2018年
1月
JANUARY

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

マイニングマルウェア「JS/CoinMiner」の爆発的流行

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

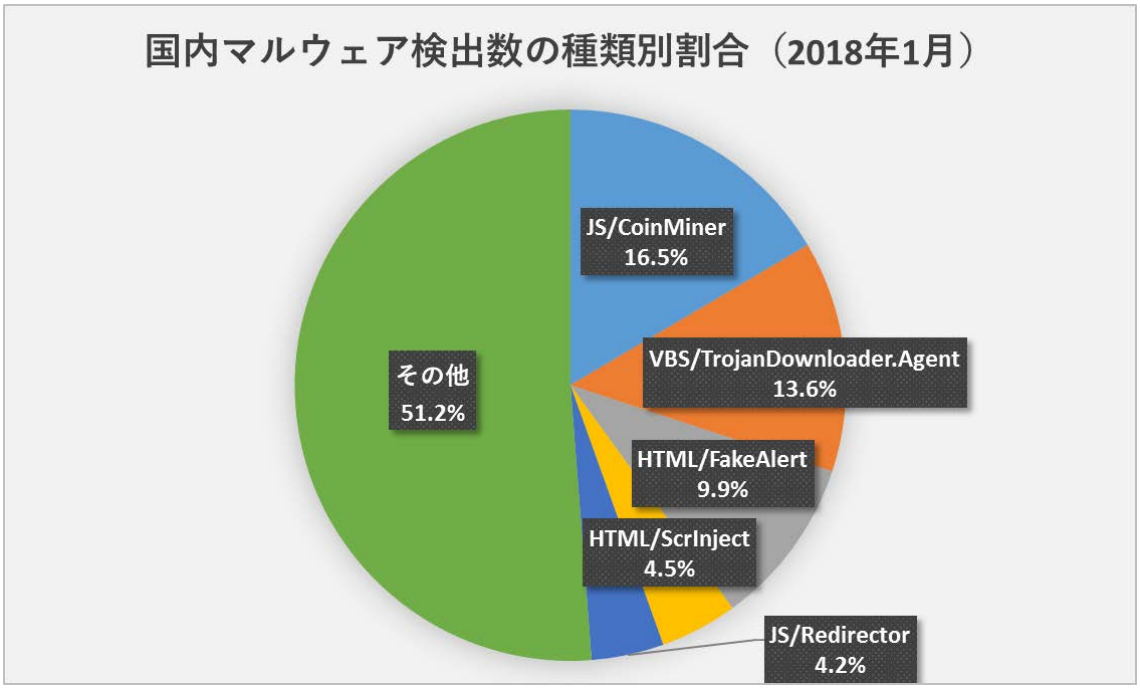
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2018 年 1 月マルウェア検出状況」

