2018年
7月
JULY

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

Google を装った詐欺サイト

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

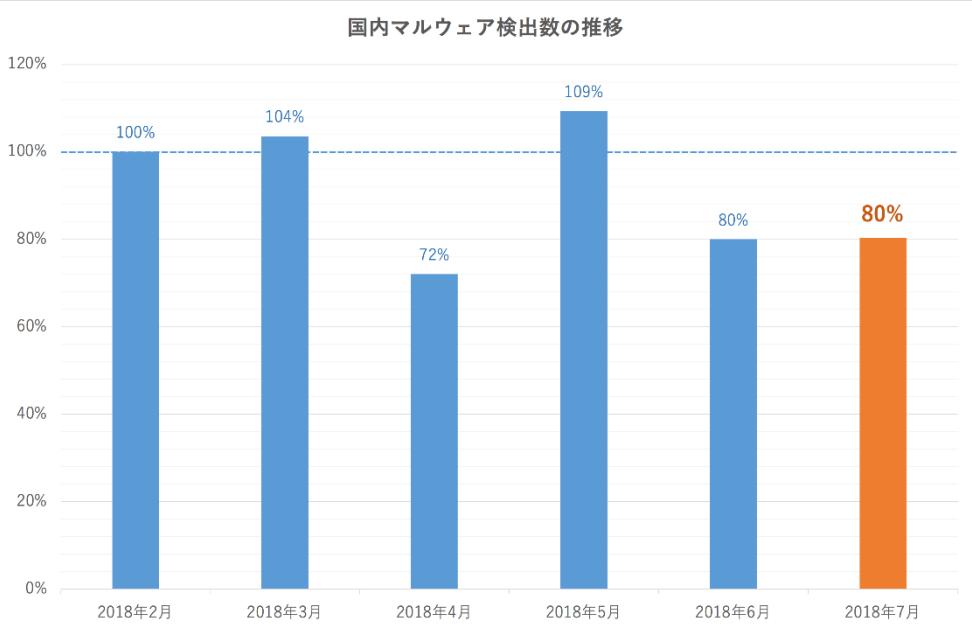
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2018 年 7 月マルウェア検出状況」

1. 7 月の概況について
2. バンキングマルウェア Ursnif 感染を狙う新たな攻撃
3. Google を装った詐欺サイト

1. 7 月の概況について

過去半年間の月別推移から見た、2018 年 7 月（7 月 1 日～7 月 31 日）に ESET 製品が国内で検出したマルウェアの検出数は以下のとおりです。



国内マルウェア検出数の推移(※1)**（2018 年 7 月）**

（※1） 2018 年 2 月の検出数を 100%として比較

7 月の国内マルウェア検出数は 6 月と同等であり、過去半年間では比較的落ち着いていました。

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上位（2018 年 7 月）

順位	マルウェア名	比率	種別
1	VBA/TrojanDownloader.Agent	14.9%	ダウンローダー
2	JS/Adware.Agent	9.8%	アドウェア
3	JS/Redirector	4.8%	リダイレクター
4	HTML/FakeAlert	4.8%	偽の警告文を表示するスクリプト
5	JS/Mindspark	4.3%	アドウェア
6	JS/CoinMiner	3.7%	マイニングスクリプト
7	Suspicious	3.2%	未知の不審ファイル呼称
8	HTML/ScrInject	3.0%	リダイレクター
9	VBS/Danger.DoubleExtension	2.4%	二重拡張子をもつ VBScript
10	VBS/TrojanDownloader.Agent	2.4%	ダウンローダー

