2018年
5月
MAY

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

ESET が新たな手口のバンキングマルウェアを発見

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。

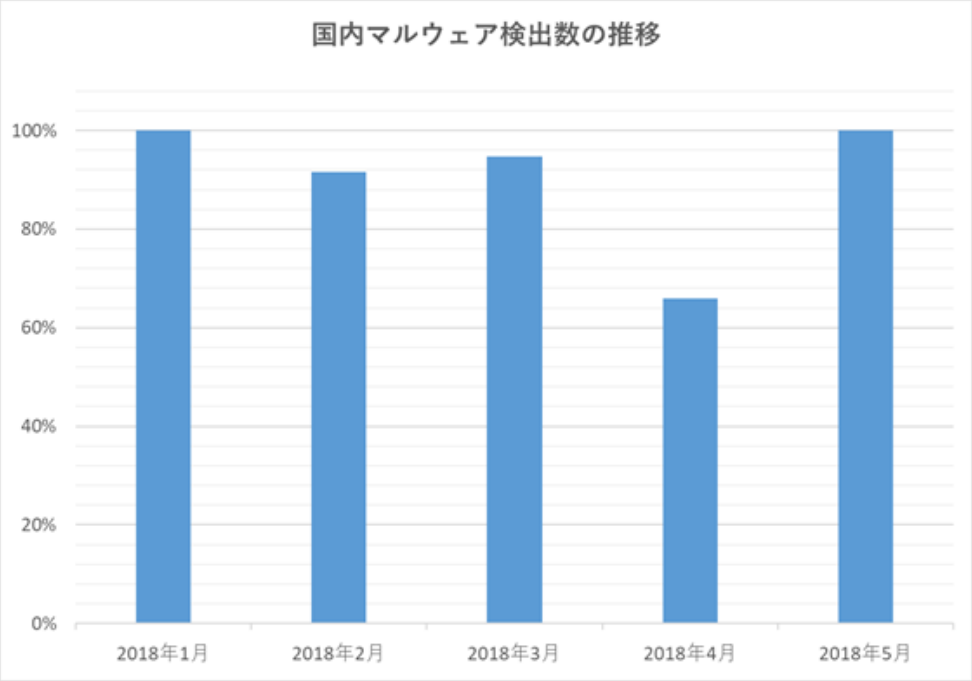
© Canon IT Solutions Inc.

ショートレポート「2018 年 5 月マルウェア検出状況」

1. 5 月の概況について
2. Web ブラウザーを問わない、新たな手口を使うバンキングマルウェアを発見
3. ランサムウェアを販売する Ransomware as a Service（RaaS）

1. 5 月の概況について

2018 年 5 月 1 日から 5 月 31 日までの間、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(※)（2018 年 5 月）

（※） 2018 年 1 月の検出数を 100%として比較。

© Canon IT Solutions Inc.

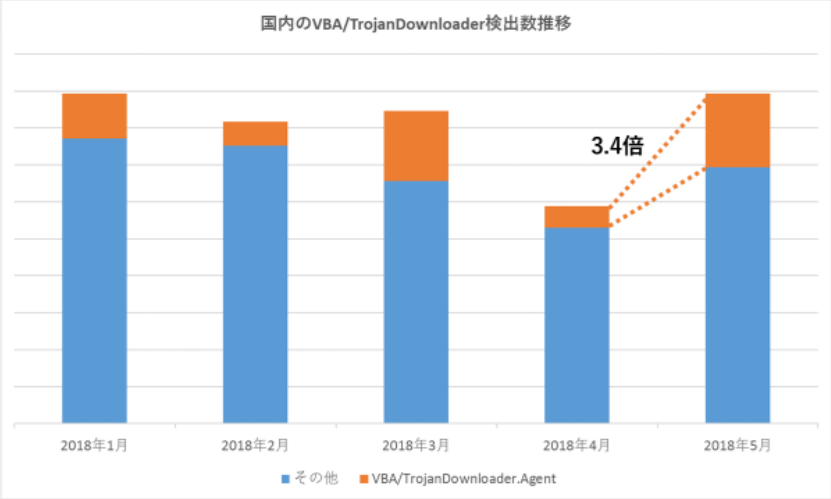
5 月の国内マルウェア検出数の合計は、4 月のおよそ 1.5 倍でした。ファミリー別の割合は以下のとおりです。