1. 1 月の概況について
2. マイニングマルウェア「JS/CoinMiner」の爆発的流行
3. 脆弱性を悪用した攻撃の種類が増加

1. 1 月の概況について

2018 年 1 月 1 日から 1 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。



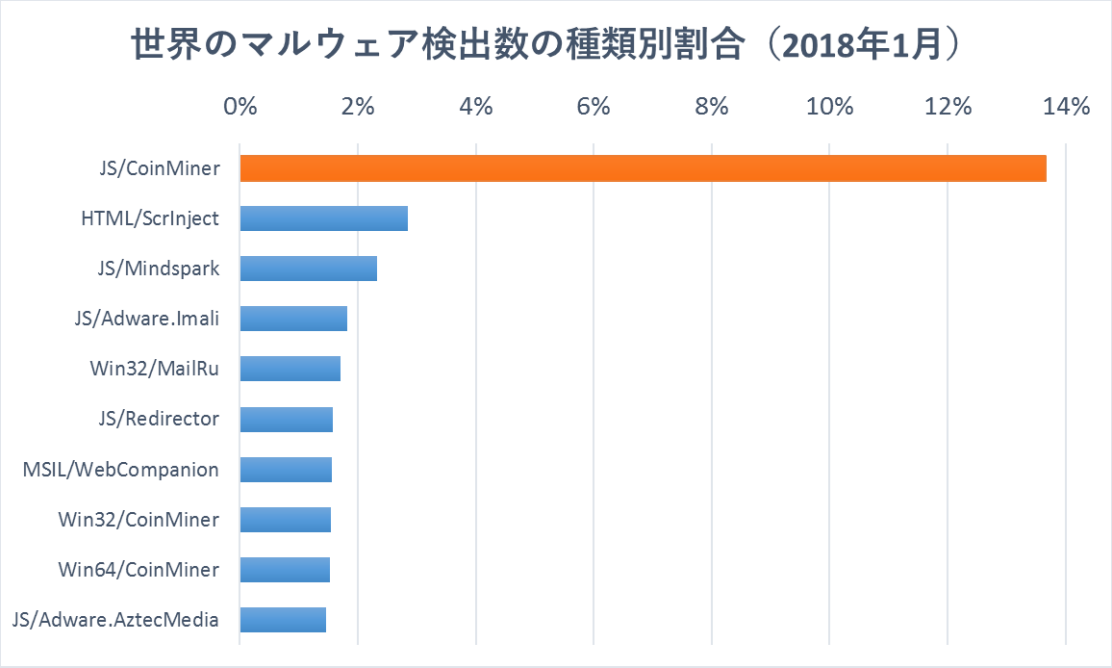
国内マルウェア検出数の比率（2018 年 1 月）

国内マルウェア検出数上位（2018 年 1 月）

順位	マルウェア名	比率	種別
1	JS/CoinMiner	16.5%	マイニングマルウェア
2	VBS/TrojanDownloader.Agent	13.6%	ダウンローダー
3	HTML/FakeAlert	9.9%	偽の警告文を表示するスクリプト
4	HTML/ScrInject	4.5%	埋め込まれた不正なスクリプト
5	JS/Redirector	4.2%	別のページに遷移させるスクリプト
6	VBA/TrojanDownloader.Agent	4.0%	ダウンローダー
7	JS/TrojanDownloader.Agent	1.6%	ダウンローダー
8	Win32/FusionCore	1.5%	PUA(※)
9	Win32/RiskWare.PEMalform	1.5%	PUA(※)
10	Win32/KingSoft	1.4%	PUA(※)

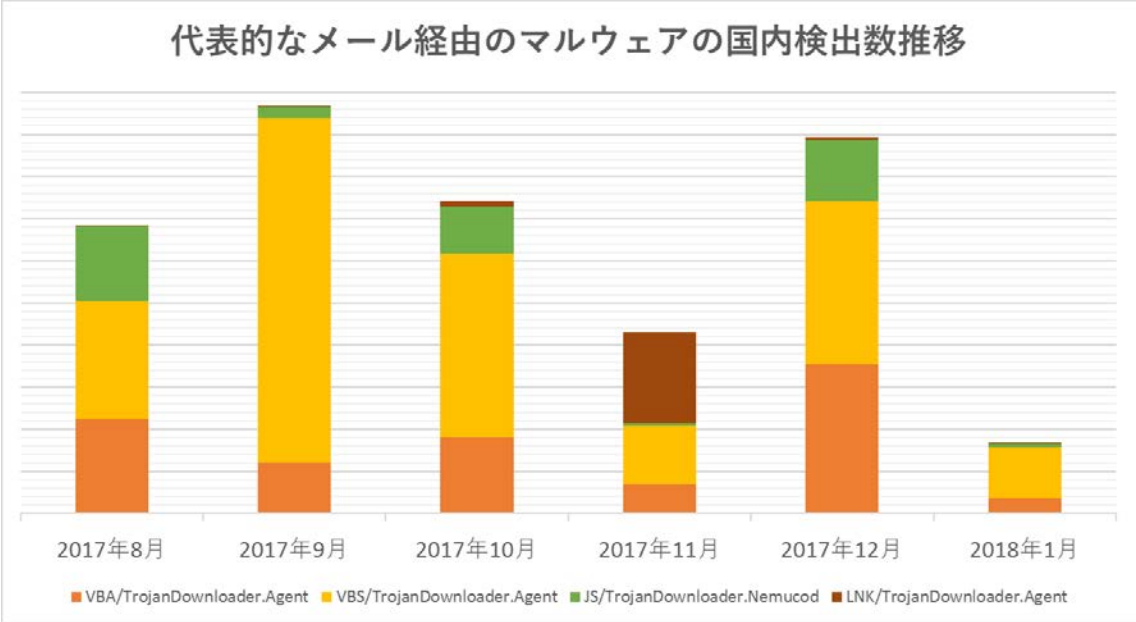
（※）Potentially Unwanted Application(望ましくない可能性のあるアプリケーション)：コンピューターの動作に悪影響を及ぼすことや、ユーザーが意図しない振る舞いなどをする可能性があるアプリケーション。

