MALWARE REPORT

マルウェアレポート

2020

年間

安全なネット活用のための

セキュリティ情報

はじめに

2020年は新型コロナウイルスの影響でリモートワークが増加し、それに伴いRDP（リモートデスクトッププロトコル）を狙った脅威が多く観測されました。

また、新型コロナウイルスに対する人々の不安に付け込んだばらまき型メールなども確認されました。

本レポートでは、2020年1月から12月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解説し、これらの脅威に対する対策を紹介します。

「第1章　2020年年間マルウェア検出統計」では、2020年に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の検出を比較して傾向を分析します。また、検出数が多かった3つのマルウェアについて詳しく分析します。「 第2章　特定の組織を標的にする暴露型ランサムウェアの攻撃事例」では、2020年に猛威を振るった 暴露型（二重の脅迫を行う）ランサムウェアについて解説します。Avaddon、Ragnar Locker、SunCrypt による実際の被害事例を紹介します。「 第3章　Emotetの継続的な活動とさらなる攻撃手法の巧妙化」では、2020年に再流行したボットネットマルウェアEmotetの観測状況を紹介します。さまざまな新しいメールテンプレートが確認されています。「第4章　継続的に検出されるVBAで作成されたダウンローダーの主流テクニック」では、VBA（Visual Basic for Applications）で作成されたダウンローダーの VBA/TrojanDownloader.Agent を紹介します。本ダウンローダーは近年継続的に検出され続けており、2020年も国内で多数確認されました。ダウンロードサーバーと通信するまでの挙動と、アンチウイルスソフトによる検出回避や解析妨害の主流の機能をまとめています。

contents

1

2020年年間
マルウェア検出統計

第1章　　2020年年間マルウェア検出統計

本章では、2020年に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紹介します。

1.1　検出数の比較

2020年に国内と全世界で検出されたマルウェアの検出数の推移は、図1.1.1と図1.1.2の通りです。国内で最も多くのマルウェアが検出された月は、12月でした。全世界では、3月が最も多くのマルウェアが検出された月となりました。国内と全世界のそれぞれの2020年1月からの増加・減少傾向を比べてみると図1.1.3のようになっています。1～7月においては増加・減少傾向が概ね一致しています。一方で、8月以降には差異が生じています。全世界では減少傾向が見られますが、国内では増加傾向が見られます。国内でのマルウェアの検出数増加は、VBA/TrojanDownloader.AgentやJS/Agent.OAYなどのマルウェアが増加したことが影響していると考えられます。中でもVBA/TrojanDownloader.Agentの検出数増加は、7月中旬頃から活動を再開したEmotetへの感染を狙ったばらまきメールの増加によるものだと考えられます。

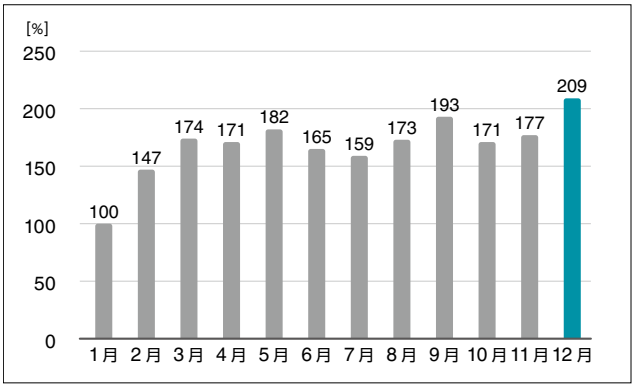


図1.1.1　マルウェア検出数の月別推移（2020年国内）
※2020年1月の検出数を100%としています

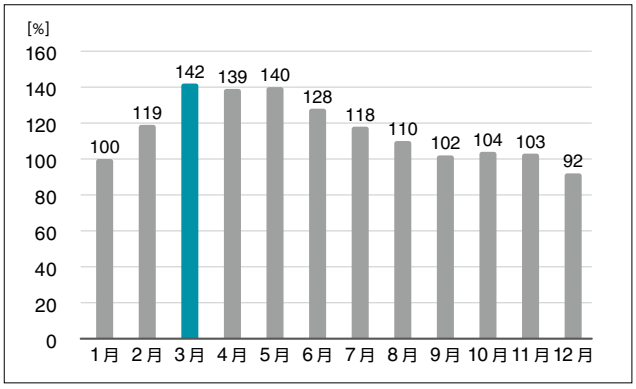


図1.1.2　マルウェア検出数の月別推移（2020年全世界）
※2020年1月の検出数を100%としています

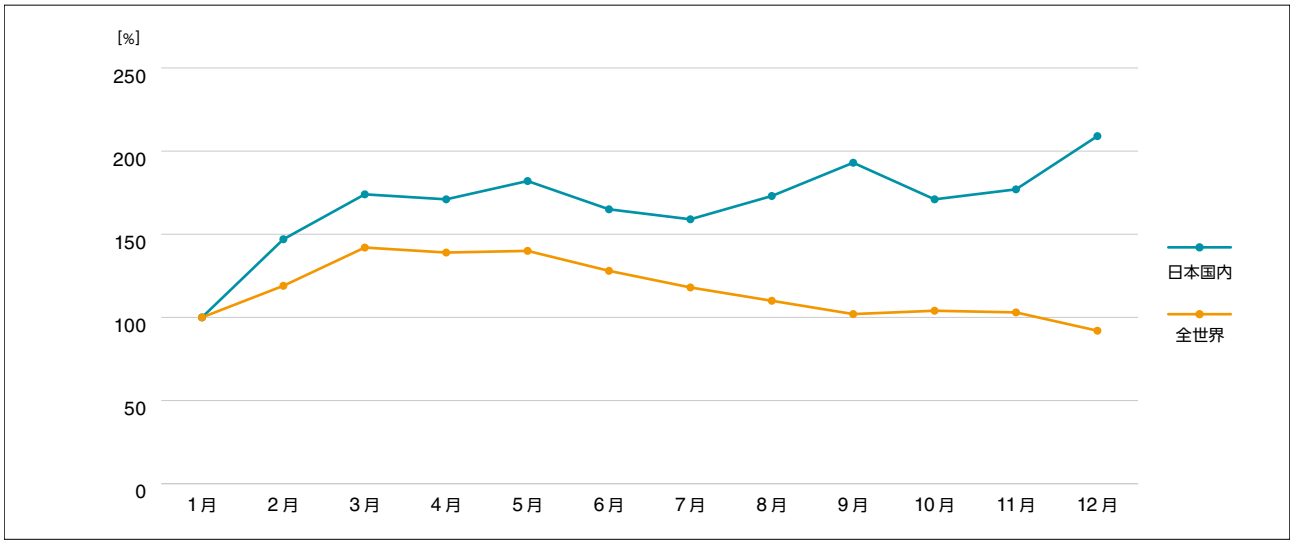


図1.1.3　国内と全世界でのマルウェア検出数の月別比較（2020年）
※2020年1月の検出数を100%としています

国内における2018年～2020年の半期ごとの検出数推移は図1.1.4の通りです。
半期に検出されたマルウェアの検出数が、2018年と比較して約2倍に増えていることがわかります。2020年の検出数増加の要因の1つとして、Webバナーやネット広告を悪用するアドウェアが挙げられます。攻撃者はアドウェアの設置場所の変更やアドウェアの更新を行っており、依然多く検出されています。そのため、検出数の増加は今後も続くと考えられます。

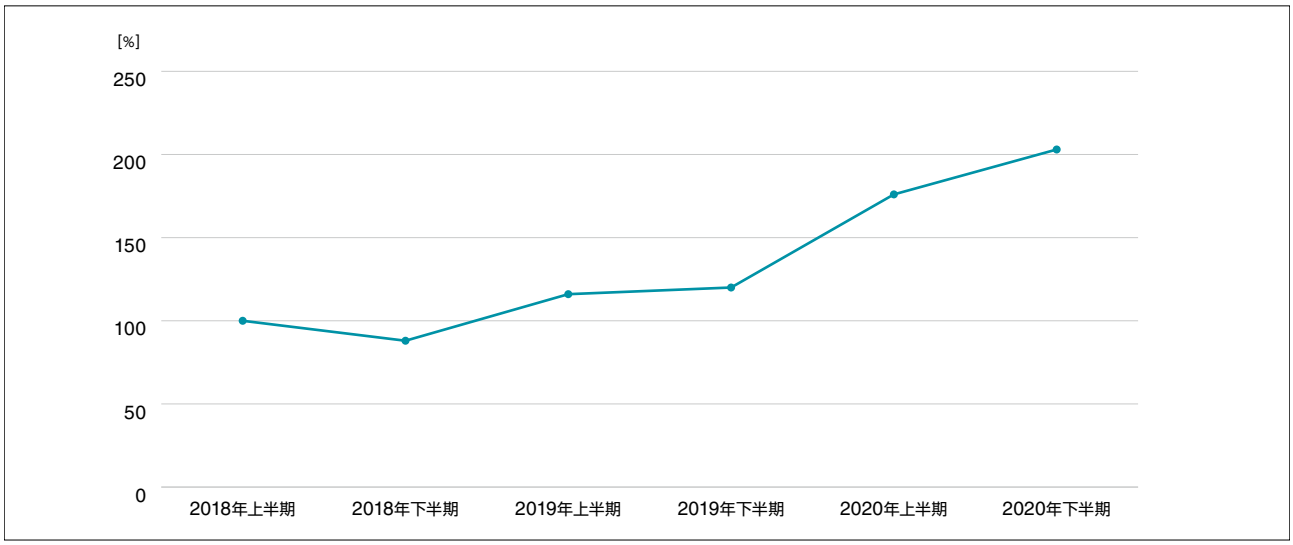


図1.1.4　半期ごとの検出数推移（2018年～2020年・国内）
※2018年上半期の検出数を100%としています

1.2 2020年に多く検出された脅威

1.2.1　2020年におけるマルウェアの検出状況

2020年に国内で検出されたマルウェアの上位10種が図1.2.1.1です。2020年に国内で最も多く検出されたマルウェアは、JS/Adware.Subpropです。JS/Adware.Agent、HTML/ScrInjectがそれに続きます。各マルウェアの詳細については、「1.4 国内検出数TOP3」で紹介します。検出数上位10種を見ると、8種がWebブラウザー上で実行される脅威だとわかります。Webサイト閲覧時にスクリプトや悪意のあるプログラムが実行されるため、攻撃者が多くのユーザーを対象にすることができます。それによって、検出数が増加していることが考えられます。不正な広告を表示させるものから詐欺サイトへ誘導するものなどさまざまな被害が想定されます。他にもメールに添付されたファイルによる脅威であるVBA/TrojanDownloader.Agentが多く検出されています。VBA/TrojanDownloader.Agentは、実行されると他のマルウェアをダウンロードします。ダウンロードするマルウェアとして、EmotetやDridex、Ursnifなどが確認されています。被害はダウンロードされるマルウェアによって異なりますが、重大な被害を生じさせる可能性が高いです。

図1.2.1.1　日本におけるマルウェア検出数の上位10種（2020年）

2020年に全世界で検出されたマルウェアの上位10種が図1.2.1.2です。全世界で最も多く検出されたマルウェアは、JS/Adware.Subpropです。JS/Adware.AgentやHTML/ScrInjectが、それに続いて検出されています。国内と同様にWebブラウザー上で実行される脅威が多数検出されています。他にもMicrosoft Office数式エディターに存在する脆弱性（CVE-2017-11882）を悪用するマルウェアであるWin32/Exploit-CVE-2017-11882が検出されています。新しく発見される脆弱性も危険ですが、発見されてから時間が経過している脆弱性はエクスプロイトキットが作成されている可能性が高いです。エクスプロイトキットはプログラムや脆弱性に関する専門的な知識がなくてもサイバー攻撃を可能にするため危険です。攻撃に遭わないためにも、セキュリティパッチの適用などの対策が重要です。

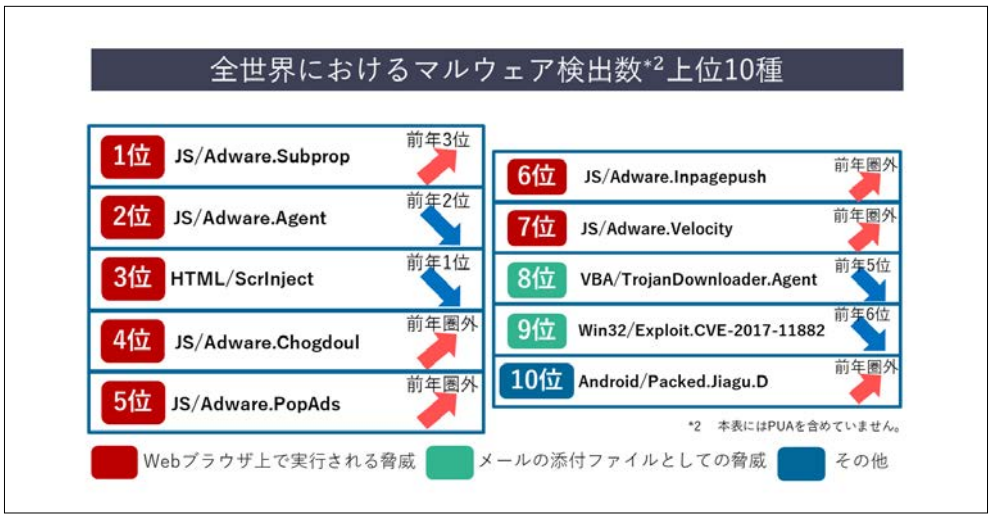


図1.2.1.2　全世界におけるマルウェア検出数のTOP10（2020年）

1.2.2　2020年におけるネットワーク攻撃保護による検出状況

ESET製品では、マルウェア以外にも通信プロトコルであるRDPやSMB（Server Message Block）経由のネットワーク攻撃を検出することができます。2020年に国内で検出された上位10種をまとめました。

