2017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

バンキングマルウェアの感染を狙った攻撃が日本に集中

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

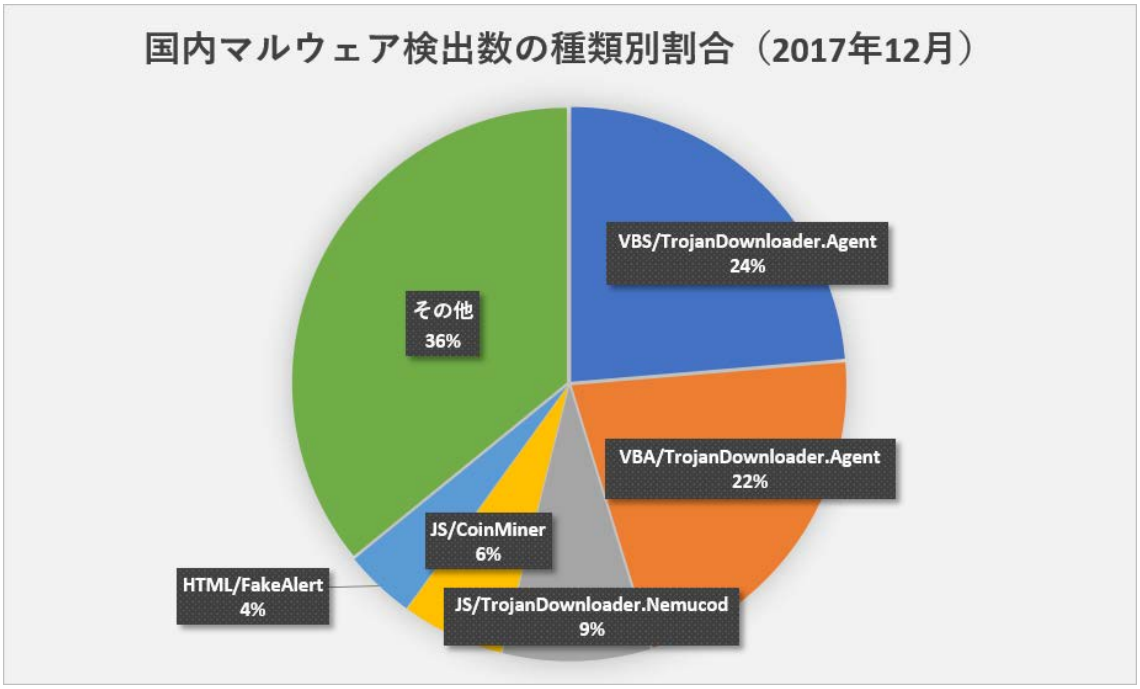
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2017 年 12 月マルウェア検出状況」

1. 12 月の概況について
2. バンキングマルウェアの感染を狙った攻撃が日本に集中
3. ランサムウェアのダウンローダーを数多く確認

1. 12 月の概況について

2017 年 12 月 1 日から 12 月 31 日までの間、ESET 製品が国内で検出したマルウェアの比率は、以下のとおりです。



国内マルウェア検出数の比率（2017 年 12 月）

国内マルウェア検出数上位（2017 年 12 月）

順位	マルウェア名	比率	種別
1	VBS/TrojanDownloader.Agent	24%	ダウンローダー
2	VBA/TrojanDownloader.Agent	22%	ダウンローダー
3	JS/TrojanDownloader.Nemucod	9%	ダウンローダー
4	JS/CoinMiner	6%	マイニングマルウェア
5	HTML/FakeAlert	4%	偽の警告文表示
6	Suspicious	4%	未知の不審なファイル
7	Win32/RealNetworks	3%	PUA(※)
8	JS/Redirector	3%	リダイレクター
9	JS/TrojanDownloader.Agent	3%	ダウンローダー
10	Win32/FusionCore	1%	PUA(※)

（※）Potentially Unwanted Application(望ましくない可能性のあるアプリケーション)：コンピューターの動作に悪影響を及ぼすことや、ユーザーが意図しない振る舞いなどをする可能性があるアプリケーション。

