WEBROOT®
an opentext™ company

CARBONITE®
an opentext™ company

WEBROOT

# THREAT REPORT

# 目次

# はじめに

ハル・ロナス、シニアバイスプレシデント兼最高技術責任者 (中小企業および消費者部門、OpenText)

新たな 10 年間を迎えるにあたり、重要な変化のどれだけ多くがごく最近起きたものであるかを考えると驚かざるを得ません。考えてみてください。私たちが生きているスマートフォン時代が始まって 10 年余りです。そのさらに先を振り返ると、1960 年代に単なる概念だった「クラウド」は、2000 年代初頭に流行語となり、パブリッククラウド、プライベートクラウド、ハイブリッドクラウドが至るところにある今日の戦略的コンピューティングのユビキタス状態へ到達しました。特に、ユーザーの期待は世界中でビジネスの運営方法に課題を投げかけます。ダイヤルアップの日々を覚えている私たち世代。画像のダウンロードは無論、接続にかかった時間を思い出してください。今日は、我々一人ひとりが、クラウド、モバイル、ソーシャルおよび人工知能を介して、パーソナライズされた関連性のある即時の体験を迅速かつ遅れなく受け取ることを期待しています。

唯一変わっていないのは、データを盗み、システムを侵害し、利益を生み出すハッカーの容赦なさです。彼らの戦術の多くは変わってません。フィッシングはとうの昔から存在しており、未だにマルウェアを投下し機密情報への不正アクセスを得るための主要なツールです。一方、他の戦術は大幅に進化しました。10 年前には、ランサムウェアについて聞いたことはありませんでした。クラウドコンピューティングがセキュリティへに及ぼす影響については大きな疑問符がついていましたし、ソーシャルエンジニアリングの戦術を使用していたのは攻撃の 28% にすぎませんでした。[1] 特にここ数年は、脅威の状況に著しい影響を及ぼしています。たとえば、悪意のある IP アドレス、無警戒なユーザーを危険なサイトに誘導する URL 、無意識または同意なしにユーザーの暗号通貨をマイニングするクリプトジャッキング、そのバリエーションのランサムウェア、ますます悪質でステルス技術を高めたマルウェアなど、これらすべてが企業や個人を問わず新たな危険となっています。

今年の Webroot® 脅威レポートでは、これらのカテゴリや他のカテゴリで検知されたもの関する分析に加え、対象となった業界や一般的なマルウェアの存在箇所について詳述します。当社は Web トラフィックの善と悪に関する大量の分析と、充分な情報に基づく過去 10 年間の出来事についての理解を用い、2020 年がもたらす可能性を予測します。急速に変化する世界でこれらのトレンドを理解するお役にたてれば幸いです。

> 今日は、我々一人ひとりが、
> クラウド、モバイル、ソーシャル
> および人工知能を介して、
> パーソナライズされた
> 関連性のある即時の体験を
> 迅速かつ遅れなく
> 受け取ることを期待しています。

# ウェブルートの観点

本稿、2020 年 Webroot 脅威レポート中の統計、トレンドおよび洞察は、当社の高度な機械学習ベースのアーキテクチャである Webroot® プラットフォームによって継続的かつ自動的に取得された大量のデータに基づいています。このデータは、数百万の実世界のエンドポイントとセンサー、専門の第三者のデータベース、および当社のテクノロジーパートナーによって保護されたエンドユーザーから取得され、その後、当社の高度な機械学習エンジンと脅威調査チームによって継続的に分析および解釈されます。本稿の回顧、トレンドおよび予測は、次のような幅広い脅威活動を対象としています。

- マルウェアのトレンド: 感染対象、感染箇所、地理的および業界分析
- URL 分類とセキュリティの傾向 (クリプトジャッキングを含む)
- フィッシング攻撃とその標的
- 悪意のある IP アドレスとそれがセキュリティに及ぼす影響
- ランサムウェアの継続的な被害
- モバイルアプリの脅威とその進化例

前述の脅威のそれぞれが複数の業界、地域、およびユーザーグループ全体にわたり広範囲に影響を及ぼします。これらのすべてを数値で分類し、さらにエンドユーザーの認識とトレーニングを効果的に使用することで、侵害のリスクを軽減できることも示します。最後に、予測セクションでは、当社の包括的でグローバルな観点から向こう 1 年間に予測される事象についてみていきます。

# WEBROOT BRIGHTCLOUD® 脅威インテリジェンス

**9,500 万以上の** 実世界のセンサー

テクノロジーパートナーを通じて保護された
**7,800 万人以上の**エンドユーザー


**8 億 4,200 万以上の** ドメイン


**370 億以上の** URL

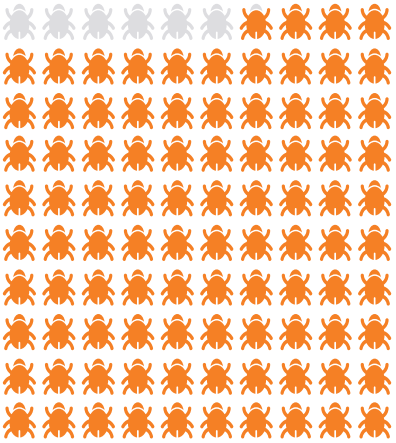

**40 億以上の** IP アドレス

**360 億以上の** ファイル動作記録

**3,100 万以上の** 有効なモバイルアプリ

# マルウェア

過去 10 年間にかけて、マルウェアの作者と攻撃者は適応性が非常に高く、対象をきわめて絞り込んでいることが判りました。単一のマシンで検出された悪意のあるファイルの急激な増加を調べるだけで、作成者が亜種戦略を介して従来のサイバー防御を回避する方法を学習したことがわかります。



*2019 年に **検知されたマルウェアの 93.6% は 単一の PC 上のみで発見されました。**その数は 2014 年以降 90% を超えて推移しているものの、これは当社の見た中で最高これは当社の見た中で最高の数値です。*

マルウェアは国家のお気に入りのツールになりました。彼らは、高度に進化したゼロデイ エクスプロイトを採用 (場合によってはコントロールを失い)、ビジネス、政府、および組織全体に大混乱をもたらします。「EternalBlue」エクスプロイトで目の当たりにしたように。[2] それに加えて、クラウドの影響、至るところにある携帯電話から、過去10年間にどれ位マルウェアが進化したかを簡単に確認できます。

確実に言えることが一つあります。Windows® マルウェアは消滅していないということです。Webroot で保護された Windows エンドポイントでは、毎日 160 万以上の新たなマルウェアとWindowsアプリケーションが検出されています。この数は、前年実績である 1 日あたり約 136.9 万件から増加し続けています。2018 年には最大 5 億、2019 年に 6 億近かったことになります。言い換えると、大量の、増大する、絶え間ないファイルデータの流れが見られます。

**個人のデバイス対企業向けデバイス**

感染を報告するエンドポイントのうち、 62% が個人 (ホームユーザー) のデバイス、38% が企業のデバイスでした。この差は、企業がより多くのセキュリティ層を備えていること、さらに従業員にセキュリティ意識向上トレーニングを提供する企業が増えているためであると思われます。総じて、デバイスあたりのマルウェアファイルの数は、個人の PC では年々減少していますが、企業の PC では昨年実績とほぼ変わっていません。

個人向けのデバイスは、これまで同様、企業のデバイスよりもはるかに頻繁に感染しています。このため、従業員個人のデバイスを企業ネットワークに接続することを認めるにあたり、企業が直面するリスクを強調することが重要です。マルウェアの普及率が上昇し、概してセキュリティ防御の整備が比較的少ないため、マルウェアが従業員の個人用デバイスを介して企業ネットワークに侵入しやすくなっています。

*個人向けデバイスは依然として企業のシステムよりも感染する可能性が 2 倍近く高いです。*

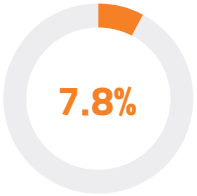
特に興味深いのは、PC が再感染する頻度です。

2019 年、個人向け PC の 12.6% が感染しました。これらの内訳:

- 1 回の感染で済んだケース 46.3%
- 2 - 5 回再感染したケース 35.8%
- 6 - 10 回再感染したケース 8.6%
- 10 回以上感染したケースが 9.2% でした。

対照的に、企業向け PC で 1 回感染したのは僅か 7.8%。


感染した個人向け PC




感染した企業向け PC

これらの内訳:

- 1 回の感染で済んだケース 50.4%
- 2 - 5 回感染したケース 33.2%
- 6 - 10 回感染したケース 7.9%
- 10 回以上感染したケース 8.5% でした。

システムが複数回感染する理由はいくつか考えられます。複数のポリモーフィックファイルが単一の PC を攻撃した結果、または単一のマルウェアが複数のファイルを投下した結果です。さらに、マシンに Webroot 保護が最初にインストールされた時点で、複数の感染が見つかっている場合も考えられます。とにかく、ここで言えるのは、管理者と個人が同様に警戒しなければならないということです。

### OS が重要な理由

過去 2 年間に見られたように、Windows®10 (概して安全性が向上した OS ) への移行は、データ内でマルウェアが減少した理由の一つと考えられます。総じて、Windows®7 を実行しているシステムが感染する可能性は、Win10 デバイスの約 3 倍です。各オペレーティングシステムでは、エンドポイントごとに平均 0.11 回と 0.04 回の感染が見られます。

*マルウェアターゲティング*
*Windows 7 は 125% 増加しました。*

概して、Win10 の感染は比較的少ないと言えます。個人向け PC ではデバイスあたり 0.06 回、企業向け PC ではデバイスあたり 0.02 回です。Win7 の問題の規模は、その OS を実行している個人向け PC と企業向け PC の数次第です。2019 年には、個人向け PC の 82% が Win10 を実行していたのに対し、Win7 は僅か 10% でした。一方、企業向け PC では Win10 が 63%、Win7 が 25% 以上でした。Microsoft が Win7 のサポートを終了したため、この割合は減少すると見込まれます。

エンドポイントごとの感染率を見ると、個人と企業の世界の相違が明白です。個人のシステムごとの感染は総じて徐々に減少しています (2017 年の 0.11 から 2018 年に 0.10、2019 年には 0.08) が、総計した数値からは重要な事実が見えていません。Win7 の感染率は、デバイスごとに 0.17 から 0.20 に増加したのです。Win7 エンドポイントの数は減少すると予想しているものの、Win7 をターゲットとして特定したマルウェアの量は同じ理由で増加する可能性があります。Microsoft が Win7 のサポートを終了するのならば、同 OS の脆弱性にパッチを当てることはないでしょう。

