2018年
11月
NOVEMBER

MALWARE REPORT

マルウェアレポート

国内のマルウェア検出状況を解説

自己拡散するバンキングマルウェア Emotet を国内で確認

キヤノン IT ソリューションズ株式会社

はじめに

「マルウェアレポート」は、キヤノンITソリューションズが運営する

「マルウェアラボ」が「ESETセキュリティ ソフトウェア シリーズ」の検出データを基に

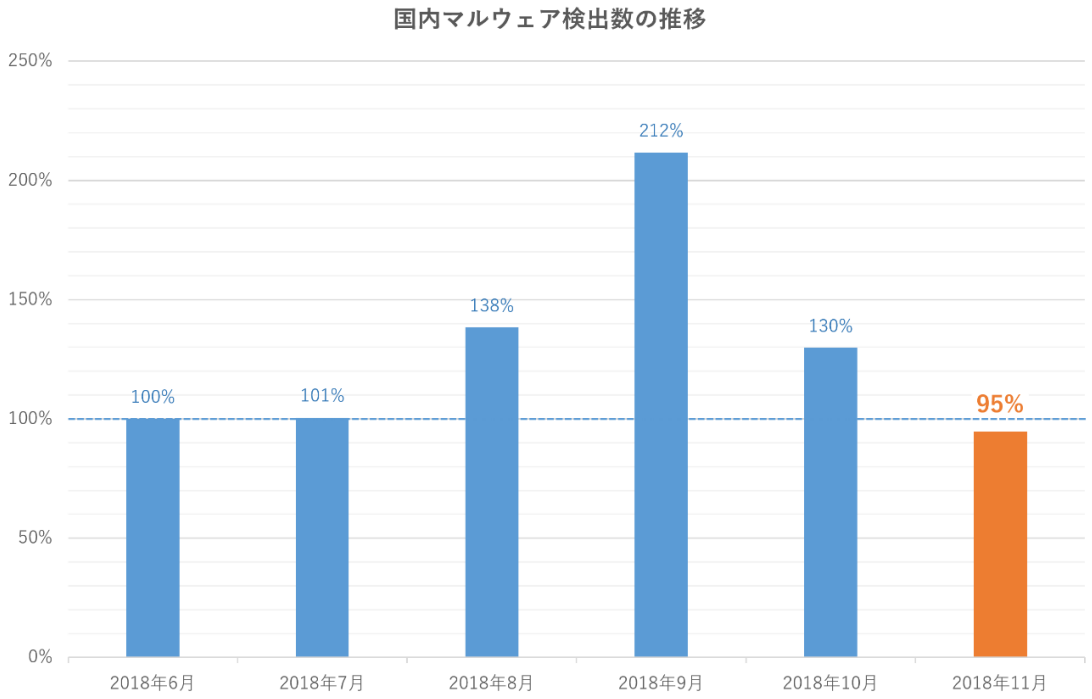
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2018 年 11 月マルウェア検出状況」

1. 11 月の概況について
2. バンキングマルウェア Emotet を国内で確認
3. インターネット広告収入を不正に得たサイバー犯罪グループが解体

1. 11 月の概況について

2018 年 11 月（11 月 1 日～11 月 30 日）に ESET 製品が国内で検出したマルウェアの検出数は 8 月～10 月の増加が落ち着き、2018 年では最も検出の少ない月となりました。



国内マルウェア検出数*1 の推移

（2018 年 6 月の全検出数を 100%として比較）

*1 検出数には PUA（Potentially Unwanted/Unsafe Application；必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション)を含めています。

検出されたマルウェアの内訳は以下の通りです。

国内マルウェア検出数*2 上位（2018 年 11 月）

順位	マルウェア名	比率	種別
1	HTML/ScrInject	19.0%	HTML に埋め込まれた不正スクリプト
2	JS/Adware.Agent	18.5%	アドウェア
3	VBA/TrojanDownloader.Agent	9.5%	ダウンローダー
4	JS/CoinMiner	4.7%	マイニングスクリプト
5	JS/Redirector	4.4%	リダイレクター
6	Suspicious	2.9%	未知の不審ファイルの総称
7	JS/Adware.Subprop	2.7%	アドウェア
8	Win32/RiskWare.PEMalform	2.4%	ブラウザハイジャッカー
9	PDF/Phishing	2.3%	フィッシング PDF
10	Win32/GenKryptik	2.0%	暗号化/難読化された実行ファイル

