WEBROOT®
Smarter Cybersecurity™

2019 年ウェブルート

# THREAT REPORT

# 内容


# はじめに

ハル・ロナス ｜ 最高技術責任者

最近よく聞く「アジャイル」という言葉。この言葉はソフトウェア開発の世界だけでなく、サイバー犯罪の世界でも合言葉として使われるようになりました。2018 年は、 新たなアプローチや攻撃ベクトルの組み合わせ、 AI ( 人工知能 ) 導入など、 アジリティやイノベーションという言葉がぴったりの事件が数々と起こり大混乱を巻き起こしました。　従来型のアプローチがまだ猛威をふるっている一方、日々新たな脅威が出現し、新しい攻撃方法の試行やテストが繰り広げられています。

データを見ると、マルウェアまたは潜在的に望ましくないアプリケーション (PUA) に分類される新種のファイルの割合が依然として驚くほど多いことがわかります。 主な脅威は引き続きフィッシングで、 最近は Netflix や Amazon、 Target などのブランドを装い、 人々のパスワード使い回し癖を利用してオンラインバンキングなどの口座に不正アクセスしようとする手口が流行しています。ランサムウェアはいくらか減少し、それに取って代わりクリプトジャッキングやクリプトマイニングが出回り、直接攻撃を仕掛ける犯罪としてニュースになっています。詐欺も横行しています。 高リスクIPアドレスも引き続き問題で、特にスパム配信に使われるIPアドレスは問題です。配信元は3つの国に集中しています。

高リスク IP アドレスは検出を逃れるために悪質から無害、無害から悪質へとレピュテーションの状態を頻繁に変えます。 またルーターを狙った攻撃も増え始めています。 これはネットワーク上にあるデバイスの情報を入手し、暗号化されていないトラフィックを探しあてて中間者攻撃やクリプトジャッキング攻撃を仕掛けるというもので、古いデバイスや、家庭用ルーターのログインのしにくさ、不正アクセスされている兆候が少ないなどといった点を利用します。

ウェブルートが注力しているのも「アジリティ」と「イノベーション」です。当社では世界中の現場に設けた6,700万点ものセンサーから実データを集め、 これを特許取得済みの機械学習モデルを使用して分析し、 新たな脅威の予測に役立てています。この機械学習モデルは年々、改善されています。当社の年次脅威レポート 2019 年版では、当社が 2018 年中に蓄積した脅威アクティビティを解説しながら過去のデータと比較します。 皆様の今日そして今後のサイバー犯罪対策に当社の知識と洞察が役に立つことを願っています。

# ウェブルートの見解


Webroot® プラットフォームには莫大な量のデータが取り込まれます。これらはフィールドのエンドポイントやセンサー数百万点をはじめ、よく吟味されたサードパーティのデータベースや当社技術パートナーの保護下にあるエンドユーザー約5,000万人のインテリジェンスから自動的に取得されます。本レポートで提供する統計ならびに傾向、洞察はこれら何十億ものデータポイントの分析・解釈に基づいています。また、次の広範な脅威アクティビティに対する洞察とコンテキストについても、ウェブルートの脅威研究チームが詳しく掘り下げて解説します。

- マルウェア ( 主にポリモーフィック型 ) と潜在的に望ましくないアプリケーション (PUA) の傾向
- ランサムウェア、クリプトジャッキング、クリプトマイニング
- 悪質な IP アドレスとそのリスク
- URL 分類とセキュリティ動向
- フィッシング攻撃とその標的
- エンドユーザーの意識向上とトレーニング
- モバイル アプリの脅威

昨年も取り上げましたが、今年も Windows® 10 の導入が消費者や企業のセキュリティ強化にどう貢献したかという点について解説します。また今年は、個々の PC が何度も感染する可能性を検証するセクションや、マルウェアが企業や消費者のシステムに潜んでいそうな場所を説明するセクションを新たに設けています。クリプトジャッキングやクリプトマイニングなど、ランサムウェアに取って代わり増加し始めた金儲け目的の新たな攻撃手法についても徹底的に検証します。攻撃の成功率を高めるために一度の攻撃で複数の手法を使うという新たな傾向にも注目します。本レポートの情報や洞察をもとに脅威の現状を明確に把握するとともに、今年の攻撃トレンドに応じた対策を講じていただけたらと願っています。

本分野のパイオニアであるウェブルートでは、機械学習を使用してきた 10 年以上の経験と過去 10 年分の脅威データ ( なんと 6 ペタバイトを超えます ) を駆使し、極めて正確に脅威と攻撃手法を予測します。

**デイブ・デュフォー | エンジニアリング担当副社長**

## 現在、ウェブルートのプラットフォームでは第六世代の機械学習技術を使用しています。これを駆使して日々分析するデータオブジェクトの数は 5,000 億個にもなります。


**7 億 5 千万件以上**

ドメイン


**320 億件以上**

URL


**40 億件以上**

IP アドレス

**310 億件以上**

ファイル動作

**6,200 万件以上**

モバイル アプリ

**6,700 万件以上**

接続センサー

# ポリモーフィック型マルウェアと PUA


2017 年は、マルウェアの 93% と潜在的に望ましくないアプリケーション (PUA) の 95% がポリモーフィック型でした。この傾向は 2018 年も同じです。ポリモーフィックコードは、名前や暗号化キー、シグネチャ、ハッシュ、関数命令、実行フロー順序などを使用してマルウェアの単一インスタンスを変えることで検出を逃れながら、多数のユーザーに自身を送り付けます。このようにポリモーフィック型マルウェアや PUA は識別情報が絶えず変化することから、既存のシグネチャでは新しく生まれた亜種をマッチングできません。つまり、パターン マッチング型のセキュリティ製品では新たな亜種をすばやく検出することができず感染してしまう可能性があるのです。

## ウェブルートが 2018 年に検出したマルウェアの 93% がポリモーフィック型でした。

Webroot® 製品で守られたエンドポイントでは、これまで検出されたことのない未知の実行ファイル (PE) を毎年 50 億点以上も検出しており、この数は増加する一方です。にもかかわらず、マルウェアまたは PUA と判断されるファイルの割合は減少傾向にあり、2018 年に検出された新たな PE のうち、マルウェアと判断されたものはわずか 1% 足らずでした (2016年は 2.5%、2017 年は 1.5%)。2018 年の PUA 検出数の減少はこれよりも劇的で ( 図 1 を参照 )、2016 年の 2.2%、2017 年の 0.4% から 0.11% へと減りました。この減少傾向の理由については後ほど考察します。

感染を報告するエンドポイントの 68% が消費者のデバイス、32% が企業のエンドポイントでした。デバイス 1 台あたりのマルウェア ファイルの平均数を見てみると、2018 年は劇的に減少しています ( 図 2)。

| | 2016 | 2017 | 2018 |
|---|---|---|---|
| 実行可能ファイルがマルウェアである割合 | 2.5% | 1.5% | 0.88% |
| PUA である割合 | 2.2% | 0.4% | 0.11% |

図 1: マルウェアまたは PUA と判断された PE

| | 2016 | 2017 | 2018 |
|---|---|---|---|
| デバイス 1 台あたりのマルウェア ファイル合計数 | 0.66 | 0.48 | 0.07 |
| 消費者デバイス 1 台あたりのマルウェア数 | 0.59 | 0.53 | 0.09 |
| 企業デバイス 1 台あたりのマルウェア数 | 0.61 | 0.42 | 0.04 |

図 2: デバイス 1 台あたりのマルウェア ファイル平均数

図 2 を見ると、消費者のデバイスの方が企業のデバイスに比べ感染件数が 2 倍以上多いことがわかります。ただし、企業の数字は企業所有の PC のみを対象にした数字ではありません。多数の企業が PC などの個人デバイスを企業ネットワークに接続することを従業員に許可しているためです ( このことにより企業が被るリスクは大きく増加しています )。

マルウェアが減少しているのは事実ですが、セキュリティの任務完了はまだまだ先の話です。**2018** 年は特に **Emotet** や **Trickbot** など、**UPnP** 機能や **Tor** 機能を悪用したあの手この手の新戦術、新手口が見受けられました。これらのマルウェアは回復性が強化されておりオフライン中の検出が困難です。

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

### オペレーティング システムの役割

オペレーティング システム (OS) が新種のマルウェアや PUA ファイルの減少に果たす役割は重要です。昨年も取り上げましたが、アンチウイルスが常時有効な Windows® 10 への移行はこの減少傾向を説明するひとつの理由となっています。

## Windows 10 搭載デバイスは、Windows 7 実行デバイスよりも 2 倍以上安全です。

ウェブルート製品で守られている企業のエンドポイントのうち、 Windows 10 を使用しているものはWindows 7 を使用しているものより若干多く (それぞれ 45%、43%)、Windows 8 はわずか 3% です。 今も Windows XP (Microsoftのサポートが数年前に中止されました) を使っているのは 1% です。 実際、 企業での Windows 10 の使用率は 2017 年 11 月に転機を迎えて以来、 月におよそ 1.2% の割合で着実に増加しています。にもかかわらず使用率の増加には予想以上の時間がかかっています。 企業での Windows 10 の使用率が消費者による導入率と肩を並べるには、セキュリティ上のメリットが明らかなのにかかわらず、あと 2 ～ 3 年かかりそうです。一般に、旧バージョンの Windows オペレーティング システムからの移行には企業の方が時間がかかっています。これはおそらく、Windows 7 や XP などのレガシー オペレーティング システムのソフトウェア要件が原因だと考えられます。一方、消費者側の Windows 10 の導入は安定しておりこの一年間大きな動きがなく現在およそ 75% です。ちなみに、 Windows 7 は 13%、 Windows 8 は 9% です。