国内マルウェア検出数上位（2018 年 5 月）

順位	マルウェア名	比率	種別
1	VBA/TrojanDownloader.Agent	22.3%	ダウンローダー
2	Suspicious	9.8%	未知の不審ファイル呼称
3	HTML/FakeAlert	8.0%	偽の警告文を表示するスクリプト
4	JS/CoinMiner	7.0%	マイニングスクリプト
5	JS/Redirector	4.2%	リダイレクター
6	JS/Mindspark	3.8%	アドウェア
7	JS/Adware.Agent	2.7%	アドウェア
8	PowerShell/TrojanDownloader.Agent	2.5%	ダウンローダー
9	JS/Adware.Imali	2.2%	アドウェア
10	HTML/Adware.Agent	1.7%	アドウェア

© Canon IT Solutions Inc.

4 月に引き続き、検出数トップのマルウェアは「VBA/TrojanDownloader.Agent」でした。検出数は 4 月と比較して、3.4 倍となりました。
このマルウェアは VBA（Visual Basic for Applications）で書かれたダウンローダーで、ファイル形式は Microsoft Word 文書や Microsoft Excel 文書です。主にメールの添付ファイルとして拡散されています。



国内の VBA/TrojanDownloader 検出数推移

© Canon IT Solutions Inc.

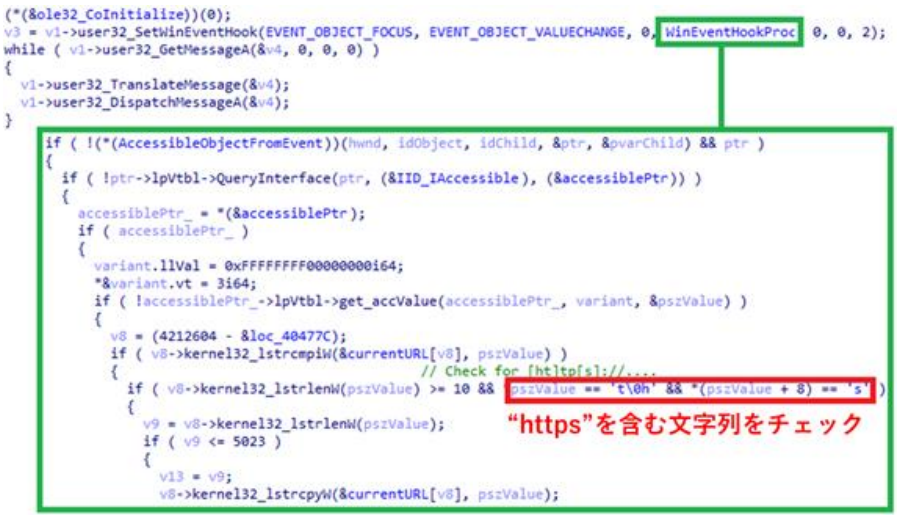
2. Web ブラウザーを問わない、新たな手口を使うバンキングマルウェアを発見

ESET はポーランド人を狙った、新しいテクニックを使うバンキングマルウェア「BackSwap」を発見しました。

従来のバンキングマルウェアは、Web ブラウザーに DLL（コード）インジェクション(※)する手口が一般的でした。ところが今回発見された「BackSwap」は全く新しい手口で情報を盗み取ります。以下、その手法をご紹介します。

（※） Web ブラウザーのプロセスに自身のコードを挿入し、実行させる攻撃手法。

「BackSwap」は Windows メッセージの仕組みを通じて、ユーザーの操作を監視します。この手法は、Web ブラウザーの種類やバージョンを問わず攻撃が可能な点で、非常に強力です。「BackSwap」ははじめに、「https」で始まる文字列を検索し、Web ブラウザーが現在アクセスしている URL を取得します。