*2 本表には PUA を含めていません。

11 月に最も多く検出されたマルウェアは、不正なスクリプトが埋め込まれた HTML ファイルの総称である HTML/ScrInject でした。HTML/ScrInject は、単体の JavaScript ファイルである JS/Redirector や JS/Adware.Agent などと同様に Web ページ閲覧中に自動的に実行されます。その結果、不正な Web サイトへのリダイレクト、マルウェアのダウンロード、不正広告の表示、Web 閲覧情報の窃取などが行われるおそれがあります。

HTML/ScrInject は Web サイト管理者によって置かれる場合もありますが、多くは攻撃者によって Web サイトが改ざんされ、置かれたものです。過去の事例では、正規の Web サイトが改ざんされて Web ブラウザーの脆弱性を突いたドライブバイダウンロードが仕掛けられていました。その結果、脆弱性の残る Web ブラウザーを利用している閲覧者にマルウェアが配布されていました（参考：ウイルスはどこから来るのか？急増する Web 改ざん事件）。

2 番目に多く検出された JS/Adware.Agent や JS/Redirector、JS/Adware.Subprop、Win32/RiskWare.PEMalform も Web ブラウザー上で動作するマルウェアです（参考：2018 年 8 月マルウェアレポート）。HTML/ScrInject と合わせると 11 月に検出されたマルウェア全体の 3 割以上が Web をプラットフォームとしたマルウェアであり、攻撃基盤としての Web の広がりや、そこに対する攻撃者の関心の高さが伺えます。

JPCERT/CC が公開しているインシデント報告対応レポートによると、2018 年 7 月～9 月は不正 Web サイト（フィッシングサイト、マルウェアサイト）が 1,400 件、Web サイト改ざん被害が 226 件報告されています。悪意ある Web サイトや Web サイト改ざんの被害に遭わないよう、継続的に情報収集を行い、対策を講じていくことが重要です。

ESET 製品は、悪意ある Web サイトや Web サイト改ざんによって設置・配布されるスクリプトやマルウェアを検出・ブロックし、悪意あるコードの侵入を防ぎます。

