2017年
10月
OCTOBER

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

DDE を悪用したダウンローダーを多く検出

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

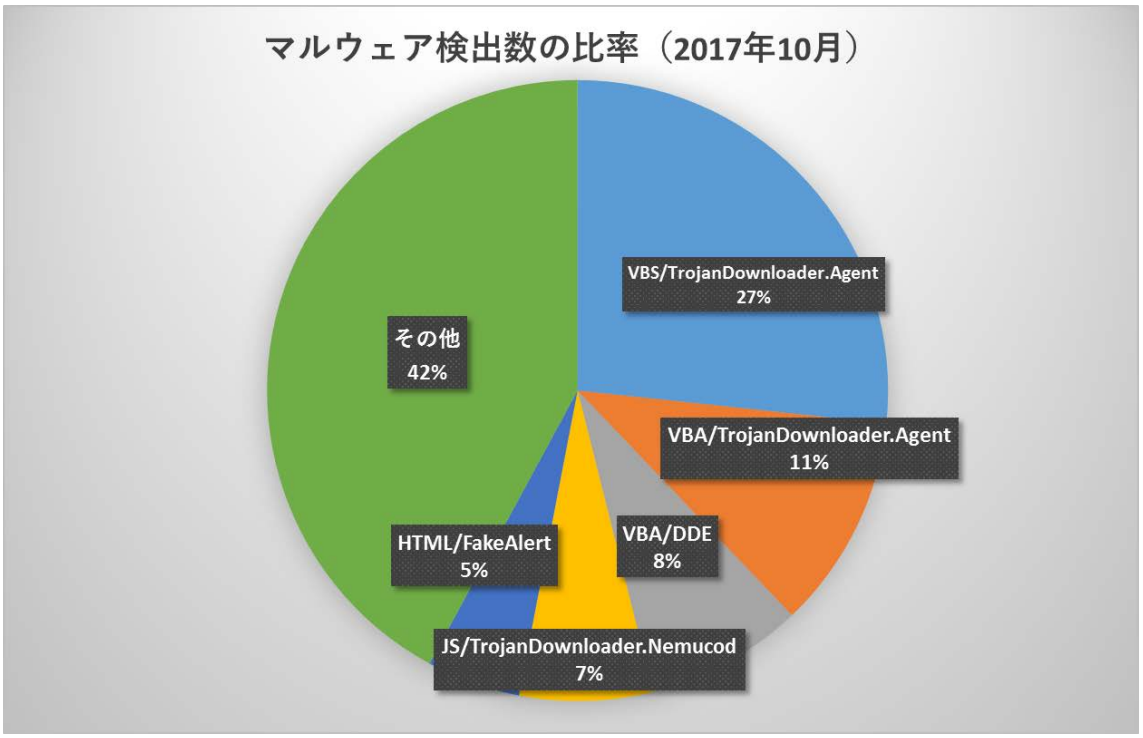
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2017 年 10 月マルウェア検出状況」

1. 10 月の概況について
2. DDE を悪用したダウンローダー
3. 新種のランサムウェアの出現
4. マイニングマルウェアの流行

1. 10 月の概況について

2017 年 10 月 1 日から 10 月 31 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 10 月）

10 月は VBS（VBScript）形式のダウンローダーは減少し、VBA（Visual Basic for Applications）形式のダウンローダーが増加しました。10 月後半には新たな手口である DDE（Dynamic Data Exchange）を悪用したダウンローダー「VBA/DDE」が多く検出されました。
主流となったダウンローダーの形式は、9 月 VBS 形式、8 月 JS（JavaScript）形式、7 月 VBA 形式と変化しています。攻撃者は、攻撃の初期段階に利用するマルウェアを試行錯誤し、セキュリティソフトに検知されないようにしている可能性が考えられます。