1 月は JavaScript 形式のマイニングマルウェア「CoinMiner」が月別の統計で初めて検出数 1 位になりました。「JS/CoinMiner」は日本国内だけでなく、世界全体の統計でも最も多く検出されています。



世界のマルウェア検出数の種類別割合（2018 年 1 月）

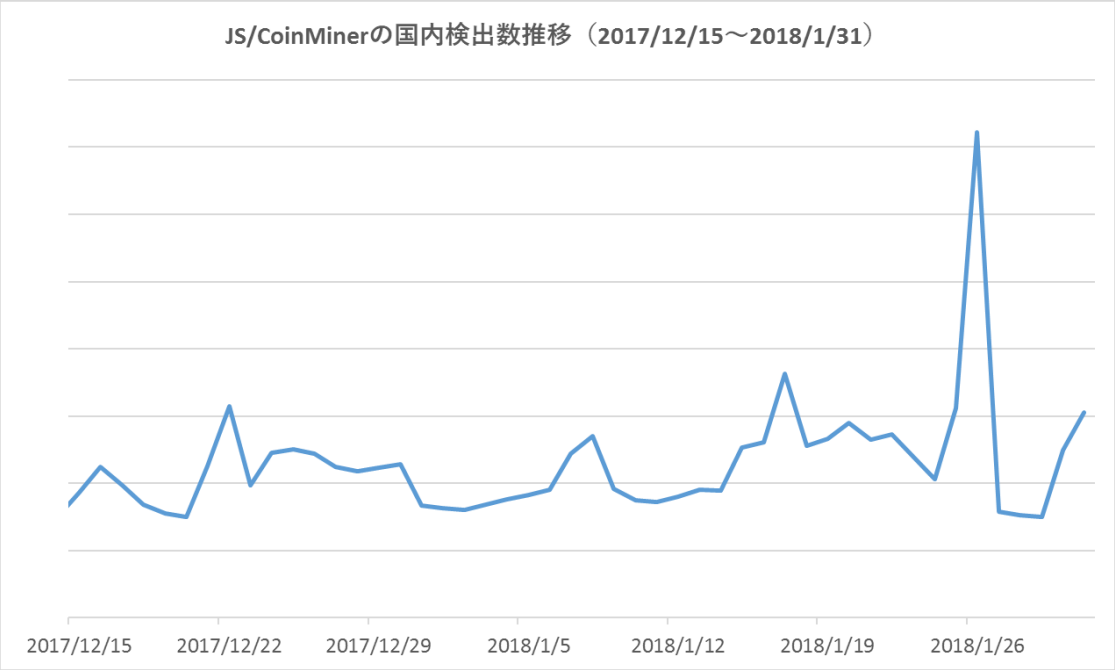
3 位の「HTML/FakeAlert」および 4 位の「HTML/ScrInject」は共に Web サイト上に潜む脅威です。Web サイト上の脅威は、Web ブラウザーを搭載しているあらゆるプラットフォーム（Windows PC/Mac/Android/iPhone など）を攻撃の対象としています。Web サイト上の脅威が拡大する一方で、2017 年に猛威を振るったメールを経由した攻撃は激減しています。メールの添付ファイルから検出されるマルウェアのうち、最も代表的な 4 種の検出数の推移は以下グラフのとおりです。2017 年 12 月と比較して 2018 年 1 月の検出数は 1/5 以下となっています。