エンドポイント デバイス 1 台あたりの感染率は Windows 7 が 0.07%、 Windows 10 が 0.05% と全体的には Windows 7 の方が若干高めです。ところがこれを消費者のデバイスと企業のデバイスで比較すると大きく異なり、消費者のシステムでは 0.09%、企業のシステムでは 0.04% と消費者の方がエンドポイント デバイス 1 台当たりの感染率が 2 倍以上高くなっています。これを OS 別に見るとさらに顕著な差が出ています。 Windows 7 を実行している消費者のシステムでは平均感染率が 0.18%、企業のシステムではわずか 0.04%、 Windows 10 の場合は、消費者のエンドポイントで 0.07%、企業のエンドポイントでわずか 0.02% となっています。 ほぼすべての項目が前年より減少しています ( 図 3 を参照 )。

| | | 2016 | 2017 | 2018 |
|---|---|---|---|---|
| **消費者** | 平均 | 0.66 | 0.48 | 0.09 |
| | Windows 7 | 0.59 | 0.53 | 0.18 |
| | Windows 10 | 0.61 | 0.42 | 0.07 |
| **企業** | 平均 | 0.11 | 0.07 | 0.04 |
| | Windows 7 | 0.19 | 0.07 | 0.04 |
| | Windows 10 | 0.05 | 0.03 | 0.02 |

図 3: エンドポイント 1 件あたりの感染率

Windows 10 搭載マシンでは消費者、企業とも昨年一年を通じて、比較的着実にマルウェアの減少が見られました。9 月から 12 月にかけては、Windows 10 を実行する企業の PC で急増が見られましたが、これは新学期とクリスマスを狙ったマルウェア キャンペーンの展開が原因だと考えられます。

マルウェアと PUA は新種のファイルの割合という点で減少していますが、これら数字は無視できるものでなく脅威の一掃を意味するものではありません。ウェブルートの保護下にあるデバイスでマルウェア、PUA ファイルの検出数が減少した理由は以下のとおりいくつか考えられます。

» 第 1 の理由は、悪意のあるアクティビティをキルチェーンの早期段階で検出できるようになったことです。つまり、エンドポイントを感染させるために悪質な URL 経由で入ってくる実行可能ファイルをブロック (14 ページの「URL」を参照 ) できるようになったことと、実行可能ファイルによる他の悪質な実行可能ファイルのダウンロードをエンドポイントで防止できるようになったことです。
» 第 2 の理由は、マルウェア エコシステムの変化を受けて「悪質」に分類される新種のファイルの割合が減少していることです。つまり、「ドライブバイ ダウンロード」がほとんど使われなくなり、マルウェアをインストールする方法よりも簡単に金儲けできる方法が考え出されていることです。
» 第 3 の理由は前述のとおり、Windows 10 が従来のオペレーティング システムより安全であることです。Windows Defender® は他のアンチウイルス ソリューションが無効になると自動的に有効になります。そのため、全体的に安全で感染数の減少に貢献しています。

PUA の減少には、AppEsteem[i] などの企業も貢献しています。これらの企業はリスクの少ないアプリのダウンロードと使用をエンド ユーザーに認めています。クリーンなアプリの開発と提供は、サイバーセキュリティ企業の検証した明確なルールに従いアプリ ベンダーが行います。そのため、アプリの安全性が保証されています。

**マルウェアの徹底解説**

ウェブルートでは 2018 年、情報源と分析の増加に努めました。管理者向けに提供できる情報が増えれば増えるほど、企業を守る力が強まるためです。今年は、マルウェアの検出されたマシンの数やマルウェアが潜んでいそうな場所など、新たなデータを盛り込んでいます。

## 一度感染したデバイスの半数以上が年内に再度感染していました。

2018 年は、マルウェアの 93% が 1 台の PC でしか検出されなかったこと、感染したマシンの半数以上 (54%) が年内に再度感染していたことがわかりました。一度でも感染したことのある消費者のエンドポイントのうち 39% 以上が 2 度～ 5 度感染しており、この割合は企業のエンドポイントでは若干低く 35% でした。

これは、複数のポリモーフィック型ファイルが個人デバイスを攻撃した結果だと考えられます。また、インストールされたばかりのウェブルート保護機能が、PC が現在、複数のウイルスに感染していることを検出することもひとつの理由です。PC の複数感染の報告が多いもうひとつの理由として、一部のマルウェアによる複数ファイルのドロップも挙げられます (19 ページの「スイス アーミー ナイフ」のセクションを参照してください )。ここで重要なのは、一度感染したエンドポイントは年内に再度感染する可能性があるため、管理者は常に警戒しておく必要があるという点です。

## 2018 年は検出されたマルウェアのおよそ 54% が %appdata% フォルダと %temp% フォルダに潜んでいました。

何度も感染を繰り返す原因は大抵の場合、行動にあります。ゲーム チートやアクティベーション キーなどを入手するために動画共有サイトを頻繁に訪れるユーザーなら、これらのサイトがほぼ間違いなく感染していることを知っています。うっかりしていてバンドルされているソフトウェアを回避するのを忘れて、信用できないアプリをインストールするような行動も感染を何度も繰り返す原因です。

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

今年のレポートでは新たに、マルウェアのインストール場所の説明を追加しています。データのコンパイルにあたっては、各 Windows オペレーティング システムと各バージョンのパスを標準化してつじつまの合ったパス ビューを作成し、新種ファイルとの遭遇件数とマルウェア検出率に基づき割合を算出するという方法を使用しました。そして分析に基づき、%appdata% や %temp% などマルウェアの潜んでいそうな場所をいくつか突き止めました ( ただし現実的には、マルウェアはほぼどこにでも潜んでいる可能性があります )。図 4 に詳細を示しています。

| マルウェア インストール先 | % |
|---|---|
| %appdata% | 29.4% |
| %temp% | 24.5% |
| %cache% | 17.5% |
| %windir% | 12.3% |
| %desktop% | 6.1% |
| %programfiles% | 4.4% |
| その他 | 5.8% |

図 4: マルウェアのインストール先としてよく使われる Windows マシン上の場所

%appdata% ディレクトリは場所が重要視される良い例です。マルウェア開発者は大抵の場合、アプリケーション設定やファイル、アプリ固有のデータなどが格納されている、Windows PC 上の %appdata% フォルダ サブディレクトリに主要な起動アプリケーションをインストールしようと試みます。当社が検出した悪意のある %appdata% ファイルの割合は消費者のシステムで 31%、企業ユーザーのシステムではわずか 24% でした。悪意のあるファイルが消費者のフォルダで多く見つかったのは、%appdata% の更新が新しくアプリをインストールするときしか行われないこと、そしてアプリ チャーン率が企業よりも消費者の方が低いことが理由だと考えられます。いずれにせよ、実行されると、これらのアプリが不正アプリである可能性は高く、消費者の PC は企業の PC に比べ一般的にセキュリティが劣っているため、非常に危険です。

2018 年に検出された新種ファイルを検証した結果、%appdata% 以外にも次のフォルダにマルウェアが潜んでいました。

» %temp% – 企業 30%、消費者 23%、全体で 24.5%
» %cache% – 企業 11.3%、消費者 19.2%、全体で 17.5%
» %windir% – 企業 19.2%、消費者 10.5%、全体で 12.3%

管理者の方には、%cache% や %temp% のディレクタ内での異常な動作を検出するポリシーを作成することをお勧めします ( 例 : これらディレクトリからはファイルが実行されないポリシーなど )。こうすることでマルウェアが自身を起動させる確率を 40% 以上減らすことができます。

全体の結論としては、マルウェアや PUA の感染事例はいくらか減少しているものの、これは問題がなくなったのではなく変化しただけで依然として厳重な警戒が必要だと言えます。全体的な減少傾向に貢献しているのは、オペレーティング システムのクリーン化と PUA インストールの複雑化に向けた取り組みです。企業の PC の方が消費者の PC よりも安全であること、また Windows 10 を実行している PC の方が Windows 7 実行 PC よりも安全であることは確かですが、職場への個人デバイスの持ち込みと企業ネットワークへの接続を認める傾向があることから企業のリスクも高まっています。

## ランサムウェアに何が起こったのか

2017 年はランサムウェア攻撃によって世界中が恐怖とパニックに陥り、企業がミッションクリティカルなデータを守ろうと慌てふためいたり、暗号通貨で何百万ドルもの身代金を支払わされたりしましたが、2018 年はこれとは大きく情勢が異なりました。ランサムウェアはセキュリティ対策を講じていない人たちから資金を搾取するには効果的ですが、最近はユーザー側もデータを安全な形でバック アップするなどしっかりしたセキュリティ対策を講じており、脅して身代金を巻き上げることが難しくなっています。そのためランサムウェアは従来以上に標的を絞った実行性に優れた冷酷な犯罪と化しています。

2018 年に起こったランサムウェア攻撃には、バルセロナ港やサンディエゴ港、ロングビーチ港、ブリストル空港、アトランタ国際空港など港や空港を狙った攻撃のほか、政府機関やヘルス ケア機関 ( 身代金 5 万 5,000 ドルを支払わされた米国の医療機関もそのひとつ [ii]) を狙った攻撃がありました。SamSam ( サムサム ) [iii] として知られるランサム攻撃でひときわ注目を浴びた事例では、米国をはじめ数々の国で何百ものネットワークが暗号化され、犯罪者が起訴されるまでの間に 600 万ドル以上もの大金がかすめとられました。被害者数 200 人あまりを出したこの攻撃の被害合計額は 3,000 万ドルを超えていました。サムサムではリモート デスクトップ プロトコル (RDP) が攻撃ベクトルとして使用され、RDP 設定の不十分なシステムを Shodan などのツールでスキャンするという手口が用いられました。セキュリティの不十分な RDP 接続を利用すればシステムにアクセスしたりシステム上のデータや共有ドライブを閲覧することが可能で、犯罪者はこれを利用して十分な情報を入手しランサムウェアやその他のマルウェアを仕掛けるかどうかを判断します。残念なことに何度にもおよぶ警告にかかわらず、RDP 接続を十分に保護していない企業がまだまだたくさんあります。

# 悪質な IP アドレス


ウェブルートが検出する悪質な IP アドレスは毎年何百万件にものぼります。これら IP アドレスはスパム送信やマルウェア配布、悪質なトラッフィクの起点の難読化などに使われます。さもなければ、消費者や企業のコンピュータを荒らし回ることが目的です。ウェブルートではこうした悪質な IP アドレスをアクティビティ別 ( スキャナー、プロキシ、スパム、Windows エクスプロイト、Web 攻撃、DoS 攻撃、ボットネット、フィッシング、モバイル攻撃 ) に追跡しています。危険をはらむ悪質な IP アドレスに対する最善の対策は、それらアドレスを自動的にブロックし被害が及ばないようにすることです。しかしそのためには、IP アドレスそのもの、そしてその場所、アクションに対する徹底的な理解が必要です。さもなければ先手を打つことができません。