最も検出数が多かったのは、Incoming.Attack.Genericでした。Incoming.Attack.Genericは、RDPのデフォルトのポート番号である「3389」以外のポートを狙ったブルートフォース攻撃の検出数を示しています。同様にそれぞれのポートを狙ったブルートフォース攻撃を検出するSMB.Attack.GenericやRDP.Attack.Genericが、これに続きます。RDPやSMBといった通信プロトコルに対するブルートフォース攻撃などの検出以外にも、通信プロトコルの脆弱性を悪用した攻撃も検出しています。例えば、検出数第6位のSMB/Exploit.EternalBlueは、SMB1.0の脆弱性であるEternalBlueを悪用したツールを検出したものです。
2020年は、RDP経由で侵入したPCに対してランサムウェアを感染させる事例も確認されています。メールの添付ファイルによる感染と異なり、感染するまで気づきにくいと考えられます。設定の見直しやパッチの適用を行ってください。

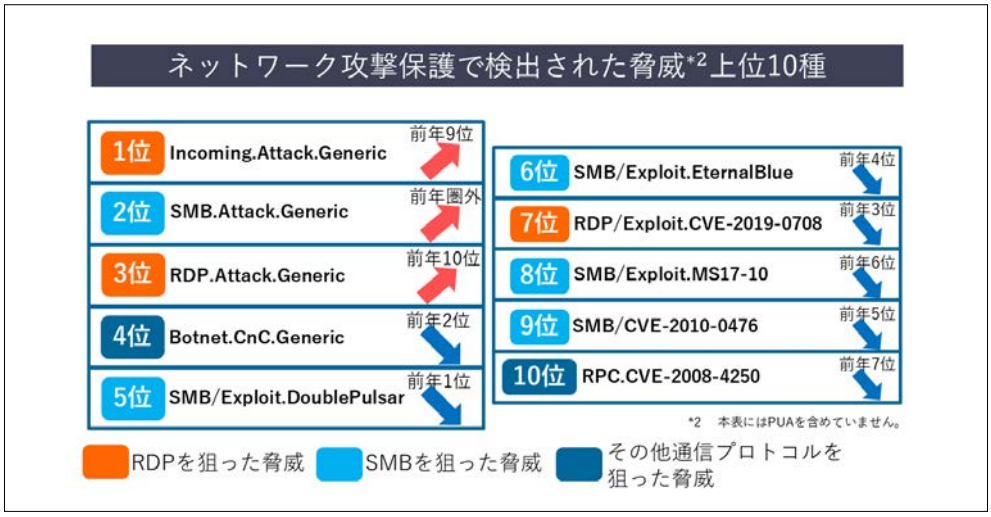


図1.2.2.1　ネットワーク攻撃保護で検出された脅威検出数上位10種（2020年・国内）

1.3　マルウェア検出数のファイル形式別割合

ESET製品で検出されるマルウェアはファイル形式（プラットフォーム）で大別することができます。国内と全世界におけるファイル形式別検出数の割合を図1.3.1と図1.3.2に示します。
国内ではJS（JavaScript）形式のマルウェアが最も多く検出されています。Win32形式やHTML形式のマルウェアが次いで検出されています。他にも、VBA形式のマルウェアが多く検出されています。年間検出数第5位のVBA/TrojanDownloader.Agentの影響が大きいと考えられます。

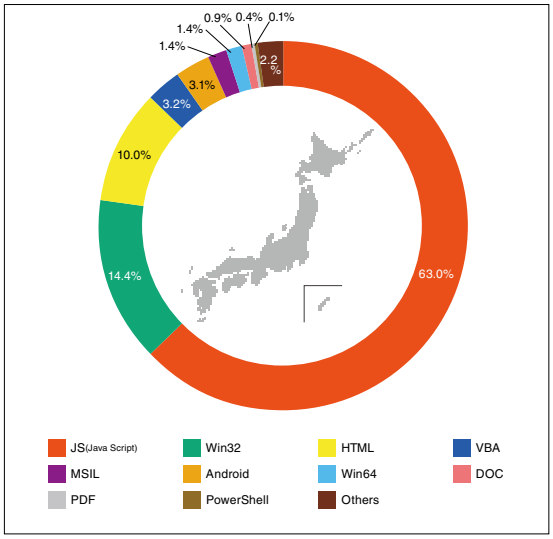


図1.3.1　形式別マルウェア検出数の割合（2020年国内）

全世界も同様に、JS形式のマルウェアが最多となっています。上位3位の形式は、国内と同様です。
全世界ではAndroid形式のマルウェアが多く検出されています。これは、国内ではあまり検出されていなかったAndroid/Packed.Jiagu.Dの検出に影響を受けています。Android/Packed.Jiagu.Dは、Android上で動作しJiaguというパッカーによってパックされたマルウェアの汎用検出名です。
国内と全世界の共通の特徴として、JS形式のアドウェアの検出数が増加し、大きな割合を占めています。また差異が出ている特徴として、VBA形式とAndroid形式の検出割合において両者の間に差が生じています。

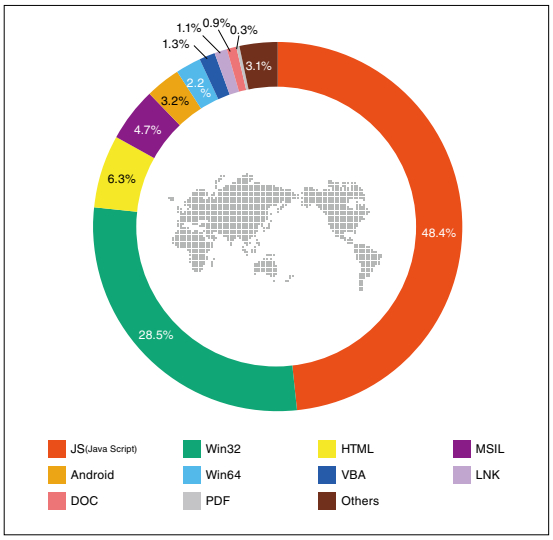


図1.3.2　形式別マルウェア検出数の割合（2020年全世界）

1.4 国内検出数TOP3

国内検出数TOP3は、すべてWebブラウザー上で実行されるマルウェアです。国別の検出数を見たとき、さまざまな言語圏の国で検出されていることがわかります。Webブラウザー上で実行されるため、多くのユーザーが被害の対象となっていると考えられます。上半期統計でも見られたペルーにおける多数の検出数は、年間統計においても確認されています。スペイン語圏のユーザーの情報を収集するために多くのアドウェアを設置していたことやペルーのユーザーが設置されたWebサイトによく訪れていたことが考えられます。

① JS/Adware.Subprop

JS/Adware.Subpropは、偽のAdobe Flash Playerのアップデートや有名ベンダーのWebバナーを悪用して、悪意のあるコンテンツや不要なソフトウェアを配布するスクリプトの検出名です。2020年6月マルウェアレポートで感染までの流れを紹介しています。

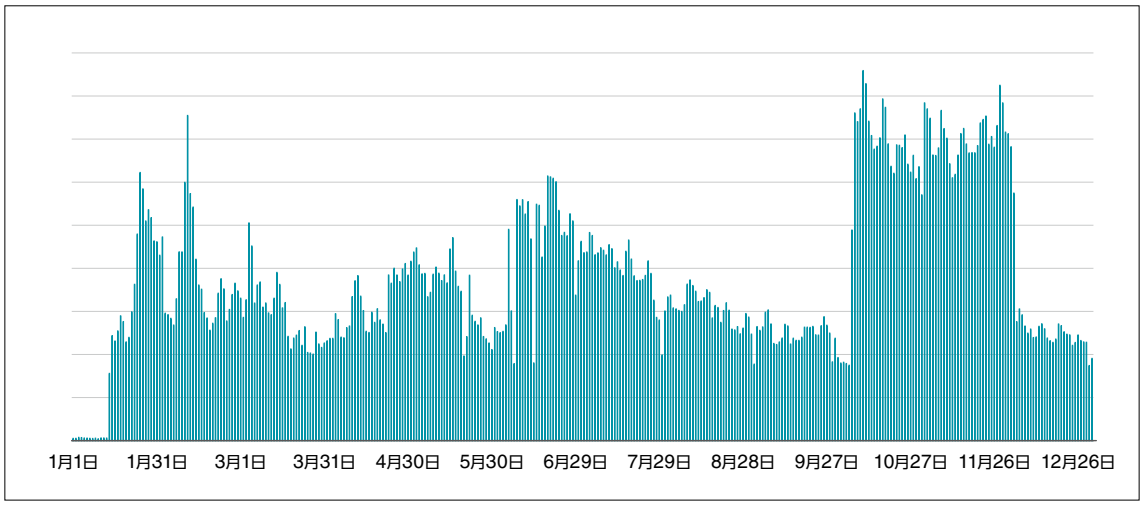


図1.4.1　JS/Adware.Subpropの国内検出数推移（2020年）

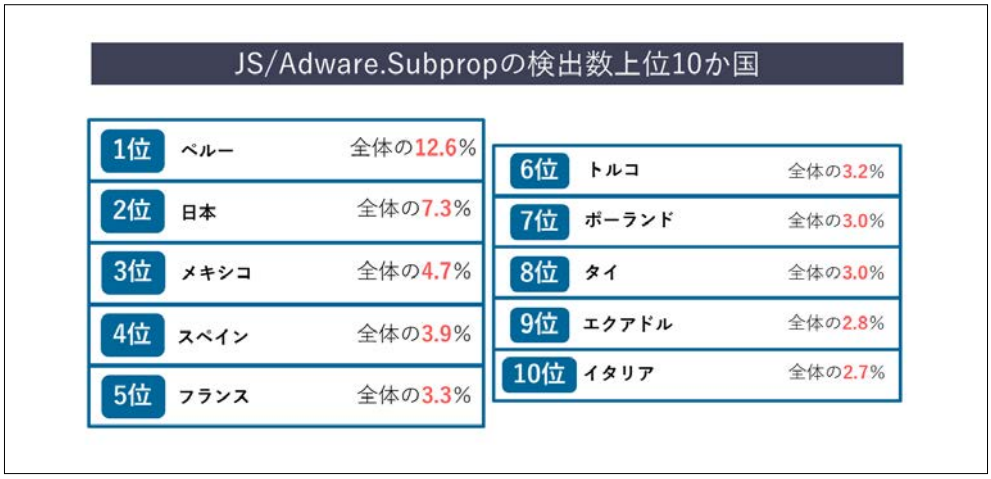


図1.4.2　JS/Adware.Subpropの検出数TOP10の国と地域（2020年）

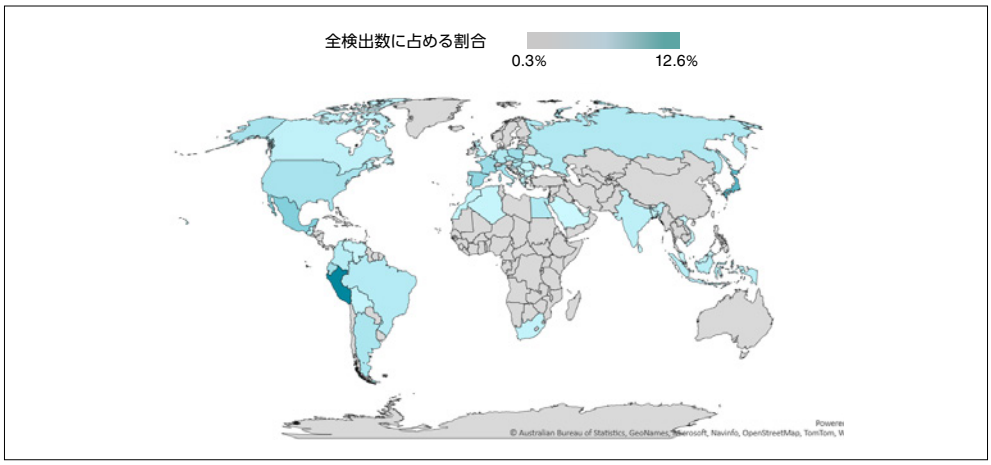


図1.4.3　JS/Adware.Subpropの検出数TOP50の国と地域のヒートマップ（2020年）

② JS/Adware.Agent

JS/Adware.Agentは、不正な広告を表示させるアドウェアの汎用検出名です。汎用検出名ということもあり、ロシア、アメリカやフランスといったさまざまな国で検出されています。

