2020年
1·2月
JAN / FEB

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

## 新型コロナウイルス感染症の流行に便乗するサイバー攻撃

キヤノンマーケティングジャパン株式会社

# はじめに

「マルウェアレポート」は、キヤノンマーケティングジャパンが運営する

「サイバーセキュリティラボ」が「ESET セキュリティ ソフトウェア シリーズ」の

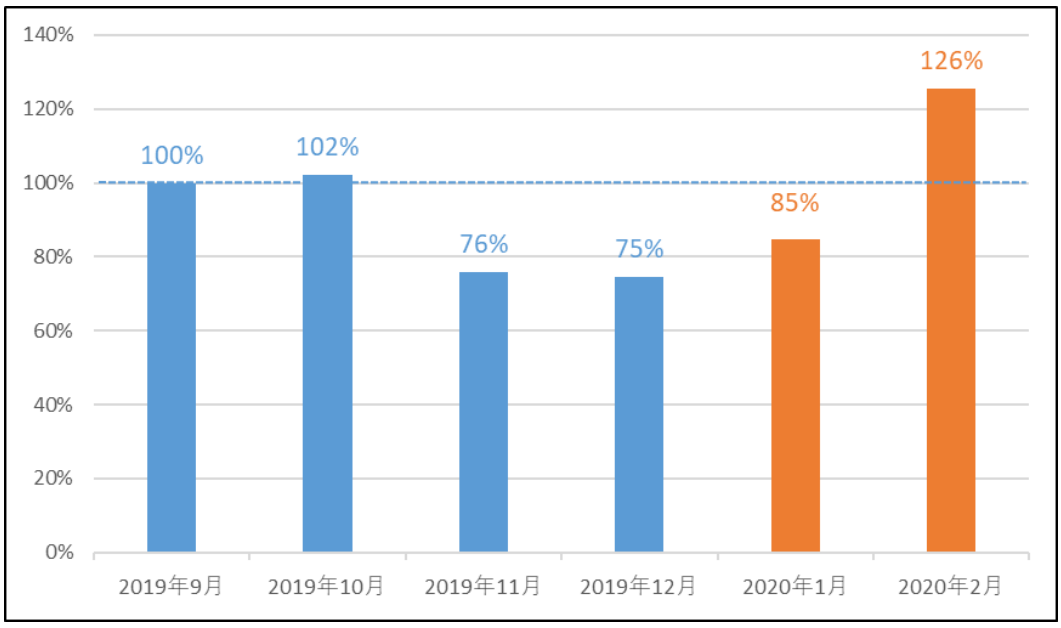
マルウェア検出データを基に国内のマルウェア検出状況を分析し、まとめたレポートです。

# ショートレポート「2020 年 1 月 2 月マルウェア検出状況」



## 1. 1 月と 2 月の概況

2020 年 1 月（1 月 1 日～1 月 31 日）と 2 月（2 月 1 日～2 月 29 日）に ESET 製品が国内で検出したマルウェアの検出数の推移は、以下のとおりです。




**国内マルウェア検出数*1 の推移**

**(2019 年 9 月の全検出数を 100%として比較)**

*1 検出数には 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)を含めています。

2020 年 1 月と 2 月の国内マルウェア検出数は、減少傾向にあった昨年 12 月から一転して増加しました。検出されたマルウェアの内訳は以下のとおりです。

**国内マルウェア検出数*2 上位（2020 年 1 月 2 月）**

| 順位 | マルウェア | 割合 | 種別 |
|---|---|---|---|
| 1 | JS/Adware.Subprop | 9.6% | アドウェア |
| 2 | HTML/ScrInject | 7.9% | HTML に埋め込まれた不正スクリプト |
| 3 | JS/Adware.Agent | 7.1% | アドウェア |
| 4 | JS/Adware.PopAds | 5.2% | アドウェア |
| 5 | JS/Danger.ScriptAttachment | 4.1% | ダウンローダー |
| 6 | VBA/TrojanDownloader.Agent | 3.2% | ダウンローダー |
| 7 | JS/Adware.Chogdoul | 1.6% | アドウェア |
| 8 | Win32/Exploit.CVE-2017-11882 | 0.8% | 脆弱性を悪用するマルウェア |
| 9 | HTML/FakeAlert | 0.7% | 偽の警告文を表示するスクリプト |
| 10 | JS/Redirector | 0.6% | 別のページに遷移させるスクリプト |

*2 本表には PUA を含めていません。

**国内マルウェア検出数*2 上位（2020 年 1 月）**

| 順位 | マルウェア | 割合 | 種別 |
|---|---|---|---|
| 1 | HTML/ScrInject | 13.8% | HTML に埋め込まれた不正スクリプト |
| 2 | JS/Adware.Subprop | 9.1% | アドウェア |
| 3 | JS/Adware.Agent | 8.7% | アドウェア |
| 4 | VBA/TrojanDownloader.Agent | 5.7% | ダウンローダー |
| 5 | Win32/Exploit.CVE-2017-11882 | 1.0% | 脆弱性を悪用するマルウェア |
| 6 | JS/Packed.Agent | 1.0% | パックされた JS 形式ファイルの汎用名 |
| 7 | GenScript | 1.0% | 不正スクリプトの汎用名 |
| 8 | HTML/FakeAlert | 0.9% | 偽の警告文を表示するスクリプト |
| 9 | MSIL/Kryptik.UGW | 0.9% | 難読化された MSIL 形式ファイルの汎用名 |
| 10 | JS/Redirector | 0.8% | 別のページに遷移させるスクリプト |