2018 年に検出された悪質な IP アドレスのうち、スパムという理由で「悪質」に分類されたものは 82% もありました ( 図 5 を参照 )。この数字を見ただけで、以前よりスパムが増加していることがわかります (2017 年は検出された悪質な IP アドレスの 65% がスパムの送信元でした )。

悪質な IP アドレスに関連して頻繁に行われたその他のアクティビティとしては、オープン プロキシ 9% ( 匿名のトラフィックのパススルーを許可。匿名および Tor を含む ) やボットネット 4.3% ( 昨年の 3% から若干増加 ) が挙げられます。

スキャナーはわずか 2% でしたが、厄介な脅威であることに変わりはありません。スキャナーとは、ハッカーが環境をスキャンしネットワーク構成やインストールされているソフトウェア、ユーザーのデータなどといった詳細情報を入手し、環境ごとに攻撃をカスタマイズするという攻撃手法です。Windows エクスプロイトは昨年の 9% からわずか 1.1% へと激減しました。この減少の理由は Windows 10 への移行だと考えられますが、他にもうひとつ重要な理由があります。それはホワイト ハット スペースつまり Google Project Zero 内で行われるアクティビティで、このアクティビティのおかげで脆弱性の早期発見や公開性の向上、エクスプロイト キットの減少が実現しています。Windows エクスプロイトはオペレーティング システムやソフトウェア、ブラウザ、プラグインの脆弱性を利用するものであるため、マルウェア配布の


図 5: 2018 年に検出された悪質な IP アドレスの分類

エクスプロイト キットは今もまん延していますが、パッチがすべて適用されたシステムにはさほど効果がありません。バグ バウンティ プログラムや Google の Project Zero、自動ファジング ツールなどのおかげでソフトウェアは安全性と安定性の両面で非常に強化されており、これを感染ベクトルとして利用するのが難しくなっています。

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

## 何度もリストにあがった悪質な IP アドレスのトップ 25 は 95 回も使い回しされていました。

手段として今後もよく使われる方法であることに変わりなく、衰退を繰り返しながらもさらに大々的な標的型攻撃に使われるようになるだろうと予想されます。

重要なのは、IP アドレスは静的でないこと、無害から悪質、悪質から無害へとレピュテーションの状態が頻繁に変わることを覚えておくことです。2018 年に当社が検出した悪質な IP アドレス数百万件のうち、一度しかリストにあがらなかったものが全体の 60% を占めるものの、二度以上あがったものも莫大な数あります。何度もリストにあがった IP アドレスのトップ 25 は 95 回も使い回しされていました。IP アドレスはボットネットやスパム、スキャナー攻撃などを実行するために何度も使われます。別のレビューでは、193 件の IP アドレスで状態移行が 11,000 回以上も行われていたことがわかります ( つまり IP アドレスがボットネットに利用され、その後、無害な目的で利用される時期を経て、再びボットネットに利用されるというサイクルを一年の間に何度も繰り返したことを意味します )。なお、状態移行はスパムに使われた 8,704 件の IP アドレスで 18 万 5,000 回以上、スキャナーに使われた 4,848 件の IP アドレスで 10 万 3,000 回以上も行われていました。

この仕組みを説明すると次のとおりです。スパム メールを送信しているサーバーが検出され、その IP アドレスをスパム配布ノードとして特定します。この疑わしい動作を理由にこの IP アドレスをブラックリストに追加します。ただし、無期限に載せておくわけではなく、今なお悪質な動作を見せるか、ブラックリストの IP アドレス見直しを行います。見せない場合は、ブラックリストから削除します。ただしどの IP アドレスも動作履歴を記録します。この記録はレピュテーション スコアに影響します。新たな IP アドレスが何十万件もブラックリストに追加され、これらの追加と削除が日に何度も行われます。

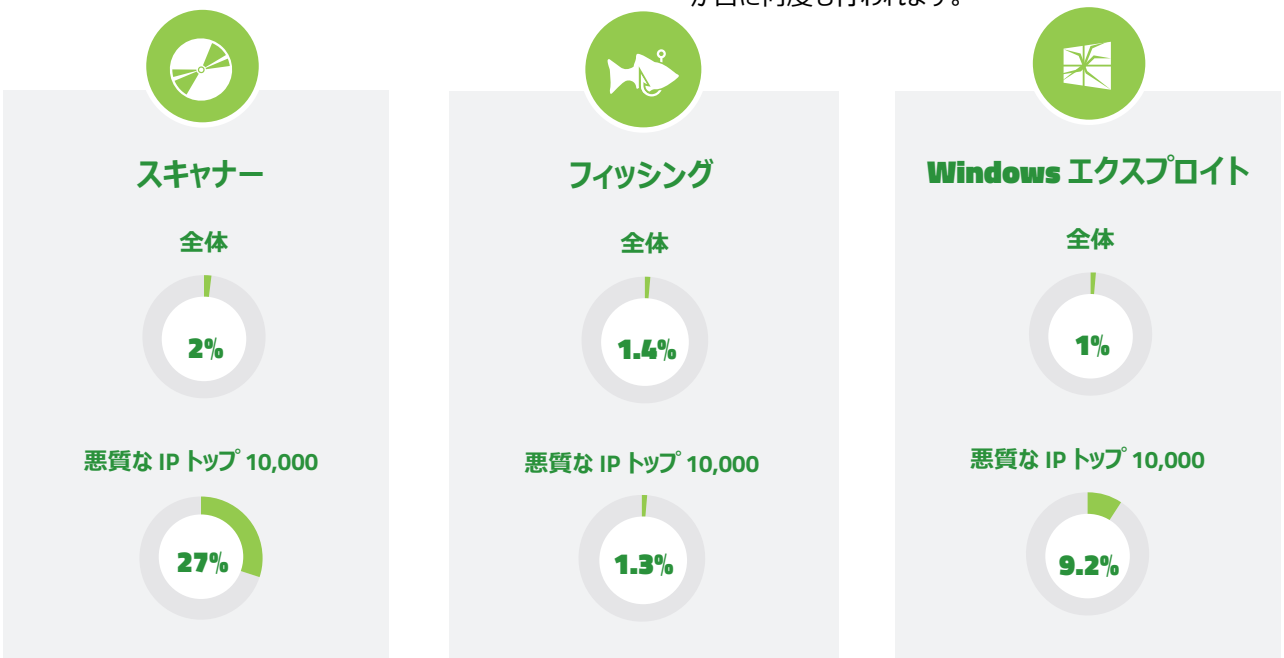
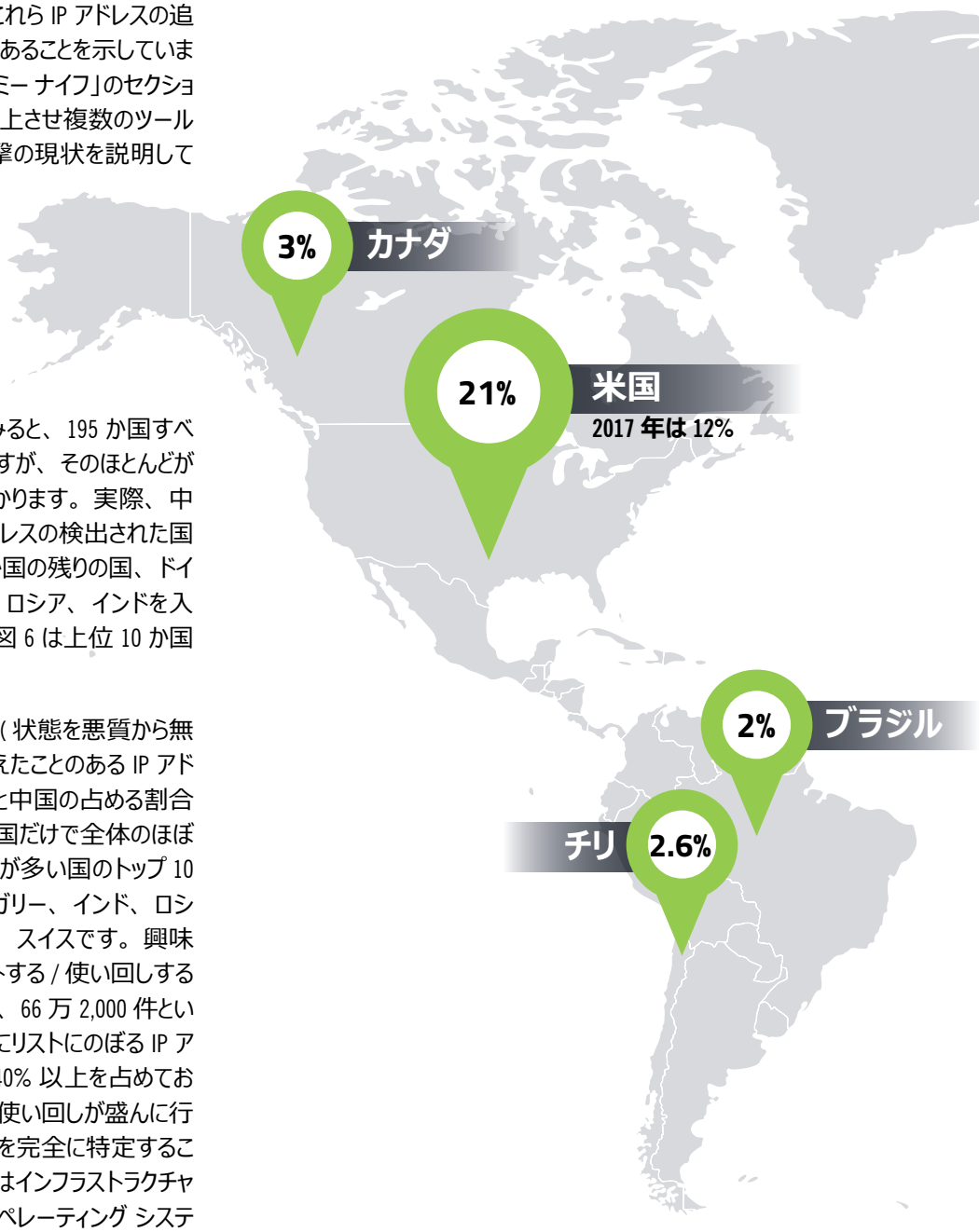