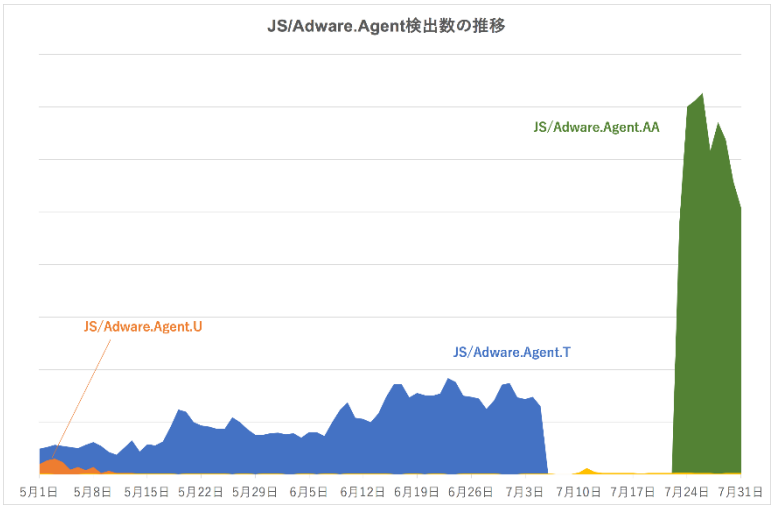
＊ ファミリー名の詳細については ESET 製品サポート情報をご参照ください。

7 月に最も検出されたマルウェアは、Microsoft Office のマクロ機能を悪用したダウンローダーである

「VBA/TrojanDownloader.Agent」でした。主にメールの添付ファイルとして多数拡散されています。

次いで検出数の多かった「JS/Adware.Agent」はブラウザ上で不正広告を表示する JavaScript で、7 月の検出数は 6 月の 1.7 倍近くに達しています。

「JS/Adware.Agent」の検出数の推移は以下のとおりです。



JS/Adware.Agent 検出数の推移

この「JS/Adware.Agent」ファミリーのマルウェアは、5 月、6 月に検出数の多数を占めていた「JS/Adware.Agent.U」や「JS/Adware.Agent.T」ではなく、7 月下旬に新たに出現した「JS/Adware.Agent.AA」でした。このことから、次々と新たな不正広告スクリプトが開発・利用されていることが推測されます。

「JS/Adware.Agent」はメールに添付されて拡散される JavaScript ファイルとは異なり、広告収入を得ようとしている Web ページに埋め込まれています。そのため、Web ページの閲覧中にブラウザ上で自動的に実行され、ユーザーの特別な操作が実行のトリガーとならないことが特徴です。ESET 製品は Web ページの閲覧中にこれらの JavaScript ファイルを検出・遮断し、実行を防ぎます。

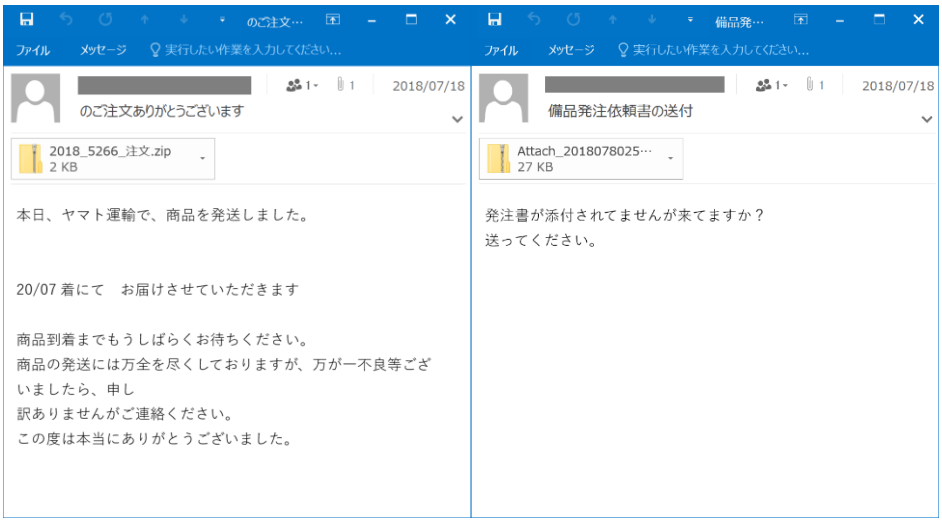
2. バンキングマルウェア Ursnif 感染を狙う新たな攻撃手法

2018 年は 2017 年に引き続き、バンキングマルウェア Ursnif への感染を狙うばらまき型メール攻撃を多数確認しています。Ursnif に感染するとインターネットバンキングの認証情報（ユーザーID やパスワード等）やクレジットカード情報を窃取され、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。

多くの場合、Microsoft Office 文書や JavaScript ファイルがメールに添付されており、それらを開くと Ursnif がダウンロード・実行されます（参考情報：2018 年 3 月のマルウェアレポート）。

