2021 年 03 月 29 日

サービス＆セキュリティ株式会社 e-Gate センター

Emotet テイクダウン成功後の現状と今後の対策

1. 概要

マルウェア「Emotet」(エモテット)は主にメールの添付ファイルを利用し、感染を拡大させるマルウェアです。過去メールの返信を模したメールを送信し、添付ファイルの開封を誘導するなど手口が巧妙化していました。

2021 年 1 月 27 日に UROPOL（欧州刑事警察機構）は Emotet のボットネットのテイクダウンに成功したと発表しています。これにより最大規模のボットネットが無害化されたことになり、Emotet による被害は収束すると考えられます。

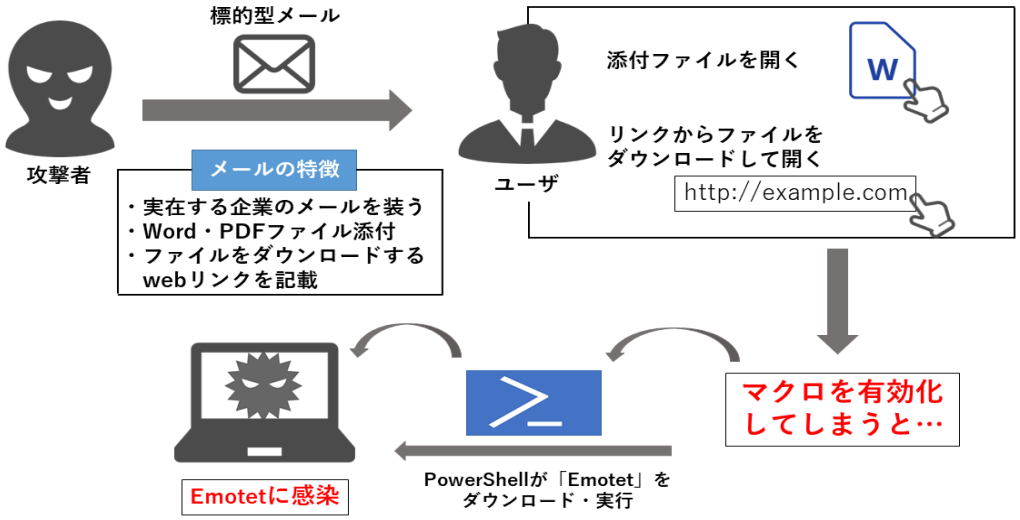
今回は Emotet の特徴や e-Gate センターの検知実績等を踏まえて最新の動向についてご紹介いたします。

2. 「Emotet」の特徴のおさらい

Emotet の主な感染経路はメールの添付ファイルです。他の種類のマルウェアをダウンロードし拡散するローダーとして使用されています。感染すると重要なファイルが窃取され、同ネットワーク内の端末にまで感染する恐れがあります。

Emotet の感染拡大を狙う攻撃者は特定の相手に狙いを絞った「標的型攻撃」を仕掛けます。標的型メールは過去メールの返信を模したメールを送信する等、巧妙化しており Emotet に限らず標的型メールに対しては注意が必要です。

Emotet の感染パターンとしては下図 1 のような標的型メールに添付されたファイルから感染します。



【図 1】「Emotet」感染イメージ

また、Emotet の特徴については過去に弊社の e-Gate セキュリティニュースで取り上げております。詳細は下記ニュースをご参照ください。

https://www.ssk-kan.co.jp/topics/topics_cat05/?p=10400

3. 「Emotet」がもたらす影響

Emotet の感染時には下記のような影響が発生します。

- メール、ブラウザに保存したパスワードの窃取、メール本文、メールアカウントの窃取
- ネットワーク内の他のパソコンへの感染拡大
- 他のマルウェアの感染拡大

4. 「Emotet」を含むマルウェアへの対策方法

Emotet の攻撃と同様にメールを利用した標的型攻撃に対しては下記のような対策が有効です。

- 身に覚えのないメールを開かない
- 身に覚えのないメールの添付ファイルを開かない
- 身に覚えのないメールに記載のある URL をクリックしない
- 例え自身が送信したメールへの返信メールであっても不自然な点があれば添付ファイルを開かない
- 信頼できないメールに添付された Word 文書や Excel ファイルを開いた時に、マクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない
- OS やアプリケーション、セキュリティソフトを常に最新の状態にする
- メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味が分からない場合は、操作を中断する
- 身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理部門等へ連絡する
- 組織内への注意喚起を行う
- メールセキュリティ製品の導入
- マルウェア不正通信ブロックサービスの導入
- ソフトウェアのマクロ自動実行機能の無効化

5. 「Emotet」感染時の対応方法

Emotet の感染端末に関しては海外の捜査当局から警察庁に対して、日本国内の約 2 万 6000 件の感染している機器に関する情報提供がありました。2021 年 2 月下旬より警察庁、総務省、一般社団法人 ICT-ISAC 及び ISP が連携して、Emotet に感染した可能性のある機器の利用者への注意喚起を行う取組を開始したと公開されています。

Emotet に感染した場合は ISP より通知されるコンピューター名を元に調査する必要があります。JPCERT/CC が公開しているツール「EmoCheck」でダウンロードし、感染が疑われる端末へコピーし、実行することで感染の有無を確認することができます。