図 5: 2018 年に検出された悪質な IP アドレスの分類

同じ IP アドレスが後日、悪意のある目的で再び使用されるケースがよくありますが、当社が分析した IP アドレスのトップ 10,000 件でも、20 回以上「悪質」と記録されたものが 48.6% もありました。うち 150 件以上がブラックリスト掲載と削除を 50 回以上も繰り返していました。この回数を大幅に上回ったものもごくわずかでしたがありました (1.5%)。

興味深いことに、頻繁にリストにのぼる IP アドレス 10,000 件のうち、半数以上が複数の悪質アクティビティに使用されていました (Web 攻撃や Windows エクスプロイト、プロキシ、Tor など)。16 件は主要な悪質アクティビティ 6 種に、2 件は 7 種すべてに使用されていました。明らかに小数派ではあるものの、この多目的戦術は IP レピュテーション サービスに影響を及ぼすもので、これら IP アドレスの追跡、対処の方法を見直す必要性のあることを示しています。詳しくは 19 ページの「スイス アーミー ナイフ」のセクションを参照してください。アジリティを向上させ複数のツールを使用した手法へと移りつつある攻撃の現状を説明しています。




悪質な IP アドレスを地域別に見てみると、195 か国すべてにおいてアクティビティが確認されますが、そのほとんどが一部の地域に集中していることがわかります。実際、中国と米国、ベトナムが悪質な IP アドレスの検出された国の 60% 以上を占めます。上位 10 か国の残りの国、ドイツとカナダ、韓国、チリ、ブラジル、ロシア、インドを入れるとこの数字は 80% を超えます。図 6 は上位 10 か国を示した図です。

頻繁にリストにのぼる上位 10,000 件 ( 状態を悪質から無害、無害から悪質へと一度でも変えたことのある IP アドレス ) に絞って分析すると、ベトナムと中国の占める割合が最も高いことがわかります。この 2 国だけで全体のほぼ 57% となります。リストにのぼる回数が多い国のトップ 10 は、ベトナム、中国、米国、ハンガリー、インド、ロシア、フランス、マレーシア、ブラジル、スイスです。興味深いことに、悪意のある目的でホストする / 使い回しする IP アドレスの数が多い国はベトナムで、66 万 2,000 件という異常な多さです。ベトナムは頻繁にリストにのぼる IP アドレスという点でも上位 10,000 件の 40% 以上を占めており、このことはベトナムで IP アドレスの使い回しが盛んに行われていることを示しています。理由を完全に特定することはできませんが、おそらくベトナムではインフラストラクチャの老朽化や旧式、安全性の低いオペレーティング システム (Windows XP など ) への過度の依存、法執行力の弱さなどが理由で、企業ネットワークに侵入しやすいのだと考えられます。

# 中国と米国、ベトナムが悪質な IP アドレスの検出された国の **60% 以上** を占めます。

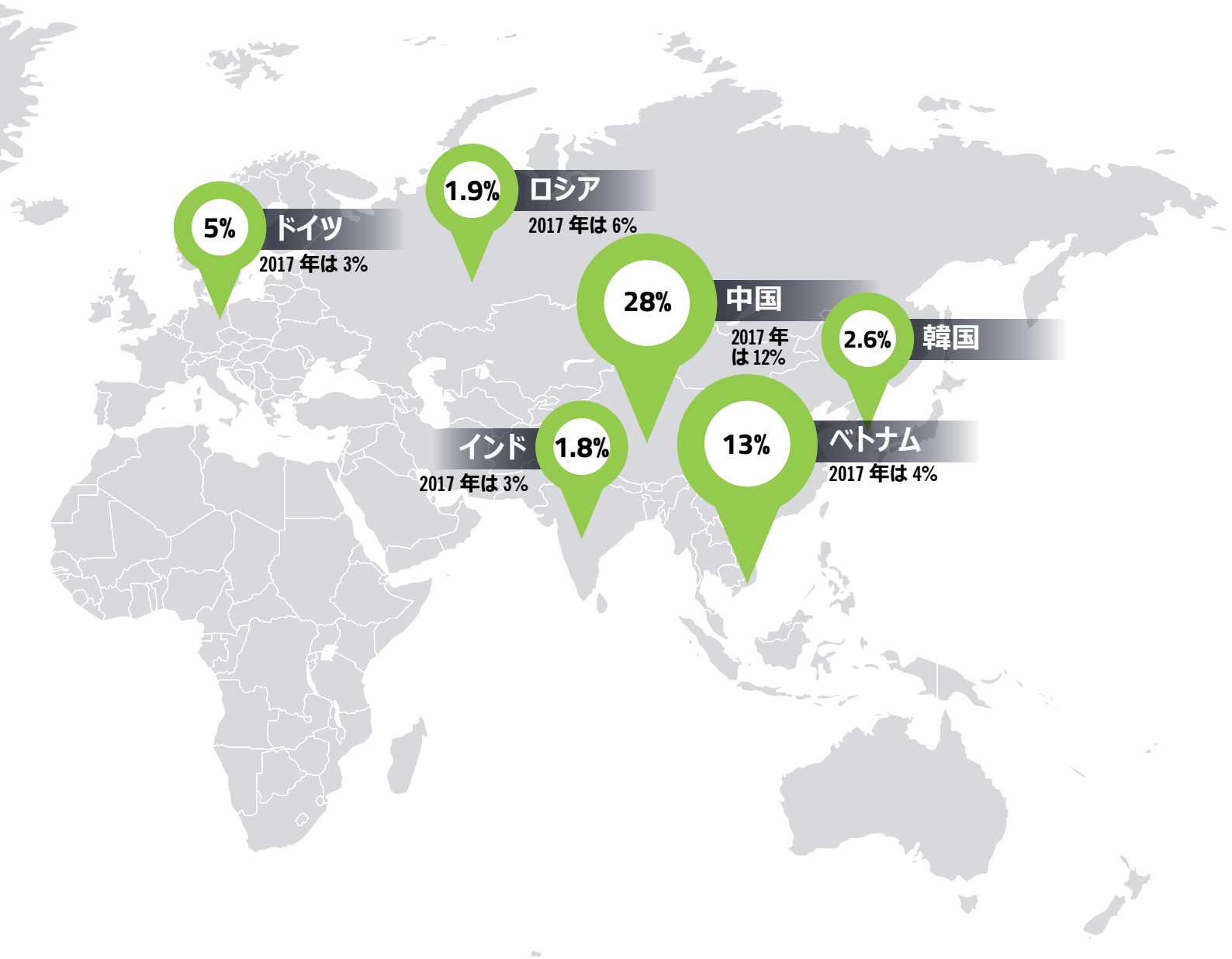
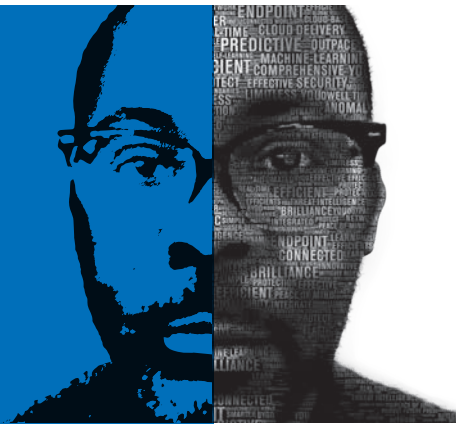



図 6: 悪質な IP アクティビティが検出された国トップ 10

# 高リスク URL



ウェブルートがこれまでに分類した URL は 320 億件を超え、当社では引き続き、それらの履歴や運営期間、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、動作を検証しています。分類は各 URL の主な目的 ( ショッピング、アダルト サイト、ギャンブルなど ) と悪意の種類 ( フィッシング、ボットネット、マルウェア サイト、スパム サイトなど ) 別に行います。この情報は Webroot BrightCloud® の Web クラシフィケーション サービスや Web レピュテーション サービスを通じてネットワークやセキュリティ ベンダーへと提供され、組織による Web ポリシーの設定、ユーザー保護に役立てられます。

## 2018 年 1 月から 12 月にかけて検出されたフィッシング サイトの数は 220% 増加しました。

ウェブルートが 2018 年に分類した URL は数百万件、そのうちおよそ 3% が高リスクに分類されました。とりわけ 1 日あたりのフィッシング サイトの数がこの一年の間に 2 倍以上増加しました。ボットネットの数は上下しましたが、10 月と 11 月に急増が見られ、これは Emotet ( 詳細は 19 ページの「スイス アーミー ナイフ」のセクションを参照 ) などの感染力の高い攻撃に関連していると考えられます。アクティビティ レベルが上下した原因のひとつとして時期を狙ったものである ( 新学期やクリスマス時期に攻撃数が増加 ) ことが挙げられます。

高リスク URL の中でもマルウェアは間違いなく関心が非常に高いカテゴリーです。その理由はクリプトジャッキングとクリプトマイニングの流行です。訪問者のハードウェアから暗号通貨を採掘するこうしたサイトはウェブルートによって検出された悪質 URL の大多数を占めます。最近強化された追跡機能を使えば、この数はこれまでの数をはるかに超えることでしょう。

### クリプトジャッキングとクリプトマイニング

クリプトジャッキングとは、Web コンテンツに埋め込まれたスクリプトからブラウザベースのプログラムを実行することで、未使用の CPU を利用しユーザーに気づかれぬ間あるいはユーザーの同意を受けることなく暗号通貨を採掘することです。クリプトマイニングとはマルウェアをインストールし、これを使って CPU を占有して暗号通貨を採掘することです。どちらの手法もランサムウェア攻撃より金儲けしやすく違法行為の形跡が小さいことから急増しており、大きな脅威となっています。この種の攻撃でよく指定される暗号通貨はモネロです。その理由はいくつかあります。モネロでは、リング署名という画期的な方式を使用して取引元を隠し、追跡不可能な状態が生じます。この状態でモネロ ウォレット アドレスへと支払いを要求し、受け取った資金を取引所に送金して現金化します。洗浄の必要もありません。