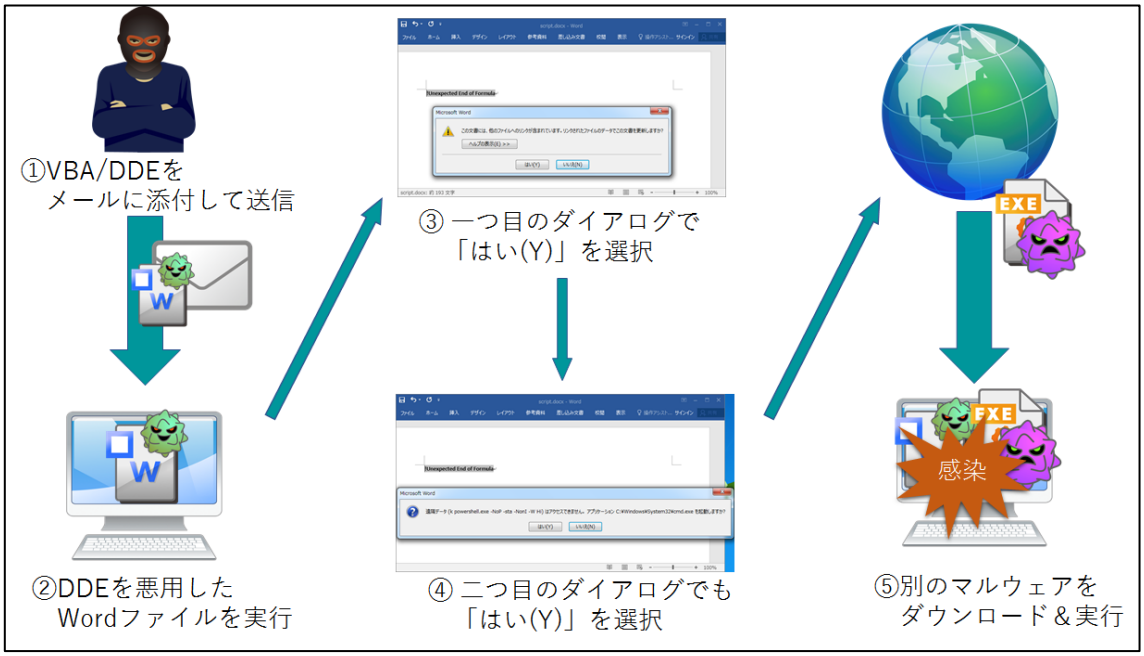
順位	マルウェア名	比率	種別
1	VBS/TrojanDownloader.Agent	27%	ダウンローダー
2	VBA/TrojanDownloader.Agent	11%	ダウンローダー
3	VBA/DDE	8%	ダウンローダー
4	JS/TrojanDownloader.Nemucod	7%	ダウンローダー
5	HTML/FakeAlert	5%	偽の警告文表示
6	HTML/IFrame	4%	リダイレクター
7	Suspicious	3%	未知の不審なファイル
8	DOC/TrojanDownloader.Agent	3%	ダウンローダー
9	JS/Danger.ScriptAttachment	3%	ダウンローダー
10	JS/Mindspark	2%	PUA（※）