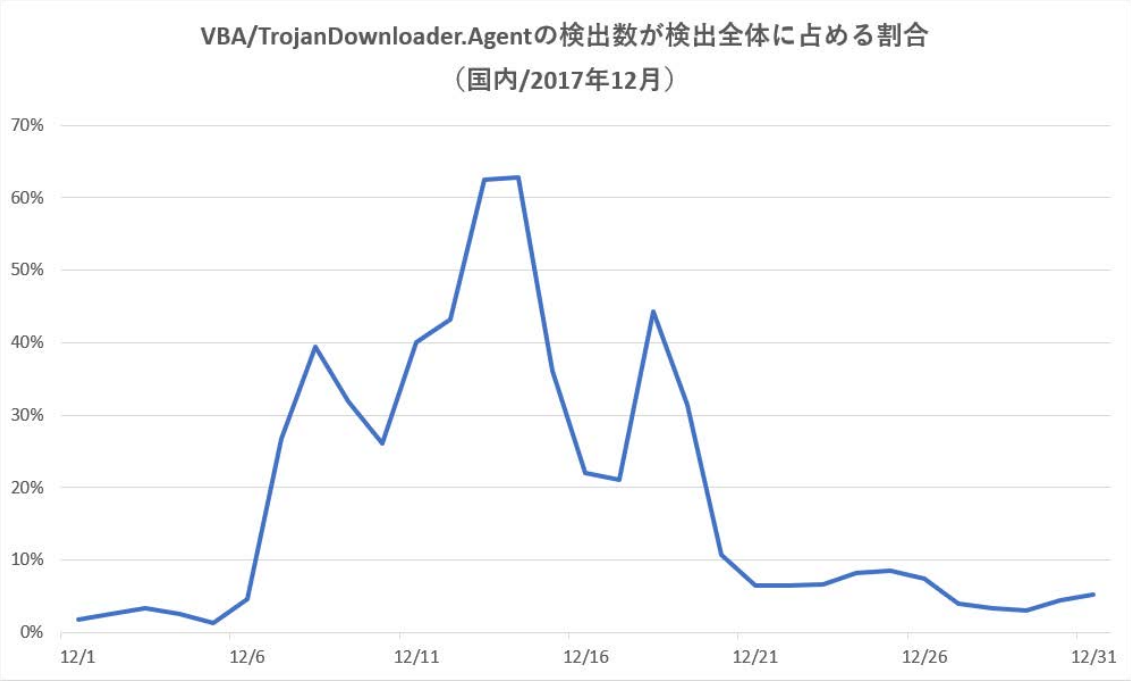
12 月は VBS（VBScript）形式のダウンローダーと VBA（Visual Basic for Applications）形式のダウンローダーが数多く検出されました。ダウンローダーがダウンロードするマルウェアは時間や実行環境によって様々に変化しますが、12 月はランサムウェアおよびバンキングマルウェアをダウンロードするタイプが数多く確認されています。

4 位の「JS/CoinMiner」は ESET における分類が変更されたため、検出数が増加しています。

2. バンキングマルウェアの感染を狙った攻撃が日本に集中

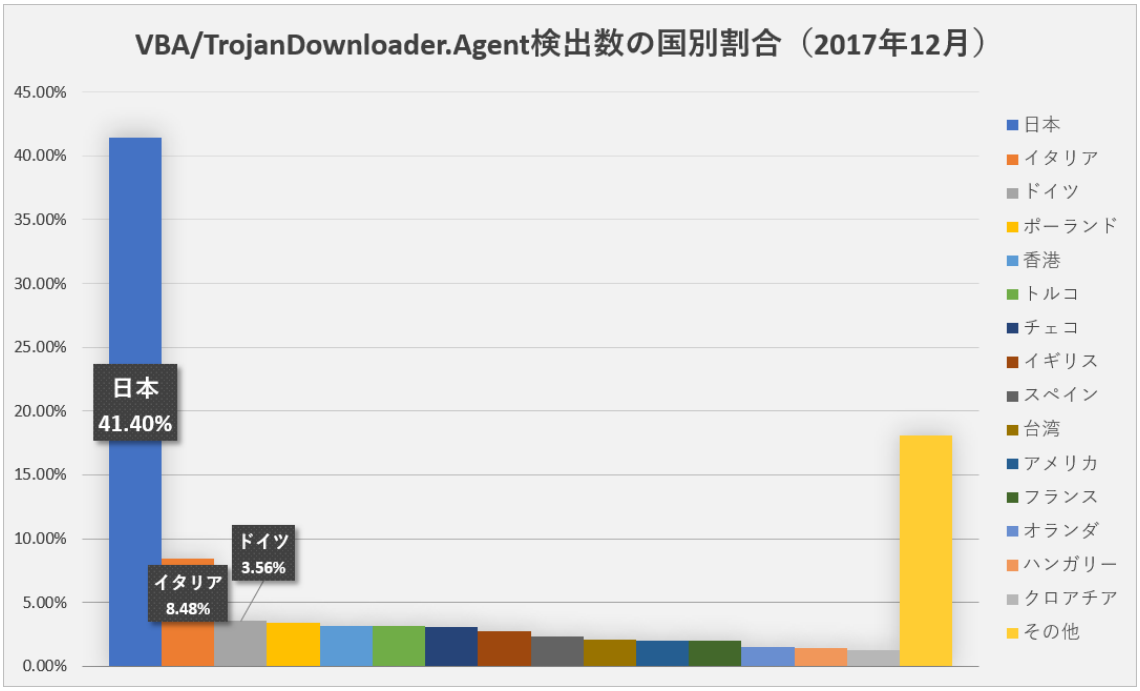
12 月上旬から中旬にかけて、VBA 形式のダウンローダー「VBA/TrojanDownloader.Agent」が数多く検出されました。このダウンローダーは「Win32/Spy.Ursnif」の亜種（別名 DreamBot）をダウンロードすることが確認されています。
「Win32/Spy.Ursnif」は、インターネットバンキングサイトの認証情報（ユーザ ID やパスワード等）やクレジットカード情報を窃取します。本マルウェアに感染した場合、銀行口座からの不正送金やクレジットカードの不正利用などの被害に遭う可能性があります。

