メールを悪用したサイバー攻撃「Emotet」は昨年確認されて以降一旦は落ち着いていましたが、2020年後半から第2波として急速に日本国内での被害が拡大しています。「Emotet第2波」は市販のウィルスソフトをすり抜けて入ってくる危険なマルウェアです。今回はその実態と対策について詳しく解説いたします。

＼ いやします。ひやします。／
おんせん県おおいた

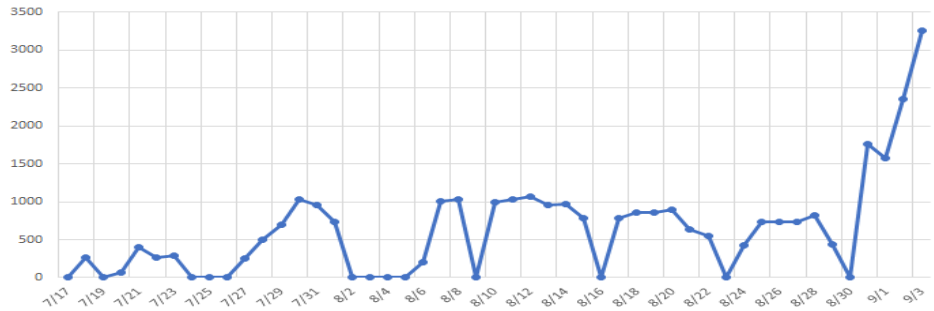
SECURITY ACTION ★★ セキュリティ対策自己宣言

38th GODO

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

(1) Emotet の感染拡大

JPCERT/CCは、2020年9月から マルウェア Emotet に感染し、感染拡大を試みるスパムメール送信に悪用される可能性のある国内ドメイン (.jp) のメールアドレスの急増を確認しています。また、Emotet の感染に関する相談件数も増加しており、Emotet の感染が拡大している状況を把握しています。引き続き、Emotet の感染に繋がるメールへの警戒が必要です。感染拡大を防ぐためにも、後述する内容を参照いただき、組織内への注意喚起を推奨します。



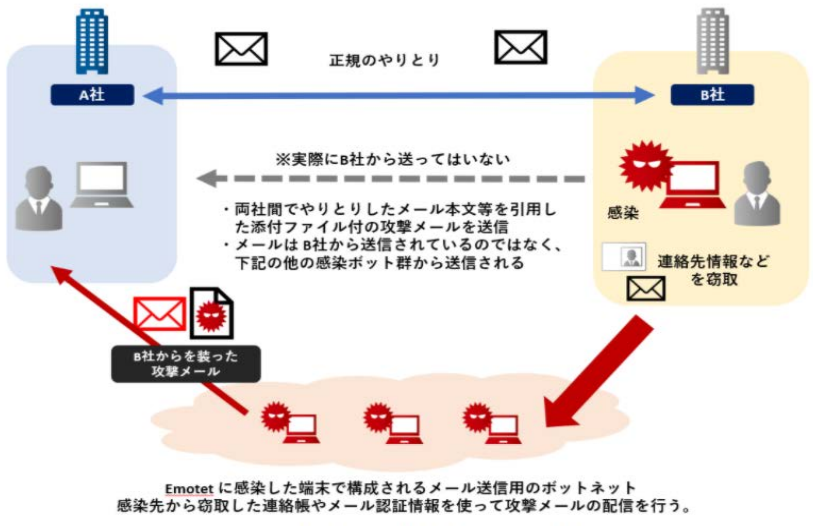
［図 I：Emotet に感染し、メール送信に悪用される可能性のある .jp アドレスの推移 (外部からの提供観測情報)］

(2) Emotet の新たな手法を確認

Emotet の主な感染経路は、これまでと変わらず、添付ファイルまたは本文中にリンクを含むメールです。添付ファイルまたはリンクからダウンロードされるファイルを実行すると、マクロやコンテンツの有効化を促す内容が表示されます。有効化すると、Emotet の感染に繋がることが確認されています。しかし、2020年7月に Emotet の配布活動が再開して以降、Emotet が感染を広げるための手口が巧妙化しています。
Emotet は、感染した端末から、メールアカウントの認証情報や過去に取引先などとやりとりしたメールの件名や本文などのデータを窃取し、窃取した情報を用いてスパムメールを配信する場合があります。最近ではそれ以外にも、Emotet が正規のメールから添付ファイルを窃取し、Emotet の感染を引き起こすWord 形式のファイルとともに、窃取したファイルを添付してスパムメールを送るケースが確認されています。