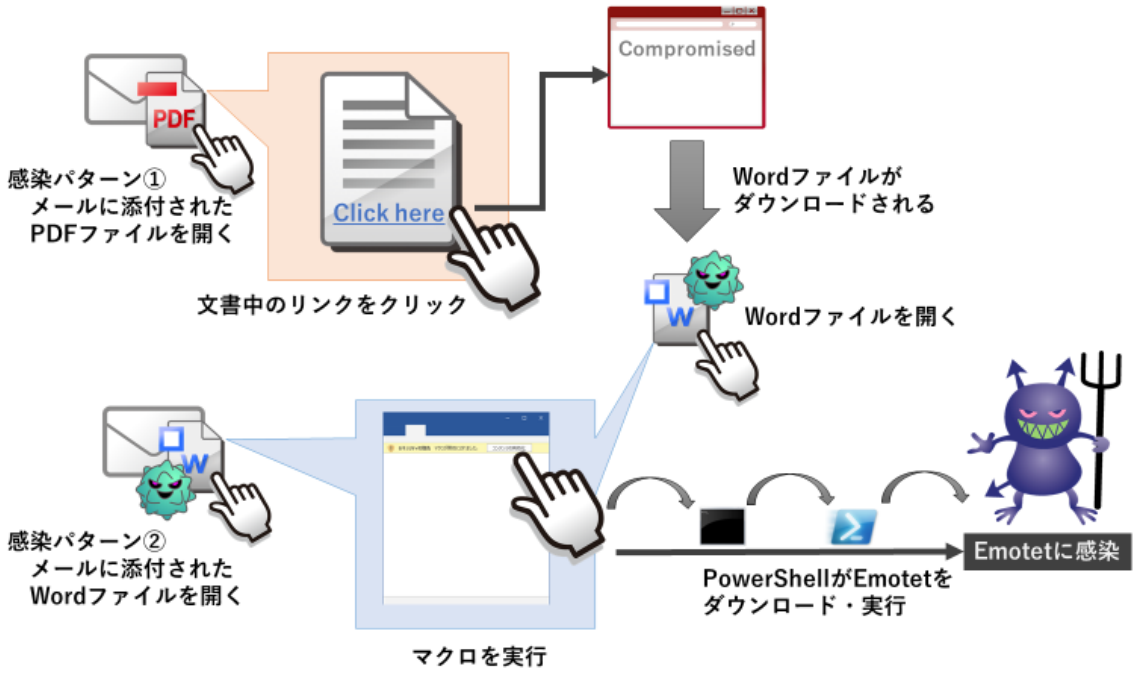
ESET 製品により悪意ある Web サイトが検出された画面

2. バンキングマルウェア Emotet を国内で確認

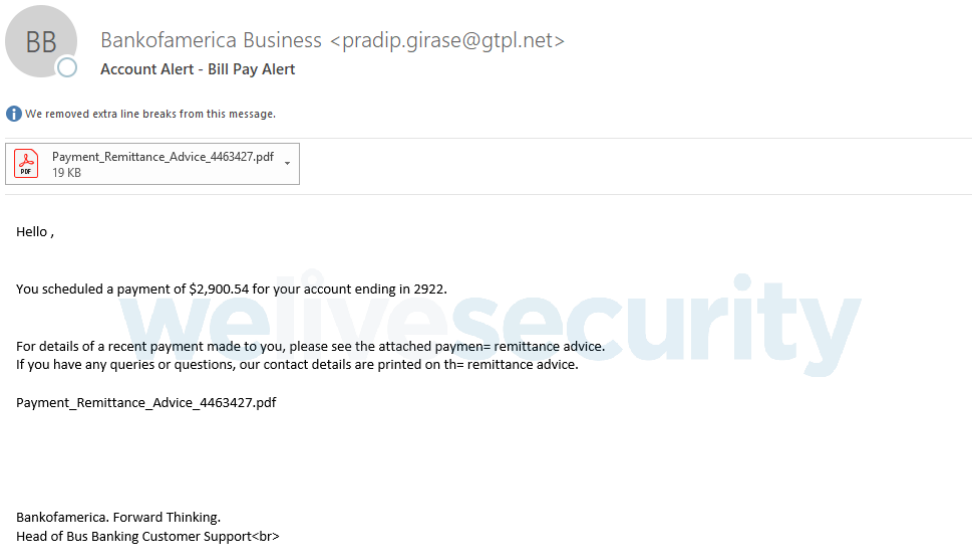
バンキングマルウェア Emotet が、今年の夏頃から世界中で猛威を振るっています。11 月には、日本国内においても Emotet が検出されました。

■ Emotet ダウンローダー

Emotet の主要な感染経路はメールです。メールには Emotet のダウンローダーとして機能する Word ファイルや PDF ファイルが添付されています。メールの差出人は実在する組織を装っており、請求書や銀行口座の支払通知などを送付するとの名目で受信者がファイルを開くよう誘導します。PDF に記載された URL からダウンロードしたファイルを実行（下図①）、あるいは Word ファイルのマクロを実行（下図②）すると、Emotet に感染します。



Emotet 感染までの流れ



BB Bankofamerica Business <pradip.girase@gtpl.net>
Account Alert - Bill Pay Alert

We removed extra line breaks from this message.