代表的なメール経由のマルウェアの国内検出数推移

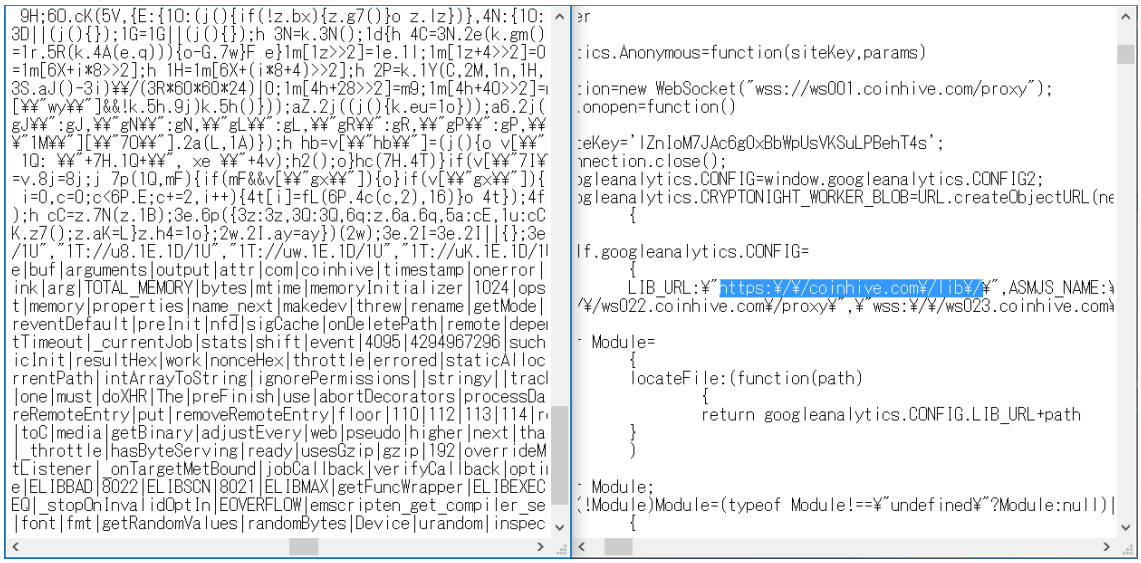
2. マイニングマルウェア「JS/CoinMiner」の爆発的流行

「JS/CoinMiner」は JavaScript で記述された マイニングマルウェア で、感染した PC の CPU などの計算処理能力を利用して仮想通貨をマイニングします。1 月 26 日前後に最も多く検出されました。

