2019年
12月
DECEMBER

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

「Emotet」のばらまきメール本文の変化について

キヤノンマーケティングジャパン株式会社

はじめに

「マルウェアレポート」は、キヤノンマーケティングジャパンが運営する

「サイバーセキュリティラボ」が「ESET セキュリティ ソフトウェア シリーズ」の

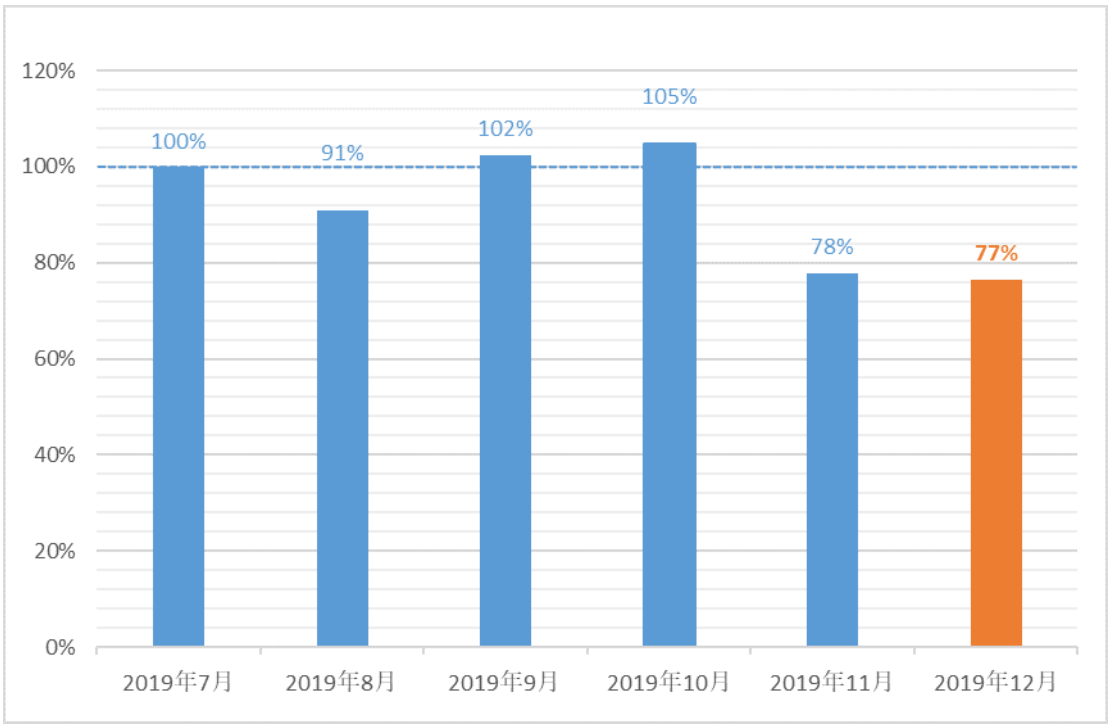
マルウェア検出データを基に国内のマルウェア検出状況を分析し、まとめたレポートです。

ショートレポート「2019 年 12 月マルウェア検出状況」

1. 12 月の概況
2. 「Emotet」のばらまきメール本文の変化について

1. 12 月の概況

2019 年 12 月（12 月 1 日～12 月 31 日）に ESET 製品が国内で検出したマルウェアの検出数の推移は、以下のとおりです。



国内マルウェア検出数*1 の推移

(2019 年 7 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。

2019 年 12 月の国内マルウェア検出数は、11 月に引き続いて、減少しました。直近 6 か月間の中で最も検出数の少ない月となりました。
検出されたマルウェアの内訳は以下のとおりです。