Payment_Remittance_Advice_4463427.pdf
19 KB

Hello ,

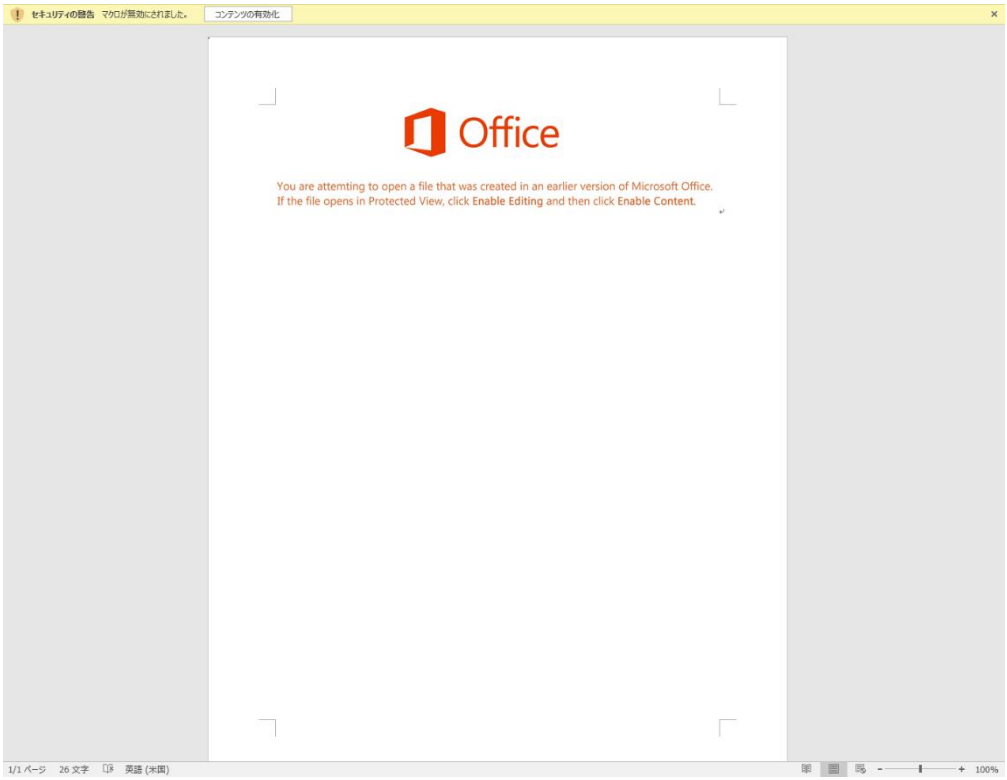
You scheduled a payment of $2,900.54 for your account ending in 2922.

For details of a recent payment made to you, please see the attached paymen= remittance advice.
If you have any queries or questions, our contact details are printed on th= remittance advice.

Payment_Remittance_Advice_4463427.pdf

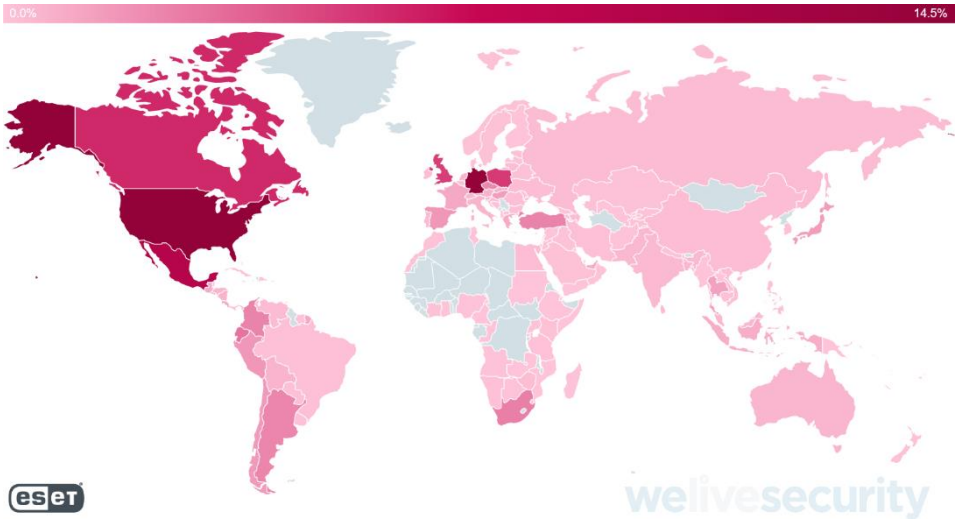
Bankofamerica. Forward Thinking.
Head of Bus Banking Customer Support

Emotet メールの文面例（welivesecurity より）

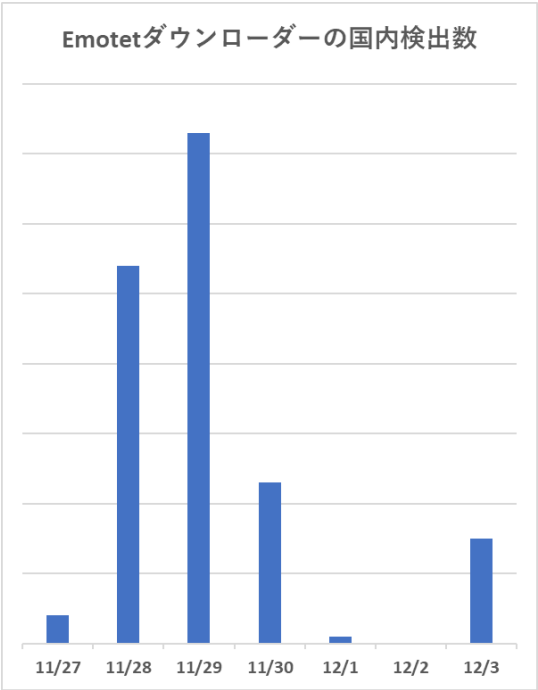


メールに添付された悪性 Word ファイル（Emotet ダウンローダー）

今回の Emotet メールの拡散は 11 月 5 日頃から活動が始まりました。メールの件名に英語やドイツ語が使われていることから、英語圏およびドイツ語圏のユーザーが主な標的と考えられます。日本国内においては 11 月 29 日頃に検出のピークを迎えています。