：			
19	JS/CoinMiner	0.6%	安全ではない可能性があるアプリケーション

（※）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。

2. DDE を悪用したダウンローダー

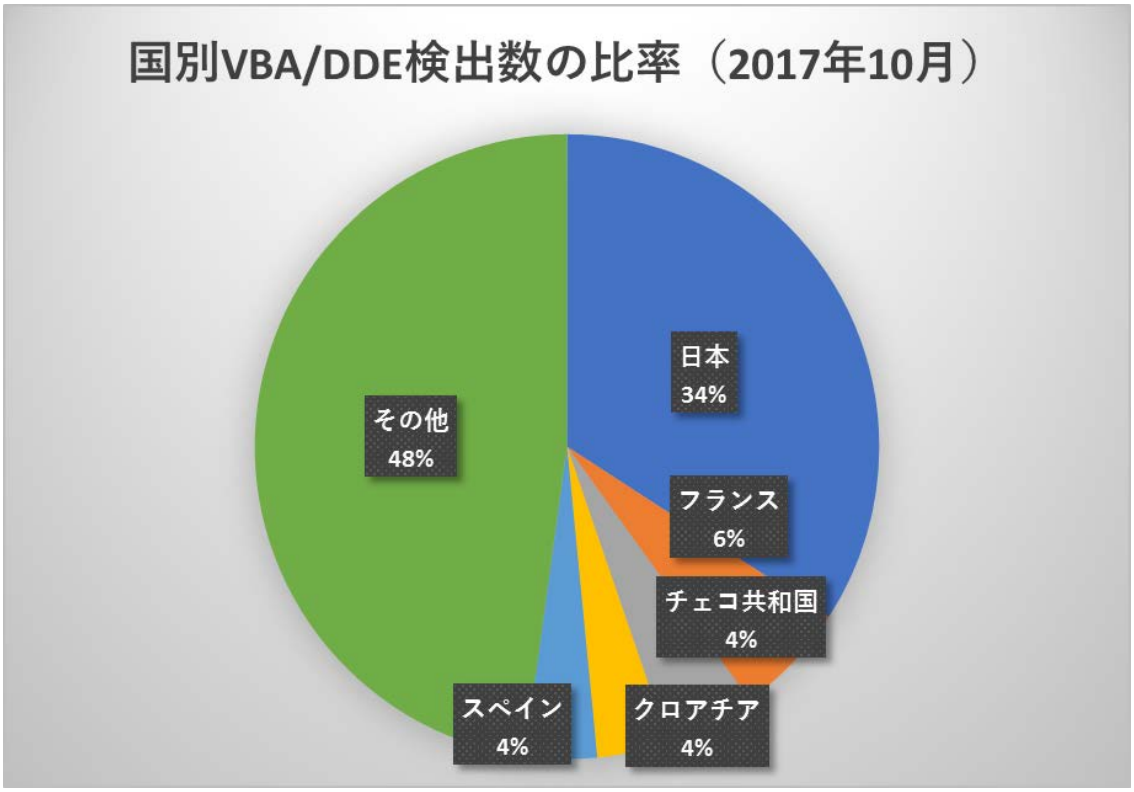
10 月の中旬より DDE を悪用した新たな手口による攻撃が検出されています。
DDE（Dynamic Data Exchange）とは、Windows アプリケーション間でデータを転送するための仕組みの一つです。アプリケーション間でコマンドの送信や受け取りが可能です。DDE 自体は古くからある Windows の技術ですが、攻撃者は新たな手口としてこの技術を悪用し攻撃に利用しています。



メールに添付された「VBA/DDE」の感染フロー

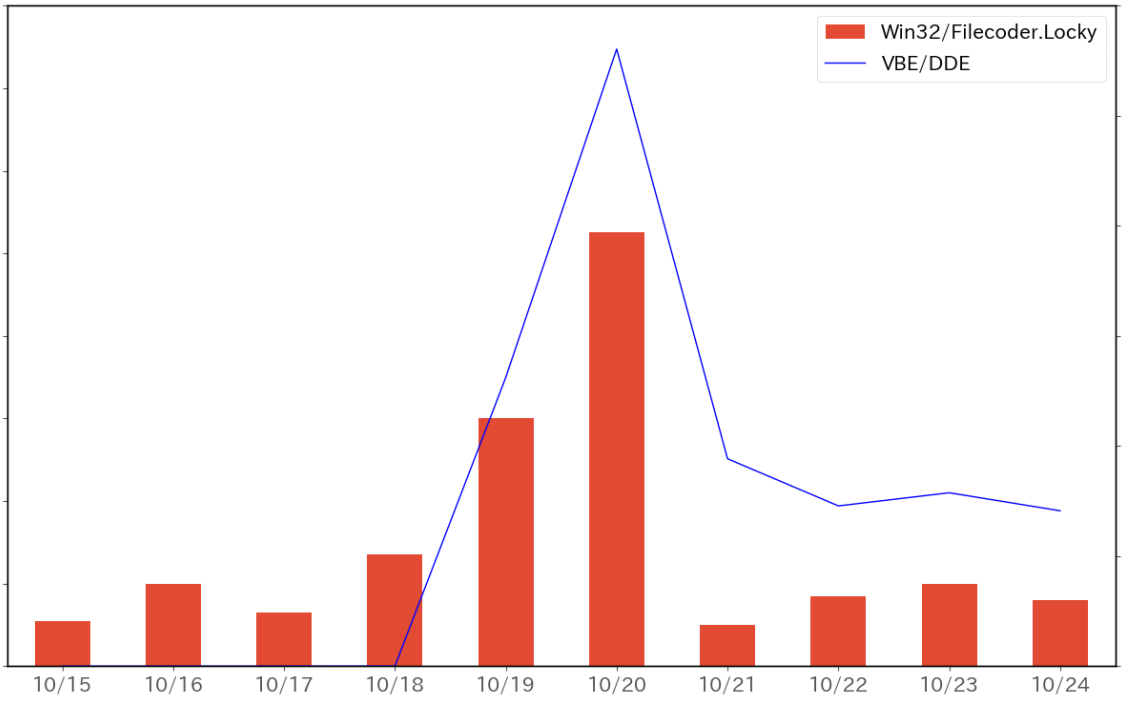
DDE を悪用したマルウェア（ダウンローダー）の感染フローは次のとおりです。
① 攻撃者は DDE を悪用したファイルをメールに添付し送信します。
②この添付ファイルを開くと、1 つ目のダイアログが表示されます。
③「はい(Y)」を選択すると、2 つ目のダイアログが表示されます。
④2 つ目のダイアログで「はい(Y)」を選択すると、ダウンローダーが実行されます。
⑤別のマルウェアをダウンロード後、実行されます。
※どちらかのダイアログで「いいえ(N)」を選択することで、マルウェアの実行を回避できます。

