2017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

ソフトウェアの脆弱性を悪用した攻撃を検出

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

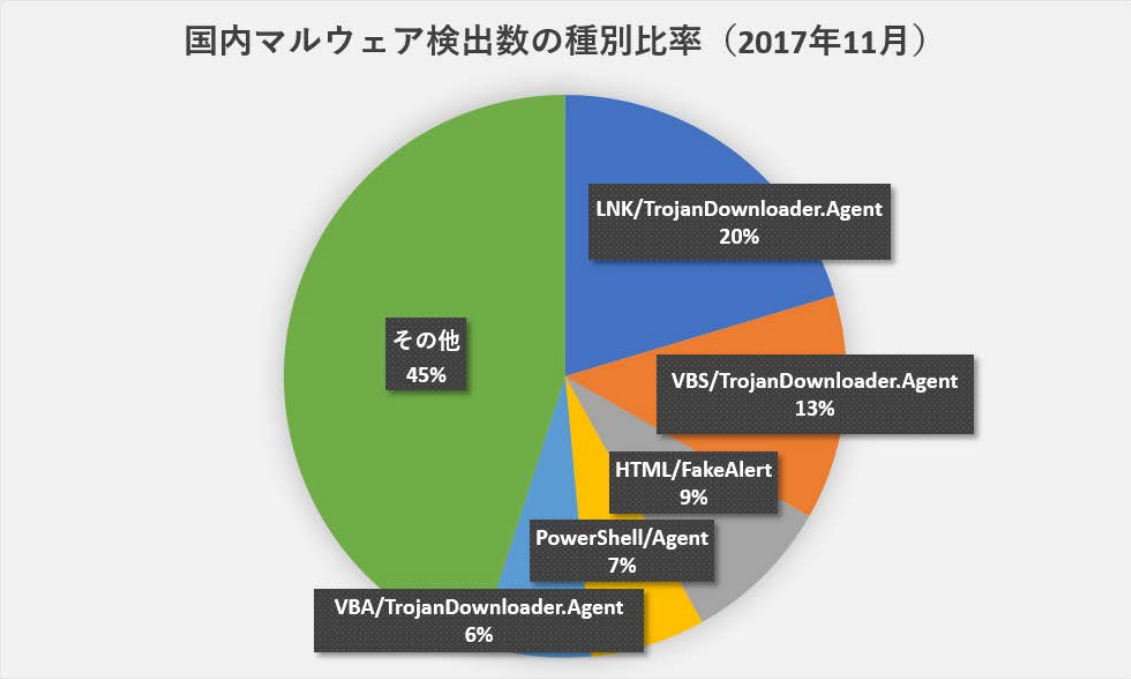
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2017 年 11 月マルウェア検出状況」

1. 11 月の概況について
2. Microsoft Office 数式エディターの脆弱性を悪用した攻撃の出現
3. Windows Movie Maker を改ざんした偽プログラムの増加

1. 11 月の概況について

2017 年 11 月 1 日から 11 月 30 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 11 月）

順位	マルウェア名	比率	種別
1	LNK/TrojanDownloader.Agent	20%	ダウンローダー
2	VBS/TrojanDownloader.Agent	13%	ダウンローダー
3	HTML/FakeAlert	9%	偽の警告文表示
4	PowerShell/Agent	7%	トロイの木馬
5	VBA/TrojanDownloader.Agent	6%	ダウンローダー
6	PowerShell/TrojanDownloader.Agent	3%	ダウンローダー
7	JS/Redirector	3%	リダイレクター
8	VBA/DDE	2%	ダウンローダー
9	Suspicious	2%	未知の不審なファイル
10	Win32/RiskWare.PEMalform	2%	PUA(※)
⋮			
14	Win32/Exploit.CVE-2017-11882	1%	エクスプロイト