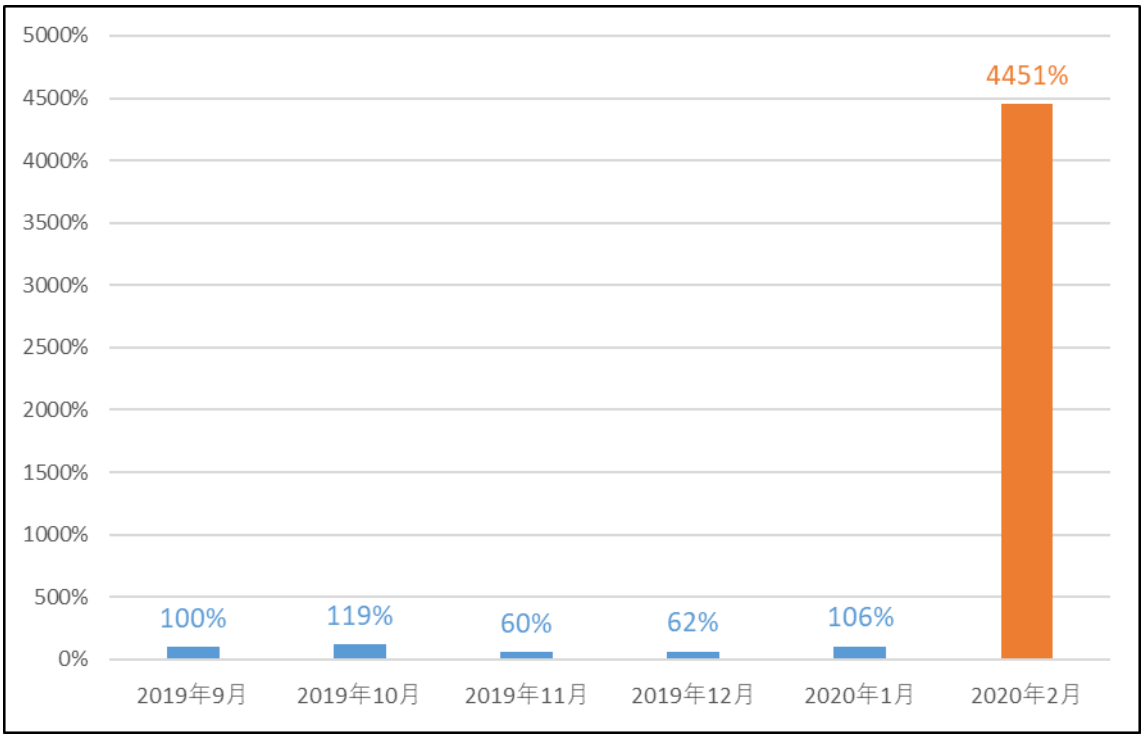
**国内マルウェア検出数*2 上位（2020 年 2 月）**

| 順位 | マルウェア | 割合 | 種別 |
|---|---|---|---|
| 1 | JS/Adware.Subprop | 9.9% | アドウェア |
| 2 | JS/Adware.PopAds | 8.7% | アドウェア |
| 3 | JS/Danger.ScriptAttachment | 6.7% | ダウンローダー |
| 4 | JS/Adware.Agent | 6.0% | アドウェア |
| 5 | HTML/ScrInject | 3.9% | HTML に埋め込まれた不正スクリプト |
| 6 | JS/Adware.Chogdoul | 2.7% | アドウェア |
| 7 | VBA/TrojanDownloader.Agent | 1.6% | ダウンローダー |
| 8 | PDF/Fraud | 0.8% | 詐欺サイトのリンクが埋め込まれた PDF |
| 9 | Win32/Injector.Autoit | 0.7% | 他のプロセスにインジェクションするマルウェア |
| 10 | Win32/Exploit.CVE-2017-11882 | 0.7% | 脆弱性を悪用するマルウェア |

*2 本表には PUA を含めていません。

1 月と 2 月に国内で最も検出されたマルウェアは、JS/Adware.Subprop でした。
JS/Adware.Subprop は、悪意のある広告を表示させるアドウェアで、Web サイト閲覧中に実行されます。
2 位の HTML/ScrInject は、HTML に埋め込まれた不正スクリプトで、こちらも Web サイト閲覧時に実行されます。

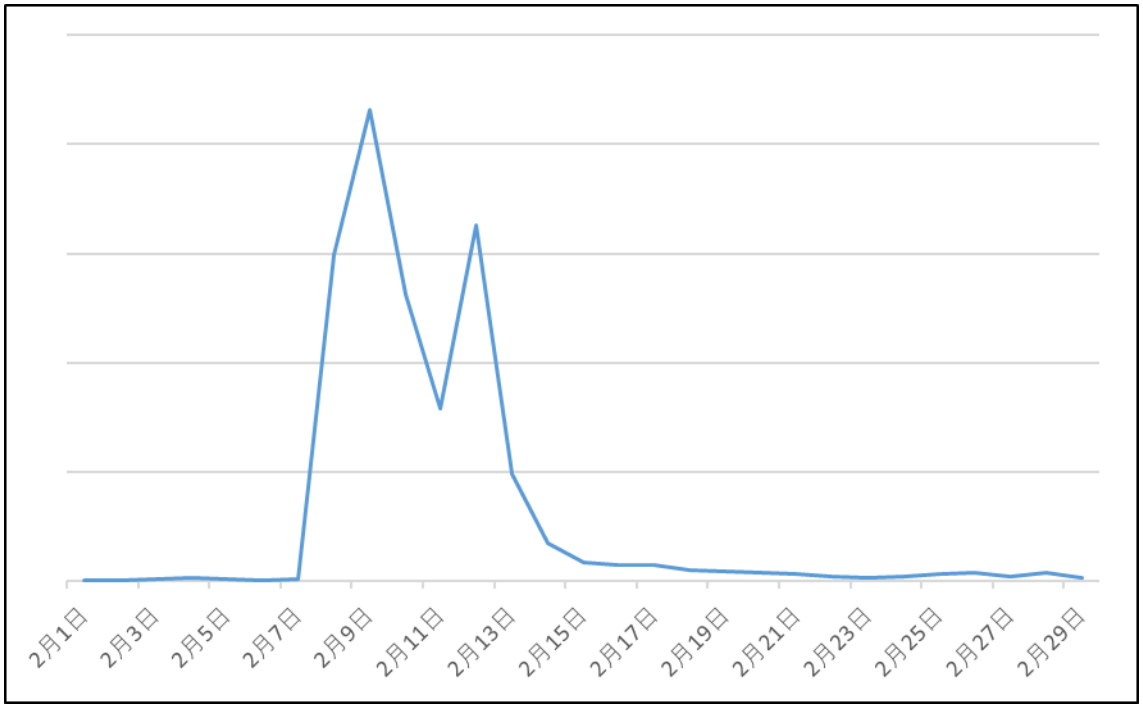
1 月と 2 月では、その他にもメールを介して拡散されるマルウェアの脅威が多く検出されています。
1 月では VBA/TrojanDownloader.Agent が多く検出され、2 月では JS/DangerScriptAttachment が多く検出されています。特に、JS/DangerScriptAttachment は直近 6 か月の検出数の推移を見ると、検出数の急激な増加が確認できます。




