2019年
9月
SEPTEMBER

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

## 犯罪に悪用されるダークウェブ

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

「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

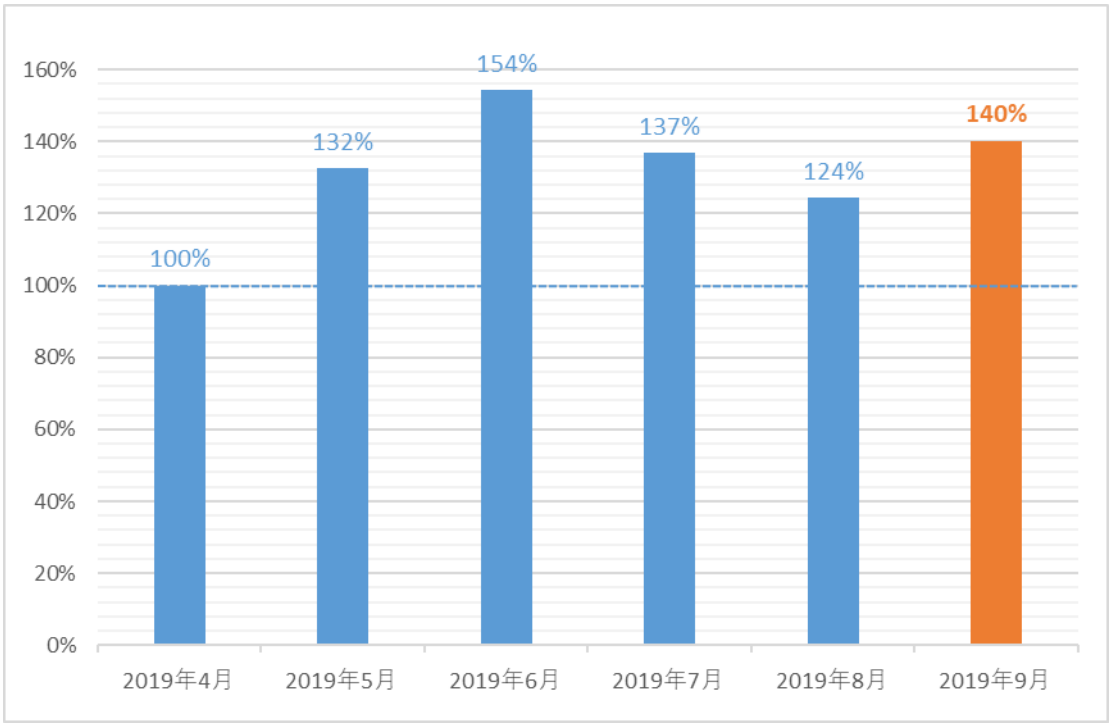
国内のマルウェア検出状況についてまとめたレポートです。

# ショートレポート「2019 年 9 月マルウェア検出状況」

1. 9 月の概況
2. 犯罪に悪用されるダークウェブ

## 1. 9 月の概況について

2019 年 9 月（9 月 1 日～9 月 30 日）に ESET 製品が国内で検出したマルウェアの検出数は、以下のとおりです。




**国内マルウェア検出数*1 の推移**

**（2019 年 4 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。

2019 年 9 月の国内マルウェア検出数は、減少傾向にあった 7 月・8 月と異なり、増加しました。直近 6 か月の中で、最も検出数の多かった 6 月に次いで、高い水準ということがわかります。
検出されたマルウェアの内訳は以下のとおりです。