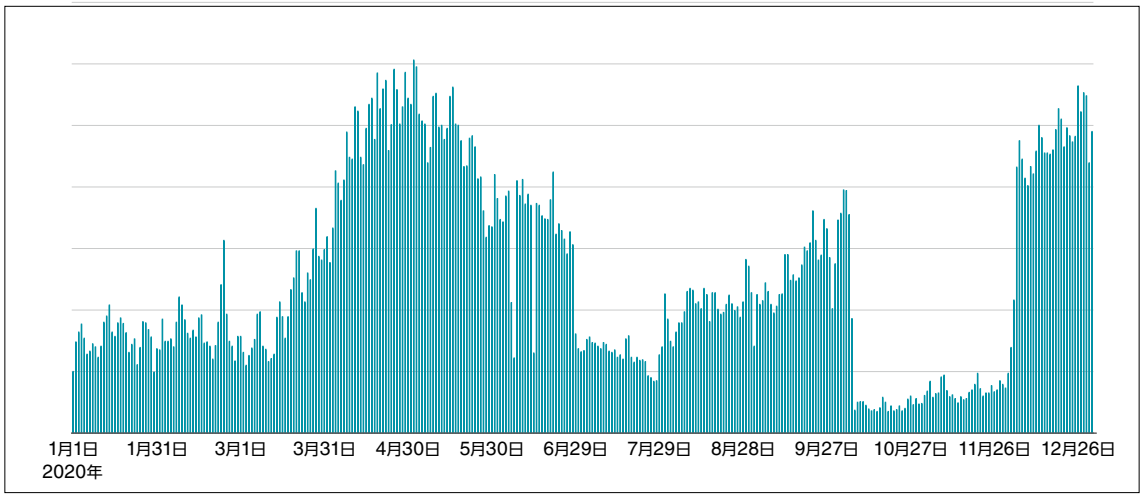


図1.4.4　JS/Adware.Agentの国内検出数推移（2020年）

図1.4.5　JS/Adware.Agentの検出数TOP10の国と地域（2020年）

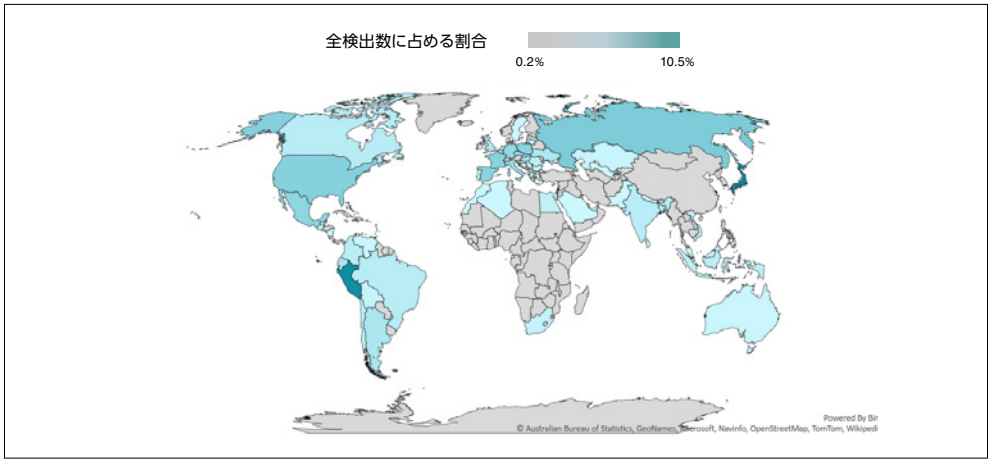


図1.4.6　JS/Adware.Agentの検出数TOP50の国と地域のヒートマップ（2020年）

③ HTML/ScrInject

HTML/ScrInjectは、HTML形式の悪意のあるスクリプトの汎用検出名です。2020年に確認されたサンプルの中には、Guloaderをダウンロードさせるurlへのリンクが埋め込まれたものがありました。Guloaderはダウンローダーで、感染するとさまざまなマルウェアをダウンロードします。

図1.4.7　HTML/ScrInjectサンプルのコードの一部

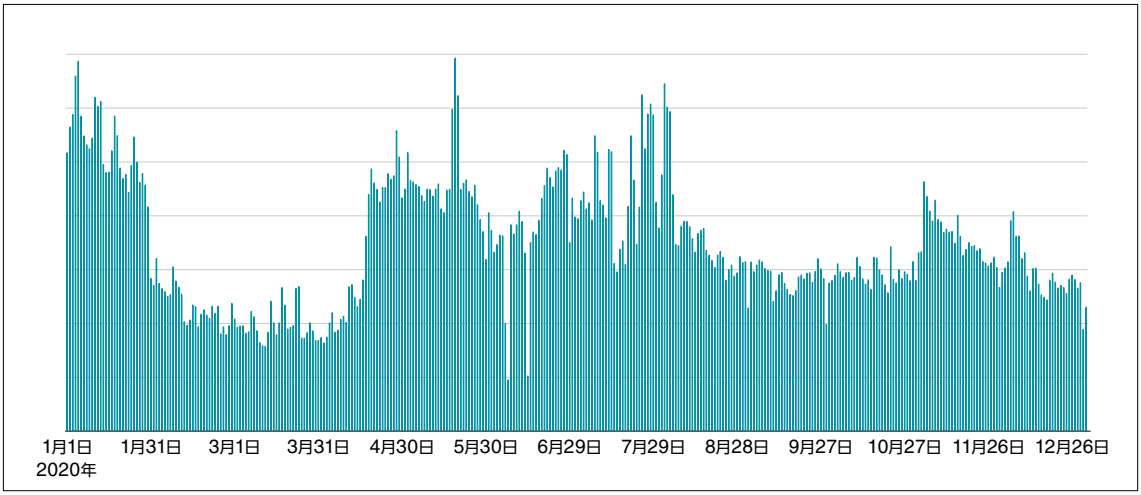


図1.4.8　HTML/ScrInjectの国内検出数推移（2020年）

図1.4.9　HTML/ScrInjectの検出数TOP10の国と地域（2020年）

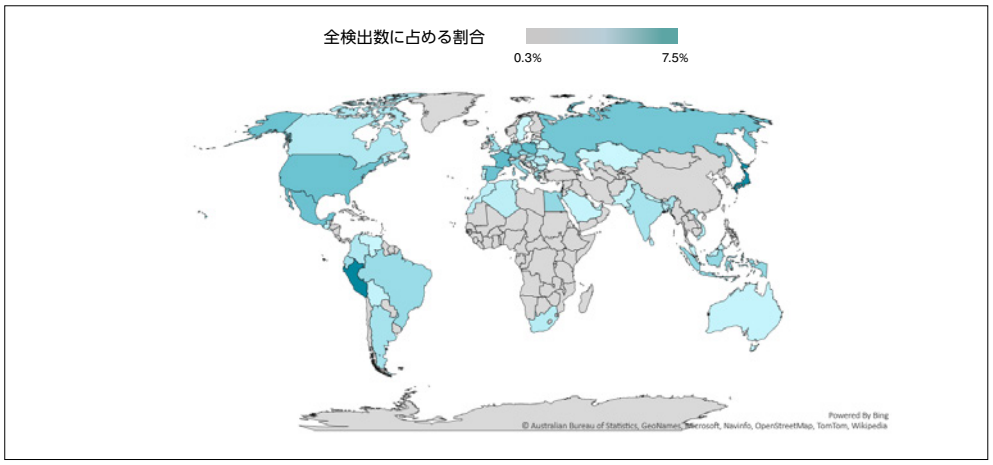
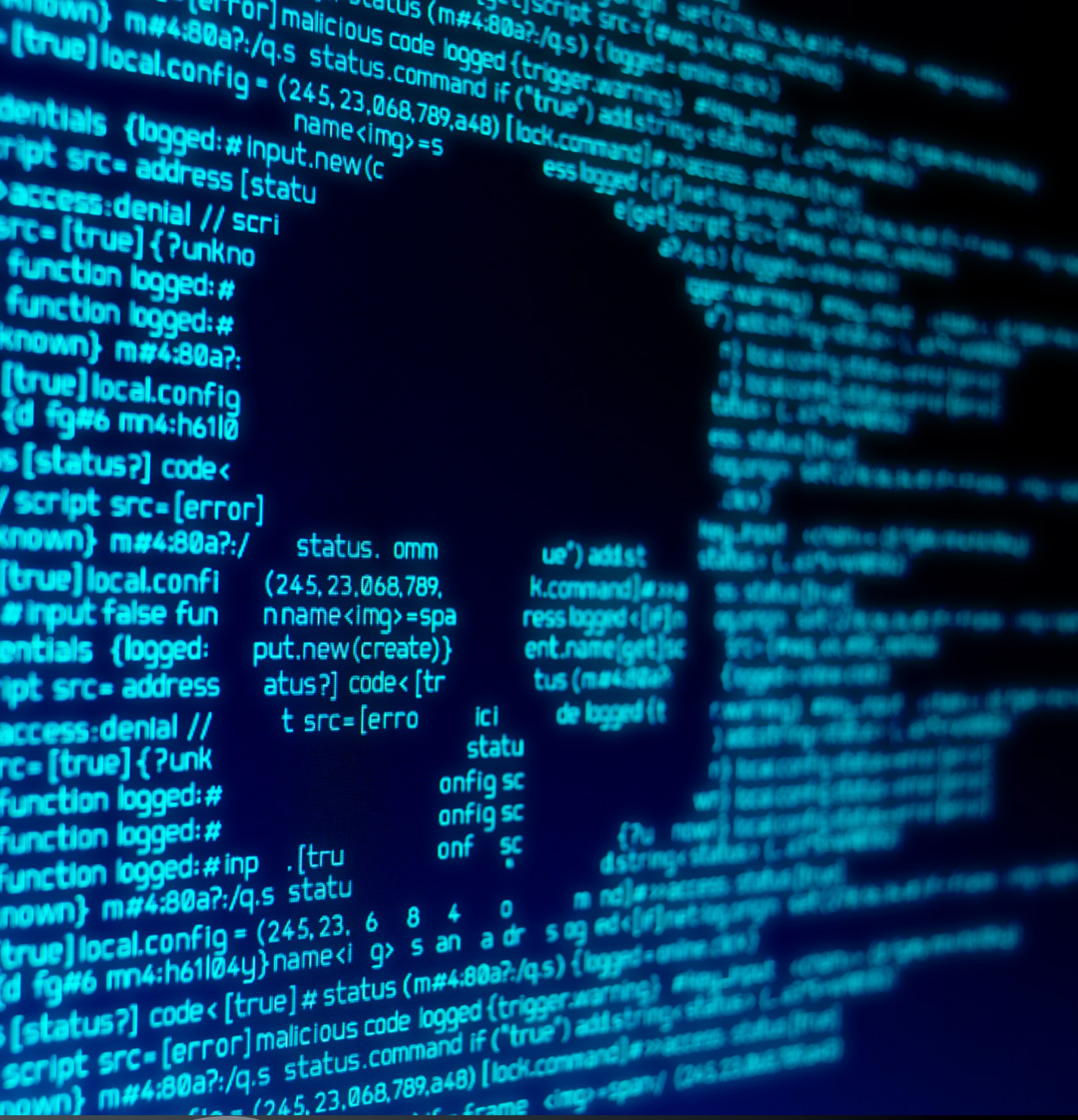


図1.4.10　HTML/ScrInjectの検出数TOP50の国と地域のヒートマップ（2020年）

以上が2020年年間マルウェア検出統計です。



2 特定の組織を標的にする暴露型ランサムウェアの攻撃事例

第2章　　特定の組織を標的にする暴露型ランサムウェアの攻撃事例

本章では、2020年に猛威を振るった暴露型ランサムウェアによる攻撃事例について解説します。

1.　2020年のランサムウェア攻撃の概要

2019年に引き続き[i]、2020年もランサムウェアによる攻撃が多く確認されました。従来の不特定多数に対する攻撃ではなく、特定の（規模の大きい）組織に標的を絞って攻撃を行う傾向が年々高まっています。それに伴って身代金の要求額も増加の一途を辿っており、2020年に実施された調査によると日本企業の身代金支払い額は平均で1.2億円に上ることが明らかになっています。[ii]
IPA（情報処理推進機構）は新たなランサムウェアの手口を人手によるランサムウェア攻撃（human-operated ransomware attacks）と二重の脅迫（double extortion）の2つに分類して注意喚起を行っています。[iii]

■「人手によるランサムウェア攻撃」とは
攻撃者が標的のネットワークに秘密裏に侵入し、管理サーバーを乗っ取った上でネットワーク上の端末をランサムウェアに感染させる手法。攻撃の隠密性が高く比較的規模の大きい企業が標的になることが多い。

■「二重の脅迫」とは
ファイルを暗号化する前に機密情報等を窃取し、それらを公開するとして脅迫する手法。この手法を用いるランサムウェアは暴露型ランサムウェアと呼ばれる。

表2.1　従来のランサムウェア攻撃と新しいランサムウェア攻撃との違い

	従来のランサムウェア攻撃	新しいランサムウェア攻撃
ターゲット	不特定多数（個人および組織）	（高収益を見込める）特定の組織
侵入経路	ばらまきメール（添付ファイル、URL）	スピアフィッシングメール サーバーへの不正アクセス （窃取した認証情報、脆弱性等の悪用）
脅迫方法	ファイルの暗号化	● ファイルの暗号化 ● 情報の公開 ● DDoS攻撃
身代金要求額	数万円	数百万円～数億円

2.　暴露型ランサムウェアの攻撃事例

2020年にはさまざまな暴露型ランサムウェアが登場しました。中でも特に猛威を奮った3つの暴露型ランサムウェアおよび攻撃者グループによる攻撃事例を紹介します。

■Avaddon

Avaddonは2020年6月上旬に確認されたランサムウェアです。AvaddonはRaaS（Ransomware as a Service）型のランサムウェアで、複数の攻撃者が使用していると推測されています。