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

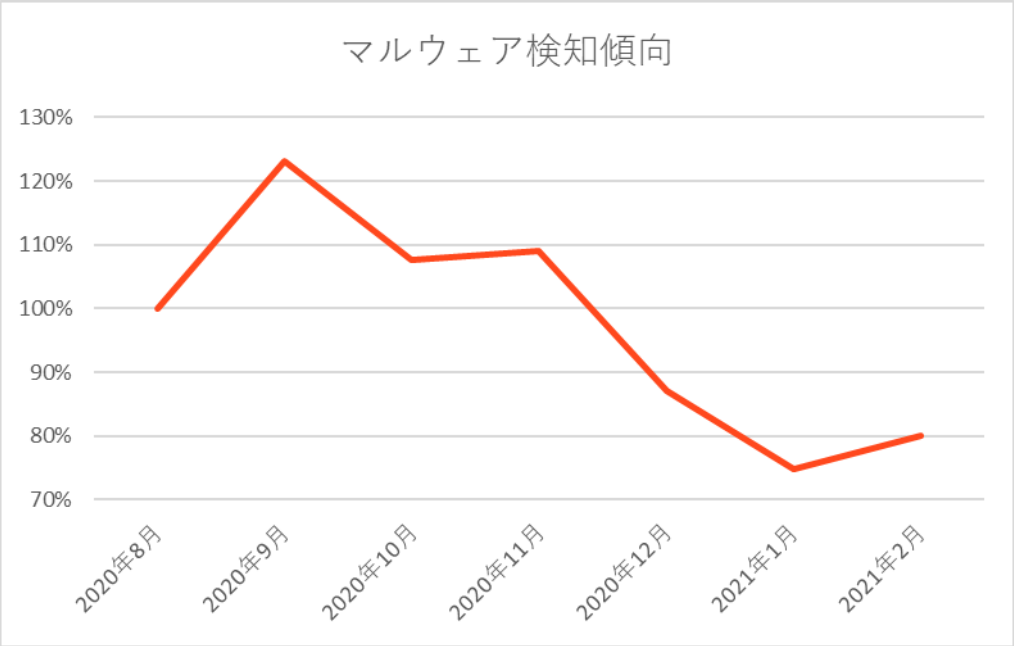
EmoCheck を実行時に「Emotet のプロセスが見つかりました」と表示された場合、Emotet に感染しています。感染端末を特定できた場合、感染端末で次のような対応が必要です。

- EmoCheck 実行結果に表示されるイメージパスに存在する Emotet を削除する
- メールアカウントやブラウザに保存されたアカウントのパスワードを変更する
- 他のマルウェアに二次感染していないか確認する

詳細については JPCERT/CC の下記対応方法をご参照ください。
JPCERT/CC：マルウェア Emotet のテイクダウンと感染端末に対する通知
https://blogs.jpcert.or.jp/ja/2021/02/emotet-notice.html

6. 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取ったところ、全体として 2020 年 9 月をピークに減少傾向になっています。これは 2020 年上半期に発生した新型コロナウィルス感染症の流行に便乗したサイバー攻撃が落ち着いてきたことが要因として考えられます。



【図 2】マルウェア検知傾向（2020 年 8 月を 100%として算出）

EUROPOL（欧州刑事警察機構）は Emotet のボットネットのテイクダウンに成功したと 2021 年 1 月 27 日に発表しています。これにより大きな被害を世界に与え続けてきた最大規模のボットネットを無害化されたことになります。今後はテイクダウンされたことで Emotet が持つ検知回避機能が動作しなくなるため、ウイルス対策ソフト等で徐々に検知、対処が進んでいくと考えられます。

7. 今後の対策

Emotet のボットネットはテイクダウンされましたが、まだ海外の捜査当局の調査結果では日本国内に約 2 万 6000 件の Emotet 感染機器が存在するという情報があります。攻撃者は過去に感染させた端末を利用し新たなマルウェアを混入することができるため、テイクダウンされたからと言って感染端末を放置しないようにご注意ください。Emotet 感染時には速やか

にツール「EmoCheck」を使用し、感染の有無を確認し対処することを推奨いたします。

マルウェア全体としては Emotet 以外のメールを利用した標的型攻撃を継続検知しております。Emotet の対策方法として紹介した「4.「Emotet」を含むマルウェアへの対策方法」は他のマルウェアでも有効ですので継続して対策を実施することを推奨いたします。

1 つの脅威がなくなってもサイバー犯罪者は日々、進化した巧妙な手口で利用者を陥れてきます。マルウェアも Emotet の 1 つだけではありません。今後も Emotet のような大規模なマルウェア感染活動が発生する可能性がありますので、「身に覚えのないメールや添付ファイルを開かない」といった基本的な対策を継続し、常に攻撃から身を守ることを意識して頂くことが大切です。

8. 参考情報

・警察庁

マルウェアに感染している機器の利用者に対する注意喚起の実施について

https://www.npa.go.jp/cyber/policy/mw-attention.html

・EUROPOL

WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION

https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

・JPCERT/CC

マルウェア Emotet のテイクダウンと感染端末に対する通知

https://blogs.jpcert.or.jp/ja/2021/02/emotet-notice.html

9. 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おります。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おります。

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。

«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