2022 年 02 月 24 日

サービス＆セキュリティ株式会社 e-Gate センター

注意喚起:感染が急拡大中のマルウェア「Emotet」について

1. 概要

2021 年 11 月頃に活動を再開したマルウェア「Emotet」(エモテット)の感染が 2 月以降拡大しています。Emotet とは情報窃取や他のマルウェアの感染に悪用されるマルウェアで、主にメールの添付ファイルやリンクから感染します。

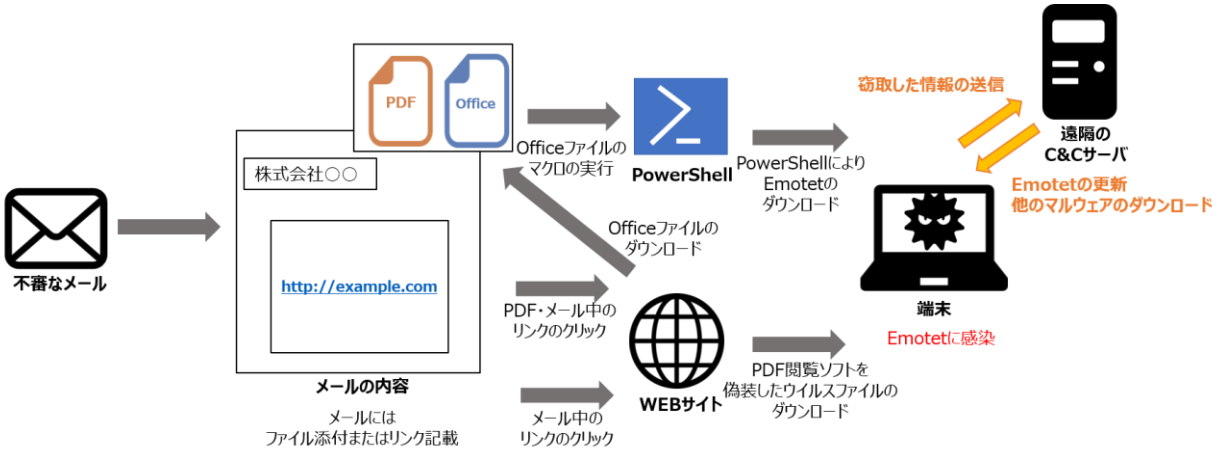
2021 年 1 月に UROPOL(欧州刑事警察機構)から Emotet のテイクダウン(※1)が発表されましたが、2021 年 11 月には Emotet の活動再開が世界各地で確認されました。そして今月に入り複数の国内企業から感染被害が報告され、感染の急拡大が観測されています。今回は急拡大している Emotet についてご紹介いたします。

※1:テイクダウンとは、攻撃目的に使用されるサーバを停止することで、Emotet の場合は遠隔から Emotet とやり取りするサーバを停止させています。

2. Emotet の特徴について

2021 年 11 月頃から活動を再開した Emotet ですが、攻撃手法に 11 月頃との大きな違いはありません。攻撃者はメールの添付ファイルとして「Microsoft Office」ファイルや PDF ファイルを送付したり、リンクを記載したメールを送付したりします。受け取ったユーザが添付ファイルの「Microsoft Office」ファイルを開き、マクロを有効にすると Emotet 本体がダウンロードされ、感染してしまいます。また、PDF ファイルやメール本文に記載された不正なリンク先からダウンロードされる「Microsoft Office」ファイルから感染させる場合もあります。その他には、メール本文のリンク先の不正な WEB サイトから PDF 閲覧ソフトを偽装したウイルスファイルをダウンロードさせ、実行すると Emotet に感染するという攻撃手法も確認されています。

感染すると、メール内容や設定内容、認証情報などを盗み取ります。他にも、盗んだメール情報を利用して他の端末への感染を広めたり、他のマルウェアをダウンロードしたりします。さらに遠隔の C&C サーバ(※2)へ接続し、Emotet 自身を最新の状態に更新することも行います。



【図 1】Emotet の感染イメージ

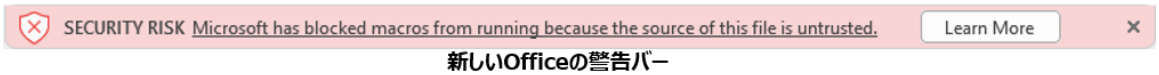
窃取された情報は、他の端末への感染のために悪用されます。この情報を用いて過去のメールの返信を装ったり、取引先になりすましたりしているため、受信者は攻撃メールと気づきにくくなっています。このため日頃から、メールの不審なリンクはクリックしない、メールに添付された Word や Excel などの「Microsoft Office」ファイルのマクロはむやみに実行しないなどの注意が必要です。