**JS/Danger.ScriptAttachment の検出数の月別推移（国内）**
**(2019 年 9 月の検出数を 100%として比較)**

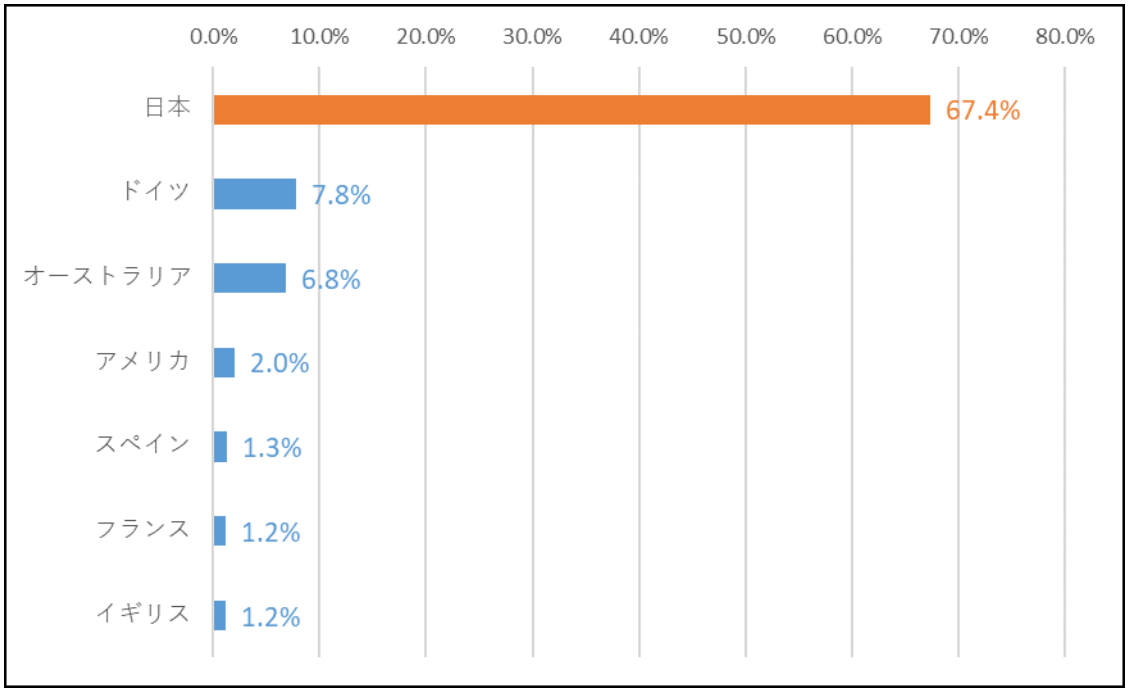
JS/Danger.ScriptAttachment とは、電子メールに添付された悪意のある JavaScript ファイルの汎用検出名です。特定のマルウェアではなく、受信したメールの添付ファイルに悪意があると判断されることで検出されます。同検出名で検出されたマルウェアの中にバンキングマルウェアのダウンローダーが含まれていたことも過去にはありま

した。
今月の JS/Danger.ScriptAttachment の検出は、2 月 8 日～2 月 15 日の間に検出されたものが大半を占めています。また、この期間には、ばらまきメールが送信されており、JS/Danger.ScriptAttachment の検出数増加の要因の 1 つになったと考えられます。




**JS/Danger.ScriptAttachment の検出数の日別推移（国内･2020 年）**

国別の検出数を見てみると、日本が最も JS/Danger.ScriptAttachment を検出した国となっています。割合も 67.4%と非常に高く、他の国の割合からも大きな差があります。




**JS/Danger.ScriptAttachment の国別検出割合（2020 年 2 月）**

メールを介して拡散されるこれらのマルウェアによる被害に合わない為にも、メールセキュリティ製品の利用やメールに添付されたファイルを不用意に開かないといった対策が重要です。

## 2. 新型コロナウイルス感染症の流行に便乗するサイバー攻撃

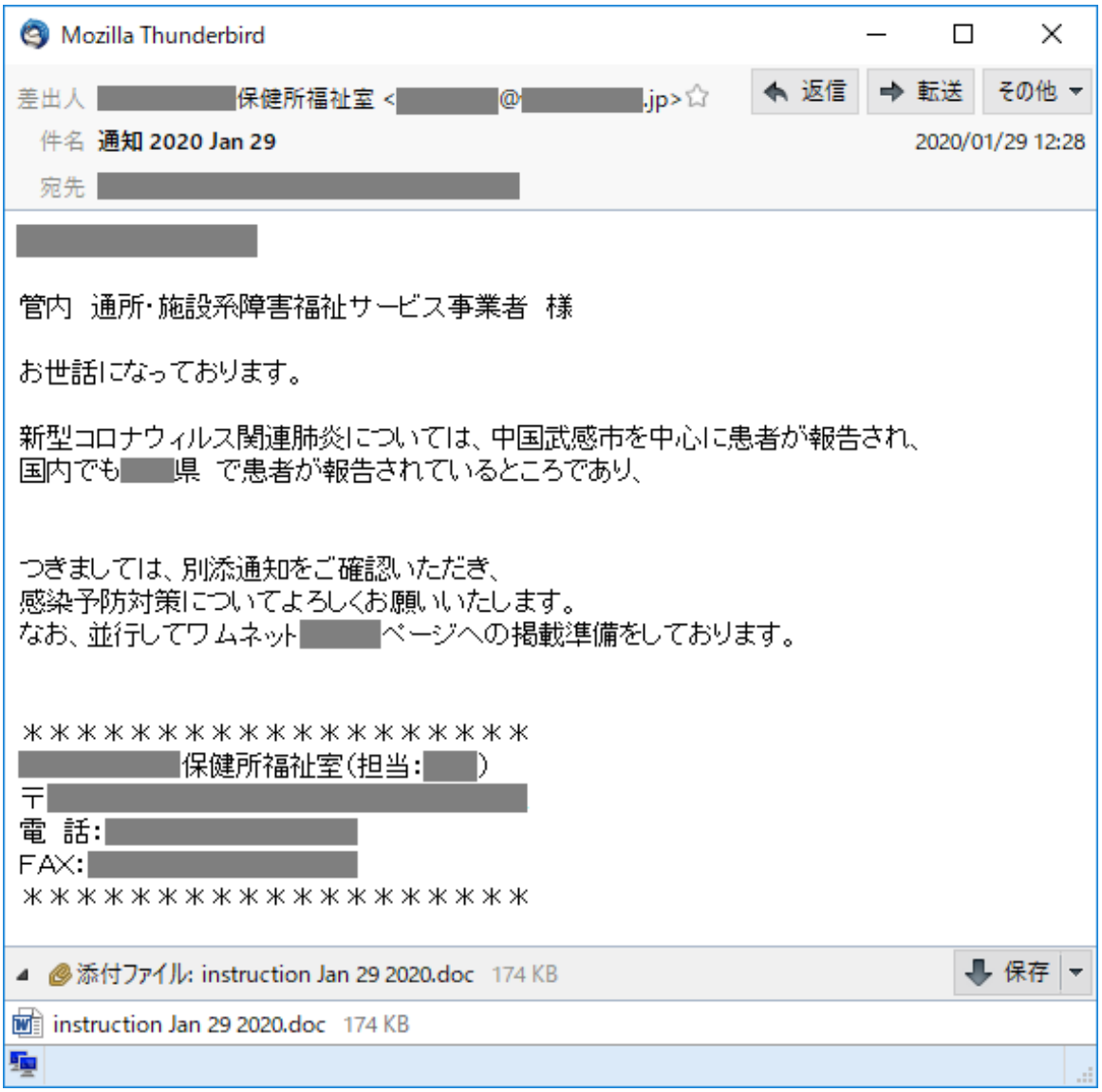
新型コロナウイルス感染症（COVID-19）が大多数の国で猛威を振るっている中、人々の不安に付け込むサイバー攻撃が確認されています。本章では、新型コロナウイルス感染症の流行に便乗した、サイバー攻撃の事例やマルウェアを紹介します。

■公的機関や民間企業を装うフィッシングメール攻撃

政府機関・研究所・保健所などの公的機関や民間企業を装ったフィッシングメールが、世界各地で多数確認されています。特に、ダウンローダーが添付されたものと不審な Web サイトへのアクセスを促すものが多いです。それぞれの事例を紹介します。