Emotet ダウンローダー検出割合の国別分布（welivesecurity より）



Emotet ダウンローダーの国内検出数

国内では、以下の悪性 Word ファイル（Emotet ダウンローダー）が多く検出されています。

＜ファイル名＞

- Acuerdo.doc
- Facture_Num_RPF403885.doc
- Tax Return Transcript.doc
- Verification of Non-filing Letter.doc
- Contrato.doc

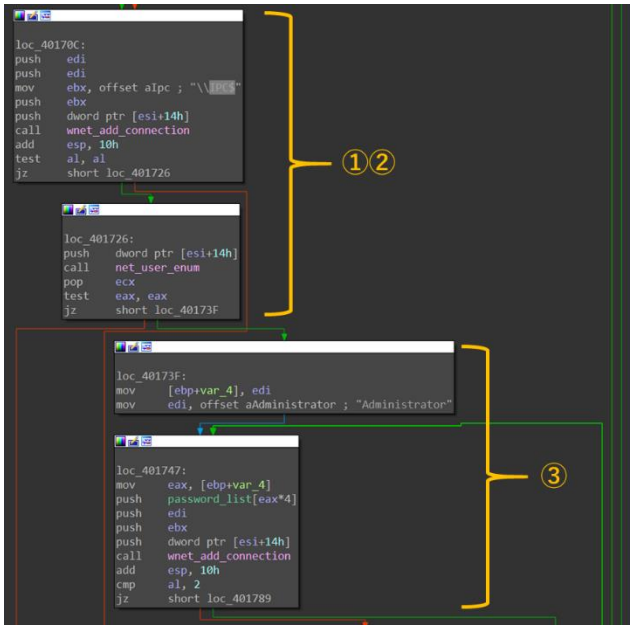
＜検出名＞

- VBA/TrojanDownloader.Agent.LOL
- VBA/TrojanDownloader.Agent.LNV
- VBA/TrojanDownloader.Agent.LLT
- VBA/TrojanDownloader.Agent.LQE
- VBA/TrojanDownloader.Agent.LNN

■ バンキングマルウェア Emotet

Emotet はバンキングマルウェアの一種です。感染するとインターネットバンキングサイト等の Web サービスにおける認証情報（ID、パスワードなど）を窃取され、不正送金やクレジットカードの不正利用の被害に遭う可能性があります。
Emotet は追加のモジュール（機能）をダウンロードすることで、様々な活動を行います。特筆すべき点として、ワームのように自身を複製しネットワーク内に感染を広げる機能を持つことが挙げられます。その感染力の高さから、Emotet が組織のネットワークに感染した場合、復旧するために最大で 100 万ドル（日本円でおよそ 113 億円：2018/12/13 現在）を要するとも言われています。
感染拡大モジュールの動作は以下のとおりです。

1. ローカルネットワークに接続されているコンピューター名を列挙
2. サーバー上のすべてのユーザーアカウントを列挙（下図①）
3. 列挙したユーザーアカウントに対し、モジュールに含まれるパスワードリストを用いて接続を試行（下図②）
4. Administrator アカウントに対して、同様にパスワードリストを用いて接続を試行（下図③）
5. 接続したコンピューターに自身をコピー



