ZDNet Japan

猛威を振るった Emotet -- その脅威を知る

- マルウェア「Emotet」、感染ホストから一斉削除へ -- 蘭警察がアップデート配信
- 日本でもマルウェア「Emotet」のバラマキ攻撃拡大
- マルウェア「Emotet」の攻撃拡大 -- 新手法も確認
- マルウェア「Emotet」の攻撃急増、米 CISA も警告

猛威を振るった Emotet-- その脅威を知る

マルウェア「Emotet」、感染ホストから一斉削除へ -- 蘭警察がアップデート配信

オランダの警察当局がマルウェアの「Emotet」を削除するアップデートの配信計画を進めていることを、米 ZDNet が現地時間 1 月 27 日に確認した。このアップデートは、Emotet に感染しているすべてのコンピューターからこのマルウェアを削除する動作を、3 月 25 日に開始するという。

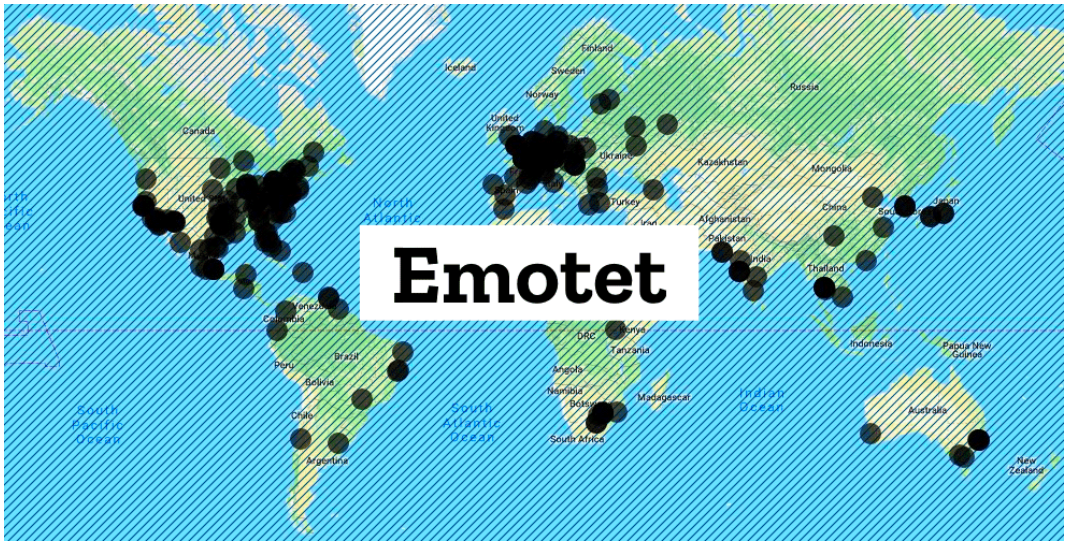
このアップデートの配信が可能になった背景には、8 カ国の警察がこのほど一斉摘発を実施し、現時点で最大のマルウェアボットネットと考えられている Emotet を拡散したサーバーの押収やこのボットネットに関与した人物の逮捕を進めたという事情がある。

サーバーは複数の国に設置されていたが、オランダ当局によれば、Emotet の主要な C&C（コマンドアンドコントロール）サーバー 3 台のうち 2 台がオランダ国内に設置されていたという。

オランダ警察は、この 2 台のサーバーへのアクセス権を用いて、ブービートラップを仕掛けた Emotet のアップデートを、このマルウェアに感染したすべてのホストに配信したと述べた。

これまでの報道によると、このアップデートには時限爆弾のようなコードが埋め込まれており、各マシンの時刻が 2021 年 3 月 25 日正午になった時に、そのコンピューターから Emotet マルウェアをアンインストールするという。

「オランダ警察がプレスリリースで説明した技術的作戦が説明どおりに機能すれば、Emotet は事実上消滅するだろう」と、サイバーセキュリティ企業の Binary Defense でシニアディレクターを務める Randy Pargman 氏は 27 日、米 ZDNet のオンラインチャットでの取材に対して語った。



