2018年
3月
MARCH

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

インターネットバンキングの認証情報窃取を狙ったマルウェアを多く検出

Canon 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

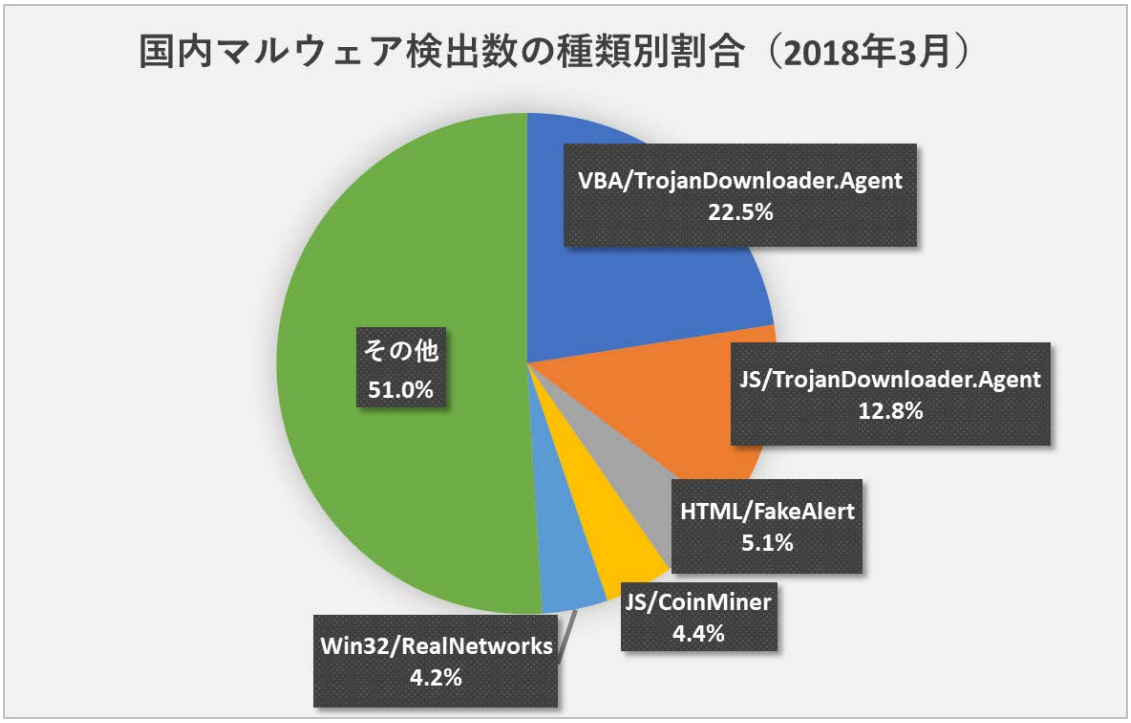
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2018 年 3 月マルウェア検出状況」

