2017年
9月
SEPTEMBER

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に流行の兆し

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

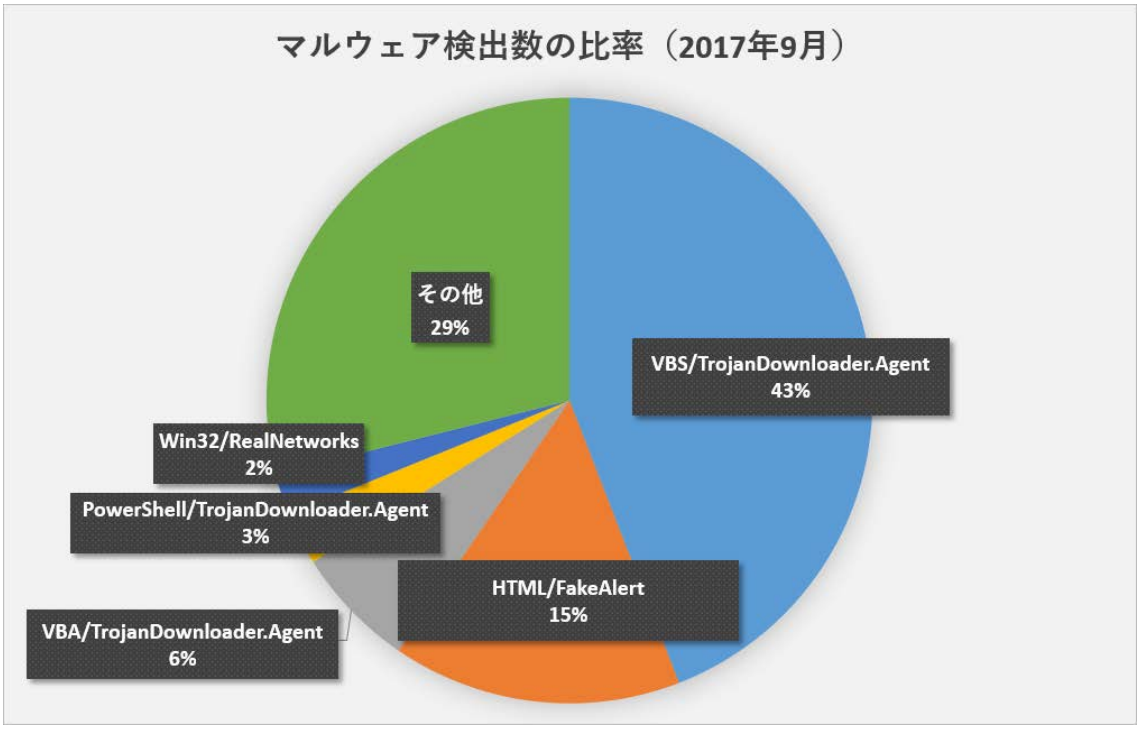
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2017 年 9 月マルウェア検出状況」

1. 9 月の概況について
2. CCleaner の改ざん被害
3. マイニングマルウェアの流行

1. 2017 年 9 月の概況

2017 年 9 月 1 日から 9 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（2017 年 9 月）

9 月は VBS（VBScript）形式のダウンローダーが数多く検出されました。7 月は VBA（Visual Basic for Applications）形式のダウンローダー、8 月は JS（JavaScript）形式のダウンローダーがそれぞれ主流であったことから、マルウェアを PC に送り込む攻撃の初期段階において、攻撃者がさまざまな手法を試していることがうかがえます。
また、当社で 7 月から動向を注視していた「HTML/FakeAlert」の検出数が 8 月から 55%増加し、過去最大となりました。