感染拡大モジュールの処理

```
.data:004041D0                dd offset aBusiness     ; "business"
.data:004041D4                dd offset aManager      ; "manager"
.data:004041D8                dd offset aTemporary    ; "temporary"
.data:004041DC                dd offset aIhavenopass  ; "ihavenopass"
.data:004041E0                dd offset aNothing      ; "nothing"
.data:004041E4                dd offset aNopassword   ; "nopassword"
.data:004041E8                dd offset aNopass       ; "nopass"
.data:004041EC                dd offset aInternet_0   ; "Internet"
.data:004041F0                dd offset aInternet     ; "internet"
.data:004041F4                dd offset aExample      ; "example"
.data:004041F8                dd offset aSample       ; "sample"
.data:004041FC                dd offset aLove123      ; "love123"
.data:00404200                dd offset aBoss123      ; "boss123"
.data:00404204                dd offset aWork123      ; "work123"
.data:00404208                dd offset aHome123      ; "home123"
.data:0040420C                dd offset aMypc123      ; "mypc123"
.data:00404210                dd offset aTemp123      ; "temp123"
.data:00404214                dd offset aTest123      ; "test123"
.data:00404218                dd offset aQwe123       ; "qwe123"
.data:0040421C                dd offset aPw123        ; "pw123"
.data:00404220                dd offset aRoot123      ; "root123"
.data:00404224                dd offset aPass123      ; "pass123"
.data:00404228                dd offset aPass12       ; "pass12"
.data:0040422C                dd offset aPass1        ; "pass1"
.data:00404230                dd offset aAdmin123     ; "admin123"
.data:00404234                dd offset aAdmin12      ; "admin12"
.data:00404238                dd offset aAdmin1       ; "admin1"
.data:0040423C                dd offset aPassword123  ; "password123"
.data:00404240                dd offset aPassword12   ; "password12"
.data:00404244                dd offset aPassword1    ; "password1"
.data:00404248                dd offset aDefault      ; "default"
```

モジュールに格納されたパスワードリストの一部

他にも Emotet には以下の機能があります。

- 電子メールクライアントに保存されているアカウント情報の窃取
- Outlook の連絡先（名前とメールアドレス）の窃取
- Outlook で送受信した電子メールの件名と本文の窃取（2018 年 10 月頃に追加）
- 別のマルウェア（TrickBot, IcedId など）のダウンロード

ESET 製品では Emotet を以下の検出名で検出し、攻撃を防ぎます。

- Win32/Emotet.*
- Win32/Kryptik.*
- Win32/Agent.*

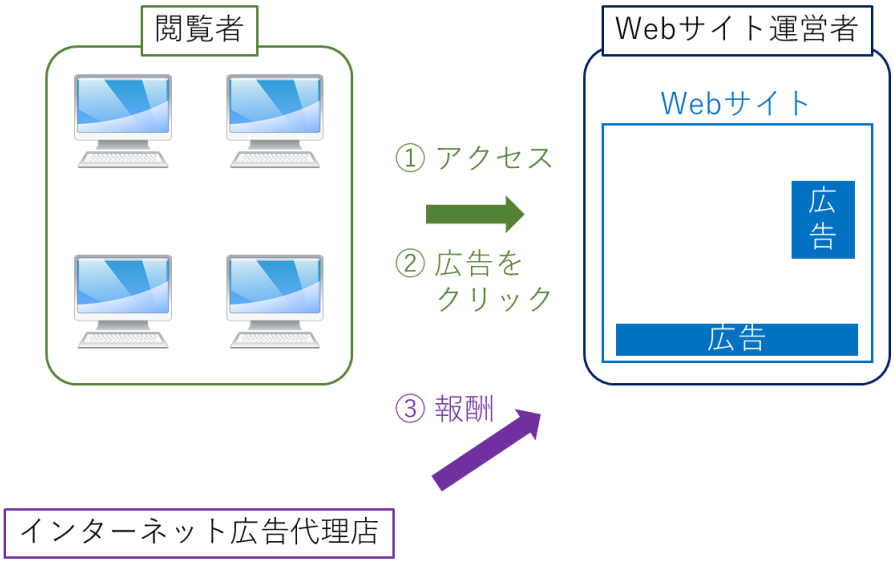
前述のように現在のところ Emotet の主要なターゲットは英語圏やドイツ語圏の国々とみられていますが、今後日本のユーザーを標的として、日本語で書かれたメールの本文や添付ファイルによる攻撃が発生することも考えられます。

Emotet などのバンキングマルウェアへの感染を防ぐために、メールで受信したファイルや Web からダウンロードしたファイルは安易に開かないことを推奨します。また、ネットワーク内の感染拡大を抑えるために OS やアプリケーションには最新の修正パッチを適用し、簡易なパスワードの使用は控えることを推奨します。