Web ブラウザーが現在アクセスしている URL を取得する処理

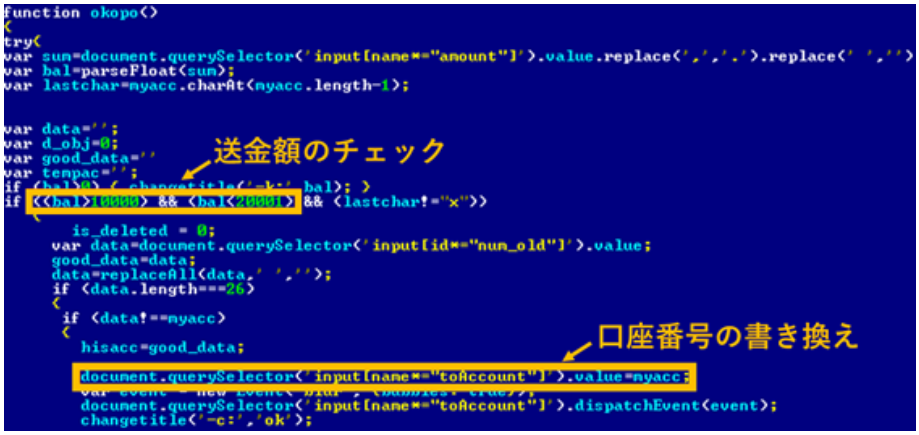
次に、「BackSwap」は取得した URL の中に標的の金融機関の Web サイトが含まれているかどうかを調べるために、ウィンドウタイトルと URL をチェックします。標的の Web サイトが含まれていた場合、その Web サイトに対応する悪性の JavaScript のコードを実行します。今回、ポーランドの 5 つの銀行を対象としたスクリプトを確認しています。

© Canon IT Solutions Inc.

ウィンドウタイトルと URL をチェックする処理

スクリプトは、送金先の口座番号を攻撃者の口座に置き換えます。
今回の手口では、送金額が 10,001～20,000 ポーランド・ズウォティ（日本円で 30 万～60 万円、1 ポーランド・ズウォティ＝30 円として計算）の範囲内の場合に送金先を書き換えることが確認されています。また、書き換えたことをユーザーに気付かせないために、Web サイトの表示上は元々の送金相手の口座番号を表示するように細工されています。

© Canon IT Solutions Inc.



送金額をチェックする処理と口座番号を書き換える処理

このように、インターネットバンキングユーザーを狙う攻撃者は日々新しい攻撃手法を開発しています。
ESET 製品では、このマルウェアを「Win32/BackSwap.A トロイの木馬」として検知し、ブロックします。

© Canon IT Solutions Inc.

3. ランサムウェアを販売する Ransomware as a Service（RaaS）

昨年（2017 年）5 月に発生したランサムウェア「WannaCryptor（ESET 検出名：Win32/Filecoder.WannaCryptor）」の攻撃は、世界規模で拡大し、多くのシステムに深刻な被害をもたらしました。
日本でも、「WannaCryptor」が工場のコンピューターに感染し、商品の生産に影響を及ぼすなどの被害が発生しました。