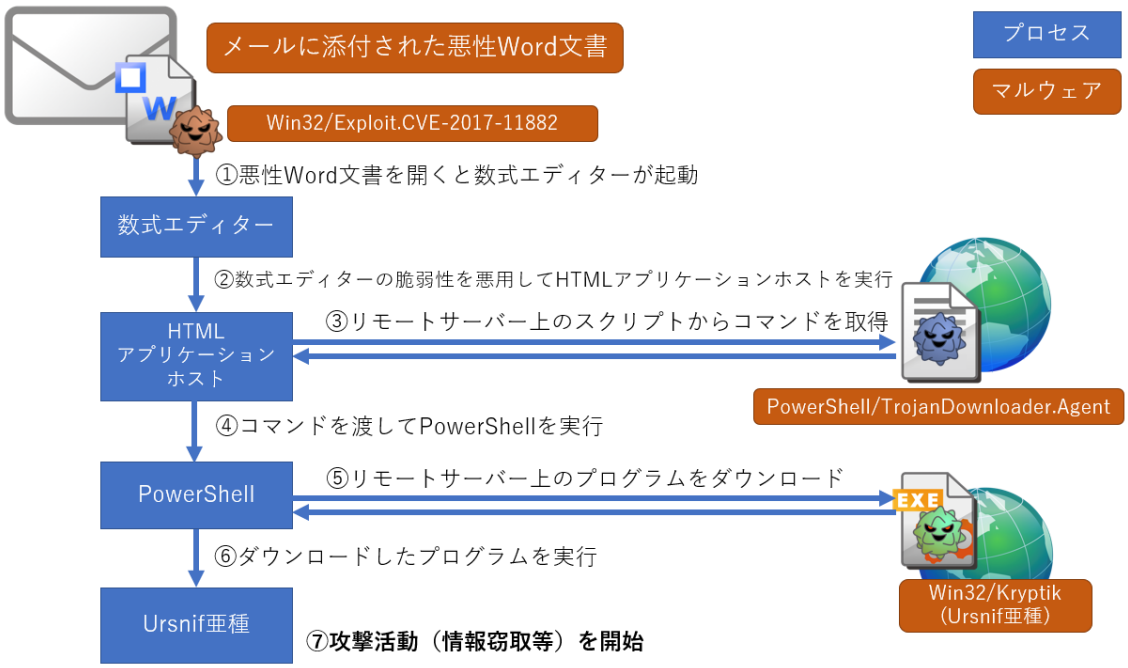
（※）Potentially Unwanted Application(望ましくない可能性のあるアプリケーション)：コンピューターの動作に悪影響を及ぼすことや、ユーザーが意図しない振る舞いなどをする可能性があるアプリケーション。

11 月に国内で最も多く検出されたマルウェアは「LNK/TrojanDownloader.Agent」（LNK 形式のダウンローダー）です。LNK 形式のダウンローダーは、Windows に標準で搭載されている cmd.exe や powershell.exe を悪用し、別のマルウェアをダウンロードします。また、10 月に増加した「VBA/DDE」が 11 月も多く検出されました。

2. Microsoft Office 数式エディターの脆弱性を悪用した攻撃の出現

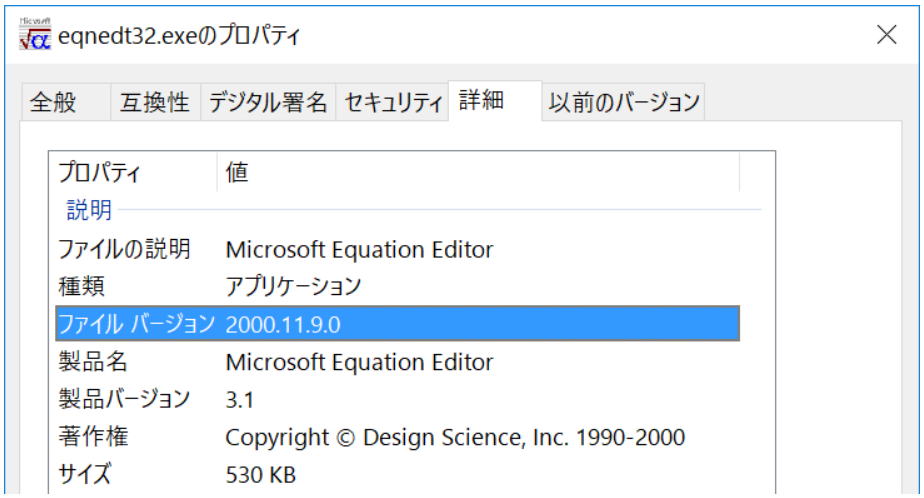
11 月から 12 月にかけて、Microsoft Office 数式エディターに存在する脆弱性（CVE-2017-11882）を悪用した攻撃が新たに確認され、その検出数は 11 月度では 14 位でした。

