MALWARE REPORT

マルウェアレポート

2019

上半期

安全なネット活用のための

セキュリティ情報

はじめに

本レポートでは、2019年1月から6月（以降2019年上半期）に検出されたマルウェア、および発生したサイバー攻撃事例についてご紹介します。

「第1章　2019年上半期マルウェア検出統計」では、2019年上半期にESET製品で検出されたマルウェアについて、日本国内と世界全体との検出を比較して傾向を分析します。また、特に検出数の多い3つのマルウェアについて詳しく分析します。「第2章　Emotetの感染を狙ったばらまき型メール」では、Emotetの概要とEmotetが登場してからの検出数の推移、さらに2019年上半期に確認された日本向けのばらまき型メールについて紹介します。「第3章　GandCrabの終焉」では、2018年初頭から継続的に観測され続け、突如サービスが終了することになったランサムウェアGandCrabについて、流行した要因を考察し、攻撃事例を紹介します。「第4章　圧縮・展開ソフトウェアの脆弱性を悪用したマルウェア」では、多くの圧縮・展開ソフトウェアが利用しているライブラリに発見された脆弱性について解説します。「第5章　売買される脆弱性情報」では、脆弱性を利用したサイバー攻撃の現状とディープウェブ・ダークウェブで売買される脆弱性情報の事例をご紹介します。

contents

1

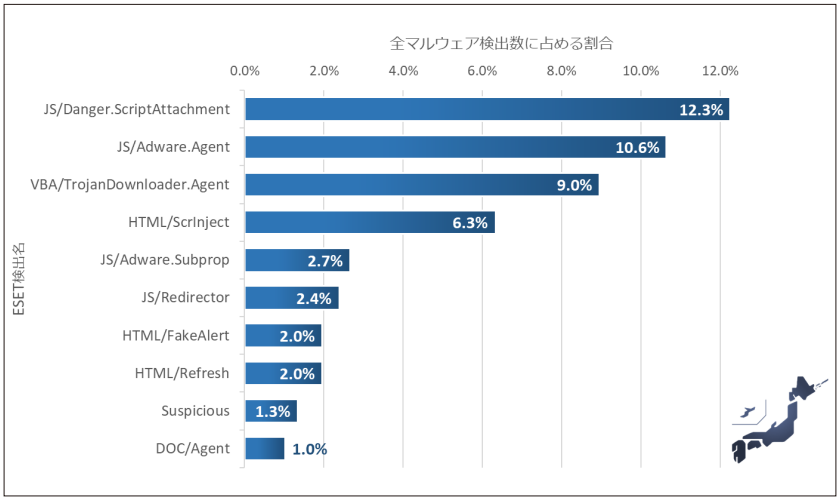
2019年上半期
マルウェア検出統計

第1章　　2019年上半期マルウェア検出統計

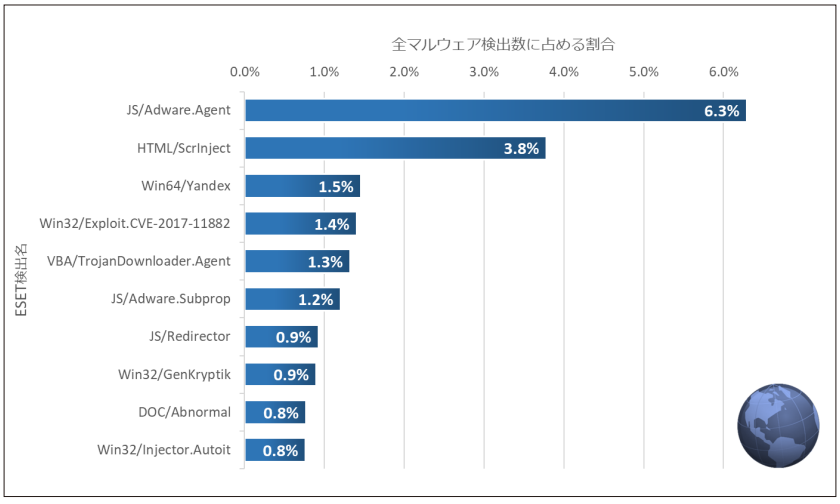
本章では、2019 年上半期に ESET 製品が国内外で検出したマルウェアの検出数に関する分析結果をご紹介します。

1.1　マルウェア検出数TOP10

2019 年上半期に日本国内で最も多く検出されたマルウェアは JS/Danger.ScriptAttachment です。日本国内で検出されたマルウェア総数のうち 12.3% を占めています。
JS/Adware.Agent（全体の 10.6%）、VBA/TrojanDownloader.Agent（全体の 9.0%）がそれに続きます。
これら 3 種類のマルウェアについては、1.3 節「国内検出数 TOP3」で詳しくご紹介します。
世界全体では、JS/Adware.Agent（全体の 6.3%）が最も多く検出されています。



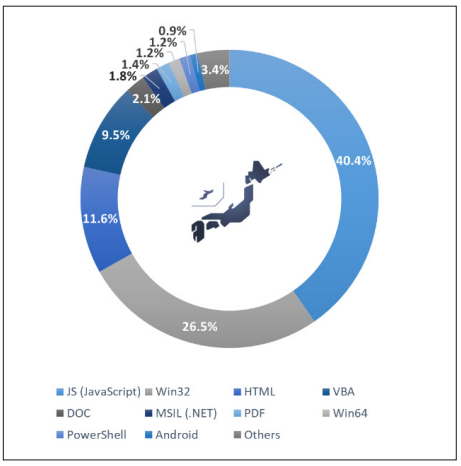
日本国内におけるマルウェア検出の割合（2019年上半期）



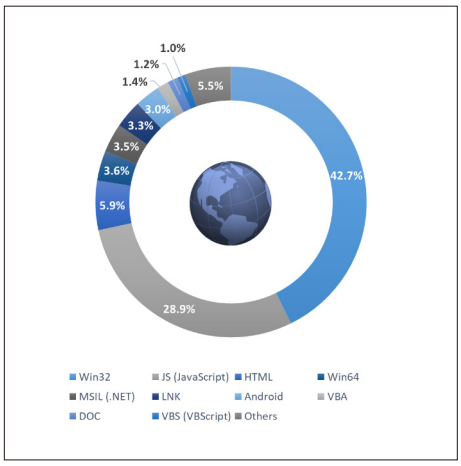
世界全体におけるマルウェア検出の割合（2019年上半期）

1.2 マルウェア検出数のファイル形式別割合

次にファイル形式別のマルウェア検出割合を見ていきます。
日本国内では JavaScript 形式や VBA(Visual Basic for Applications) 形式の検出が多く、メールによる攻撃が多いことを伺わせています。
世界では、Win32（32 ビット Windows アプリケーション）形式のマルウェアが最多となっています。



形式別マルウェア検出数（2019年上半期国内）

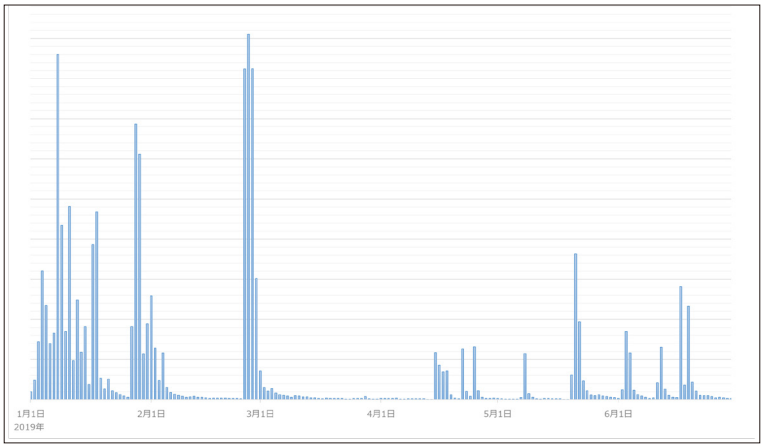


形式別マルウェア検出数（2019年上半期世界）

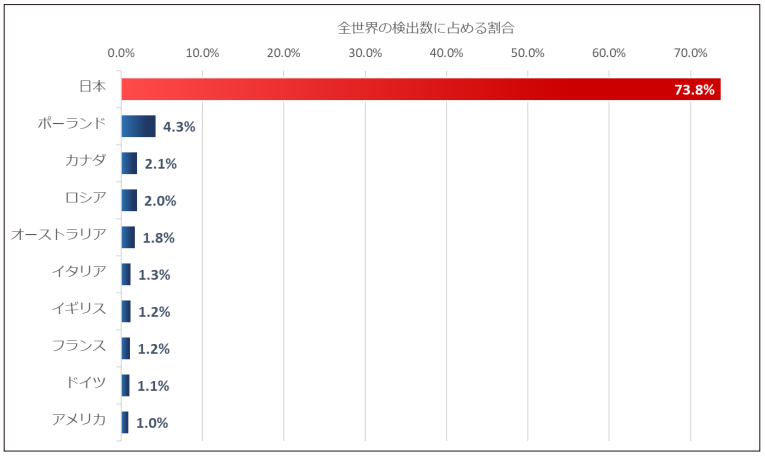
1.3 国内検出数TOP3

① JS/Danger.ScriptAttachment

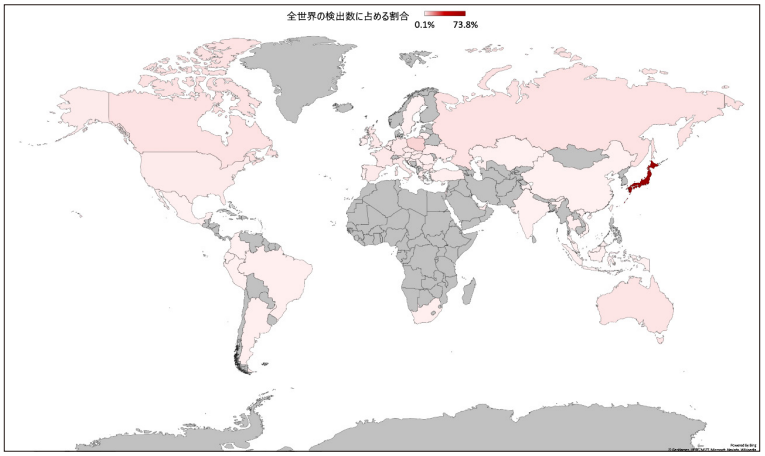
JS/Danger.ScriptAttachment は、電子メールに添付された悪意のある JavaScript ファイルの汎用検出名です。2018年にはほとんど観測されていませんでしたが、2019年1月以降多数の攻撃が確認されています。攻撃に使われた電子メールの件名には日本の芸能人の名前が含まれており、日本のユーザーを狙った攻撃と考えられています。実際に、日本における検出が大多数を占めています。