3. インターネット広告収入を不正に得たサイバー犯罪グループが解体

11 月 27 日にインターネット広告ビジネスの仕組みを悪用し、不正に広告収入を得た罪で、2 つのサイバー犯罪グループが解体され、8 名が逮捕されました（米国法務省：https://www.justice.gov/usao-edny/pr/two-international-cybercriminal-rings-dismantled-and-eight-defendants-indicted-causing）。この逮捕には様々な企業が協力しており、ESET 社は容疑者らが使用したマルウェアを解析し、技術提供を行いました。

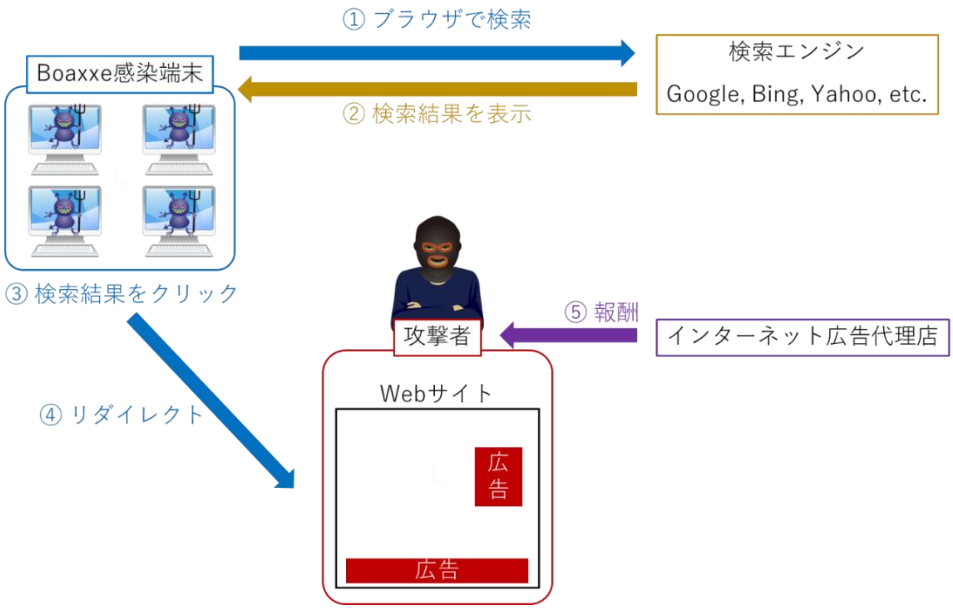
Web サイトにおける正規のインターネット広告ビジネスでは、Web サイト運営者が自身の Web サイトに広告を掲載することで、インターネット広告代理店から報酬が支払われます。報酬額は、広告の表示回数、広告のクリック数、広告先での収益発生などに応じて変動します。



正規のインターネット広告ビジネス

そのため、サイバー犯罪者はより多くの収益を得るために、広告の表示回数を水増しさせようとします。広告の表示回数を水増しする一般的な方法としては、同一の IP アドレスから同一の Web サイトに何度もアクセスする方法があります。しかし、この方法ではネット広告代理店から不正が疑われます。そこで、攻撃者は異なる IP アドレスからアクセスさせるために、不特定多数の端末にマルウェアを感染させ、Web サイトにアクセスするように感染端末を制御していました。この手法は、3ve（読み方：イブ）と呼ばれており、被害額は数百万ドル（数億円）、不正広告は 1 日に最大で 30 億回以上も表示されていました。

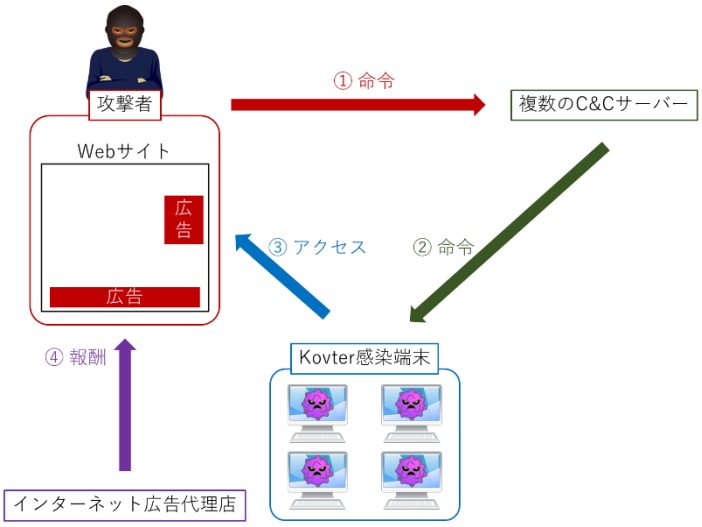
3ve で使用されるマルウェアは 2 種類あり、どちらもアドウェアです。1 つ目のアドウェアは、Boaxxe です。Boaxxe は、ブラウザーのプラグインとして動作するものが主流です。Boaxxe に感染した端末は、下図のように不正広告収入を得るために利用されます。