具体的には、メールに添付された本脆弱性への攻撃コードを含む悪性の Word 文書が、「Ursnif（アースニフ）」と呼ばれるバンキングマルウェア（バンキングサイトの認証情報等を窃取するマルウェア）のダウンローダーとして使われた事例を確認しています。ESET 製品では、悪性 Word 文書を「Win32/Exploit.CVE-2017-11882」として検出し、その後の脅威を防ぎます。



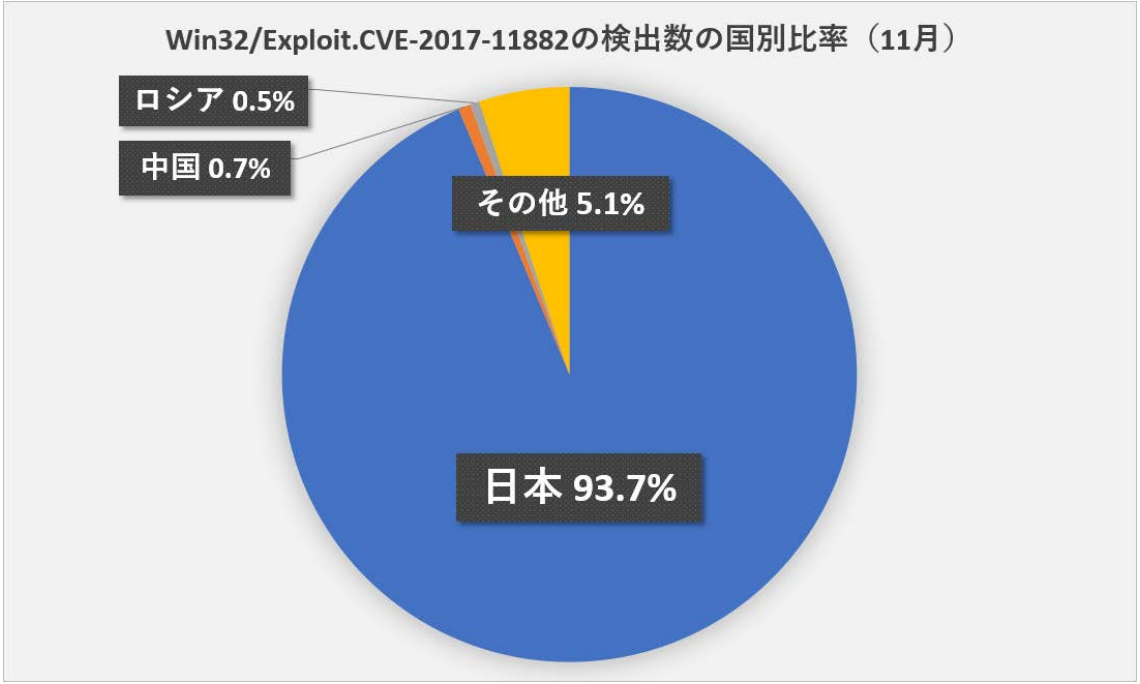
Microsoft Office 数式エディターの脆弱性を悪用した攻撃の事例

数式エディターは Microsoft Office 2003 以前のバージョンの Microsoft Office で数式を入力するために搭載されたソフトウェアで、Microsoft Office 2007 以降においても互換性を確保するために搭載されています。このソフトウェアは 2000 年以来一度も更新されていませんでした。



脆弱性を含む eqnedt32.exe（数式エディター）のプロパティ情報

本脆弱性を悪用した攻撃（ESET 検出名：Win32/Exploit.CVE-2017-11882）はとくに日本国内における検出が顕著で、日本のユーザーを狙った攻撃に多く使われました。