1. 3 月の概況について
2. バンキングマルウェア「Ursnif」感染を狙った添付メール攻撃
3. 偽のシステム警告を表示する詐欺サイト

1. 3 月の概況について

2018 年 3 月 1 日から 3 月 31 日までの間、ESET 製品が国内で検出したマルウェアの種類別の割合は、以下のとおりです。



国内マルウェア検出数の比率（2018 年 3 月）

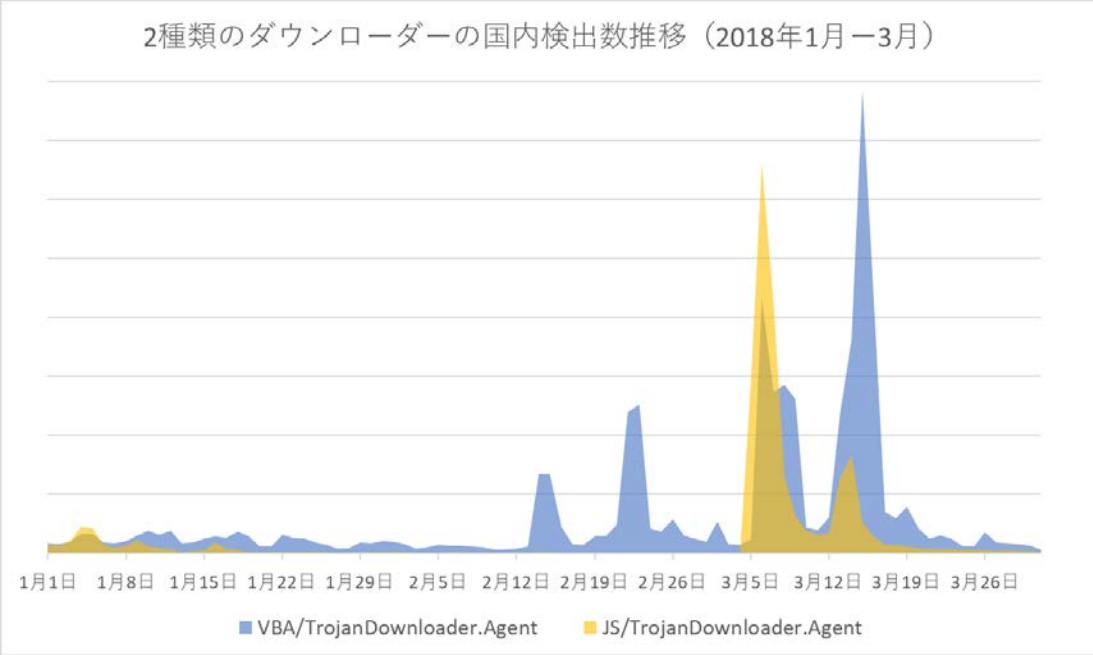
国内マルウェア検出数上位（2018 年 3 月）

順位	マルウェア名	比率	種別
1	VBA/TrojanDownloader.Agent	22.5%	ダウンローダー
2	JS/TrojanDownloader.Agent	12.8%	ダウンローダー
3	HTML/FakeAlert	5.1%	偽の警告文を表示するスクリプト
4	JS/CoinMiner	4.4%	マイニングスクリプト
5	Win32/RealNetworks	4.2%	PUA(※)
6	Suspicious	3.7%	未知の不審ファイル呼称
7	JS/Redirector	3.3%	リダイレクター
8	JS/Adware.Agent	2.1%	アドウェア
9	HTML/IFrame	1.5%	別のページに遷移させるスクリプト
10	Win32/Toolbar.MyWebSearch	1.5%	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。

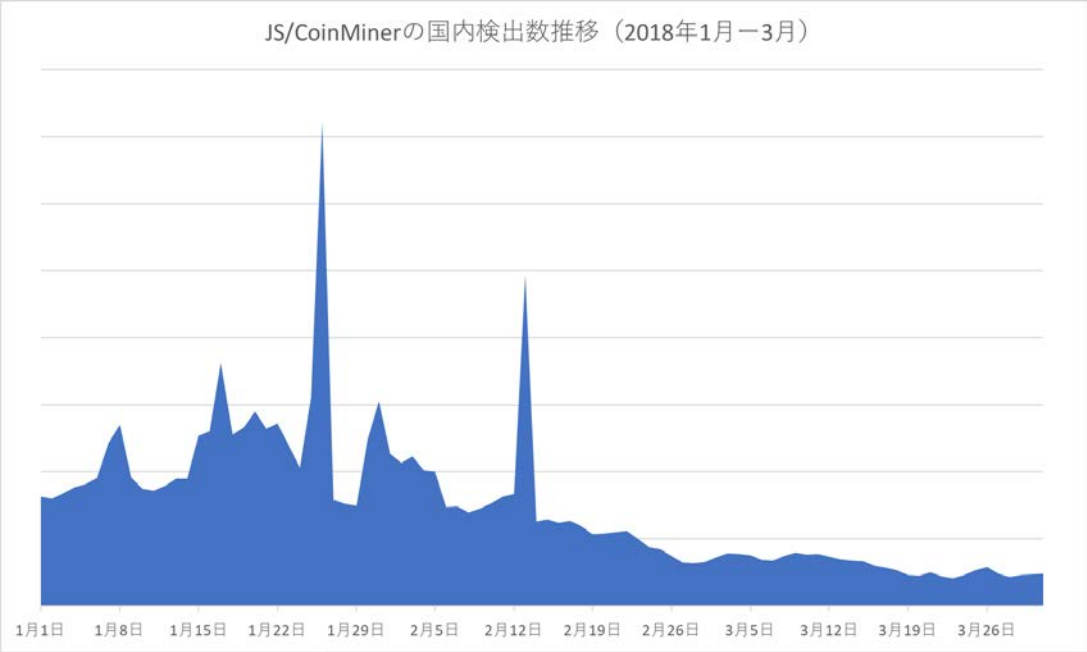
3 月に最も多く検出されたマルウェアは VBA（Visual Basic for Applications）機能を悪用したダウンローダー「VBA/TrojanDownloader.Agent」でした。次いで、JavaScript 形式のダウンローダー