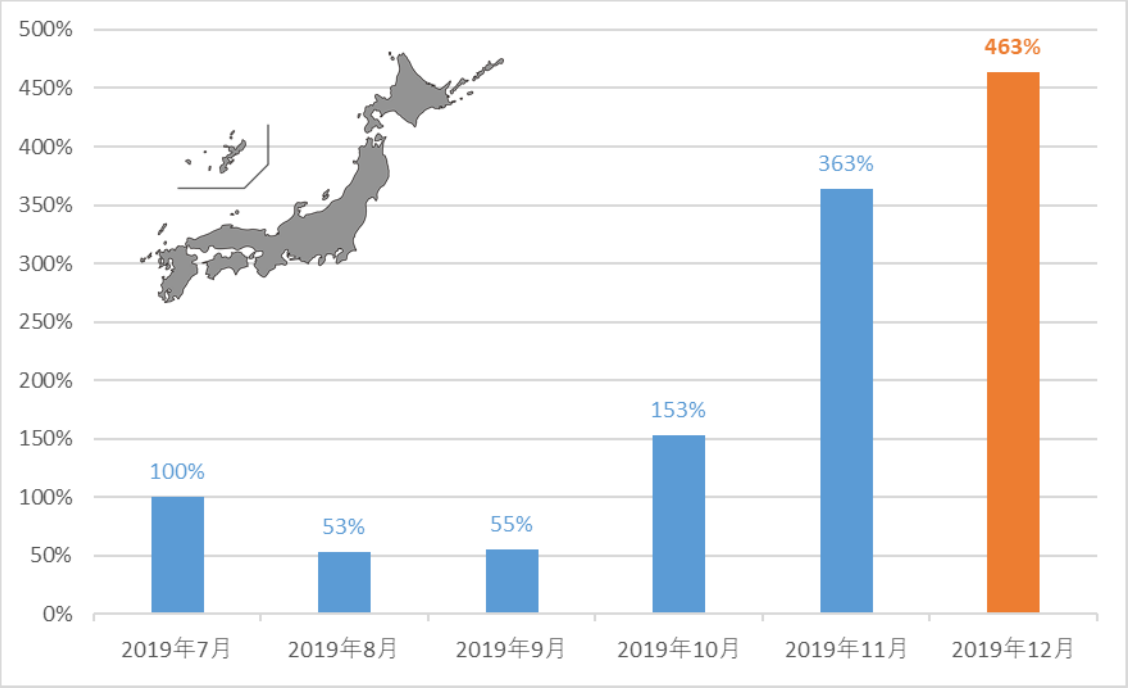
国内マルウェア検出数*2 上位（2019 年 12 月）

順位	マルウェア名	割合	種別
1	HTML/ScrInject	17.7%	HTML に埋め込まれた不正スクリプト
2	VBA/TrojanDownloader.Agent	8.4%	ダウンローダー
3	JS/Adware.Agent	8.0%	アドウェア
4	HTML/FakeAlert	3.2%	偽の警告文を表示するスクリプト
5	Win32/Exploit.CVE-2017-11882	1.9%	脆弱性を悪用するマルウェア
6	GenScript	1.4%	不正スクリプトの汎用名
7	DOC/Abnormal	1.4%	トロイの木馬
8	HTML/Refresh	1.4%	別のページに遷移させるスクリプト
9	JS/Redirector	1.3%	別のページに遷移させるスクリプト
10	DOC/Fraud	0.9%	詐欺サイトのリンクが埋め込まれた doc ファイル