国内マルウェア検出数上位 10 種（2017 年 9 月）

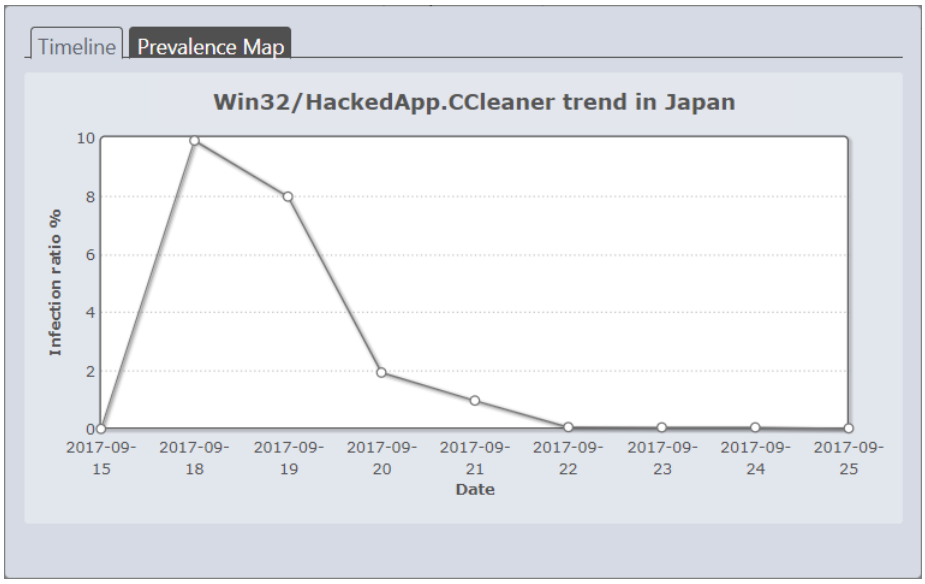
順位	マルウェア名	種別	比率
1	VBS/TrojanDownloader.Agent	ダウンローダー	43%
2	HTML/FakeAlert	偽の警告文表示	15%
3	VBA/TrojanDownloader.Agent	ダウンローダー	6%
4	PowerShell/TrojanDownloader.Agent	ダウンローダー	3%
5	Win32/RealNetworks	PUA（※）	2%
6	HTML/IFrame	リダイレクター	2%
7	JS/TrojanDownloader.Nemucod	ダウンローダー	2%
8	Suspicious	未知の不審なファイル	1%
9	JS/Danger.ScriptAttachment	ダウンローダー	1%