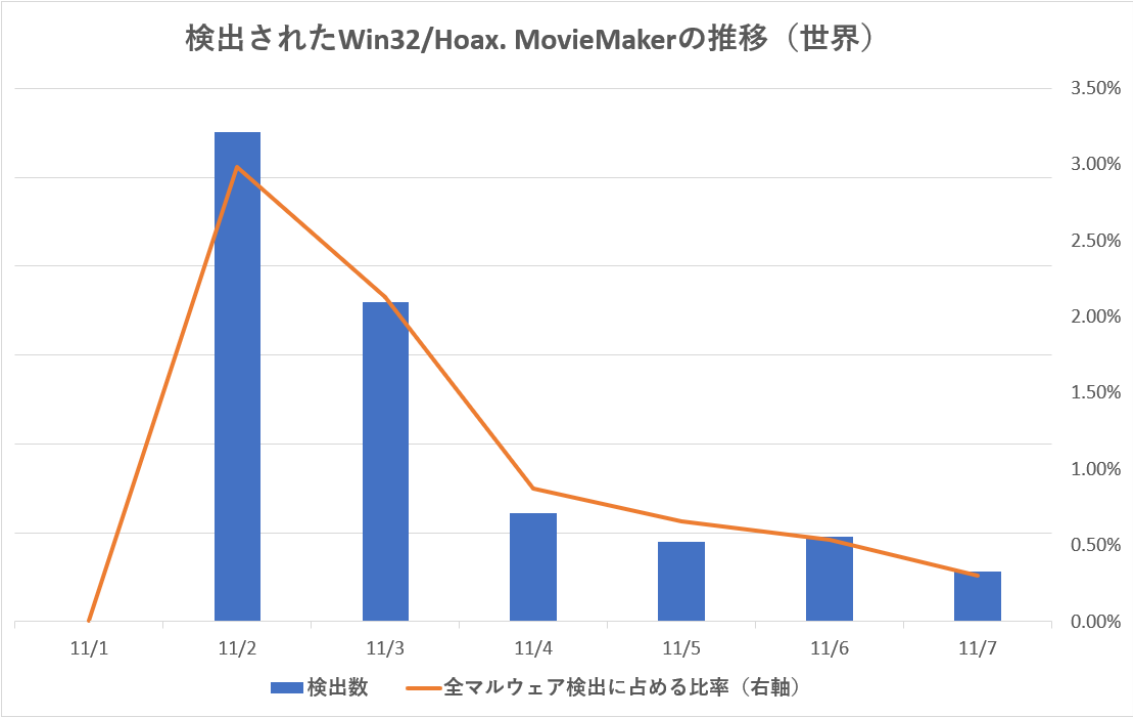
Win32/Exploit.CVE-2017-11882 の検出数の国別比率（11 月）

この脆弱性に対する修正プログラム は既に公開されています。未適用の場合、速やかに適用されることを推奨します。

すぐに修正プログラムを適用できない場合は、Microsoft Office の数式エディターを無効にする ことを推奨します。ESET マルウェアラボでは、数式エディターを無効にすることで、本脆弱性に対する攻撃を回避できることを確認しています。