「JS/TrojanDownloader.Agent」が多く検出されています。いずれのダウンローダーも、1 月や 2 月と比較して非常に多く検出されています。



2 種類のダウンローダーの国内検出数推移（2018 年 1 月－3 月）

一方、1 月と 2 月に猛威を奮った JavaScript 形式のマイニングスクリプト「JS/CoinMiner」の検出数は減少傾向にあります。暗号通貨（仮想通貨）の価格下落や、ウイルス対策製品のマイニングスクリプト対策が進んだことにより、攻撃者の利益が減少したことがその背景として考えられます。

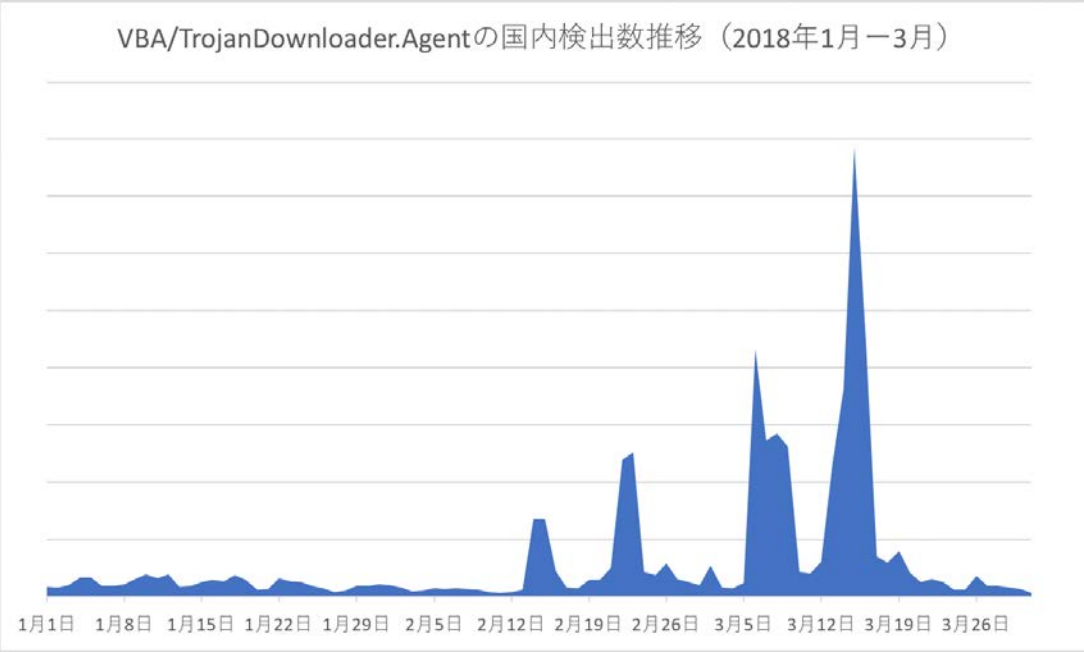


「JS/CoinMiner」の国内検出数推移（2018 年 1 月－3 月）

2. バンキングマルウェア「Ursnif」感染を狙った添付メール攻撃

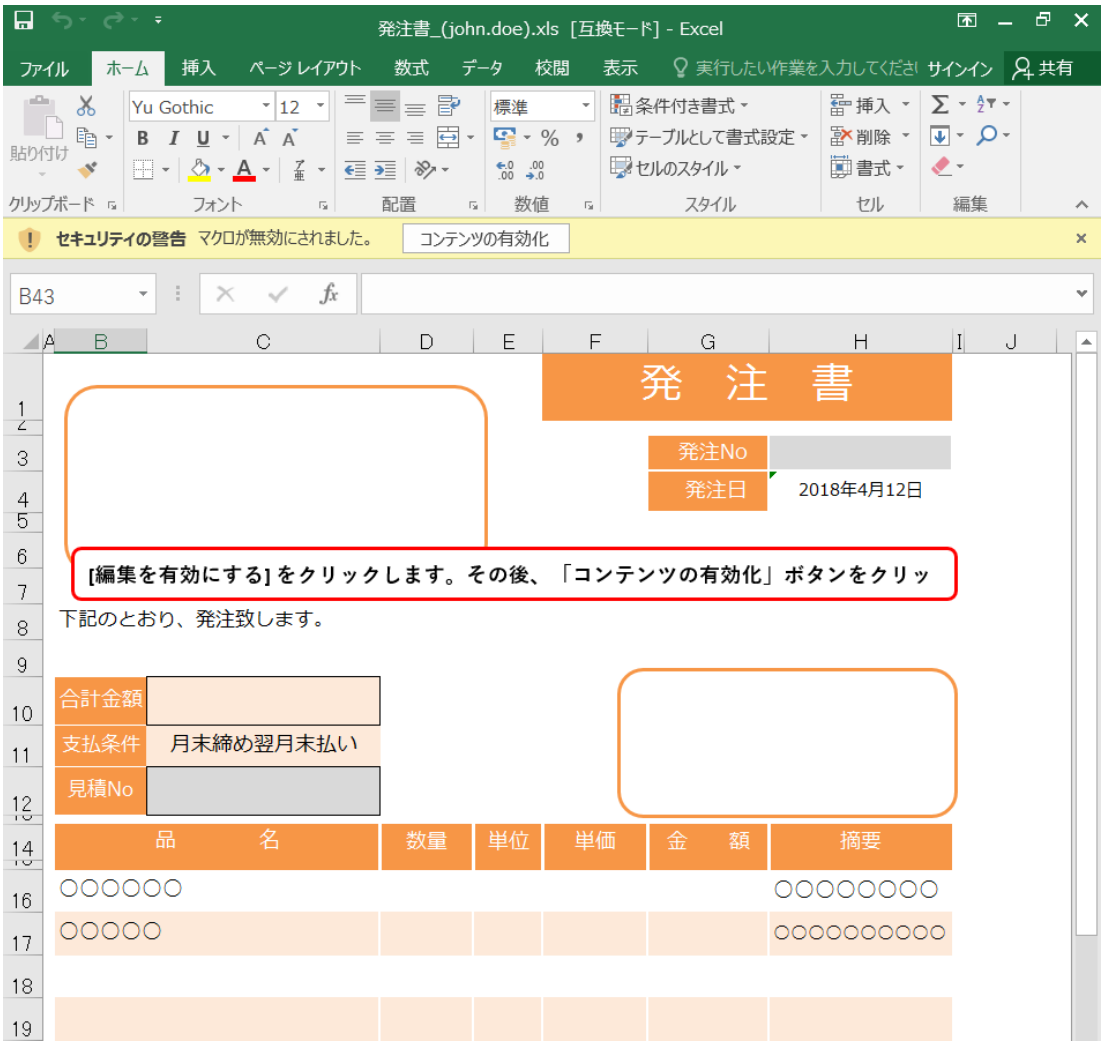
3 月に最も多く検出されたマルウェア「VBA/TrojanDownloader.Agent」は、Microsoft Office の VBA（Visual Basic for Applications）機能を悪用したダウンローダー型のマルウェアで、ファイル形式は Microsoft Word 文書や Microsoft Excel 文書です。

2018 年 1 月以降では、「VBA/TrojanDownloader.Agent」の検出日のピークは 3 月 15 日、次いで 3 月 6 日でした。



VBA/TrojanDownloader.Agent の国内検出数推移（2018 年 1 月－3 月）