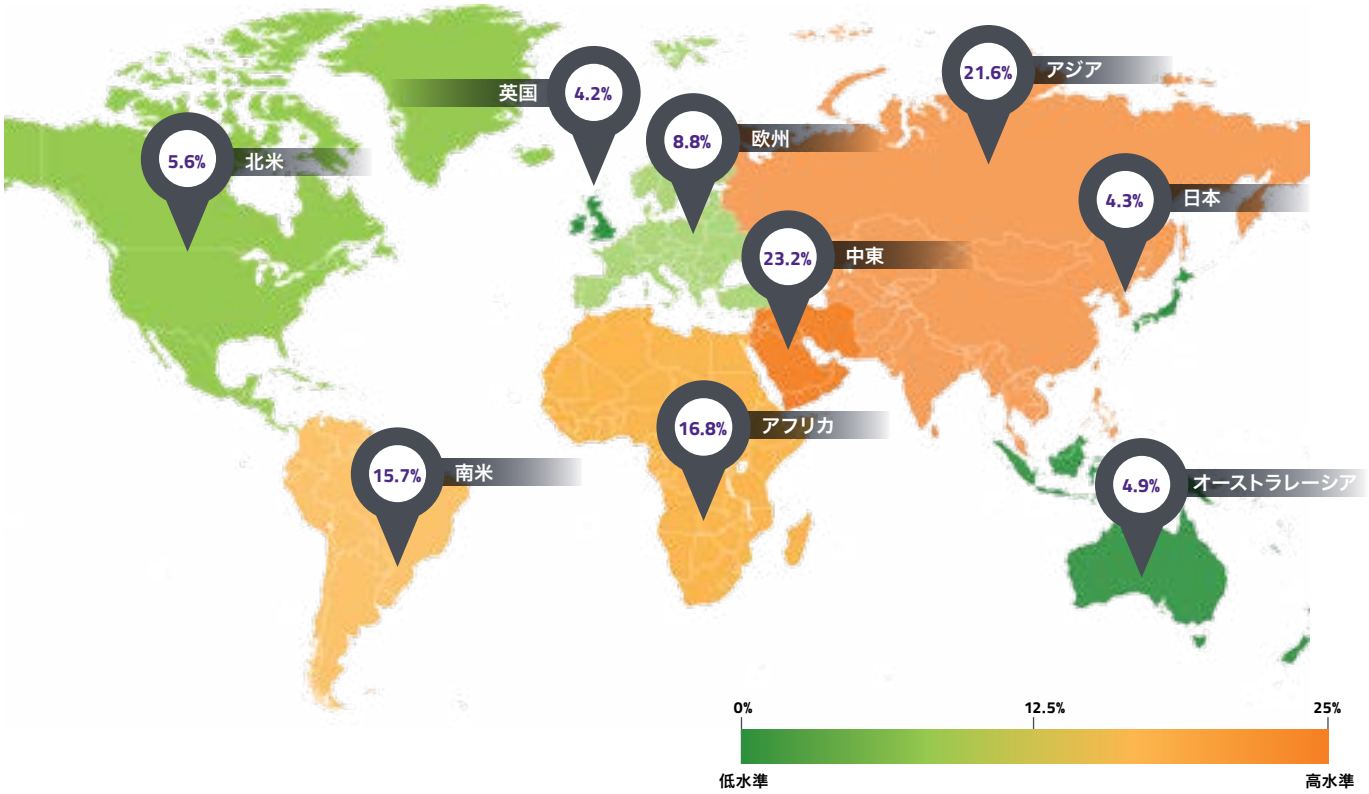
マルウェアファイルの年間合計が僅かに減少したのは、いくつかの要因によると考えられます。

- **セキュリティ意識向上トレーニング**
  ユーザーが防衛の最前線であるため、セキュリティ認識トレーニングの重要性がますます高まっています。ガートナーは、エンドユーザーに焦点を当てたセキュリティ教育とトレーニングは急速に成長している市場であり、「2022 年までに、大企業/企業の 60% が包括的なセキュリティ意識トレーニングプログラムを設ける」と予測しています。[3]

- **技術的有効性**
  当社が提示するデータは、Webroot で保護されたエンドポイントから収集したものです。階層化されたマルチベクトルアプローチは、キルチェーンの早期の段階でアクティビティを検出してブロックします。たとえば、悪意のある URL を介してエンドポイントを攻撃する実行可能ファイルをブロックするか、".exe " が追加のマルウェアファイルをダウンロードするのを防ぐことにより、保護されたエンドポイントでマルウェアが実行されるインシデントを減らすことができます。

- **サイバー犯罪活動における変化**
  一部のサイバー犯罪者は、フィッシングやクリプトジャッキングなど、リモートシステムからマルウェアよりも簡単に利益を生み出す攻撃方法に再び焦点を合わせています。さらに、犯罪者はより標的を絞ったマルウェアビジネスモデルに移行しています。このビジネスモデルでは、攻撃の開始とマルウェアの展開が少なくなる一方で成功率は高くなります。

- **オペレーティングシステムのセキュリティの向上**
  Windows 10 の大規模な採用 (ウイルス対策が常にオンになっている) およびセキュリティコミュニティとセキュリティ業界全体の努力も要因となっています。




図表 1a: 地域別の感染デバイス

| | 感染した個人向けデバイス | 感染した企業向けデバイス |
|---|---|---|
| アフリカ | 20.3% | 15.7% |
| アジア | 27.9% | 16.6% |
| オーストラレーシア | 11.6% | 4.6% |
| 欧州 | 21.5% | 7.3% |
| 日本 | 4.6% | 4.1% |
| 中東 | 26.9% | 16.6% |
| 北米 | 6.9% | 3.9% |
| 南米 | 17.9% | 10.5% |
| 英国 | 9.6% | 3.7% |

0% 14% 28%

図表 1b: 地域別の感染した個人向けおよびビジネス向けデバイス

| | Win7 を実行しているデバイス | Win10 を実行しているデバイス |
|---|---|---|
| アフリカ | 31.5% | 53.9% |
| アジア | 33.4% | 54.6% |
| オーストラレーシア | 24.8% | 62.0% |
| 欧州 | 26.9% | 59.2% |
| 日本 | 39.6% | 51.3% |
| 中東 | 35.3% | 50.1% |
| 北米 | 19.6% | 69.8% |
| 南米 | 22.5% | 63.1% |
| 英国 | 26.0% | 62.2% |

0% 35% 70%

図表 1c: 感染した Win7 および Win10 デバイスの地域別内訳

### 地域および産業別の感染

Windows デバイス上の感染率を地域別に追跡すると、違いが鮮明になります。一見したところ、感染した個人向けデバイスの割合は、企業向け PC よりも簡単にわかります。

さらに、感染率は地域によって大きく異なります。2019 年に感染したデバイスの約 4 分の 1 (23%) は中東のもので、僅差でアジアが次点、アフリカ、南アメリカがそれに続きました。対照的に、ヨーロッパ、北米、および日本の感染率ははるかに低水準でした。

感染率をよりよく理解するには、OS ごとに地域データを調べる必要があります。概して、Win7 はベースの 21% を、Win10 は 68% を占めます。しかし、感染率が非常に高い地域に目を向けると、感染率の高さを Win7 の普及と関連づけることができます。たとえば、南アメリカでは、PC の 22% 以上が Win7 を実行しています。アフリカでの割合は 31.5%、アジアでは 33.4% です。そして中東では、35.2% です。これらの地域はすべて、デバイスごとに高い感染率を示しており、Win7 PC が大量に存在する地域は、ますます多くの脅威にさらされています。ここでも、Win7 の脅威率が増加する一方、Win10 の脅威率は横ばいまたは減少しています。対照的に、北米では、PC のほぼ 70% が Win10 を実行しており、感染率は低いです。

これらの感染率にはさまざまな要因が関係している可能性があります。たとえば、経済的資源が比較的大きく、最新技術へのアクセスに優れ、サイバーセキュリティの懸念とリスクに対する認識の強い地域 (米国やヨーロッパなど) では、デバイスごとの感染数が少なくなる傾向があり、特に企業向けデバイスについてそれが言えます。最新のデバイスが比較的少ない地域、すなわち Win7 PC が多い地域では、脅威の数も比較的大きくなっています。

感染率について考えるもう 1 つの方法は、さまざまな業界の感染率を総合平均と比較することです。当社に業界を報告している Webroot のお客様のすべてが、2019 年にはデバイスあたりのマルウェアの割合が前年比で低下しました。しかし、他社よりも多くのマルウェアを経験しているターゲットは変化しています。たとえば、製造業、行政、天然資源/開発、運輸および倉庫管理では、デバイスごとのマルウェアについて平均以上の遭遇が報告されました。一方、金融と保険、医療と社会的支援、非営利団体、教育サービスなどの従来の攻撃対象では、マルウェアの割合が平均を下回っています。(これらの後者の業界は過去数年間サイバー犯罪者の照準を合わせており、その結果、多くの企業がセキュリティを改善するために大規模な投資を行ってきたため、その割合が改善するのは当然のことです。)

### マルウェアが隠れている場所

マルウェアはどこにでもありますが、マルウェアが隠れているシステムの箇所は、個人向け PC と企業向け PC とで異なります。例として %appdata% を見てみましょう。個人向け PC の場合、すべての感染の 26.5% がこのフォルダー内で発見されています。

対照的に、企業向け PC では %appdata% で検出されたマルウェアは 16.7% にすぎません。個人向けのシステムで appdata がよく使用される理由の 1 つは、ユーザーが Win8 以降でプログラムをインストールするのにローカル管理者のサービスを必要としないためです。個人向けデバイスの大半は単一のユーザーが所有者であり、当人がデバイス管理者です。しかし、ビジネス環境ではこうはいかず、多くの場合、ユーザーがインストールできる新しいアプリについては制限があります。

*脅威の 85% は以下の 4 箇所のうちの 1 つに隠れています。これらは、%temp%、%appdata%、%cache%、および %windir% です。*

このほかの例として、企業向け PC の不良ファイルの 54.4%、個人向け PC の 28.7% を占める %temp% などがあります。Temp は、企業向け PC の感染の隠れ場所である可能性が個人向け PC の倍高いです。(朗報があります。悪意があるかどうかに関係なく、プログラムが %temp% ディレクトリから実行されないように Windows ポリシーを設定するのは簡単です。これは優れたサイバー衛生であり、ユーザーのセキュリティ意識向上トレーニングと併せ、保護を確保するのに大いに役立ちます。)

当社はよりクリーンなオペレーティングシステム、特に Win10 のプラスの影響を引き続き確認しています。個人が新しい PC を購入すると、特に Microsoft がすべてのユーザーを Win7 から移行させようとしているため、概して Win10 がデフォルトのオペレーティングシステムとして使用されることに留意することが重要です。ただし、企業にとっては、大規模なアップグレードを行うことはより困難です。Win7 を必要とするレガシーアプリが存在する場合がある上、アップグレードにコストがかかるからです。