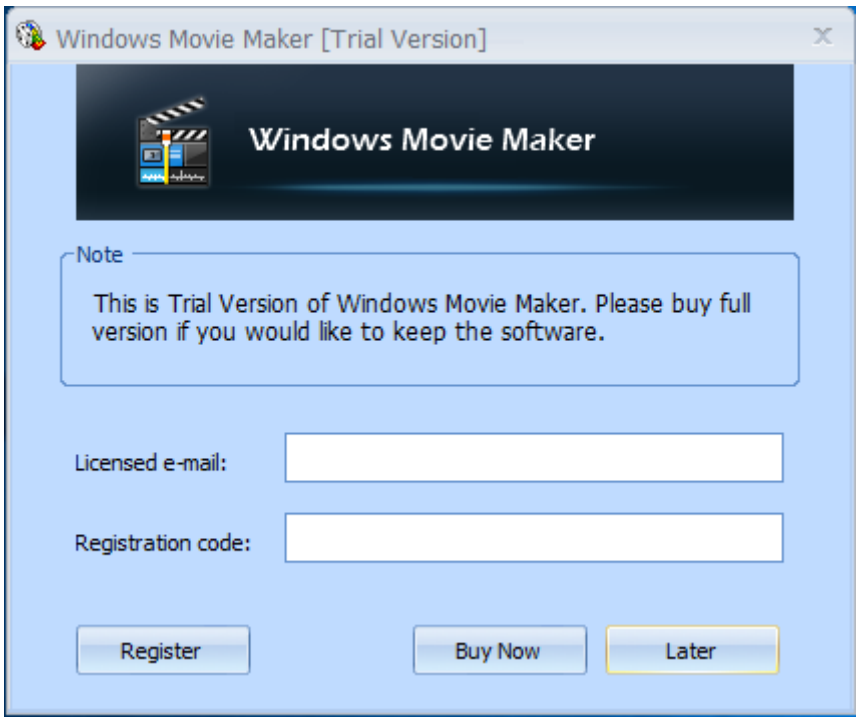
3. Windows Movie Maker を改ざんした偽プログラムの増加

11 月上旬に「Windows Movie Maker」を改ざんした偽プログラムの検出が増加しました。検出が急増した偽プログラム（ESET 検出名：Win32/Hoax.MovieMaker）は 11 月初めに検出が増加し、11 月 2 日には Win32/HoaxMovieMaker が世界で検出されたすべてのマルウェアのうち、3 番目に多く検出されたマルウェアとなりました。



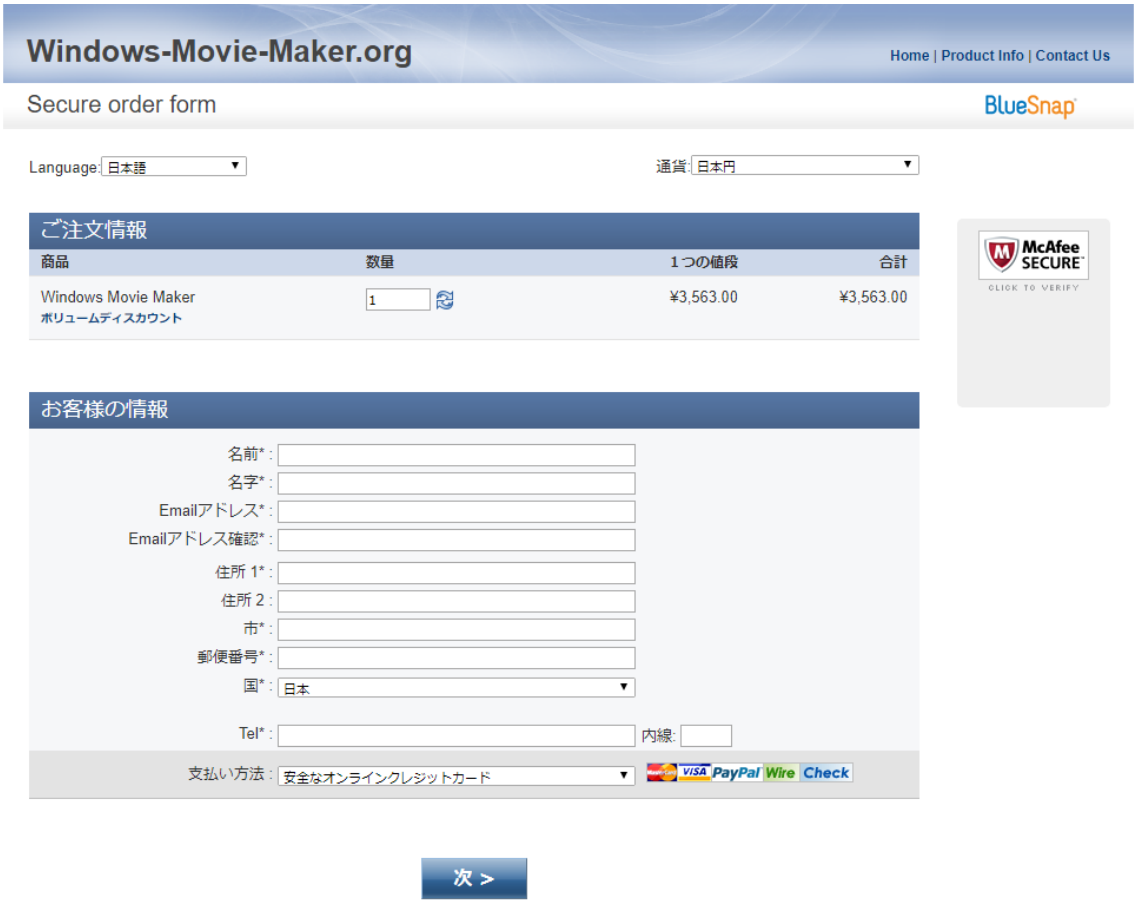
検出された Win32/Hoax. MovieMaker の推移（世界）

この偽プログラムは、すでに配布が終了している Microsoft 社製の無料ビデオ編集ソフトウェア「Windows Movie Maker」を改ざんして作成されており、実行すると「Windows Movie Maker」のトライアルバージョンを装ったプログラムがインストールされます。
そして、プログラム起動時に、フルバージョンの偽プログラムを購入するように要求するメッセージを表示します。