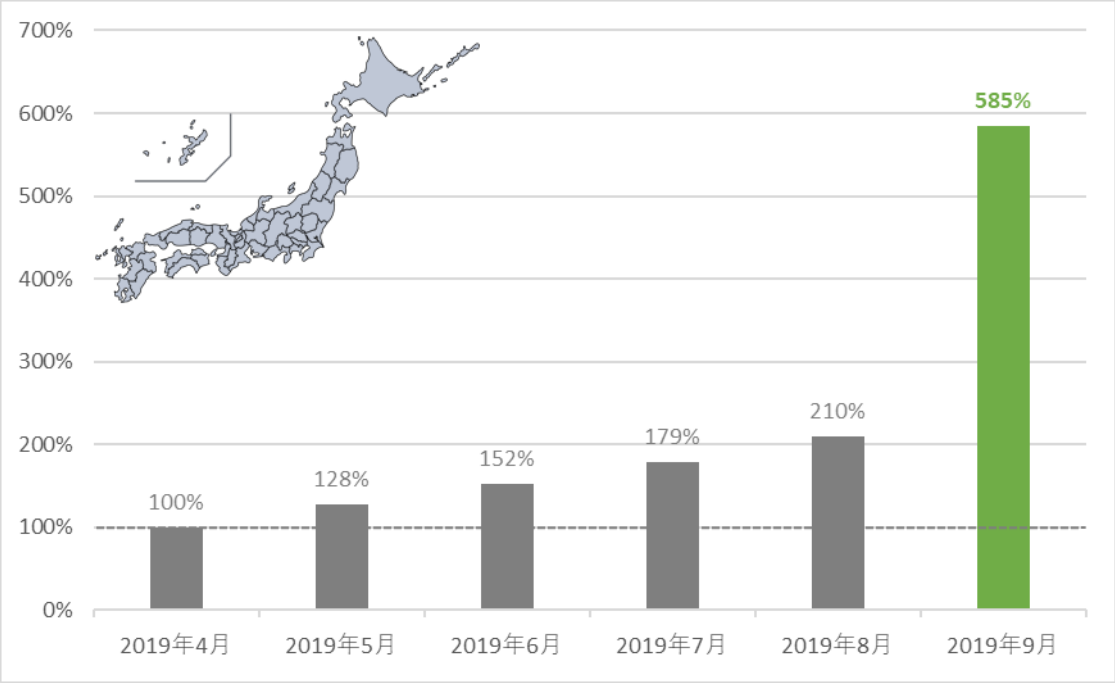
**国内マルウェア検出数*2 上位（2019 年 9 月）**

| 順位 | マルウェア名 | 割合 | 種別 |
|---|---|---|---|
| 1 | HTML/ScrInject | 21.1% | HTML に埋め込まれた不正スクリプト |
| 2 | JS/Adware.Agent | 9.9% | アドウェア |
| 3 | JS/Adware.Subprop | 8.9% | アドウェア |
| 4 | HTML/FakeAlert | 3.2% | 偽の警告文を表示するスクリプト |
| 5 | HTML/Refresh | 1.8% | 別のページに遷移させるスクリプト |
| 6 | Win32/Exploit.CVE-2017-11882 | 1.2% | 脆弱性を悪用するマルウェア |
| 7 | JS/Redirector | 1.1% | リダイレクター |
| 8 | Win32/Injector.Autoit | 1.0% | 他のプロセスにインジェクションするマルウェア |
| 9 | HTML/IFrame | 1.0% | リダイレクター |
| 10 | Win32/GenKryptik | 0.9% | 暗号化/難読化された実行ファイル |