※2:C&C(コマンド＆コントロール)サーバとは、マルウェアに指示を出したり、マルウェアから情報を受け取ったりするサーバです。

3. Emotet への対策

Emotet の対策方法としては、身に覚えのないメールの添付ファイルやリンクを開かない、Word や Excel などのマクロを不用意に有効にしないことが重要です。マクロに関してはマルウェア攻撃への悪用が多々あることから、Microsoft は今月に「Microsoft Office」アプリに対して 4 月上旬よりインターネットから入手した VBA マクロをデフォルトでブロックする方針を発表しています。従来は警告バーの「コンテンツの有効化」をクリックすることでマクロを有効にできましたが、変更後はファイルのプロパティから MOTW(Mark of the Web)を削除する必要があります。MOTW は、インターネットなどの信頼できない場所から入手したファイルが NTFS ファイルシステムに保存される場合にファイルの属性として付与されます。Microsoft は最新チャネルから変更を適用し、将来的には他のバージョンの「Microsoft Office」にも適用する予定です。インターネットからのファイルに対して従来のような警告バーからのワンクリックではマクロを有効にできなくなるため、マクロを利用した Emotet の感染がこれまでより抑止されると思われます。

従来のOfficeの警告バー



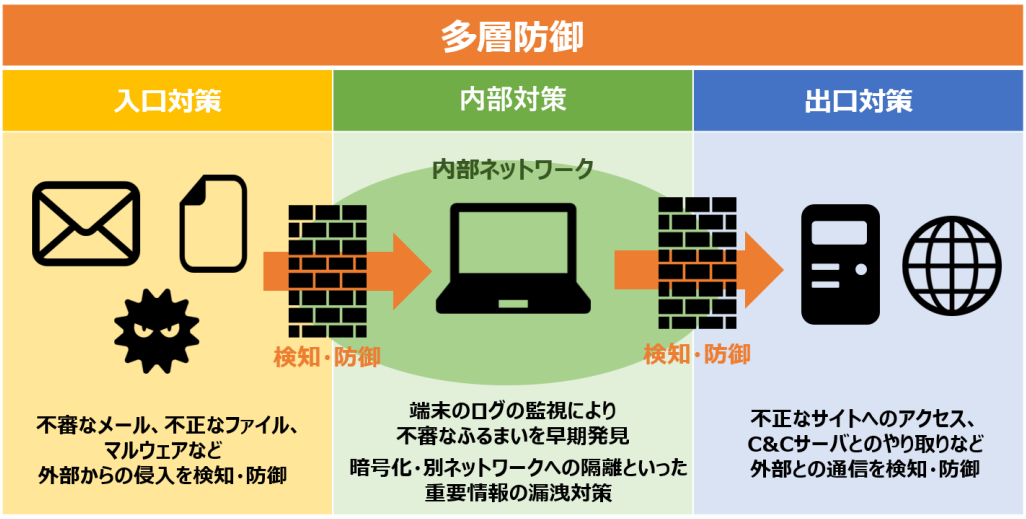
新しいOfficeの警告バー

【図 2】マクロの有効化の表示
(Microsoft「Helping users stay safe: Blocking internet macros by default in Office」から一部出典)

また、セキュリティ製品での検知・防御も有効です。IPS やサンドボックスを導入することで添付ファイルや C&C サーバとの通信、不審な URL へのアクセスの検知・防御ができます。またウイルス対策ソフトや EDR 製品をエンドポイントに導入することで感染からの防御や感染時の早期発見・対応が可能となります。万が一感染した場合に情報の漏えいを抑え、他の端末への感染を防ぐためにも早期発見は重要です。

しかし、セキュリティ製品での検知・防御は 100%ではありません。Emotet 自体の検知が難しい上に、添付ファイルをパスワード付き ZIP ファイルにすることでセキュリティ製品での検知を回避しようとする事例も報告されています。パスワード付き ZIP ファイルの送信後にパスワードを記載したメールを送る PPAP は、メールでの添付ファイルの送信手段として国内で広く用いられてきましが、このようにセキュリティ製品をすり抜けてマルウェアの感染経路に利用される場合があるため、PPAP を廃止

する動きが広がっています。Emotet の攻撃手法は日々巧妙化しているため、複数のセキュリティ製品の導入による多層防御の実現が有効となってきます。多層防御では、入口対策、内部対策、出口対策の３要素がポイントとなります。入口対策によって、内部への侵入を検知・防御することが可能となります。また侵入された場合に備えた内部対策、出口対策によって、情報漏洩のリスク軽減や被害の早期発見が可能となります。被害の早期発見や対応には、SOC(※3)や CSIRT(※4)の自社設置、外部委託といった手段も有用です。