猛威を振るったEmotet-- その脅威を知る

日本でもマルウェア「Emotet」のバラマキ攻撃拡大

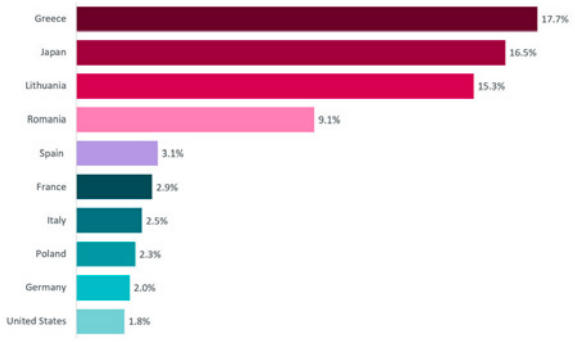
セキュリティ企業のESETは、10月16日にマルウェア「Emotet」の感染を狙った大規模な攻撃が欧州や日本で発生したと伝えた。日本での検出率がわずか数日で6ポイント近く増加したという。

同社によれば、この攻撃ではリトアニア、ギリシャ、ルーマニア、フランス、日本が主な標的となり、同社製品における主な国別の検出ではリトアニアが14.8%、ギリシャ13.8%、日本が10.6%だった。翌17日に攻撃はいったん収束したものの、日本は18～19日に再び急増し、検出率が16.5%に上昇した。

Emotetは、主に実在する企業や人物などになりすまし、「請求」や「添付」などビジネス関連の語句あるいは「新型コロナウイルス感染症」などの時事に関する文言を用いた内容のスパムメールを通じて感染する。感染を狙うメールはリンクや添付ファイルなどがあり、受信者がリンク先からEmotetの感染につながる不正プログラムをダウンロードしてしまったり、添付ファイル（主にはOffice関連ファイル）に埋め込まれた不正なマクロによって不正プログラムをダウンロードしてしまったりすることで、最終的にEmotetに感染する。

Emotet感染後は、感染端末での操作内容や通信内容などが盗聴されたり、接続するネットワークの先に感染範囲を広げたりするほか、正規ユーザーのアカウントを不正使用し、さらなる感染のために上述のなりすましメールを送信したりする。さらに、Emotet経由で「Trickbot」や「Qbot」などの不正なボットプログラムやランサムウェアなどにも感染する恐れがある。Cryptolaemusによると、14日にはスパムメールの文言にWindowsやOfficeのアップデート通知を装う新たな手口も確認された。

また、情報処理推進機構（IPA）が21日に発表した2020年7～9月期の情報セキュリティ安心相談窓口の相談状況によれば、Emotetに関する相談が308件寄せられ、4～6月の1件から急増している。