JS/Danger.ScriptAttachmentの国内検出数推移（2019年上半期）



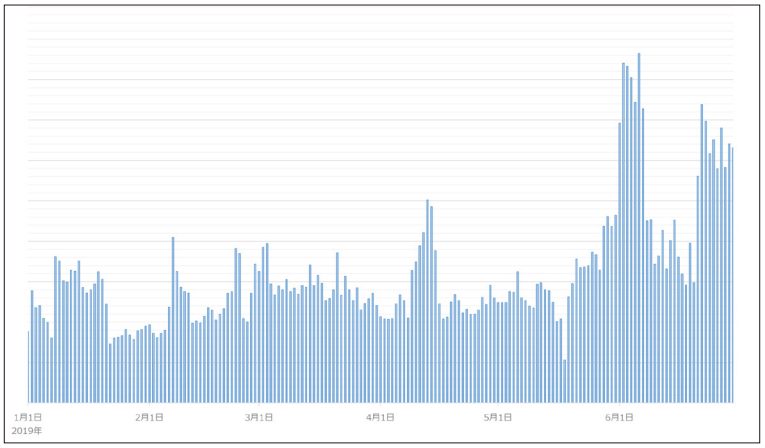
JS/Danger.ScriptAttachment検出数TOP10の国と地域（2019年上半期）



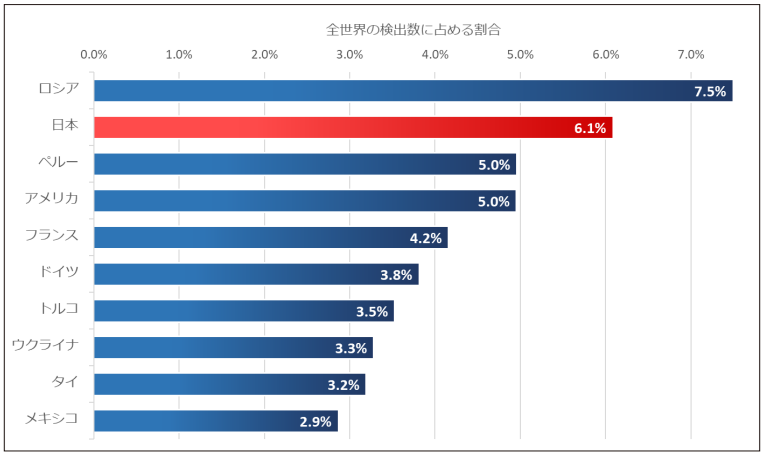
JS/Danger.ScriptAttachment検出数TOP50の国と地域（2019年上半期）

② JS/Adware.Agent

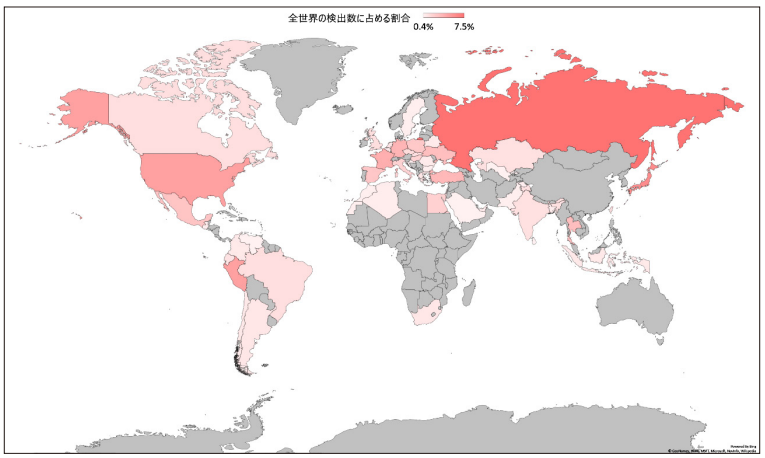
JS/Adware.Agent は Web ブラウザー上で不正な広告を表示する JavaScript で作成されたプログラムです。
2019 年年初から一定数検出されていますが、6 月に特に多く検出されています。
国別で比較した場合、日本における検出数はロシアに次いで 2 番目に多くなっています。



JS/Adware.Agentの国内検出数推移（2019年上半期）



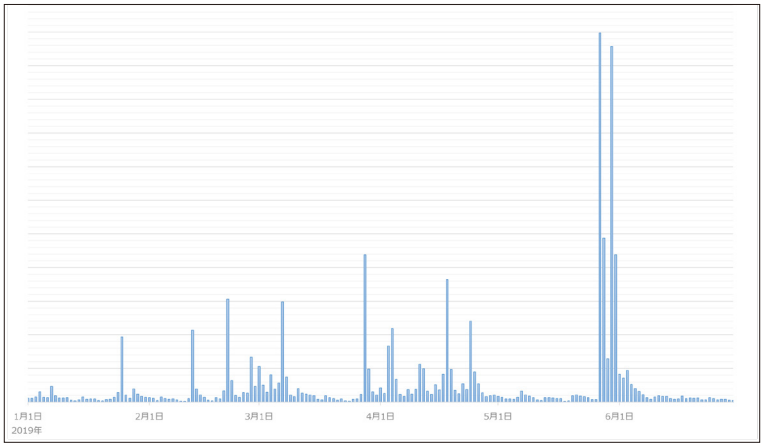
JS/Adware.Agent検出数TOP10の国と地域（2019年上半期）



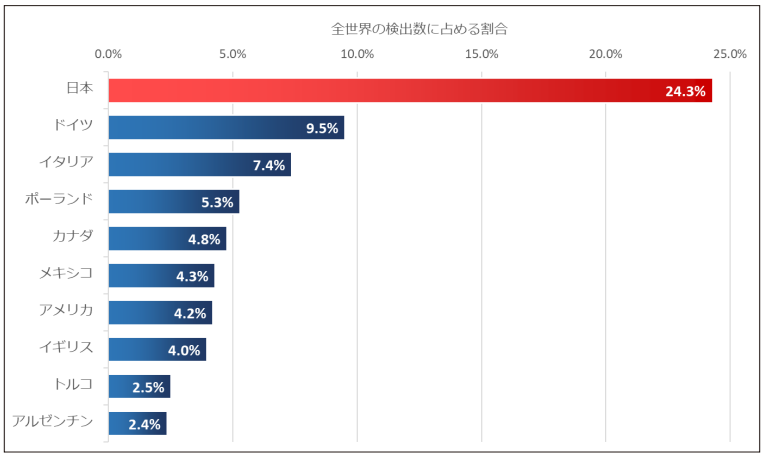
JS/Adware.Agent検出数TOP50の国と地域（2019年上半期）

③　VBA/TrojanDownloader.Agent

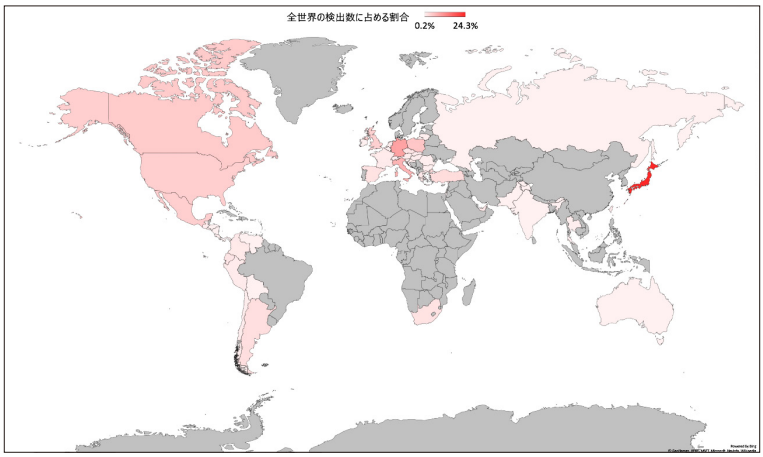
VBA/TrojanDownloader.Agent は Microsoft Office で利用されるプログラミング言語の VBA で作成されたダウンローダーです。ファイル形式は Microsoft Word 文書（拡張子 .doc/.docm 等）あるいは Microsoft Excel（拡張子 .xls/.xlsm 等）文書であることが大半です。一般的にばらまき型のメールに添付されることで配布拡散されます。日本国内における検出数は、世界の国と地域の中で最多です。



VBA/TrojanDownloader.Agentの国内検出数推移（2019年上半期）



VBA/TrojanDownloader.Agent検出数TOP10の国と地域（2019年上半期）



VBA/TrojanDownloader.Agent検出数TOP50の国と地域（2019年上半期）

以上が 2019 年上半期のマルウェア検出統計です。

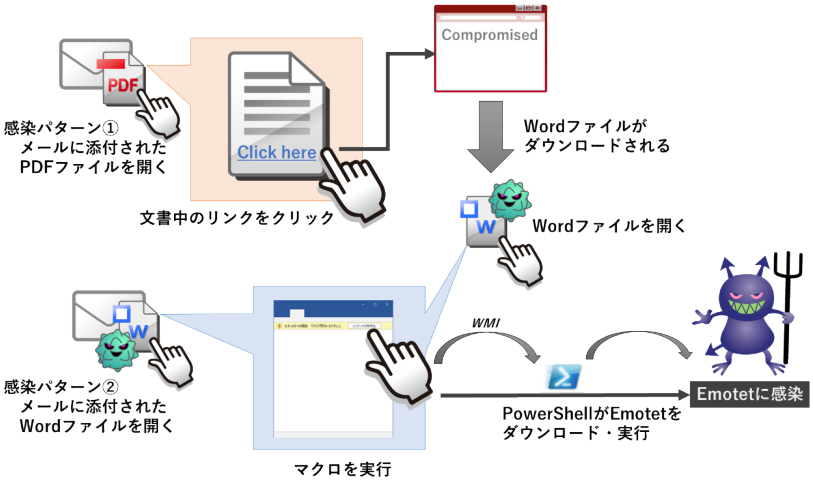
2

Emotetの感染を狙った
ばらまき型メール

第2章　　Emotetの感染を狙ったばらまき型メール

■ Emotetとは

Emotet は、バンキングマルウェアの一種ですが、追加のモジュール (機能) をダウンロードすることで様々な活動を行います。
「2018 年 11 月 マルウェアレポート」でもご紹介しているように、Emotet には「ネットワーク内に感染を拡大するワーム機能」、「メールの情報を窃取する機能」、「TrickBot などの他のマルウェアをダウンロードする機能」などの様々な機能が存在します。また、Emotet は頻繁に新機能が追加されています。
Emotet は主にメール経由で侵入し、添付ファイルやメール本文内のリンクからダウンロードしたファイルを実行することで感染します。