「VBA/TrojanDownloader.Agent」の多くは請求書などを装ったメールに直接添付されています。メール本文と添付ファイルの中身がともに日本語で書かれているものを数多く確認しています。



メールに添付された悪性の Microsoft Excel ファイル（「VBA/TrojanDownloader.Agent」）

悪性の Microsoft Excel ファイルに埋め込まれた VBA のコード

悪性の Microsoft Excel ファイルを開きマクロを有効化すると、ファイルに埋め込まれた VBA のコードが別のマル

ウェアをダウンロード・実行します。そして最終的に、バンキングマルウェア「Win32/Spy.Ursnif」に感染します。

「Win32/Spy.Ursnif」は以下のような様々な情報を窃取することを確認しています。

Microsoft Office の標準設定では、VBA コンテンツの実行前に警告が表示されます。もし警告を非表示に設定されている場合は、セキュリティの観点から Microsoft Office のマクロは無効、もしくは警告を表示するよう設定しておくことをおすすめします。

また、「Win32/Spy.Ursnif」の感染を狙ったメール攻撃には、本文中に「Ursnif」のダウンローダーの URL を記載しているパターン もあります。併せて注意が必要です。

3. 偽のシステム警告を表示する詐欺サイト

警告文を表示する詐欺サイト（ESET 検出名：HTML/FakeAlert）が多数検出されています。以下に紹介する事例では、「Windows セキュリティシステムが破損しています」と偽の警告メッセージを表示し、PC 修復ツールと称したソフトウェアをユーザーに購入させようとします。