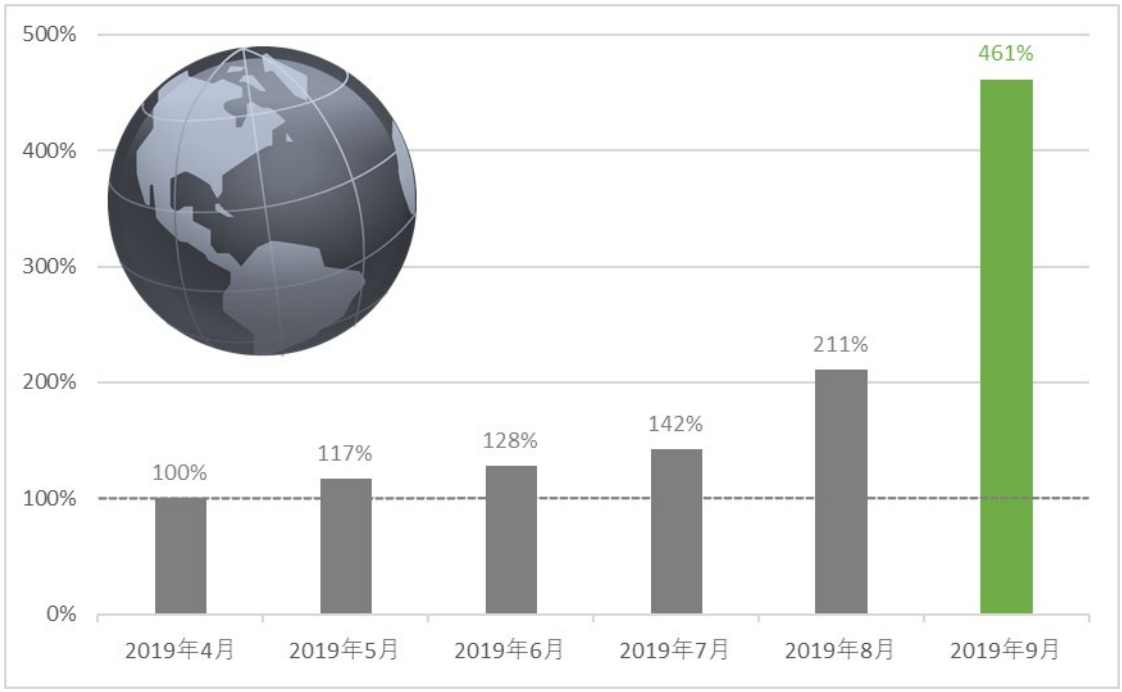
*2 本表には PUA を含めていません。

9 月に国内で最も多く検出されたマルウェアは、HTML/ScrInject でした。HTML/ScrInject は HTML に埋め込まれた不正スクリプトで、Web サイト閲覧時に実行されます。不正なスクリプトが実行されると、不正な Web サイトへのリダイレクト、マルウェアのダウンロード、不正広告の表示、Web 閲覧情報の窃取など様々な被害に遭う可能性があります。

国内で検出された本マルウェアの数は、2019 年 4 月以降、常に増加しています。また、8 月から 9 月にかけては、検出数が特に大きく増加しました。この傾向は、世界全体でも確認されています。




**国内で検出された HTML/ScrInject 検出数の推移**
**(2019 年 4 月の国内検出数を 100%として比較)**




**世界全体で検出された HTML/ScrInject 検出数の推移**
**(2019 年 4 月の世界検出数を 100%として比較)**

国内で 2 番目に多く検出されたマルウェアは、Web サイト閲覧時に実行されるアドウェアの JS/Adware.Agent でした。JS/Adware.Agent は、6 月～8 月まで連続して最も多く検出されていましたが、9 月は 2 位に後退しました。

## 2. 犯罪に悪用されるダークウェブ

**●はじめに**

最近、ニュースなどで「ダークウェブ」という言葉をよく耳にするようになりました。
「ダークウェブ」とは、匿名性の高い特別なネットワーク上に構築された Web サイトで、昨年発生した仮想通貨 NEM（ネム）の流出事件において、犯人が盗み取った仮想通貨をダークウェブ上で販売したことでも話題になりました。
現在、この「ダークウェブ」では、犯罪を行う上で必要な情報やサービスを売買できるエコシステムが構築され、サイバー犯罪が増加する要因の 1 つになっています。

**●ダークウェブとは**

日頃、私たちが閲覧している Web サイトは、主に 3 つの種類に分けることができます。
1 つ目は、「サーフェスウェブ（表層ウェブ）」と呼ばれる Web サイトです。
「サーフェスウェブ」は、Google などの検索エンジンで検索ができ、誰でも閲覧することが可能です。具体的には、私たちが日頃アクセスしている無料のニュースサイトや企業のホームページなどになります。