このマルウェアは、ESET 製品では「VBA/DDE トロイの木馬」として検出されます。国別にみると、VBA/DDE は世界の中でも特に日本で多く検出されていることが特徴です。



国別の VBA/DDE 検出数の比率(2017 年 10 月)

また、ランサムウェア「Locky（Win32/Filecoder.Locky）」の攻撃としても利用されていました。10 月 19 日～20 日にかけて、VBA/DDE の検出数に比例して、Win32/Filecoder.Locky の検出数が増えていることがわかります。



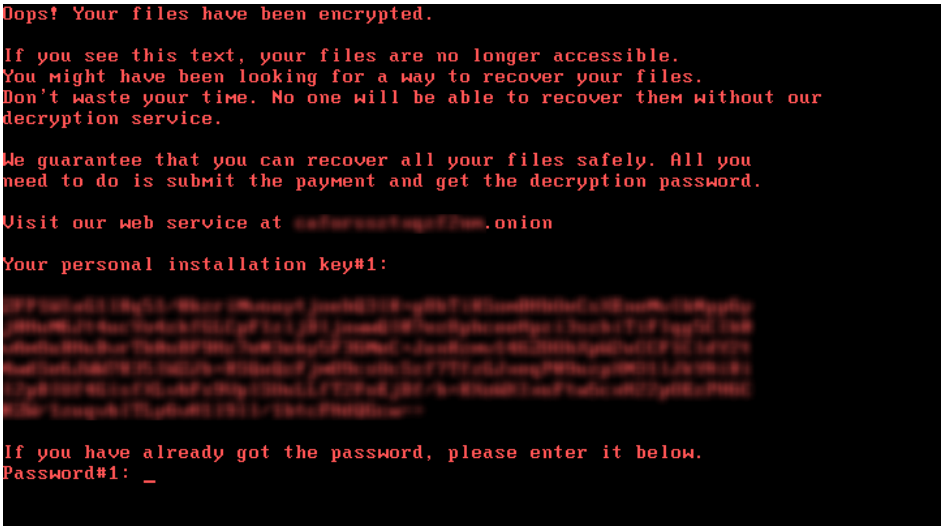
VBA/DDE とランサムウェア Locky の検出数（2017 年 10 月）

この攻撃では、メールに添付された DDE を悪用したダウンローダーを実行すると、Locky をダウンロードし実行します。これにより、Locky に感染しファイルが暗号化されます。

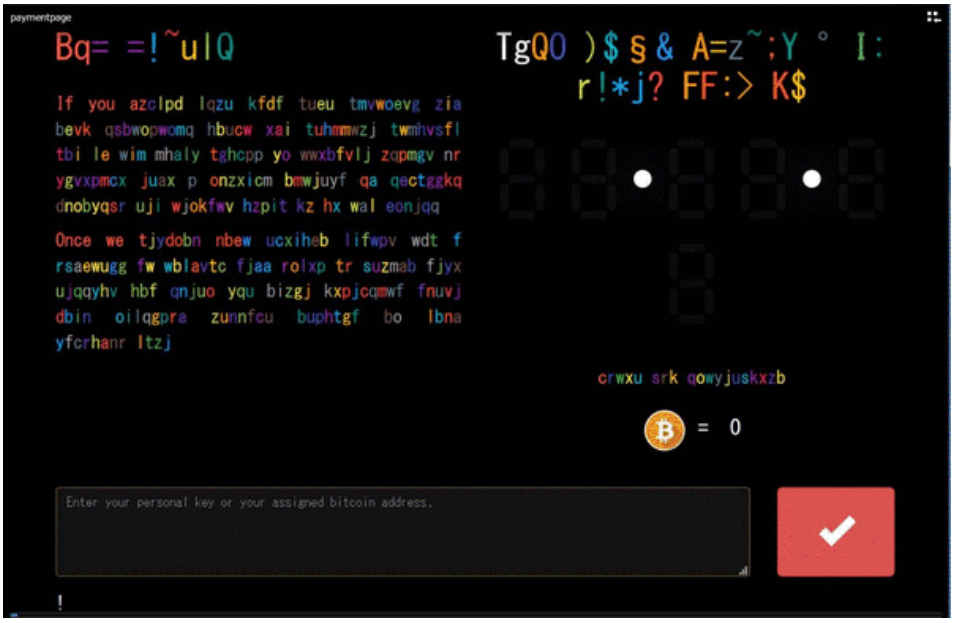
DDE を悪用したマルウェアは、レジストリを変更することで、感染リスクを低減することができます。詳しくは、「Dynamic Data Exchange (DDE) フィールドを含む Microsoft Office ドキュメントを安全に開く方法」を参照してください。