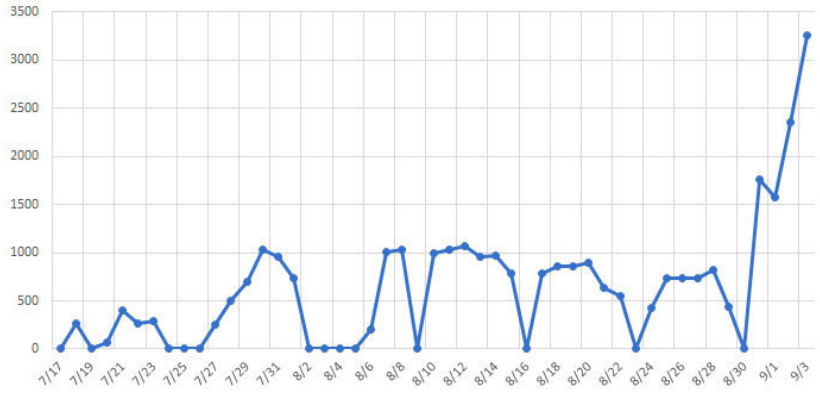
猛威を振るった Emotet-- その脅威を知る

マルウェア「Emotet」の攻撃拡大 -- 新手法も確認

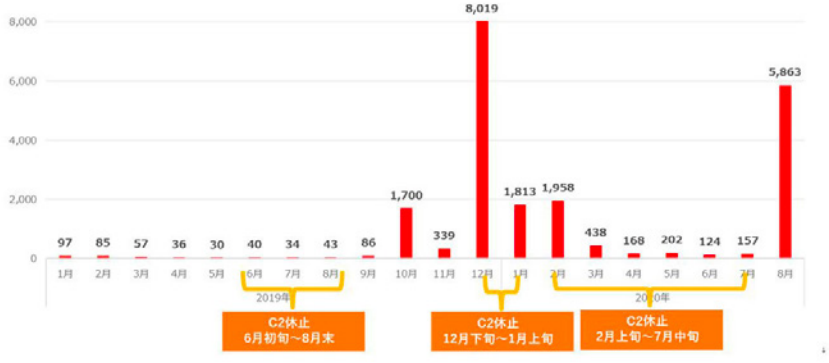
９月に入りマルウェア「Emotet」の感染を狙うサイバー攻撃が拡大しているとして、情報処理推進機構（IPA）や JPCERT コーディネーションセンター（JPCERT/CC）が相次いで注意を呼び掛けた。攻撃手法もさらに多様化しているという。

Emotet の感染攻撃は、2019 年から断続的に続いており、なりすましメールなどを使って相手を巧妙にだます手口が知られる。なりすましの手口に用いる内容も常に変化しており、業務や取引に関する連絡を装ったり、新型コロナウイルス感染症（COVID-19）に便乗したりするものが確認されている。

JPCERT/CC によれば、Emotet に感染してメール送信に悪用される可能性のある「.jp」アドレスが、７月中旬～８月では１日当たり最大 1000 前後だったが、９月１日から急増して３日には 3000 を突破した。IPA によると、Emotet に関連した相談は７～８月は計 34 件だったが、９月は２日午前までに 23 件寄せられているという。



Emotet に感染し、メール送信に悪用される可能性のある「.jp」アドレスの推移（出典：JPCERT/CC、外部からの提供観測情報）



Emotet の検知数と推移（出典：トレンドマイクロ）

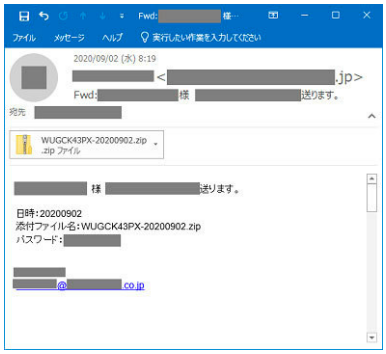
猛威を振るった Emotet-- その脅威を知る

1 日に IPA が確認した新たな手口は、「協力会社各位」という書き出しで始まり、悪意のあるマクロを仕掛けた Word ファイルをメールに添付して受信者にファイルを開かせるものだった。「消防検査」「ご入金額の通知・ご請求書発行のお願い」「次の会議の議題」「変化」などの件名や添付ファイル名もあった。2 日には、Word ファイルをそのまま添付するのではなく、パスワード付きの ZIP 形式の圧縮ファイルに含ませて送り付ける別の手口も見つかった。

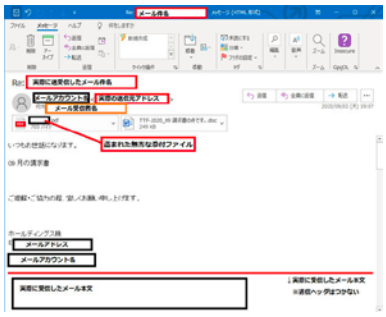
いずれの手口も、受信者が Word ファイルのマクロを実行してしまうと、複数の不正プログラム（ダウンローダーなど）がダウンロード、実行され、最終的にコンピューターが Emotet に感染してしまう。Emotet に感染したコンピューターでは攻撃者によって機密情報を窃取されたり、コンピューターが接続するネットワーク上の別のコンピューターにも感染を広げたり、なりすましメールを拡散する攻撃の踏み台にされたりさまざまな影響を受ける恐れがある。