Avaddonはばらまき型の攻撃と標的型攻撃との両方で使用されていたことを確認しています。ばらまき型の攻撃では、Phorpiexボットネットを介して拡散が行われました。2020年6月9日前後には、国内のメールアドレス宛にも多数配信されていたことを確認しています。

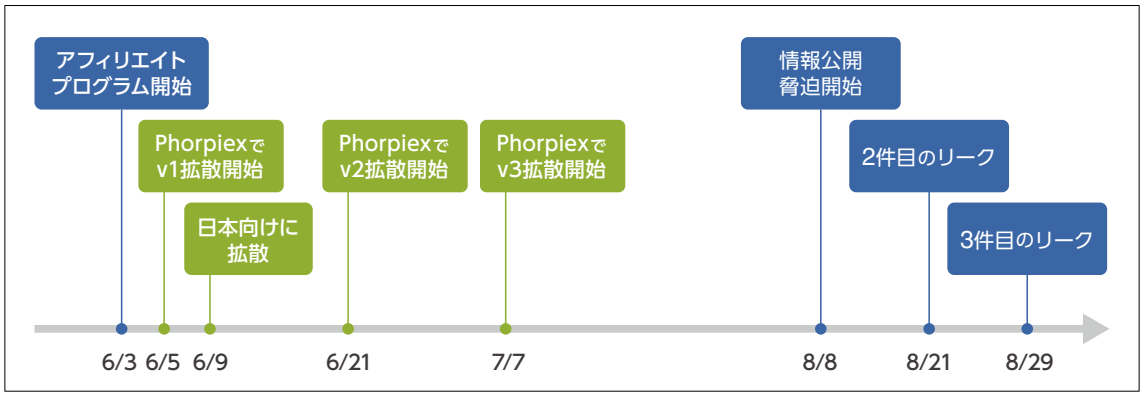


図2.1　Avaddonに関連するイベントのタイムライン（2020年）

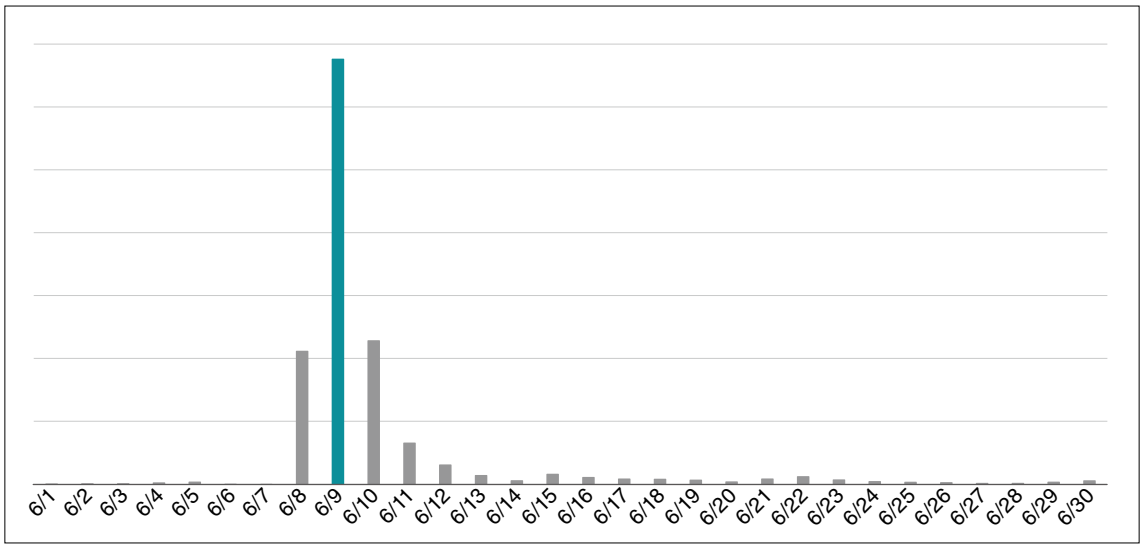


図2.2　Avaddonのダウンローダー（JS/Danger.ScriptAttachment[1]）の日別検出数の推移（2020年6月・国内）

2020年8月にはAvaddonの攻撃者グループは窃取した機密情報を公開するためのWebサイト（リークサイト）を立ち上げています。はじめに窃取した情報の一部を公開し、被害に遭った企業が交渉に応じない場合は追加の情報を公開すると脅迫しています。

1　JavaScript形式の汎用検出名のため、その他の悪性スクリプトも含まれます。

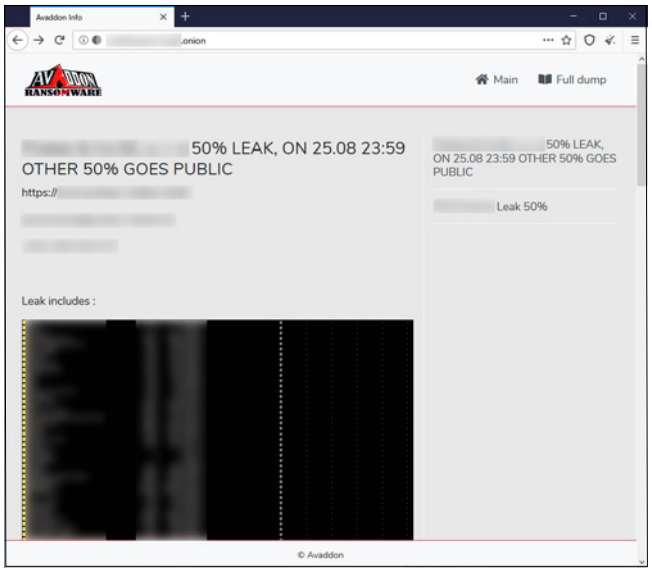


図2.3　Avaddonのリークサイト

Avaddonランサムウェアに関する詳細は、「Avaddonランサムウェアの解析」レポート[iv]で解説しています。

■Ragnar Locker

Ragnar Lockerは2020年4月頃初めて確認されたランサムウェアです。

暴露型ランサムウェアの中でも被害件数が多く、2020年11月19日にはFBIが警戒を呼びかけるアラートを発出しています。[v]

Ragnar Lockerによる攻撃の特徴の一つに、攻撃の隠密性の高さがあります。2020年5月の事例では、攻撃プログラムに埋め込まれた仮想化ソフトウェアVirtualBoxのイメージを展開し、VirtualBox上（ゲストOS）のランサムウェアがホストOS上のファイルを暗号化しています。この手法を用いることで、ホストOS上のセキュリティソフトウェアによる検出を巧みに回避しています。[vi]

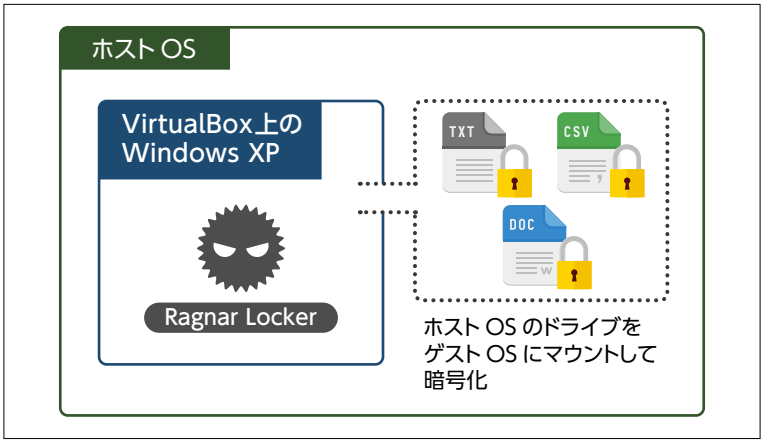


図2.4　VirtualBoxを悪用した暗号化のイメージ

また、Ragnar Lockerのランサムノート（身代金要求文書）には標的となった組織の名前が書かれていることがあり、標的を絞って攻撃を行っていることが伺えます。

図2.5　Ragnar Lockerのランサムノート

Ragnar Lockerの攻撃者グループは2020年6月11日から12月18日の間に少なくとも22組織のデータを取得し、リークしたと主張しています。

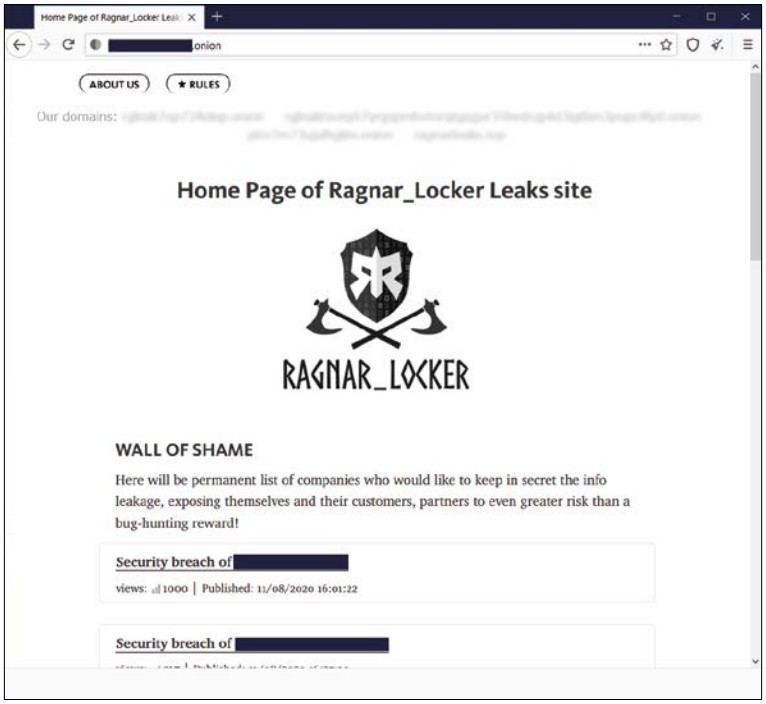


図2.6　Ragnar Lockerのリークサイト

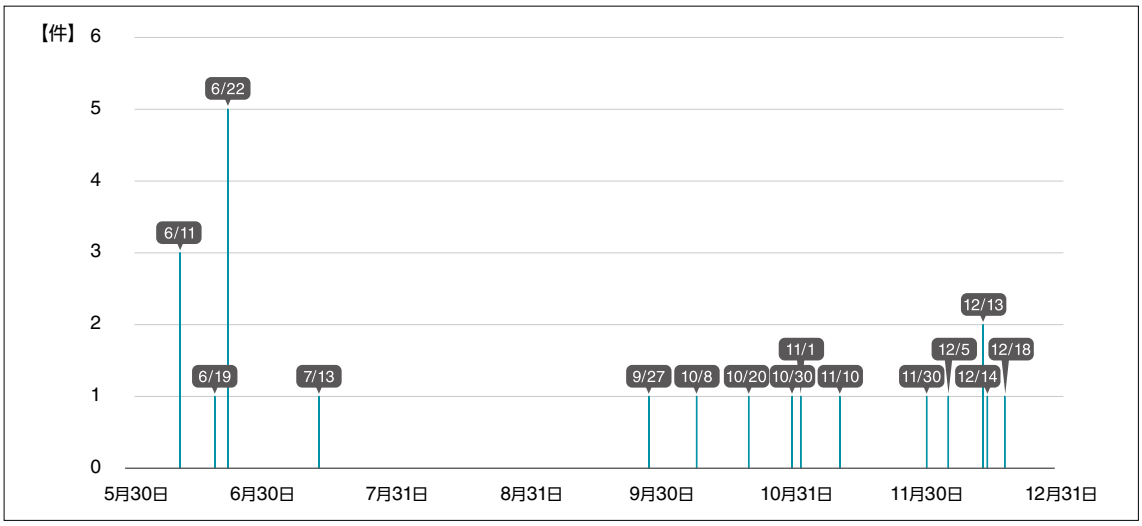


図2.7　Ragnar Locker日別の新規リーク件数（2020年）

Ragnar Lockerが情報をリークしたとされる組織の半数以上はアメリカ合衆国に本社を置く企業です。日本国内の企業も1社含まれています。
業種別では製造業やサービス業が多く、比較的規模の大きい企業が標的となっています。