# ランサムウェア

ランサムウェアが大挙して出現したのは 2015 年以降です。それ以前は、システムが危険にさらされているとポップアップで脅かし、システムを「浄化する」ためにリンクをクリックする必要があるとユーザーに警告する偽のウイルス対策ソフトウェアがかなり出回っていました。このアクションは通常、何らかのコストを発生させ、システムをさらに侵害しました。2010 年代半ばまでには、ハッカーが暗号通貨の使用を開始したために、法務当局が彼らの活動を追跡することがより困難になりました。この利点と暗号通貨の価値の高さから、ランサムウェアは急成長するビジネスになりました。ランサムウェアの進化に伴い、無料の単一ファイル暗号化解除、多言語サポート、およびカスタマーサービスのすべてが最初に攻撃を実行した悪意のある攻撃者たちから提供されました。

2017 年にはランサムウェア攻撃によるパニックが世界中に広まりました。組織は、ミッションクリティカルなデータを保護しようと急いで身代金を支払うことがよくありましたが、失われたファイルを復号化するためのキーを常に受け取るとは限りませんでした。2018 年には、ランサムウェア攻撃が成功する件数が少なくなりました。バックアップの向上、意識の向上、防御の進化により、生産的なキャンペーンを実行することが難しくなったのが一因です。

Webroot は過去 1 年間でランサムウェア攻撃の件数がさらに減少していると確認しましたが、確実に無くなった訳ではません。代わりに、ランサムウェアはより標的を絞ってより適切に実装され、より冷酷になりました。犯罪者は特により価値が高く弱い標的に狙いを定めています。さらに、この脅威はシステムを侵害するために引き続きリモートデスクトッププロトコル (RDP)、特にマネージドサービスプロバイダー (MSP) が一般的に使用する RDP ツールの侵害を標的にしています。単一の MSP を侵害すると犯罪者は企業の顧客基盤全体にアクセスできるようになることから、プロバイダーは特に有利なターゲットになっています。

過去 10 年間にランサムウェアによって使用され著しく成功したエクスプロイトには、米国家安全保障局 (NSA) によって開発され、後にハッカーグループによってリークされた EternalBlue などがあります。税のソフトウェアを介してウクライナのターゲットに対するサプライチェーン攻撃として始まった世界的な WannaCry ランサムウェア攻撃は、この脆弱性を使用してパッチ未適用のシステムを攻撃し、キルスイッチにもかかわらずその攻撃は数十億ドルの損害とダウンタイムを引き起こしました。同じエクスプロイトが後日、依然多くのパッチが適用されていないシステムで NotPetya 攻撃を実行するために使用されました。

## 最新のランサムウェアのトレンド

### より多くの偵察

攻撃者は、重要なサーバーやバックアップの場所など、企業とそのインフラストラクチャについて学ぶことに努力を集中しています。そうすることで、成功の可能性を高めるためにどのマルウェアとエクスプロイトを使用するかを把握します。この種の偵察攻撃は、準備が不十分 (つまり、緊急時対応計画、リスク評価構造、サイバー保険などが不在) な中小企業 (SMB) を標的とする場合に特に効果的です。

### 身代金費用の上昇

身代金の平均額は増加しています。2019 年第 3 四半期に、身代金の平均額は 41,198 ドルと、第 1 四半期の 36,295 ドルから上昇しました。[4] これらの数値は、ランサムウェアの被害者による身代金支払いを支援するために特別に設立された会社である Coveware によって報告されています。そもそもこのような企業が存在することは、ランサムウェア攻撃の継続的な成功の証です。

**二重のトラブル**

2018 年と同様、Trickbot-Emotet のワンツーパンチが 2019 年に普及しました。 Emotet は、他の感染をデプロイできるボットネット配信ネットワークです。多くの場合、Trickbot (データを盗むだけでなく、組織に関する情報を収集するバンキング型トロイの木馬) を投下します。最近、このような攻撃は巨額の身代金を支払う有利な被害者を見つけようと、比較的規模の大きい企業を標的としています。2019 年に Trickbot は双方向の攻撃を行い、情報を盗むと共に別種のランサムウェアである Ryuk を投下しました。Trickbot は、認証情報と個人データを盗むことに加え、後日ランサムウェアを介して同じ被害者を再び攻撃することができました。

*これらの攻撃は、フィッシングメールに大きく依存して、ネットワークでの手掛かりを得ています。ヘルスケアの登録や気候変動などのタイムリーなトピックを使い、利用者がリンクをクリックしてトロイの木馬、ランサムウェア、またはその他のマルウェアをダウンロードする可能性を高めます。*

もう一つの非常に成功したランサムウェア組織「Evil Corp」 は、米国司法省の狩りの標的になっており、責任者であるとみられるハッカー、マクシム・ヤクベッツの有罪判決につながる情報には 500 万ドルの報奨金が提供されています。ロシアの組織は、企業や個人から約 1 億ドルを盗んでいます。このグループは、Dridex マルウェアを使用して、中小企業の従業員から銀行の認証情報を盗み、「マネーミュール」 (無意識の共謀者または共犯者) を採用して、スキームを通じて得た資金の洗浄を支援しています。2019 年終盤にスペインの複数の企業を襲ったランサムウェア攻撃 BitPaymer もこのグループの仕業です。[5]

## 身代金の上昇

ランサムウェアの最近の傾向は、組織のデータを盗む、またはロックするだけでなく、データの漏洩や不正使用で被害者を脅かすことです。これにより、適切なバックアップが設けられている場合でも、被害者が支払う可能性が高くなります。

## ターゲットのシフト

2019 年には、米国の都市に対するランサムウェア攻撃が蔓延する一方、輸送、医療、教育、中小企業など好まれる標的に対する体系的な攻撃も散見されました。これらの攻撃の多くは、ダークウェブ上で無料で入手でき、経験の浅いサイバー犯罪者でも簡単に使用できるサービスとしてのランサムウェア (Ransomware-as-a-Service) マルウェアを利用しています。

# 高リスク URL

Webroot はこれまで、何十億件もの URL を調査し、継続的にそれらの動作、履歴や運営期間、頻度、場所、ネットワーク、リンク、リアルタイム パフォーマンスを検証してきました。今年は高リスクの URL の数がわずかに増加しました。しかし、悪意のないサイトで発見された悪意のある URL の数は減少しました。現在は 24% です (2018 年の 40% から減少)。それでも、その数は無視できません。

*悪意のある URL の 4 つのうち 1 つは、それ以外の悪意のないサイトでホストされています。*

ウェブサイトをより安全にするためにはデューデリジェンス、既存のコンテンツのパッチ適用とレビュープロセスの常時把握、コンテンツを公開できるユーザーのアクセス制御の見直しが必要です。多くの組織が問題に取り組んでいることは明らかですが、24% は依然として高い数値であり、他の点では良いドメインで悪いコンテンツをブロックするのが難しいとサイバー犯罪者が知っている事実を証明しています。HTTPS トラフィックは暗号化されているため、HTTPS サイトでホストされているページの可視性が比較的低いことに注意してください。さらに、HTTPS の採用が増え、トラフィックを復号化できない、または復号化しないデバイス内のドメインレベルへの可視性が制限されています。これらのデバイスは通常、家庭または小規模ビジネスでの使用を目的としていますが、企業の領域まで及ぶこともあり、その影響が広範囲に及ぶ可能性があります。最終的に、リスクを評価するためにドメインのみを見るソリューションは、サイト内のページを評価するソリューションほど効果的ではありません。

**URL の分類**

当社は高リスクの URL をいくつかのカテゴリに分類しています。これらは、フィッシング、ボットネット、キーロガー及び監視、プロキシ回避と匿名化、マルウェアサイト、スパムサイト、およびスパイウェアとアドウェアです。フィッシングは、今年発見された高リスク URL の 45% を占めています。7 月と 8 月に大幅急増 (フィッシングサイトの年間合計の 26%) が見られ、年末に向けてさらに増加しました。実際、フィッシング URL の 62% は下半期に見られました。これは、新学期や休暇中のオンラインアクティビティの増加に関連している可能性があります。

高リスク URL の増加傾向は過去数年間から継続しており、2019 年の増加は主にフィッシングサイトにけん引されたものです。フィッシングは、ホリデーシーズン前の顕著な増加を伴い、引き続き発生頻度が増加しています。フィッシングサイトへのアクセスはブラックフライデーで 21%、サイバーマンデーでは 58% へと急増した一方、サイバーマンデーにはスパム、疑わしいスパイウェア、アドウェア、プロキシサイトへのアクセスが増加しました。

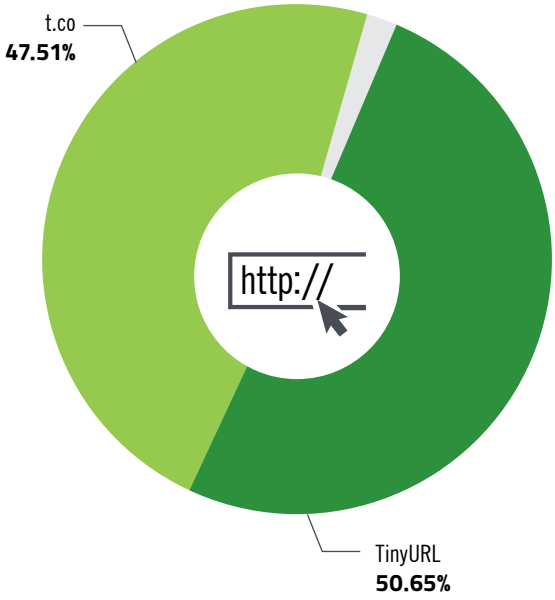
*フィッシング URL は年間を通じて 640% 増加しました。*

対照的に、マルウェアホスティングに関連すると思われる URL の割合が徐々に低下していることがわかりました。割合は 1-1.5% の間で変動しましたが、年初の 1.45% から年末には 1.06% へと大幅に低下しました。