クリプトジャッキングが出回り 1 年以上になり、一般の方々もその存在や対策を理解しておられるようです。しかしながら、ブラウザのアドオンでブロックするという方法はあまりにも初歩的過ぎます。脅威は刻一刻と進化しています。犯罪者がドメイン難読化を始めると、そのようなアドオンでは対抗しきれずリアルタイムの脅威インテリジェンスでなければクリプトジャッキングを効果的にブロックすることができなくなるでしょう。

**タイラー・モフィット | セキュリティ アナリスト**

# 2018 年中にクリプトジャッキングを使用した URL は数百万もありました。

洗浄の必要のない追跡不可能な取引方式を使用する以外に、モネロは ASIC 抵抗を維持する数少ない暗号通貨のひとつでもあります。大半の暗号通貨はプルーフ オブ ワーク システムを利用していますが、ブロックの採掘に使用されるアルゴリズムは特定のアルゴリズムをハッシュし特定の暗号通貨を採掘するために設計された特殊チップ (ASIC) によって実行されます。Bitmain などの企業は、効率が非常に高く消費者グレードの CPU や GPU を使えなくする ASIC マシンを構築して成功しています。モネロ開発チームは ASIC 抵抗を維持するためにアルゴリズムの継続的な変更に取り組んでいます。言い換えれば、PC の消費者グレードの CPU と GPU を使用すればモネロ採掘で大儲けできる可能性があり、しかも近い将来これが実現するということです。ただし、どちらの攻撃も暗号通貨の価格大変動を受け頻度という点で上下しています。この一年、暗号通貨市場の時価総額が 85 ～ 90% 下落したことが原因です。

いずれにせよ、2018 年は次のような強盗やハッキング、マイニングなどの大事件がニュースに取り上げられました。

» 武装集団が暗号通貨投資家や投機家の要人を狙った強盗事件が相次ぎ、総額何百万ドルもの大金が脅し取られました。中には殺害事件に発展したケースもありました。[iv]
» 2018 年前半に約 7 億 3,100 万ドル相当の暗号通貨が暗号通貨取引所から盗み出されました。[v]

2018 年は暗号通貨の価格下落にかかわらず、こうした攻撃手法を用いるサイトの数が激増しました。電気料金の負担も、違法マイニングに伴いハードウェアにもたらされた多大なストレスの責任も被害者側が負うため、攻撃者側のコストはただも同然で、攻撃を仕掛けるや否や金儲けすることができます。いくらかでも価値がある限り、金儲けの方法として依然として大きな魅力があるのです。昨年前半に当社が検出したクリプトジャッキング URL の数は 9 月から 12 月にかけて 2 倍以上も増加しました。クリプトジャッキングは PC を感染させる必要なく金儲けできることから、依然としてよく使われます。2018 年は Web ベースのクリプトジャッキング機能を提供する新たなサイトのいくつかで盛んに競い合いが行われました。これまで長い間、実質的に活動していたのは Coinhive 1 社のみでした (2017 年に新種の攻撃法を開発した会社 )。Coinhive は今なお市場シェア 80% 以上と大きな勢力を誇りますが、Coinhive のスクリプトを模倣した Cryptoloot や JSEcoin、Deepminer、Coinimp、Minr、Omine など新たなクリプトジャッキングスクリプトも頻繁に使われ始めています。

これら URL の訪問を試みたウェブルート エンド ユーザーのクリプトジャッキング検出率を見ると、2018 年のクリプトジャッキング発生件数は 9 月 ( 図 7 を参照 ) の急増にかかわらず着実に減少していることがわかります。 年間を通して見ると、1 月は 11%、12 月はわずか 5% となっています。この減少の理由はおそらく、暗号通貨価額の下落とネットワーク レイヤーでの検出機能とブロック機能の向上にあると考えられます。

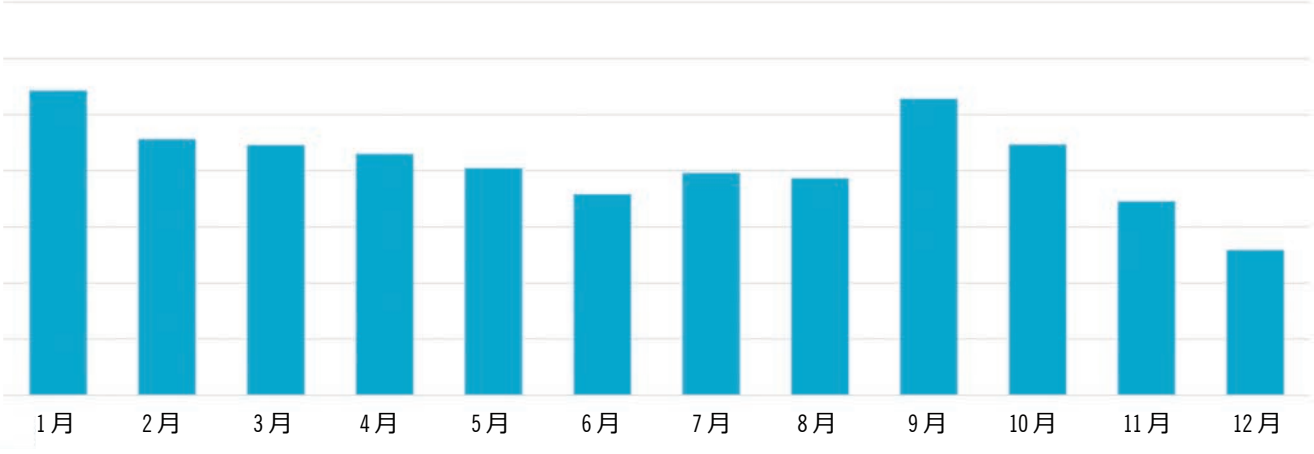



図 7: 2018 年全体のクリプトジャッキング検出率

当社ではまた、クリプトジャッキング実行時のブラウザの保護機能向上も確認しています。ただし、難読化による検出回避という新たな方法で犯罪者側が対抗してくるため、ブラウザやエクステンションによるクリプトジャッキング防止機能の有効性は将来低下すると考えられます。

マイニングはある意味、クリプトジャッキングより融通が利き金儲けしやすい方法です。それは、ユーザーがたとえ乗っ取りサイトから移動したとしても被害がそこで止まらず、JavaScript の制限による抑圧が簡単でないためです。クリプトマイニングは執拗さと難読化を武器に、CPU アイドル中に CPU を実行して負荷が増加していることを巧みに隠します。流通しているモネロ全体の 4.3% 以上が被害者のハードウェアから違法に採掘されたものです。[vi] また、2018 年にボットネット (19 ページの「スイス アーミー ナイフ」のセクションを参照してください) がクリプトマイナー ペイロードをドロップし、そのとき XMRig が指定されたことも注目すべき事実です。マイニングはユーザーの同意や意思に関係なく実行できるため、ミッションクリティカルなデータが見つからない場合やランサムウェアが適切なオプションでない場合に金儲けするための方法となります。

### 国別の悪質 URL

悪質な URL が圧倒的に多いのは米国で全体の 63% を占め、続いて中国が 5%、ドイツと香港がそれぞれ 4% となっています。ロシアとオランダはそれぞれ 3% でした。

これまでとの大きな相違点はマルウェアをホストするサイトの大多数が米国内にあることです ( 米国が占めた割合は 2016 年は 22%、2017 年はわずか 12%)。割合が劇的に増加した理由は米国内の非常に多くのサイトがクリプトジャッキングに感染しているか利用されていることです。

### URL の難読化

ボタンやハイパーリンクをクリックするときに、クリック先がどこにとぶのかわからないことがあります。このようなことは企業や製品、サービスなどの詳細情報の入手先として「ここをクリック」が表示される場合など、悪意がなくても起こり得ます。ところが、URL の難読化はこれとは違い、ユーザーを悪質サイトや無害なサイトの悪質コンテンツに誘導するために頻繁に使われます。なんと、悪質な URL の 40% が良好なドメインで検出されたものです。これは、正規の Web サイトが感染し悪質コンテンツをホストしていることを意