2 つ目は、「ディープウェブ」と呼ばれる Web サイトです。
「ディープウェブ」は、一般に公開されておらず、特定のメンバーだけに公開されている Web サイトです。具体的には、有料の Web サイトや特定のメンバーのみが閲覧ができるよう設定されているフォーラムなどです。
「ディープウェブ」は、Google などの検索エンジンによってインデックス化されないため、検索しても検索結果に表示されません。別名、「深層ウェブ」などとも呼ばれます。

3 つ目は、「ダークウェブ」です。
「ダークウェブ」は、匿名性の高い特別なネットワーク上に構築された Web サイトで、Google など日頃私たちが利用している検索エンジンでは検索することができません。
また、通常、Internet Explorer や Google Chrome、Firefox と言った Web ブラウザーでは閲覧することができず、専用の Web ブラウザーを利用して閲覧する必要があります。
この「ダークウェブ」は、Tor（The Onion Router）や I2P（The Invisible Internet Project）といった匿名化されたネットワーク上に存在するため、Web サイトへのアクセス元などを特定することが難しいのが特徴です。

| 名称 | 概要 |
| --- | --- |
| サーフェスウェブ | ● 誰でもアクセスが可能<br>● 通常（Googleなど）の検索エンジンで検索できる |
| ディープウェブ | ● 特定の人物のみアクセスが可能（認証などが必要）<br>● 通常（Googleなど）の検索エンジンで検索できない |
| ダークウェブ | ● 匿名性の高い接続方式を使用する必要がある<br>● 専用のブラウザ（Torブラウザなど）を必要とする<br>● 通常（Googleなど）の検索エンジンで検索できない |

**サーフェスウェブ、ディープウェブ、ダークウェブの違い**

**●ダークウェブを支える匿名化技術**

「ダークウェブ」を閲覧するには、Tor や I2P といった専用のソフトウェアや通信方式を利用する必要があります。この Tor や I2P では、「Onion Routing（オニオン・ルーティング）」という技術を利用することで高い匿名性を実現しています。

「Onion Routing」の技術は、元々アメリカ海軍の調査研究所 NRL（United States Naval Research Laboratory）によって、捜査や諜報活動で得た情報などを秘匿する目的で開発されました。この「Onion Routing」は、通信を行う際に、複数のノードを経由し、データを多重に暗号化します。そのため、第三者から送信元などを特定することが難しく、匿名性が高いことが特徴です。この技術は、その後、オープンソースとして公開され、Tor や I2P といった匿名性の高いネットワークやソフトウェアで利用されるようになりました。

**●ダークウェブで売買されている情報やサービス**

「ダークウェブ」は、匿名性が高いことから、プライバシーや通信を守る意味で非常に有用な仕組みと言えます。しかし、現在、一部の犯罪者たちにより犯罪に必要な情報やサービスを売買する市場としても利用されています。

