JPCERT/CCが急きょ会見:

「あなたのPCはEmotetに感染しています」と通知されたユーザーがまずやるべきこと

https://www.itmedia.co.jp/enterprise/articles/2102/25/news043.html

国内外で感染を広げた悪名高いマルウェア「Emotet」が欧州の捜査当局によってついにテイクダウンされた。日本で情報提供を受けるJPCERT/CCや警察庁は、国内でEmotetに感染したユーザーに向けた通知を続けている。

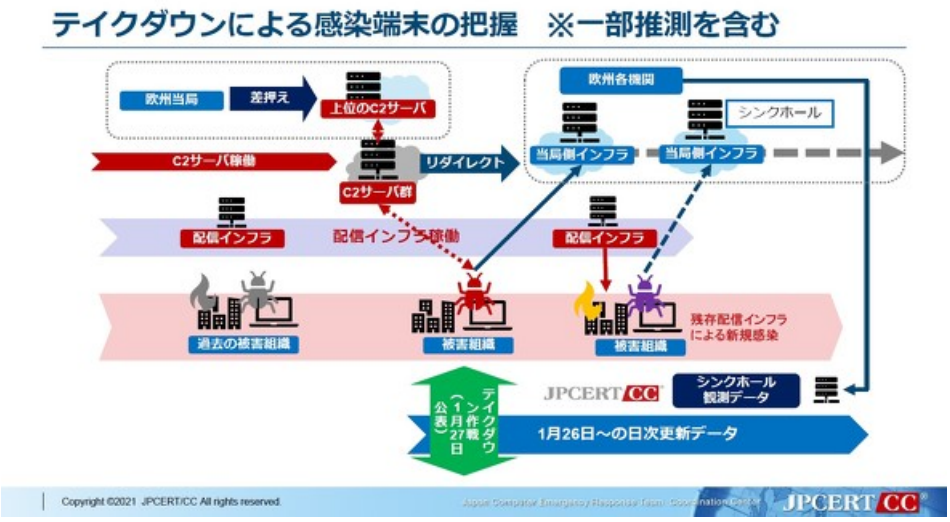
2021年02月25日 07時00分 更新

[高橋睦美, ITmedia]

国内でもたびたび流行し、多くの被害をもたらしたマルウェア「Emotet」に、ひとまずの“終止符”が打たれた。2021年1月27日、欧州刑事警察機構(Europol)と欧州司法機構(Eurojust)が8カ国の法執行機関による合同捜査作戦「Operation LadyBird」(レディバード作戦)を実施し、Emotetをテイクダウンしたのだ。

これまでEmotetをコントロールしていたC2サーバ(注)は差し押さえられ、当局のコントロール下に置かれた他、運用していたメンバーの一部も逮捕された。もともとEmotetがセキュリティ対策ソフトをかいくぐるために持っていたアップデート機能を逆手に取り、無害化された検体に更新することで、これ以上の新規感染を抑えようとしている。

(注)コマンド&コントロール(C&C)サーバとも呼ばれる。サイバー攻撃において、乗っ取ったコンピュータを制御したり命令を出したりする役割を担う。



JPCERT/CCが示した、レディバード作戦がEmotetをテイクダウンした動きの概要(一部推測を含む)(出典:JPCERT/CC)

しかし、これで一件落着というわけではない。JPCERTコーディネーションセンター(JPCERT/CC)は2月23日に急きょ記者説明会を実施し、テイクダウンのあらましと「その後」に留意すべき事柄について説明した。

実在する人物をかたって感染を広げたEmotet

既にご存じの方も多いだろうが、Emotetは、主にメールの添付ファイル経由で感染を広げるマルウェアだ。なりすましメールに添付されたファイルをユーザーが開き、そこで促されるマクロやコンテンツの有効化を実行すると、Emotetに感染してしまう。Emotetは、感染先のPCからメールアドレスや本文、メールやブラウザに保存されたパスワードなどの情報を盗みとって利用することで、さらに感染を広げていく。また、別のマルウェアを引き入れるダウンローダーとしても機能する。

国内でEmotetの被害が目立ち始めたのは2019年10月ごろからだ。2020年2月になると、新型コロナウイルス感染症(COVID-19)の拡大と入れ替わるかのようにいったん終息したが、2020年7月以降再び急増し、あちこちで被害の声が聞かれるようになった。

Emotetの厄介な点は、知り合いや取引先など、実在する人物や組織の名前をかたったなりすましメールで感染を広げる点だ。一見すると自然な日本語で書かれ、中にはターゲットの過去のメールのやりとりに返信するような形で送られてくる場合もあり、見破りにくかった。