7 月は、すでに広く対策が行われているそれらの手法ではなく、他のファイル形式や判読不能な画像ファイルを用いた攻撃が観測されました。

今回の攻撃では、VBScript ファイルに加え、PDF ファイルもしくは画像ファイルが、1 つの ZIP ファイルに圧縮されてメールに添付されていました。



ZIP ファイルが添付された不審メール

メールに添付されていた ZIP ファイルの内容

メールの件名は、「ご確認下さい」「備品発注依頼書の送付」「のご注文ありがとうございます」「Fw: 資料」などが確認されており、本文も様々です。

PDF ファイルや画像ファイルはダミーで、何も書かれていないページや、ぼかしのような加工がされており判読不能な画像が記載されています。

メールに添付されていた判読不能な画像

これは、判読不能な画像をあえて添付することで、同梱された VBScript ファイルを実行させるよう誘導を試みた可能性があります。

VBScript ファイルは JavaScript ファイルと同様に、Windows のスクリプト実行機能 WSH（Windows Script Host）を用いて実行されます。この VBScript ファイルを実行すると PowerShell スクリプトがダウンロード・実行され、最終的にバンキングマルウェア Ursnif がダウンロード・実行されます。VBScript を実行しなければ、Ursnif には感染しません。

ESET 製品では、この一連のマルウェアを以下のような名称で検出します。

- VBS/TrojanDownloader.Agent.PUO（VBScript ファイル）
- PowerShell/TrojanDownloader.Agent.ASS（PowerShell スクリプト）
- PowerShell/TrojanDownloader.Agent.ATE（PowerShell スクリプト）
- Win32/Spy.Ursnif.AO（Ursnif）
- Generik.JOIJUAD の亜種（Ursnif）

VBScript を日常的に使用していない場合は、以下のような対策によって感染を防ぐことが可能です。

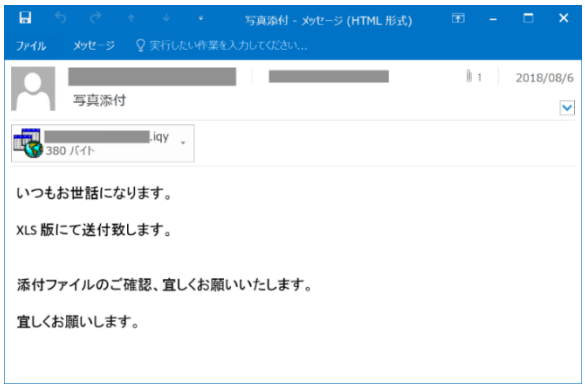
- VBScript ファイル(.vbs, .vbe）の関連付けをメモ帳などに変更して、VBScript ファイルをダブルクリックしても VBScript が実行されないようにする（詳細については 2018 年 2 月のマルウェアレポートをご参照ください）。
- グループポリシー(ソフトウェアの制限や AppLocker）を利用して、wscript.exe やスクリプトファイルの実行を制限する。
- メールサーバーで VBScript ファイルおよび VBScript ファイルが含まれる ZIP ファイルを受信しないよう設定する。

VBScript ファイルを日常的に使用している場合は、実行しようとしている VBScript ファイルが正当なものかどうか十分に確認してから実行してください。また、VBScript ファイルをメールで送受信しないといった運用面でのリスク回避も実施が望まれます。

加えて、個別の攻撃手法に対する対策だけではなく、新たな攻撃にも対応できるよう以下のような心構えを持っておくことも重要です。

- 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マルウェアかどうか疑い、安易に開かない。
- 見慣れないファイルはマルウェアかどうか疑い、安易に開かない。

また、8 月上旬には Excel の Web クエリ機能で用いられる Web クエリファイル（.iqy ファイル）を用いた攻撃も観測されました。



Web クエリファイルが添付されたメール

メールの件名は、「写真添付」「写真送付の件」「ご確認ください」「お世話になります」といったものが確認されています。

この Web クエリファイルを開くと、Excel の Web クエリ機能（Web 上のデータをダウンロードして計算に利用する機能）と外部参照機能（他の Excel ファイルや Excel 以外のプログラムのデータを利用する機能）、コマンドプロンプト、PowerShell を次々に使用して最終的に Ursnif がダウンロード・実行されます。