「VBA/TrojanDownloader.Agent」は 12 月 8 日前後、14 日前後、18 日前後に顕著に検出されています。



VBA/TrojanDownloader.Agent の検出数が検出全体に占める割合（国内/2017 年 12 月）

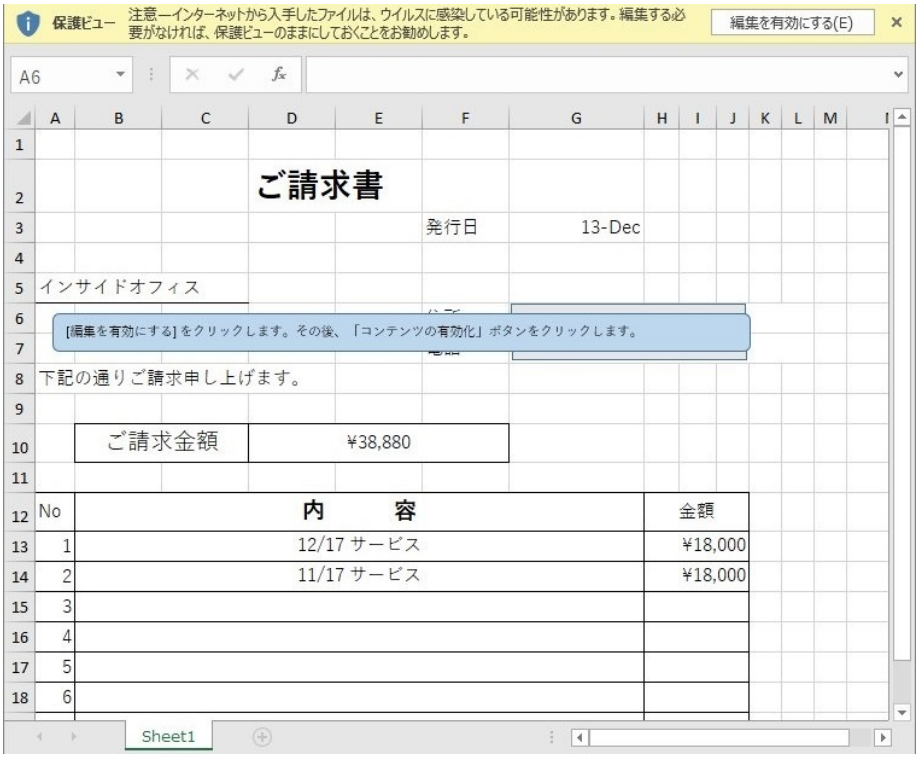
「VBA/TrojanDownloader.Agent」は、日本国内における検出数が他の国と比べて非常に高く、日本在住の方が主なターゲットと考えられます。



