2018年
4月
APRIL

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

金銭目的以外のランサムウェアを確認

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

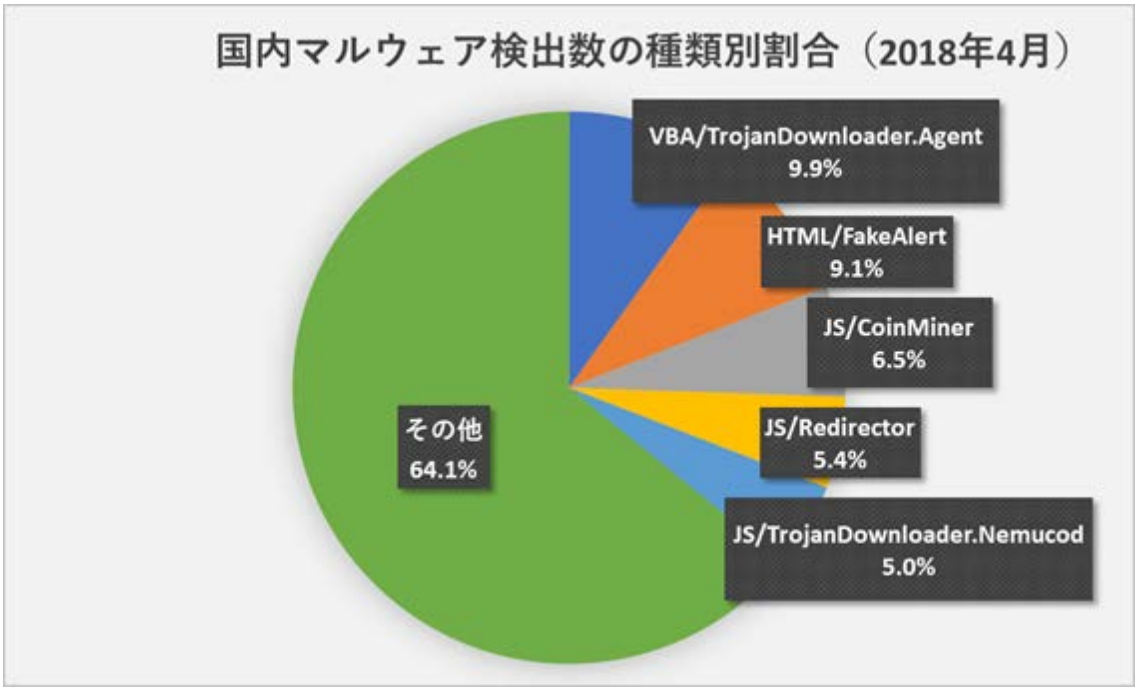
国内のマルウェア検出状況についてまとめたレポートです。

ショートレポート「2018 年 4 月マルウェア検出状況」

1. 4 月の概況について
2. Adobe Flash Player の脆弱性を悪用しランサムウェアに感染させる攻撃
3. ゲームで遊ぶことを強要するランサムウェア

1. 4 月の概況について

2018 年 4 月 1 日から 4 月 30 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種類別割合（2018 年 4 月）

国内マルウェア検出数上位（2018 年 4 月）

順位	マルウェア名	比率	種別
1	VBA/TrojanDownloader.Agent	9.9%	ダウンローダー
2	HTML/FakeAlert	9.1%	偽の警告文を表示するスクリプト
3	JS/CoinMiner	6.5%	マイニングスクリプト
4	JS/Redirector	5.4%	リダイレクター
5	JS/TrojanDownloader.Nemucod	5.0%	ダウンローダー
6	Suspicious	4.6%	未知の不審ファイル呼称
7	JS/Adware.Imali	2.2%	アドウェア
8	JS/Adware.Agent	2.2%	アドウェア
9	PowerShell/TrojanDownloader.Agent	2.1%	ダウンローダー
10	JS/TrojanDownloader.Agent	2.0%	ダウンローダー