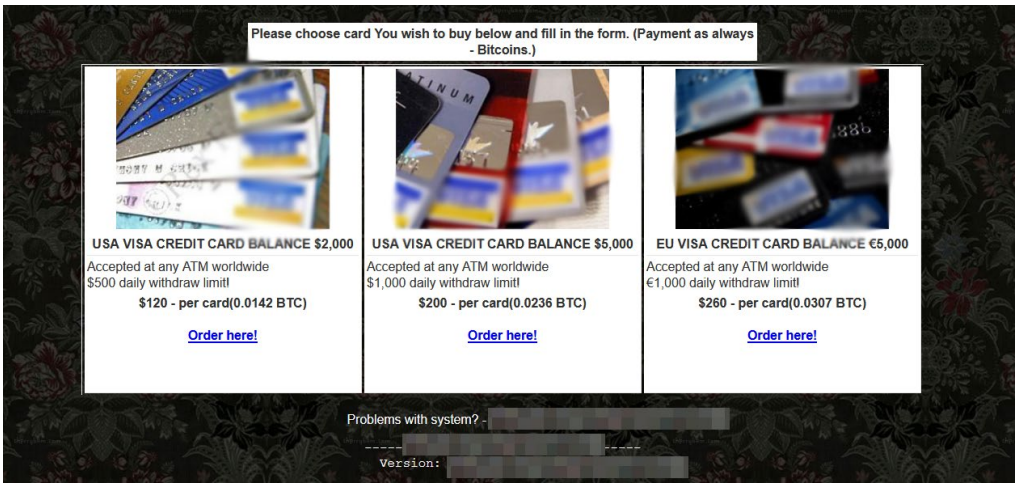
**クレジットカード情報の売買**

以下の Web サイトは、フィッシング攻撃やマルウェア、盗難などで盗み出されたクレジットカード情報を販売しているダークウェブ上のサイトです。

通常、フィッシング攻撃やマルウェア、盗難などで盗み出されたクレジットカード情報は、盗み出した本人自らが直接使用することは少なく、第三者に転売され、ダークウェブで販売されるケースが多いと言われています。なぜなら、盗み出した情報を自身が使用するより、他の犯罪者に転売する方が安全かつ確実に収益を得ることができるからです。

この Web サイトで販売されているクレジットカード情報の金額は、約 13,000 円～28,000 円（1 ドル 110

円換算）で、クレジットカードに登録されている国や利用残高によって販売額が異なります。

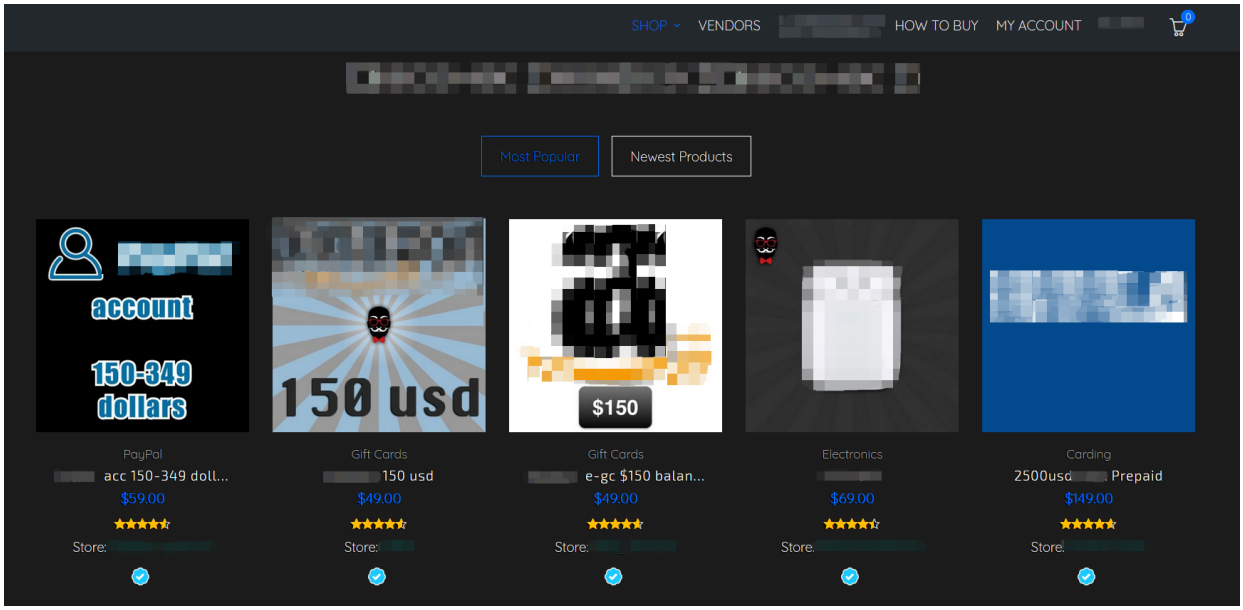



**ダークウェブ上のクレジットカード情報販売サイト**

また、クレジットカード情報を購入する場合は、購入に必要な情報を入力した後、仮想通貨を使って費用を支払うことで、クレジットカード情報を購入できると説明されています。