巧妙な手口の変遷も特徴的だった。年末には「賞与支払」といった用語をメールのタイトルに使ったかと思えば、COVID-19に関連するメールを装うこともあった。さらには日本企業でよく扱われる「パスワード付きZIP」を手法に取り入れるなど、世の中の情勢やターゲットの特徴に合わせて少しずつ手口を変えながら感染を広めていった。

併せて読みたい関連記事

- Emotetのテイクダウンが発表も「安心」はまだ早い　今求められるセキュリティ対策
- 猛威を振るうEmotet……これは単なる「種まき」だ？　辻伸弘氏の危惧する近未来
- 日本のIoTは、なぜ今でも“危ない”のか　脆弱性チェックと法改正を重ねる総務省の現在地と

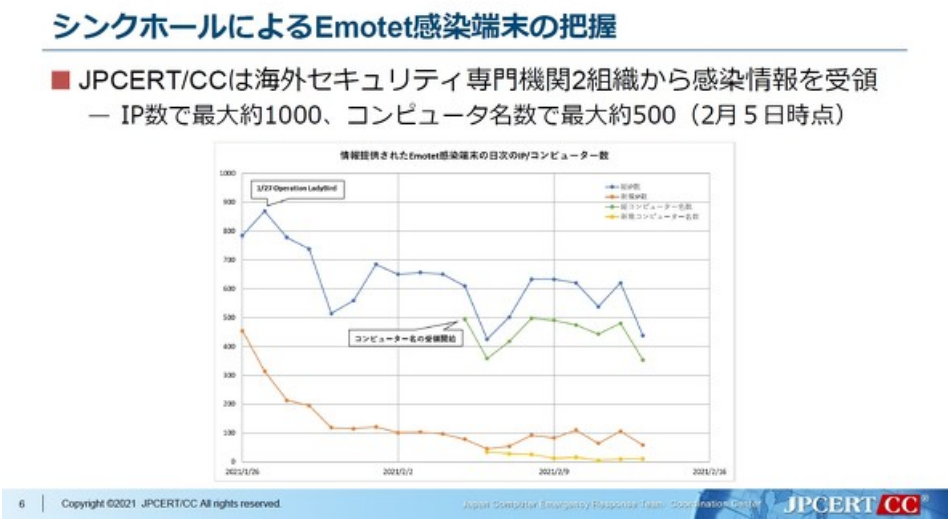
コンピュータ名だけで約500件――国内に残るEmotet感染の現状

こうした特徴も相まって、Emotetは日本のみならず全世界に被害をもたらした。テイクダウンという手段が取られたのも、こうした被害の大きさ故だろう。

JPCERT/CCの佐條 研氏

テイクダウンによって、感染端末からC2サーバに向けた通信は、法執行機関が管理する「シンクホール」に向かうことになった。シンクホール側のログから感染端末のIPアドレス情報などが得られた他、押収されたC2サーバからはEmotetが詐取したメールアドレスやユーザー名、パスワードなどの情報も判明した。その中には当然ながら、日本国内の端末の情報も含まれている。

テイクダウン後、JPCERT/CCは複数の国外組織から国内でEmotetに感染している端末の情報提供を継続的に受け、感染端末の特定や駆除の依頼を続けている。変動はあるが、IPアドレス数で最大約1000、コンピュータ数では約500件確認され、「徐々に数は減っていっている」と、JPCERT/CCの佐條 研氏（インシデントレスポンスグループ　マルウェアアナリスト）は説明した。



JPCERT/CCは、感染通知や駆除などの対応によって数に変動はあるものの、国内で相当数のEmotet感染が観測されたと明かした（出典：JPCERT/CC）

同様に警察庁も、海外の捜査当局から感染端末に関する情報を受け、総務省やICT-ISACと連携しながらISP経由で利用者を特定し、注意喚起を進める。

Emotet自体の駆除だけで終わりではない、本質的な対策は

前述のテイクダウンによって、C2サーバを介した二次攻撃や情報窃取、これ以上の新規感染はないとみられる。また、レディバード作戦で用意されたシンクホール経由で、4月25日12時になると自動的に機能を停止するコードを送り込んであ