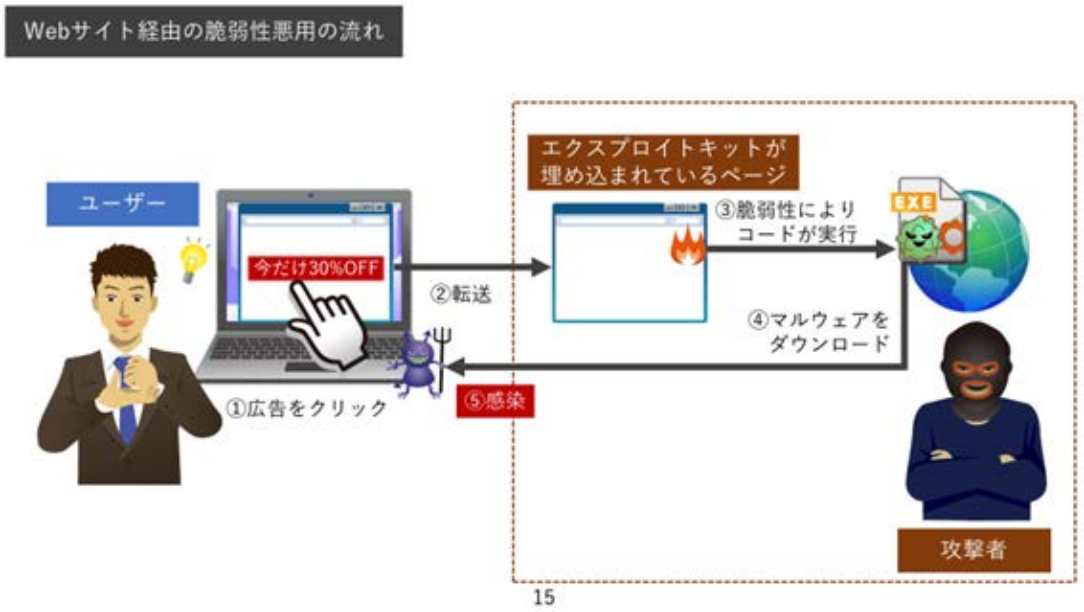
4 月は、検出割合が目立って多いマルウェアはありませんでした。検出 1 位は、昨月に引き続き「VBA/TrojanDownloader.Agent」でした。このマルウェアは、Microsoft Office 上で利用可能なプログラミング言語の VBA(Visual Basic for Applications)で書かれたダウンローダーです。発注書や請求書等を装ったメールに添付されていることが確認されています。これらのファイルは絶対に開かないようご注意ください。

VBA/TrojanDownloader.Agent が添付されたメールの例

2. Adobe Flash Player の脆弱性を悪用しランサムウェアに感染させる攻撃

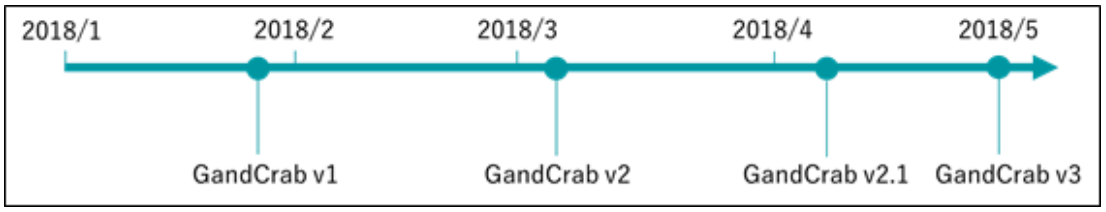
Adobe Flash Player の脆弱性（CVE-2018-4878）を悪用した攻撃が続いています。脆弱性を悪用するコードを含む Microsoft Office ファイルを添付したメール経由の拡散 の他に、Web サイト経由の拡散が確認されています。

攻撃者は、ユーザーをエクスプロイトキットが埋め込まれたページに誘導します。
エクスプロイトキット（Exploit Kit）とは脆弱性を悪用するための攻撃ツールのことです。今回の事例では、Rig、Magnitude、Sundown、Grandsoft などのエクスプロイトキットが使われました。エクスプロイトキットが埋め込まれたページを開くと、マルウェアがダウンロードされ、実行されます。
以下に、脆弱性悪用の流れを図で示します。



Web サイトを経由した脆弱性悪用の流れ

この事例では最終的に、GandCrab をダウンロードすることを確認しています。GandCrab は今年発見されたランサムウェアで、盛んに開発が行われています。



GandCrab のバージョンと出現時期

GandCrab はコンピューター名などの基本情報のほかに、グローバル IP アドレスや利用しているセキュリティソフトウェアの情報など、ユーザーに関する様々な情報を取得し、攻撃者（C&C サーバー）に送信します。これらの情報はさらなる攻撃に悪用される可能性があります。

```
E8 EB+call    internet_open
68 01+push    2801h           ; dwSize
8D 4D+lea     ecx, [ebp+var_18]
E8 49+call    virtual1_alloc
68 00+push    2800h
8D 4D+lea     ecx, [ebp+var_18]
E8 81+call    data_op
68 DC+push    offset word_4103DC ; lpString
8B F8 mov     edi, eax
FF 15+call    ds:lstrlenW
56    push    esi             ; dwHeadersLength
56    push    esi             ; lpszHeaders
68 44+push    offset aGet     ; "GET"
83 EC+sub     esp, 0Ch
8D 4D+lea     ecx, [ebp+var_8]
57    push    edi             ; lpBuffer
56    push    esi             ; dwOptionalLength
56    push    esi             ; lpOptional
68 E0+push    offset asc_4103E0 ; "/"
68 E4+push    offset szServerName ; "ipv4bot.whatismyipaddress.com"
E8 12+call    get_my_own_global_ip
85 C0 test    eax, eax
74 23 jz      short loc_405DE4
```