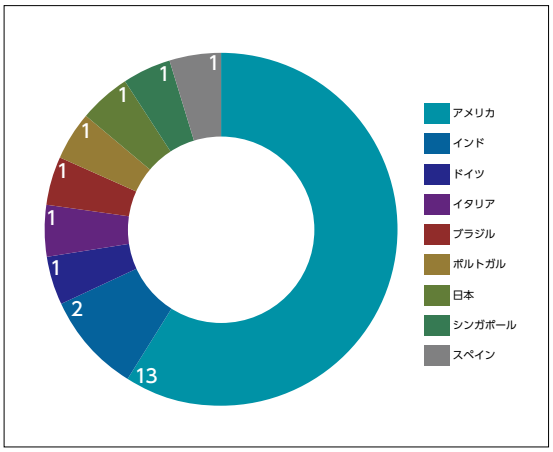


図2.8　Ragnar Lockerが情報をリークしたとされる企業の国籍
（2020年12月31日時点）

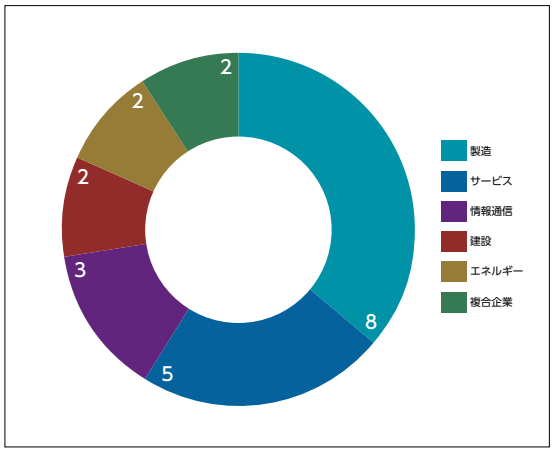


図2.9　Ragnar Lockerが情報をリークしたとされる企業の業種
（2020年12月31日時点）

■SunCrypt
SunCryptは2019年から活動が確認されていたランサムウェアです。2020年8月にリークサイトを開設しました。
ランサムウェアを使用する攻撃者グループの多くが医療機関を標的にしないことを表明している一方で [vii]、SunCryptはアメリカの大学病院を相手に情報公開脅迫を行い61.9ビットコイン（2020年10月当時のレートでおよそ7000万円）を得ています。[viii]

SunCryptは情報公開脅迫（二重の脅迫）に加えて、DDoS攻撃を仕掛けるとして脅迫するいわば、三重の脅迫と言える手法を取っています。DDoS攻撃はWeb サービスの事業継続に多大な影響を及ぼすため、ECサイトを運営する企業が狙われる傾向にあります。
この手法はその後Avaddon等、他のランサムウェアを使う攻撃者も取り入れています。

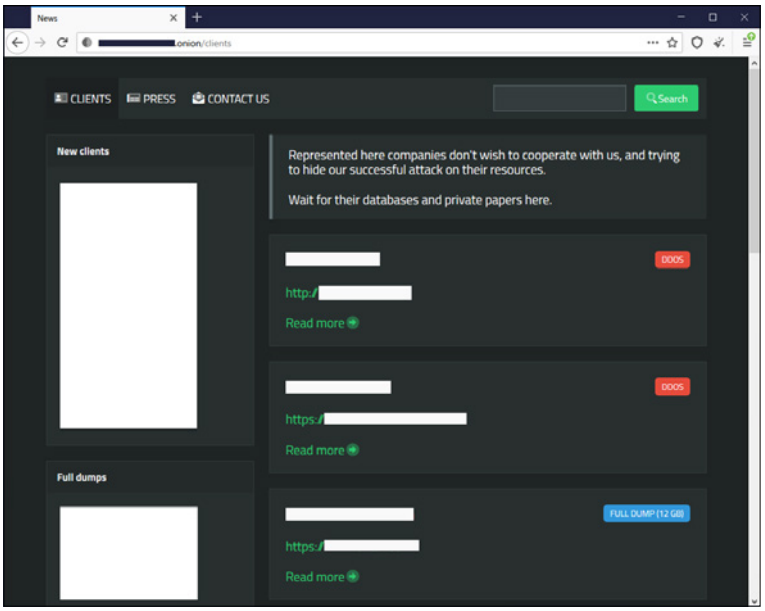


図2.10　SunCryptのリークサイト

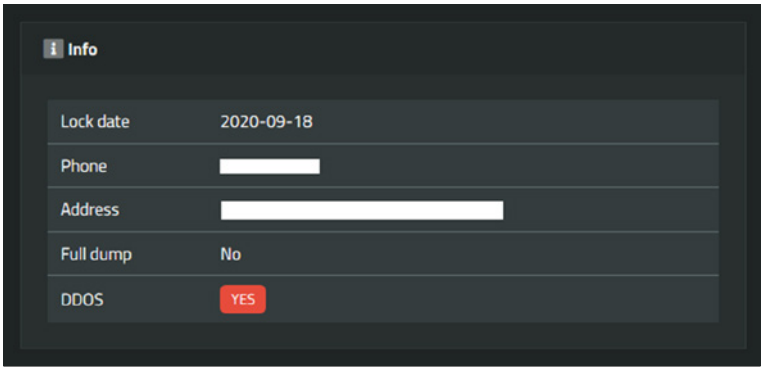


図2.11　標的に対してDDoS攻撃を仕掛けたことを示す記述（SunCryptリークサイト）

SunCryptの攻撃者グループは2020年8月1日から9月29日の間に少なくとも17の組織の情報を取得し、リークしたと主張しています。

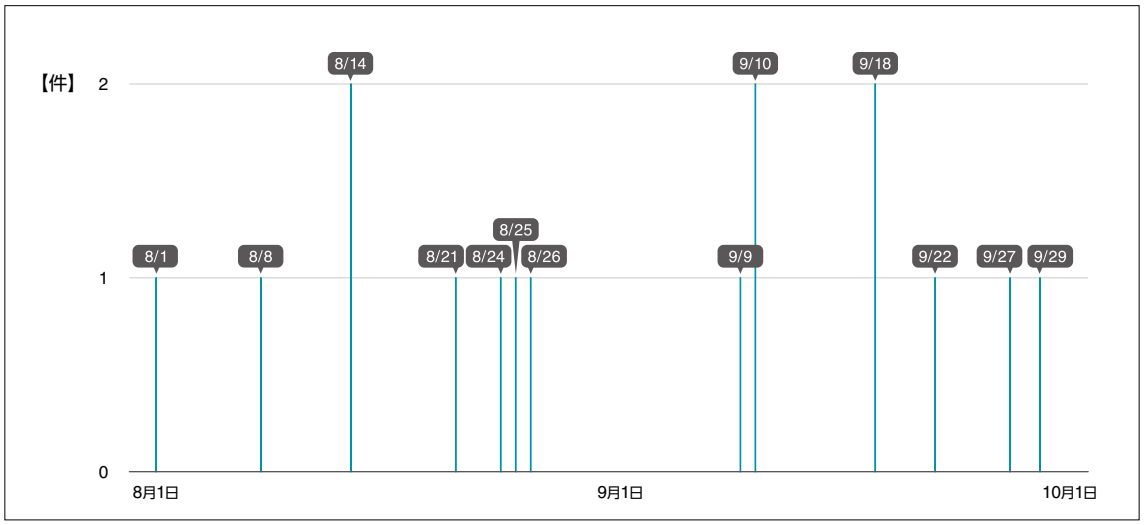


図2.12　SunCrypt日別の新規リーク件数

SunCryptが情報をリークしたとされる組織もアメリカ合衆国の企業に集中しています。製造業から美術館に至るまで、幅広い業種の組織が標的となっています。

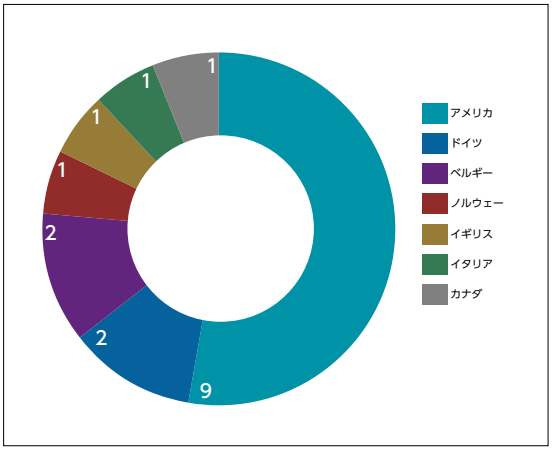


図2.13　SunCryptが情報をリークしたとされる企業の国籍
（2020年12月31日時点）

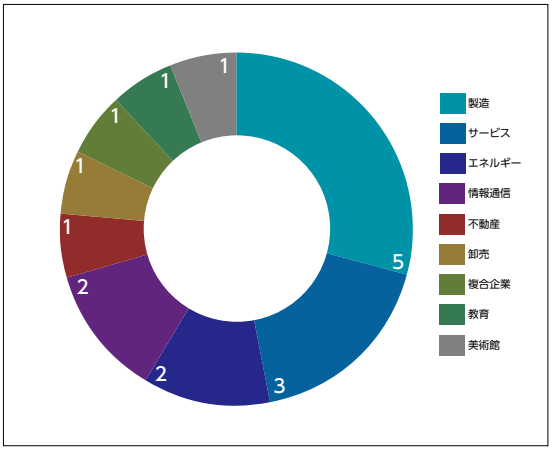


図2.14　SunCryptが情報をリークしたとされる企業の業種
（2020年12月31日時点）

3. まとめと脅威への対策

紹介したように、最近のランサムウェアによる攻撃は従来のファイル暗号化だけではなくデータの公開脅迫等を併用しています。
また、攻撃者が高収益を見込めるような規模の大きい企業が特に狙われる傾向にあります。
リモートワークの増加によって外部から社内ネットワークに接続する機会が増加している今、改めてセキュリティを見直す必要があります。
今回紹介した脅威による被害に遭わないために、以下のセキュリティ対策を推奨します。

■ ランサムウェアやその他のマルウェアへの感染を防ぐための対策
- OSやソフトウェアに更新プログラムを適用し、常に最新の状態に保つ
- アンチウイルス製品を導入し、常に最新の状態に保つ
- Microsoft Officeのマクロ実行設定が無効になっていることを確認する
- スクリプトファイル（JavaScript、VBScript等）を開く既定のアプリケーションをテキストエディターに変更する（スクリプトファイルのローカル実行を防ぐ）
- ファイアウォールを適切に設定する

■ ランサムウェアに感染した場合に被害を最小限に抑えるための対策
- 定期的にバックアップを取得し、取得後はバックアップをネットワークから切断する
- ファイルサーバーのアクセス権やファイル共有を適切に設定する
- 管理共有を無効にする

■ 情報窃取への対策
- 重要な情報は通常利用しているネットワークとは別のセグメントに保管する
- ファイルサーバーのアクセス権設定やファイル共有の設定を見直す
- ファイルに対する操作ログを記録する

3 Emotetの継続的な活動とさらなる攻撃手法の巧妙化

第3章　Emotetの継続的な活動とさらなる攻撃手法の巧妙化

本章では、2020年に再流行したEmotetの観測状況と新たに確認されたメールテンプレートを紹介します。

1.　2020年のEmotet観測状況

マルウェアEmotetの攻撃活動が2020年も多数確認されました。Emotetはモジュールやほかのマルウェアをダウンロードし、情報窃取などを行うマルウェアです。ボットネットを形成し、急速に感染を拡大させています。
Emotetの主要な感染経路は電子メールです。メールに添付されたダウンローダー（大部分がMicrosoft Office形式のファイル）がEmotetをダウンロード・実行することで、Emotetに感染します。

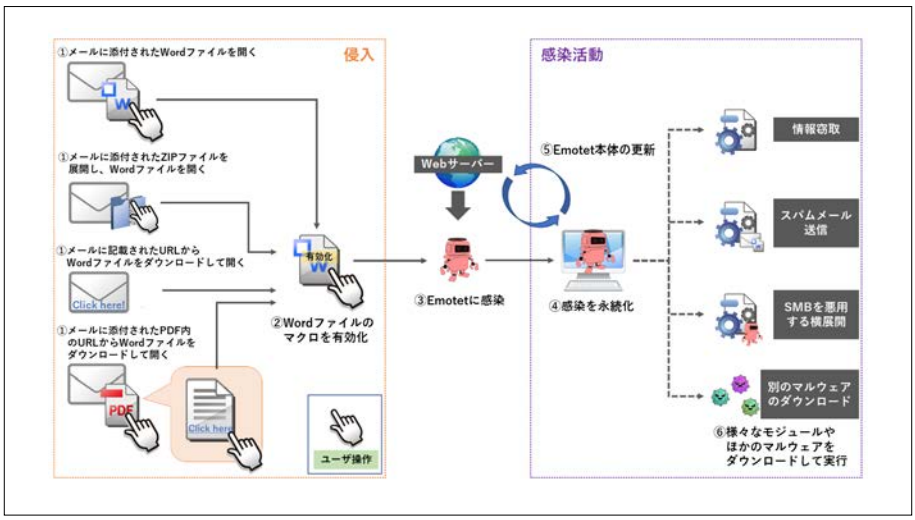


図3.1　Emotet感染の流れ

2020年8月以降、Emotetの感染を狙ったメールが国内外で特に多く観測されました。
8月から12月におけるEmotet（Win32/Emotet）およびEmotetのダウンローダー（VBA/TrojanDownloader.Agent）[2]の検出統計は図3.2、図3.3の通りです。国内では9月に検出数のピークを迎えており、世界全体では下半期の間継続的に検出されています。