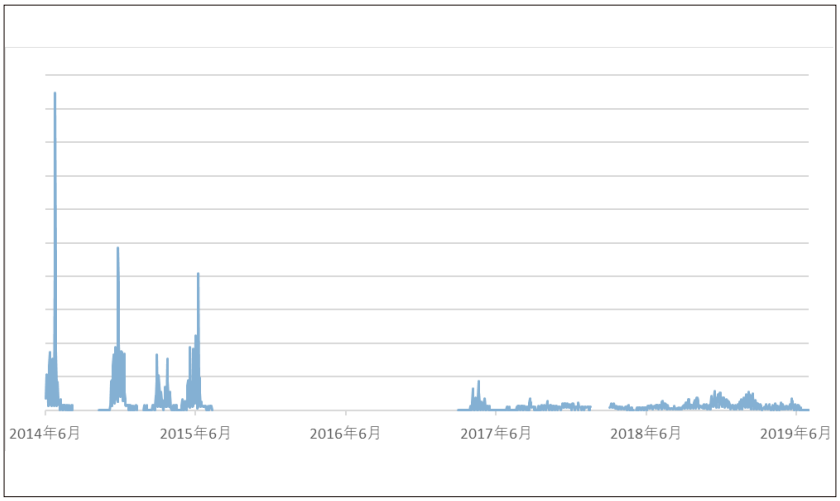


Emotetの感染の流れ

Emotet に感染した場合、ワーム機能によりネットワーク内に感染が拡大し、対処するためには、1 インシデントあたり最大で 100 万ドル（日本円でおよそ 1 億 600 万円：1 ドル 106 円で換算）を要するとも言われています。[i]
また、2019 年 5 月、都内の医療機関においても Emotet の亜種と推定されるマルウェアの感染が報告されています。

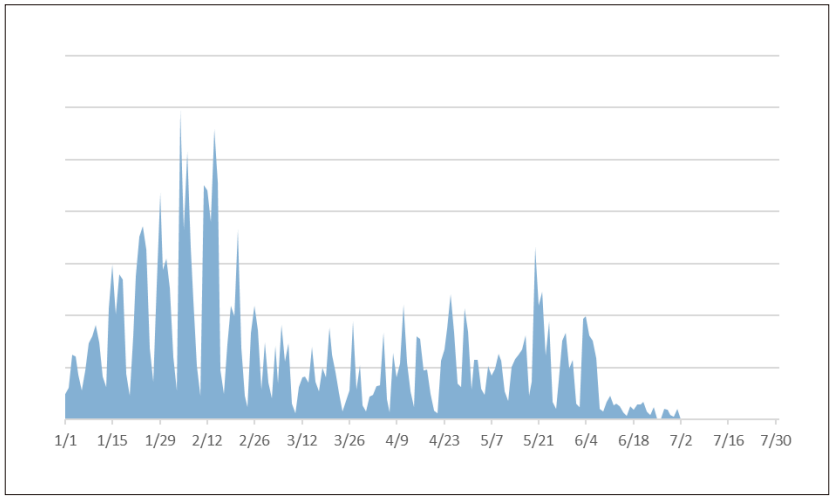
■ Emotetの推移

Emotet は 2014 年に登場し、その後も継続的に検出が確認されています。元々は、バンキングマルウェアとして利用されていましたが、現在では主に他のマルウェアに感染させるローダーとして利用されています。



世界全体におけるEmotetの検出数の推移[1]

ESET による検出では、Emotet が登場した 2014年は多く検出していますが、2015年後半～ 2017年初期はほとんど検出していないことが確認できます。そして、2017年 3月頃から再び検出され、2019年も継続的に検出しています。



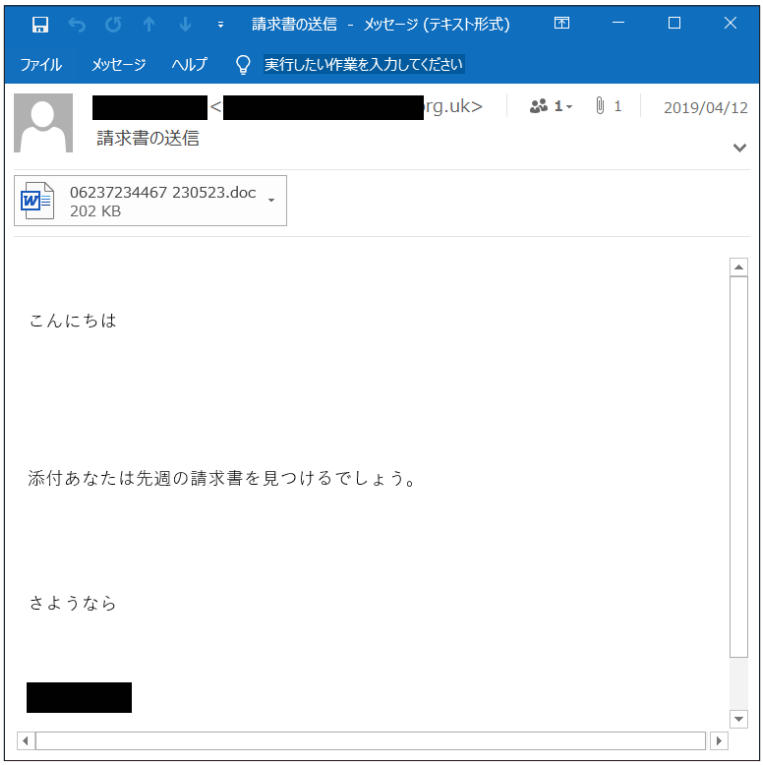
世界全体におけるEmotetの検出数(2019年)

2019年の検出を詳しくみると、6月中旬から検出数が減少し、7月はほとんど検出していないことが確認できます。
Emotet は過去にも活動を停止後、新規機能を追加して活動を再開しています。
このため、検出が減ってきたからと安心することはできず、今後も脅威になると考えられます。

1　Emotetとして検出したもののみ、kryptik等の汎用検出名は除く。EmotetはkryptikやそのほかのAI用検出名で検出されることがあります。

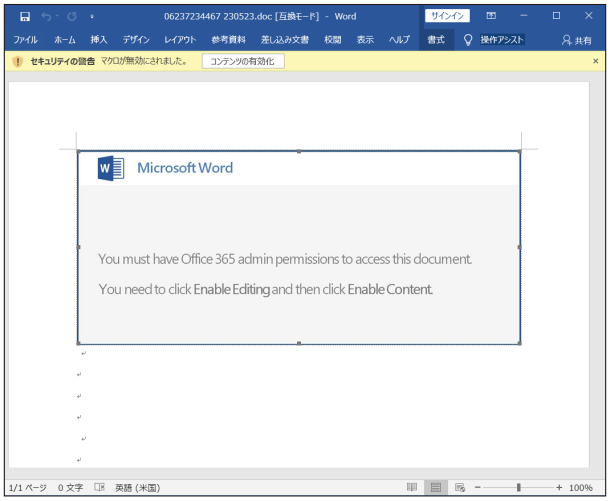
■ 上半期の日本でのばらまき型メール

バンキングマルウェア Emotet の感染を狙ったばらまき型メールは、昨年 11 月に日本で確認されて以来、2019 年上半期も複数回ばらまかれたことを確認しています。



Emotetの感染を狙ったばらまき型メールの一例

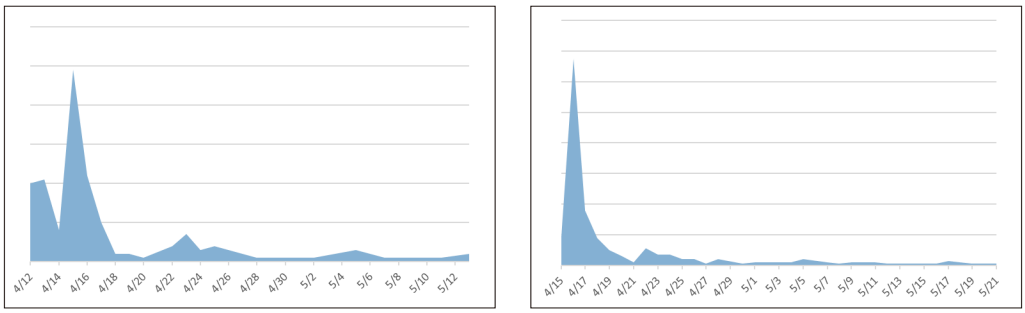
メールの件名や本文は日本語になっていますが、自動翻訳したような文章になっています。



メールに添付されたWordファイル

メールに添付された Word ファイルは、翻訳されておらず英語表記になっています。

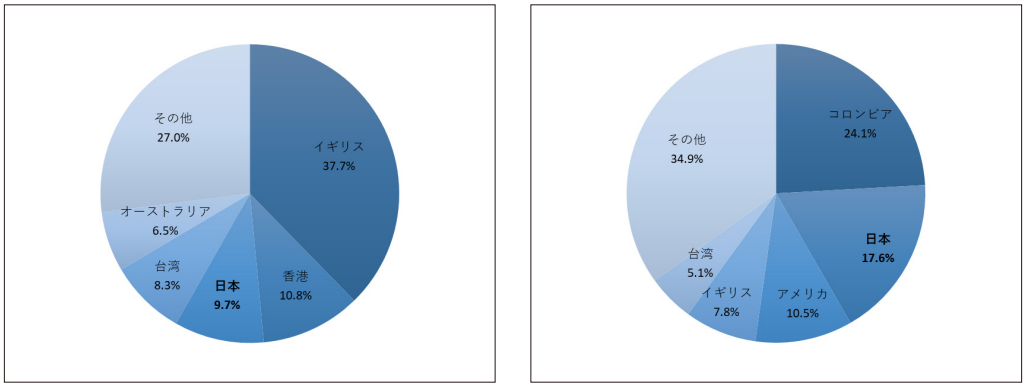
4 月に確認された Emotet の感染を狙ったばらまき型メールは、VBA/TrojanDownloader.Agent.NNZ、VBA/TrojanDownloader.Agent.NOU、GenScript.CXP などの検出名で検出します。