10	Win32/RiskWare.PEMalform	PUA（※）	1%
⋮			
14	Win32/HackedApp.CCleaner	スパイウェア	0.6%

（※）Potentially Unwanted Application：コンピューターやプライバシーを危険にさらす可能性のあるアプリケーション

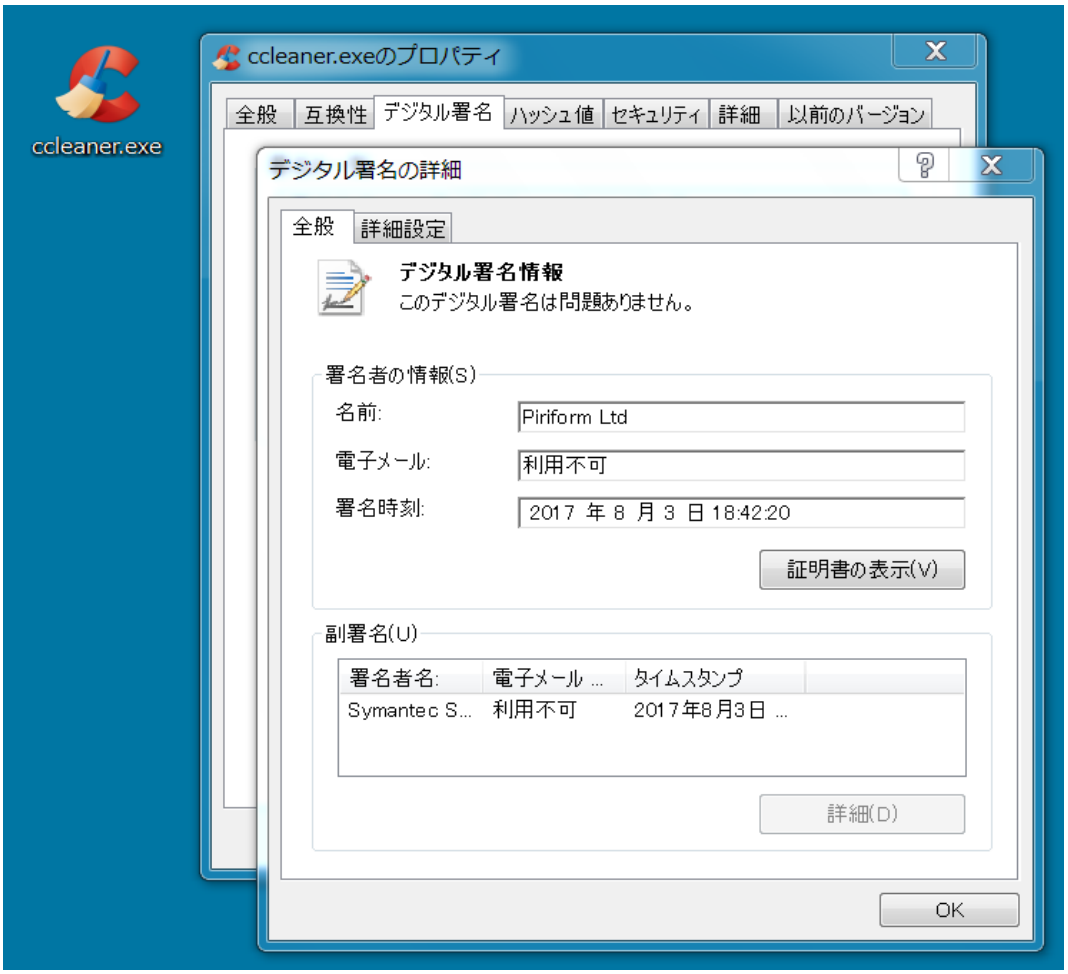
2. CCleaner の改ざん被害

Piriform 社が提供するシステムクリーナーソフトウェア「CCleaner」のプログラムコードが改ざんされ、マルウェアが仕込まれた状態で配布されていたことが 9 月中旬に明らかになりました。
この改ざんされた「CCleaner」は日本でも数多く検出されました。9 月 18 日にはすべてのマルウェア検出のうち、10%をこのマルウェアが占めていました。