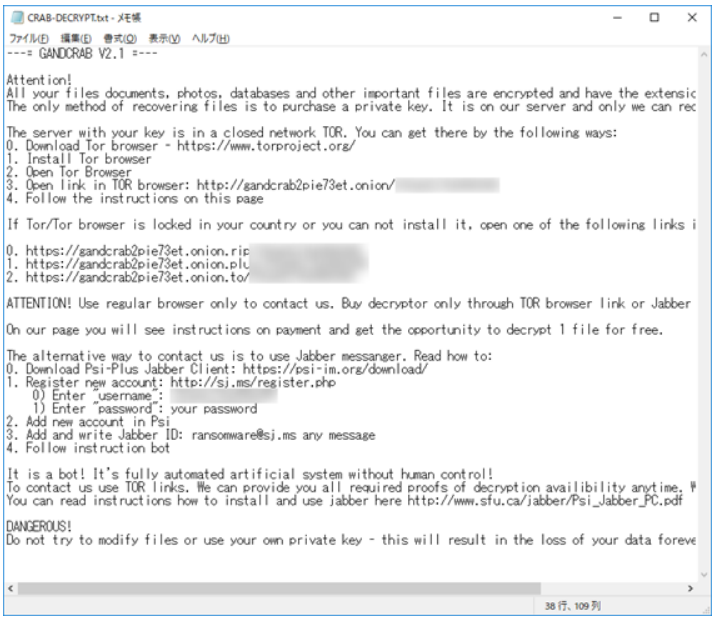
ユーザーのグローバル IP アドレスを取得する処理

```
53    push    ebx             ; lpAddress
C7 45+mov     [ebp+lpString1], offset aAvpExe ; "AVP.EXE"
C7 45+mov     [ebp+var_44], offset aEkrnExe ; "ekrn.exe"
C7 45+mov     [ebp+var_40], offset aAvgntExe ; "avgnt.exe"
C7 45+mov     [ebp+var_3C], offset aAshdispExe ; "ashDisp.exe"
C7 45+mov     [ebp+var_38], offset aNortonantibotE ; "NortonAntiBot.exe"
C7 45+mov     [ebp+var_34], offset aMcshieldExe ; "Mcshield.exe"
C7 45+mov     [ebp+var_30], offset aAvengineExe ; "avengine.exe"
C7 45+mov     [ebp+var_2C], offset aCmdagentExe ; "cmdagent.exe"
C7 45+mov     [ebp+var_28], offset aSmcExe ; "smc.exe"
C7 45+mov     [ebp+var_24], offset aPersfwExe ; "persfw.exe"
C7 45+mov     [ebp+var_20], offset aPccpfwExe ; "pccpfw.exe"
C7 45+mov     [ebp+var_1C], offset aFsguiexeExe ; "fsguiexe.exe"
C7 45+mov     [ebp+var_18], offset aCfpExe ; "cfp.exe"
C7 45+mov     [ebp+var_14], offset aMsmpengExe ; "msmpeng.exe"
FF D6 call    esi ; VirtualAlloc
8B F0 mov     esi, eax
85 F6 test    esi, esi
75 07 jnz     short loc_40686F
```

ESET製品のプロセス名

セキュリティソフトウェアの情報を取得する処理

C&C サーバーへの送信を完了すると、PC 上のファイルを暗号化します。暗号化されたファイルと同じフォルダーに、脅迫メッセージの書かれているテキストファイルが作成されます。テキストファイルには、暗号化されたファイルを元に戻す方法として、TOR と呼ばれる匿名のネットワーク上で支払いをするよう指示されています。



GandCrab V2.1 のランサムノート（脅迫メッセージ）

Adobe Flash Player の脆弱性に対する Adobe 社のセキュリティアップデート は既に公開されています。未適用の場合、速やかに適用されることを推奨します。

ESET 製品では、脆弱性を悪用した Flash ファイルを「SWF/Exploit.CVE-2018-4878」、GandCrab ランサムウェアを「Win32/Filecoder.GandCrab」として検出します。

3. ゲームで遊ぶことを強要するランサムウェア

身代金の代わりにゲームで遊ぶことを強要するランサムウェア（PUBG Ransomware）が発見されました。

このランサムウェアは、感染するとデスクトップのファイルを暗号化し、ファイル名の拡張子を".PUBG"に変更します。そして、ファイルの暗号化が完了するとデスクトップに以下のような脅迫画面を表示します。