*2 本表には PUA を含めていません。

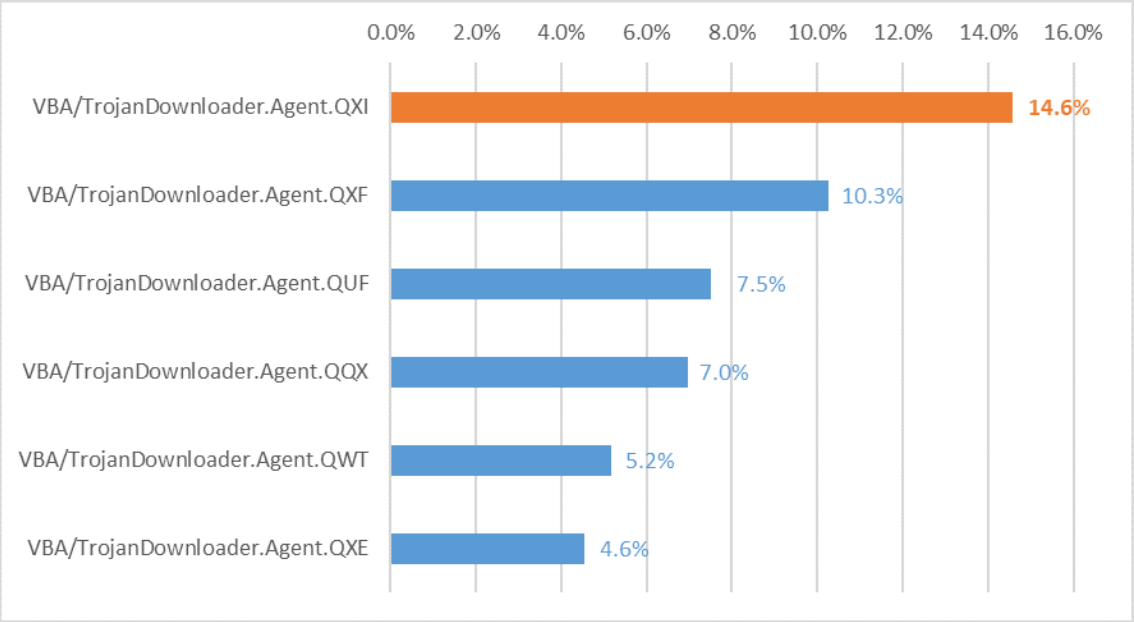
12 月に国内で最も多く検出されたマルウェアは、11 月に引き続き HTML/ScrInject でした。HTML/ScrInject は HTML に埋め込まれた不正スクリプトで、Web サイト閲覧時に実行されます。

2 位の VBA/TrojanDownloader.Agent は、Office 製品で利用されるプログラミング言語の VBA で作成されたダウンローダーです。他のマルウェアをダウンロードすることで知られています。ファイル形式は、Word ファイルや Excel ファイルであることが大半です。
今月は、11 月の検出数を超える数の VBA/TrojanDownloader.Agent が検出されました。2019 年 7 月と比較すると、4 倍以上の検出数となっています。この原因の一つとして考えられるのが、「Emotet」による攻撃の増加です。



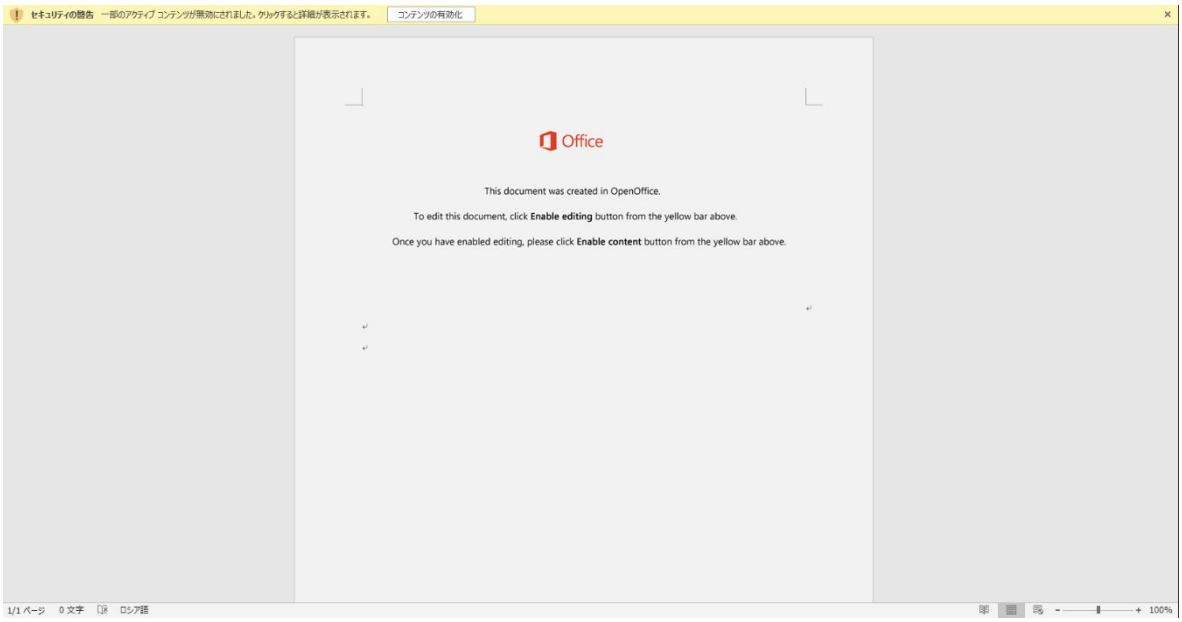
VBA/TrojanDownloader.Agent の国内での検出数の推移
（2019 年 7 月の検出数を 100%として比較）