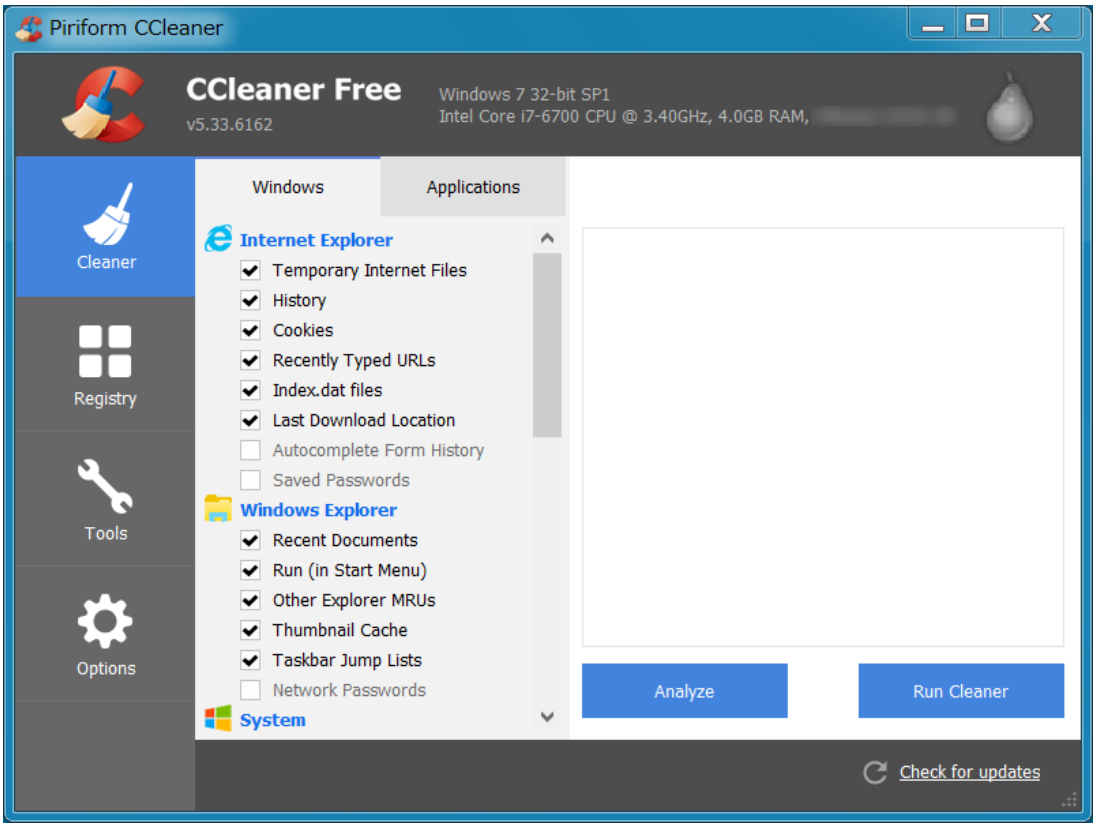


改ざんされた CCleaner の国内検出比率（9 月 15 日～9 月 25 日）

改ざんされた「CCleaner」はデジタル署名されており、一見すると正規の「CCleaner」と違いはありませんが、裏でコンピューター内の情報を外部に送信します。



悪意のあるコードを含む Piriform CCleaner v5.33.6162 のデジタル署名情報



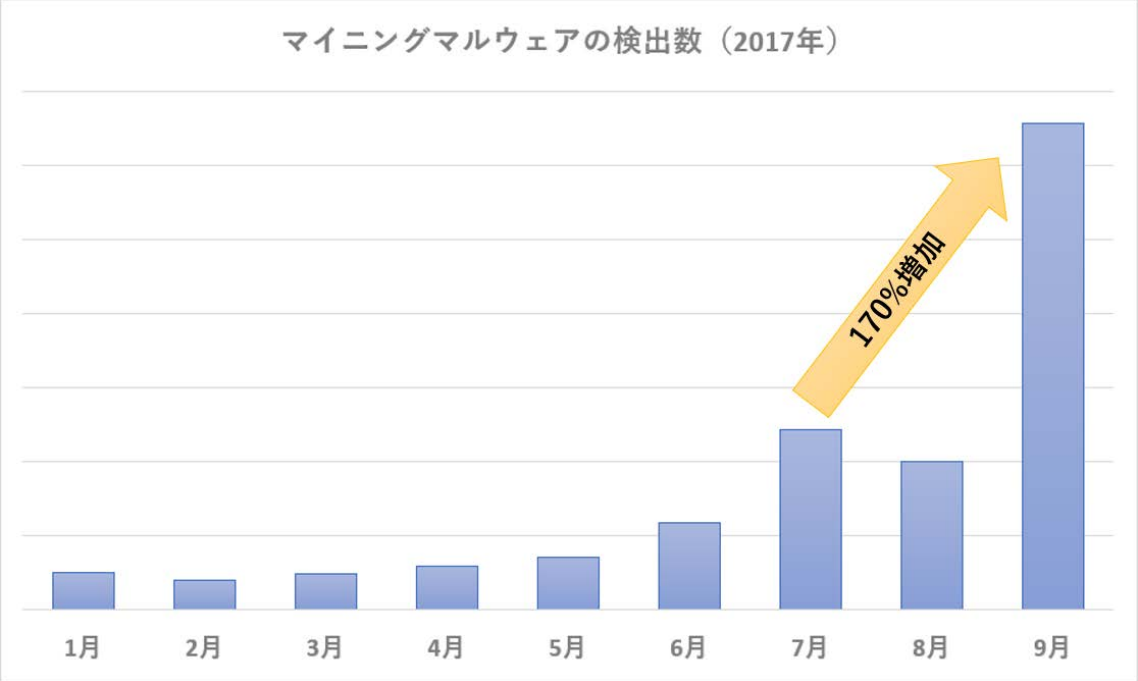
悪意のあるコードを含む Piriform CCleaner v5.33.6162