〇ダウンローダーが添付されたフィッシングメール

日本では 1 月末に、保健所を装い、Emotet への感染を目的とするメールが大量に確認されました。




**保健所を装うフィッシングメール**

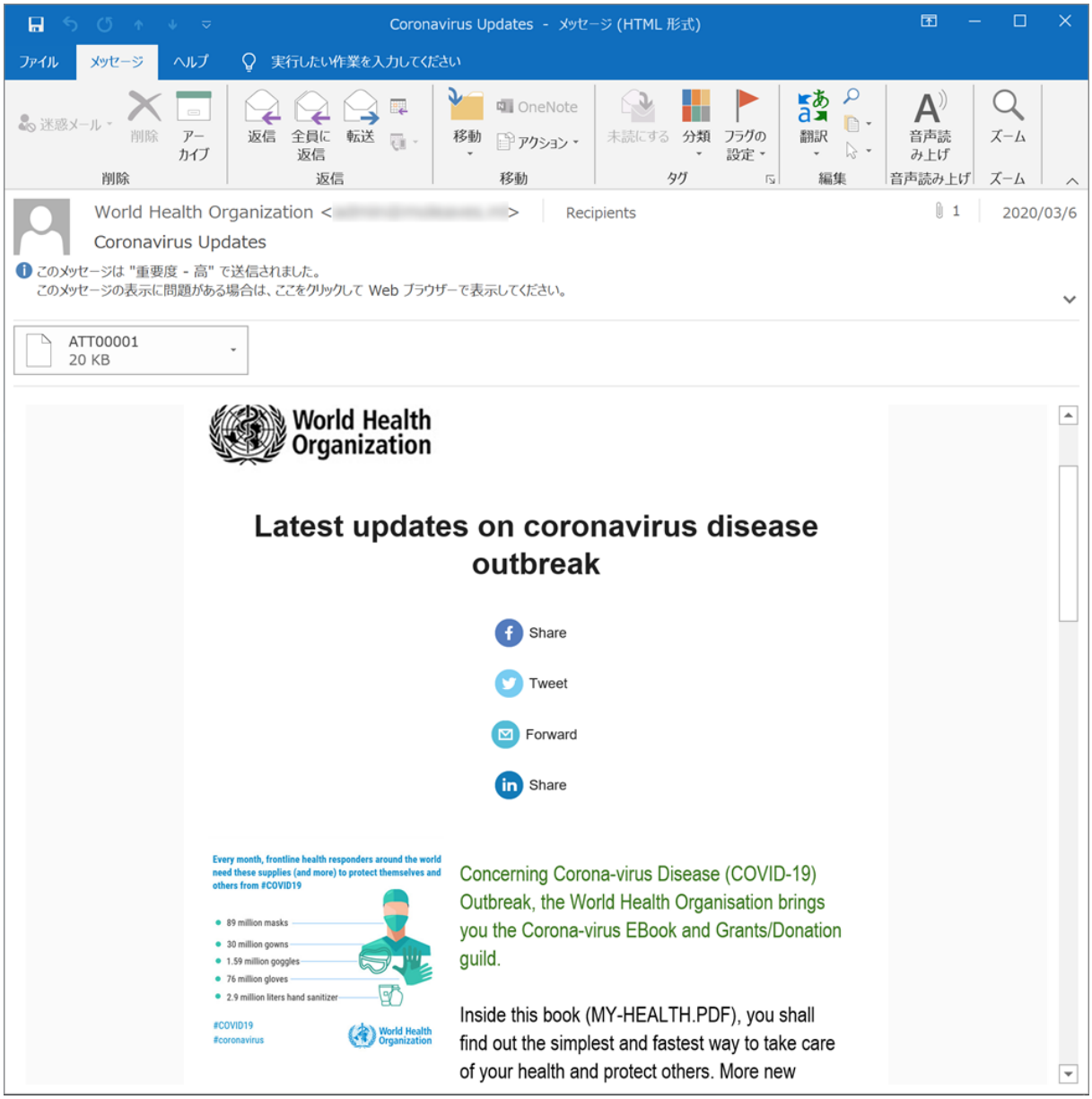
**（IPA |「Emotet」と呼ばれるウイルスへの感染を狙うメールについてより引用）**

本メールに記載されている保健所の組織名・住所・電話番号には、実在するものが使用されています。これらの情報は、公開されているホームページ等から収集されたことが予想されます。加えて、本メールの文章は比較的整っているため、違和感を覚えにくいものになっています。

添付された doc ファイルは、Emotet のダウンローダーとして機能します。ダウンロードされた Emotet は、情報の

窃取や他のマルウェアをダウンロードします。Emotet の詳細な挙動は、2019 年 年間マルウェアレポートの第 2 章やキヤノンオンラインセミナー[動画]をご覧ください。

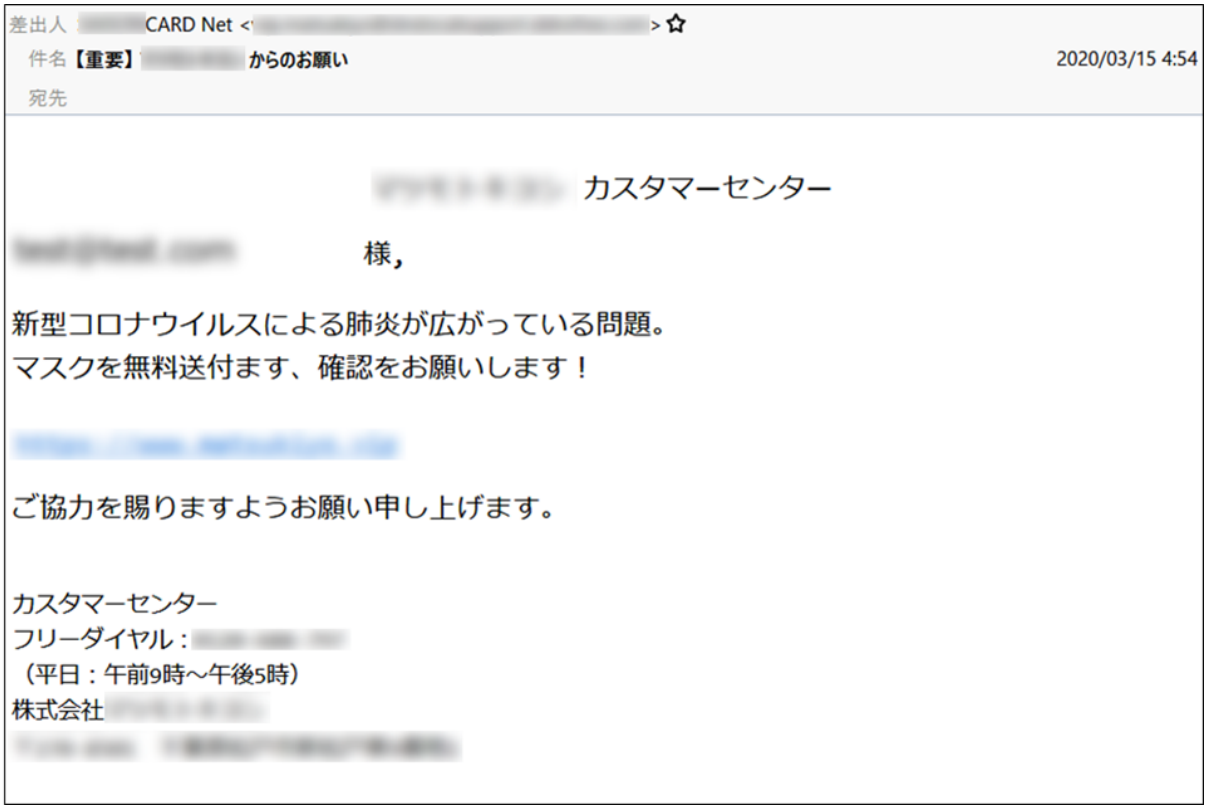
日本以外では、世界保健機構（WHO）を装ったフィッシングメールが確認されました。