日本国内におけるVBA/TrojanDownloader.Agent.NNZ(左)および
VBA/TrojanDownloader.Agent.NOU(右)の検出数(2019年)

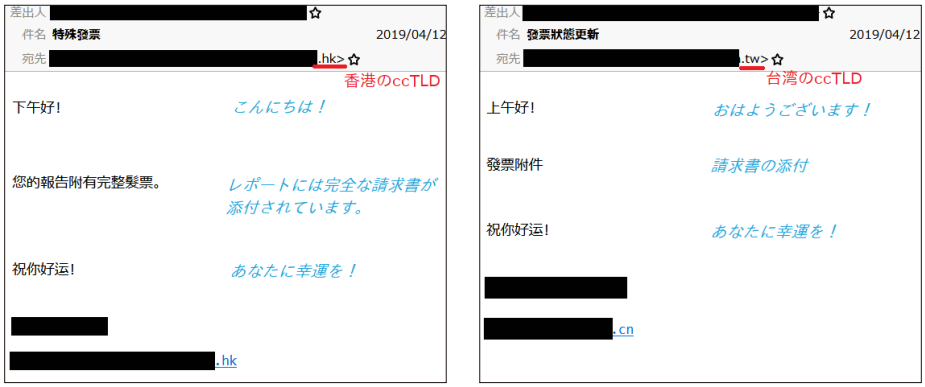
VBA/TrojanDownloader.Agent.NNZ および VBA/TrojanDownloader.Agent.NOU の検出数の推移を確認すると、4 月中旬に多くばらまかれていたことが確認できます。
VBA/TrojanDownloader.Agent.NNZ と VBA/TrojanDownloader.Agent.NOU は、それぞれ 4 月 12 日と 4 月 15 日からばらまかれたメールに添付された Word ファイルです。
これらは Word に表示される画像や VBA の処理の流れはほとんど同じですが、Emotet をダウンロードする通信先 URL やダウンロードしたファイルを保存するときのファイル名等が異なります。

次にこれらの国別検出割合を確認すると、様々な国で検出していることが確認できます。



VBA/TrojanDownloader.Agent.NNZ(左)および
VBA/TrojanDownloader.Agent.NOU(右)の国別検出割合(2019年上半期)

日本を狙ったばらまき型メールで多い Ursnif の感染を狙ったメールとは異なり、国を限定せずに感染拡大を図っていることが伺えます。



香港(左)や台湾(右)を狙ったばらまき型メール[2]

宛先の ccTLD（国別コードトップレベルドメイン）を確認すると、香港や台湾を狙ったメールであることが確認できます。これらのメールから、その国の言語に合わせて翻訳されたと考えられるメール文が使用されていることがわかります。

■ まとめ

本章では、2019 年上半期に複数回ばらまき型メールが確認された Emotet について紹介しました。
Emotet は当初、バンキングマルウェアとして利用されていましたが、現在では他のマルウェアのローダーとして使われています。Emotet はモジュール型のマルウェアであり、追加のモジュールをダウンロードすることで、様々な活動を行います。また、攻撃者により頻繁に更新・機能追加されています。
現在は一時的に検出が減少していますが、今後は攻撃者により機能が追加され、活動が活発になる恐れがあります。また、ばらまき型メールのメール本文や添付ファイルの日本語がより高度になっていく可能性があるため、今後とも注意が必要です。

使用している PC が Emotet に感染しないためにも、セキュリティソフトの導入、セキュリティパッチの適用、最新の脅威を知ることなど基本となる対策を行うことが重要です。
また、Emotet を配布するサーバーとして、国内の Web サイトが改ざんされる事例が報告されています。[ii]
Web サイトの管理者は古い状態のまま放置されていないか確認し、プログラムの更新や脆弱性のあるプラグインの削除などを行い、知らないうちに攻撃者に悪用されないように適切に管理することが重要です。

参考文献

- 2018年11月 マルウェアレポート | マルウェア情報局
  https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1811.html#anc_02
- 2019年6月 マルウェアレポート | マルウェア情報局
  https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1906.html
- Emotet launches major new spam campaign | WeLiveSecurity
  https://www.welivesecurity.com/2018/11/09/emotet-launches-major-new-spam-campaign/

2　水色の斜体文字は自動翻訳した日本語を追加したものです。

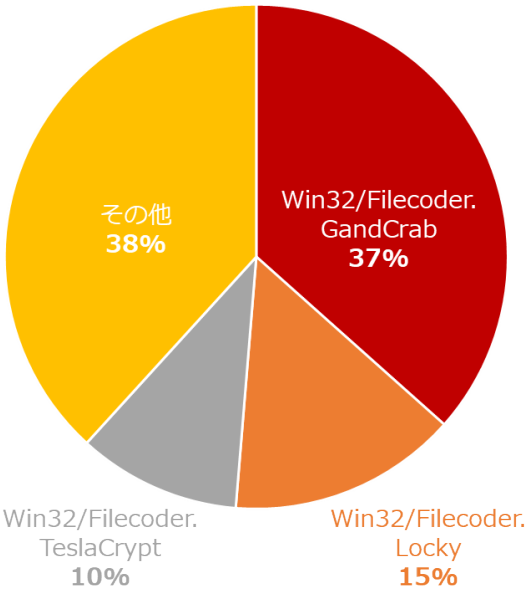
3 GandCrabの終焉

第3章　　GandCrabの終焉

■ GandCrabとは

GandCrab は、感染した端末上のファイルを暗号化し、復号するための身代金を要求するランサムウェアです。ESET 製品では、本マルウェアを Win32/Filecoder.GandCrab の検出名で検出します。

本マルウェアは、2018 年初頭に登場して以来、継続的に観測されています。欧州刑事警察機構（ユーロポール）によると、登場してからわずか 1 ヵ月で 5 万人もの被害が出たことが報告されています。[iii] 2019 年上半期においては、日本国内で最も多く検出されたランサムウェアでした。



日本国内で検出されたランサムウェアの比率（2019年上半期）

このように非常に流行していたランサムウェアでしたが、2019 年 5 月末、突如 GandCrab 作成者が提供サービスをやめることを発表しました。発表内で作成者は、20 億ドル以上の収益を上げたことを示しました。

■ GandCrabが流行した要因

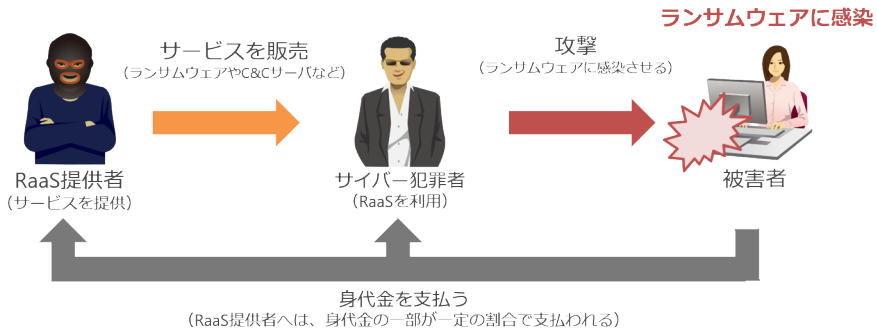
GandCrab が多く検出された主な要因は、２つ考えられます。

○ **要因 1**：検体の頻繁なアップデート
GandCrab は、メジャーなものだけで 4 回もアップデートが行われたため、Version 5 まで存在します。
過去のアップデートで実装された機能の一部は以下のとおりです。

- 旧バージョンの復号ツールを無効化
- セキュリティ製品による検知を回避
- 暗号化したファイルの拡張子を変更
- 身代金を要求する脅迫文の変更
- 身代金支払いページの変更
- 暗号アルゴリズムの変更による暗号処理の高速化
- 新たなエクスプロイトキットの使用

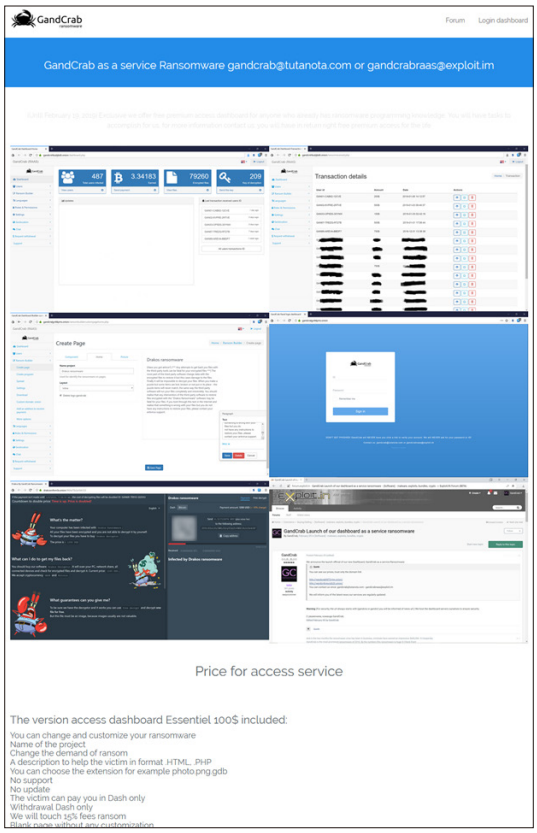
2019 年上半期中には、Version 5.1 ～ 5.3 が多く確認されました。頻繁に新しいバージョンが出現するため、対策が難しかったことが流行の要因の 1 つであると考えられます。

○ **要因 2**：Ransomware as a Service (RaaS) の存在
RaaS は、サイバー犯罪者向けのサービスで、ダークウェブ上に存在します。RaaS 提供者は、サイバー犯罪者に対して、攻撃に必要なプログラム（ランサムウェア本体、ダウンローダー、C&C サーバー等）を販売します。そして、ランサムウェアの被害者が身代金を支払った場合、身代金は RaaS 提供者とサイバー犯罪者で分配される仕組みになっています。



