくることです。

フォーティネットの調査によると、Emotetは欧州で流行が始まった14年当時に、オンラインバンクを狙うトロイの木馬をばらまくために用いられました。これに対し最近では、Emotetを経由し、TrickBotのように情報を盗み出すマルウェア、あるいはランサムウェアが展開されていることが確認されています。

いわば「任意のマルウェアを拡散するための基盤として、サービスとして提供されている」状態です。寺下氏によるとEmotetはモジュール化されていることもあり、常にアップデートが繰り返されているといいます。このことを踏まえると、やはり侵害を前提にした検知体制、インシデント対応体制の整備が必要だといえそうです。



Emotetの概要と歴史＝フォーティネット提供

BEC対策でプロセス再整備に取り組む企業も

こうした動向を目にすると、疑わしいと思われるメールを受け取ったり、自分から送った時には、別途電話やメッセンジャーなどで「かくかくしかじかのメールを受け取ったけど、開いてもいい？」と確認するプロセスが必要になるかもしれないなと思ってしまいます。

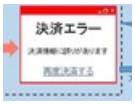
Emotetではありませんが、過去にBECによって甚大な被害を受けたり、ヒヤリハットを経験した企業では、こうした対策……より正確には手順・プロセスの再整備を進めているそうです。

BECもEmotetのように、ある会社にマルウェアなどで侵害し、メールアカウントを乗っ取ることがきっかけになります。攻撃者は乗っ取ったメールアドレスで収集したやりとりを基に、タイミングを見計らって「振込先がこちらの口座に変更になりました」といったメールを送りつけ、数千万、時には億単位の額をだまし取ってしまうのです。

これを防ぐため、フィルタリングや端末でのマルウェア対策に加え、まとまった額の金銭を動かす際にはメールのみで完結しないようにしたり、複数の担当者が確認するなどプロセスを再整備する必要があります。ただ、電話やテレビ会議ならば確実に本人確認ができるかというと……。林氏は、ディープフェイクによって偽装される可能性を指摘しています。

このように19年に起こったさまざまなインシデントを振り返ると、残念ながらこれまで無条件で成り立ってきた「信頼」があちこちで揺らいできていることを感じます。「ゼロトラスト」という言葉が注目され始めている通り、無条件に「信頼」したり「丸投げ」するのではなく、自分が相手を、相手に自分を信頼してもらうために何を確認する必要があるのか、問い直さなければいけない時代になってきたのかもしれません。

関連記事



「見破るのは実質不可能」――ECサイトからカード番号盗む“最新手口”、セキュリティ専門家の徳丸氏が解説
セキュリティ専門家の徳丸浩氏は、「情報漏えい事件が急増した1年だった」と振り返る。情報を盗もうとする攻撃者の最新手口については「自分でも気付けるか分からない」と状況は深刻だ。

「賞与支払い届」装うスパムメールに注意　中身はマルウェア「Emotet」　パスワードなど流出の恐れ
賞与支払い届を装ったスパムメールが出回っているとして、IPAが注意喚起。本文には出金口座の情報と振り込み指定日、不正なファイルのダウンロードに誘導するリンクが記載されている。誤ってクリックするとマルウェア「Emotet」に感染する。

史上最悪規模のDDoS攻撃　「Mirai」まん延、なぜ？
インターネットの普及期から今までPCやITの世界で起こった、あるいは現在進行中のさまざまな事件から得られた教訓を、IoTの世界で生かせないか――そんな対策のヒントを探る連載がスタート。

イープラスに聞く、悪徳転売業者を駆逐するまで　チケット購入アクセスの「9割占めた」botを徹底排除
botを駆使してチケットを買い占める高額転売業者にイープラスがどのように立ち向かったのか。「迷惑bot事件簿」（特別編）では、イープラスの小西雅春氏にインタビューし、当時の戦いを振り返る。