## 2018 年はわずか 10 か国が高リスク URL の大多数をホストしていました。

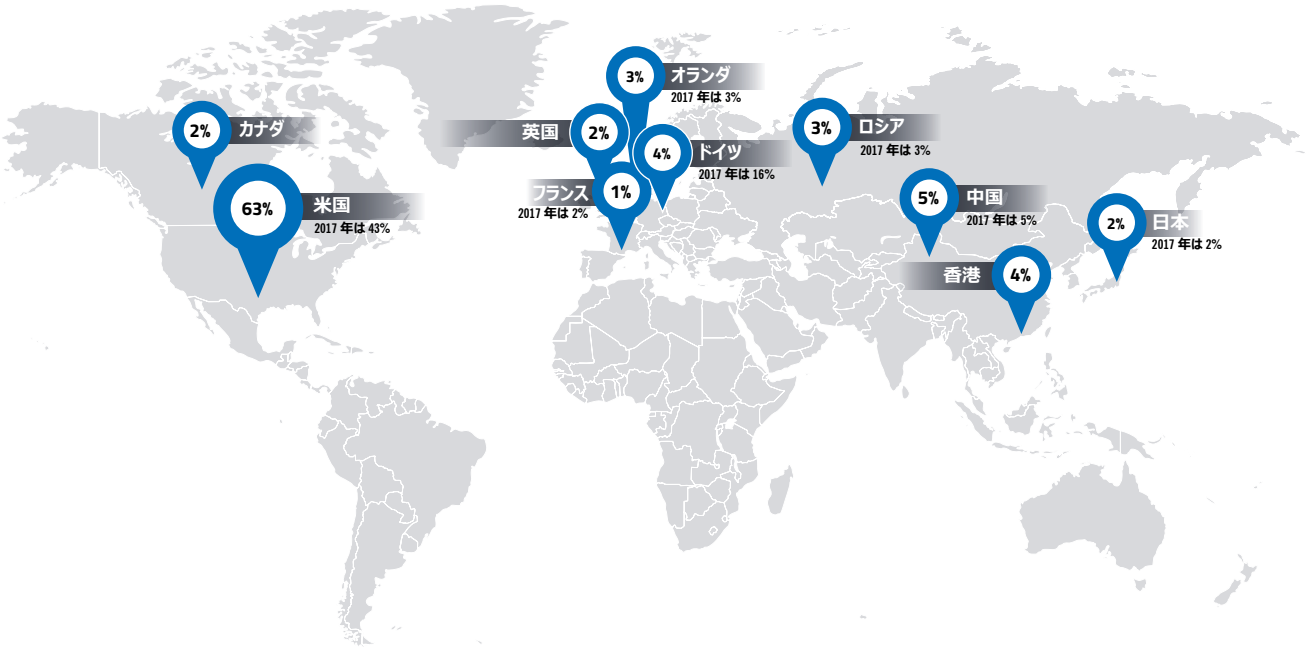



図 8: 高リスク URL の検出数が多かった地域

# なんと、悪質な URL の 40% が正規のドメインで検出されたものです。

味します。このような理由から、SSL 調査機能のない中間デバイスを使用している人は、セキュリティ ポリシーに抜け道がある可能性を重々承知しておく必要があります。

URL の本当のクリック先を隠すために最もよく使われる方法は URL 短縮ツールを使う方法とクラウド ストレージを使う方法の 2 つです。URL 短縮ツールは使いやすくコンテンツ投稿の文字数制限がある Twitter などのアプリケーションで便利なため、よく使われます。短縮された URL は本当のクリック先が明らかでないという危険をはらんでいます。また SSL を回避しブラウザ攻撃やワンクリック詐欺、DoS 攻撃などを実行するために使われることもあり、ユーザーやサーバーにもリスクをもたらします。[vii] ウェブルートでは何千もの URL 短縮ツールを評価、それに基づき短縮された URL がユーザーに大きなリスクを呈することを確認しています。その例として bit.ly や goo.gl が挙げられます。ユーザーは 130 分の 1 の確率で bit.ly をクリックし悪質サイトへと誘導されます。また goo.gl は 190 分の 1 の確率でクリックしています。ちなみに goo.gl は 2018 年 5 月、Google によって (Google ™ マップでの共有などわずかな例外を除き ) サービス中止となりました。短縮された URL の正当性確保という Google らの取り組みにもかかわらず、当社では引き続き何千もの悪質 URL を検出しています。

URL を隠すチャンスはデータがクラウドに保存されている場合にもあります。ユーザーがドメイン ( これ自体は無害 ) のリンクを入手する場合です。当社でこのような URL のパスを確認したところ、少なくとも 4 分の 1 が悪質コンテンツを含んでいました。これらドメインは既知のドメイン、信頼できるドメインであることから、ちらっと見ただけやドメイン名のみを確認するツールでは問題がないように見えます。しかしながら、このような信頼できるサイトが ( 検出されるまでのごく短い期間であっても ) 感染している可能性もあります。また、犯罪者はこのようにして検出を逃れられることを知っています。たとえば Photobucket のアカウントが感染すると、このアカウントは悪質なファイルを配布するホストとして使われることになります。

これは URL ホワイトリスト機能のみに頼るのではなく、URL レベルのインテリジェンスを活用することが重要であることを強調する例です。ウェブルートではパス全体を評価し、ユーザーが悪質 URL にさらされるリスクを取り除きます。

# フィッシング攻撃と URL


## 2018 年のフィッシング攻撃の件数は 2017 年に比較し全体的に 36% 増加しました。

フィッシング攻撃はこれまでと同様、企業と消費者の両方を狙う最もよく使われる攻撃手法のひとつです。2018 年の 1 月から 12 月にかけてのフィッシングサイト検出件数は 220% 増加しました。これは 2017 年に比較し、攻撃件数が全体で 36% 増加したことを意味します。ほとんどのフィッシング攻撃は金融機関へのなりすましです。フィッシングの標的とされた企業全体のうち、金融機関が占めた割合は 77% でした。興味深いことに 2018 年は、20 もの業界がフィッシングの標的となりました。金融以外にも標的とされた割合が高かった業界は、決済サービス業 (4.78%)、暗号通貨業と小売業 ( どちらも 2.53%)、政府機関 (2.25%) でした。その他にもソーシャル メディアやストリーミング、SaaS、医療機関、宅配サービス、ギャンブル、ファイル ホスティング、教育機関、保険業などが標的となりました。

> 私の予想では、暗号通貨がフィッシング攻撃の標的の大多数を占めると思います。その理由は人的ミスの影響を受けやすい取引所や Web ウォレットを使用している標的が多数あることです。
>
> **タイラー・モフィット**
> **セキュリティ アナリスト**

なりすましの対象として狙われるサイトは年々変わるものの、Google、Microsoft、Dropbox、Paypal、Apple、Facebook、Yahoo など 2017 年にリストにあがった名前の多くが 2018 年も引き続きトップ 10 に名を連ね、これに Adobe と Bank of America が加わりました ( 図 9)。

とりわけ Dropbox はなかなか良い標的で、Dropbox の認証情報を狙ったフィッシング攻撃では、そこに格納されている金融口座やその他個人情報などといった消費者や企業の機密データに不正アクセスできるほか、マルウェアをホストすることも可能です。企業の管理者アカウントに入り込んだ犯罪者は知的財産や暗号鍵など何でも盗み見することができます。そうすると、膨大な量の機密データやミッションクリティカルなデータを盗まれることになります。

視野をもう少し広げフィッシング攻撃の標的とされた企業トップ 20 を見てみると、Netflix や Target、Amazon など新たな名前が加わっていることがわかります。Netflix になりすますことでどのような利益が得られるのか首を傾げたくなると思います。ところが、ユーザーにはパスワード使い回しの癖があるため犯罪者はこれを利用し、( フィッシング攻撃の標的となっていることが ) わかりにくいアカウント タイプを狙うことで認証情報を入手し、そこから銀行のサイトやその他金儲けができるサイトへと入り込むのです。犯罪者はどのブランドにも Web サイトがあることを知っています。ユーザーがあちこちのサイトでパスワードを使い回せば、一度フィッシング攻撃を仕掛けただけで大金を手にすることができます。ただし Amazon を標的としたフィッシング攻撃はこの域を超えており、その脅威は Prime アカウントへのアクセスにとどまりません。Amazon Web Services (AWS) アカウントのマスター キーにアクセスされると、企業のクラウド インフラストラクチャ全体を盗み見されます。これが深刻な事態に発展することは言うまでもありません。

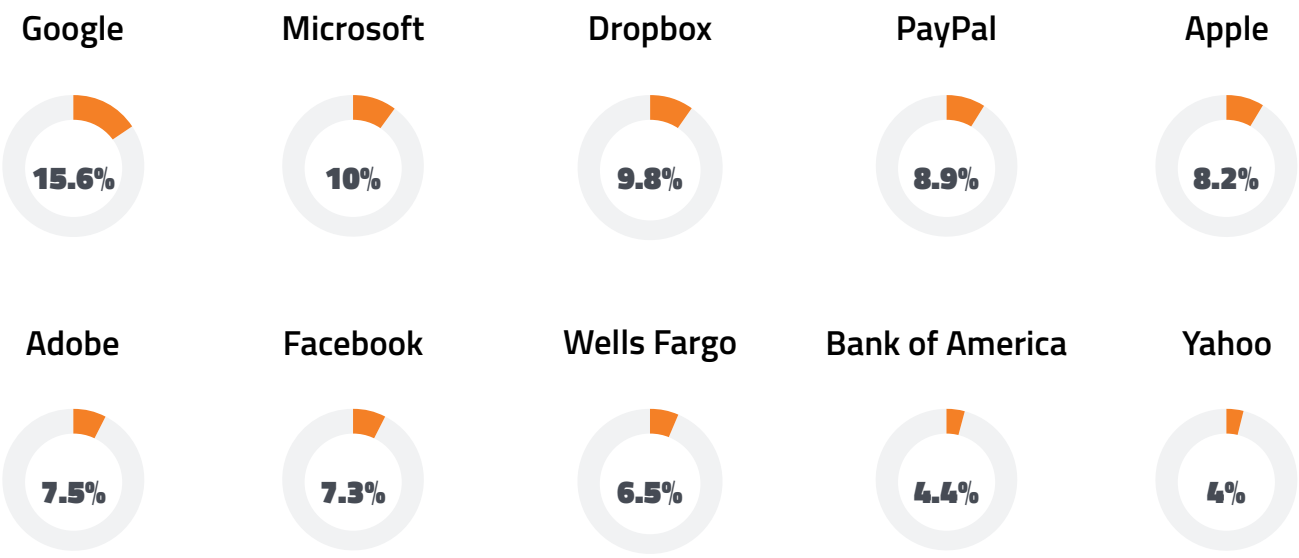



図 9: なりすましの対象となった企業トップ 10

## ユーザーのセキュリティに貢献する HTTPS、しかしそこでも注意が必要です

HTTPS はユーザーを保護するために作られたもので、ブラウザとサーバー間を行き来する機密情報を暗号化し盗聴を防止します。ユーザーは、ブラウザ バーに鍵マークの付いたサイトは信頼でき安全だということを知っています。ところが、新たなセキュリティ対策が発明されると、犯罪者はそれを利用する方法を考え出すもので、SSL 証明書を悪質な Web サイトに追加し、安全なサイトに見せかけます。SSL 証明書は、信用できない証明書発行機関や乗っ取られた認証局からなら簡単に入手できます。その結果、一部のフィッシング サイトでは HTTPS 鍵マークが年中表示されるようになりました。