RaaSの仕組み

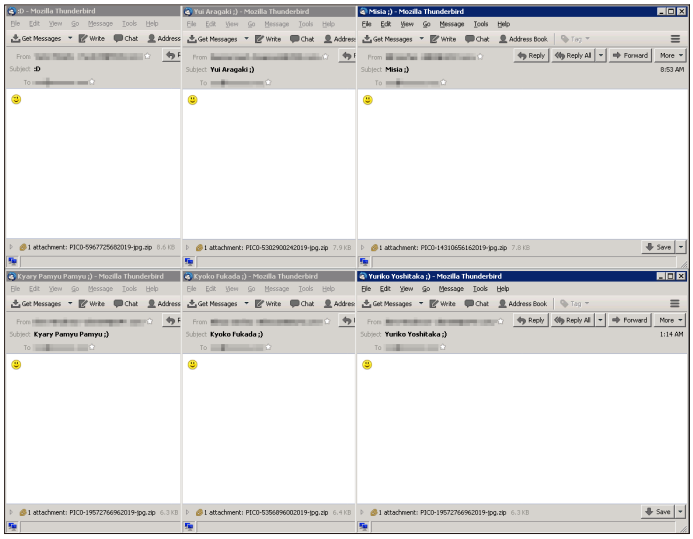
GandCrab は、RaaS で販売されていたマルウェアの 1 つです。RaaS が存在する場合、サイバー犯罪者はランサムウェア等を開発する必要がないので、攻撃が容易にできます。そのため、GandCrab を用いた攻撃が多く確認されたことが考えられます。



GandCrab用RaaSの広告に使用された画像

■ GandCrabが用いられた攻撃事例

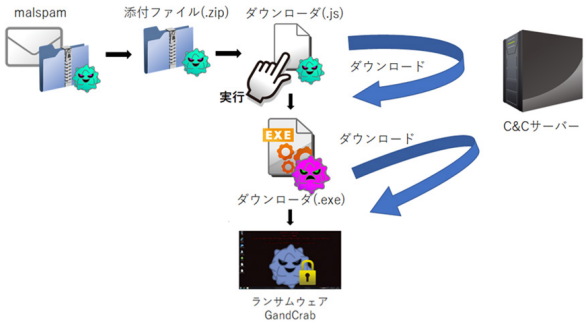
2019 年の 1 月と 2 月は、GandCrab の感染を狙ったばらまき型メールが多数観測されました。ばらまき型メールの件名や添付ファイルの名前には、Love you といった文字列が含まれていた時期があったことから、ESET ではこの攻撃を“Love You” malspam[3] campaign と呼んでいます。
件名には日本の芸能人の名前がローマ字で記載されている時期もありました。



“Love you” malspam campaignにおけるメール例

3　malware spamまたはmalicious spamの略です。ここでは、マルウェア感染を狙ったスパムメールを指します。

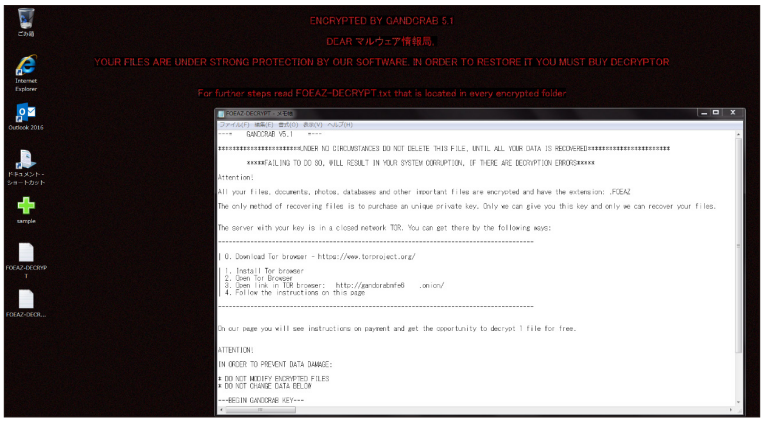
メール添付されている zip ファイルは、GandCrab ではなくダウンローダーです。zip ファイルを解凍し、ダウンローダーを実行すると、C&C サーバーと通信を行い、最終的に GandCrab をはじめ、様々なマルウェアをダウンロードします。



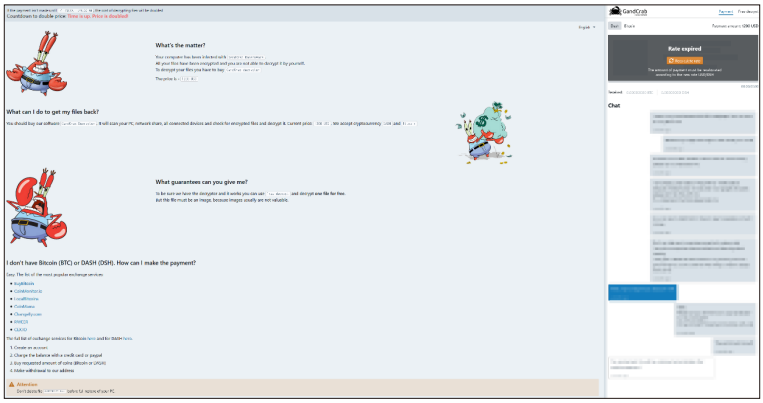
“Love You” malspam campaignにおけるGandCrabに感染するまでの経路

“Love You” malspam campaign で最終的に感染する GandCrab には、Version5.1 と 5.2 のものが確認されました。

感染すると以下のような脅迫文と身代金の払い方が表示されます。



GandCrab感染後に表示される脅迫文(Version 5.1)



身代金の支払いページ

■ 今後のランサムウェアによる脅威

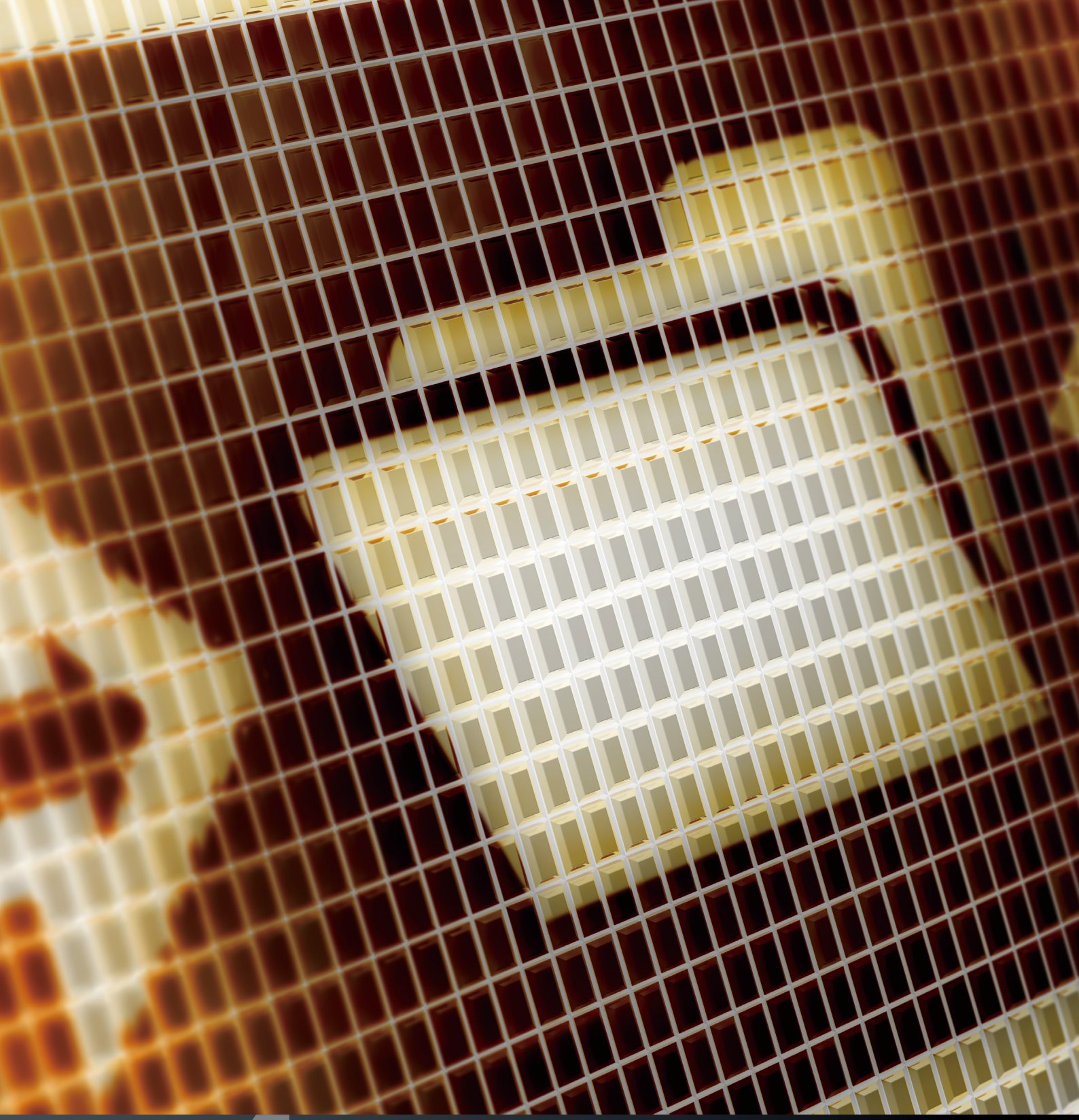
2018 年初頭から確認され続けた GandCrab は終焉を迎えましたが、ランサムウェアによる脅威が去ったわけではありません。GandCrab 以外のランサムウェアによる事例も 2019 年上半期に確認されています。メールを媒介とする事例以外に、脆弱性を悪用する事例等も確認されています。

- JNEC.a（ESET 検出名：MSIL/Filecoder.SC トロイの木馬）による事例
  2019 年 3 月：WinRAR の脆弱性（CVE-2018-20250）を悪用

- Sodinokibi (ESET 検出名：Win32/Filecoder.Sodinokibi) による事例
  2019 年 4 月：Oracle WebLogic の脆弱性（CVE-2019-2725）を悪用

- Crysis（ESET 検出名：Win32/Filecoder.Crysis）
  2019 年 4 月：ばらまき型メールを媒介とし、ESET 社製正規ツールを悪用

ランサムウェアの対策には、通常の対策に加えて、バックアップを取っておくことが有効です。
もしランサムウェアに感染してしまった場合は、身代金を支払うのではなく、復号ツールが公開されているかどうかを確認してみることを推奨します。GandCrab においては、Version 1、Version 4 、Version5 - V5.2 に対応した復号ツールが「No More Ransom[iv]」で公開されています。また、このサイトでは、GandCrab 以外のランサムウェアに対しても復号ツールが公開されています。