2　Emotetダウンローダーの大部分を占めるマルウェアの名称です。Emotet以外のマルウェアをダウンロードする場合もあります。

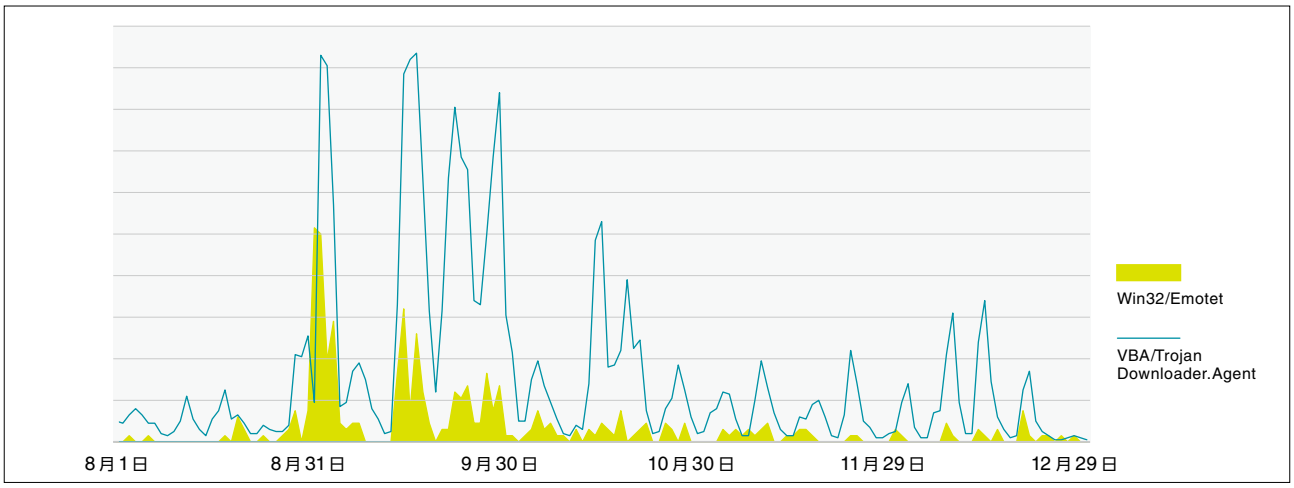


図3.2　Win32/EmotetとVBA/TrojanDownloader.AgentのESET検出数（2020年・国内）

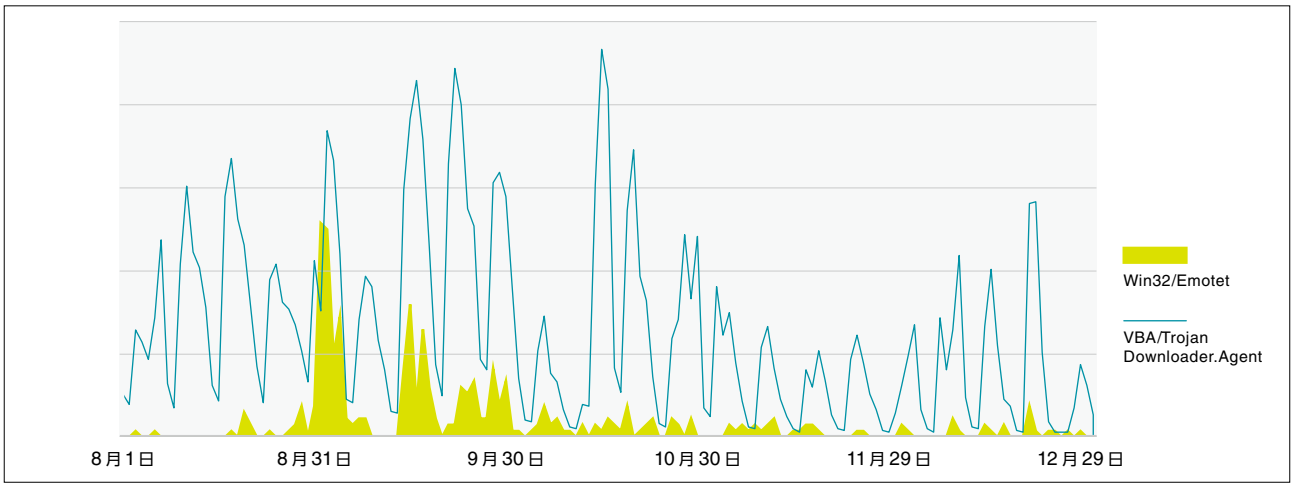


図3.3　Win32/EmotetとVBA/TrojanDownloader.AgentのESET検出数（2020年・世界全体）

検出数が増加した下半期には実際の感染被害も多く発生しており、IPA（情報処理推進機構）の情報セキュリティ安心相談窓口には2020年7～9月において過去最多の308件の相談が寄せられています。

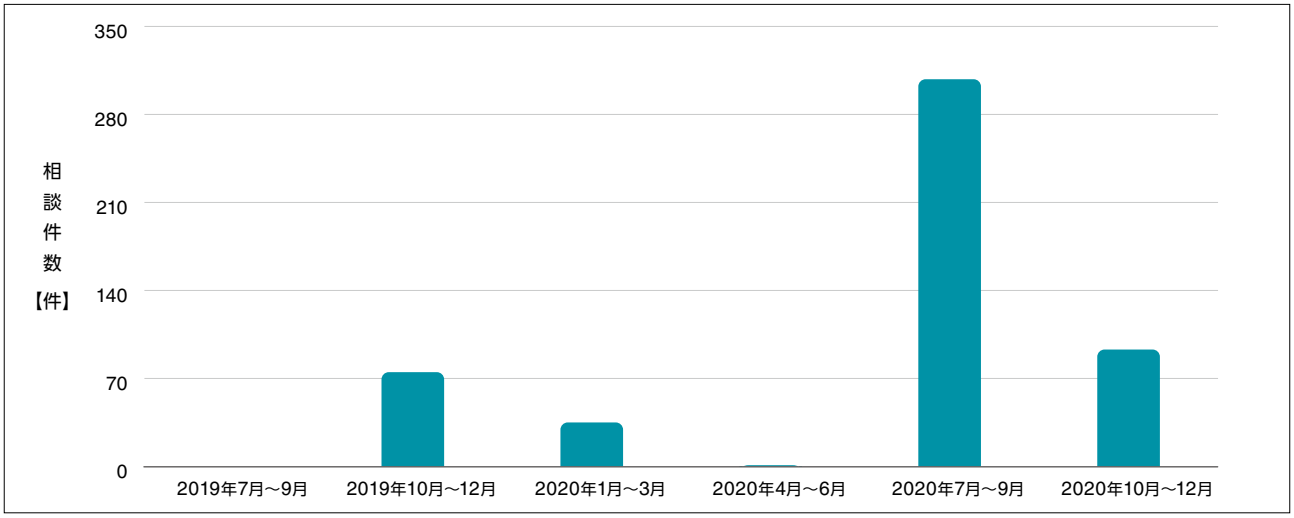


図3.4　Emotet関連の相談件数の推移（出典：IPA[ixx]）

2.　Emotetへの感染を狙ったばらまきメールの新しいテンプレート

2020年の9月以降、Emotetへの感染を狙ったばらまき型メールにいくつか新しいテンプレートが確認されました。

■アンチウイルスベンダーを装う事例（2020年9月上旬に確認）
2020年9月上旬にはアンチウイルスベンダーのサポートセンターを装ったメールが観測されました。実在するアンチウイルスベンダーの名前を使用することで、ユーザーの警戒心を解く狙いがあると考えられます。

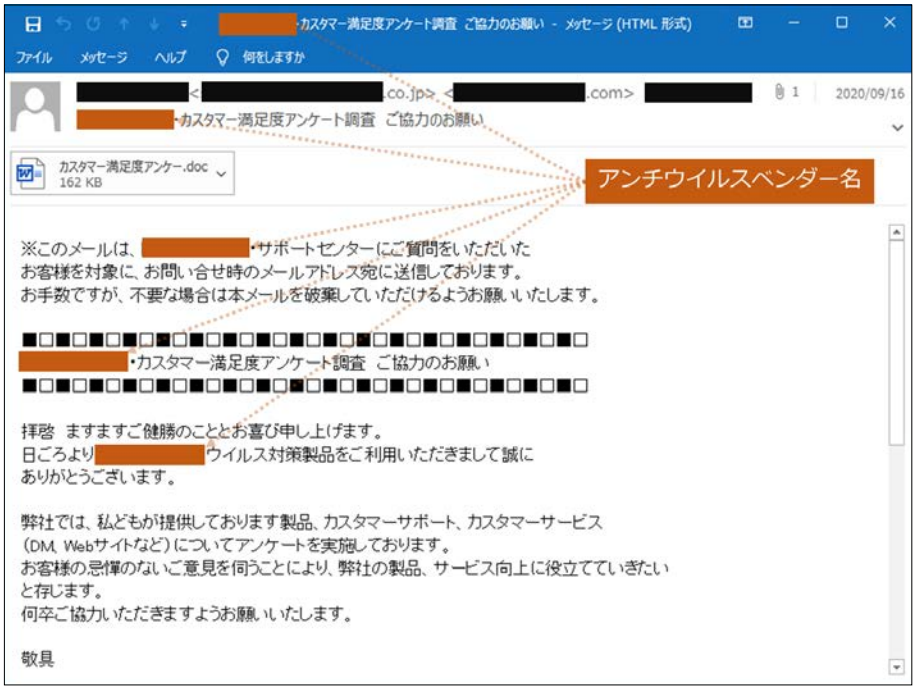


図3.5　Emotetダウンローダーが添付されていたメールの文面

■パスワード付きZIPファイルを使用する事例（2020年9月下旬に確認）
2020年9月下旬には、添付ファイルにパスワード付きのZIPファイルを使用する手法が確認されました。ファイルを展開するためのパスワードは本文中に記載されています。
この手法には攻撃者にとって以下のメリットがあると考えられます。

- セキュリティ製品を回避すること
- 日本企業においてパスワードZIPファイルの利用が習慣化しており、警戒心を持たずに展開する人が多いと考えられること

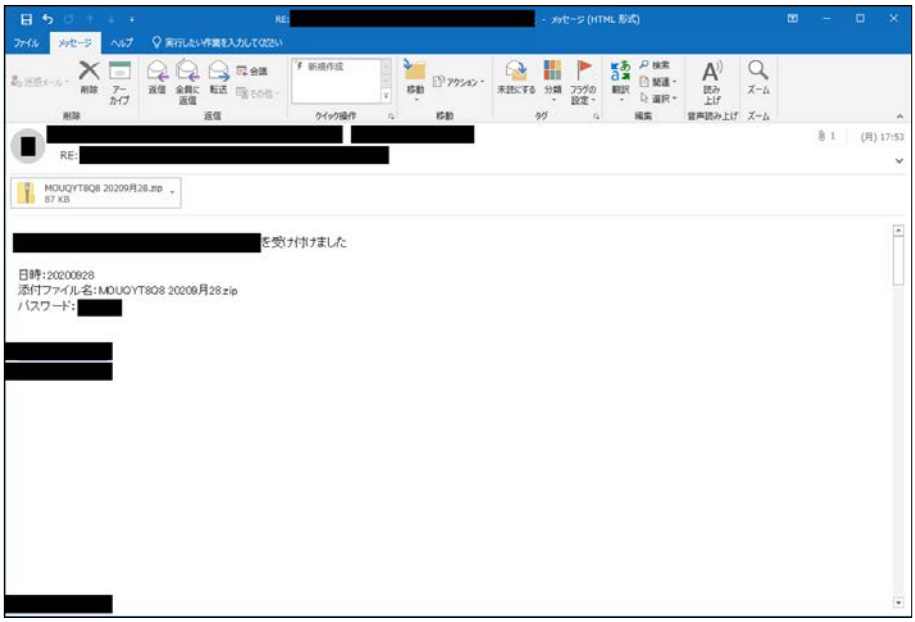


図3.6　パスワード付きZIPを添付したメールの文面

添付のWordファイルは日本語で書かれており、日本のユーザーを狙っていることがわかります。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、PowerShellのスクリプトが実行された後Emotetに感染します。

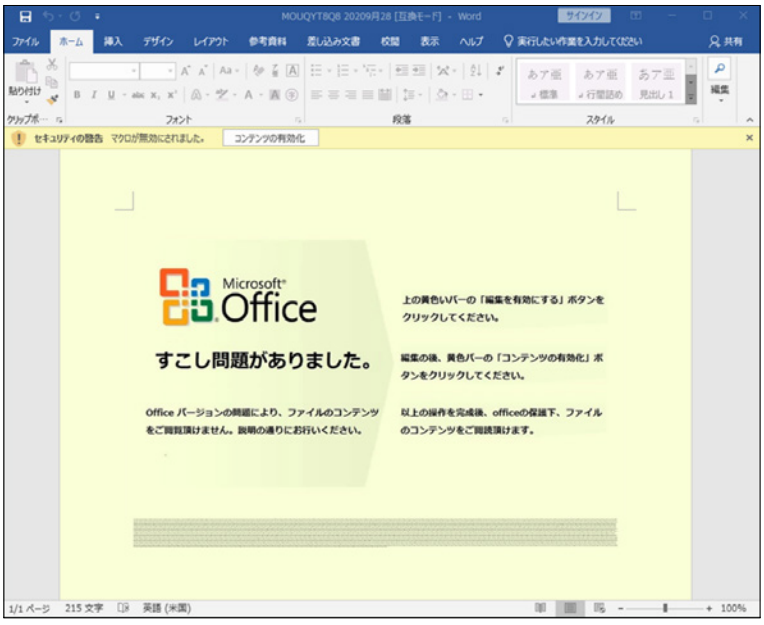


図3.7　ZIPファイルの中身のWordファイル

■アップデート通知を装う事例（2020年10月中旬から確認）

2020年10月中旬には、アップデート通知を装うWordテンプレートを用いた攻撃が確認されました。偽のアップデート通知は本事例の他に悪性Webサイト等においてユーザーのクリックを誘導する目的で頻繁に使われています。