トレンドマイクロも 9 月 3 日、同社からの連絡やアンケート協力などを装う Emotet の感染を狙ったなりすましメールを確認したとして、注意を呼び掛けた。同社からの正規のメールではファイルを添付しないといい、「弊社から送付されたように見えるメールにおいてファイルの添付があった場合、添付ファイルは実行せず破棄いただきますようお願いします」としている。

Emotet の感染を狙うなりすましメールの例（出典：IPA）



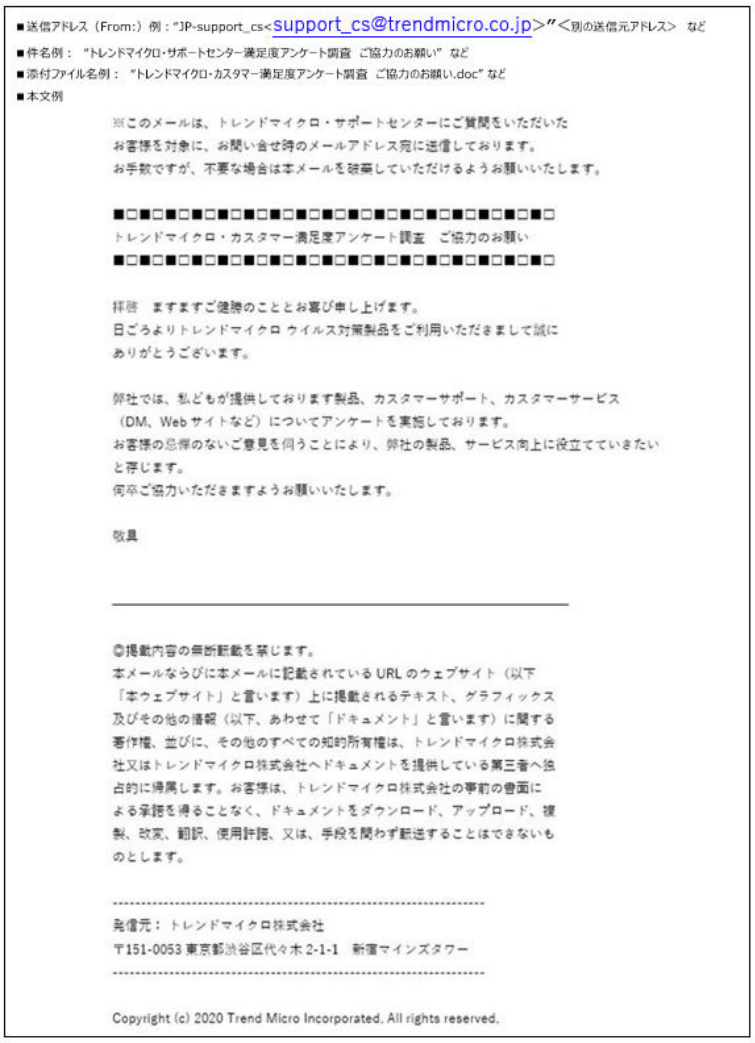
Emotet の感染を狙うなりすましメールの例（出典：IPA）



Emotet の感染を狙うなりすましメールの例（出典：JPCERT/CC）

Emotet の感染を狙うなりすましメールの例（出典：JPCERT/CC）

猛威を振るったEmotet-- その脅威を知る



■送信アドレス（From:）例："JP-support_cs<support_cs@trendmicro.co.jp>"＜別の送信元アドレス＞　など
■件名例：　"トレンドマイクロ・サポートセンター満足度アンケート調査　ご協力のお願い"　など
■添付ファイル名例：　"トレンドマイクロ・カスタマー満足度アンケート調査　ご協力のお願い.doc"　など
■本文例

※このメールは、トレンドマイクロ・サポートセンターにご質問をいただいた
お客様を対象に、お問い合せ時のメールアドレス宛に送信しております。
お手数ですが、不要な場合は本メールを破棄していただけるようお願いいたします。