また、スパム、プロキシ回避、アノニマイザー (匿名プロキシ)、アドウェア、スパイウェアに関連する URL の発生率が着実に減少していることも確認しました。

**スポットライト: 悪意のあるコンテンツの配布**

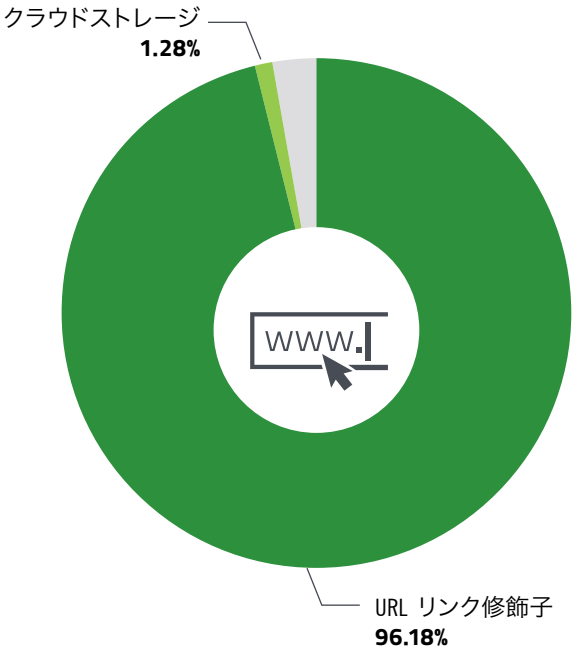
2019 年にセキュリティ カテゴリに分類された URL の 4 分の 1 (28%) はマルウェアコンテンツ配信サイトでした。悪意のあるコンテンツの配信のカテゴリを調べると、過去 1 年と同様、URL 短縮サービスとクラウドストレージがコンテンツが実際にどこから来たのかを曖昧にする上位 2 つの方法であることがわかります。Alexa Internet が公開している最も人気のあるドメイン上位 1 万件につい




図表 2: URL リンク修飾子カテゴリにおける悪意のある URL の上位 2 種

てみると、20 以上のさまざまなコンテンツカテゴリが悪意のある URL をホストしており、それらの 96% が URL リンク修飾子/短縮機能を介してホストしていることがわかりました。URL 短縮サービスは使いやすく人気があり、ユーザーが限られた数の文字（Twitter など）で会話できるようにしますが、ユーザーが実際にどのサイトに飛ばされるかを曖昧にしています。

クラウドストレージもユーザーにリスクをもたらします。ドメイン自体は悪意のあるものとして分類さ




図表 3: Alexaの上位 1 万件の良性ドメイン間での悪意のあるコンテンツの配布

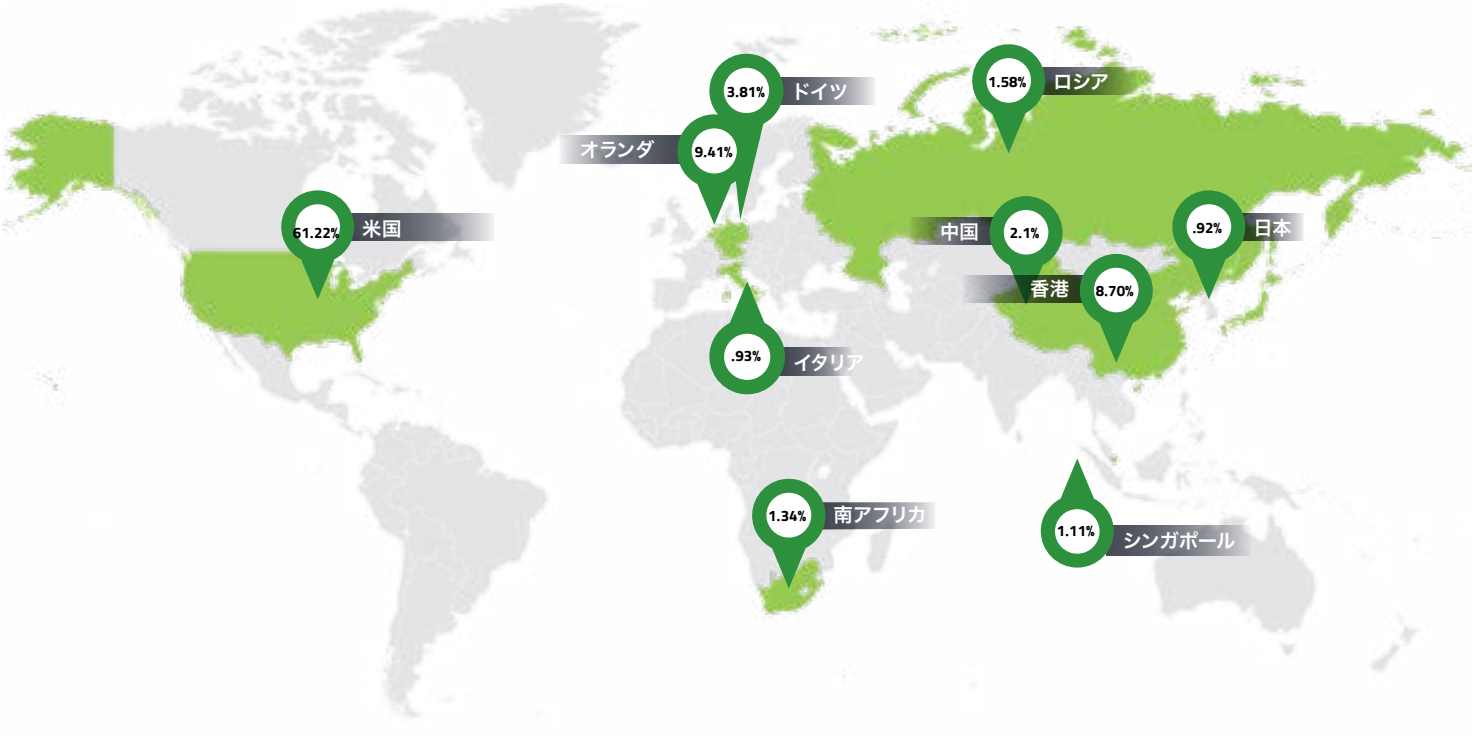
れない場合でも、URL のパスに悪意があると分類される場合があります。たとえば、ユーザーがクラウドサービスへのリンクを受け取る際、URL が指すファイルに悪意がある場合があります。昨年、クラウドストレージの URL パスの 3% が悪意のあるものであり、2018 年の 1.28% から大幅に増加しました。

Alexa の最も人気のあるドメイン上位 100 万件で見られたように、悪意のあるコンテンツの配布は数多くの種類の良性ドメインで発生します。

| URL カテゴリー | 不正な URL をホストしている割合 |
|---|---|
| 製造業 | 19.87% |
| シェアウェア/トレント | 11.84% |
| 成人向け | 9.43% |
| ソーシャル ネットワーキング | 8.71% |
| エンターテインメント | 8.63% |
| 医学 | 7.66% |
| URL リンク修飾子 | 5.81% |
| その他 | 28.06% |

図表 4: 2019 年に悪意のある URL をホストする上位のサイトカテゴリ

シェアウェア/トレント、アダルトサイト、ソーシャルネットワーキングが悪意のあるコンテンツ配信の明らかな手段となることは容易に理解できますが、他のサイトがリストに表示される理由はそれほど明白ではありません。たとえば、製造業は、最もターゲットにされるカテゴリーのリストの最上位です。これは、製造業のサイトが常に最新かつパッチが適用されている可能性が比較的低いために、それらのサイトが比較的脆弱になると考えられます。また、製造組織のサプライチェーンの関係が複雑で、API により駆動されていることが多いことが攻撃対象となると考えられます。マルウェアのセクションで述べたように、製造業のデバイスの感染率は、業界を報告した Webroot の




図表 5: 2019年に高リスク URL の大半をホストしている上位 10 か国

顧客の全体的な平均よりもわずかに高く、サイバー犯罪者が同業界を標的にしているとの見方を強めています。トップ 10 を締めくくるのは、不動産、食品と飲料、およびブログです。

### 地理的分布

2019 年、高リスク URL の大部分をホストした 10 か国は 2018 年とかなり類似していたものの、英国、カナダ、フランスはリストから外れました。代わりに南アフリカ、シンガポール、イタリアがランク入りしました (いずれのシェアも全体の 5%未満)。

昨年見られたのと同様、マルウェアをホストするサイトの大半は米国から発生しています。この割合は比較的安定しており、昨年の 63% からわずかに増加しました。*

### クリプトジャッキングとクリプトマイニング

2018 年に、クリプトジャッキング (ブラウザーベースのプログラムを使用してユーザーの同意または無意識に暗号通貨をマイニングする慣行) とクリプトマイニング (ユーザーの CPU を横取りして暗号通貨をマイニングするマルウェア) が大きな脅威になりました。サイバー犯罪者はそれらを使用して攻撃を簡単に収益化でき、またクリプトコインの価値が非常に高いため、この慣行は非常に儲かるものとなりました。大規模な強盗やハッキング、マイニングなどの事件がニュースに取り上げられました。

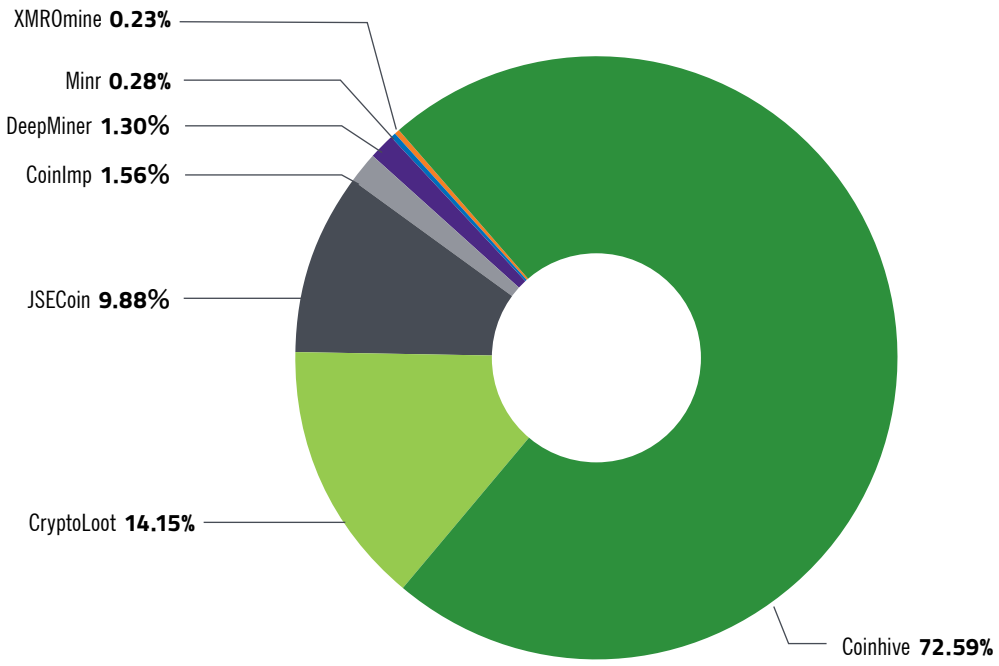
クリプトジャッキングの流行は 2019 年も持続しました。この年、数百万ドルの暗号通貨が暗号通貨取引所から盗まれました。[6] すべてのWeb ページにスクリプトが含まれる可能性のある非常に危険なタイプのルーター攻撃が流行しました。この問題は法執行機関の注意を引くほどの規模になりました。国際警察が主導した 5 か月間のオペレーションにより、東南アジアのコインマイナーに感染したルーターの数は 78% 減少しました。[7]