また、これまではメールに Emotet の感染を引き起こす Word 形式のファイルが添付されていましたが、新たにパスワード付き zip ファイルを添付し、パスワードはメール本文中に記載されているケースを確認しています。この場合、メール配信経路でのセキュリティ製品による検知や検疫をすり抜け、これまでセキュリティ製品により防いでいた受信者に対して、メールが配信されてしまうことが想定されます。

このように、メールの受信者に添付ファイルを実行させるための工夫や、検知回避のための手法の変化が確認されており、今後も引き続き警戒が必要です。一見すると業務に関係がありそうな内容で、取引先から送付されているようにみえる添付ファイルであっても、Emotet の感染に繋がるファイルである可能性があることを念頭に置き、信頼できるものと判断できない限りは「マクロやコンテンツを有効化」のボタンをクリックしないよう注意してください。



Emotet に感染した端末で構成されるメール送信用のボットネット
感染先から窃取した連絡帳やメール認証情報を使って攻撃メールの配信を行う。

Emotet の感染により発生する被害のイメージ ― JPCERT/CC

引用文献：https://www.jpcert.or.jp/

ウィルスへの感染を狙う攻撃メールマルウェア「Emotet」第2波に警戒を！

GODOかわら版

第31号

令和 2年 11 月号

ゴードービジネスマシン株式会社

2020年10月公開された被害事例（2020年10月28～29日発表分）

協力会社で「Emotet」感染か、なりすましメール出回る - 大多喜ガス

2020年10月28日

大多喜ガスは、同社や協力会社を装い、マルウェアを送りつけるなりすましメールが確認されているとして注意喚起を行った。協力会社のパソコンがマルウェアに感染したものと見られている。

同社によれば、10月20日に同社や協力会社の従業員を装ったなりすましメールが配信されていることを確認したもの。メールには、マルウェアが添付されていたり、外部サイトへ誘導するリンクが記載されていた。

過去に同社や協力会社とメールでやり取りをした関係者に対して送信されており、攻撃メールを誤って開いた協力会社のパソコンが、マルウェア「Emotet」に感染したことが原因と見られている。

同社や協力会社などになりすましたメールを受信した場合は、添付ファイルや本文中のURLを開かず、メールごと削除するよう注意を呼びかけた。

端末36台が「Emotet」感染 - 三協フロンテア

建設用設備器材の製造、販売を手がける三協フロンテアは、社内のパソコンがマルウェアに感染し、同社従業員を装ったなりすましメールが送信されたことを明らかにした。

同社によれば、従業員が使用するパソコンがマルウェア「Emotet」に感染したことが9月18日に判明したもの。

パソコンにはマルウェア対策ソフトを導入していたが、マルウェアを検知できず、同社内で36台が感染。感染端末を調べたところ、同社従業員を装ったなりすましメールが送信されていたという。

10月23日の時点でなりすましメールにメールアカウント43件が利用されたことが判明している。

同社従業員名で送信されたメールについて、心当たりのないもの、取引に関係ないもの、過去にやり取りしたものが不自然に再送信されたものなどへ注意するよう求めている。

次世代セキュリティ製品の検知回避を狙う「Emotet」

約５カ月の沈黙を経てふたたび７月に活動を再開したマルウェア「Emotet」。近年注目されている機械学習ベースのマルウェア対策製品から検知を回避する機能なども備えていた。

大量の亜種により、定義ファイルベースの製品による検出を逃れる手法は、多くのマルウェアで見られるが、7月以降出回っている「Emotet」ではサンドボックスを利用したゲートウェイ製品や、機械学習により作成されたマルウェアの検出エンジンなど、いわゆる「次世代セキュリティ製品」の検知を回避しようとする機能を備えていた。

ゲートウェイによる検出を避ける手段としては、パスワードを用いないとファイルを開けない暗号化した「zipファイル」を悪用している。

メールに記載されたパスワードを用いてzipファイルを復号し、チェックが行える製品も一部存在しているが、OSの標準機能では復号できない「AES256ビット」の暗号化を用いることで高度な検出についても回避を試みている。

エンドポイントにおける検出回避の手法も巧妙だ。ハッシュ値の異なる大量の亜種にも対応できるよう、機械学習ベースの検出エンジンを搭載したセキュリティ製品も登場しているが、機械学習の手法を逆手に取り、検出を回避する手法が用いられていた。

対策のポイント

①添付ファイルメールの開封は十分に注意する。
（取引先からのメールでも要注意）

②従業員に周知徹底する
（是非このかわら版を社内回覧することをお勧めします。）

③UTMを導入する。
（ただし、防御だけでなく、万が一の場合でも感染拡大を防ぐ機能のある機器を選定する）

情報セキュリティのご相談は弊社担当営業へご相談下さい。

引用文献：https://www.security-next.com/