**クレジットカード情報の購入画面**

この他にもダークウェブ上では、オンライン決済サービスのアカウント情報をはじめ、SNS などのアカウント、ギフトカードなども販売されており、仮想通貨を利用して購入することが可能です。これらのクレジットカード情報やアカウント情報、ギフトカードなどは、不正な手段で盗み出された可能性が高く、興味本位で購入すると罪に問われたり、犯罪に巻き込まれたりする可能性があります。そのためむやみにアクセスしないことをお勧めします。




**SNS アカウントやギフトカードの販売画面**

### 個人情報や偽造した証明書の売買

ダークウェブでは、クレジットカード情報など金銭に直接関連した情報以外にもパスポートや運転免許証などの個人情報や証明書も売買されています。

たとえば、以下のサイトは、偽造したパスポートや運転免許証を販売している Web サイトの画面です。

Ordering form

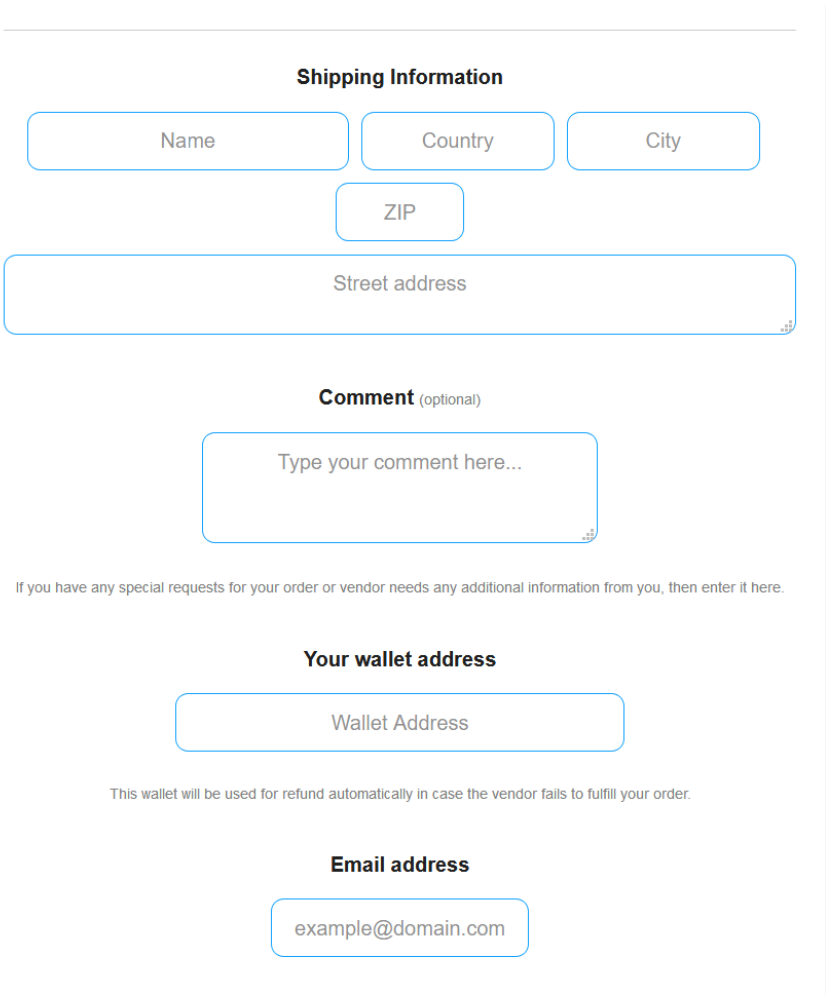
| | | | |
|---|---|---|---|
| UK Passport | 2299$ | 0.2851 BTC 43.38 LTC 13.524 ETH | Quantity: |
| UK Driver's License | 599$ | 0.0743 BTC 11.3 LTC 3.524 ETH | Quantity: |
| UK New Identity Pack (Passport+Driver's License+free SIM card) | 2599$ | 0.3223 BTC 49.04 LTC 15.288 ETH | Quantity: |
| USA Passport | 1799$ | 0.2231 BTC 33.94 LTC 10.582 ETH | Quantity: |
| USA Driver's License | 399$ | 0.0495 BTC 7.53 LTC 2.347 ETH | Quantity: |
| USA New Identity Pack (Passport+Driver's License+free SIM card) | 1999$ | 0.2479 BTC 37.72 LTC 11.759 ETH | Quantity: |
| Australian Passport | 1799$ | 0.2231 BTC 33.94 LTC 10.582 ETH | Quantity: |
| Australian Driver's License | 399$ | 0.0495 BTC 7.53 LTC 2.347 ETH | Quantity: |
| Australian New Identity Pack (Passport+Driver's License+free SIM card) | 1999$ | 0.2479 BTC 37.72 LTC 11.759 ETH | Quantity: |
| New Zealand Passport | 1799$ | 0.2231 BTC 33.94 LTC 10.582 ETH | Quantity: |
| New Zealand Driver's License | 399$ | 0.0495 BTC 7.53 LTC 2.347 ETH | Quantity: |
| New Zealand New Identity Pack (Passport+Driver's License+free SIM card) | 1999$ | 0.2479 BTC 37.72 LTC 11.759 ETH | Quantity: |
| Canadian Passport | 1899$ | 0.2355 BTC 35.83 LTC 11.171 ETH | Quantity: |
| Canadian ID | 699$ | 0.0867 BTC 13.19 LTC 4.112 ETH | Quantity: |