このマルウェアは、ESET 製品では「Win32/HackedApp.CCleaner」として検出されます。最新のバージョンの CCleaner ではこの問題はすでに修正されています。

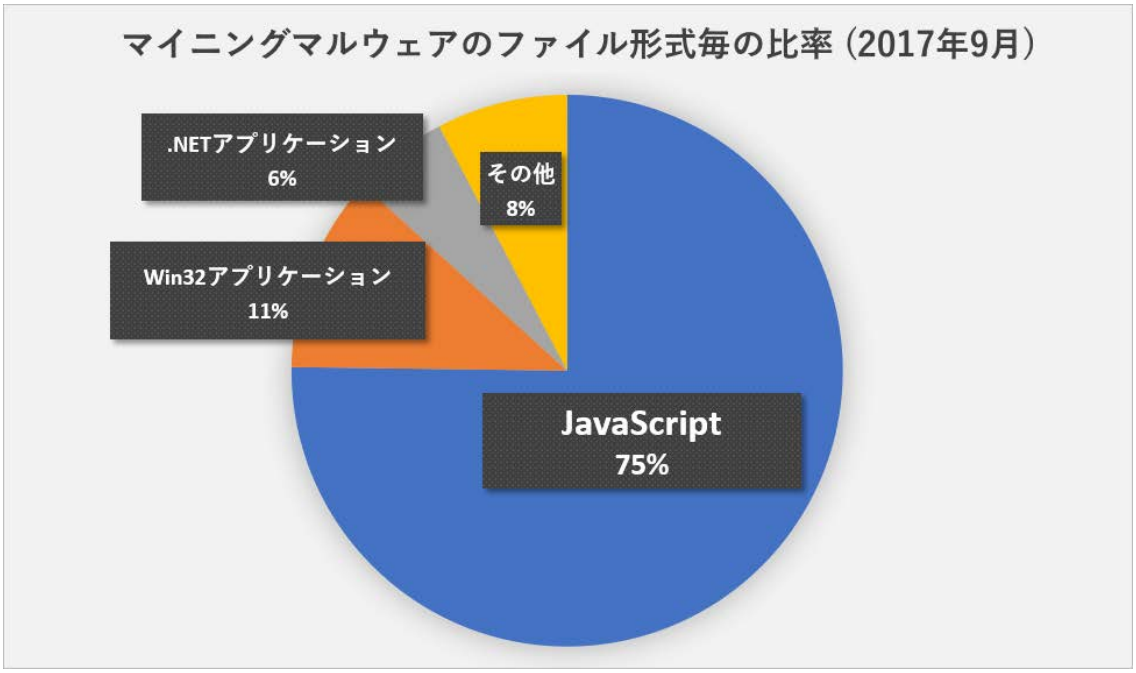
このように、信頼されているソフトウェアに悪意のあるコードを埋め込む手法は「サプライチェーン攻撃」と呼ばれています。6 月にはウクライナなど欧州各地において会計ソフトウェアの改ざんによる大規模な被害が発生しました。お使いのソフトウェアの更新情報について、こまめにチェックすることをお勧めします。

3. マイニングマルウェアの流行

攻撃者の新たなる資金源として、当社が警戒を強めていた マイニングマルウェア の検出が 9 月に急増しています。
マイニングマルウェアは、感染 PC のハードウェアリソース（CPU や GPU）を使って、仮想通貨をマイニング（採掘）します。攻撃者は、採掘された仮想通貨を自身のウォレット（仮想通貨の保管場所）に送付し、それを受け取ることで収益を得ます。