2019 年、Webroot はクリプトジャッキングのスクリプトをホストする 146,000 件以上のドメインと、結果的にクリプトジャッキングのスクリプトをホストする 890 万件の URL に遭遇しました。

2019 年、クリプトジャッキングの URL は 12 月に 1 月よりも大幅に減少して終了しましたが、年内を通じて顕著な上昇が数多く見られ、サイトはこの手法を引き続き活用しています。最も数字に影響を与えたイベントは、最大のプレイヤーである

*クリプトジャッキングスクリプトをホストしている 890 万件の URL が見つかりました。*

* 注: この数字にはフィッシングサイトが含まれており、これらは米国由来の割合が大きい可能性があります。不正な URL はターゲットと同じ地理的地域にあることが多く、Webroot の顧客が最も集中しているのは米国です。




図表 6: 最も普及している 7 つのクリプトジャッキングサービスで追跡されたクリプトジャッキングスクリプトをホストする URL
(注: Coinhive はクリプトマイニングを終了。)

Coinhive の閉鎖です。2019 年初頭に、Coinhive はクリプトマイニング活動の 84.5% を占めていました。年末までに、閉鎖されたにもかかわらず、クリプトマイニング活動の 60.67% を占めていました。3月には、約 70 万の URL が同スクリプトを実行していました。年末までに、Coinhive はまだ稼働していましたが、マイニングはしていませんでした。Coinhive のスクリプトが非常に多くのドメインで依然実行されていたという事実は、それらが悪意のある者によってそこに配置された可能性が高いことと、ウェブサイトの所有者がスクリプトの存在を認識していないことを示唆しています。

Coinhive の解散によって残されたギャップの一部は、CryptoLoot (暗号化サイトへのトラフィックの 14.15%)、JSEcoin (9.88%)、CoinImp (1.56%) によって埋められています。総じて、ほとんどすべてのクリプトジャッキングサービスが年間を通じて減少し、CoinImp だけが例外的に僅かに増加しました。上位 20 のドメインが、クリプトジャッキングドメインへのすべての顧客トラフィックの 25% を占めています。

昨年と同様、年間を通じてエンドポイントでの検出が徐々に減少しました。年間のクリプトジャッキング事件の 22% は、年初数カ月間に発見され、年末までに 7 - 8% へと減少しました。これは、Web ベースのクリプトマイナーに対するブラウザベースのセキュリティの向上が原因であると考えられます。

| | |
|---|---|
| ass1st.com | 5.64% |
| tpbproxyone.org | 2.48% |
| rotate4refs.com | 1.93% |
| propertiesyoulike.com | 1.66% |
| smokingarchive.com | 1.63% |
| anddev.org | 1.32% |
| cheatcodesgalore.com | 1.10% |
| vidics.to | 1.05% |
| koinohajimari.com | 0.98% |
| erogifs.com | 0.94% |
| airproxyunblocked.org | 0.89% |
| warly.ir | 0.77% |
| svobdoska.ru | 0.73% |
| oklahomaball.com | 0.71% |
| themelike.net | 0.62% |
| nepallist.com | 0.60% |
| coinhive.com | 0.60% |
| boya.com.sg | 0.59% |
| pepitos.tv | 0.59% |
| thepiratebay.bet | 0.57% |

図表 7: クリプトジャッキングドメイン上位 20

# フィッシング攻撃

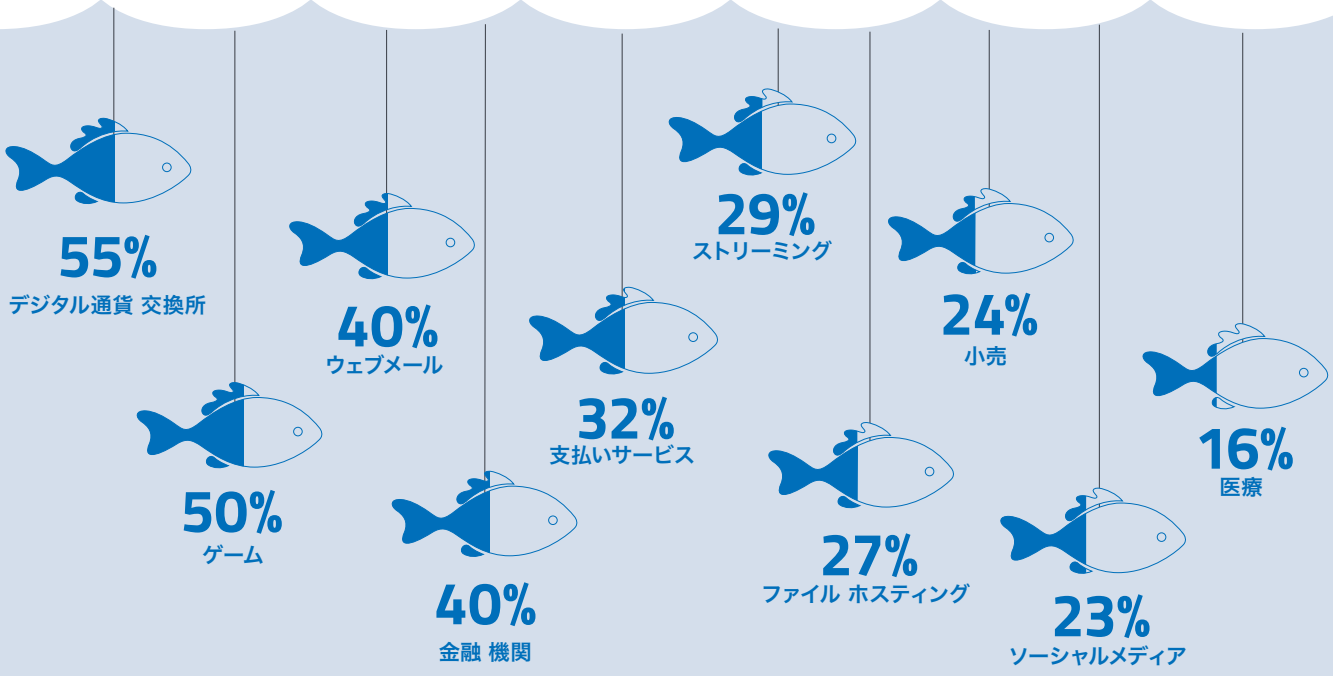
フィッシングは過去 10 年間よりはるか昔から存在していましたが、大幅に進化しています。当初の試みは広範で、無差別に膨大な数の受信者に送信されていました。しかし、ハッカーは後に、スピアフィッシングを介して犠牲者を選択的に標的にできれば、成功率を高めることができることを学びました。ソーシャルネットワークを介して自由に共有された豊富な個人情報により特定の被害者のオンライン習慣が習得しやすくなり、代わりに当人専用のフィッシングメールを簡単に作成できるようになりました。

フィッシングの継続的な進化を示す最近の例は、電子メールの返信チェーンのハイジャックです。ハッカーは個人の電子メールにアクセスし、正当な会話を引き継いだ後、悪意のあるペイロードを添付して当人の友人または同僚のいずれかに転送します。会話の詳細が説得力のあるものであり、それらが事実であることから、電子メールはどのような電子メールフィルタリングでも通過する可能性が高く、受信者がそれを開く可能性があります。しかし、ファイルを開くと、Emotet または別のバンキング型トロイの木馬 (Ursnif / Goziなど) に感染する可能性があります。

年々、フィッシング攻撃が増加し続けています。フィッシング攻撃は、依然として認証情報やその他の機密データを得るための効果的な手段です。その脅威は常に存在しており、Webroot の顧客の 1.6% は、毎月フィッシングページに遭遇します。これは、年間の Webroot エンドポイント保護の顧客の約 20% を占めています。総じて、既知のフィッシングサイトの数は 2019 年 1 月から 12 月にかけて 6 倍増加しました。全てのサイトの 0.15% から 0.96% に拡大しました。2019 年のフィッシングに関する最大の相違は、HTTPS フィッシングサイトの数の急増です。2018 年、フィッシングサイトの 15% が HTTPS を使用し、ユーザーを欺いてサイトが安全だと思わせました。2019 年までにこの割合は 27% に上昇しました。

### 最もなりすましの多い企業

総じて、2019 年にフィッシング攻撃で最も頻繁になりすまされた企業のうち、8 社は 2018 年に上位 10 社にランクされていた企業でした。 Chase (3.1%) は Bank of America に入れ替わりましたが、後者は上位 10 位から脱落したものの、2.4% で上位 20 位内に留まりました。*



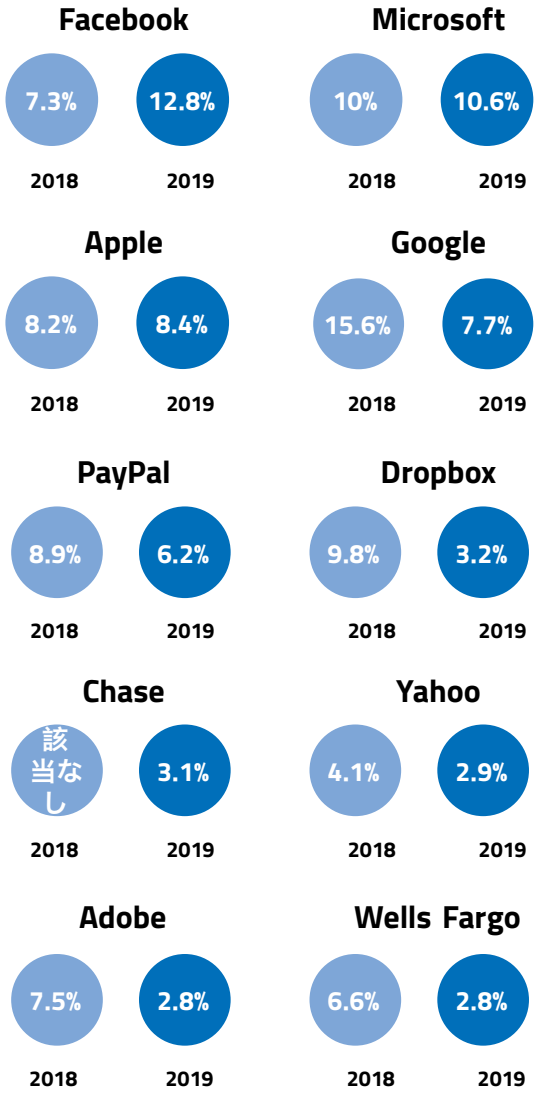

図表 8: HTTPS ホスティングの対象となる上位 10 業種



* Webroot データは、エンドポイント保護の顧客ベースから取得されます。これは、主に米国中心であるため、以下のデータは米国のオンライン習慣に偏っています。

昨年、Googleは15.6%でトップを占め、Microsoft、Dropboxおよび PayPalがそれに続きました。リストを上位 20 まで拡大すると、Amazon や Netflix、DocuSign、Instagram、Steam など、他の多くの馴染みのある企業名が見つかります。DocuSign は、重要な文書に電子署名する手段として頻繁に使用されるため、特に興味深いエントリーです。DocuSign になりすますことにより、データが正当なユーザーに送信されると思いつつ疑いを持たない被害者が個人情報をフォームに入力する可能性があります。同様に、ゲームの自動更新を可能にする、ビデオゲームのデジタル配信サービス Steam になりすまして、マルウェアをデバイスにダウンロードさせる可能性があります。