VBA/TrojanDownloader.Agent の亜種内訳を見てみると、VBA/TrojanDownloader.Agent.QXI が最も多く検出された亜種でした。その割合は、VBA/TrojanDownloader.Agent の検出数の約 14.6%でした。



日本国内における VBA/TrojanDownloader.Agent の亜種内訳（12 月）

VBA/TrojanDownloader.Agent.QXI は、10 月以降被害が増えている「Emotet」をダウンロードするダウンローダーでした。
これ以外にも、VBA/TrojanDownloader.Agent.QXF や VBA/TrojanDownloader.Agent.QQX も、現時点では「Emotet」のダウンロードを行うことを確認しています。
VBA/TrojanDownloader.Agent.QXI を実行すると、2019 年 10 月のマルウェアレポートでご紹介した 6 種類の画像の一つが表示されます。
VBA/TrojanDownloader.Agent.QXF と VBA/TrojanDownloader.Agent.QQX を実行すると下記のような画像が表示されます。これは、以前に紹介した 6 種類とは異なる表示画面です。



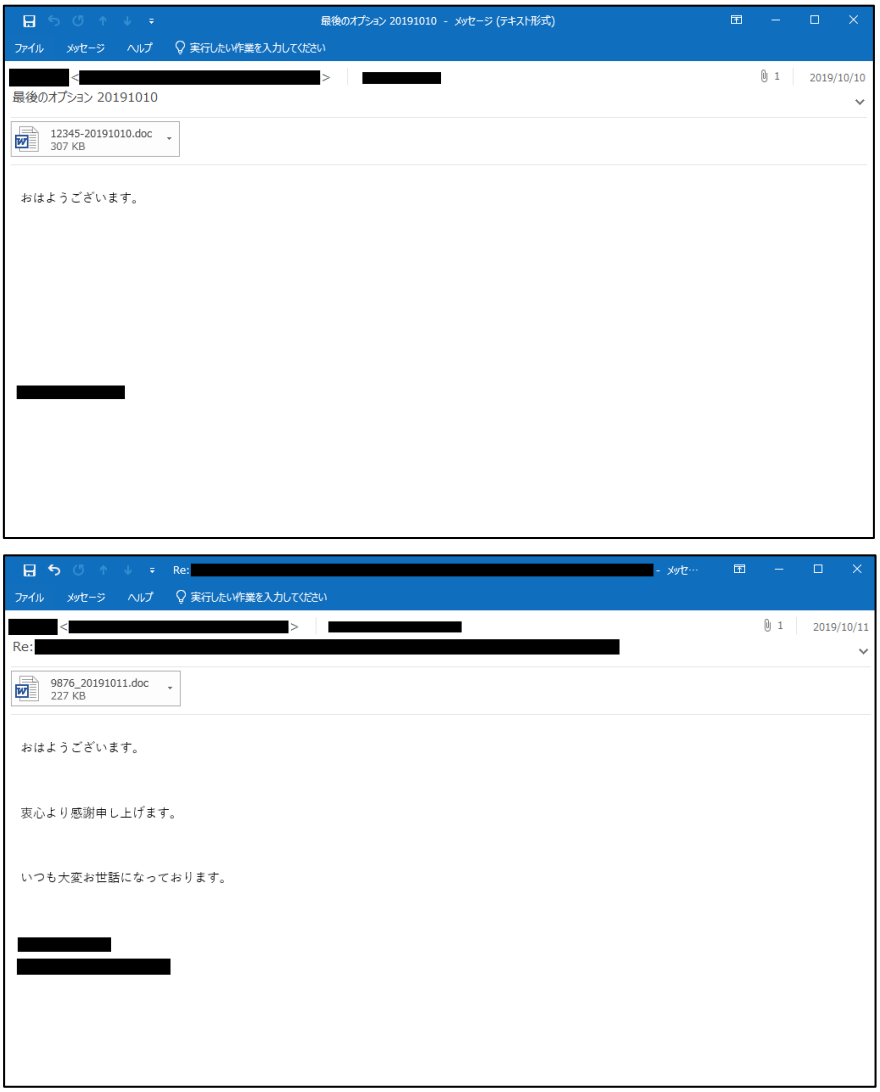
開いた Word の表示画面

ここからコンテンツを有効化してしまうと、最終的に「Emotet」へ感染します。
感染後は、情報窃取や他のマルウェアをダウンロードされるといった被害を受ける可能性があります。「Emotet」の詳細については、2019 年 10 月のマルウェアレポートでも紹介しています。

次章では、「Emotet」への感染を狙ったメール本文の変化について紹介していきます。

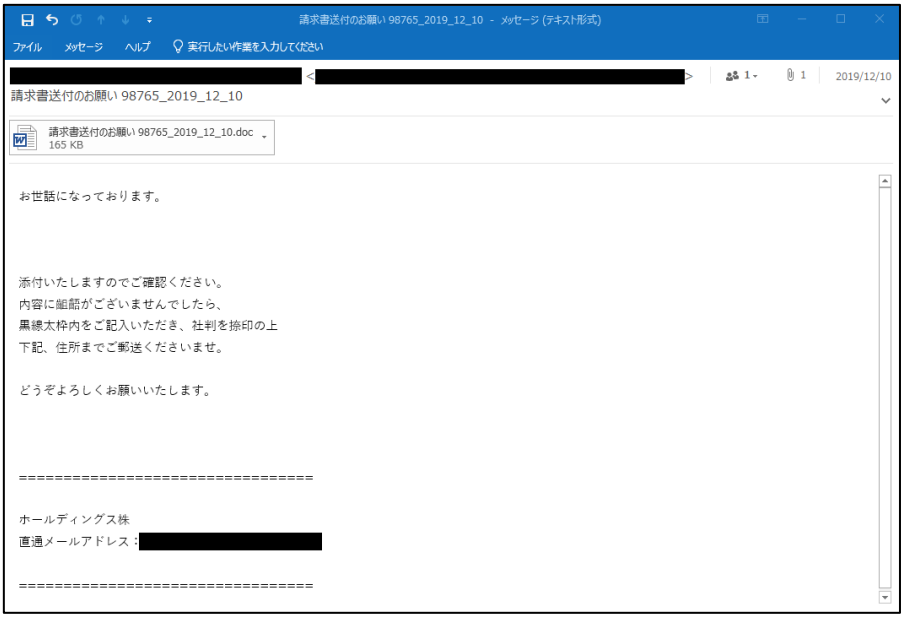
2. 「Emotet」のばらまきメール本文の変化について

前章でも触れましたが、「Emotet」への感染被害報告は今も増えています。現在確認されている主な侵入経路はメールに変わりないのですが、送られてくるばらまきメールの内容に少し変化が出てきています。
2019 年 10 月頃に確認されたメールの中には、「おはようございます」などの一言だけのものや「いつも大変お世話になっております」「衷心より感謝申し上げます」といった定型文が羅列されたものがありました。