Boaxxe を用いた不正広告収入を得る手法

Boaxxe 感染端末のユーザーが、ブラウザー上で検索エンジンを用いた任意の検索をすると（図①）、通常通りの検索結果が表示されます（図②）。この時、その結果の 1 つをクリックしても、ユーザーが希望するサイトにはアクセスできません。バックグラウンド上では、偽の検索結果が用意されており、ユーザーがどの検索結果をクリックしても（図③）、攻撃者の Web サイトにリダイレクトされてしまいます（図④）。

2 つ目のアドウェアは、Kovter です。Kovter は隠密性に長けており、感染端末のユーザーは、攻撃者が用意した Web サイトにアクセスする様子を見ることはできません。Kovter に感染した端末は、下図のように不正広告収入を得るために利用されます。



Kovter を用いた不正広告収入を得る手法

攻撃者は、複数の C&C サーバーを介して、Kovter の感染端末に対して攻撃者が用意した Web サイトにアクセスするように命令を出します（図①－③）。
Kovter の隠密性として、感染端末が Web サイトにアクセスする際には、Chromium Embedded Framework を用いた目視できないブラウザーが使用されることが挙げられます。その他にも、Network Monitor（マイクロソフト製のプロトコルアナライザー）を検知すると、攻撃者の Web サイトにはアクセスしないことや、ユーザーがタスクマネージャーを起動すると Kovter のプロセスを終了させるなど、ユーザーに気づかれないような工夫が施されています。そのため、ユーザーが Kovter に感染していることに気づく確率が低くなり、攻撃者は長期間感染端末を制御することができます。

ESET 製品では、3ve に使用されたアドウェアをそれぞれ Win32/Boaxxe.BE、Win32/Kovter という検出名で検出し、駆除します。また、2 つのマルウェアは、無料で公開されている「ESET Online Scanner」を用いることでも、感染の有無を確認することができます。

不正広告収入は、利益率が高いことからサイバー犯罪者に注目されています。ここ数か月間、アドウェアが国内マルウェア検出数の上位を占めているため、注意が必要です。

ご紹介したように、今月はバンキングマルウェア Emotet が国内で確認されたほか、インターネット広告収入を不正に得たサイバー犯罪グループが解体されました。常に最新の脅威情報をキャッチアップし、対策を実施していくことが重要です。

■ 常日頃からリスク軽減するための対策について

各記事でご案内しているようなリスク軽減の対策をご案内いたします。
下記の対策を実施してください。

1. ESET 製品プログラムのウイルス定義データベースを最新にアップデートする
ESET 製品では、次々と発生する新たなマルウェアなどに対して逐次対応しております。
最新の脅威に対応できるよう、ウイルス定義データベースを最新にアップデートしてください。

2. OS のアップデートを行い、セキュリティパッチを適用する
ウイルスの多くは、OS に含まれる「脆弱性」を利用してコンピューターに感染します。
「Windows Update」などの OS のアップデートを行い、脆弱性を解消してください。

3. ソフトウェアのアップデートを行い、セキュリティパッチを適用する
ウイルスの多くが狙う「脆弱性」は、Java、Adobe Flash Player、Adobe Reader などのアプリケーションにも含まれています。
各種アプリのアップデートを行い、脆弱性を解消してください。

4. データのバックアップを行っておく
万が一ウイルスに感染した場合、コンピューターの初期化（リカバリー）などが必要になることがあります。 念のため、データのバックアップを行っておいてください。

5. 脅威が存在することを知る
「知らない人」よりも「知っている人」の方がウイルスに感染するリスクは低いと考えられます。ウイルスという脅威に触れてしまう前に「疑う」ことができるからです。
弊社を始め、各企業・団体からセキュリティに関する情報が発信されています。このような情報に目を向け、「あらかじめ脅威を知っておく」ことも重要です。

Canon

キヤノン ITソリューションズ株式会社

eset-info.canon-its.jp/