偽プログラムを購入するよう要求するメッセージ

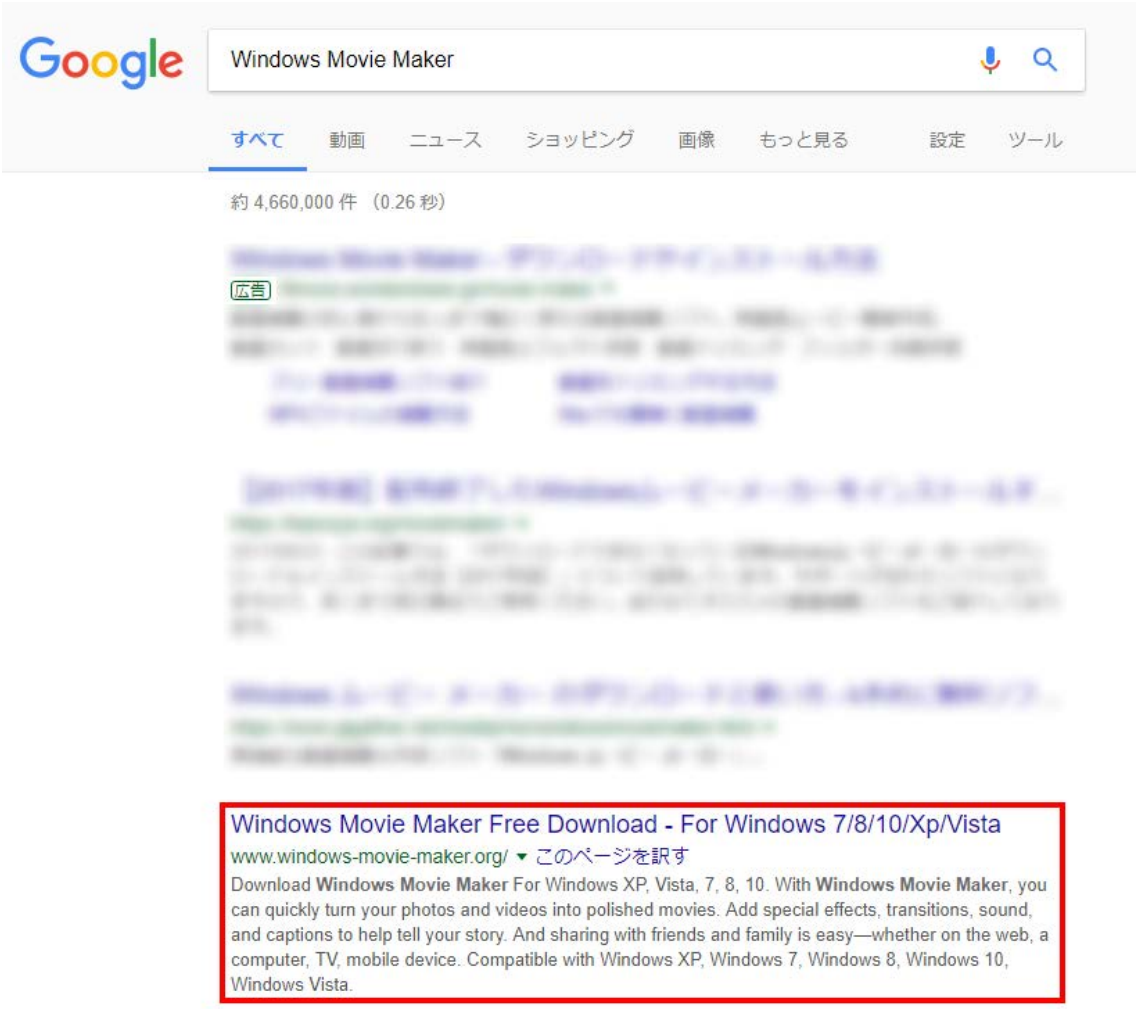
表示されたメッセージにある購入ボタン（[Buy Now]ボタン）をクリックすると購入ページが表示され、フルバージョンの偽プログラムを購入するために、住所や氏名、クレジットカード番号の入力を要求します。