「Emotet」のばらまきメール本文（2019 年 10 月頃に確認されたもの）

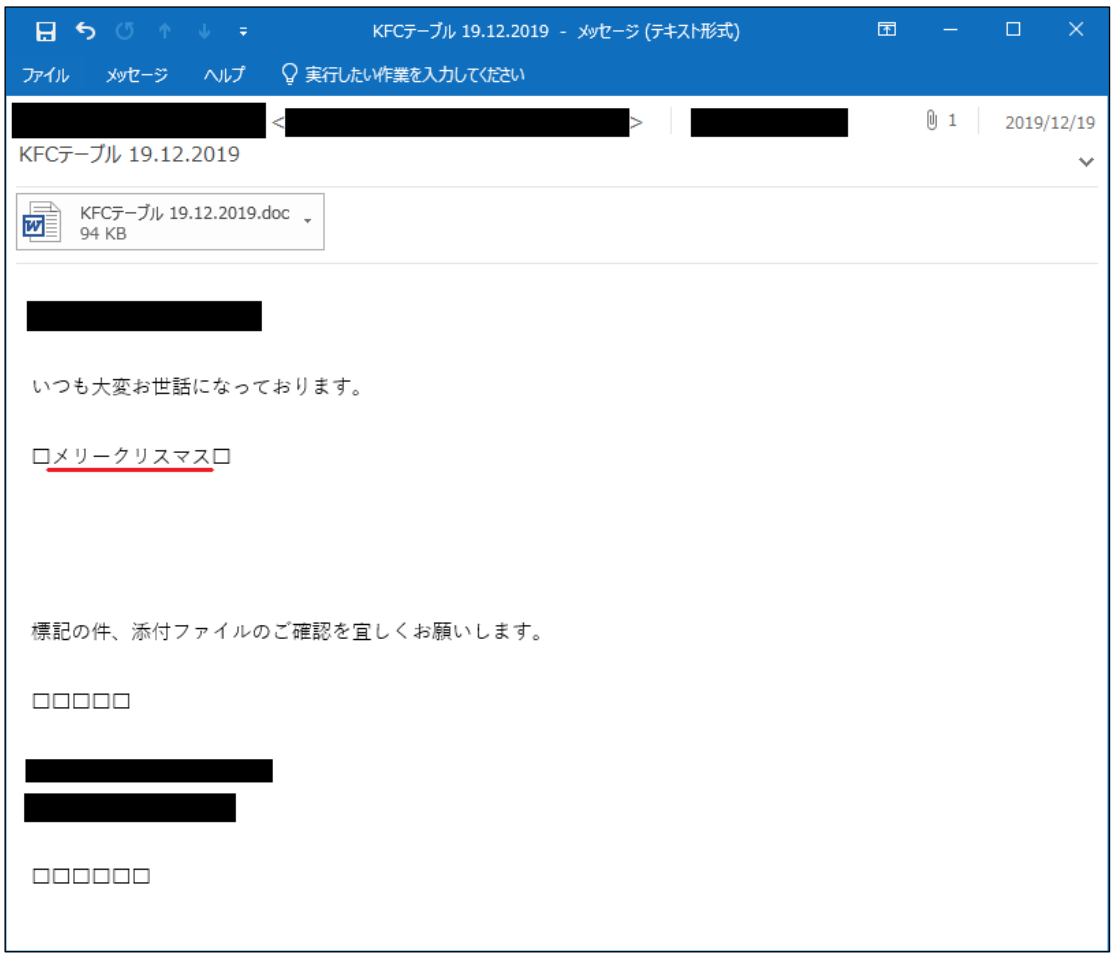
今月、確認されたメールの中には、以前より流暢な日本語の文章で書かれたものがありました。内容も文章として成立しています。