4 圧縮・展開ソフトウェアの脆弱性を悪用したマルウェア

第4章　　圧縮･展開ソフトウェアの脆弱性を悪用したマルウェア

2019 年 2 月、多くの圧縮・展開ソフトウェアが利用しているライブラリ UNACEV2.DLL に脆弱性（以降、本脆弱性と記載）が発見されました。さらに、その脆弱性を悪用するマルウェアが確認されています。

■ 脆弱性の概要と影響を受けるソフトウェア

本脆弱性（CVE-2018-20250）はディレクトリトラバーサルの脆弱性です。ディレクトリトラバーサルとは、通常はアクセスできないディレクトリやファイルにアクセスする脆弱性（攻撃手法）のことです。攻撃者によって細工された圧縮ファイルを展開した場合、任意のフォルダーに悪意のあるファイルが展開されるおそれがあります。

WinRAR（バージョン 5.61 以前）のほか、UNACEV2.DLL を利用しているすべての圧縮・展開ソフトウェアが本脆弱性の影響を受ける可能性があります。
WinRAR は既に修正版（バージョン 5.70）が公開されています。[v]
以前のバージョンをお使いの場合は速やかにアップデートされることを推奨します。

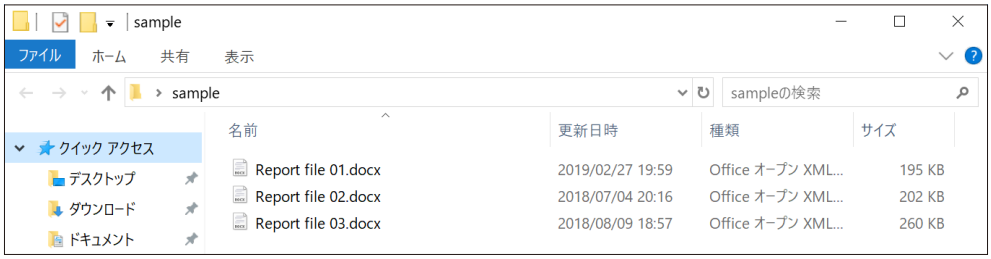
■ 本脆弱性を悪用するマルウェア

本脆弱性を悪用するマルウェアがいくつか確認されています。
「2019 年 3 月 マルウェアレポート」ではランサムウェア JNEC.a を紹介しましたが、ここではバックドアの事例を紹介します。

今回確認したバックドア（ESET 検出名：Win32/Agent.ZUR）は CVE-2018-20250 を悪用した圧縮ファイルに格納されています。細工された圧縮ファイルを WinRAR などの圧縮・展開ソフトウェアで開くと、ドキュメントファイルと C ドライブへの参照が表示されます。

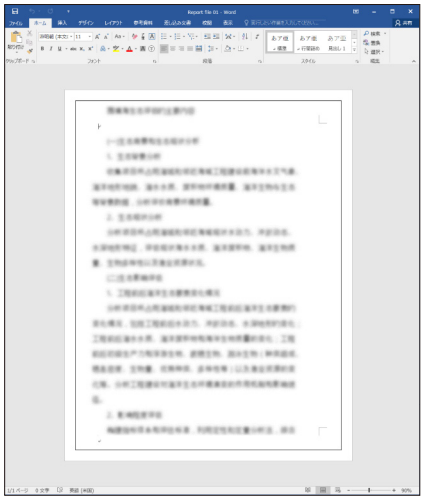
細工された圧縮ファイルの中身

圧縮ファイルを展開すると、ユーザーが指定したフォルダーに 3 つの Microsoft Office 文書が展開されます。これらのファイルは、元の圧縮ファイルはマルウェアではないとユーザーに信じさせるためのおとり（デコイファイル）であると考えられます。

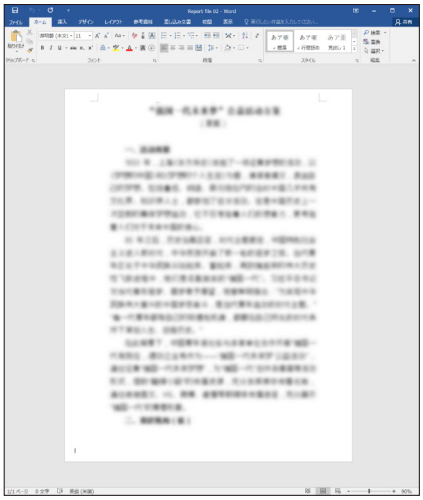


展開されたフォルダー

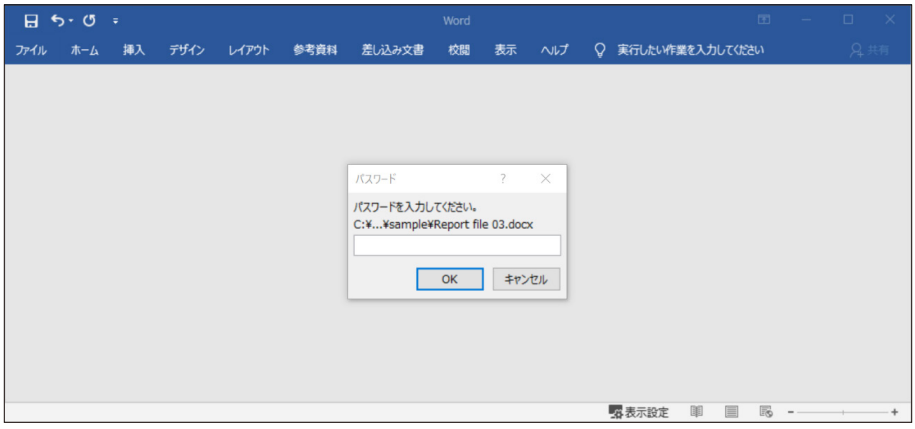
はじめの 2 つのデコイファイル（Report file 01.docx、Report file 02.docx）には何らかの文章が書かれていますが、モザイク処理されており内容を読み取ることはできません。また、3 つ目のデコイファイル（Report file 03.docx）はパスワードで保護されており、開くことはできません。



Report file 01.docx



Report file 02.docx



Report file 03.docx

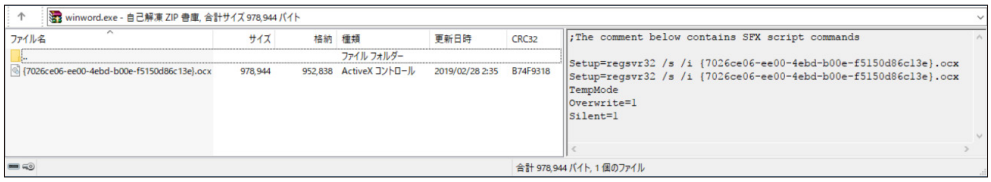
デコイファイルの展開と同時に、スタートアップフォルダーに自己解凍形式の圧縮ファイル（winword.exe）が展開されます。スタートアップフォルダーに含まれるプログラムは PC 起動時に自動で実行されます。このファイルが展開されたことはユーザーには通知されません。

自己解凍形式の圧縮ファイル

この圧縮ファイルは実行（展開）時に以下のコマンドを実行します。

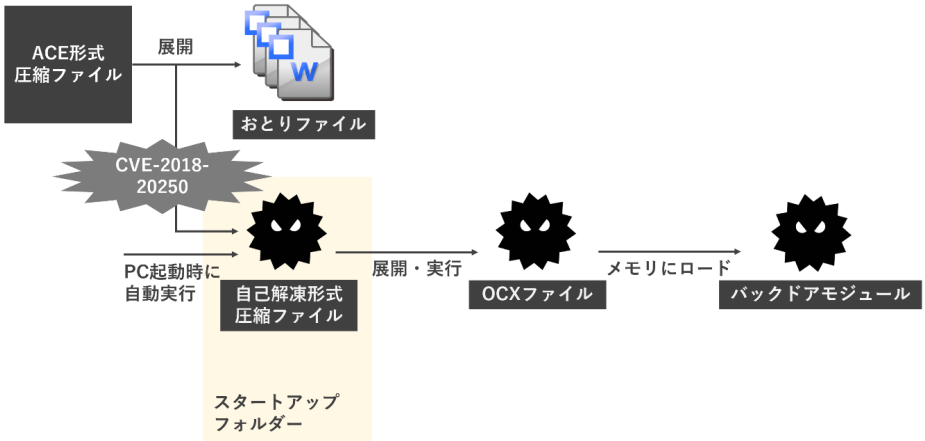
```
regsvr32 /s /I {7026ce06-ee00-4ebd-b00e-f5150d86c13e}.ocx
```

Windows 標準機能の regsvr32 によって、OCX 形式[4] のプログラムがシステムに登録されます。最終的にバックドアモジュールがメモリ上にロードされます。



自己解凍形式ファイルの中身

本マルウェアの感染の流れを以下にまとめます。



本マルウェアの感染の流れ

4　ActiveXコントロール形式のプログラムファイル。DLLと同じく他のプログラムに読み込まれることによって動作する。

■ まとめ

多くの圧縮・展開ソフトウェアが利用しているライブラリ UNACEV2.DLL には脆弱性があり、その脆弱性を悪用したマルウェアが数多く確認されています。

脆弱性のある古いバージョンの圧縮・展開ソフトウェアをお使いの場合は、速やかに最新版にアップデートされることを推奨します。お使いの圧縮･展開ソフトウェアで脆弱性が修正されていない場合は､手動で UNACEV2.DLL を削除するか､脆弱性が修正されるまでの間は脆弱性に対応済みの他のソフトウェアを使用されることを推奨します。