毎月、最も偽装対象になる上位 10 のブランドへの攻撃を見ると、興味深いことが判ります。実際、Microsoft は年初、Facebook の倍以上、同社のなりすましによるフィッシング攻撃にあっています。その数は 3 月から 5 月にピークに達した後、大幅に減少し、10 月に跳ねあがりました。Apple のなりすまし攻撃は 3 月に 4 倍になった後低下し、10 月に再び急上昇しました。(この大半が Apple® 製品のリリース日と関係している可能性が高いです。) Google の攻撃は年初ゆるやかでしたが、徐々に増加して Microsoft と Apple に匹敵する攻撃数になりました。さらに、Office 365 と Google Cloud は両方ともサイバー脅威の標的にされています。最近では盗まれたパスワードをスパムキャンペーンの脅し戦術として使用するフィッシング脅威などの事例が見られます。はびこるパスワードの再利用とソーシャルメディアのヘビーユースにより、ハッカーが被害者を絞り込み、彼らを脅迫して認証情報を明らかにする能力が高まっています。さらに、AI を使用して多面的なキャンペーンを作成することにより、ユーザーがフィッシングメールと正当な通信を区別することがより困難になりました。




図表 9: フィッシング攻撃で最もなりすまし対象となった上位 10 社

## ビジネスメール侵害はまだ減速していない

ビジネスメール侵害 (BEC) は過去数年間と同様に流行し続けています。このタイプの電子メール詐欺は、上級管理職または信頼できる顧客に不正になりすまし、商業、行政、および非営利組織を攻撃します。当該電子メールには通常、送金 (特に電信送金) または顧客データの公開の指示が含まれています。BEC は、上級管理職および大切な顧客に対する従業員の固有の信頼に大きく依存しています。大手出版社の日経は、子会社である日経アメリカの社員が騙されて詐欺師が管理している銀行口座に送金したことで約 2,900 万ドルを失いました (2019 年 11 月)。リトアニア人の男性が、Google と Facebook の社員を騙して 1.12 億ドルを送金させた BEC 詐欺で有罪を認めました (2019 年 3 月)。[8] FBI によると、BEC は 260 億ドルの詐欺であり、2018 年 5 月から 2019 年 7 月までに特定された世界的な損失は 100% の増加を示しました。[9] AIG Insurance は、昨年 EMEAで企業がサイバー保険の申し立てを行った主な理由として BEC がランサムウェアやデータ侵害を追い抜いたと主張しています。[10]

# 悪質な IP アドレス

過去 10 年間に渡り、Tor がサイバーセキュリティに与えた影響を見てきました。属性を悪意のある行為者から保護するために階層化されたプロキシネットワークが使用されたり、サービスとしてマルウェアをホストするマルウェアが増加しています。2019 年には、IPv4 空間で悪意のある IP が大量に再利用されました。IP アドレスはすべて割り当てられていることを利用したものです。しかし、IPv6 はこの筋書きを完全に書き換えるでしょう。これまでのところ、IPv6 は攻撃者が攻撃を開始する際、これまで使用されていなかったまったく新しいアドレスを使用しやすくします。

*毎日 2,600 万件を超える IP 関連のセキュリティインシデントが発生しています。*

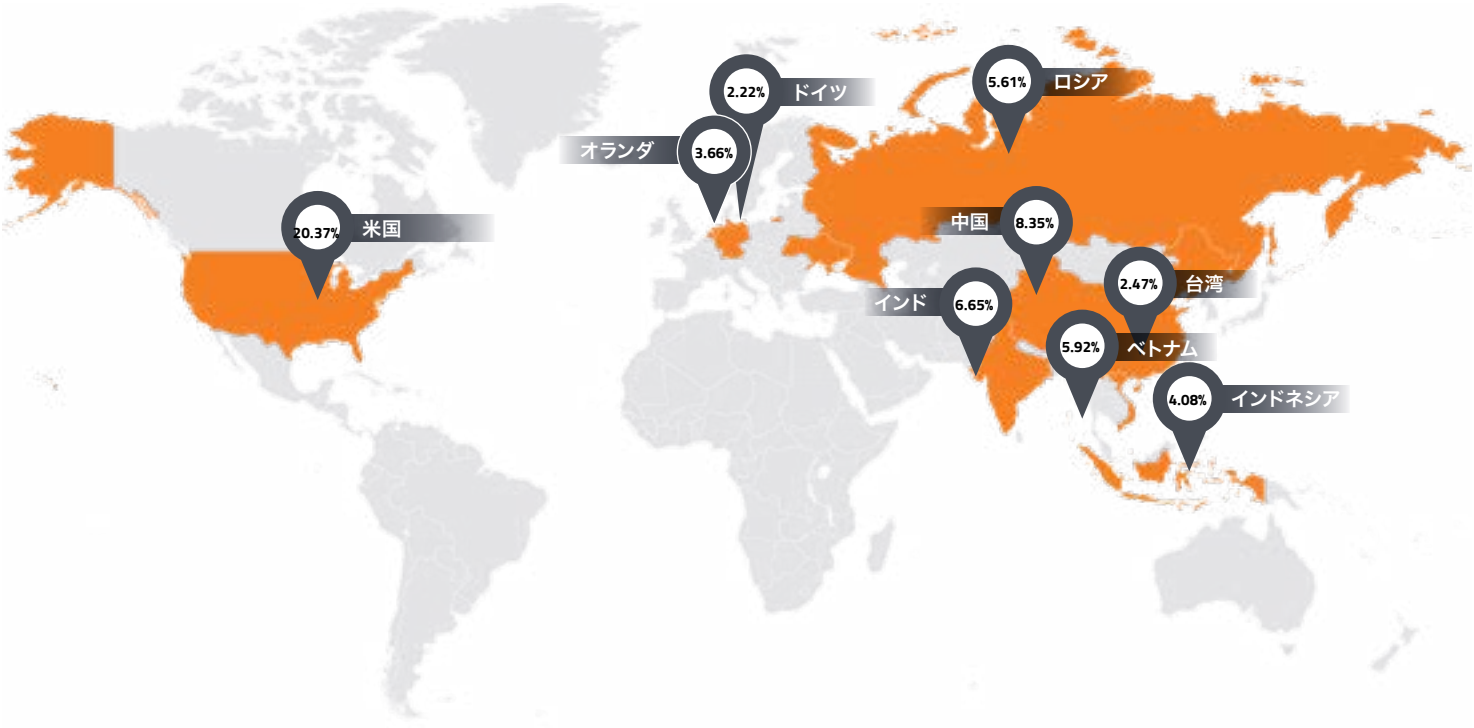
Webroot は悪意のある攻撃の種類 (スキャナーまたはプロキシ、スパム、Windows エクスプロイト、Web 攻撃、ボットネット、フィッシング、モバイル攻撃) ごとに IP アドレスを追跡しているので、積極的にそれらをブロックすることができます。全体的に、2019 年の悪意のある IP アドレス全体の 88% は、スパムのトリガーが繰り返されるタイプのものでした。これらの攻撃の総数は真に膨大で、1 日で 460 万ものスパム IP が検知されました。しかし、本稿の目的上、追跡する数百万個ではなく、最も頻繁に発生する上位 5 万の悪意のある IP、つまり観察された悪意のあるトランザクションの数が最も多い IP を提示します。

### 地理的内訳

悪意のある IP は世界的な現象です。上位 5 万件の悪意のある IP は 184 か国に及びます。実際、有罪判決となった事例の 80.6% が 23 か国で発生し、その半数以上がわずか 6 か国で発生しています。

**悪意のある IP の 50% を占める上位 6 か国:**

- アメリカ
- 中国
- ベトナム
- ロシア
- インド
- インドネシア




図表 10: 悪意のある IP の地域別内訳

**四捨五入した上位 10 カ国は次の通り。**

- オランダ
- ウクライナ
- 台湾
- ドイツ

Webroot は、いくつかの方法で悪意のある IP を追跡します。IP 自体、各カテゴリの IP の総数、および有罪判決によってです。「有罪判決」という用語は、悪意のある動作によって IP が良性ではなく悪意のあるまたは危険なものとして分類された回数を指します。(スパム、ボットネット、Windows エクスプロイトなど、同じ IP に複数のタイプの動作が示される可能性があります。)IP カウントを見ると、悪意のある IP の 60% は 10 か国に広がっています。しかし、上位 10 か国すべてに 5 回以上悪意のある動作を示した IP があり、6 つ以上のカテゴリで有罪判決を受けた IP のある国が 25 カ国ありました。

## IP の詳細な分析

スパムはもう 1 年間も引き続き悪意のある IP のトップの座を占め続けています。しかし、ボットネットは昨年のわずか 3% から今年は 8% に上昇し、スキャナーは去年の 19% からは若干低下したものの、依然として上位 5 万件 (16%) のかなりの割合を占めています。

スキャンに使用される悪意のある IP の発生率はいくらか低下しましたが、スキャナーは依然として重大な脅威です。ハッカーは環境をスキャンして、ネットワーク構成、使用中のアプリケーション、ユーザーの行動に関する詳細を学習します。この情報を利用して、より有利なターゲットを選択し、その特定の環境に合わせて攻撃を仕立てることができます。

Windows エクスプロイトは、はるかに小さなカテゴリですが、驚くべき傾向を示しています。たとえば、ハッカーは更新されていない Windows の脆弱性 (前述の EternalBlue など) が含まれるシステムをスキャンし、標的を絞り込んだマルウェアを展開することでそれらを悪用する可能性があります。Windows エクスプロイトに関連付けられた IP の数は、2019 年に最も大きく成長し、1 月の約 2.6 万件から 12 月には 12 万件を超えました。これは 360% の増加です。