3. 新種のランサムウェアの出現

10 月は、新種のランサムウェア「Bad Rabbit」が話題になりました。



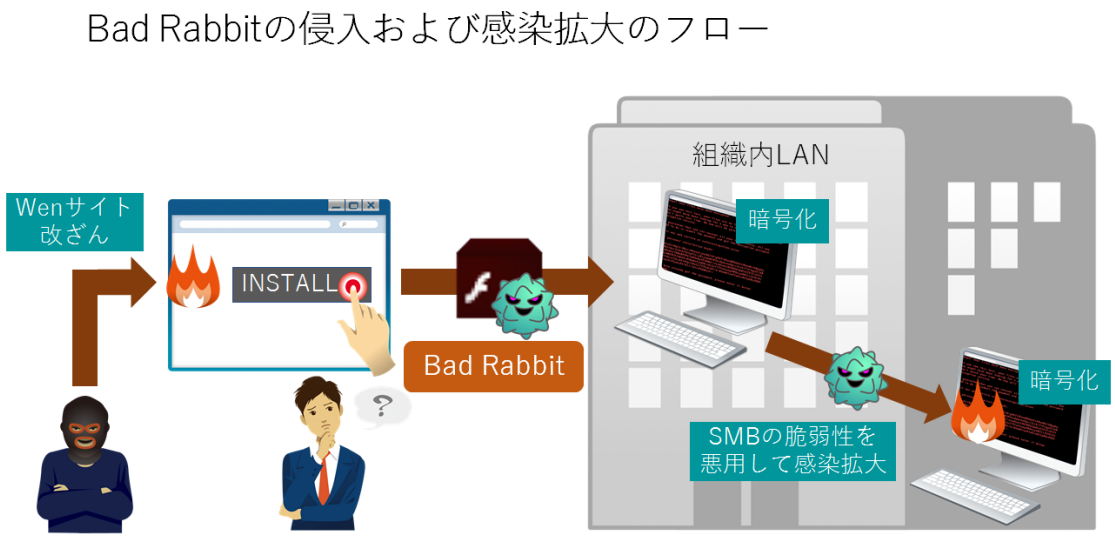
Bad Rabbit の再起動後の身代金要求画面



Bad Rabbit の身代金要求文に記載されている支払いページ（クリックで gif 画像へリンクします）

このランサムウェアは、主に水飲み場型攻撃によって配布され、Adobe Flash Player に偽造したインストーラを実行することで感染します。このマルウェアに感染すると、ファイルが暗号化されます。そして再起動後にディスクの暗号化、及びマスターブートレコード（MBR）の書き換えが行われ、身代金要求画面が表示されます。またSMB※を介してネットワーク内に感染を拡大します。