VBA/TrojanDownloader.Agent 検出数の国別割合（2017 年 12 月）

「VBA/TrojanDownloader.Agent」の主な感染経路はメールです。メールに添付されている「VBA/TrojanDownloader.Agent」を開くと、最終的に「Win32/Spy.Ursnif」がダウンロードされ実行されます。また、メールの中には、実際に存在する企業のサービスを装ったものも確認されています。身に覚えのない不審なメールの添付ファイルや URL リンクは絶対に開かないでください。

「VBA/TrojanDownloader.Agent」が添付されているメール例

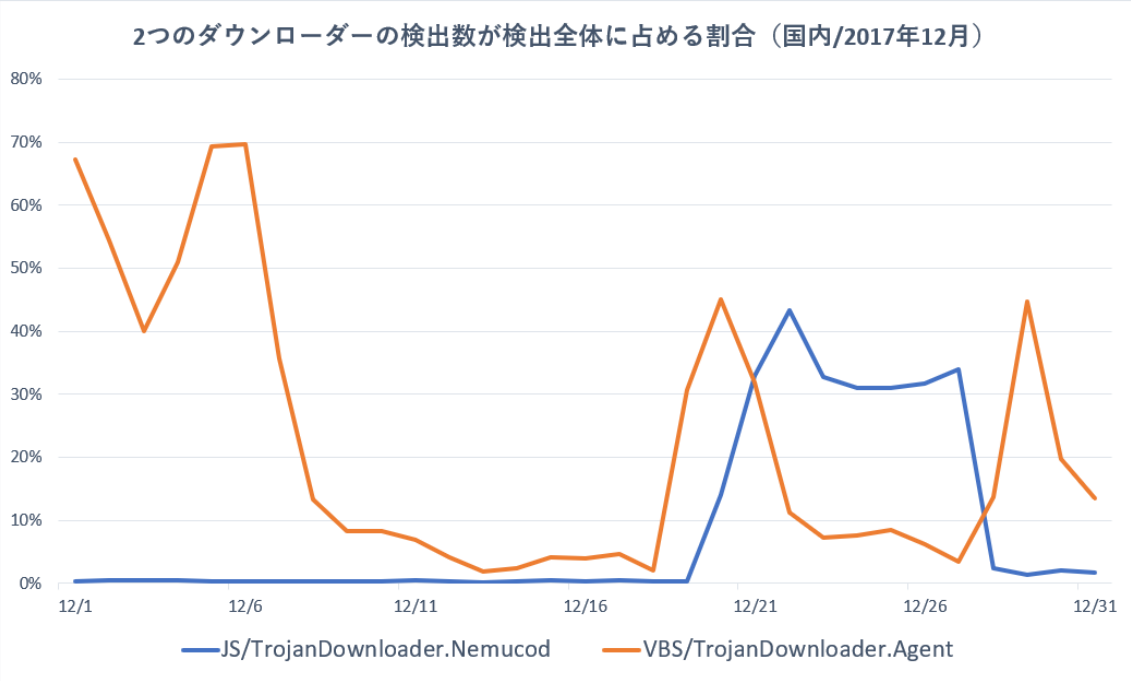


「VBA/TrojanDownloader.Agent」を Microsoft Excel で開いた画面

ESET 製品では、これらのマルウェアを「VBA/TrojanDownloader.Agent」および「Win32/Spy.Ursnif」として検出します。
また、一般社団法人日本サイバー犯罪対策センターの DreamBot・Gozi 感染チェックサイト【試験運用中】では、DreamBot に感染しているかどうかを確かめることができます。

3. ランサムウェアのダウンローダーを数多く確認

12 月はランサムウェアのダウンローダーも数多く検出されました。検出数の推移から、攻撃者が日によって「JS/TrojanDownloader.Nemucod」と「VBS/TrojanDownloader.Agent」との 2 つの形式のダウンローダーを使い分けていることが推測されます。これらのダウンローダーの特徴は、「.7z」形式で圧縮されている点です。広く利用されている「.zip」で圧縮されたファイルはゲートウェイのスパムメールフィルター等でブロックされる可能性が高く、検知を回避するために「.7z」形式を使っているものと考えられます。



2 つのダウンローダーの検出数が検出全体に占める割合（国内/2017 年 12 月）

ダウンロードされるランサムウェアとして、「Win32/Filecoder.Locky」および「Win32/Filecoder.FV（別名 GlobeImposter）」が確認されています。