**WHO を装うフィッシングメール（英語）**

本メールには、新型コロナウイルス感染症への対策方法をまとめた電子ブックと助成金を送付する旨が記載されています。添付ファイルは、ZIP 形式で圧縮されたダウンローダーです。添付ファイルをユーザーが解凍し実行すると、他のマルウェアがダウンロードされます。

〇不審な Web サイトへのアクセスを促すフィッシングメール
日本では、ドラッグストアを装ったフィッシングメールが確認されました。


差出人 CARD Net <
件名【重要】からのお願い 2020/03/15 4:54
宛先

カスタマーセンター

様,

新型コロナウイルスによる肺炎が広がっている問題。
マスクを無料送付ます、確認をお願いします！

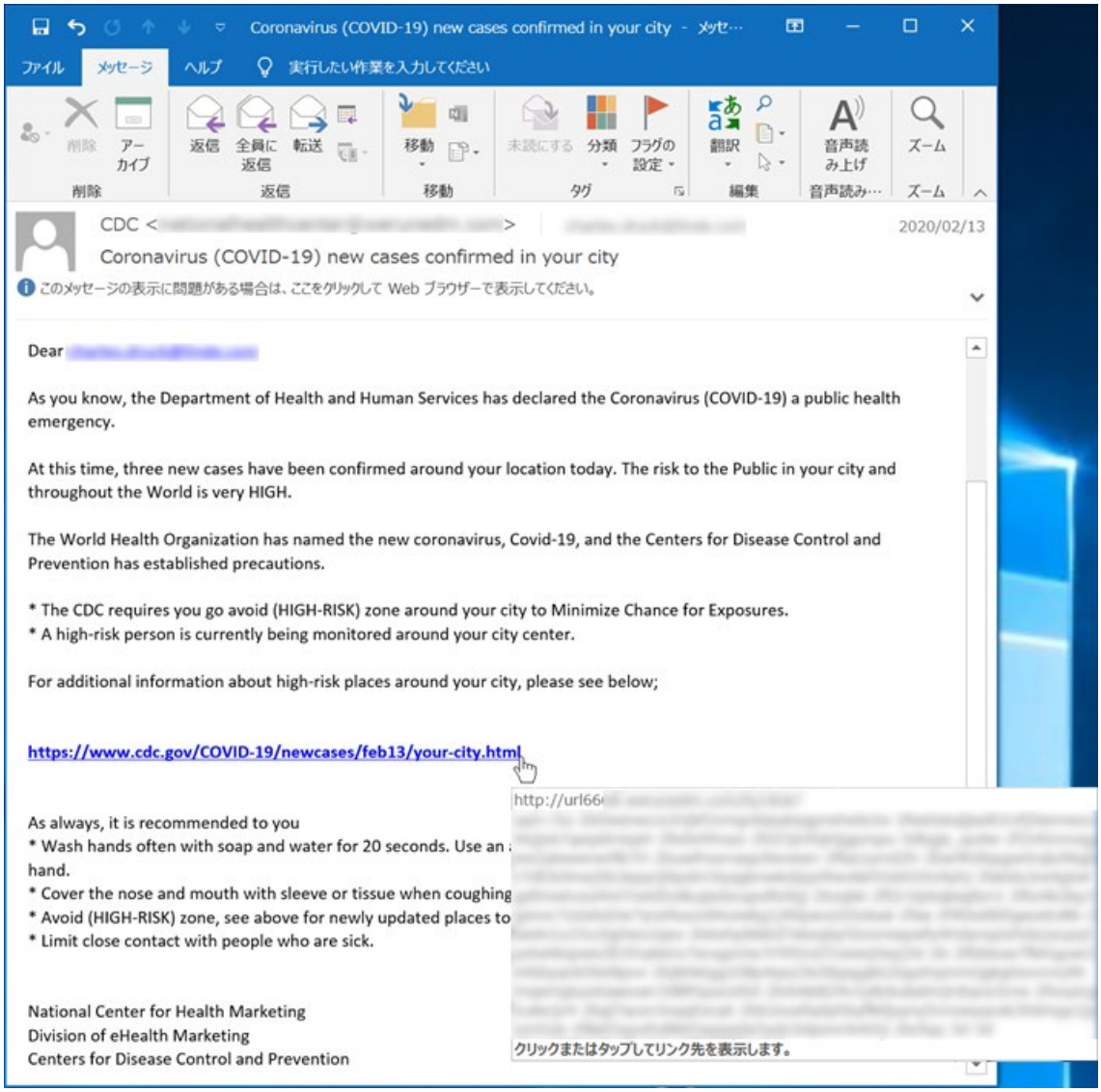
ご協力を賜りますようお願い申し上げます。

カスタマーセンター
フリーダイヤル：
（平日：午前9時～午後5時）
株式会社

**ドラッグストアを装うフィッシングメール**

本メールには、ドラッグストアの公式 Web サイトとは異なる URL が記載されています（上図青色部分[モザイク処理済み]）。

日本以外では、アメリカ疾病予防管理センター（CDC）を装ったフィッシングメールが確認されました。

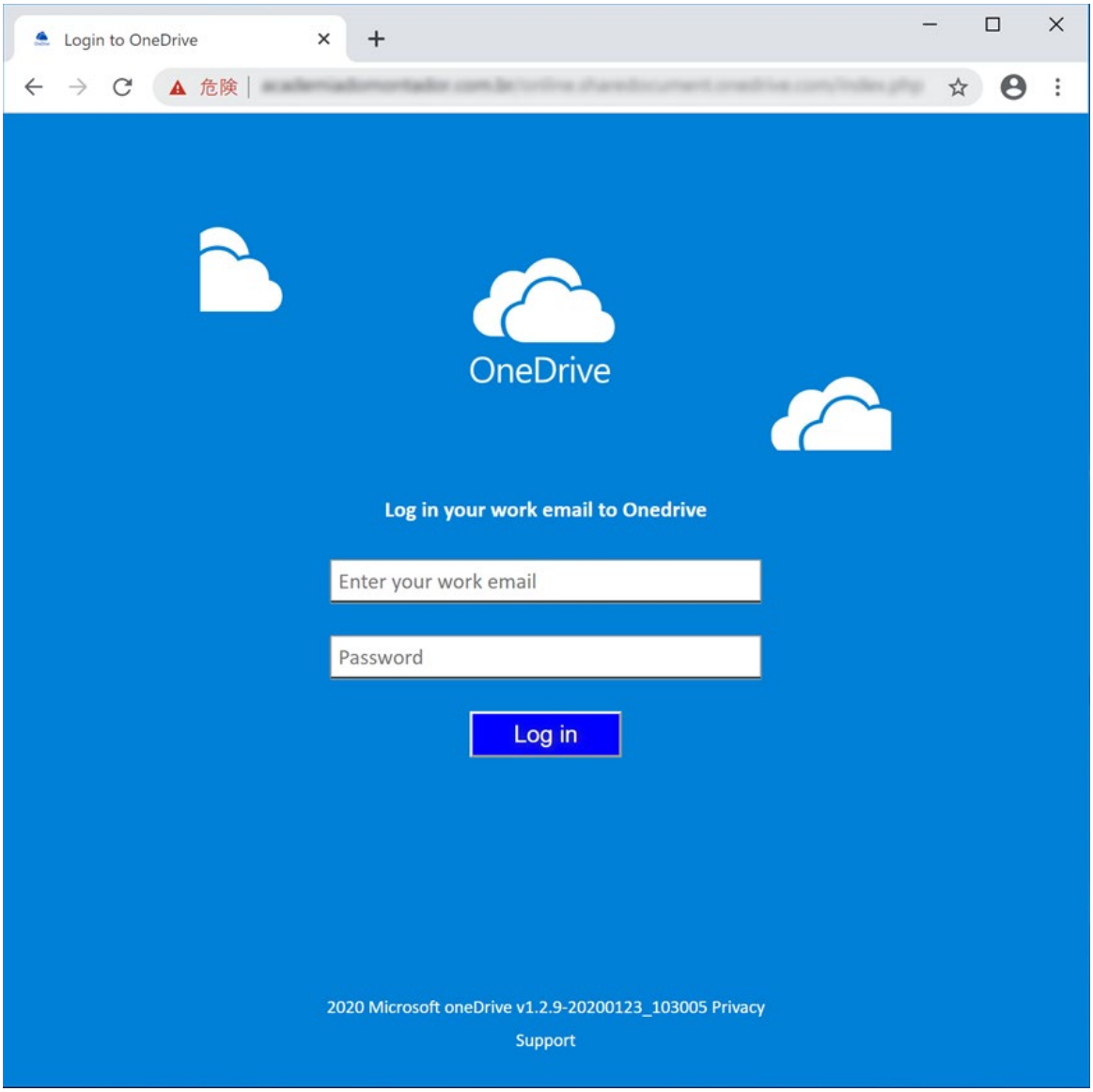



**CDC を装うフィッシングメール**

本メールには、新型コロナウイルス感染症への感染リスクが高い場所をまとめた Web サイトの閲覧を推奨する旨が記載されています。表示されている URL は CDC の公式 Web サイトですが、全く異なる URL がリンク先に設定されています。カーソルを URL に移動させると、実際にアクセスする Web サイトの URL を確認することができます。