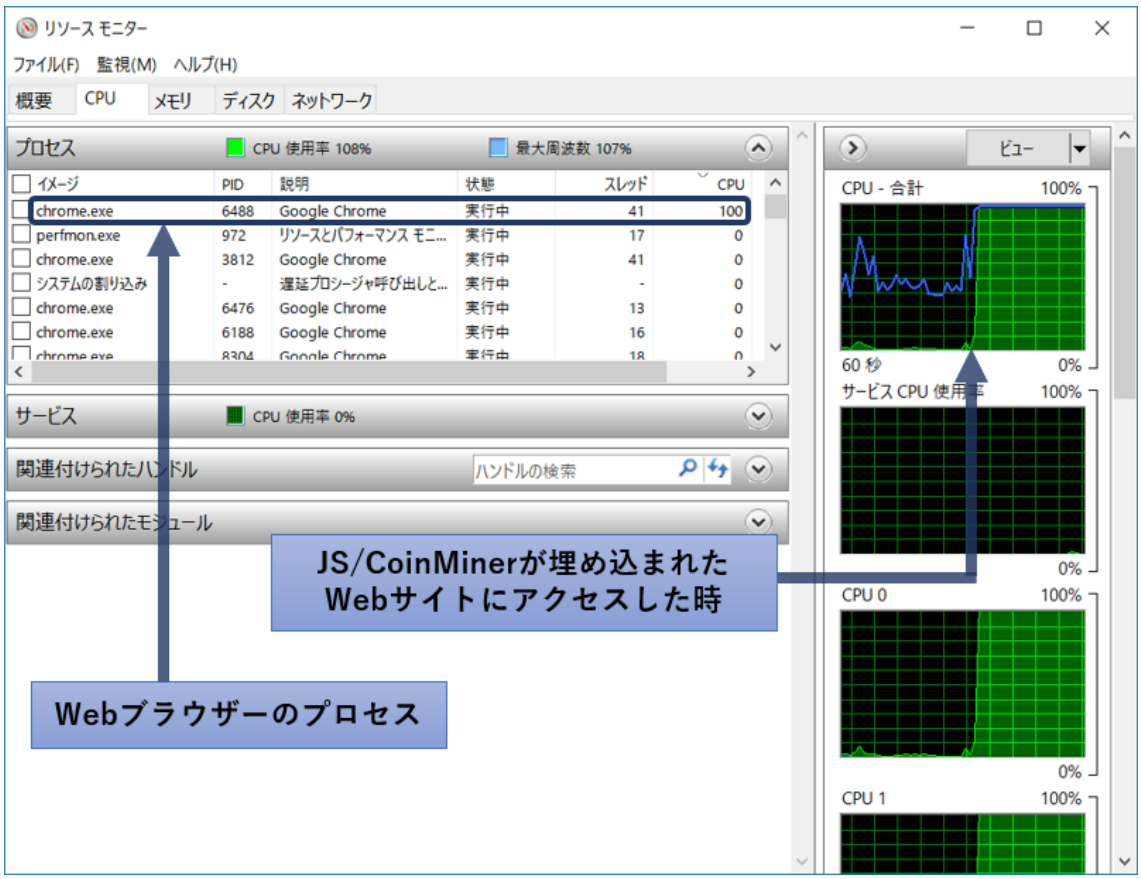


9 月に検出されたマイニングマルウェアをファイル形式別に比較すると、
JavaScript 形式のマイニングマルウェアが非常に多く検出されていることがわかります。