**偽造したパスポートや運転免許書を販売している Web サイトの画面**

この Web サイトでは、イギリスやアメリカ、カナダ、オーストラリア、ニュージーランドの偽造パスポートや運転免許証が販売されています。

この Web サイトでは、偽造したパスポートを約 20 万円（1 ドル 110 円換算）から購入することできます。価格は、偽造するパスポートの国などにより、異なる値段が設定されているのが一般的です。

偽造パスポートや運転免許証を購入する場合、クレジットカード情報を購入する場合と同様に Web サイトの画面から偽造パスポートの作成に必要な情報を入力し、仮想通貨を使って費用を支払う必要があります。



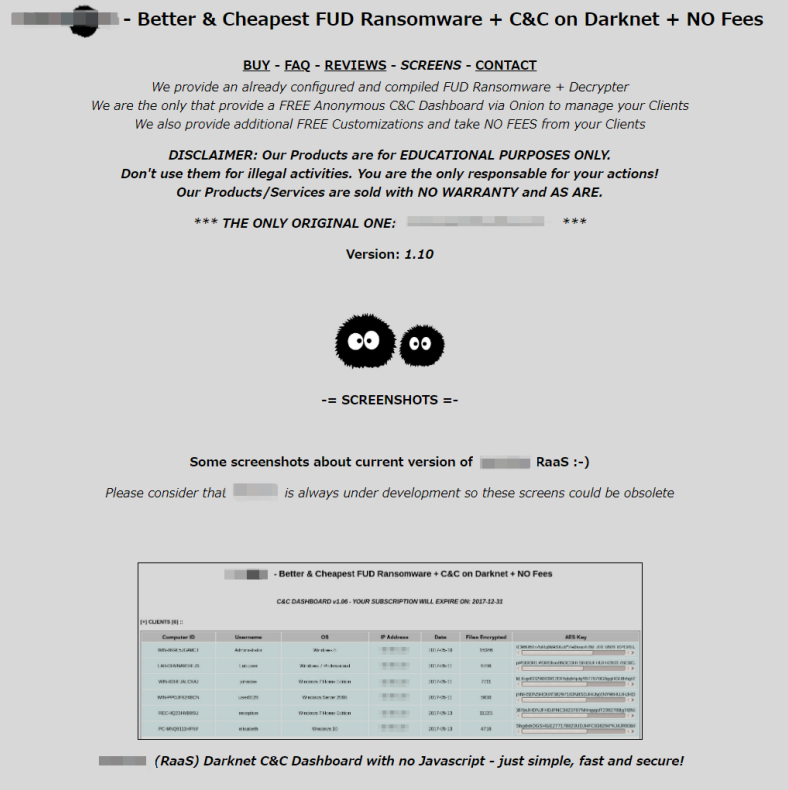

**偽造パスポートの購入に必要な情報の入力画面（一部）**

ダークウェブで販売されているパスポートには、この他にも電子化されたパスポート情報や盗難などで不正に入手したと推測される正規のパスポートなども存在します。特に正規のパスポートにおいては、非常に高額で取引されています。

**サイバー攻撃を行うための各種サービス**

ダークウェブでは、サイバー攻撃を行うための各種サービスやツールも販売されています。

具体的には、以前のマルウェアレポートでも取り上げた「ランサムウェアを提供するサービス（Ransomware as a Service）」や「マルウェアを販売するサービス（Malware as a Service）」、「簡単にフィッシングサイトを作成できるサービス（Phishing as a Service）」「サイバー攻撃を請け負うハッキングサービス」などが存在します。




**ランサムウェアを提供するサービス（Ransomware as a Service）**

技術力が高くないサイバー犯罪者でも上記のようなサービスの中から自身の目的に合ったサービスを購入し、サイバー攻撃に利用することができます。そのため、プログラミングなど特別な技術を必要とせず、比較的簡単に利用できることから犯罪者にとって、とても魅力的なサービスと言えます。一方で、これらの Web サイトの中には、マルウェアなどが仕掛けられている場合も多く、アクセスすることでマルウェア感染や遠隔操作などのサイバー攻撃を受ける可能性もあります。そのため、一般の人がアクセスするには、非常に危険です。

この他にも、ダークウェブでは、違法薬物や武器、児童ポルノ、偽造通貨、違法なホスティングサービスなど、違法