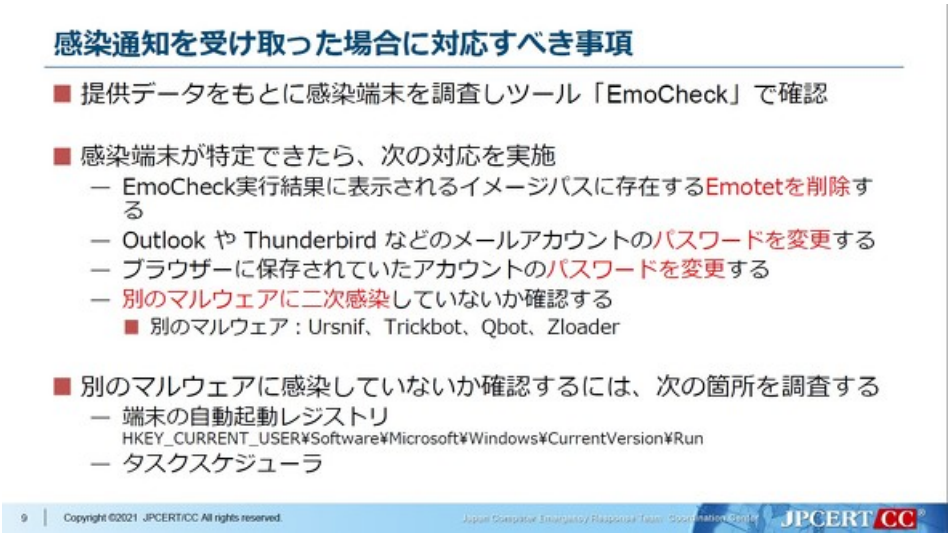
る。そのため、Emotetそのものによる被害は食い止められることになるだろう。しかし、これで終わりではない

問題は、Emotetがすでに盗み取った情報や二次感染したマルウェアへの対応だ。

まず、Emotetのテイクダウン以前に盗まれ、何らかの形で別のサイバー攻撃者の手に渡ってしまったさまざまな情報が悪用される恐れがある。また、Emotetがプラットフォームとなってばらまかれた別のマルウェアに二次感染していた場合、別途ウイルスチェックをして駆除しなければ、別の被害に遭う恐れがある。

佐條氏によると「Ursnif」や「Trickbot」「Qbot」「Zloader」といった、いわゆる「Banking Trojan」と呼ばれるマルウェアへの二次感染例が確認されている。これらに感染した状態でオンラインバンクやECサイトにアクセスすると、銀行を利用した際の認証情報が盗み取られて不正送金されたり、クレジットカード情報が詐取されたりする恐れがある。

もしもJPCERT/CCやISP経由で「Emotetに感染している恐れがある」と連絡を受けた場合には、JPCERT/CCが提供する「EmoCheck」を使ってEmotetそのものの存在を検査するだけでは十分とはいえない。メーラーやブラウザに保存していたパスワードの変更、ウイルス対策ソフトによるチェックやレジストリの確認による二次感染の確認までを実施して初めて、本当の意味での対策が完了したことになる。



JPCERT/CCは、Emotetの感染通知を受け取ったユーザーに、メールアカウントのパスワード変更や別のマルウェアの感染チェックを含めた複数の対処を求めている（出典：JPCERT/CC）

レディバード作戦が1月のテイクダウン時点で即座にEmotetを無効化するのではなく、4月までしばらく猶予期間をおいて停止に持っていく背景も、感染端末を特定し、二次感染マルウェアへの対策も含めた根本的な対処を取るためと理解できるだろう。

マルウェアの駆除に向けて、組織や国境を越えた提携は今後必須か

世界的に広がったマルウェアに対するテイクダウン作戦は、botネットの「Game Over Zeus」に対するものをはじめ、過去たびたび実施されてきた。警察庁の他、JC3、APWGやJPCERT/CCなど国内のさまざまな組織も連携、協力している。また国内独自の取り組みとしても、マルウェア対策を推進する「ACTIVE」の他、脆弱（ぜいじゃく）な状態のIoT機器を特定して注意喚起を図る「NOTICE」といった活動があり、今回のEmotet対策にもそうした過去の蓄積が反映されている。


JPCERT/CCの佐々木 勇人氏

JPCERT/CCの佐々木 勇人氏（早期警戒グループマネージャー）は「今回は欧州当局と米国における官民連携のスキームが活用されたが、それ以外の国も含めた国際的なスキームとなるとまだ構築されていない」と話す。

「長年にわたって構築されてきたCERT間の連携を生かしたり、民間のリサーチャーも含めて協力して官民連携が進むことによって、欧州以外の国も関われる国際的な枠組みが形成されていくことに期待したい」（佐々木氏）

そもそも「メール経由の脅威」は、インターネットが普及し始めたことから常に存在してきた。Emotetが利用してきたさまざまな手口も、洗練度の違いはあるが「使い古されたもの」と捉えられる。逆に言えば、われわれをターゲットにするグローバルな脅威もEmotetが最後ではないだろう。そう遠くはない未来にまた新たな脅威が登場したとき、日本も含めた国際連携により、ターゲットをテイクダウンできることに期待したい。