PUBG Ransomware の脅迫画面

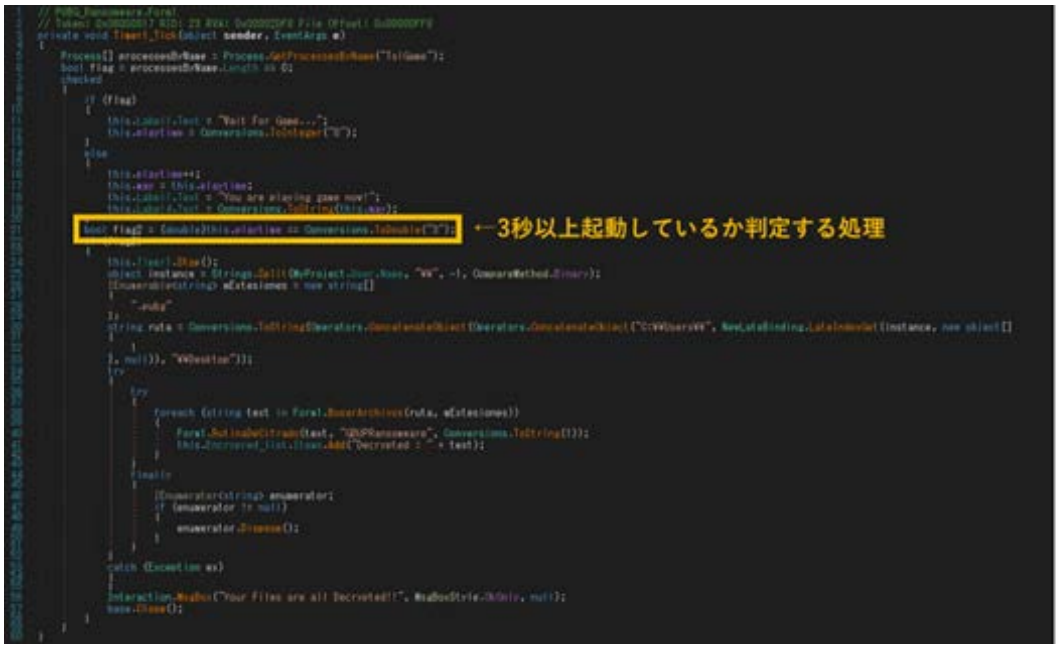
PUBG Ransomware あなたのファイル、画像、音楽、文書は暗号化されました。 あなたのファイルは、PUBG Ransomware によって暗号化されました。 しかし、心配しないでください ！ ロックを解除するのは難しくありません。 私はお金が欲しくない。 ただ、1 時間 PUBG で遊んでください。 または、回復コードは、"s2acxx56a2sae5fjh5k2gb5s2e" です。

脅迫画面のメッセージ（日本語訳）

この脅迫画面には、このランサムウェアの目的が金銭を得ることではないことと、ファイルを復号するには、「1 時間 PUBG というゲームで遊ぶ」もしくは「脅迫画面に回復コードを入力する」必要があるとのメッセージが表示されます。

通常、ランサムウェアはファイルを復号する条件として、仮想通貨などの金銭を要求しますが、このランサムウェアでは、ゲームで 1 時間遊ぶことを強要します。

しかし、実際にはファイルを復号するためにゲームで 1 時間遊ぶ必要はなく、”TslGame”という名前の実行プログラム（プロセス）が 3 秒以上起動している場合、暗号化されたファイルは復号されます(※1)。



ゲームが起動しているか確認する処理

ファイルが復号された際の画面（赤枠は復号されたファイルの一覧）

また、もう 1 つの方法として画面に表示された回復コード（s2acxx56a2sae5fjh5k2gb5s2e）を「RESTORE CODE」テキストボックスに入力することでファイルを復元することができます(※1)。

回復コードの入力処理

このランサムウェアは、パック処理や難読化処理が行われておらず、仕組みも非常に単純で、回復コードを入力することでファイルを復号できることから、冗談目的に作成されたと考えられます。しかし、他のランサムウェアと同様に、個人の大事な情報資産（画像や音楽、書類など）が、勝手に暗号化されることには変わりはありません。また、ファイルも正しく復元されないケースがある(※1)ことから注意が必要です。仕組みが単純なことから、ほかの攻撃者がコードを流用して悪用することも危惧されます。

なお、ESET 製品は、このマルウェアを「MSIL/Filecoder.HD の亜種 トロイの木馬」という名前で検出します。

ESET Endpoint Security V6.5 における検出画面

（※1） 当社で確認した検体では、復元されたファイルの一部データが欠落し正しく復元されない場合があることを確認しています。

ご紹介したように、4 月は Adobe Flash Player の脆弱性を突いた攻撃や、特徴的なランサム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/