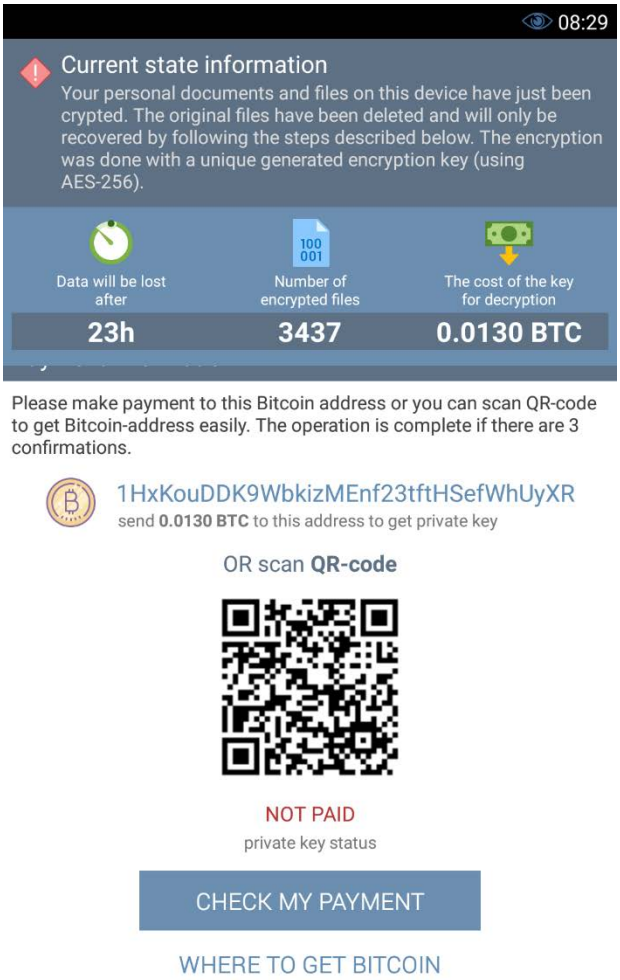
※：「サーバーメッセージブロック」の略で、ネットワークのための通信プロトコルの一種



Bad Rabbit の侵入および感染拡大のフロー

このマルウェアは、ESET 製品では「Win32/Diskcoder.D」として検出されます。

また、新種の Android 向けランサムウェア「DoubleLocker」も発見されています。DoubleLocker は、Adobe Flash Player に偽装したアプリを実行すると感染します。このランサムウェアに感染すると Android デバイス及びデータの両方がロックされます。

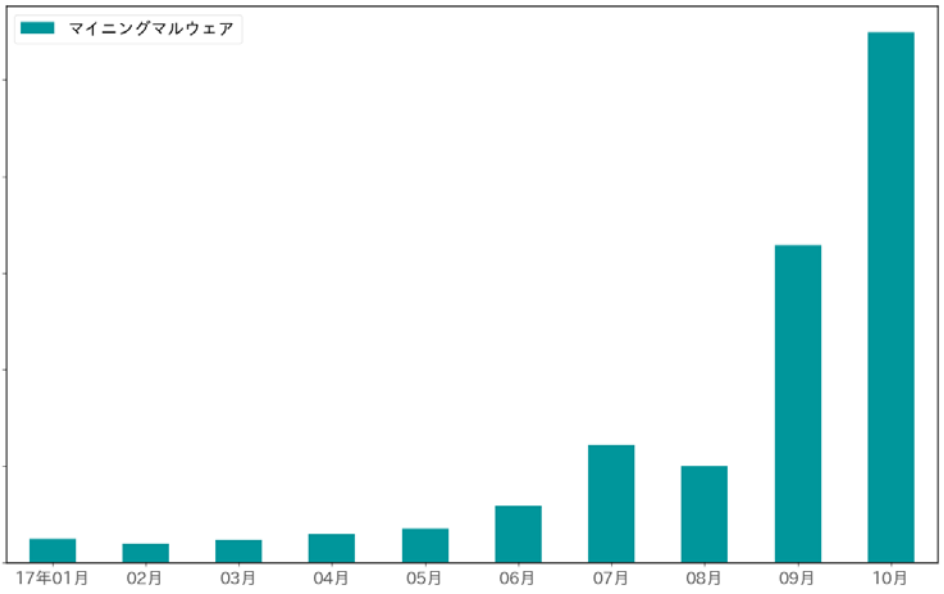


DoubleLocker の身代金メッセージの一部（WeliveSecurity より引用）

この他にも、「GIBON」と呼ばれるランサムウェアなど複数の新たなランサムウェアが出現しています。今後もランサムウェアによる脅威が予想されます。定期的にバックアップを行うことで、感染時の被害を軽減することができます。