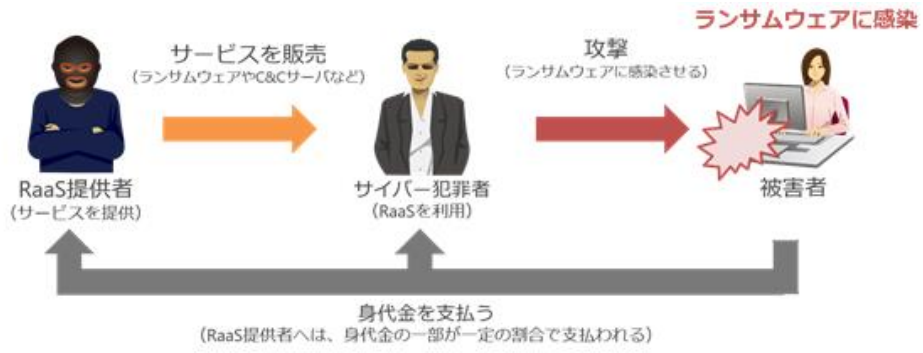
WannaCryptor の脅迫画面

また、昨年 5 月のランサムウェア"WannaCryptor"の大規模感染以降、6 月のマスターブートレコード（コンピューター起動時に OS より先に読み込まれる領域）に感染するランサムウェア「Petya」の大規模感染や 11 月の Adobe Flash Player に偽装したプログラムから感染するランサムウェア「BadRabbit」の流行などが起こり、2017 年はランサムウェアの感染が多く報告された年といえます。

ランサムウェアが流行した要因の 1 つとして、Ransomware as a Service（RaaS）の存在が挙げられます。

Ransomware as a Service（以降、RaaS と記載）は、サイバー犯罪者向けのサービスで、ランサムウェアを感染させ身代金を得ようとするサイバー犯罪者に対して、感染に必要なプログラム（ランサムウェア本体やダウンローダー、C&C サーバーなど）を販売しています。
そのため、サイバー犯罪者は、この RaaS サイトからサービスを購入することで、サイバー犯罪者自身がランサムウェアを開発する必要がなく容易に攻撃を行うことが可能です。

© Canon IT Solutions Inc.



Ransomware as a Service の流れ

このような RaaS を販売するサイト（以降、RaaS サイトと記載）は、ダークウェブ上に複数存在しています。

以下の画面はダークウェブ上で公開される RaaS サイトの一部です。
この RaaS サイトでは、2017 年以降、定期的にランサムウェアのバージョンアップを重ね、今年 4 月にバージョン 1.09 がリリースされました。

RaaS サイトのトップ画面

© Canon IT Solutions Inc.

この RaaS サイトの特徴は、サービスを利用する期間に応じて、価格や使用できる機能に差をつけ、比較的手ごろな値段でサービスを販売していることです。
たとえば、1 か月間サービスを利用する場合 120 ドル（日本円で 13,200 円：1 ドル＝110 円として計算）の費用でサービスを利用できますが、ランサムウェアを感染させるために必要な最低限の機能（ランサムウェアのカスタマイズ制限や C&C サーバーの利用）しか使えません。 一方、1 年間サービスを利用する場合は、900 ドル（日本円で 99,000 円）の費用が必要となりますが、その代わりにオフライン環境でもファイルを暗号化することができる機能やドロッパープログラムなどを使うことができます。また、RaaS 提供者によるサポートも受けることができます。
さらに、一番金額が高いサービスでは、ランサムウェアを難読化するためのツールまでも利用可能です。

-= PACKAGES COMPARISON =-

	Package #3	Package #2	Package #1	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C&C Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Dropper	No	Buy	Yes	Yes
Clone	No	Buy	Buy	Yes
FUD+Obfuscator	Buy	Buy	Buy	Yes
Unkillable Process	No	Buy	Buy	Yes
FUD Stub #	1	1	2	12
Price	120 USD	490 USD	900 USD	1900 USD

サービスの利用期間ごとに使用できる機能を説明した画面

また、サービスの購入を希望する利用者（サイバー犯罪者）向けの FAQ ページが用意されており、提供しているランサムウェアの動作要件や暗号化方式の種類、対象となるファイル拡張子の種類、ランサムウェアに実装されているオプション機能（UAC のバイパス機能など）などが説明されています。