に入手した情報や違法なサービス、商品が売買されており、犯罪を行う上で必要な情報やサービス・商品が入手できる市場が形成されています。

**●まとめ**

今回、ご紹介したようにダークウェブ上では、サイバー犯罪者などにより、犯罪を行う上で必要な情報やサービスを売買できる市場が構築されています。そのため、一定の知識とお金さえあれば、犯罪に必要な情報やツールなどを比較的簡単に入手することができます。

しかし、当然ながら正当な理由なしにマルウェアを作成・保管する行為やアカウント情報を盗み出し使用する行為、違法な薬物などを購入・使用する行為などは犯罪です。興味本位でこのようなサービスや情報・商品を購入しないようご注意ください。

インターネットが私たちの生活を便利にしている一方で、私たちの大切な個人情報がダークネット上で売買されたり、意図せず犯罪に巻き込まれたりするリスクが増加しています。そのため、日頃からセキュリティについて意識し、定期的にサイバー攻撃から身を守るために必要な対策を見直していく必要があります。

ご紹介したように、9 月は HTML/ScrInject と呼ばれるマルウェアの検出数が日本だけではなく世界全体で急増しました。また、犯罪行為に使用されるダークウェブを紹介しました。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**
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。

［引用・出典元］

- 2018 年 5 月マルウェアレポート「3.ランサムウェアを販売する Ransomware as a Service（RaaS）」
  https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1805.html
- 2018 年上半期マルウェアレポート
  https://eset-info.canon-its.jp/malware_info/trend/detail/180824.html
- 2019 年上半期マルウェアレポート
  https://eset-info.canon-its.jp/malware_info/trend/detail/190920.html
- マルウェア情報局「次世代ダークマーケットは犯罪者にとっての Amazon や eBay 的な存在」
  https://eset-info.canon-its.jp/malware_info/trend/detail/190214.html

Canon

キヤノンマーケティングジャパン株式会社