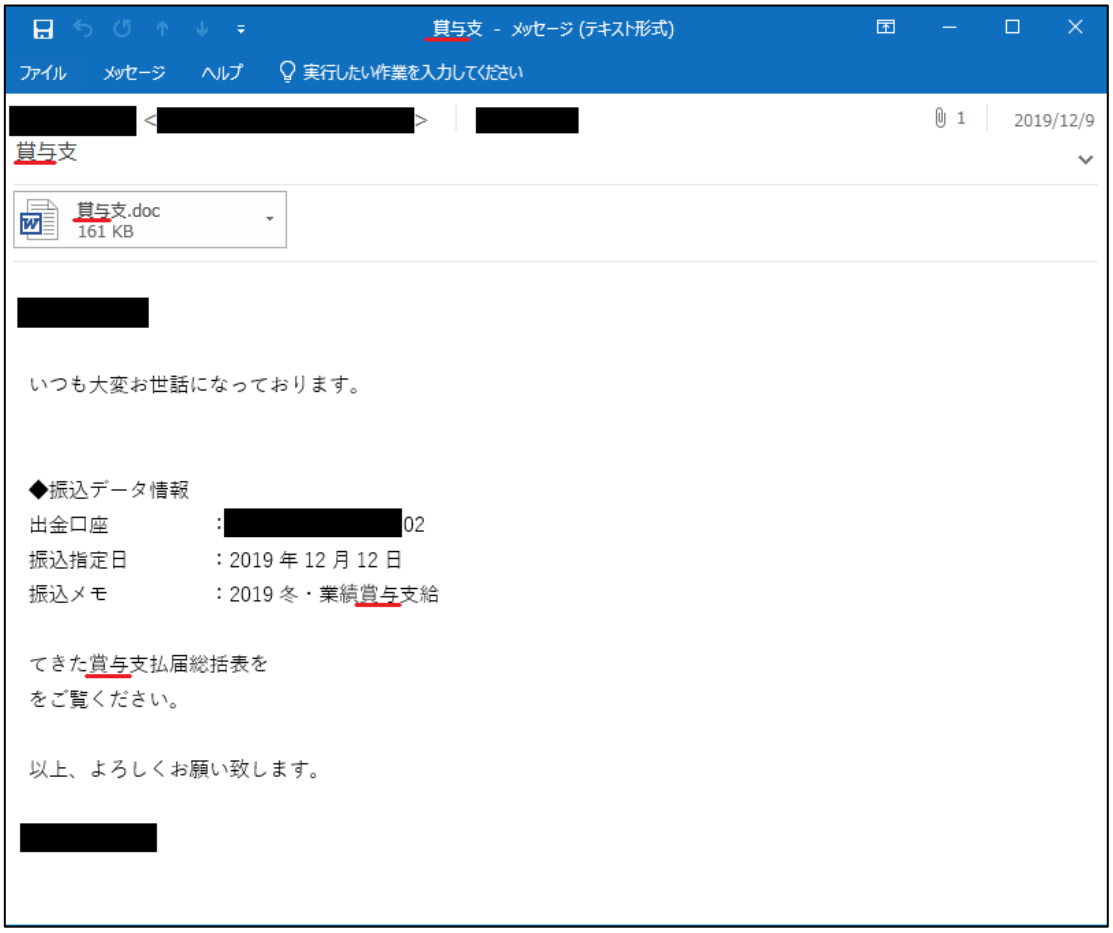
「Emotet」のばらまきメール本文（2019 年 12 月頃に確認されたもの）

もちろん、名前を名乗っていないことや表現がまだ固いなどといった点でばらまきメールだと見分けられるかもしれませんが、今後さらに日本語へのローカライズが進めば一目で判断することが難しくなる可能性があります。10 月頃と同様に一言だけのばらまきメールが今も送信されているため、このように流暢な文章のばらまきメールへの警戒心が薄くなりやすいと考えられます。

これに加えて、「メリークリスマス」や「賞与」といったイベントに合わせたメールも、今月は確認されています。「メリークリスマス」が含まれているメールでは、クリスマスに日本でよく利用されるファストフード店の名前を悪用していました。日本語だけでなく日本の習慣や文化にも対応が進んできているようです。