偽のシステム警告画面

偽のシステム警告画面を表示する攻撃では、悪質な広告からのリダイレクトやタイポスクワッティング（※）により、ユーザーをこの Web ページへ誘導します。Web ページは閉じることができないよう細工されており、ユーザーの不安を煽ります。警告画面の指示通りに[更新]をクリックするとソフトウェアのダウンロードページに遷移してしまいますので、このような Web ページに遭遇した場合は、タスクマネージャーからウィンドウを閉じてください。

（※）著名なドメインに似たドメインを取得し、URL をタイプミスしたユーザーを偽サイトに呼び込む攻撃手法のこと。
【例】example.com（正規のサイト） に対して example.cm（偽サイト）

PC 修復ツールと称したソフトウェアのダウンロードページ

偽のシステム警告画面で［更新］をクリックした際に表示される、PC 修復ツールと称したソフトウェアのダウンロードページです。

[今すぐダウンロード]ボタンをクリックすると、ソフトウェアのインストーラーがダウンロードされます。インストーラーを実行し画面の指示に従いインストールを進めると、システムに問題が見つかったことを伝えるメッセージが表示されます。

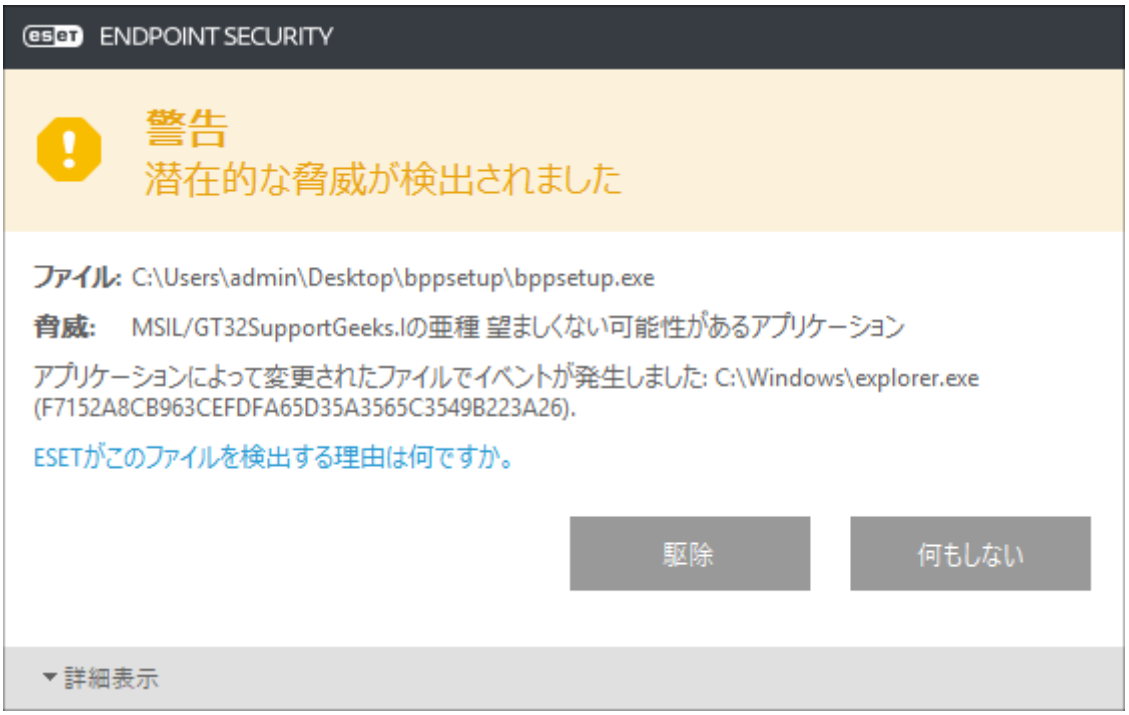
PC 修復ツールと称したソフトウェアの画面

更に画面の指示に従うと、Web ブラウザーでソフトウェアの購入ページが開かれます。購入ページでは、クレジットカードなどの支払い情報の入力を要求されます。

PC 修復ツールと称したソフトウェアの購入ページ

個人情報の入力をする場合は、そのサイトが信頼できるサイトかどうかを慎重に確認してください。

ESET 製品は、ダウンロード時にこのソフトウェアを「MSIL/GT32SupportGeeks 望ましくない可能性があるアプリケーション」として検出します。



ESET Endpoint Security V6.5 における検出画面

ご紹介したように、3 月はバンキングマルウェア「Ursnif」の感染を狙ったメールや、偽の警告メッセージを表示する詐欺サイトが確認されました。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/