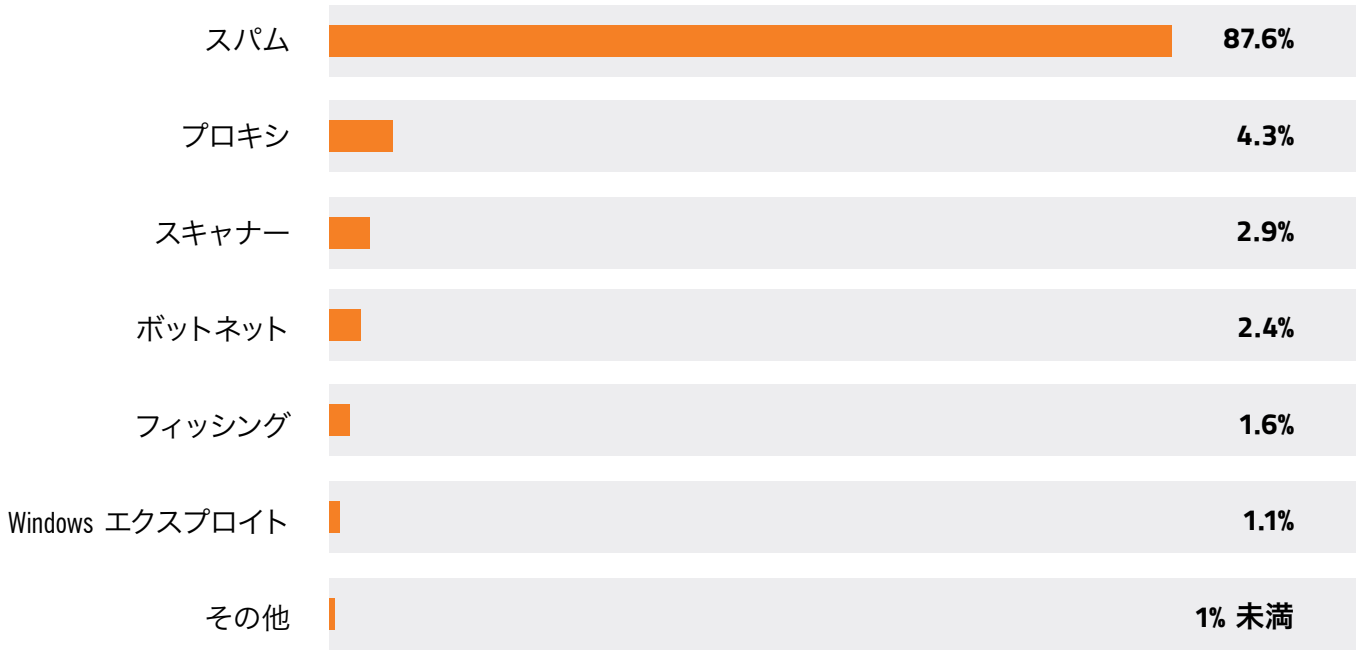
## 複数の不正な動作

悪意のある IP は、複数のタイプの不正な動作の原因となります。実際、上位 5 万件の悪意のある IP アドレスはいずれも 4 つ以上のカテゴリで有罪判決を受けています。さらに、それらは複数回表示されます。不正な IP アドレスの 96% が悪意のあるアクティビティを複数回示しました。

### 悪意のある IP の概要

- 92.9% が少なくとも 4 つのカテゴリーで有罪判決を受けた
- 当該年の有罪判決が 1 度だけだったのは、悪意のある IP の僅か 3.4%
- 年間で 700 万を超える IP が当該年に 37 回以上有罪判決を受けた
- 2019 年に有罪判決を受けた IP の上位 1% は、同年だけで 337 回以上有罪判決を受けた

*Windows エクスプロイトに関連する IP アドレスは 360% 増加。*




図表 11: 悪意のある IP アクティビティ: カテゴリー別

# 有害なモバイルアプリ

導入以来、Android™ デバイスはセキュリティに関して特に苦労しています。過去 10 年間にいくつかの重大な脆弱性が発見された上、2019 年 11 月にはさらに別の重大な脆弱性が見つかりました。Google は引き続き悪意のあるモバイルアプリと戦っていますが、オープン OS という特性が彼らの努力の妨げとなっています。

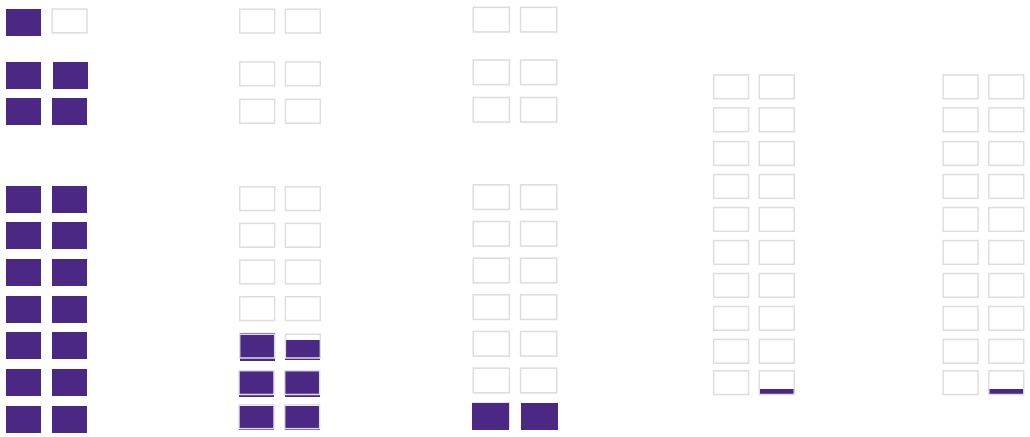
Android マルウェアは Windows マルウェアほど普及していないものの、米国の約 1 億 2,050 万人の Android ユーザーにとって拡大を続けている実際の脅威であることにかわりはありません。[11] これまで、コンピューターアルゴリズムと人間のレビューチームの両方が関与するレビュープロセスを通じて、数百の悪意のあるアプリが Google Play ストアから排除されました。Google Play で初めてアプリを公開したいデベロッパー向けに、より厳格な新しい審査を実施した Google は、潜在的に有害なアプリ (PHA) をダウンロードする確率は 2018 年に 推定 0.64% であり、アプリを Google Play からダウンロードするならば、その確率ははるかに低いと述べています。[12]

それでも、セキュリティの問題があるアプリはまだたくさんあります。Google が Google Play ストアの 1.7 万件のアプリの中から Joker マルウェア (別名Bread) を発見し、その後 Play ストアからそれらを削除。コードの分析により、Joker のオペレーターは検出を回避するため、利用可能なほぼすべての難読化手法を使用していることがわかりました。平均的な Android デバイスには 100 - 400 個のアプリがプリインストールされているため、セキュリティホールの可能性は高いままです。

Webroot で保護されたモバイルユーザーの場合、2019 年の感染率は 4.6% でした。感染はいくつかのカテゴリに分類され、中でもトロイの木馬とマルウェアが圧倒的多数を占めました。

Android デバイスで繰り返し発生する問題は、40% 以上が v9 より古い OS バージョンを使用していることです。Windows デバイスと同様に、パッチが適用されていない比較的旧型のデバイスは、悪意のあるアプリケーションに対してより脆弱です。一例として、Bad Binder というエクスプロイトは悪意のあるアプリがルート化してデバイスを完全に制御できるようにします。Android 9 とそれ以前のバージョンはこのエクスプロイトの影響を受け、また比較的古い OS バージョンはさらに古いエクスプロイトの影響を受けやすくなります。比較的古いエクスプロイトを利用するように作成されたアプリは、より安全なバージョンに更新することができない古いデバイスで引き続き成功します。

攻撃方法や意図とは無関係に、ハッカーは音声、テキストメッセージ、電子メールにアクセスでき、キーストロークの全てを監視、カメラにアクセスし、GPS を通じてデバイスの位置情報を得る以上のこともできるため、悪意のあるモバイルコードはユーザーを悩ませます。携帯電話がなぜ侵害先として非常に求められているのかが簡単にわかります。




図表 12: 悪意のあるアプリの内訳 (注: これらのうち、12.5% が不要と思われるアプリケーションまたは PUA として分類されました。)

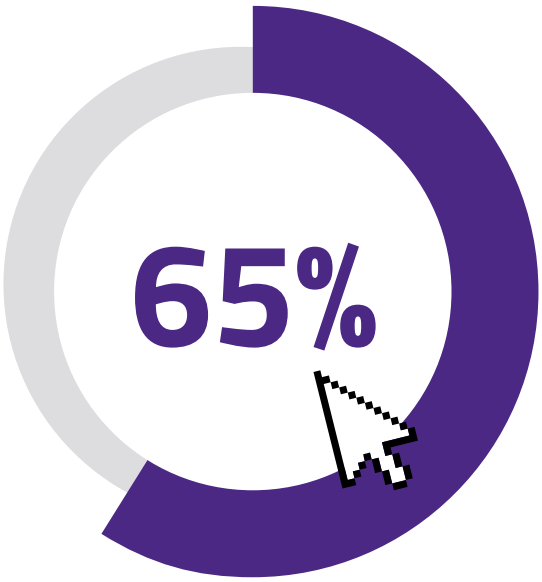
# セキュリティ意識向上トレーニング

新しいイノベーションは常に新しいリスクをもたらしますが、トレーニングはそのリスクを減らすために大いに役立ちます。予防的サイバーセキュリティ教育 (セキュリティ意識向上トレーニング) は成長分野であり、深刻な侵害の出発点となることが多いフィッシングなどのソーシャルエンジニアリングに関連するセキュリティインシデントの削減に非常に効果的です。防衛の第一線である、訓練された個人は、機密データ、知的財産、および組織自体の実行可能性を保護するのに役立ちます。

2019 年には、1 - 2 か月にかけてセキュリティ意識向上キャンペーンを 1 - 5 回実施している組織は、フィッシングシミュレーションで平均クリック率 37% であったことが判りました。しかし、3 - 4 か月間で 6 - 10 個のキャンペーンとトレーニングを実行すると、クリック率は 28% に低下しました。当該組織が 4 - 6 か月間に 11 以上のコースを実行した場合、数はさらに改善されました。その割合は 13% に低下しました。このタイプのトレーニングは、多額の金銭がかかっていると考えられる BEC (フィッシングのセクション参照) との戦いに特に関係があります。

定期的なトレーニングの成功が増えている理由の 1 つは、特にこれらの攻撃が最近のイベントやトレンドに大きく依存しているため、ユーザーは高度に多様化されますます洗練された標的型フィッシング攻撃に備えなければならないことです。最近の例には、パッケージ配信通知、ソーシャルメディアのパスワードを変更する必要がある、または特定のサービスを継続するには、クレジットカードの有効期限が切れているため更新する必要があるという警告などがあります。現行の、または人気のあるものはすべてハッカーにとって恰好の標的であり、ハッカーは迅速に方向転換してスパム方法を変更できます。ユーザーは、被害者になるのを回避するため、継続的かつ関連性のあるトレーニングが必要です。