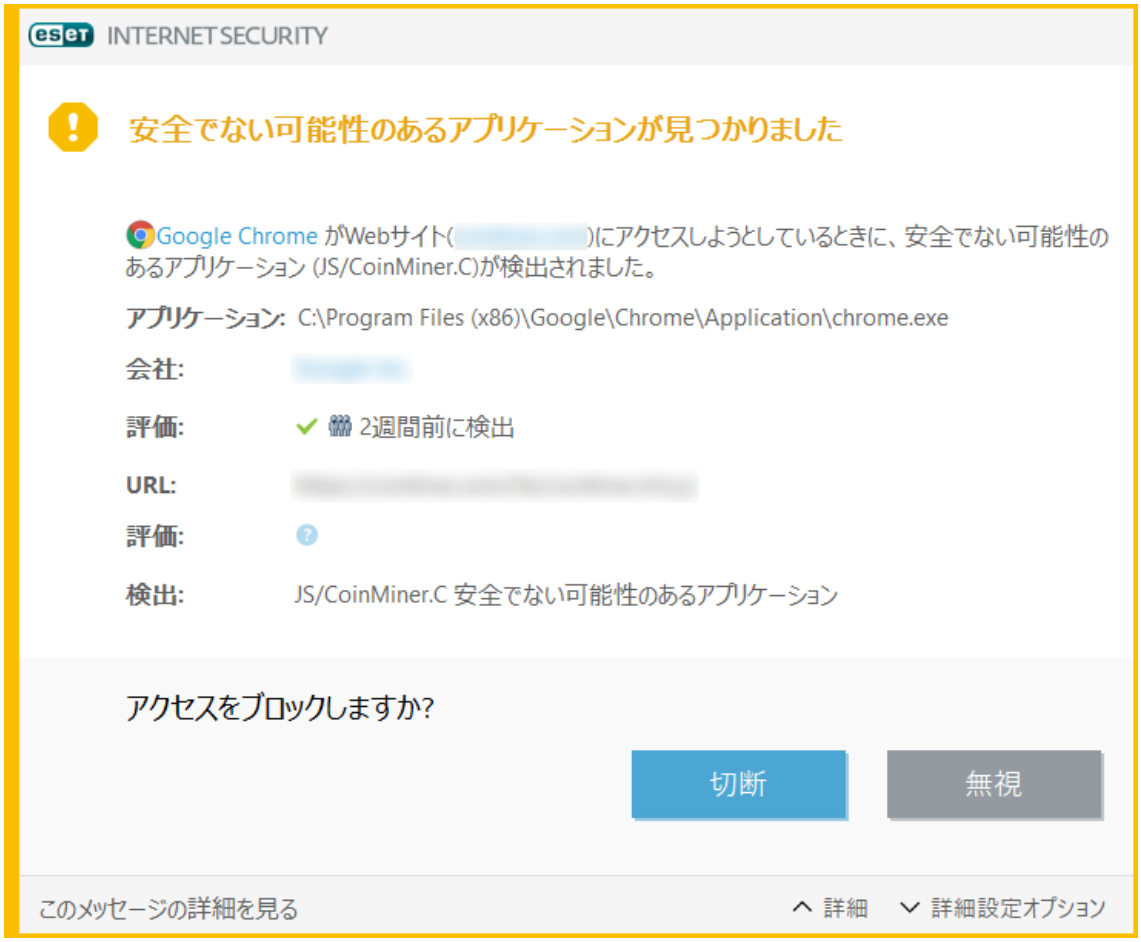
JavaScript 形式のマイニングマルウェアは、基本的に Web ブラウザー上で動作します。ユーザーが Web ブラウザーで特定のサイトを閲覧すると、（多くの場合ユーザーの同意を得ることなく）マイニングが開始されます。

次の画像は、CPU 使用率推移のグラフです。ご覧の通り、「JS/CoinMiner」が埋め込まれた Web サイトへアクセスした瞬間、CPU の使用率が 100%まで上昇しています。



JS/CoinMiner が埋め込まれた Web サイトへのアクセス時の CPU 使用率

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。この 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、「安全でない可能性があるアプリケーション」として警告されます。



ESET Internet Security V10.1 における検出画面

お使いの ESET 製品で「安全でないアプリケーション」の検出が有効になっているか確認するには、当社サポートページのページ下部の参考情報をご参照ください。

今回ご紹介した通り、9 月も多くのサイバー攻撃活動が確認されました。常に最新の脅威情報に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/