フィッシングメールからアクセスする不審な Web サイトには、OneDrive や Outlook などにおける認証情報の入

力を求めるフィッシングサイトが確認されています。

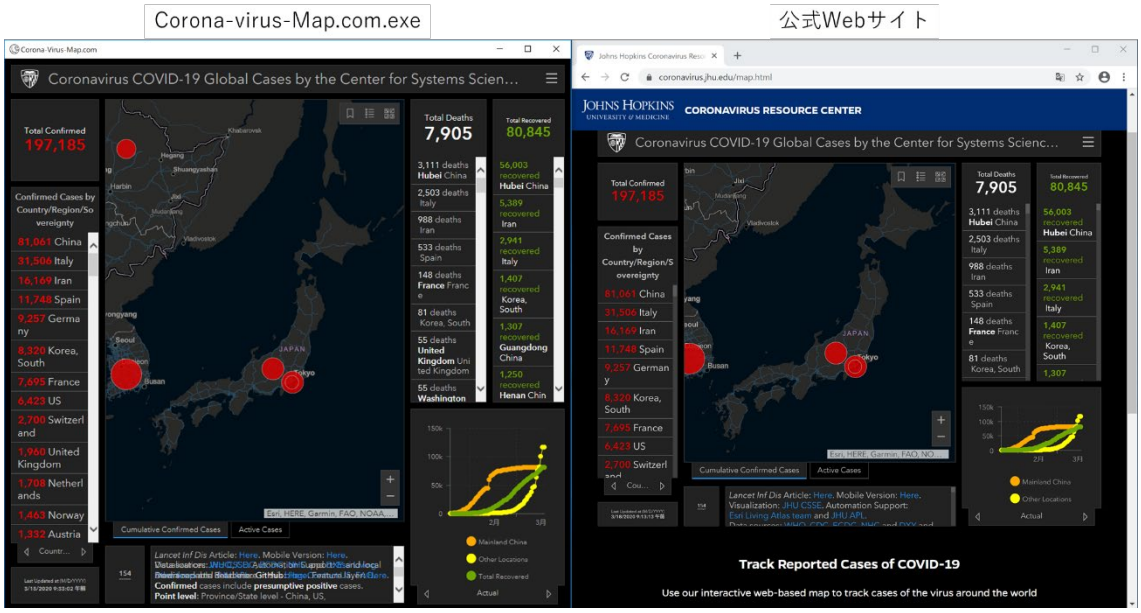



**OneDrive の認証情報を窃取するフィッシングサイト**

ユーザーがフィッシングサイトで認証情報を入力した場合、その情報は窃取される可能性があります。そして、窃取された認証情報を基に、不正アクセスの被害に遭うことが考えられます。

■新型コロナウイルス感染症に関連する名称のマルウェア

新型コロナウイルス感染症に関連する名称がつけられたマルウェア「Corona-virus-Map.com.exe」が発見されました。本マルウェアは、OS や Web ブラウザーに保存された情報を窃取するマルウェアです。
実行すると新型コロナウイルス感染症の感染状況が表示されます。表示される画面は、ジョンズ・ホプキンズ大学の Coronavirus Resource Center が提供している公式 Web サイトと同様の内容が表示されます。




**Corona-virus-Map.com.exe と公式 Web サイトの比較**

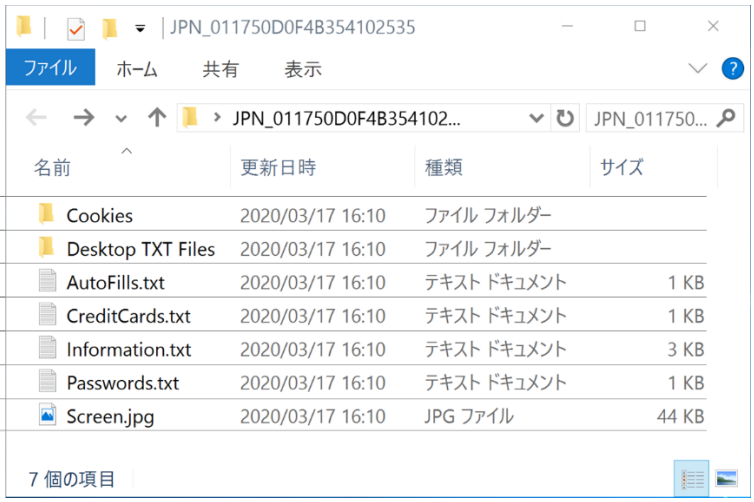
本マルウェアが、新型コロナウイルス感染症の感染状況を表示している裏では、OS や Web ブラウザーに保存された情報を取得し、C&C サーバーに送信するための様々なプロセスが実行されます。