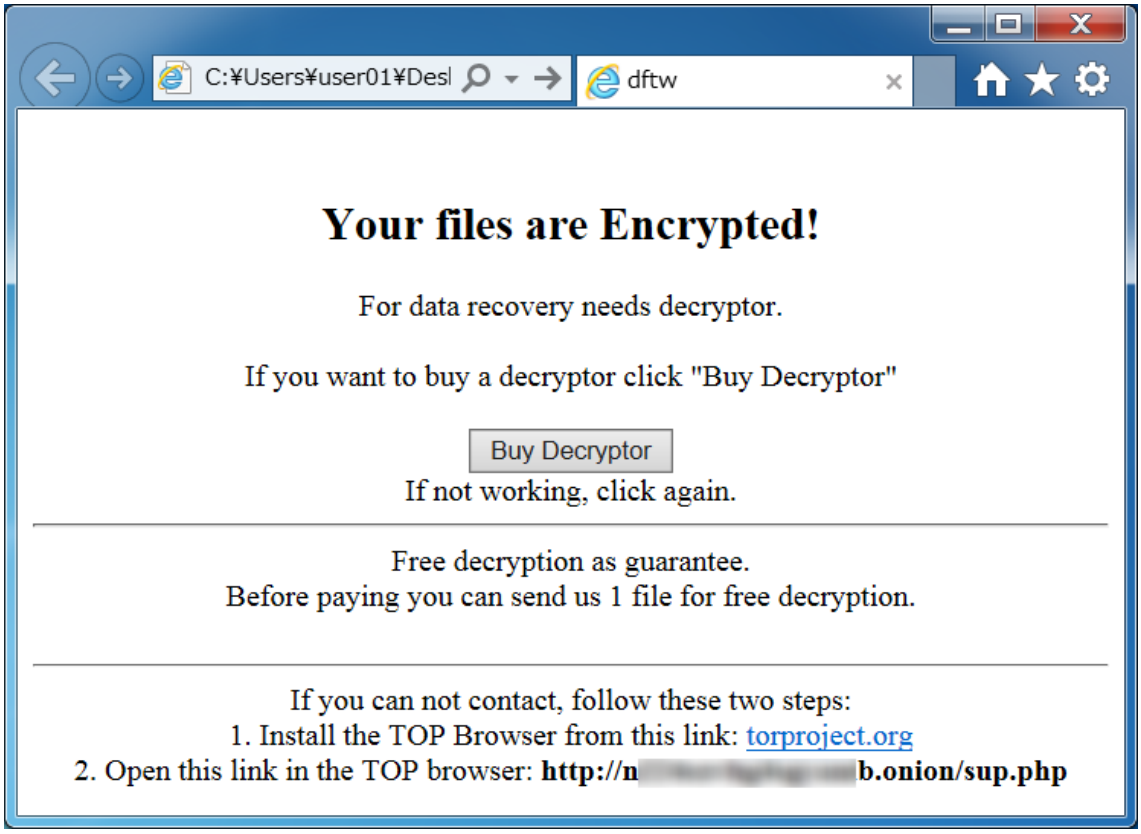
「Win32/Filecoder.Locky」に感染すると、特定の拡張子のファイルが暗号化され、その拡張子は「.asasin」に変更されます。そして身代金要求文書を表示し、ファイルを復号（元に戻す）する条件として金銭の支払いを要求します。

「Win32/Filecoder.Locky」感染時に表示される身代金要求文書

身代金要求文書に記載されている URL にアクセスすると、支払いサイトが表示されます。支払いサイトは様々な言語に対応しており、感染端末が日本語版の Windows であった場合、日本語で表示されます。支払いサイトでは復号ツール「Locky Decryptor」の販売という名目で、身代金を要求します。要求額は 0.5 ビットコインで、日本円にしておよそ 85 万円に相当します。（2018 年 1 月 15 日現在）

「Win32/Filecoder.Locky」の身代金支払いサイト

同様に、「Win32/Filecoder.FV」は PC 上のファイルを暗号化し、ファイルを復号（元に戻す）する条件として金銭の支払いを要求します。この場合の拡張子は「.doc」に変更されます。



「Win32/Filecoder.FV」感染時に表示される画面

2017 年は 1 年間を通してランサムウェアが数多く確認されました。2018 年も引き続き警戒が必要です。万が一ランサムウェアに感染した場合に備えて、日頃からバックアップを取っておくことを推奨します。

ご紹介したように、12 月はバンキングマルウェアやランサムウェアの感染を狙った攻撃が数多く確認されました。常に最新の脅威情報をキャッチアップすることが重要です。

■ 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/