偽プログラムを購入させるための個人情報の入力画面

この「Windows Movie Maker」を改ざんした偽プログラムの検出が急増した原因の 1 つとして、偽プログラムを配布しているウェブサイトが、検索サイトの検索結果で上位に表示されるようになっていたことが考えられます。

具体的には、11 月上旬に Google や Bing などの検索サイトで "Movie Maker" を検索すると、偽プログラムを配布しているウェブサイトが検索結果の上位に表示されていました。
そのため、多くのユーザーが攻撃者の用意したウェブサイトにアクセスし、偽プログラムをダウンロードしたものと考えられます。

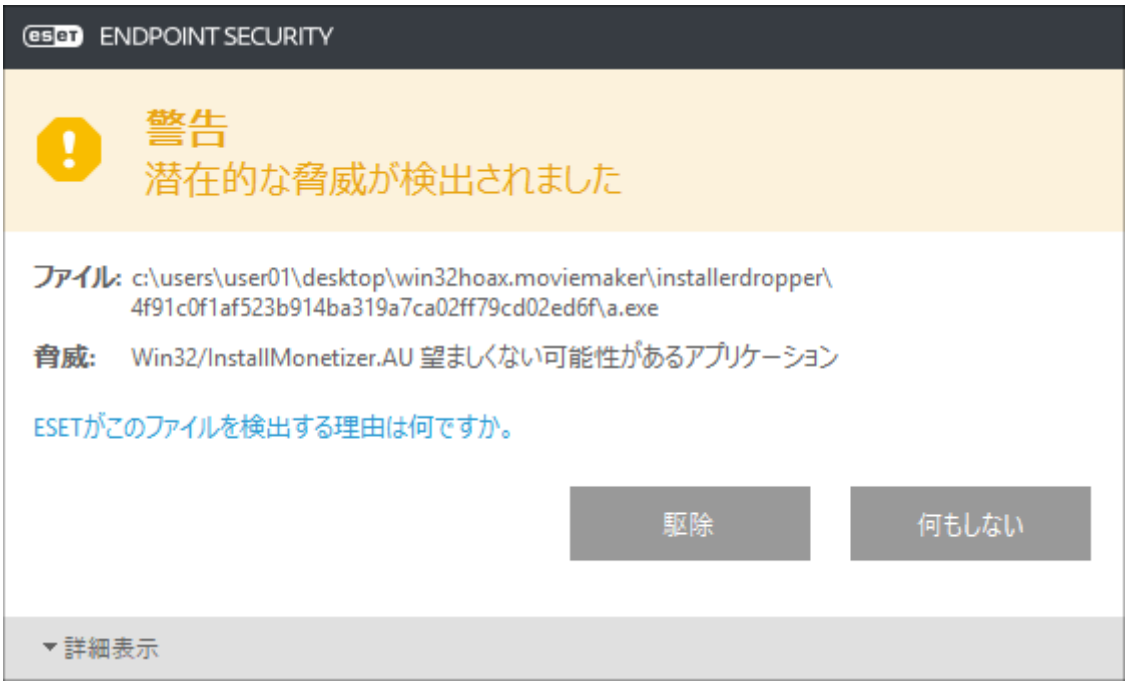


検索サイトでの”Movie Maker”の検索結果表示

ソフトウェアのダウンロードや、個人情報の入力の際は、そのサイトが信頼できるサイトであるかどうかを慎重に確認してください。

ESET 製品では、この偽プログラムを「Win32/Hoax.MovieMaker」または「Win32/InstallMonetizer.AU」という名前で検出します。
また、この偽プログラムをダウンロードするウェブサイトにアクセスした場合、ESET 製品が通信をブロックします。

Win32/Hoax.MovieMaker の検出画面（ESET ENDPOINT SECURITY）



Win32/InstallMonetizer.AU の検出画面（ESET ENDPOINT SECURITY）

ご紹介したように、11 月はソフトウェアの脆弱性を狙った攻撃や偽のプログラムを配布する攻撃が確認されました。
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/