■□
トレンドマイクロ・カスタマー満足度アンケート調査　ご協力のお願い
■□

拝啓　ますますご健勝のこととお喜び申し上げます。
日ごろよりトレンドマイクロ ウイルス対策製品をご利用いただきまして誠に
ありがとうございます。

弊社では、私どもが提供しております製品、カスタマーサポート、カスタマーサービス
（DM、Web サイトなど）についてアンケートを実施しております。
お客様の忌憚のないご意見を伺うことにより、弊社の製品、サービス向上に役立てていきたい
と存じます。
何卒ご協力いただきますようお願いいたします。

敬具

◎掲載内容の無断転載を禁じます。
本メールならびに本メールに記載されている URL のウェブサイト（以下
「本ウェブサイト」と言います）上に掲載されるテキスト、グラフィックス
及びその他の情報（以下、あわせて「ドキュメント」と言います）に関する
著作権、並びに、その他のすべての知的所有権は、トレンドマイクロ株式会
社又はトレンドマイクロ株式会社へドキュメントを提供している第三者へ独
占的に帰属します。お客様は、トレンドマイクロ株式会社の事前の書面に
よる承諾を得ることなく、ドキュメントをダウンロード、アップロード、複
製、改変、翻訳、使用許諾、又は、手段を問わず転送することはできないも
のとします。

発信元：トレンドマイクロ株式会社
〒151-0053 東京都渋谷区代々木 2-1-1　新宿マインズタワー

Emotet の感染を狙うなりすましメールの例（出典：JPCERT/CC）

猛威を振るったEmotet-- その脅威を知る

マルウェア「Emotet」の攻撃急増、米CISAも警告

米国土安全保障省のサイバーセキュリティ・インフラセキュリティ庁（CISA）は米国時間10月6日、トロイの木馬「Emotet」を使った犯罪者の動きが急激に活発化していると警告した。

Emotetはもともと、バンキング型トロイの木馬として拡散されていたが、最近ではボットネットとしてマルウェアを含むスパムを拡散し、ランサムウェアオペレーターなどのさまざまな犯罪グループに、感染したコンピューターへのアクセスを販売するのに使われている。

9月、まずフランス、日本、ニュージーランドが、その数週間後にはMicrosoft、イタリア、オランダが、Emotetを使った悪意のあるスパム活動の急増を警告していた。

2月以降おとなしくなっていたEmotetは、7月に再び猛威を振るい始めた。CISAはEmotetについて、「一般的に他のマルウェアのダウンローダーまたはドロッパーとして使われる、洗練されたトロイの木馬」で、「現在、最も蔓延している脅威の1つ」だと説明している。

このCISAの評価のとおり、Emotetは現在、世界最大のマルウェアボットネットであると見なされている。

8月以降、CISAとMulti-State Information Sharing & Analysis Center（MS-ISAC）は、Emotetのフィッシングメールを使った州政府、地方政府を標的とする攻撃の急増を検知しているという。

Emotetは、フィッシングメールへの添付ファイル、またはペイロードを起動するリンクを通じて、ワームのように拡散する。ファイルかリンクが開かれると、Emotetはブルートフォース（総当たり）攻撃でユーザーの認証情報を取得、共有ドライブに書き込むことにより、ネットワークの中を水平方向に拡散する。

CISAによると、連邦政府および民間の行政機関ネットワーク向けの侵入検知システム「EINSTEIN」は7月以降、約1万6000件のEmotetの活動に関連するアラートを検出している。

また9月にはMicrosoftが、Emotetは「Office」ドキュメントではなく、パスワードで保護された添付ファイル（ZIPファイルなど）を使用することで、電子メールのセキュリティゲートウェイを迂回していることを突き止めた。

同月、欧州各国はEmotetがランサムウェアを配信するためにマルウェア「Trickbot」をドロップしているほか、銀行の認証情報を盗むためにトロイの木馬「Qakbot」をドロップしていることを検知していた。