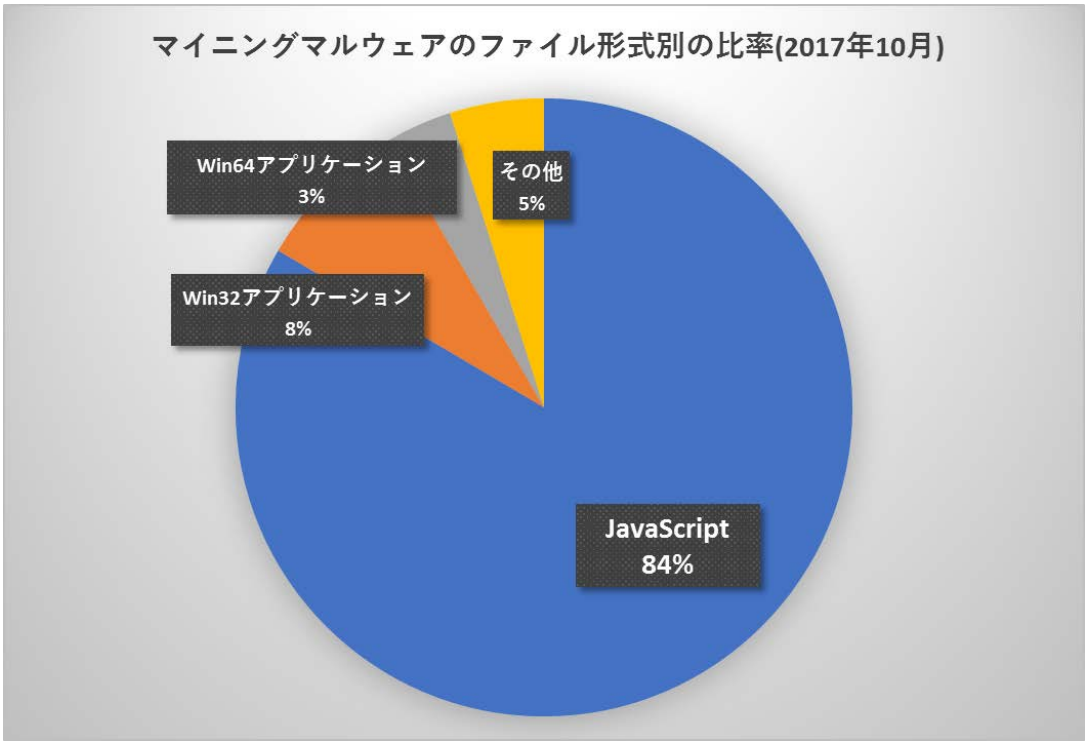
4. マイニングマルウェアの流行

9 月に続き、マイニングマルウェア の検出が増加しています。



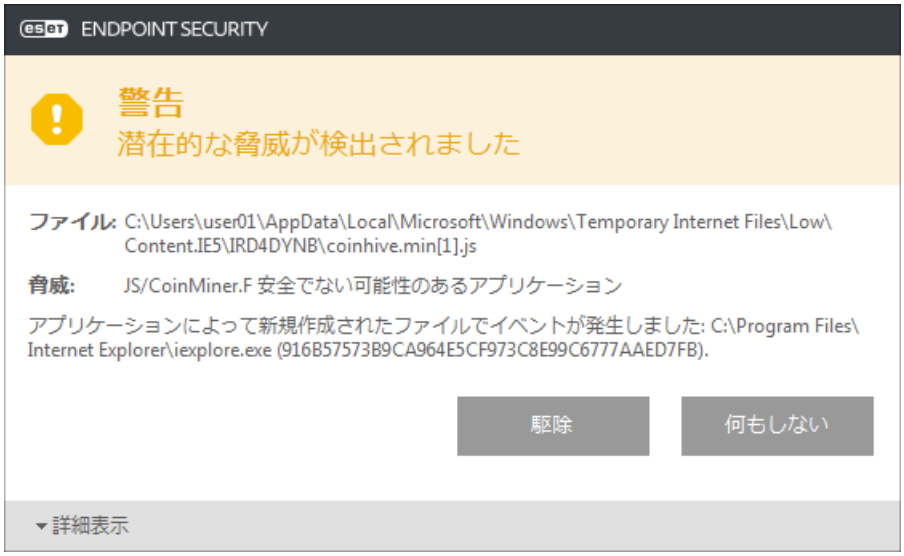
日本国内のマイニングマルウェアの検出数(2017 年 10 月)

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の割合が非常に多いことがわかります。



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。

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。
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 安全でない可能性があるアプリケーション」として検出されます。



ESET Endpoint Security V6.5 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。

ご紹介したように、10 月も多くのマルウェアが確認されました。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/