本事例に限らず、脆弱性を悪用した攻撃を防ぐためにはアプリケーションは常に最新の状態に保つことが大切です。

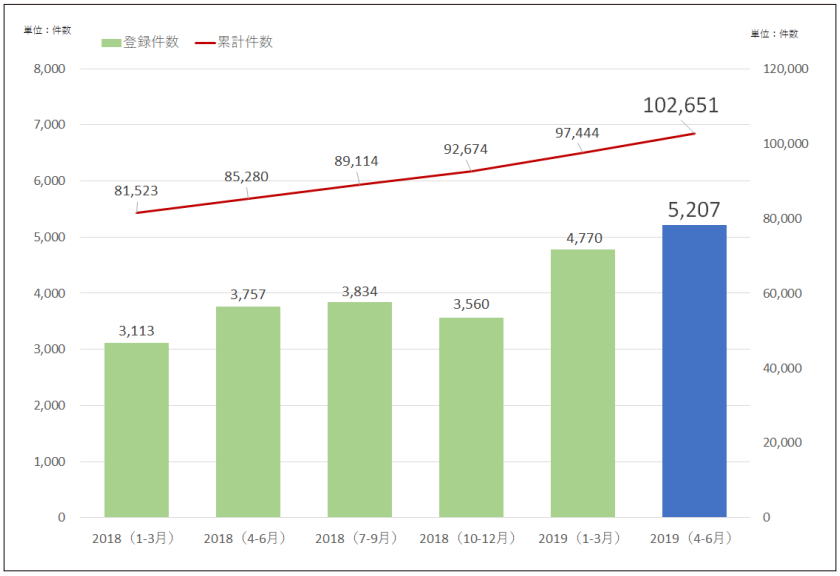
5 売買される脆弱性情報

第5章　　売買される脆弱性情報

■ 日々発見・報告される脆弱性

最近、ニュースなどで「脆弱性」という言葉をよく耳にするようになりました。
ソフトウェアにおける「脆弱性」とは、オペレーティングシステムやプログラムの不具合、設計上のミスなどが原因で発生するセキュリティ上の欠陥を意味します。
最近では、今年 5 月に、リモートデスクトップサービスに関連する脆弱性（BlueKeep）が発見され、マイクロソフトが Windows XP などサポートを終了した OS に対して、異例の更新プログラムを提供したことが話題となりました。[vi]
現在、脆弱性は、多数発見・報告されており、その数は増加傾向にあります。

以下のグラフは、2019 年第 2 四半期（4 ～ 6 月）に IPA 情報処理推進機構が運営する「脆弱性情報データベース JVN iPedia」に登録された脆弱性情報の推移です。



脆弱性情報の登録件数

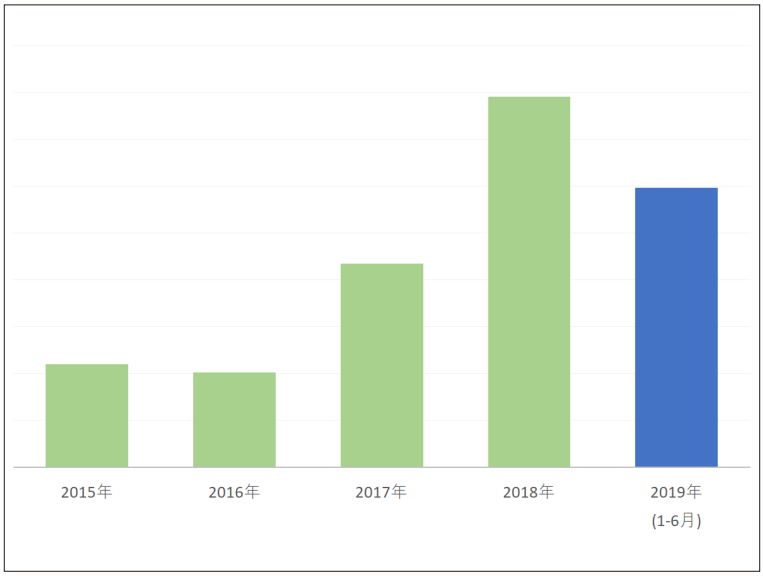
出典元:独立行政法人 情報処理推進機構 ホームページ
脆弱性対策情報データベース JVN iPediaの登録状況 [2019年第2四半期(4月～6月)][vii]

2019 年第 2 四半期（4 ～ 6 月）に登録された脆弱性の件数は 5,207 件に上り、昨年の第 2 四半期（2018 年 4 ～ 6 月）の登録件数 3,757 件を大きく上回りました。
また、2007 年 4 月からの累計で約 10 万件の大台も突破し、依然としてその数は増加傾向にあります。

■ 継続的にサイバー攻撃に悪用される脆弱性

このように多数脆弱性が発見・報告される状況の中で、発見された脆弱性がサイバー攻撃に悪用される事例も多く確認されており、組織にとって大きな脅威となっています。

以下のグラフは、ESET 製品で検出した脆弱性を利用した攻撃（文字列“CVE”を含む検出名）の数です。



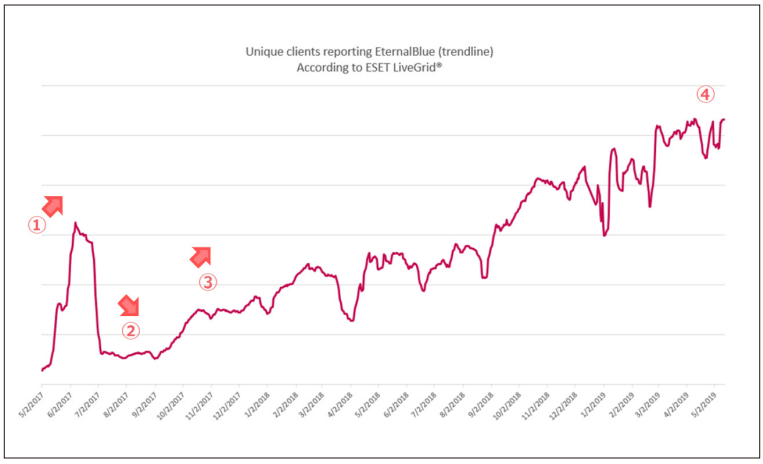
ESET製品で検出した脆弱性を利用した攻撃(国内)

2018 年に検出した脆弱性を利用した攻撃の件数は、2016 年の約 4 倍に上ります。
また、2019 年上半期（1 月～ 6 月）に検出した脆弱性を利用した攻撃の件数は、既に半年間で昨年 2018 年の約 75% に上り、昨年の検出件数に迫る勢いです。

これらのサイバー攻撃に使用される脆弱性の中には、長期にわたり継続的にサイバー攻撃に使用される脆弱性も存在します。たとえば、2 年前に世界規模で感染を拡大したランサムウェア WannaCryptor（別名：WannaCry）で使用された EternalBlue が代表的な例です。

EternalBlue は、ファイル共有やプリンタ共有で使用される通信プロトコル Server Message Block 1.0 (SMB v1.0) の内部処理に起因する脆弱性を利用したプログラムで、悪用するとリモートから任意のコードを実行することができます。そのため、ランサムウェア WannaCryptor では、他のコンピューターに感染を広げる目的で EternalBlue が悪用され、世界的規模で感染が拡大した要因の 1 つとなりました。
WannaCryptor の脅威は収束していますが、WannaCryptor で使われた EternalBlue を悪用した攻撃は、現在でも継続して観測されています。

以下のグラフは、EternalBlue を悪用した攻撃を検出したクライアントの数です。



EternalBlueの攻撃を検出したクライアントの数
(出典：WeLiveSecurity「EternalBlue reaching new heights since WannaCryptor outbreak」[viii])

2017 年 5 月から 6 月、WannaCryptor の大規模感染により、多くのコンピューターで、EternalBlue を悪用した攻撃を検出しました（グラフ①の箇所）。 その後、WannaCryptor の脅威が収束すると共に、EternalBlue を悪用した攻撃も減少します（グラフ②の箇所）。しかし、2017 年 9 月頃から増加に転じ（グラフ③の箇所）、現在では、WannaCryptor の大規模感染時（グラフ①の箇所）を上回る数のクライアントで、攻撃を観測しています（グラフ④の箇所）。

上記のように EternalBlue を悪用した攻撃が継続して行われている要因は、複数考えられます。たとえば、要因の 1 つとして、古いバージョンのファイル共有プロトコルである SMB 1.0 を使用しているコンピューターが、いまだにインターネット上に多く公開されており、これらのコンピューターに EternalBlue の更新プログラム（MS17-010）が適用されていないことが考えられます。

以下の図は、インターネットに接続されている機器情報を検索するサービス Shodan で検索した SMB 1.0 のポートをインターネット上に公開しているコンピューターの数です。

Shodanの検索結果画面（2019年6月現在） 出典：Shodan

ご覧の通り、SMB 1.0 のポートをインターネット上に公開しているコンピューターは、約 100 万台以上存在します。これらのコンピューターは、ほとんどがアメリカに存在しています。しかし、日本でも約 7 万台以上のコンピューターが存在しており、EternalBlue の更新プログラム（MS17-010）が適用されていないコンピューターも多く含まれていると推測します。

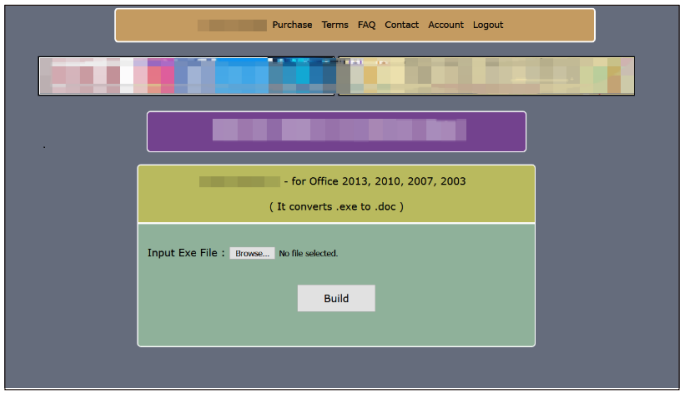
また、他の要因としては、WannaCryptor の大規模感染以降、他のマルウェアでも EternalBlue が悪用されるようになったことやペネトレーションテストの目的で EternalBlue が使用されていることが考えられます。
たとえば、EternalBlue は、WannaCryptor の大規模感染以降、2017 年 7 月に流行した DiskCoder.C（別名 :Petya）や 2018 年 4 月に流行した Satan といったランサムウェアをはじめ、仮想通貨を採掘するマイニングマルウェアや一部の標的型攻撃（Sednit など）でも悪用されており、これらのマルウェアの感染拡大を助ける役割を果たしています。
また、現在では Metasploit などのペネトレーションツールを使って、EternalBlue を悪用した攻撃を簡単にテストすることができます。そのため、ペネトレーションテストなどセキュリティ目的での検出も一部含まれていると考えられます。