*4 - 6 か月間で 11 以上のトレーニングコースを実施すると、フィッシングのクリックスルーが減少します。*



# 予測

Webroot のセキュリティ専門家は、過去の教訓を活用し、2020 年とそれ以降の数年間に何が起こるかを予測しています。予測のいくつかを次に示します。

**どのような脅威が発生するか。**

「開発途上国に対する攻撃が増えるでしょう。収益を生むためではなく、混乱させて破壊するためです」とグレイソン・ミルボーン (セキュリティ・インテリジェンス・ディレクター) は述べています。彼は、侵害によって収集されたデータがフィッシングメールに組み込まれるため、フィッシングのターゲットがより絞り込まれると予測しています。

*「ボットネットの規模と配布されるマルスパムの両面から、Emotet が引き続きトップランナーとなるでしょう。ランサムウェアは引き続き脅威となるでしょう。さほど洗練されていない行為者は、より大規模でより成功したオペレーションで使用された戦術を模倣するでしょう。」*

**ジェイソン・デイヴィソン、高度脅威調査アナリスト**

エリック・クロノウスキ (高度脅威調査マネジャー) は、身代金目的の攻撃者が自動バックアップソリューションを注意深く観察し、バックアップされたデータまたはタスク自体を削除または変更しようとすると予測します。タイラー・モフィット (セキュリティアナリスト) は、GDPR や CCPA などのプライバシー規制が全面的に施行されているため、企業が適切なバックアップを行っており当該ファイルの返却を求める必要がなくとも、企業が支払う可能性を高めるためにランサムウェアが重要な顧客データを漏洩すると脅かすだろうと付けくわえます。

**誰がターゲットになるか**

タイラー・モフィットは、中小企業が引き続き標的にされると考えています。大企業に比べ予算が少なく、セキュリティスタッフが少ないため、魅力的なターゲットになっています。ケルビン・マレー (シニア脅威調査アナリスト) は、ユーザー教育が BEC 攻撃に対する主要な防御策であるとアドバイスしています。合理的な量の電子メールフィルタリングでは、すべての偽の電子メールの通過を阻止できません。

*「あらゆる形態のエネルギー部門は引き続き深刻なリスクにさらされるでしょう。さらに、サービスプロバイダーは攻撃者にとって非常に儲かる標的になります。彼らは多くのビジネスへと入り込める単一の入り口だからです。幹部は引き続きますます洗練化が進む BEC 攻撃の標的となるでしょう。」*

**マシュー・オルドリッジ、プリンシパル・ソリューション・アーキテクト**

**AI / MLはどのような役割を果たすか**

ハル・ロナス (シニアバイスプレシデント兼最高技術責任者) は、サイバー犯罪者による AI の実験が増え、2020 年に攻撃の規模と深刻度が増加するだろうと警告しています。ジョー・ジャロック (サイバーセキュリティ戦略のシニアディレクター) も同様の路線に沿って、AI ベースのセキュリティ製品に対する敵対攻撃が範囲と複雑さの両方で拡大すると考えています。

比較的恐ろしいシナリオの 1 つは、ディープフェイクの生成に AI が使用されることです。2019 年に、ソーシャルエンジニアリング攻撃に説得力のある新たな局面を追加するため、ディープフェイクスタイルの AI 合成技術のデプロイが成功した最初の例を確認しました。

*「ディープフェイクは大きな脅威になります。技術が発展するにつれて、誰もが他の誰かに言ったことのないことを言わせる偽の動画を作成し、悪意のある (または政治的な) 目的のためにそれらを効果的に武器化することができるでしょう。」*

**グレイソン・ミルボルン、セキュリティ インテリジェンス ディレクター**

**クリプトジャッキングは滅びたか**

タイラー・モフィットは、過去 1 年ほどでクリプトジャッキングが減少してきたものの、その減少は暗号通貨市場の全体的な価格を反映すると予想しています。向こう　1　年間に暗号通貨の価格が史上最高水準に上昇することがあれば、この種の攻撃が復活する公算が高まるでしょう。マシュー・オルドリッジは、犯罪者が他人のリソースを利用してお金を稼ぐための控えめな方法として、2020　年にもクリプトジャッキングが継続されると予想しています。彼は、攻撃者が標的とする新しいタイプのコンピューティングデバイスとネットワークを見つけて、検知されないようますます巧妙な方法を使用して、投資した攻撃時間からより大きな利益を得ると予測しています。

# 結論

2019　年とそれ以前の年を振り返ると、変化は明らかです。クラウドへの大規模な移行、進化　(そして時には対立する)　ユーザーのプライバシー、セキュリティ、利便性に対する要求、サイバー犯罪者の絶え間ない革新、そして攻撃面の絶え間ない拡大を目撃してきました。

保護の取り組みという点では、攻撃の量とバリエーションが非常に多いため、包括的で多層的なアプローチが必要です。それは人々から始めるべきです。人々を教育、リスクを回避し疑わしい事件を迅速かつ正確に報告するように訓練し、他の防御層を導入して、ユーザーが誤って不良リンクをクリックした場合に予防的に停止されるようにします。(結局、最高の訓練を受けたユーザーでさえ間違いを犯します。)悪意のある　IP　アドレスにアクセスしようとする場合、アクセスを阻止するためのセキュリティレイヤーが必要です。フィッシングサイトにアクセスしようとする場合、彼らを保護するために別のレイヤーを配備すべきでしょう。たまたま悪意のあるスクリプトを実行することになった場合は、実行を防止する必要があります。悪意のあるプログラムを実行しようとした場合、または明らかに良性のアプリケーションが悪意のあるものになった場合は、これをブロックすべきでしょう。

そして、他のすべての方法が失敗した場合、完全な保護および災害復旧戦略の一環としてすべての重要なデータを安全にバックアップする必要があります。

*最終的に、特効薬はありません。これまでもなかったし、これからもないでしょう。しかし、攻撃のすべての段階でユーザーとデータを保護するセキュリティレイヤーを実装することにより、大規模なセキュリティ侵害やサイバー攻撃、およびデータ損失に直面した場合でも、企業とエンドユーザーが反発できる「サイバー弾力性」の状態を実現できます。*

**ハル・ロナス、シニアバイスプレシデント兼最高技術責任者、中小企業および消費者部門**

[1]Verizon. “2010 Verizon Data Breach Investigations Report (2010 年 Verizon データ侵害調査レポート).” (2010 年 7 月)
https://www.wired.com/images_blogs/threatlevel/2010/07/2010-Verizon-Data-Breach-Investigations-Report.pdf

[2]The Untold Story of NotPetya, the Most Devastating Cyberattack in History (歴史上最も壊滅的なサイバー攻撃である NotPetya に関する秘話)。参考記事:
www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world--

[3] Magic Quadrant for Security Awareness Computer-Based Training (Magic Quadrant - セキュリティ認識のためのコンピューターベースのトレーニング)。参考記事:
www.gartner.com/doc/reprints?id=1-1OAYVTNP&ct=190723&st=sb

[4] Ransomware Payments Rise as Public Sector is Targeted, New Variants Enter the Market (公共部門が標的になり新しい亜種が市場に参入するとランサムウェアの支払いが増加)。参考記事:
www.coveware.com/blog/q3-ransomware-marketplace-report

[5] Spanish companies' networks shut down as result of ransomware (ランサムウェアによりスペイン企業のネットワークが停止)。参考記事:
arstechnica.com/information-technology/2019/11/spanish-companies-networks-shut-down-as-result-of-ransomware/

[6] Bitcoin remains strong as 160 million stolen from crypto exchanges in 2019 (2019 年にデジタル通貨交換所から 1 億 6 千万盗難されるなか、ビッドコインは引き続き堅調)。参考記事:
cryptoslate.com/bitcoin-remains-strong-as-160-million-stolen-from-crypto-exchanges-in-2019

[7] Cryptojacking Drops by 78% in Southeast Asia After INTERPOL Action (インターポールのアクションを受け、東南アジアでクリプトジャッキングが 78% 減少)。参考記事:
www.bleepingcomputer.com/news/security/cryptojacking-drops-by-78-percent-in-southeast-asia-after-interpol-action

[8] Tech Duo Stung for $122m by BEC Attacker (Tech Duo が BEC 攻撃を受け 1.22 億ドル騙し取られる)。参考記事: www.infosecurity-magazine.com/news/tech-duo-stung-for-122m-by-bec-1?

[9]Business Email Compromise Is a $26 Billion Scam Says the FBI (ビジネス電子メールの侵害は 260 億詐欺であると FBI が発言)。参考記事:
bleepingcomputer.com/news/security/business-email-compromise-is-a-26-billion-scam-says-the-fbi/

[10]BEC overtakes ransomware and data breaches in cyber-insurance claims (BECがサイバー保険請求でランサムウェアとデータ侵害を追い抜く)。参考記事:
www.zdnet.com/article/bec-overtakes-ransomware-and-data-breaches-in-cyber-insurance-claims

[11] Number of Android smartphone users in the United States from 2014 to 2021 (2014 から 2021 年真での米国における Android スマートフォンのユーザー数)。参考記事:
www.statista.com/statistics/232786/forecast-of-andrioid-users-in-the-us

[12] To Stop Shady Apps, Google To Scrutinize First-Time Developers (怪しいアプリを停止するため、Google が初めての開発者を精査)。参考記事:
uk.pcmag.com/news-analysis/120501/to-stop-shady-apps-google-to-scrutinize-first-time-developers

## Webroot と Carbonite について

Webroot と Carbonite は OpenText 企業であり、クラウドおよび人工知能を活用してデータに対するサイバーおよび自然の脅威から企業および個人を保護します。我々は両社を合わせて管理されたサービスプロバイダーと中小企業向けに構築されたエンドポイント保護、ネットワーク保護、セキュリティ認識トレーニングソリューション、データバックアップと災害復旧を提供します。Webroot BrightCloud® 脅威インテリジェンス サービスは、Cisco、F5 Networks、Citrix、Aruba、A10 Networks などの市場をリードする企業で採用されています。機械学習の力を活用して数百万にものぼる企業および個人ユーザーを保護することで、Carbonite と Webroot はインターネットの安全に寄与しています。Carbonite と Webroot は、北米、ヨーロッパ、オーストラリアおよびアジアでグローバルに事業を展開しています。エンドポイントのセキュリティおよび災害復旧ソリューションについては、carbonite.com および webroot.com をご覧ください。

385 Interlocken Crescent Suite 800 Broomfield, Colorado 800.870.8102 webroot.com