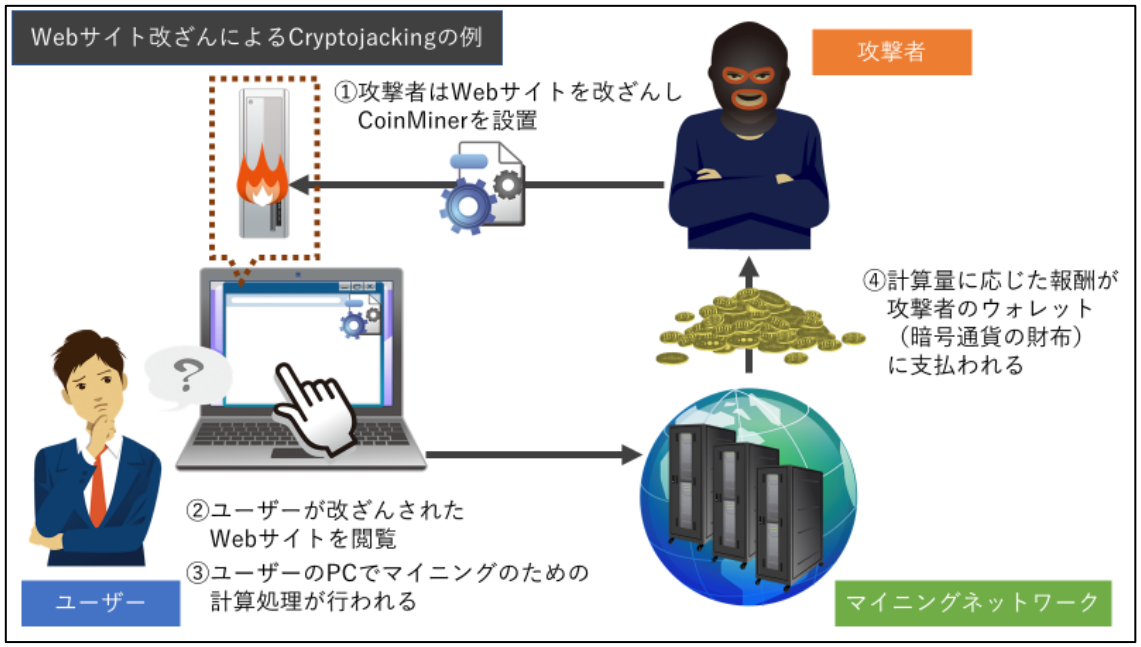


JS/CoinMiner の国内検出数推移（2017/12/15～2018/1/31）

検出されている「JS/CoinMiner」のうち、大多数のスクリプトが「Coinhive」をベースとしています。「Coinhive」は Web サイト閲覧者の PC でマイニングを行うことで、広告の代替となる収益を Web サイトの運営者に提供するサービスです。しかしながらこれを悪用し、攻撃者によって不正に Web サイトに埋め込まれる事例が多数確認されています。中には、JavaScript ライブラリの jQuery に偽装しているものや、検出を逃れるために難読化されているものもあります。Web ブラウザー上でユーザーに無断で採掘することを Cryptojacking（または Drive-by-mining)と呼びます。



難読化されたマイニングスクリプト（ESET 検出名：JS/CoinMiner.B）（左）
左のスクリプトの難読化を解除した状態（ESET 検出名：JS/CoinMiner.A）（右）



Web サイト改ざんによる Cryptojacking の例

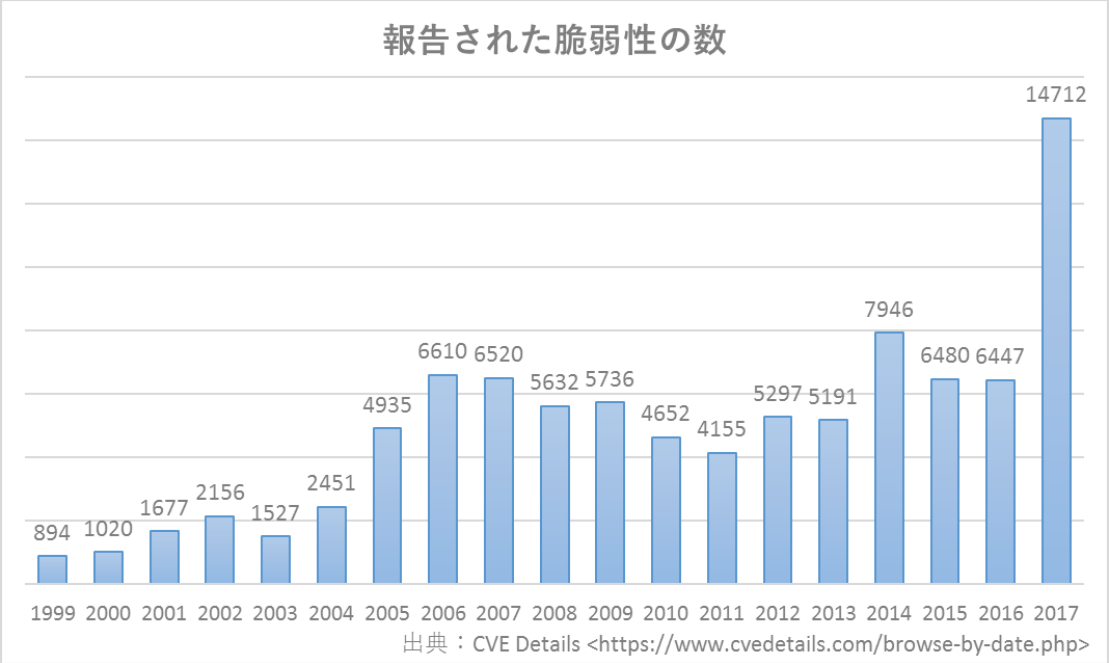
PublicWWWによると、「Coinhive」が設置されている Web サイトは全世界で 33,000 サイト以上存在します（2 月 14 日現在）。

「Coinhive」は CPU の計算処理能力を使い「Monero」と呼ばれる暗号通貨を採掘します。
「Monero」は匿名性を持つ暗号通貨で、第三者が取引の履歴を確認することができません。そのため、犯罪者にとって格好の取引手段となっており、従来の Bitcoin に代わってランサムウェアの支払いに使われる例も確認されています。