フィッシング攻撃の標的となったサイトを当社が検証したところ、どの標的に対しても HTTPS ホスティングが使われていることがわかりました。この割合は金融機関で最も高く、SunTrust Bank になりすましたフィッシング攻撃の 87% が HTTPS 攻撃でした。ちなみに BNP Paribas は 66%、Wells Fargo は 47% でした。これとは対照的に Google はわずか 17% でした。この数字から、SSL 証明書を取得しブラウザ バーに鍵マークを付けてユーザーを「安心」させることが簡単だということが伺えます。フィッシング攻撃が増加しているうえに HTTPS を使用した見かけ上安全な URL が使用されていることは、リアルタイムのフィッシング対策技術を導入し被害を受ける前に攻撃を検出し阻止することの重要性が高まっていることを示しています。

## 「スイス アーミー ナイフ」アプローチによる攻撃

犯罪者は常に失敗から学びもっと巧妙な新しい手口を考え出し、サイバー攻撃を実行します。ある方法がうまくいかなくても他の方法があるのです。いくつもの手法を採用し攻撃の成功率を高める、いわゆる「スイス アーミー ナイフ」アプローチが増加しているのはそのためです。

その代表例は Emotet です。Emotet は成功率が極めて高いポリモーフィック型トロイの木馬で、コンピュータ緊急事態対策チーム (CERT) によると「政府 ( 州、地方、部族、領土 ) をはじめ民間企業、公共機関を狙う被害額、破壊度とも最大のマルウェア」とされています。[ix] 2014 年に発見されて以来、バンキング型トロイの木馬からさまざまと姿かたちを変えて存在しており、いくつもの攻撃ベクトルを使うマルウェアへと進化しています。このマルウェアは受信者の知っていそうなブランド名で、マクロを含んだ文書が添付されたスパム メールを送り付け、これを開かせマシンを感染させるという手口を使用します。最近の攻撃キャンペーンでは、偽の Paypal 受領書や発送通知、支払期日の過ぎた請求書が使われていました。ユーザーが添付文書を開くとマクロが実行されて Emotet がダウンロードされ、脆弱性や弱いパスワードに付け込みながらマルウェアがネットワーク上の他の PC へと拡散します。特に古いシステムや旧式のシステム、パッチが適用されていないシステムはボットネットの温床となり、どんどんと拡散していきます。Emotet はブルート フォース攻撃などを仕掛けてドメインの認証情報を入手し、自身のコピーを作りながらネットワーク内を移動し電子メールの認証情報を次々と盗み出します。そしてスパム キャンペーンで次なる被害者の受信トレイへと入り込みます。

2018 年 9 月から 10 月にかけて検出されたフィッシング ドメインの 93% が HTTPS サイトを提供していました。[viii]

## 受講する価値が実証された セキュリティ意識向上トレーニング

容赦なく襲ってくるフィッシング攻撃。これを阻止するためには、セキュリティ意識向上トレーニングを提供することが大切です。その際、トレーニングの一貫性と提供頻度に注意することが劇的な結果を生み出す鍵を握っています。年に 1 ～ 2 度のトレーニングでは思うどおりの結果が出せません。それは、攻撃者が常に手法や手口を変えており、それに合わせ、セキュリティ意識向上トレーニングもシミュレーションや関連題材を取り入れていく必要があるからです。2018 年の Webroot® セキュリティ意識向上トレーニングのデータを見ると ( このトレーニングではトレーニングにフィッシング シミュレーションを組み合わせセキュリティの強化とリスクの低減を目指しました )、シミュレーション キャンペーンを開始したばかりの企業ではクリック率が 29.32% でした。この率は定期トレーニングを組み合わせることで 70% も下がります。トレーニングによって従業員がフィッシング メールの不正リンクをクリックする確率がこれほど大きく低下するのです。

月 1 度のトレーニングで最も良い結果が出ているのは興味深い事実です。キャンペーン回数 1 ～ 5 回の企業はクリック率が 28%、6 ～ 10 回後には若干下がり 24%、ところが 11 回以上すると 8.5% と驚くような結果が出ています。ウェブルート セキュリティ意識向上トレーニングなどといったプラットフォームがユーザー教育を通して、影響の最も大きなときに ( つまりフィッシング シミュレーション メールのリンク クリック直後 ) サイバー脅威のリスクとコストを軽減できるのは明白です。

**エンド ユーザーがフィッシング詐欺に引っ掛かる確率はトレーニング受講後 12 か月の時点で、70% も低下します。**


図 10: キャンペーン回数別に見た平均クリック率

Emotet の目的は、スパム ボットネットのゾンビ数を増やし認証情報を収集したり他のマルウェアの配信経路として働くことです。「ポリモーフィック型マルウェア」のセクションで説明したとおり、Emotet の産物は普通、%appdata% の Local ディレクトリや Roaming ディレクトリの任意のパス内にあります。

Emotet は昨年、能力、範囲ともに勢力を拡大し、世界中の企業を次々と攻撃しました。ペイロードの配信がものすごい速さで行われることから、キャンペーン運用のいくつかのステップが自動化されていることがわかります。また多層的となり執拗さと回復性も高まっています。被害者のルーターをコマンド＆コントロール (C2) インフラのプロキシ ノードに変えることのできる、ユニバーサル プラグ アンド プレイ (UPnP) モジュールも使用されています。その他にも電子メール ハーベスティング機能などが使用されており、被害者のマシンに格納されている Outlook メール数百万件ものコンテンツを盗み出すことができます。[x]

**一回のマルウェア キャンペーンにフィッシングやスパム、トロイの木馬、ボットネット、クリプトマイニング、脆弱性攻撃などさまざまな攻撃が組み込まれています。**

Emotet はいくつかのメジャーなマルウェア キャンペーンで配信経路として使用されています。そのひとつ Trickbot でも必ず Emotet が使われています。Emotet が感染し拡散すると Trickbot が情報を盗み出し資金を要求するという構造です。Trickbot は、レベル 1 の C2 インフラに Tor サーバーが追加されたことで、攻撃モジュールや Web インジェクションの拡散に使用されるサーバーが長期間にわたってアクティブな状態を維持できるようになりました。[xi] また、暗号化ランサムウェアやその他バンキング型トロイの木馬をドロップすることもあります。ユーザーがバックアップしている場合に備えてランサムウェアと一緒にクリプトマイナー ペイロードをドロップすることもあります。金儲けできるよう常に別のオプションを用意しているのです。

このように、たったひとつの攻撃ベクトルを使うのではなくなり、マルウェアの回復性を強化し、検出されにくくし、長続きさせることに犯罪者が力を入れていることは明白です。

# 悪質なモバイル アプリ

2017 年現在、Android™ スマートフォン ユーザーが約 1 万 2,500 万人おり[xii]、潜在的に有害なアプリまたは PHA が優勢 (Google のレポートによるとスマートフォン ユーザーが PHA をダウンロードする確率は 0.02%[xiii]) であることから、米国では非常に多数のデバイスが感染します。実世界の Android ユーザー数百万人を対象とした当社の分析でも同様の数字が出ています。実際、2018 年の 9 月から 12 月にかけての当社のデータでは、Android アプリは平均 0.22% ～ 0.62% がマルウェア、平均 0.04% ～ 0.13% が PUA だという結果が出ています。

悪質アプリはさまざまな形で活動します。その多くは Google の防禦策を回避することが目的です。TimpDoor キャンペーンがその一例で、これは米国内の電話番号とデバイスを狙い、これらをネットワーク プロキシに変えようとした事例です。これは、ボイス メッセージがありますという SMS メッセージをユーザーに送り付け、聞くにはあるアプリをダウンロードする必要があるというもので、このアプリは Google Play ストアのセキュリティ手順と保護対策を迂回します。これをダウンロードすると、ファイアウォールとネットワーク モニタを迂回して内部ネットワークへと入り込まれます。ウェブルートでは、お客様のデバイスにこのアプリがダウンロードされている事例を多数確認しています。このことから、ユーザーがこのようなソーシャル エンジニアリング キャンペーンにまだ騙されることが伺えます。Google が信頼されたソースか Google Play ストアからのみアプリをダウンロードするよう強く注意を呼びかけているにかかわらず、「未知のソース」からのインストールを有効にするオプションがあるのです。Google では、未知のソースからのインストールを有効にしたユーザーの方が信頼されたソースまたは Google Play ストアからのみインストールしたユーザーよりも感染率が高かったことを確認しています ( 前者の場合 2017 年の第 2 四半期の平均 0.65%、第 3 四半期 0.86%、第 4 四半期 0.92%、後者の場合それぞれ 0.08%、0.12%、0.09%)。

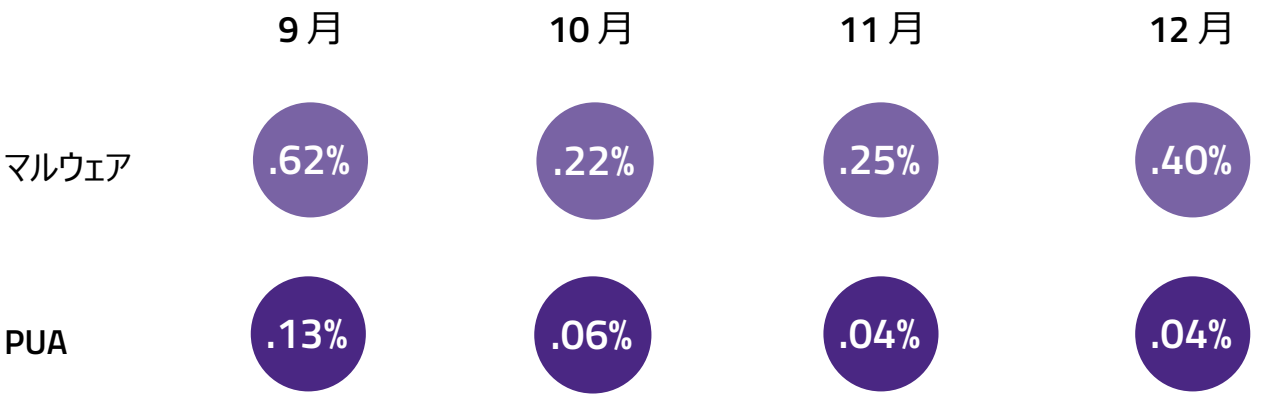



図 11: マルウェア または PUA と判断されたアプリの割合

# 2019 年の概要と予測


犯罪者は攻撃手法を組み合わせ大きな儲けを出すために、常に新たな方法、革新的な方法を模索しています。ウェブルートの 2018 年のデータを見ると、攻撃者が次から次へと攻撃ベクトルを変えていることがわかります。その第一の目的は金儲けです。当社が収集・分析したデータは、最新の脅威やアプローチに対応する多層防御の重要性を強調するものです。