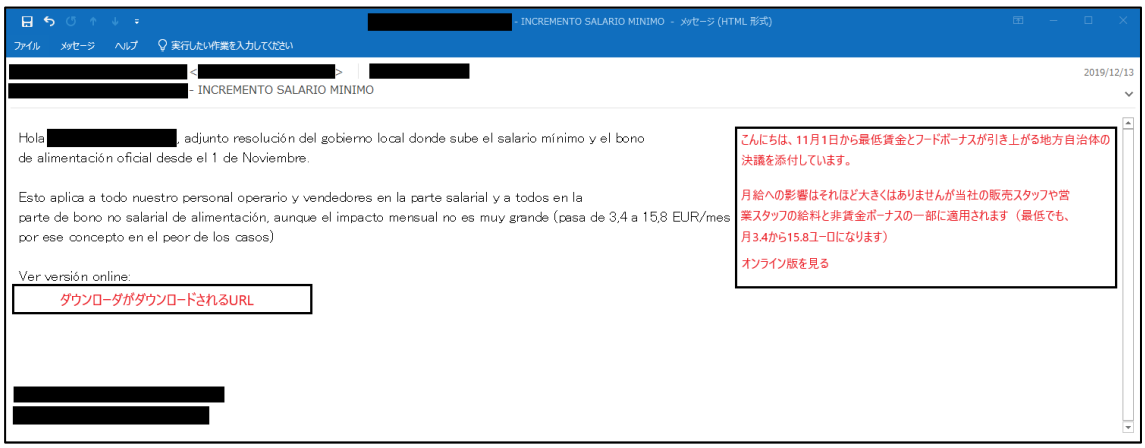


「メリークリスマス」を悪用したばらまきメール本文



「賞与」を悪用したばらまきメール本文

このようにイベントに合わせたメールは、他の国でも同様に確認されています。具体例を挙げますと、「昇給」というイベントを悪用したばらまきメールが、スペインで確認されています。



スペイン語で書かれた「昇給」を悪用したばらまきメール本文
（日本語訳は自動翻訳を少し整形したものです）

このメールに書かれた URL をクリックすることでダウンローダーがダウンロードされ、最終的に「Emotet」へ感染します。
このように、国ごとのイベントや習慣・文化に合わせたメールが送信されています。
今後も、イベントに合わせたメールが新たに出てくる可能性があるので注意が必要です。

以上のことから分かるように、「Emotet」への感染を狙ったばらまきメールに変化が出てきています。届いたメールに不審な点を感じた場合は、メールを開かないといったことが重要です。開いてしまった際に感染を防ぐためにも「Office 製品のマクロ自動実行が無効になっているかの確認」といった基本的な対策をあらかじめ実施しておいてください。
また、IPA や JPCERT からも注意喚起が出ているので、そちらも参照してください。

ご紹介したように、12 月は Web ブラウザー上で実行される脅威に加えて、ダウンローダーの脅威が多く検出されています。また、「Emotet」のばらまきメール本文に変化が出てきており、日本語への対応が進んできています。
今後の「Emotet」の変化に対応するためにも情報収集は欠かさないようにしましょう。

■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 製品の検出エンジン（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、検出エンジン（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
マルウェアの多くは、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
マルウェアの多くが狙う「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
万が一マルウェアに感染した場合、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」の方がマルウェアに感染するリスクは低いと考えられます。マルウェア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。

［引用・出典元］

- 2019 年 10 月 マルウェアレポート | マルウェア情報局
  https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1910.html

- 「Emotet」と呼ばれるウイルスへの感染を狙うメールについて | IPA
  https://www.ipa.go.jp/security/announce/20191202.html

- マルウエア Emotet の感染に関する注意喚起 | JPCERT
  https://www.jpcert.or.jp/at/2019/at190044.html

Canon

キヤノンマーケティングジャパン株式会社