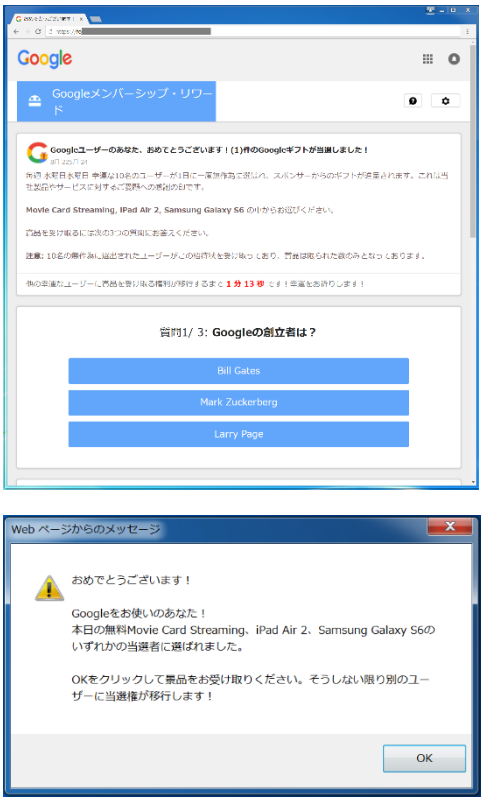
こちらの攻撃については、8 月のマルウェアレポートで詳しく解説します。

バンキングマルウェア感染を狙う攻撃手法は日々変化しています。一つの対策のみに頼らず、複数の対策を講じていくことが重要です。

3. Google を装った詐欺サイト

7 月は、Google を装った詐欺サイトが多数確認されました。
この事例では、

① ネットサーフィン中に、今まで見ていたページから別のページに遷移し、景品に当選したことを示すポップアップウィンドウが表示されます。



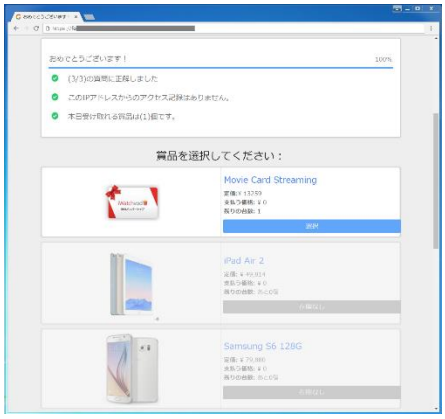
（上）Google を装った詐欺サイトの当選画面、（下）ポップアップウィンドウ

ページが突如移動した原因としては、ネットサーフィン中に閲覧していたサイトにリダイレクト（ページを移動させる）広告が存在していたことが考えられます。

詐欺サイトは、Google を装ったデザインになっており、Google ギフトに当選したことが記されています。しかし、このサイトのドメイン名に、「Google」は含まれていません。

ここでは、景品を受け取るために、3 つのクイズに答えることが要求されています。図（上）の赤文字部分には、この当選が無効となるまでの時間が示されており、カウントダウンすることでクイズへの回答を急かします。

② 3 つのクイズに回答すると、正誤関係なく景品の選択画面が表示されます。



詐欺サイトの景品選択画面

景品は、3 つの選択肢のうち 1 つしか選択することができません。また、選択できる景品は、在庫数が 1 になっており、売り切れる直前であることを演出し、ここでも閲覧者を急かします。

③ 景品を選択すると、個人情報を入力する別のサイトに移動します。

個人情報入力サイト

ここでは、氏名、住所、クレジットカードといった個人情報の入力が求められます。また、5 日以内に契約をキャンセルしなければ、毎月 45.95 US ドル（約 5,000 円）が発生すると記されています。

もし、クレジットカードなどの個人情報を入力してしまった場合、攻撃者によって情報を収集され、悪用される可能性が考えられます。加えて、景品を受け取れない可能性も高いです。

Google を装った詐欺サイトと個人情報を入力するサイトは、ドメイン名、ページデザイン、当選する景品などが頻繁に変更されおり、本記事で紹介したものは、一例です。また、8 月下旬においても、同様の詐欺サイトが依然として確認されているため、引き続き注意が必要です。

個人情報を入力する際は、そのサイトが信頼できるサイトであるかどうか慎重に確認することが重要です。また、今回のような有名サイトを装ったフィッシングの対策には、以前にマルウェア情報局で掲載した「フィッシング詐欺にだまされないための 5 つの方法」を参照してください。このような詐欺サイトは日々新規に作成されています。
ESET 製品は、新規に作成されるフィッシングサイトにも随時対応していきますが、お客さま自身でも十分にご注意ください。

ご紹介したように、今月はバンキングマルウェア感染を狙う新たな攻撃や Google を装った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/