Web サイト閲覧時に PC に異常な負荷が掛かっている場合は、このマルウェアが動作している可能性があります。JavaScript 形式のマイニングマルウェアは、ESET 製品では「JS/CoinMiner」として検出されます。

3. 脆弱性を悪用した攻撃の種類が増加

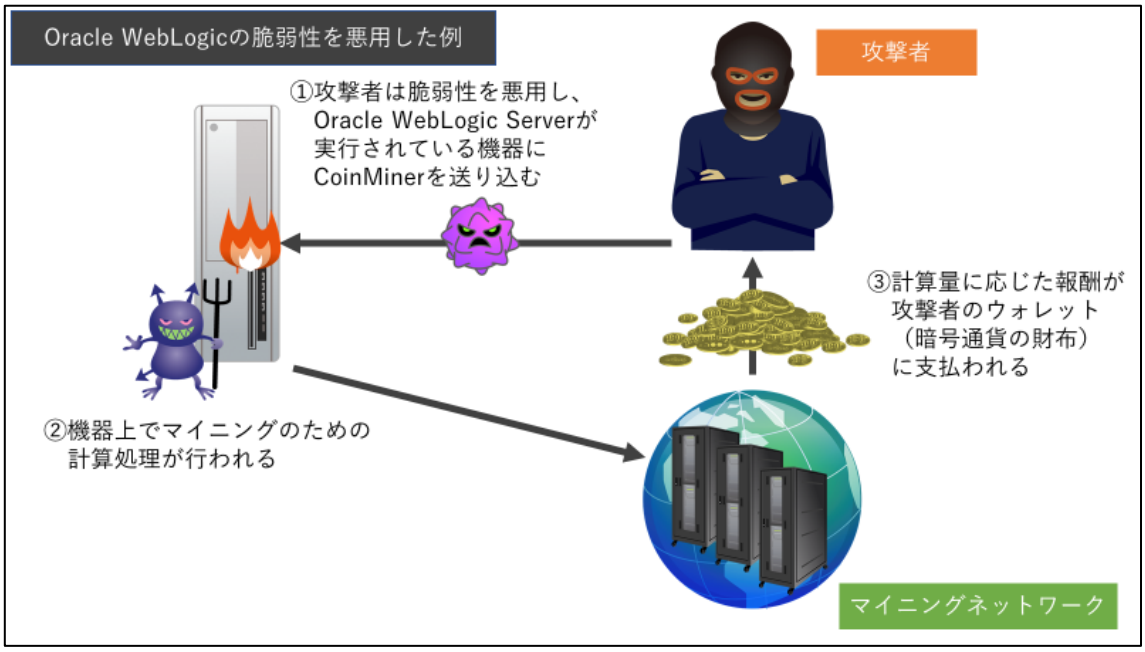
ソフトウェアに関する脆弱性の発見数が増加しています。CVE Detailsによると 2017 年に報告された脆弱性の数は 14,712 件に上り、2016 年の 2 倍以上で過去最高の件数を記録しました。



報告された脆弱性の数（CVE Details）

発見された脆弱性の増加と比例するように、それらの脆弱性を悪用した攻撃の数も増加しています。昨年発見された脆弱性のうち、Microsoft Office の脆弱性（CVE-2017-0199 および CVE-2017-8570）、Microsoft Office 数式エディターの脆弱性（CVE-2017-11882）（リンク先→https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1711.html#anc_02）、Apache Struts 2 の脆弱性（CVE-2017-5638）を狙った攻撃は 2018 年に入った今も検出されています。

最近では、Oracle WebLogic Server の脆弱性（CVE-2017-10271）を悪用した攻撃が確認されました。ある事例ではこの脆弱性を悪用し、マイニングマルウェアを送り込まれる被害が発生しています。



Oracle WebLogic Server の脆弱性を悪用した攻撃事例

このマイニングマルウェアは ESET 製品では「Linux/CoinMiner」、あるいは「Linux/BitCoinMiner」として検出されます。
今回ご紹介した脆弱性は、既に各ベンダーから修正プログラムが公開されています。ご利用しているすべての OS・ソフトウェアに、最新の修正プログラムが適用されているかどうか今一度ご確認ください。

ご紹介したように、1 月はマイニングマルウェアをはじめとした Web 上の脅威、またソフトウェアの脆弱性を悪用し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/