| | |
|---|---|
| Corona-virus-Map.com.exe (224) | "C:¥Users¥User01¥Desktop¥Corona-virus-Map.com.exe" |
| Corona.exe (4788) | "C:¥Users¥User01¥AppData¥Roaming¥Z11062600¥Corona.exe" |
| cmd.exe (3536) | C:¥Windows¥system32¥cmd.exe /c ""C:¥Users¥User01¥AppData¥Local¥Temp¥RarSFX0¥Corona.bat" " |
| conhost.exe (1124) | ¥??¥C:¥Windows¥system32¥conhost.exe 0xffffffff -ForceV1 |
| Corona.sfx.exe (344) | Corona.sfx.exe -p3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r -dC:¥Windows¥System32 |
| Corona.exe (4860) | "C:¥Users¥User01¥AppData¥Local¥Temp¥RarSFX1¥Corona.exe" |
| bin.exe (5144) | "C:¥Users¥User01¥AppData¥Roaming¥Z58538177¥bin.exe" |
| Build.exe (3740) | "C:¥Users¥User01¥AppData¥Roaming¥Z58538177¥Build.exe" |
| Windows.Globalization.Fontgroups.exe (4340) | C:¥Users¥User01¥AppData¥Roaming¥amd64_netfx4-system.runti..dowsruntime.ui.xaml¥Windows.Gl.. |
| Windows.Globalization.Fontgroups.module.exe (5976) | C:¥Users¥User01¥AppData¥Roaming¥amd64_netfx4-system.runti..dowsruntime.ui.xaml¥Windows.Gl.. |
| conhost.exe (4296) | ¥??¥C:¥Windows¥system32¥conhost.exe 0xffffffff -ForceV1 |
| attrib.exe (4624) | attrib +s +h "C:¥Users¥User01¥AppData¥Roaming¥amd64_netfx4-system.runti..dowsruntime.ui.xaml" |
| conhost.exe (2788) | ¥??¥C:¥Windows¥system32¥conhost.exe 0xffffffff -ForceV1 |
| Corona-virus-Map.com.exe (4916) | "C:¥Users¥User01¥AppData¥Roaming¥Z11062600¥Corona-virus-Map.com.exe" |

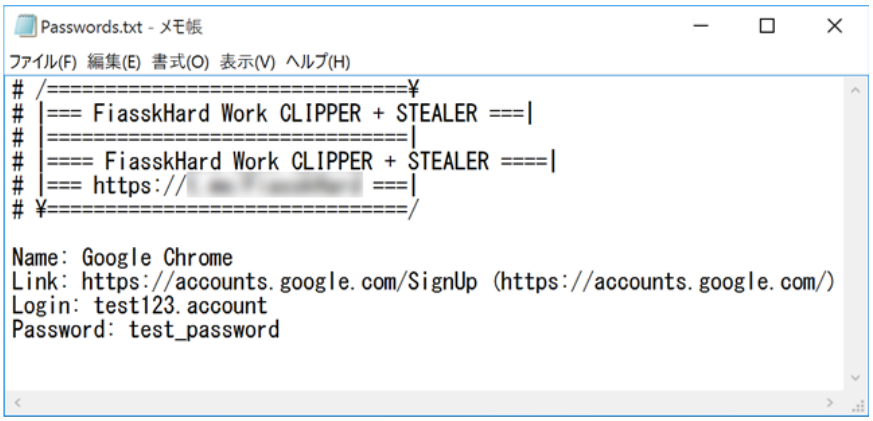
**Corona-virus-Map.com.exe 実行時のプロセスツリー**

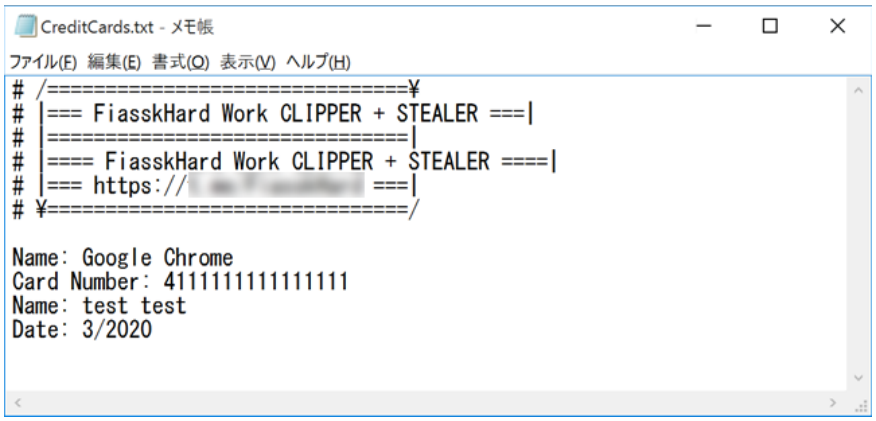
搾取される情報には、OS や Web ブラウザーに保存された認証情報やクレジットカード情報などがあります。