以上のように、現在、発見された脆弱性が継続的にサイバー攻撃に悪用され、組織にとって大きな脅威となっています。

■ ディープウェブやダークウェブで売買される脆弱性情報

このような状況の中、ディープウェブやダークウェブ上では、脆弱性情報や脆弱性を悪用したプログラムなどが「商品」として取引されています。

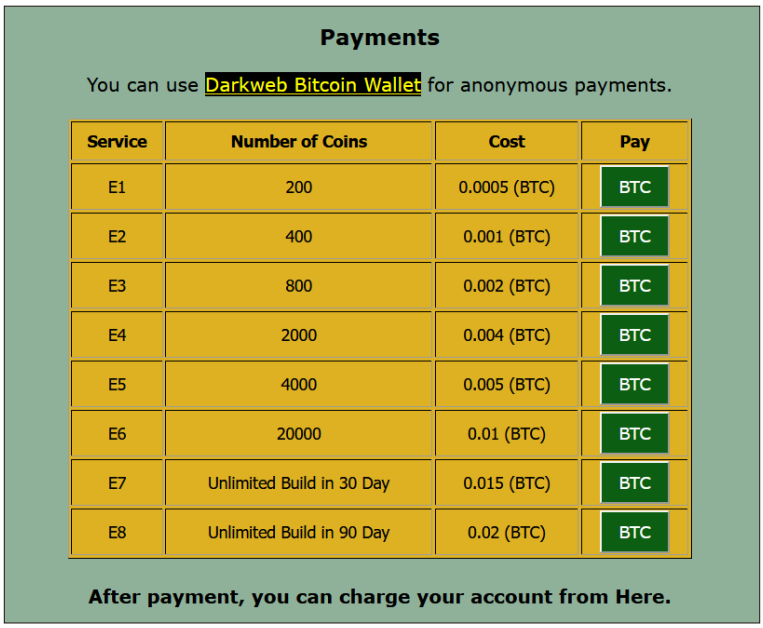
たとえば、以下のサイトは、Microsoft Office の脆弱性を悪用したマルウェアを作成できるサービスです。



Microsoft Officeの脆弱性を悪用するマルウェア作成画面

Web サイトの画面から攻撃対象のクライアントで実行させたいプログラム（マルウェア）を指定すると、指定したプログラムが埋め込まれた Word ファイルが作成されます。
この Word ファイルを実行すると Microsoft Office の脆弱性が悪用され、埋め込まれたプログラム（マルウェア）を自動的に起動することができます。そのため、作成した Word ファイルは、電子メールなどに添付し攻撃対象へ送信するなど、さまざまなサイバー攻撃に利用することができます。また、このサービスで設定できる Microsoft Office の脆弱性は、数パターン用意されており、複数の脆弱性を組み合わせる設定やインターネット上にアップロードしたマルウェアをダウンロードさせる設定なども可能です。

このサービスを利用するには、事前にサービス内で使用できるコインを仮想通貨で購入する必要があります。先ほどの Microsoft Office の脆弱性を悪用した Word ファイルは、1 ファイルにつき約 70 円程度（1 ビットコイン 1,077,344 円で換算）で作成することが可能です。



Payments

You can use Darkweb Bitcoin Wallet for anonymous payments.

Service	Number of Coins	Cost	Pay
E1	200	0.0005 (BTC)	BTC
E2	400	0.001 (BTC)	BTC
E3	800	0.002 (BTC)	BTC
E4	2000	0.004 (BTC)	BTC
E5	4000	0.005 (BTC)	BTC
E6	20000	0.01 (BTC)	BTC
E7	Unlimited Build in 30 Day	0.015 (BTC)	BTC
E8	Unlimited Build in 90 Day	0.02 (BTC)	BTC

After payment, you can charge your account from Here.

サービスの価格画面

上記のサービス以外にも、ディープウェブやダークウェブ上では、脆弱性を売り買いできるサービスや脆弱性などを利用したサイバー攻撃を代行するハッキングサービス、マルウェアの販売サービス（Malware as a Service）なども存在します。

以下のハッキングサービスでは、更新プログラムなどが提供されていない脆弱性などを使用して、電子メールやFacebook、Web サイトの改ざんを請け負う宣伝されています。また、費用は、ハッキングの規模や品質に応じて、約23,000 円（200 ユーロ）[5] から依頼することができます。

ハッキングサービスのWebサイト画面

5　1ユーロ 118円で換算

このようにディープウェブやダークウェブ上では、脆弱性情報や脆弱性を悪用したプログラムなどが商品として取引されており、技術力のないサイバー犯罪者でも比較的簡単に利用することも可能です。

■ まとめ

以上のように、現在、脆弱性がサイバー攻撃に悪用され、ディープウェブやダークウェブ上では、脆弱性情報や脆弱性を悪用したプログラムなどが「商品」として取引されています。
そのため、組織にとって大きな脅威となっています。

脆弱性は、対策がとられないまま放置すると大きな被害につながる可能性があります。
また、場合によっては、脆弱性を放置したことにより、他の第三者に被害を与えてしまう危険性もあります。そのため、脆弱性の管理は、システムのセキュリティを維持する上で非常に重要な要素の１つと言えます。
日々発見・公開される脆弱性に対して、更新プログラムの適用やバージョンアップ作業を迅速に行うには、守るべき資産の把握をはじめ、定期的な脆弱性情報の収集・分析、適用する更新プログラム優先順位の検討、脆弱性管理を効率化するソフトウェアの導入・運用など、計画的に準備をしておく必要があります。
被害が出る前に、脆弱性管理が適切に行われているか、今一度、確認してみてはいかがでしょうか。

参考：脆弱性管理に関する情報

- IPAテクニカルウォッチ「脆弱性対策の効果的な進め方（実践編）」[ix]
- IPAテクニカルウォッチ「脆弱性対策の効果的な進め方（ツール活用編）」[x]
- パッチが当てられていない状況をなるべく早く解消する方法｜マルウェア情報局[xi]

引用・出典元

i　Emotet Malware | CISA
https://www.us-cert.gov/ncas/alerts/TA18-201A

ii　インシデント報告対応レポート | JPCERT/CC
https://www.jpcert.or.jp/pr/2019/IR_Report20190711.pdf

iii　FREE DATA RECOVERY KIT FOR VICTIMS OF GANDCRAB RANSOMWARE NOW AVAILABLE ON NO MORE RANSOM | European Police Office
https://www.europol.europa.eu/newsroom/news/free-data-recovery-kit-for-victims-of-gandcrab-ransomware-now-available-no-more-ransom

iv　No More Ransom
https://www.nomoreransom.org/ja/index.html

v　【重要】脆弱性に対応したバージョン 5.70 をリリースしました | RARLAB
https://www.winrarjapan.com/support/note-vulnerability-201902

vi　Patch now! Why the BlueKeep vulnerability is a big deal | WeLiveSecurity
https://www.welivesecurity.com/2019/05/22/patch-now-bluekeep-vulnerability/

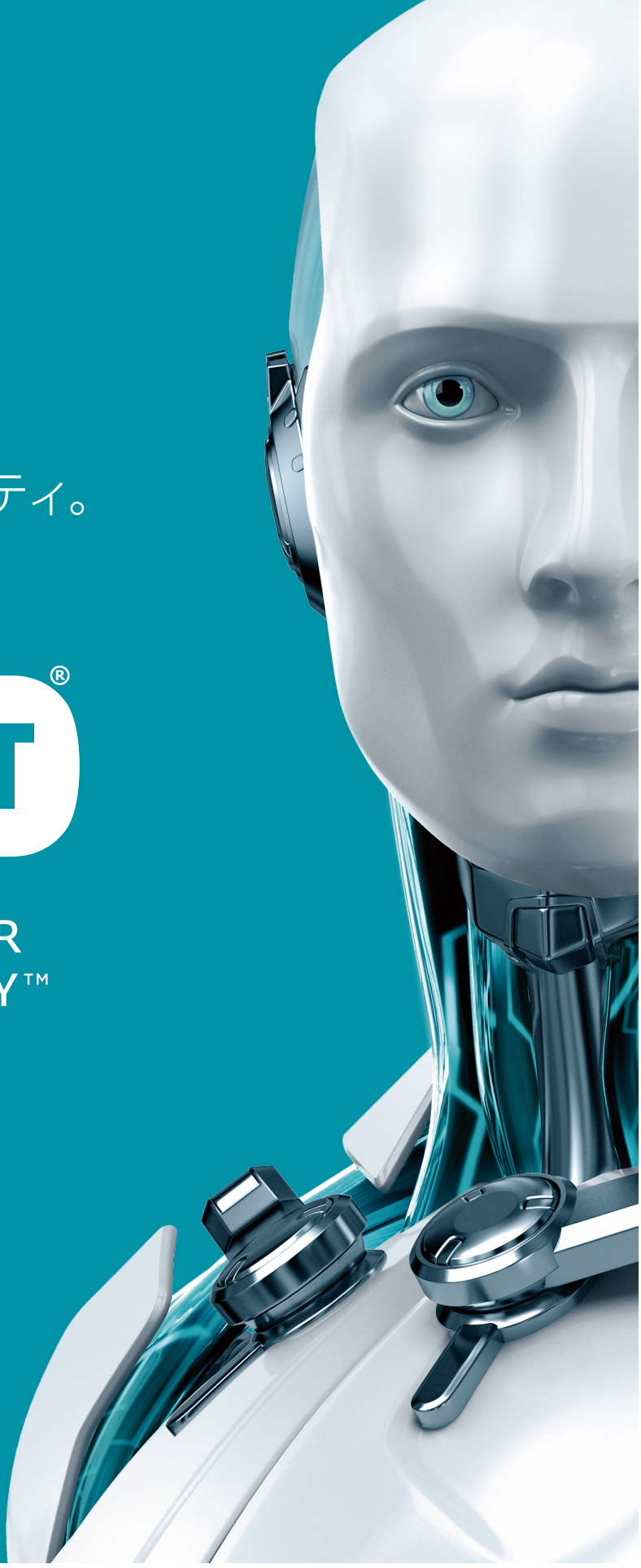
vii　脆弱性対策情報データベース JVN iPedia の登録状況 [2019 年第 2 四半期（4 月～ 6 月）] | IPA 独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/vuln/report/JVNiPedia2019q2.html

viii　EternalBlue reaching new heights since WannaCryptor outbreak | WeLiveSecurity
https://www.welivesecurity.com/2019/05/17/eternalblue-new-heights-wannacryptor/

ix　IPA テクニカルウォッチ「脆弱性対策の効果的な進め方（実践編）」| IPA 独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/technicalwatch/20150331.html

x　IPA テクニカルウォッチ「脆弱性対策の効果的な進め方（ツール活用編）」| IPA 独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/technicalwatch/20190221.html

xi　パッチがあてられない状況をなるべく早く解消する方法 | マルウェア情報局
https://eset-info.canon-its.jp/malware_info/special/detail/181009.html



Canon キヤノンマーケティングジャパン株式会社

〒108-8011 東京都港区港南2-16-6 CANON S TOWER TEL. 03-6701-3475

MWJY1909CMJ-PDF