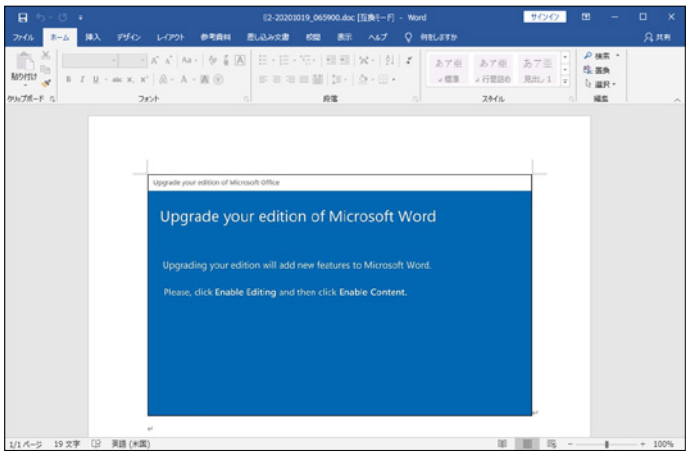


図3.8　アップデート通知を偽装するWordファイル（青背景）

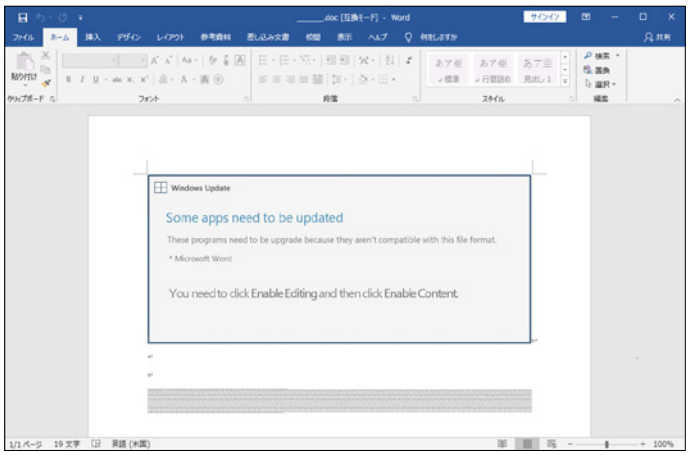


図3.9　アップデート通知を偽装するWordファイル（白背景）

3.　まとめとEmotetへの対策

ご紹介したように2020年の後半にはEmotetへの感染を狙うメール攻撃が多数確認されました。また、メールに添付されたWordファイルのテンプレートも頻繁に更新が行われていました。

本稿執筆時点（2021年2月）では、Emotetの攻撃者サーバーは既にテイクダウンされており[xi]、新規の攻撃が発生する可能性は低いと考えられます。

しかしながら同様のマルウェアは依然として数多く存在し、それらの脅威への対策が必要です。

Emotetへの感染を防ぐために、以下のセキュリティ対策を推奨します。

第3章　Emotetの継続的な活動とさらなる攻撃手法の巧妙化

■Emotetへの感染を防ぐための対策

- OSやソフトウェアに更新プログラムを適用し、常に最新の状態に保つ
- セキュリティ製品を導入し、常に最新の状態に保つ
- Microsoft Officeのマクロ実行設定が無効になっていることを確認する
- スクリプトファイル（JavaScript、VBScript等）を開く既定のアプリケーションをテキストエディターに変更する（スクリプトファイルのローカル実行を防ぐ）
- ファイアウォールを適切に設定する

■Emotetに感染した場合に被害を最小限に抑えるための対策

- サーバーのアクセス権限を適切に設定する
- 管理共有を無効にする

4

継続的に検出される VBAで作成されたダウンローダーの 主流テクニック

第4章　継続的に検出されるVBAで作成されたダウンローダーの主流テクニック

本章では、ESET製品でVBA/TrojanDownloader.Agentとして検出されるマルウェアの挙動や機能について紹介します。

1.　VBA/TrojanDownloader.Agentの概要と検出状況

VBA/TrojanDownloader.Agentは、Microsoft Office製品で利用されるプログラミング言語のVBA（Visual Basic for Applications）で作成されたダウンローダーです。VBAのマクロが実行されると、ダウンロードサーバーと通信を行い、攻撃者によって用意されたマルウェアが最終的にダウンロードされ実行されます。2020年に国内で確認された事例として、Emotet、Dridex、IcedID、Ursnif、Zloaderなどの感染を狙った攻撃に、本ダウンローダーが使用されました。

第1章で紹介した通り、本ダウンローダーは2020年の国内における検出割合上位5位に位置付けており、頻繁に確認されたマルウェアです。また、Webブラウザー上ではなく、ローカル環境で動作するマルウェアに限定すると、最も多く検出されました。そして、表 4.1に示す通り、本ダウンローダーは2020年だけではなく、近年継続的に国内で多く検出されています。

表 4.1　VBA/TrojanDownloder.Agentの国内検出状況[3]

	国内検出数の順位	国内検出数の順位 （ローカル環境で動作するものに限定）
2015年	1位	1位
2016年	2位	2位
2017年	3位	3位
2018年	1位	1位
2019年	4位	2位
2020年	5位	1位

2.　VBA/TrojanDownloader.Agentの侵入経路

VBA/TrojanDownloader.Agentの主な侵入経路はメールです。不特定多数に送られる、ばらまき型メールに添付されていることが大半です。メール文や本ダウンローダーの実行画面に表示される文章には、さまざまな言語のものが確認されています。以下は、日本語が使用された事例です。
本ダウンローダーが添付されたばらまきメールは、図 4.1に示すようなビジネスメールを装う文面や、当時の時事問題や年間行事を取り上げる文面が多く存在します。

3　PUAのデータを含めていません。

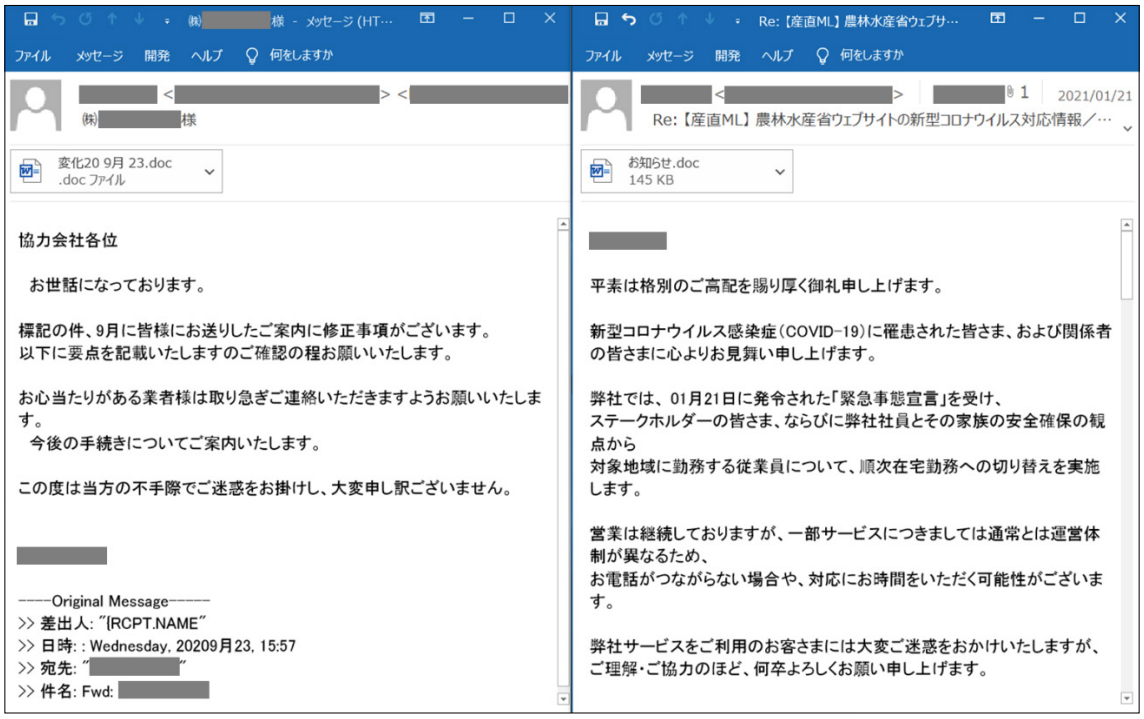


図 4.1　VBA/TrojanDownloader.Agentが添付されたばらまきメール
ビジネスメールを装ったメール（左）、時事問題を取り上げたメール（右）

添付ファイルを実行すると、図 4.2に示すような画像と文章が表示されます。実行時に表示される画像と文章には、さまざまなパターンが存在します。文章には、「編集を有効にする」と「コンテンツの有効化」をクリックすることを推奨する内容が記載されていることがあります。これは、Microsoft Officeがデフォルトで設定している保護機能を解除させるためです。ユーザーが記載された文章の指示通りに、「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、ダウンロードサーバーと通信を行います。

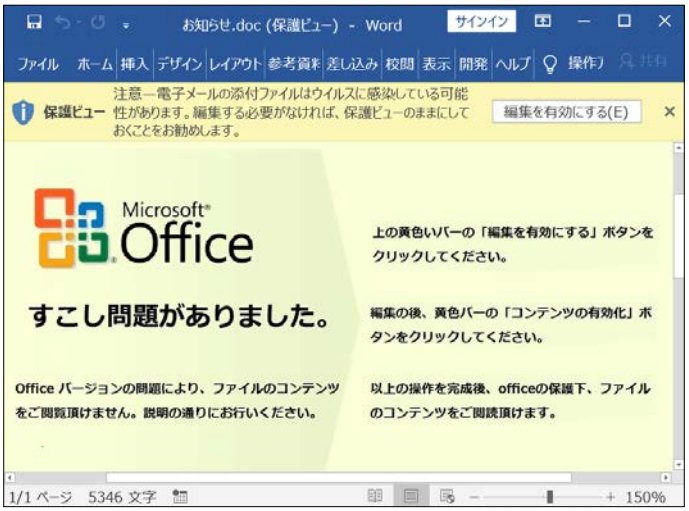


図 4.2　VBA/TrojanDownloader.Agentの実行画面（一例）

3.　ダウンロードサーバーと通信を行うまでのプロセス呼び出しの流れ

マクロ実行後、ダウンロードサーバーと通信を行うまでのプロセス呼び出しの流れには、複数の経路が存在します。主な経路（3種類）を図 4.3に示します。

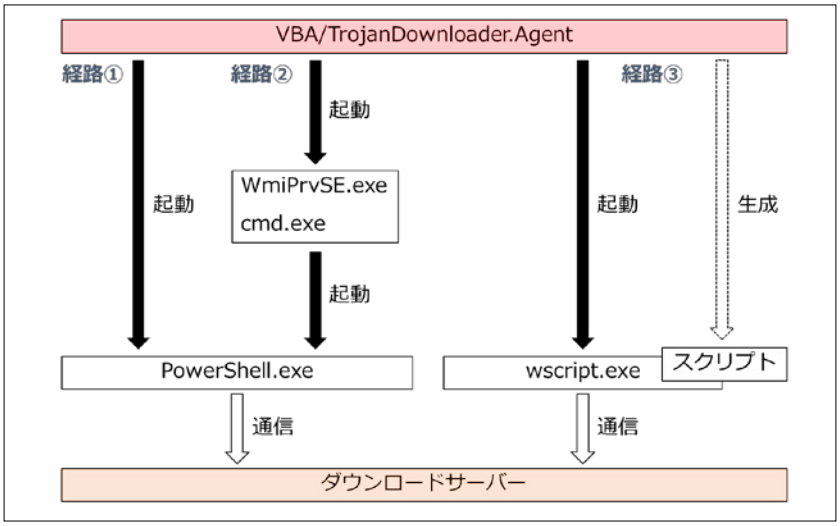


図 4.3　ダウンロードサーバーと通信を行うまでのプロセス呼び出しの流れ

図 4.3で示した3つの経路は、PowerShell.exeを経由する経路（経路①&②）と、本ダウンローダーが作成したスクリプトをwscript.exeが実行する経路（経路③）の2種類に大別されます。前者経路のPowerShell.exeが実行されるまでのプロセスにおいては、本ダウンローダーから直接起動される経路やWmiPrvSE.exe[4]やcmd.exeを経由する経路が確認されています。

ダウンロードサーバーと通信した結果、攻撃者が目的とするマルウェアがすぐにダウンロードされるケースもありますが、複数のダウンロードサーバーと通信を行うケースも存在します。例えば、新たなダウンローダーをダウンロードし実行するもの、スクリプトをダウンロードし実行するもの、ステガノグラフィが施された画像ファイルをダウンロードし、コードを抽出し実行するものなどがあります。

以上で示したように、本ダウンローダーは攻撃者が目的とするマルウェアをダウンロードするまでにさまざまな経路が存在します。また、次節で紹介するセキュリティ製品による検出回避や解析妨害の機能が施されたものも存在し、さらにダウンロードサーバーのURLも頻繁に変化します。そのため、本ダウンローダーには非常に多くの亜種が存在します。2020年に国内で検出された本ダウンローダーの亜種は582種類も確認されており、日々新しい亜種も発見され続けています。