クッキー情報
デスクトップ配下のTXTファイル
オートコンプリート情報
クレジットカード情報
OS・実行プロセスなどの情報
パスワード情報
スクリーンショット




**Corona-virus-Map.com.exe が窃取した情報**

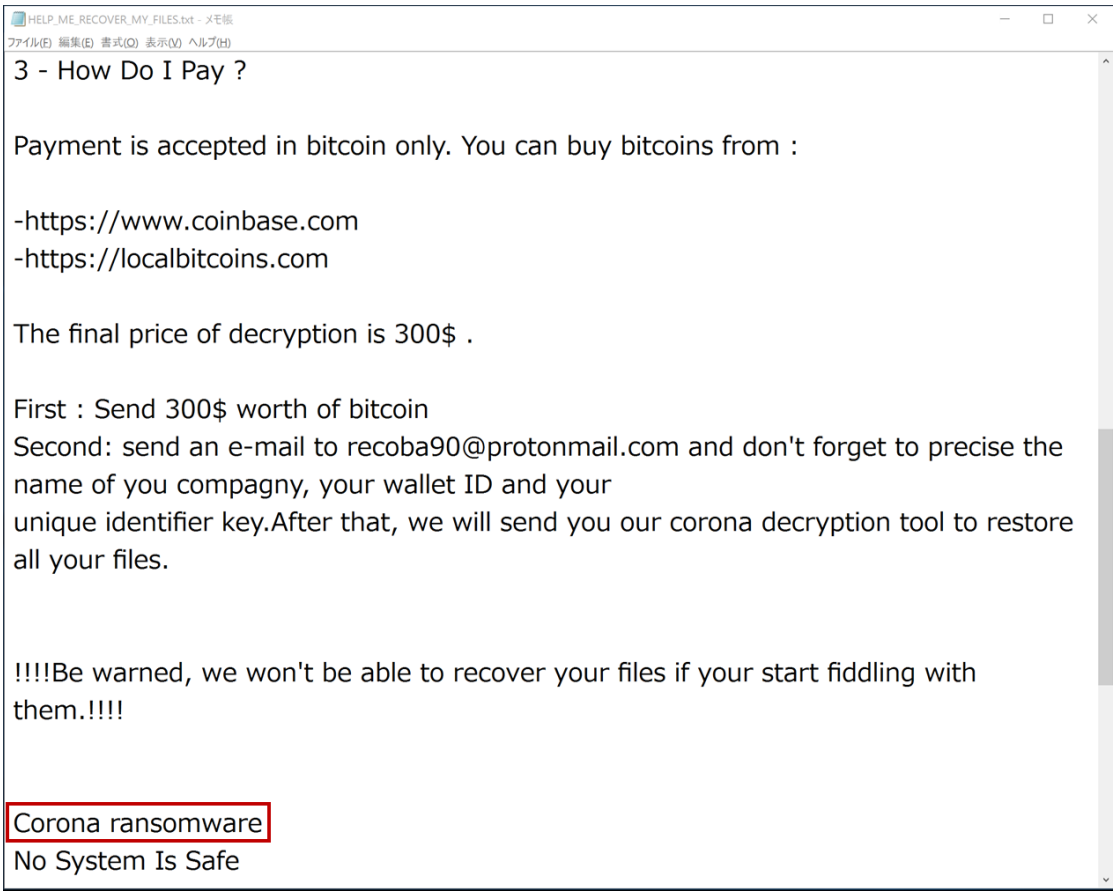


**Web ブラウザーから窃取された認証情報（上）とクレジットカード情報（下）**

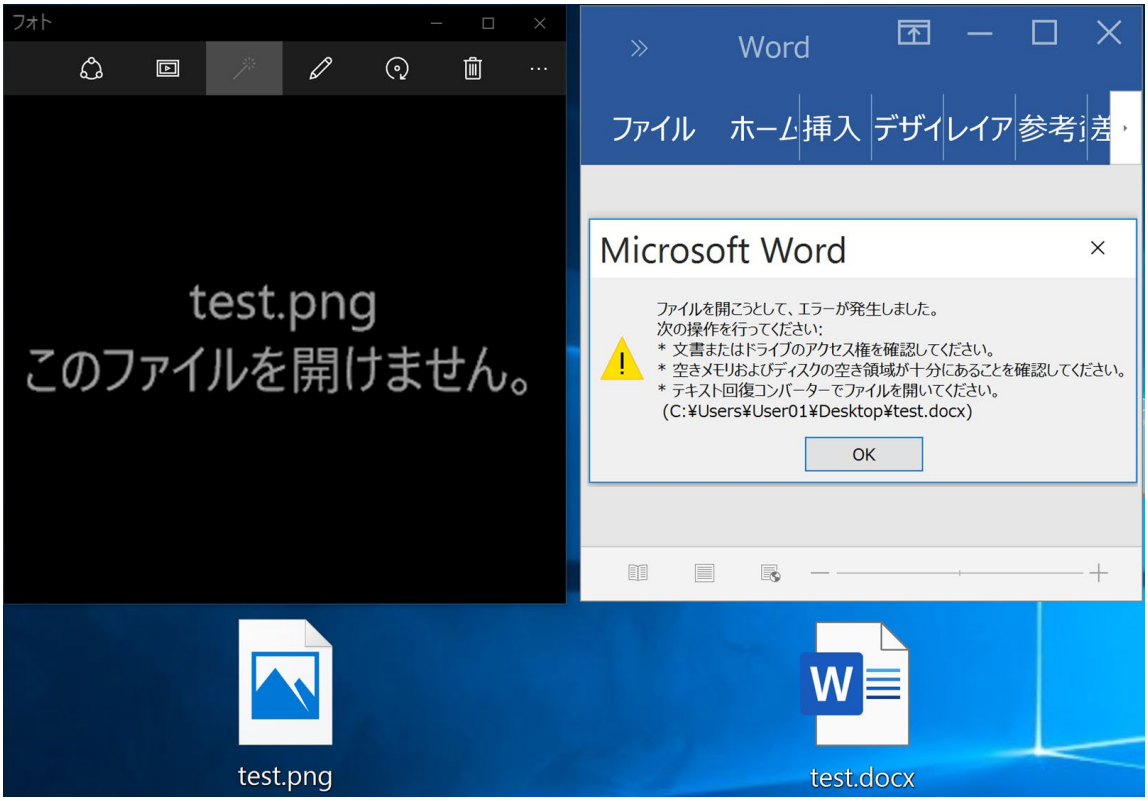
窃取された情報を基に、不正アクセスやクレジットカードの不正利用など、様々な被害に遭うことが想定されます。

新型コロナウイルス感染症に関連する名称のマルウェアには、そのほかに「Corona ransomware」があります。本マルウェアは、ランサムウェアです。本ランサムウェアの名称は、ファイル暗号化後に表示される脅迫文に"Corona ransomware"の文字列がある（下図の赤枠部分）ことに由来します。




**Corona ransomware の脅迫文**

暗号化されたファイルは、ファイル名や拡張子は変更されませんが、破損し内容を確認することはできなくなります。また、本ランサムウェアは壁紙も変更しません。3 月 19 日現在、復旧方法は確認されていません。




**Corona ransomware によって暗号化された画像・文書ファイル**

■まとめ

新型コロナウイルス感染症の流行に便乗したサイバー攻撃が、世界各地で多数確認されました。今回紹介したものは一例であり、そのほかにもチェーンメール、スミッシングなど様々な事例が確認されています。

新型コロナウイルス感染症の流行など情勢が大きく変化する際、攻撃者は様々な手法を用いて人々の不安を煽ります。しかし、不審なメールを開かない、不審なファイルを実行しない、といった基礎的な対策が身についていれば、被害を防げるものが大半です。加えて、最新の攻撃事例を収集したり、セキュリティ製品を導入したりすると、より効果的です。

ご紹介したように、1 月と 2 月は Web ブラウザー上で実行される脅威に加えて、メールを介して拡散されるマルウェアの脅威が多く検出されています。また、新型コロナウイルス感染症の流行に便乗するサイバー攻撃が多発しています。

■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 製品の検出エンジン（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、検出エンジン（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**
マルウェアの多くは、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**
マルウェアの多くが狙う「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**
万が一マルウェアに感染した場合、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」の方がマルウェアに感染するリスクは低いと考えられます。マルウェア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。

［引用・出典元］


- 「Emotet」と呼ばれるウイルスへの感染を狙うメールについて｜IPA
  https://www.ipa.go.jp/security/announce/20191202.html#L12

- 2019 年 年間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/trend/detail/200305.html

- 【緊急セミナー】いまさら聞けない！？Emotet の脅威と対策について｜キヤノンオンラインセミナー[動画]
  https://onlineseminar-mj.adobeconnect.com/p9rje2oooh3x/

- COVID-19 Interactive Map｜ジョンズ・ホプキンズ大学 Coronavirus Resource Center[英語]
  https://coronavirus.jhu.edu/map.html

Canon

キヤノンマーケティングジャパン株式会社