» ポリモーフィック型マルウェアが依然として出回り、悪質な Windows 実行可能ファイル全体の 93% を占めます。

» 2018 年は、ランサムウェアは以前ほど問題ではなくなったものの、標的を絞ったものへと変わり始めました。コモディティ化された主なランサムウェアは 2019 年も引き続き減少傾向を見せますが、標的を絞った新たな亜種が出回り、被害に遭う企業もあるでしょう。

» クリプトジャッキングとクリプトマイニングは暗号通貨の激しい価額変動にかかわらず、儲けの量という点でランサムウェアを上回り、手っ取り早い金儲けの方法となっています。当社では、2019 年もこの傾向が続きクリプトジャッキングとクリプトマイニングが脅威の大半を占めると予想しています。ユーザー デバイスのハードウェアを利用する攻撃のおそらく半数程度が暗号通貨の採掘となるでしょう。

» 引き続き高リスク IP アドレスの使用や使い回しが行われ、ブラック リストに再三のぼるものが数百万はあるでしょう。その大多数がスパム サイトですが、ボットネットやスキャナーもかなりの数となりそうです。動的に更新される IP アドレスのリストとコンテキスト分析が危険な IP アドレスに対する最善の対策となるでしょう。

» 2018 年に当社が分類した数百万件の URL から、フィッシング サイトやスパム サイト、ボットネットが非常に流行していることがわかりました。悪質 URL の 40% が正規のドメインで検出されたもので、ユーザーにはクリック先が無害なのか悪質なのかが簡単にはわからない状態でした。当社の予想では、2019 年もこの傾向が続きます。ユーザーを守るためには、URL レベルの可視性または正確に危険を示す優れたドメイン レベルの指標を備えたソリューションを導入する必要があります。

» 2019 年はルーターや IoT を標的とした攻撃が増加するでしょう。すでにその実例が確認されており、MikroTik 製ルーター 40 万台以上が世界各地で乗っ取られモネロ採掘を実行しています。[xiv] 家庭用ルーターは要注意です。ネットワークやスマート ホーム デバイス (IoT) のハブとして機能しますが、その動作を確認しようとしてもほとんどの場合 Linux ベースのルーターにはログインすることができません。その間にハッカーはユーザーの環境を知り尽くし、URL をリダイレクトして中間者攻撃を実行します。ジャッキング スクリプトをインジェクトすることもあります。

私の予想では、非公開台帳と流用可能性という理由で引き続きモネロがサイバー犯罪の指定暗号通貨となるでしょう。SamSam の犯罪者が起訴されたのは、FBI が取引所まで捜査し身代金の支払い先となったアドレスをすべて追跡できたためです。ビットコインは匿名性が低く、犯罪者はこれに対応すると思われます。

**タイラー・モフィット | セキュリティ アナリスト**

リプトジャッキング、クリプトマイニング、悪質なモバイル アプリ、標的型フィッシング、ランサムウェア攻撃など、ソーシャル エンジニアリングを使用して人間の本質を悪用する脅威の数々。それらは洗練されアジャイルで革新性に優れています。このことは常に防御策を新たにする必要があることを物語っています。攻撃者が「スイス アーミーナイフ」アプローチを使うのなら、企業も多層的なセキュリティ戦略を採用してこれに応じる必要があるのです。ユーザーを最新の脅威から守るには、継続的に更新される脅威インテリジェンスとコンテキスト分析、高度なエンドポイント、ネットワーク プロテクションに基づく自動化されたリアルタイム ツールが必要です。また、常に最新の内容を取り入れたセキュリティ意識向上トレーニングを適切な時期に提供する必要もあります。このようにツールとトレーニングを組み合わせることで、企業は許容しがたいリスクにさらされる危険性を実質的に軽減することができるのです。

## データについて

本年次脅威レポートで使用しているデータは、弊社のクラウドベースの高度機械学習アーキテクチャである Webroot® プラットフォームにより自動的に取り込まれて分析された指標から導き出されたものです。このシステムは、既知の脅威だけでなく、ゼロデイ脅威、これまでにない脅威、および APT 攻撃のすべてからユーザーとネットワークを保護する積極的な保護対策を提供します。このプラットフォームで生成される脅威インテリジェンスは、Webroot® エンドポイントセキュリティ製品、および Webroot BrightCloud® 脅威インテリジェンス サービスを介してテクノロジー パートナーによって使用されています。弊社の脅威インテリジェンスは、すべての IPv4 および使用中の IPv6 スペース、数十億もの URL、数千万もの新規および最新版モバイル アプリ、そして世界中のすべての ウェブルート保護下にあるエンドポイントの可視性に基づいています。高度な機械学習技術、信頼度を伴うリアルタイムのスコア判定、および継続的な更新により、ウェブルートの脅威インテリジェンスは洗練された高度な脅威の識別とそれからの保護において非常に効果的に機能します。ウェブルートでは、膨大なデータを処理する能力、入手可能な最先端テクノロジーの独自の実装、強力なコンテキスト分析エンジンをもとに、機械学習に対して独自のアプローチを採用しています。コンテキスト化とは、インターネットのオブジェクト同士を結ぶ「連座制」モデルと考えることができます。確認したインターネットの各オブジェクトについて大規模な範囲でその特性を取り込むことで(1 オブジェクトあたり最大 1 千万個の特性 )、オブジェクトの正確な分析時における脅威の有無を判断することが可能になります。特許取得済みの弊社のアプローチでは、複数のベクトル間で攻撃と脅威の動作を対応付けて、URL、IP、ファイルおよびモバイルアプリ間の関係を分析します。たとえば、連絡先リストにアクセスしてそれを特定の IP アドレスに転送しようとするモバイルアプリをユーザーが実行した場合、そのアプリによる悪質な動作が当該 IP アドレスのレピュテーションスコアに反映されます。オブジェクト間の現在の関連付けと、数百万にものぼるオブジェクトの長期間にわたる動作を相関させる能力により、ウェブルートの脅威インテリジェンスの優れた予測能力が実現します。

[i] www.appesteem.com

[ii] US hospital pays $55,000 to hackers after ransomware attack.ZDNet、2018 年 1 月。www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators

[iii] Wanted by the FBI: SamSam subjects.FBI、2018 年 11 月。www.justice.gov/opa/press-release/file/1114746/download

[iv] Town, Sam.Physical Bitcoin Attacks and Burglaries on the Rise.CryptoSlate、2018 年 7 月。cryptoslate.com/physical-bitcoin-attacks-and-burglaries-on-the-rise

[v] $731 Million Stolen from Crypto Exchanges in 2018: Can Hacks be Prevented? Bitcoin Exchange、2018 年 7 月。www.ccn.com/731-million-stolen-from-crypto-exchanges-in-2018-can-hacks-be-prevented

[vi] S. Pastrana, G, Suarez-Tangil. A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth. Cornell University、2019 年 1 月。arxiv.org/abs/1901.00846

[vii] A. Newmann, J. Barnickel, U. Meyer. Security and Privacy Implications of URL Shortening Services. RWTH Aachen University、2011 年。pdfs.semanticscholar.org/e9a0/8f1bc561310db382bdacbb397b4ca005b9bb.pdf

[viii] 2018 Phishing and Fraud Report: Attacks Peak During the Holidays. F5 Labs、2018 年 11 月。2018 Phishing and Fraud Report: Attacks Peak During the Holidays

[ix] Alert (TA18-201A).US-CERT, United States Computer Emergency Readiness Team. 2018 年。www.us-cert.gov/ncas/alerts/TA18-201A

[x] Emotet Malware gang is mass harvesting millions of emails in mysterious campaign. ZDNet、2018 年 10 月。www.zdnet.com/article/emotet-malware-gang-is-mass-harvesting-millions-of-emails-in-mysterious-campaign

[xi] Advisory: Trickbot Banking Trojan. National Cyber Security Centre、2018 年 9 月。www.ncsc.gov.uk/alerts/trickbot-banking-trojan

[xii] Insights into the 2.3 Billion Android Smartphones in Use Around the World. New Zoo、2018 年 1 月。newzoo.com/insights/articles/insights-into-the-2-3-billion-android-smartphones-in-use-around-the-world/

[xiii] Google Android Security report 2017: We read it so you don’t have to. ZDnet、2018 年。www.zdnet.com/article/google-android-security-report-2017-we-read-it-so-you-dont-have-to-and-here-are-the-takeaways

[xiv] 415,000 routers infected by cryptomining malware – prime target MikroTik. ETHNews、2018 年 12 月。www.ethnews.com/researchers-claim-400-000-mikrotik-routers-infected-with-mining-malware

## ウェブルートについて

ウェブルートは、サイバー脅威からの企業および個人ユーザーの保護にクラウドおよび AI ( 人工知能 ) を取り入れた初めてのサイバー セキュリティ会社です。ウェブルートでは、マネージド サービス プロバイダーや中小企業のお客様に向けて、エンドポイント プロテクション、ネットワーク プロテクション、セキュリティ意識向上トレーニングなど、最高のセキュリティ ソリューションを提供しています。Webroot BrightCloud® 脅威インテリジェンス サービスは、Cisco、F5 Networks、Citrix、Aruba、Palo Alto Networks、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、ウェブルートはインターネットの安全に寄与しています。ウェブルートは米国コロラド州に本社を置き、北米、ヨーロッパ、アジア地域においてグローバルなビジネスを展開しています。Smarter Cybersecurity® ソリューションについては webroot.com をご覧ください。

〒107-0062 東京都港区南青山3-13-18 313南青山8F ウェブルート株式会社 TEL 03.4588.6500 www.webroot.co.jp