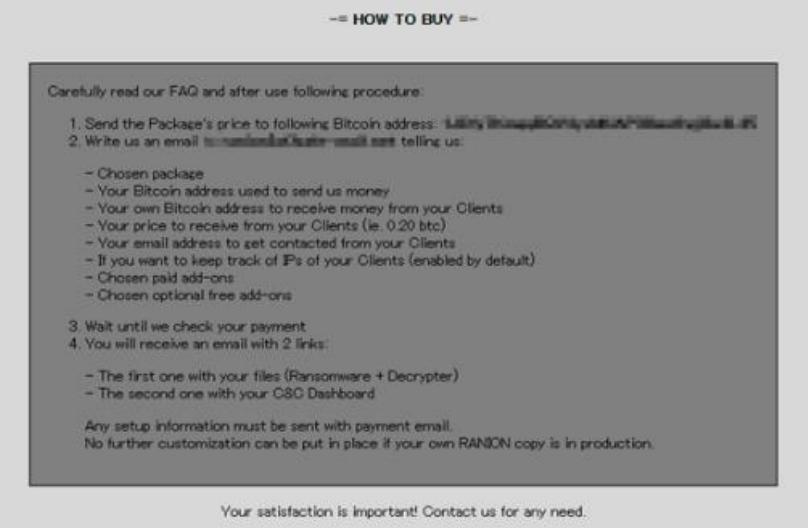
© Canon IT Solutions Inc.

RaaS サイトの FAQ 画面

このように、この RaaS サイトでは、複数のサービスメニューや FAQ など利用者（サイバー犯罪者）がサービスを使いやすいように工夫が行われています。

RaaS サイトの購入方法を記載したページには、利用者（サイバー犯罪者）が、このサービスを使用したい場合、指定のビットコインアドレスに仮想通貨を振り込み、電子メールアドレスで連絡を行うとサービスの利用が可能となる記載があります。

© Canon IT Solutions Inc.



サービスの購入方法を記載した画面

この RaaS サイトで提供されているランサムウェアは、.NET Framework を利用して作成されており、ESET 製品では、「MSIL/Filecoder.FU」という名前で検出されます。
このランサムウェアに感染するとローカルコンピュータのファイルを暗号化し、ファイルの拡張子を".ransom"に変更します。 そして、ファイルを暗号化した後、以下のような脅迫文（8 か国の言語に対応）を画面に表示し、7 日以内にビットコインで身代金を支払うよう要求します。

ランサムウェア感染時に表示される脅迫画面

また、ファイルの暗号化が行われると RaaS 提供者が運用している C&C サーバーに対して、感染したコンピューターの情報が送信されます。
この感染したコンピューターの情報は、RaaS サイトの C&C ダッシュボード画面から確認することができます。
この画面には、ランサムウェアに感染したコンピューターの ID やユーザー名、OS の種類、IP アドレス、暗号化したファイルの数、暗号に使用したキーなどが一覧で表示されており、利用者（サイバー犯罪者）にとって非常に分かり易い画面になっています。

ランサムウェアの感染端末を一覧表示するダッシュボード画面（サンプル）

以上のように Ransomware as a Service（RaaS）は、プログラミングなど特別な知識を必要とせず、比較的簡単に利用できることから、サイバー犯罪者にとって非常に魅力的なサービスです。
今回ご紹介したような RaaS サイトは、ダークウェブ上に複数存在しており、頻繁に機能追加が行われているサービスも存在します。そのため、今後もサイバー犯罪者にとってより魅力的な機能が追加される可能性があります。
当然のことながら、正当な理由なしにマルウェアを作成・保管することは犯罪です。興味本位にこのようなサービスを利用されることがないよう、ご注意下さい。

ご紹介したように、マルウェアに使われているテクニックや、RaaS サイトに代表される攻撃者のためのプラットフォームは日々巧妙化しています。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。

© Canon IT Solutions Inc.

■ 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。

※ESET は、ESET, spol. s r.o.の商標です。Microsoft、Windows は、米国 Microsoft Corporation の米国、日本およびその他の国における登録商標または商標です。

© Canon IT Solutions Inc.

Canon

キヤノン ITソリューションズ株式会社

eset-info.canon-its.jp/