4　Windows Management Instrumentation Provider Host Serviceの略で、主にWindowsホストを管理する目的で利用されます。

4.　VBA/TrojanDownloader.Agentの検出回避&解析妨害のテクニック

VBA/TrojanDownloader.Agentは、セキュリティ製品による検出を回避したり、解析者による解析を妨害したりするための機能を複数保有しています。回避や妨害には、シグネチャの回避、コード解析による検知の回避、サンドボックスや解析システムの回避などがあります。以下に、主流のテクニックを紹介します。

① パスワード保護

攻撃者はVBAコードを解析者に閲覧できなくさせるために、コードにパスワード保護を施したり、プロジェクトにロックをかけたりします。これらは、バイナリを書き換える方法や、専用のツール（EvilClippyなど）を使用することで解除できる場合があります。

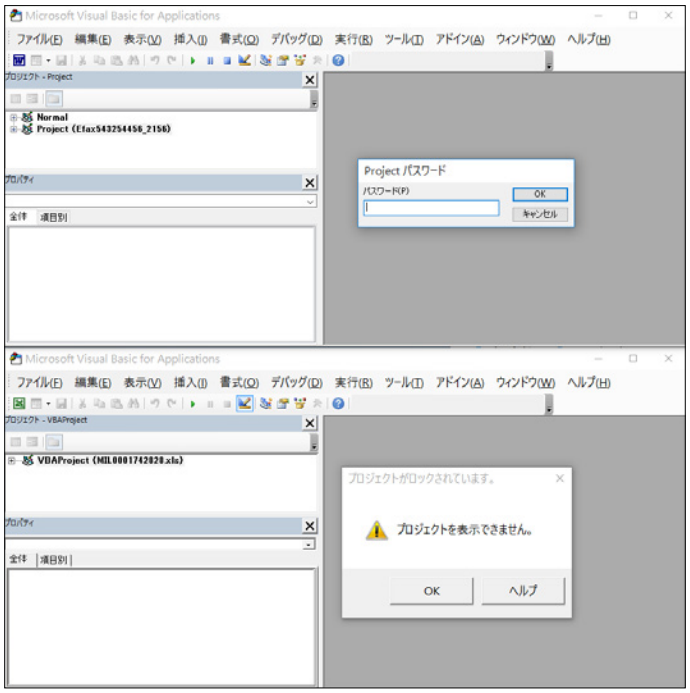


図 4.4　パスワード保護されたVBAマクロ（上）　ロックされたプロジェクト（下）

② ダミーコード

攻撃者は、シグネチャベースのセキュリティ製品による検知を回避したり、解析者による解析に時間がかかるようにしたりするために、不要な処理を記述したダミーコードを挿入します。

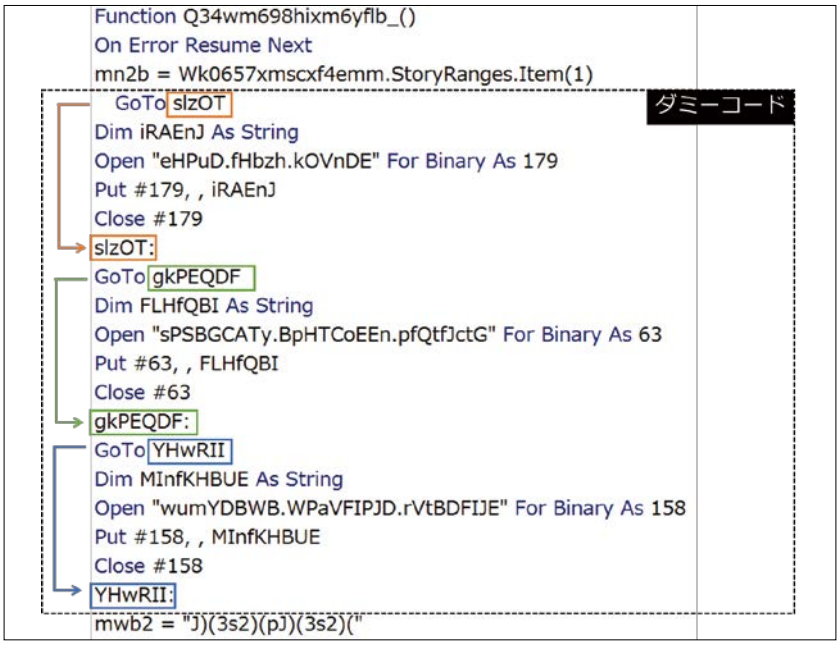


図 4.5　ダミーコードが挿入されたVBAコード

図 4.5に示した22行のVBAコードは、不要なGoTo文が多用されており、実際には動作に必要な行は4行しかありません。

③ 難読化

攻撃者は、セキュリティ製品による検知を回避したり、解析者による解析を遅らせたりするために難読化を施します。難読化が施されるのは、VBAのコード内、生成したスクリプト、PowerShell.exeに実行させるコマンドなど多岐にわたります。

VBAのコード内や生成したスクリプトにおける難読化には、変数名をランダムにする方法や、文字列をさまざまな方法で断片化し、後に結合する方法が多く確認されます。PowerShell.exeに実行させるコマンドには、Base64でエンコードされていることが多く確認されます。図 4.6、図 4.7、図 4.8にそれぞれの例を示します。

図 4.6　VBA/TrojanDownloader.Agentによって生成された難読化スクリプト

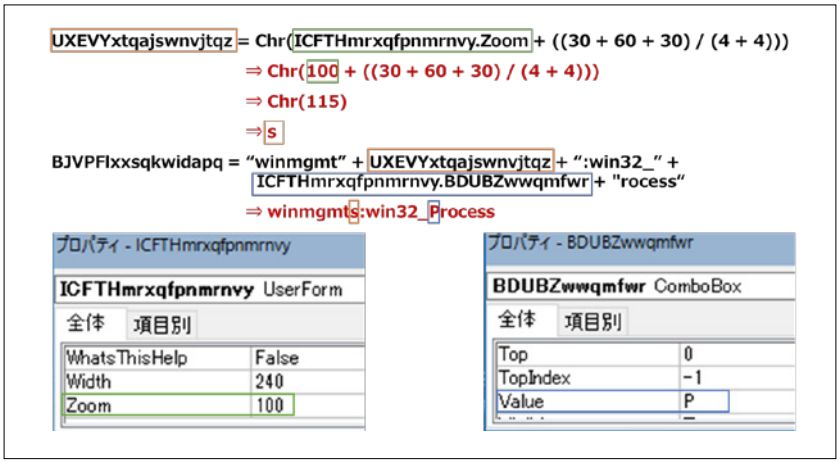


図 4.7　VBAコード内で断片化された文字列「winmgmts:win32_Process」

図 4.8　VBA/TrojanDownloader.Agentによって実行された難読化PowerShellコマンド

④ 解析環境の検知

攻撃者は、解析者や解析システムによる解析を妨害するために、解析環境を検知する機能を保有させます。解析環境と検知されると、ダウンロードサーバーとの通信は行わず、処理を終了させるものが確認されています。

図4.9に解析環境を検知するVBAコードを示します。

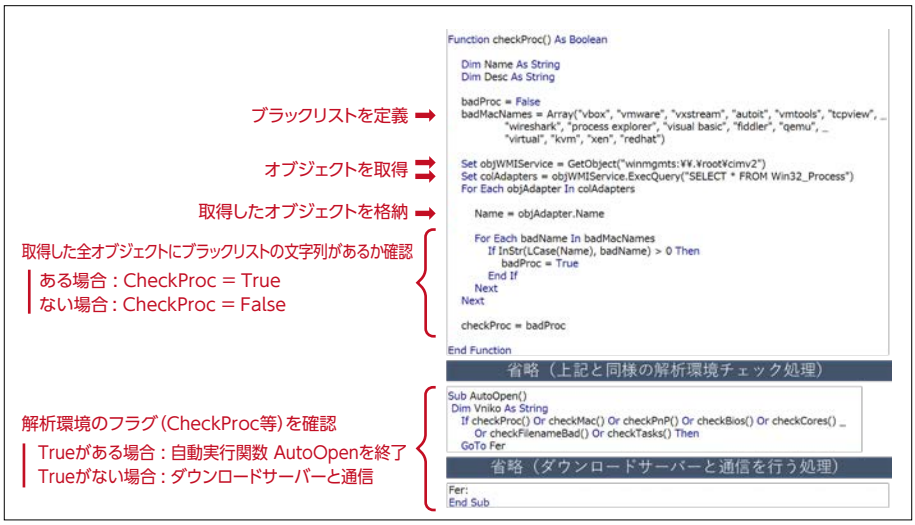


図 4.9　解析環境を検知するVBAコード

図4.9に示すVBAコードでは、objWMIService.ExecQueryを用いて、実行環境のオブジェクトを収集します。そして、収集した全オブジェクトに攻撃者があらかじめ定義したブラックリスト文字列が含まれるかどうかを確認します。ブラックリスト文字列には、著名な仮想化ソフトウェアや解析ツールなどが登録されています。ブラックリスト文字列が含まれるオブジェクトが確認された場合、ダウンロードサーバーと通信を行う処理は行われず、マクロが終了します。

上記手法では、オブジェクトを取得するobjWMIService.ExecQueryが用いられましたが、プロセスを取得するApplication.Tasksを用いて、ブラックリスト文字列を含むかどうかで検知する手法も有名です。
その他に、ファイル名が16進数の文字列だけで構成されているかどうかを確認する手法もあります。自動解析システムでは、16進数で記述されるハッシュ値で検体を管理することがあるため、自動解析システムの環境であるかどうかを判断するために本手法が用いられていると考えられます。
以上に示した手法以外に、解析環境を検知する手法は数多く存在します。そのため、解析者は回避・解決しながら解析を行います。

5.　まとめと対策

ご紹介したように、VBA/TrojanDownloader.Agentが2020年も近年と同様に国内で非常に多く検出されました。本ダウンローダーは、ビジネスメールを装ったり、時事問題を取り上げたりしたメールに添付されていることが多く確認されています。ユーザーが添付ファイルを実行し、マクロを有効化すると、ダウンロードサーバーと通信を行い、攻撃者が用意したマルウェアに最終的に感染します。

本ダウンローダーの対策をするうえで、重要なポイントを以下にまとめます。

① 情報セキュリティリテラシーの向上
基本的な対策は、メールに添付された本ダウンローダーを実行しないことです。そのため、不審なメールに添付されたファイルを実行しない、といった情報セキュリティリテラシーの基礎が重要になります。組織内で情報セキュリティリテラシーを高い状態で維持するために、教育を定期的に実施することが有効です。

② セキュリティ製品の導入

本ダウンローダーが添付された不審メールの文章には、整ったものも確認されており、判断に迷う場合もあります。またヒューマンエラーを完全に排除することは困難です。そのため、万が一に本ダウンローダーを実行してしまった際に備えて、セキュリティ製品を導入しておくことが重要です。

③ セキュリティ製品の定義データベースを最新の状態に維持

セキュリティ製品は、導入するだけでは不十分です。ご紹介した通り、本ダウンローダーには非常に多くの亜種が存在しており、新しい亜種が確認され続けています。そのため、セキュリティ製品の定義データベースを最新の状態に維持し続けることが重要です。

④ 情報共有

流行しているサイバー攻撃は、注意喚起されることがあります。不審なメールかどうか判断に迷う際に、注意喚起された情報が役に立つことがあります。以下に示すようなサイトを日々確認し、組織内で共有することが重要です。

- JPCERT/CC「CyberNewsFlash」 https://www.jpcert.or.jp/newsflash/
- 日本サイバー犯罪対策センター（JC3） https://www.jc3.or.jp/index.html

引用・出展元

i 2019年 年間マルウェアレポート [PDF] | マルウェア情報局
https://eset-info.canon-its.jp/files/user/malware_info/images/ranking/pdf/MalwareReport_2019.pdf

ii ランサムウェアの身代金支払い額、日本は平均で約1億2300万円 | ZDNet Japan
https://japan.zdnet.com/article/35162969/

iii 事業継続を脅かす 新たなランサムウェア攻撃 について [PDF] | IPA(情報処理推進機構)
https://www.ipa.go.jp/files/000084974.pdf

iv Avaddonランサムウェアの解析 [PDF] | マルウェア情報局
https://eset-info.canon-its.jp/files/user/malware_info/images/threat/201027/Malware_Report_Avaddon_202010.pdf

v FBI FLASH MU-000140-MW [PDF] | WaterISAC
https://www.waterisac.org/system/files/articles/FLASH-MU-000140-MW.pdf

vi Ragnar Locker ransomware deploys virtual machine to dodge security | Sophos
https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/

vii Ransomware Gangs to Stop Attacking Health Orgs During Pandemic | Bleeping Computer
https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/

viii New Jersey hospital paid ransomware gang $670K to prevent data leak | Bleeping Computer
https://www.bleepingcomputer.com/news/security/new-jersey-hospital-paid-ransomware-gang-670k-to-prevent-data-leak/

ix 情報セキュリティ安心相談窓口の相談状況[2020年第3四半期(7月～9月)] | IPA(情報処理推進機構)
https://www.ipa.go.jp/security/txt/2020/q3outline.html

x 情報セキュリティ安心相談窓口の相談状況[2020年第4四半期(10月～12月)] | IPA(情報処理推進機構)
https://www.ipa.go.jp/security/txt/2020/q4outline.html

xi WORLD'S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION | Europol
https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

強くて軽い。
妥協なきセキュリティ。

ENJOY SAFER TECHNOLOGY™

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. 03-6701-3452

MWJY2103CMJ_PDF