【図 3】多層防御のイメージ

※3:SOC(Security Operation Center)とは、セキュリティ製品を監視し、サイバー攻撃の検出・分析、対策の提言を行う組織です。

※4:CSIRT(Computer Security Incident Response Team)とは、コンピュータやネットワークを監視し、問題が発生したときは原因解析・調査を行う組織です。

4. Emotet 感染時の対応

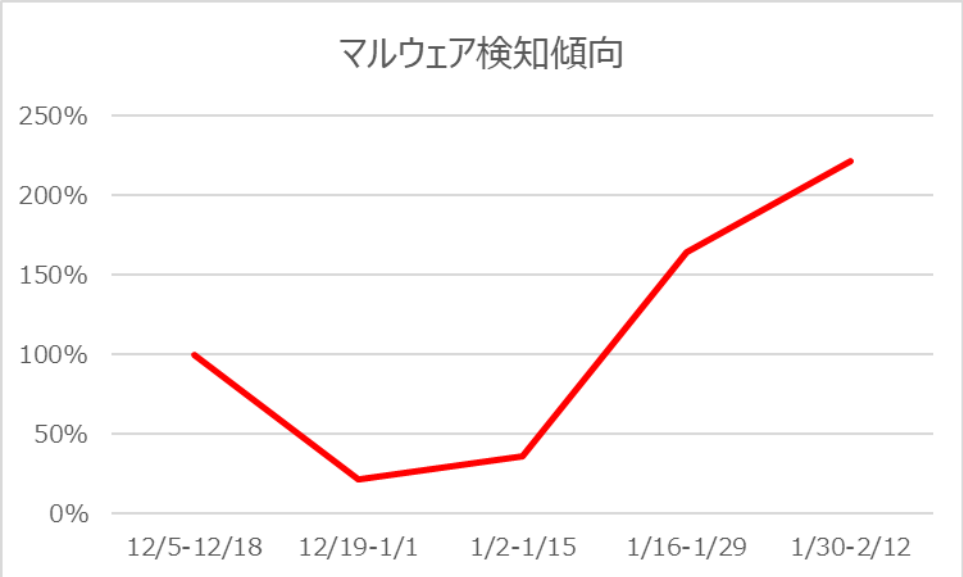
Emotet に感染した場合、まずは感染した端末を隔離します。端末から有線ケーブルを抜く、端末上で無線 LAN を無効にするなどを行い、ネットワークから隔離することで情報の漏洩や他のマルウェアの感染などを防ぎます。その後は隔離した端末上で Emotet ファイルの削除を実施します。削除手段の１つに、JPCERT/CC から GitHub で公開されている Emotet の感染確認ツール「EmoCheck」の利用があります。感染端末で EmoCheck を実行すると、Emotet ファイルが存在する場所を見つけ出すことができるので、その情報を元に Emotet ファイルを削除して端末から駆除できます。

JPCERTCC/EmoCheck – GitHub
https://github.com/JPCERTCC/EmoCheck/releases

駆除後には、Emotet はメール内容や設定内容、認証情報などを盗み出すため、メールアカウントや端末に保存しているパスワードの変更し、他のマルウェアがダウンロードされ感染していないかウイルスチェックを実施します。また、盗まれたメール情報から取引先などに被害が拡大する可能性があるため、Emotet 感染について早期の情報共有および公表が重要となります。

5. e-Gate での検知状況

e-Gate センターでマルウェア関連の攻撃統計を 2 週間ごとに取ったところ 1 月後半から増加傾向がみられます。国内でマルウェア「Emotet」の感染被害は増加しており、e-Gate センターでの検知も今後さらに増加する可能性があります。



【図 4】マルウェア検知傾向(12/5-12/18 の期間の検知数を 100%として算出)

6. 過去の Emotet に関連したセキュリティニュース

『注意喚起:進化するマルウェア「Emotet」について』(2019 年 3 月)
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=9657

『マルウェア「Emotet」(エモテット)最新攻撃メールについて』(2019 年 12 月)
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=10400

『Ryuk ランサムウェアの特徴と対策』(2020 年 11 月)
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=11221

『Emotet テイクダウン成功後の現状と今後の対策』(2021 年 3 月)
https://www.ssk-kan.co.jp/topics/topics_cat05/?p=11545

『注意喚起:テイクダウンされたマルウェア「Emotet」（エモテット）が活動再開』（2021 年 12 月）
https://www.ssk-kan.co.jp/topics/?p=12202

7. 参考情報

・JPCERT/CC

マルウェア Emotet の感染再拡大に関する注意喚起

https://www.jpcert.or.jp/at/2022/at220006.html

・Microsoft

Helping users stay safe: Blocking internet macros by default in Office

https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

8. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っています。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいています。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた「IT 運用のノウハウ」と最新のメソッドで構築した「次世代 SOC“e-Gate センター”」。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
リンク先のコンテンツは予告なく、変更、削除される場合があります。
※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp