WEBROOT®
Smarter Cybersecurity®

2018年度版ウェブルート脅威レポート

内容

資料作成 :

Nicholas Duran | Jurijs Girtakovskis | Ken Jacobi | David Kennerley | Justine Kurtz | Grayson Milbourne | Tyler Moffitt | Cameron Palan | Steve Snyder

はじめに

ハル・ロナス | 最高技術責任者

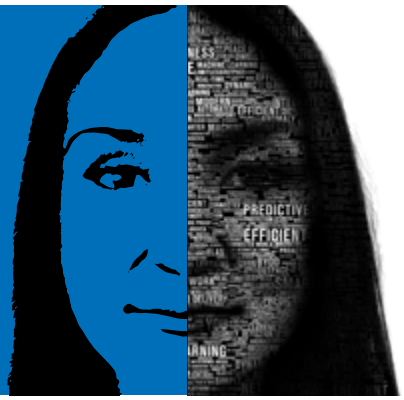
2017 年に行ったマルウェアやその他の脅威に関する弊社の分析ではっきりとしたことを 1 つ挙げるとすれば、サイバーセキュリティでは変化が絶え間なく起こり続けているということです。重大な脅威の識別およびブロックにアナリスト、リサーチャー、セキュリティ企業が迅速に対応する中、攻撃者側も同様に、防御を回避する新たな方法をすばやく考え出しています。フィッシング攻撃は標的をより絞るようになったことで成功率が高まり、多くのフィッシングサイトは 4 ～ 8 時間しかオンライン上に存在していません。ランサムウェア攻撃と同様に、匿名で行うことができ、比較的簡単に利益を上げることができるクリプトジャッキングも勢いを増しています。昨年中には多くのニュースとなり世間を騒がせました。高リスクな IP アドレスは、セキュリティステータスを無害と悪質の間で頻繁に変えることで検出を逃れる傾向が続いています。悪質なアクティビティに関連付けられることが多い上位 10,000 個の IP アドレスについては、年間で平均 18 回もそのステータスを変えています。攻撃の質と量が進化し続けている中、リアルタイムの脅威インテリジェンスを備えたセキュリティソリューションの必要性はさらに高まっています。

ウェブルートは、脅威に満ちあふれ不安定な現在の環境において、後手に回る対応のみでは企業やユーザーを保護することができないことを熟知しています。それが、弊社が独自の積極的な防御方法を考案した理由です。特許取得済みの機械学習技術により、世界中から集められた現実世界のリアルタイムのデータが分析、相互の関連付けが行われ、リアルタイムの脅威検出および自動対応だけでなく、新しい脅威が発生するであろう場所を予測することが可能になります。

蓄積し続けている膨大な履歴データと脅威の傾向を精査することで、ウェブルートは攻撃者の思考や、彼らがどのように防御回避の方法を考案して採用するかを読み解きます。そこで得られた情報を脅威インテリジェンスに採り入れ、ウェブルート全製品の基礎とすることで、この危険に満ちたインターネットを保護します。

ウェブルート脅威レポート 2018 では、2017 年の脅威活動に関する発見と分析の要点をご紹介し、最新のサイバー犯罪を回避するための知識を読者の皆様に提供いたします。

ウェブルートの見解



本レポートに含まれる統計データは、数百万の稼働エンドポイント、センサー、サードパーティデーターベースおよびセキュリティパートナーから収集された数十億におよぶ情報を統合するWebroot® 脅威インテリジェンスプラットフォームにより自動的に検出、分析、コンテキスト化された脅威インテリジェンス指標に基づいています。ウェブルートの脅威研究チームは、以下を含む幅広い脅威アクティビティに関連するデータを調査しました。

- マルウェアと潜在的に望ましくないアプリケーション (PUA) の傾向
- IP アドレスとそのセキュリティ上の影響
- ランサムウェアとクリプトジャッキングに関する最新の傾向
- URL レピュテーションと分類が攻撃への対処に役立つ仕組み
- フィッシング攻撃の進化
- モバイルアプリケーションの脅威

今年のレポートには新たにいくつかのセクションを加えました。今日の脅威に関する事実と予測に加え、セキュリティ全体に対してWindows® 10 移行が担っている役割についての詳細な調査結果を提供し、企業内での家庭用デバイスの使用に関して、見逃しがちな潜在的影響について説明します。またエンドユーザーに対する意識向上トレーニングの重要性についても言及し、企業によるリスクの軽減およびソーシャル エンジニアリングによる影響の削減を支援して、新たな脅威となりつつあるクリプトジャッキングの最近の増加傾向についても調査します。クリプトジャッキングについては、モバイルデバイス、Web、エンドポイントのセキュリティにそれがおよぼす影響、さらにはこの悪質なサービスからどのように利益が生まれるのかについても説明します。

脅威およびサイバー犯罪に対するウェブルートの脅威調査チームの分析および考察は、今日のユーザーが直面している脅威を明らかにし、今後に向けてこのような脅威に効果的に対処するための十分な知識を読者の皆様に持っていただくことを目的としています。

ウェブルートでは継続的に 1 日 3 回インターネットの 95% を分類・数値化

270

億以上の URL

6

億以上のドメイン

43

億以上の IP アドレス

150

億以上のファイル動作レコード

6,200

万以上のモバイルアプリ

5,200

万以上の接続センサー

亜種戦略：継続的な傾向

直近の 2、3 年間、亜種マルウェアおよび潜在的に望ましくないアプリケーション (PUA) の広がりが劇的に増加し、これらがサイバー犯罪者にとってマルウェアを侵入させる人気の手段であることを示しています。ウェブルートで調査した悪質な実行可能ファイルの実に 94% 以上が亜種でした。ポリモーフィズム (亜種戦略) とは、多数のユーザーに送られたマルウェアの単一インスタンスを名前、暗号化キー、シグネチャ、またはハッシュを使用して検出する従来のアンチマルウェアソリューションを回避するよう設計された戦略を指します。亜種マルウェアおよび PUA ではこれらの識別情報が常に変化するため、既存の定義ファイルでは新しく生まれた亜種に対してマッチングすることができません。パターンマッチングを採用しているセキュリティ製品ではシステム侵入前に未知の亜種を検出できないため、攻撃者は、それらの製品による保護を回避する有効な手段として亜種マルウェアを利用しています。

悪質な実行可能ファイルの 94% が亜種。

Webroot SecureAnywhere® エンドポイントプロテクションでは、毎年膨大な数の新しい実行可能ファイルが確認されています。新しい実行可能ファイルの数は実際に増えていますが、マルウェアまたは PUA と判断されるファイルの数は減少傾向にあります。2017 年に確認したこれまでに検出されたことのないファイルのうち、2% がマルウェア、1% 未満が PUA でした。2016 年にはそれぞれ 3% および 2%、2015 年にはそれぞれ 4% および 7% であったことと比較すると、2017 年の数値が非常に低いものであることがわかります。

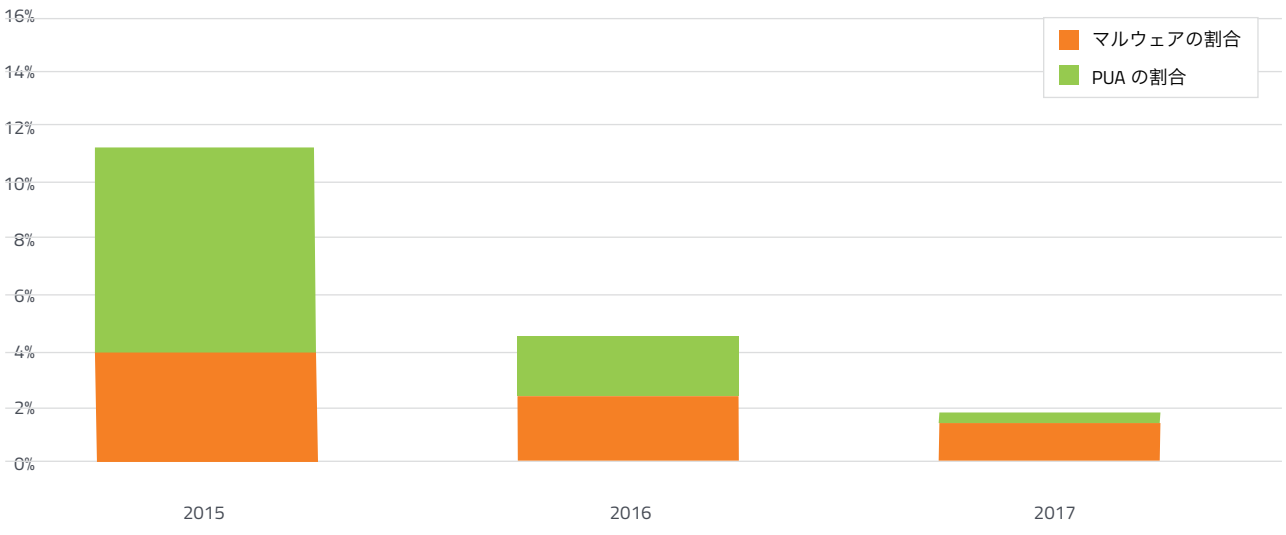


図 1: マルウェアまたは PUA と判断された新しい実行可能ファイルの年別の割合

2017 年にはマルウェアの 93% が固有の種。

1 デバイスあたりのマルウェアファイルの平均数にも同様の減少傾向が年々見られます。2016 年にマルウェアインシデントの平均数は 1 デバイスあたり 0.66 件でしたが、2017 年には 1 デバイスあたり 0.48 件に低下しました。企業と家庭のエンドポイントを分けて見た場合は、より顕著な変化が見られました。家庭の 1 デバイスあたりのマルウェアインシデントの平均数は 2016 年には 0.59 件でしたが、2017 年には 0.53 件まで低下しました。一方ビジネスデバイスについては、2016 年は 0.61 件、2017 年には 0.42 件でした。

これらのデータが示す印象とは裏腹に、マルウェアと判断されるファイルの割合の低下がマルウェアによる脅威が減少していることを示しているわけではありません。新しいマルウェアおよび PUA の数について、上述の数値が示すように大幅に増加が止まったことに関しては数多くの理由が考えられます。まず第一に、劇的な増加が見られた年は、攻撃者が従来のマルウェアおよび PUA の開発からより自動化された亜種ファイルの開発技術に移行していた時期であり、それによって、頻度に応じて迅速にブロックされる単一の実行可能ファイルとは異なる、数多くの固有の実行可能ファイルが開発されていました。大多数の攻撃者が亜種マルウェアの技術に移行した時点で、増加率の減少が見られ始めました。次にウェブルートでは、悪質な URL 経由でエンドポイントに転送される実行可能ファイルをブロックするなど、悪質なアクティビティをキルチェーンの早期段階で検出する技術や、悪質な実行可能ファイルによるエンドポイントへのさらなるファイルのダウンロードを回避する技術を強化してきました。ウェブルートは追加の実行可能ファイルがエンドポイントに到達するのを効果的に防ぐことができるため、これらの実行可能ファイルは統計には含まれていません。ウェブルートをご利用のお客様に到達する新しいマルウェアの量が減少したことは良い傾向ですが、企業のお客様はマルウェアを引き続き大きな脅威として捉える必要があります。第三に、マルウェアの配布がより困難になったことが挙げられます。2017 年 7 月に発生した RIG Exploit Kit によるテイクダウンや、2 月の Gmail による JavaScript の禁止など、2017 年に発生したエクスプロイトキットの変化および主要なテイクダウンによってマルウェアの配布が困難になる環境が形成されました。

減少に関して推測される最も重要な理由の一つに、従来のシステムより大幅にセキュリティ機能が強化された Windows 10 オペレーティングシステムへの移行が挙げられます。それでもなお、可変性に富んだ性質を持つマルウェアの増加を予測することは不可能に近く、大きなニュースの発生や季節の出来事 (例 : ホリデーショッピング、新学期、確定申告)、その他の要因によっても影響を受けます。

亜種マルウェアおよび PUA が依然として幅広く蔓延していることを確認するためには、単一のマシン上にのみ存在するファイルの数に注目すること、そして将来出現するであろうインスタンスの検出のためにウェブルートによって数十万ものルールが作成されている環境であっても、各ファイルが固有の亜種であり以前には確認されていないことを示す必要があります。2017 年には、検出したマルウェアの 93%、PUA の 95% が単一のマシン上でのみ確認されました。これは、悪質もしくは望まれないファイルの亜種を作り出すことが主流となっていることを明確に示しています。この統計データにより、ハッカーが既存の種の使用をやめて新しい亜種を開発・使用するサイクルの速さが明らかになりました。

OS 別の亜種の傾向

ウェブルートでは、マルウェアまたは PUA と判断された新しいファイルの割合の安定した減少傾向に伴い、亜種による攻撃を使用する傾向の強さを数年間にわたって確認しています。この減少傾向をより詳細に調査するために、ウェブルートでは今年、企業および家庭のデータの違いについてより深い洞察を得るための分析を強化しました。ウェブルートの調査によると、新しいマルウェアファイルおよび PUA の割合の減少に関する比較的重要な原因の一つとして、安全性が大幅に強化された Windows® 10 への移行が挙げられます。

2017 年 1 月の時点ではウェブルートが確認したシステムの 49% が Windows 10 を実行していましたが、現時点ではこれを実行するシステムは過半数 (54%) にまで増加しました。他のバージョンについては、Windows® 7 (33% 未満)、Windows® 8 (8%)、Vista® (1%)、XP® (1% 未満) となっています。全体的には、旧バージョンや将来のサポートが保証されないバージョン、または安全性が低いバージョンの OS から離れる強い傾向が見られました。しかしながら、詳細に調べてみると、普及率 (およびその結果) において企業と家庭の間に驚くべき違いがあることが明らかになりました。企業により制御および管理されているデバイスに加えて、多くの企業ユーザーは個人のデバイスを業務で使用しているため (企業ネットワークにアクセス可能)、これら両方の環境を分けて追跡することが重要です。

企業が家庭の OS 移行を注視すべき理由

家庭による Windows 10 の使用が急速に増えていることは良い傾向ですが、企業で移行が遅れていることは良いニュースではありません。しかし、その理由は理解できるものです。Windows 10 に限らず OS 移行は大きな試みであり、『CIO Magazine』 の最近の記事によると、企業の組織全体を Windows 10 に移行する作業は複数年にわたるプロジェクトであると考えられています[i]。旧バージョンの Windows オペレーティングシステムを実行しているビジネスデバイスがある限り、企業はリスクにさらされていると考えるべきであり、ウェブルートが 2 番目に最も普及していると考える Windows 7 については、非常に脆弱であると言えます。

WannaCry ランサムウェアによる攻撃で被害を受けたほとんどすべてのデバイスは Windows 7 を実行しており、その攻撃のみで企業は 40 億ドルもの損失を被ったと推測されます。[ii]

加えて、企業が所有するデバイスだけでなく、企業データにアクセス可能な、脆弱なセキュリティ設定である可能性の高い個人のスマートフォンやタブレットなどを使用する企業ユーザーによる脆弱性も挙げられます。このようなデバイスでは、企業が所有または管理するデバイスと比べて、1 デバイスあたりのマルウェア発生率が非常に高いことがわかっています (個人の 1 デバイスあたりの年間平均感染件数は 0.55 件、ビジネス デバイスは 0.42 件)。PUA についても同様の統計が見られます。厳格な BYOD ポリシーを採用している企業であっても、個人所有のデバイスの正確で詳細なセキュリティのステータスを把握していない場合がほとんどです。Windows 10 ですべてのセキュリティ問題を解決できるわけではありませんが、Windows 10 の採用が正しい方向への一歩であることは間違いありません。行動分析および機械学習を採用した高度なエンドポイントプロテクションと Windows 10 を組み合わせることで、サイバー攻撃に対する企業の脆弱性を大幅に減少させることができます。

Windows 7 のおよそ 2 倍の安全性を備えた Windows 10。

ビジネス デバイス

企業においては Windows 10 の普及は緩やかであることが判明しています。2017 年 1 月の時点では、確認した企業のコンピュータの 20% のみが Windows 10 を実行しており、2017 年末までにこれが 32% まで増加しました。それとは対照的に、1 月の時点では 62% のシステムが Windows 7 を実行していましたが、年末までにはそれが 54% に低下しました。Windows 8 は 1 月に 5%だったのが 12 月には 4% に低下し、Windows Vista™ (1%) および XP (1% 未満) の両方ついては 2017 年末にはごくわずかな割合でした。

2017 年には 2016 年と比べて確認されたマルウェアファイルの数が低下しましたが、OS ごとに見ると興味深い数値が明らかになりました。2017 年にマルウェアと判断されたファイル全体において、Windows 10 システム上で確認されたものはわずか 15% でしたが、Windows 10 に次いで企業で採用されている Windows 7 システム上で確認されたものは 63% にもおよびました。Windows 10 システムを実行する 1 デバイスあたりのマルウェアファイルの平均数は 0.04 で、Windows 7 の 0.08 と比べると大きな差があります。

Windows 10 デバイスで確認されたマルウェアの量は、2017 年 8 月 (年間合計の 14%) と 12 月 (12%) に急増が見られたものの、年間を通して比較的安定していました。

PUA について OS との関係において見てみると、Windows 10 を実行する 1 デバイスあたりの PUA 数は、最も高かった 2017 年 1 月の 0.06 から 12 月の 0.01 と、大幅な低下を確認することができました。また、OS を考慮せずに見ても、1 デバイスあたりの全体の PUA インシデント数はピークであった 1 月の 0.69 から 2017 年末の 0.06 まで低下しました。

企業での OS 移行率は低い傾向にあります。ウェブルートが確認したところでは、2017 年末までに Windows 10 を実行するビジネスデバイスの割合はわずか 32% でした。移行にかかる人件費や労力などのコストが企業の低普及率の原因となっている可能性は理解できますが、毎日のように高まるリスクに常にさらされていることも企業は考慮する必要があります。

家庭用デバイス

家庭による Windows 10 への OS 移行については異なる様相を見せています。2017 年 12 月までに家庭用デバイスのおよそ 72% が Windows 10 への移行を済ませており、1 月には 65% であったことと比べて顕著な増加が見られます。Windows 7 については 1 月の 17% から 12 月の 15% に低下しており、Windows 8 についてはそれぞれ 14% から 11% とこちらも低下しました。ビジネスデバイスの場合と同様に、Windows Vista (2%) および XP (1% 未満) についてはごくわずかな数値となっています。

2017 年末の時点で、ビジネス以外の 1 デバイスあたりのマルウェア発生件数は、Windows 10 で 0.07 件、Windows 7 で 0.16 件、Windows XP で 0.17 件でした。ビジネスデバイスの場合と同様に、家庭用デバイスの場合でも Windows 10 が Windows 7 と比べて 2 倍以上安全であることが確認されました。2017 年の 1 デバイスあたりのマルウェアの量は安定して平均 0.55 ファイルでした。

PUA の量も 2017 年 2 月のピークを境に緩やかな減少傾向が見られ、1 デバイスあたりの最高値 0.33 PUA から 0.17 PUA へと低下しました。PUA についても、Windows 10 の 1 デバイスあたりの PUA 率は Windows 7 のものと比べて約半分でした。

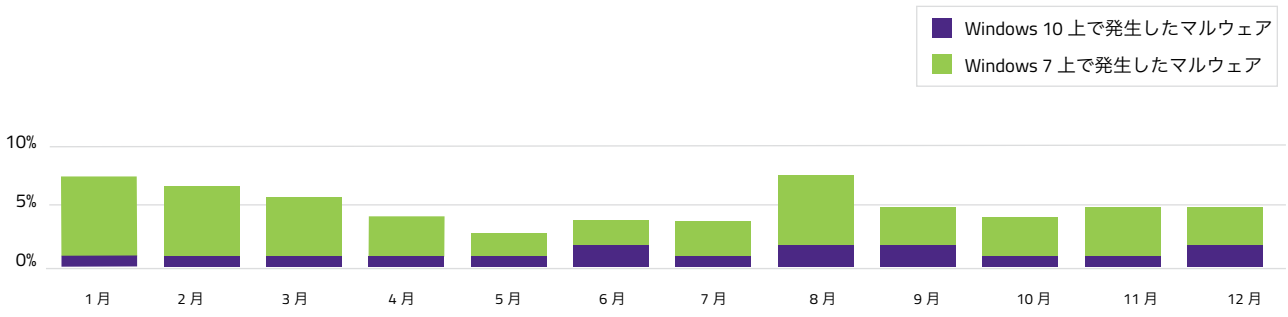


図 2: 2017 年にすべての OS 上で発生したマルウェア合計件数における、Windows 10 および Windows 7 デバイス上で発生したマルウェアの月ごとの割合 (%)

ランサムウェア、クリプトジャッキング、およびその他の脅威の傾向

ランサムウェアとその亜種は世界中で重大な脅威となっており、2017 年には、より感染力が高く大きな被害を与える、多目的のさまざまな新型亜種が確認されました。これまでで最も話題になった、最大規模の 2 つのランサムウェア、WannaCry および NotPetya は 2017 年に発生し、その洗練度は今までにないほど高度なものでした。両方を合わせると、ほんの 24 時間以内で 100 か国以上にわたる 20 万台以上のマシンに感染しました。これらの攻撃では EternalBlue エクスプロイトが使用され、Windows XP 以降で採用されている、基本的にはファイル共有に関連する脆弱性であるサーバーメッセージブロック (SMB) が標的となりました。侵入すると、このマルウェアはワームのようにネットワーク内を動き回って SMB を実行するコンピュータに到達します。感染したコンピュータには、ネットワークに直接接続していなくても、ネットワークに接続されていた他のデバイスに接続したものも含まれていました。

NotPetya の発生はその数か月後で、同じエクスプロイトを使用して、ウクライナの会計ソフトウェアのアップデートを感染源として最終的には世界中に広がりました。NotPetya はファイルを暗号化するのではなく、マスターブートレコード (MBR) を変更してハード ドライブ全体を暗号化することで、Windows OS を起動不能にするものでした。攻撃の目的は休日中のウクライナのインフラストラクチャに最大限の被害をもたらすこととされており、結果として複数の発電所や銀行、食料雑貨店チェーンが一時的に閉鎖に追い込まれました。世界中に感染が広がった後の報告では、推定被害額は 12 億ドル以上[iii] にもなるとされています。

長い間、ランサムウェアの配布においてはスパム電子メールキャンペーンが頻繁に利用されてきましたが、より簡単な方法として、セキュリティで保護されていないリモートデスクトッププロトコル (RDP) を使ったキャンペーンが感染拡大を目的として使われ始めました。サーバーや他のマシンをリモートで操作するための便利な手段である RDP には、すべての受信接続に対してポート 3389/TCP がオープンに設定 (1,100 万台以上のエンドポイントでそのように設定) されていたことや、管理アカウントのデフォルト資格情報を管理者が変更する必要がないこと、警告の発行やアカウントのロックアウト前のログイン試行回数を非常に多く設定できるなど、セキュリティ上の弱点がいくつも含まれていました。サイバー犯罪者は、多数のユーザー名およびパスワードを備えた特殊ツールを使用して最終的に侵入を試みます。侵入すると、別の特殊ツールやカスタムマルウェアを使用して、セキュリティソリューションを通過または無効にしようと試みます。攻撃者はネットワーク上の他のコンピュータも見ることができ、将来のキャンペーンのために情報を収集することができるため、RDP キャンペーンでは結果として非常に強い感染力を持つランサムウェアの拡散が最も多く見られました。利益目的か破壊目的かにかかわらず、ランサムウェアの新型開発により、サイバーセキュリティ業界は今後起こり得る世界規模の攻撃に備えて、ランサムウェアの役割および意図を再評価する必要性に迫られています。

ウェブルートのデータによると、他の攻撃よりも簡単に実行できながらもより高い収益性および匿名性を実現する可能性を秘めたクリプトジャッキングも本格的に普及し始めています。サイバー犯罪者は標的のファイルを盗んで身代金を要求するのではなく、標的となる CPU の処理能力を盗んで暗号通貨の採掘に使用します。マルウェアのペイロードが存在しないため、ユーザーはコンピュータが利用されていることに気付かないことがほとんどです。ウェブルートでは、CoinHive 社が暗号通貨モネロの採掘に JavaScript コードを使用し始めた 2017 年 9 月に、初めてクリプトジャッキングの存在を確認しました。Web サイトのオーナーに対して広告なしでサーバーコストを十分に賄える収入を得ることができるという宣伝文句をうたい、サイバー犯罪者は Web サイトをハイジャックして、サイバー犯罪者自身のモネロウォレットに収入を導くスクリプトを埋め込み始めました。(現在、モネロはホームユーザーの PC に搭載されている CPU でも最高の採掘パフォーマンスが可能で、取引の追跡を不可能にするプライベートのブロックチェーン台帳を利用するため、ビットコインよりも好まれる傾向があります。) 最近の暗号通貨の価格高騰も、犯罪者たちの間でこの種の攻撃ベクトルに人気が集まる要因の一つとなっています。2017 年 9 月以降、CoinHive 社を通して 5,000 以上もの Web サイトがこのモネロ採掘手法の被害にあっています[iv]。

第三の、そして最も危険性の高い傾向は、政府機関によるハッキングツールの拡散に関連するものです。2016 年から 2017 年にかけて「シャドーブローカーズ」と呼ばれるハッカー集団により官製ハッキングツールが流出しました。サイバーセキュリティにおいては、これらの強力なツールが悪の手にわたることは、核兵器の開発計画だけでなく高濃度ウランの輸送計画が同時に流出したほどの衝撃をもたらします。

2017 年に流行した最も高度な WANNACRY および NOTPETYA

100 か国

200,000 台のマシン

12 億ドル

NotPetya の推定被害総額

悪質な IP アドレス

毎年ウェブルートでは、弊社が悪質と判断する数千万にもおよぶ IP アドレスを確認しています。これらには、感染してスパム電子メールを送信するコンピュータ、匿名のトラフィックのパススルーを許可するオープンプロキシ、マルウェアを配布または DoS (サービス拒否) 攻撃を行うボットネットの一部として取り込まれた、セキュリティで保護されていない家庭用コンピュータや IoT デバイスが含まれています。これらに対する理想的な防御策は、被害を受ける前にこれらのアドレスからのネットワークトラフィックを自動的にブロックすることです。

2016 年と比べて 2017 年には悪質な固有 IP アドレスの大幅な増加は見られなかったものの、これらはいまだに数多く存在しています。ウェブルートでは悪質な IP アドレスからのさまざまなタイプの攻撃を追跡しており、これらをスパム、Windows エクスプロイト、スキャナー、ボットネット、DoS 攻撃、プロキシ (匿名および Tor を含む)、Web 攻撃、フィッシング、およびモバイル攻撃に分類しています。図 3 では、これらの悪質な IP アドレスの大多数がスパムサイト (65%)、スキャナー (19%) および Windows エクスプロイト (9%) であることを示しています。スキャナー攻撃は特に厄介な問題となる可能性があります。ハッカーはネットワーク環境をスキャンして、使用されているソフトウェア、ネットワーク構成、さらにはユーザーのデータなどを含む特定のデータを取得し、その環境に対してカスタマイズされた最も効果的な攻撃を仕掛けることができます。

Windows エクスプロイトは、多くの場合はユーザーからの積極的な介入を必要とせず、オペレーティングシステム、ソフトウェア、ブラウザ、またはプラグインの脆弱性を利用するため、マルウェア配布の手段として急激に人気が高まっています。ただし、より多くのユーザーが Windows 10 に移行するにしたがって、この手法の人気は低下するであろうと考えられます。

最も悪質な IP アドレスはわずか一握りの特定の国々を発生元としています。図 4 では、世界中のすべての悪質な IP アドレスのおよそ 62% が 10 か国から発生していることを示してます。残りの 38% には、悪質な IP アドレスが発見された 200 か国以上が含まれています。

図 3: 悪質な IP アドレス

悪質な IP アドレスの 84% はスパムおよびスキャナー。

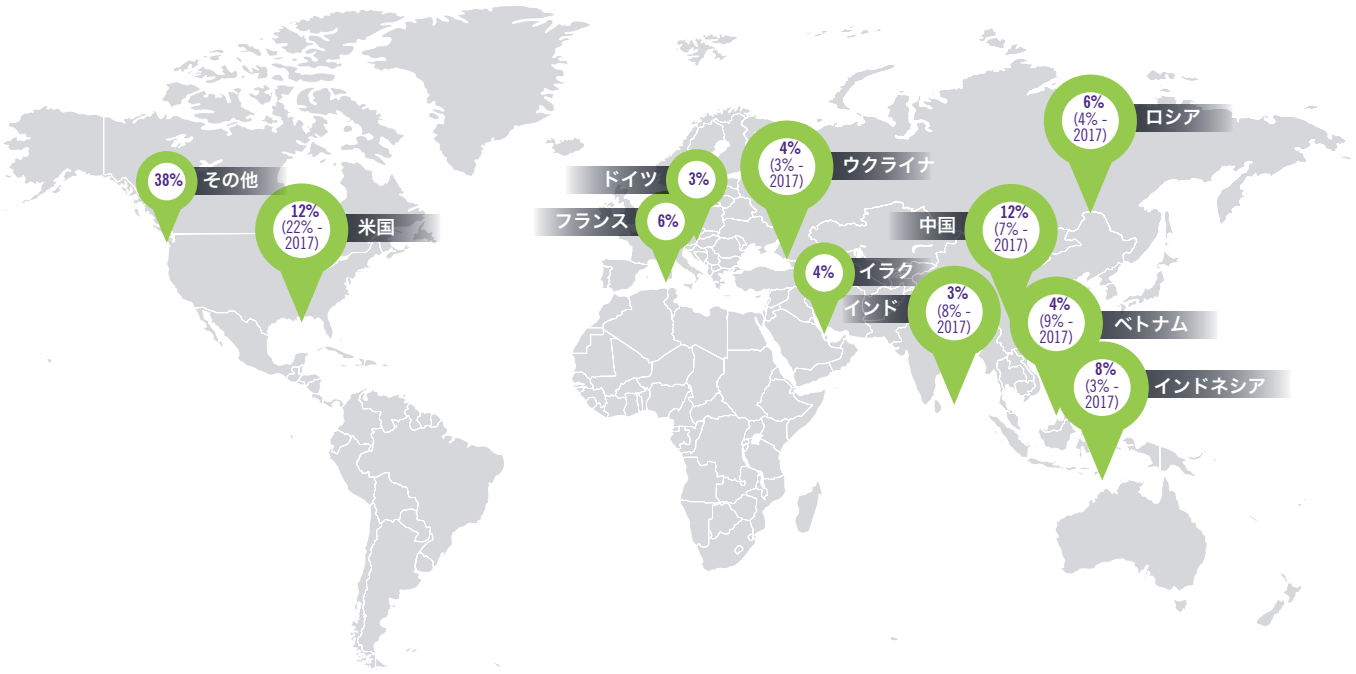


図 4: 国別の悪質な IP アドレス

米国 (12%) については、過去には悪質な IP アドレスの割合が最も高い数値を示していましたが、2015 年 (41%) から大幅に低下し、2016 年 (22%) にもその低下傾向が続きました。逆に中国は、2015 年に 9%、2016 年に 7%、2017 年には 12%を占めて、2017 年には悪質な IP アドレスによるアクティビティの大幅な増加が確認されました。ロシアについても、わずか 1% であった 2015 年から 2017 年には 6% に上昇するなど大幅な増加が見られました。ウクライナでも同様に大幅な上昇が確認され、4% に跳ね上がりました。インドは 2015 年には上位国の中でわずか 1% を占めるのみでしたが、その割合は 2016 年には 8% に上昇し、2017 年には 3% に低下しました。インドネシアでは 8% に上昇しました。イラク、ドイツ、フランスは今年に入って上位 10 か国にランクインしましたが、2016 年にはその数値は低いものでした。

攻撃のタイプは国別に多少異なることがわかっています。上位 10 か国から発生した、ブラックリストに指定されている IP アドレスの上位 10,000 個については、その 37% がスキャナー、続いて 34% がスパム、そして 21% が Windows エクスプロイトです。その多く (66%) は、脆弱性スキャナーおよびフィッシングサイトの両方として機能するなど、複数の攻撃を行うものでした。米国、中国、フランス、インドネシア、ロシアの 5 か国は、ウェブルートによって確認された去年のスキャナー攻撃の 47% 以上の割合を占めており、インドネシア、中国および米国はスパム攻撃の 31% 以上の発生元となっています。ボットネット攻撃については中国が単独で 40% 以上の割合を占めました。

また、IP レピュテーションは一定ではないことに注意する必要もあります。悪質な IP アドレスとして見られていたものが除外され、そのうちにまたブラックリストに載る場合があります。2017 年のブラックリストの内容を見てみると、悪質なアクティビティに関連付けられることが多い上位 10,000 個の IP アドレスは頻繁に再利用されており、年平均で 18 回ほどもブラックリストへの指定と解除が繰り返されていることがわかりました。中にはそれぞれ 100 回以上ずつ指定と解除が繰り返されているものもありました。これは、2016 年においてはサイバー犯罪者のリピート率を反映するものでした。数千万の新しい IP アドレスがブラックリストに指定された 2017 年を考えると、インターネットの継続した監視が今後も不可欠であることは明らかです。ウェブルートでは、新しい悪質なアクティビティの識別を継続的に行ってリアルタイムでブラックリストを更新することで、新しい悪質なアクティビティを早期にブロックし、ハッカーによる攻撃の機会を狭めます。

信じがたい数の高リスク URL

毎日数十万にもおよぶ Web サイトが新しく作成されています。そのほとんどは無害なものですが、相当数のサイトが感染したり、サイバー攻撃を行う目的で作成されたものであることがわかっています。現在 10 億以上の Web サイトが存在しているため[v]、悪質なサイトからユーザーを保護するために、企業や組織に過大な負担がかかっている可能性があります。さらに、状況をより困難にする一因として、無害なサイトが明日、さらに言えば数分後にも悪質なサイトに変化する可能性があることが挙げられます。企業や組織がそのユーザー、データおよびブランドを守る唯一の効果的な方法は、分単位で更新される最新の URL レピュテーションデータを使用することです。

各 URL は企業や組織に対する相対的なリスクの面ではそれぞれ異なっており、その割合も年ごとに異なります。図 5 は、2017 年の相対的なリスク分類の分布を示しています。すべての URL のうち、25% が企業や組織にとって深刻なリスクとなる「高リスク」、「疑わしい」、「中リスク」に分類されています。

2017 年に最も多くの高リスク URL をホストした上位 10 か国には、過去にブラックリストに登録されていた多くの URL が含まれていました。米国が 43% で他の国を大きくリードし、2016 年と実質的に同じ割合を維持して

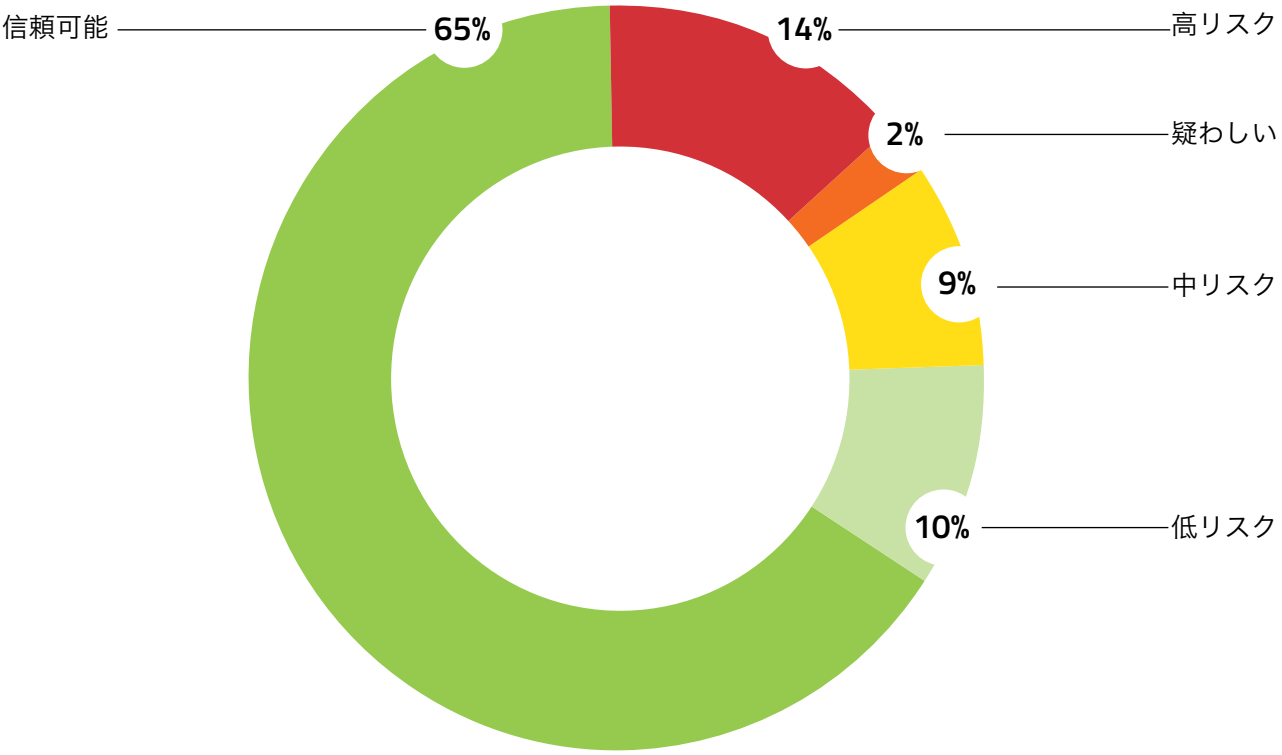


図 5: リスクカテゴリー別 URL

すべての URL の 25% は悪質、疑わしい、または中リスク (2017 年)。

います。ただし、このデータは誤った方向に考えを導く可能性があります。悪意を持った攻撃者の多くは、Web サイトの信頼性が高いとされる米国でサイトをホストしており、より危険なレピュテーションを持つ国々のサイトとは異なり、地域によるフィルタリングサービスでは、米国でホストされている悪質なサイトが自動的にブロックされないことがあるためです。ウェブルートでは、地域によるフィルタリングは悪質なサイトから利用者を保護するためのコンポーネントの一つに過ぎないことを理解しており、悪質な攻撃の分類、IP アドレス、および URL レピュテーションも同時に調査することで、セキュリティに関する正確な判断を下すよう努めています。

スイス、日本、およびブラジルは、それぞれの割合は相対的に低いものの、2016 年には上位 10 か国に入っていた英国、香港、オーストラリアの 3 つの国 / 行政区に代わって今年の上位 10 か国にランクインしました。米国、中国、ロシア、フランス、ウクライナ、およびブラジルは、悪質な IP アドレスと高リスク URL の両方において上位 10 か国にランクインされています。攻撃者は、感染率を高めるために、標的とする国向けにペイロードサーバーをローカライズしようとする傾向にあることも理解しておくことが重要です。

ウェブルートでは、他との比較において、特定のタイプのサイトが高リスクまたは疑わしいと考えらえる確率が高いことを確認しました。これらには、ビジネスおよび経済、ショッピング、社会、ストリーミングメディア、シェアウェアおよびフリーウェアのサイトが含まれています。2017 年にウェブルートが確認していた URL に基づいて信頼可能とされるサイトには、健康および医薬品、ニュースおよびメディア、社会のサイトが含まれます。

高リスク URL は大きく 2 つのカテゴリーに分類することができます。一つはマルウェアサイト (33%)、もう一つはプロキシ回避とアノニマイザー (40%) です。その他は、フィッシングや他の詐欺サイト (15%)、ボットネット (10%)、スパイウェアおよびアドウェア (2%) があります。

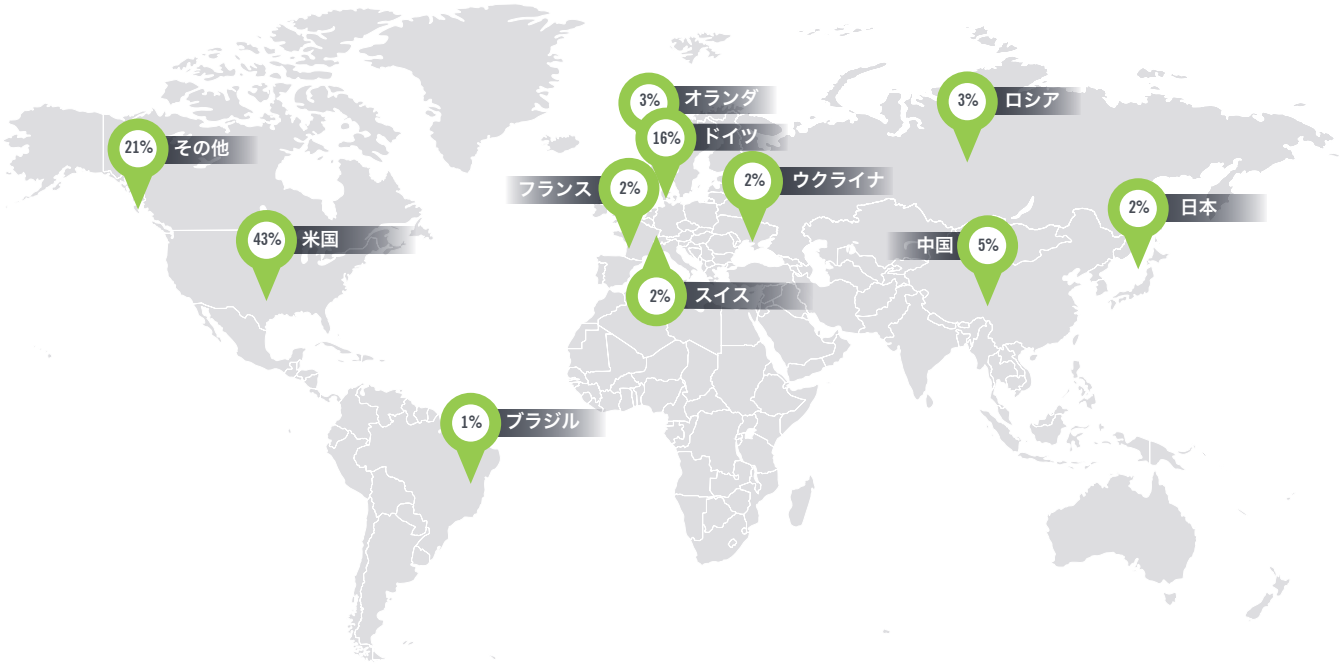


図 6: 国別高リスク URL

ショッピングカテゴリーなど、サイトのカテゴリーが悪質ではないと考えられる場合でも、企業や組織がユーザーのアクセスを制限する場合があることにも留意する必要があります。

ウェブルートでは継続的に URL の監視を行い、今日までに 270 億以上の URL を調査しました。弊社の分析プロセスでは、Web サイトの履歴、運営期間、ランキング、場所、ネットワーク、リンク、リアルタイムパフォーマンス、および動作に関する情報が考慮されます。分析の結果として、ウェブルート定義の 82 種のプライマリコンテンツカテゴリーにそれぞれの URL が分類され、不動産、ショッピング、ギャンブルなど URL の主な目的や、キーロガーおよび監視、スパイウェアやフィッシングなど悪質な目的が示されます。カテゴリーとは別に、各 URL には 1 ～ 100 の範囲でリスクスコアが付けられて、そのスコアに基づいて「高リスク」、「疑わしい」、「中リスク」、「低リスク」または「信頼可能」の 5 つに分けられます。BrightCloud® Web クラシフィケーション & レピュテーションサービスを介して入手可能なこの情報は、企業や組織がオンラインの脅威からのユーザーの保護、インターネット使用の制御、およびコンプライアンス準拠を目的とする Web アクセスポリシーを策定する際に大変役立ちます。

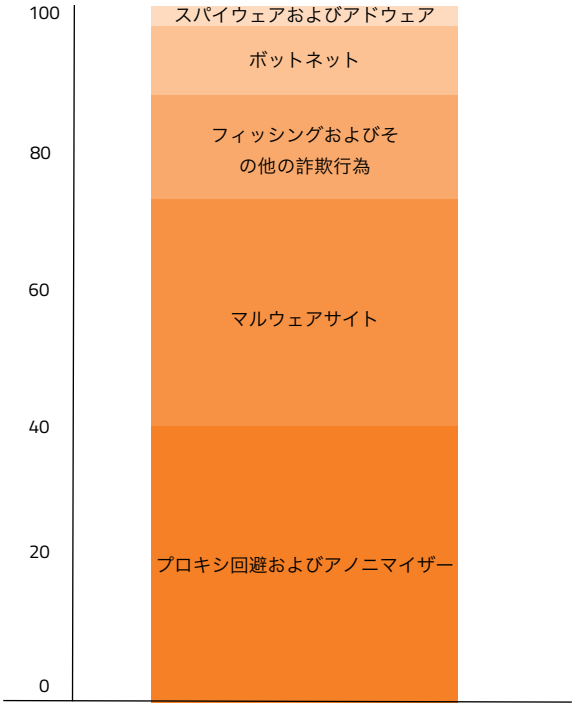


図 7: カテゴリー別高リスク URL

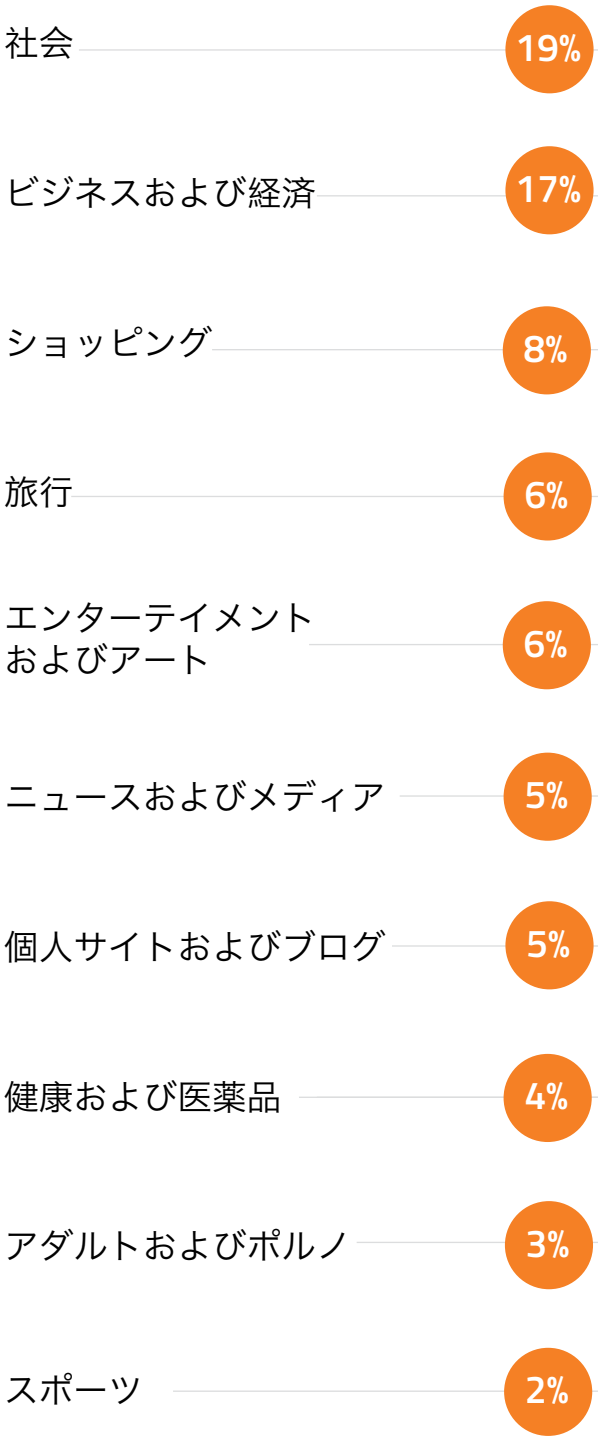


図 8: 悪質ではない URL の上位 10 カテゴリー (2017 年)

危険性が増した標的型フィッシング攻撃

フィッシングは引き続き最も頻繁に使用され、最も成功を収める攻撃ベクトルの一つです。より標的を絞った攻撃では、標的となる個人に関連する適切なテーマや興味に基づいてソーシャルエンジニアリングが使用されます。ユーザーは、悪質なサイトに移動するリンクをフィッシング詐欺メール内でクリックしたり、マルウェアが含まれる添付ファイルを開いたりした瞬間に、攻撃者を自らのネットワークに招き入れているのです。

ウェブルートの脅威研究チームにより、フィッシング攻撃は短期で消滅する傾向が続いていることがわかりました。ほとんどの場合、フィッシングサイトがオンラインになっているのは 4 ～ 8 時間です。監視したサイトの中で最も長時間存在したものでもわずか 44 時間で、最短で消滅したものについては 15 分間存在したのみでした。このような短いライフサイクルの攻撃に対応するには、企業や組織はこのような攻撃情報が含まれない静的なブラックリストに基づくのではなく、リアルタイムで対象サイトのフィッシングリスクレベルにアクセス可能なリアルタイムフィッシング対策ソシューションを採用する必要があります。

ほとんどの場合、フィッシングサイトがオンラインになっているのは 4 ～ 8 時間。

2017 年にウェブルートでは、数百万のフィッシング攻撃、そしてフィッシング サイトをホストする数万の固有 IP を確認しました。大きな数値ですが、詳細に調査してみると興味深い情報を得ることができました。

- 50 個の固有の IP により、150 万回以上のフィッシング攻撃を行ったフィッシングサイトがホストされていた。
- 単一の IP で、400,000 以上のフィッシングサイトがホストされていた。
- 2017 年に確認されたフィッシング攻撃の 90% はわずか 62 個のドメインから行われた。

攻撃者はいくつかの段階を踏んで検出を回避します。ドメイン名は、静的な IP リストによってブロックされないように、一度のみもしくはまれに使う程度にとどめます。また、フィッシングサイトのおよそ 25% は、ドメインの実際の IP アドレスの識別を困難にする IP マスキングを使用したことも判明しています。他にも、無害なドメイン名を使用して、1 つの Web ページのみをフィッシングコンテンツに置き換える手法も頻繁に使用されます。接続されていない分離されたページ (例 : サイト上のどのページもフィッシングページにリンクしていない、フィッシングページもサイト上のどのページにもリンクしていない) として仕掛けられた場合、クローラーによってそのフィッシングの脅威を検出することはほぼ不可能になります。

フィッシングサイトの約 25% は ドメインを隠すために IP マスキングを使用。

偽造の標的とされるサイトは毎年変わっていきます。2017 年に最も偽装されたサイトには、Google、Microsoft、Dropbox、Facebook、PayPal や Yahoo など、多くの人々がよく耳にする名前だけでなく、UPS (貨物運送会社)、Ria (送金サービス会社)、Bank Hapoalim (イスラエルの銀行)、および Blizzard (エンターテイメントソフトウェア会社) などの新しい名前も含まれていました。

2017 年に標的とされた上位 20 社を偽装した URL のうち、1 つを除くすべてが金融サービス会社またはテクノロジー会社のいずれかの Web サイトを偽装していました。

2017 年に最も偽装された企業は UPS であり、フィッシング攻撃の 52% が UPS を偽装したものでした。次点は別の新参の Ria で、攻撃の 23% が Ria を偽装したものでした。より多くの企業がオンラインでビジネスを展開するにつれて、荷物の配達や送金など、オンライン購入に関連したサービスを提供する会社が今後標的として狙われる可能性が高くなると予測されます。

標的とされた上位 20 社のうち大きな割合 (26%) をテクノロジー会社が占めていますが、2017 年に偽装された会社の 74% は金融機関でした。数値では金融機関より低いものの、テクノロジー会社に対する攻撃の量は深刻なものでした。Ria の 161,000 件強の攻撃に対して、偽装した UPS のページを使用しての攻撃は 356,000 件以上にも上りました。テクノロジー会社への侵入は金融サービス会社のアカウントへの侵入に比べて容易であることが多く、資格情報を再利用することで攻撃者は同時に複数のアカウントに侵入することができる場合もよくあるため、テクノロジー会社を利用してのフィッシングが有益だと考えられます。

偽造サイトをホストした国のうち、フィッシングサイトの 36% は米国でホストされており、13% がオランダでホストされていました。ブラジルおよびロシアについてはそれぞれ 2%、デンマークおよびリトアニアについてはそれぞれ 1% でした。

非常に短いライフサイクルと一見して無害に見えるドメイン名を利用することで、フィッシング攻撃の検出と保護が大変困難になっています。ウェブルートでは増加しつつあるこの問題に効果的に対処しています。Webroot SecureAnywhere® エンドポイントプロテクションを強化する BrightCloud® リアルタイムフィッシング対策サービスにより、リクエスト中の Web サイトにフィッシングリスクがあるかどうかがミリ秒単位で診断されます。先ほどまで無害だったサイトが悪質なサイトに変わることがあるため、このようなサイトへのユーザーのアクセスを防ぐには即時性が重要になります。

企業がエンドユーザー教育を通してサイバー脅威のリスクとコストを軽減するためのトレーニングプラットフォーム、Webroot® セキュリティ意識向上トレーニングでは、フィッシング攻撃を阻止するための企業全体の能力を強化します。模倣フィッシングサイトへのリンクをクリックして資格情報を入力しようとするユーザーの割合が非常に高いため、非常時に対処するためのトレーニングは欠かせません。2017 年後半のセキュリティ意識向上トレーニングで得られたデータによると、フィッシング模倣メールを開いたユーザーの約 42% はリンクをクリックして模倣フィッシング Web ページを開き、さらにリンクをクリックしたユーザーのうち 65% は資格情報を入力しようとしたことがわかりました。ユーザーが模倣に騙された際に行った教育はトレーニング内容の再確認に役立ちます。

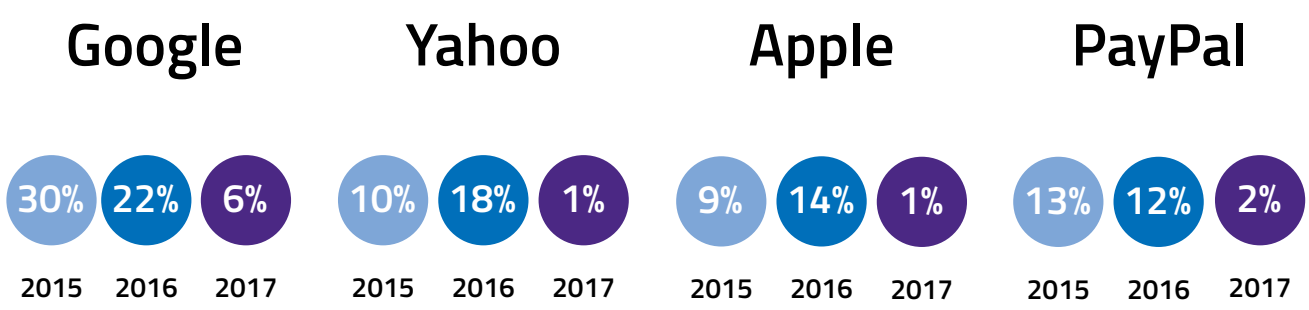


図 9: 最も多く偽装されたブランドの推移

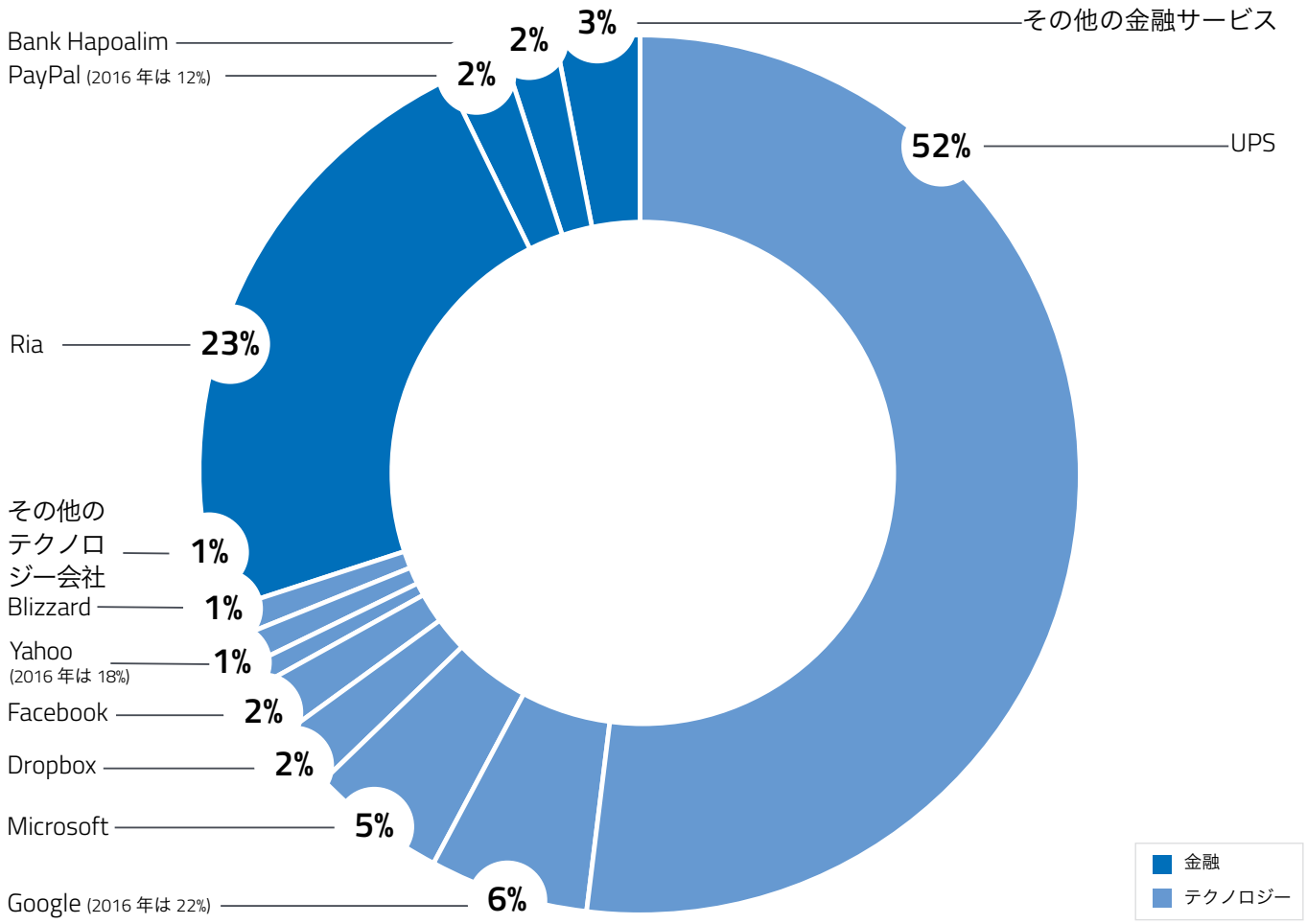


図 10: 2017 年にフィッシング攻撃で偽装された上位 10 サイト

悪質なモバイルアプリによる世界的な脅威

スマートフォンおよびタブレットの人気が高まり、多くのユーザーが利用するようになりました。世界中のスマートフォンのユーザー数は、2019 年までに 25 億人を超えると予想されています[vi]。移動中でのインターネット接続の増加に伴い、これらのデバイスが攻撃者の主要な標的となりつつあります。モバイルデバイスへの攻撃手段として、悪質なモバイルアプリが最も多く使われています。正当なアプリは公式のアプリストアからダウンロードできますが、類似したアプリや一見同じに見えるアプリもその他多数のサイトで入手することができます。このようなアプリは、人気のあるゲームや企業のユーティリティ、その他のさまざまなアプリケーションタイプを偽装した悪質なアプリである可能性があります。

ウェブルートでは常にアプリストアおよびその他のレポジトリを監視しており、新しいアプリまたは最新版を検出した際はそれらに悪質な動作がないかを分析します。このインテリジェンス情報は、ウェブルートモバイルプロテクションおよび BrightCloud® モバイルセキュリティ SDK で入手可能です。

ウェブルートでは、2017 年に数百万もの新規または最新版モバイルアプリを分析し、これまでに合計で 6,200 万以上ものアプリを分析してきました。分析結果に基づいて、各モバイルアプリをリスクの高低を表すレピュテーションカテゴリー（「悪質」、「望ましくない」、「疑わしい」、「適度」、「無害」または「信頼可能」）に分類しました。

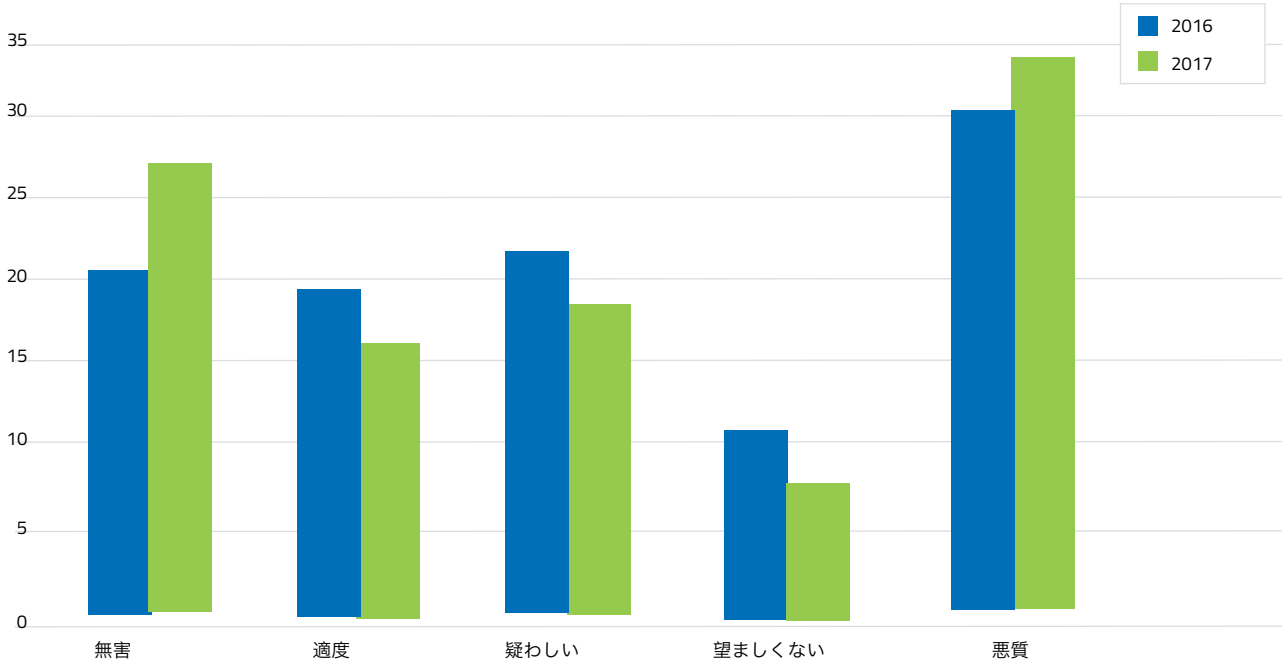


図 11: 過去 2 年間における Android™アプリのレピュテーション分布

モバイルアプリの 32% は悪質。

「悪質」として分類されたモバイルアプリは 2017 年 (32%) には 2016 年 (29%) よりもやや高い割合を占めました。「望ましくない」アプリの割合は 2017 年の方が低く (2017 年は 8%、2016 年は 11%)、「疑わしい」アプリについては両年ともほぼ同じと言えました (2017 年は 18%、2016 年は 21%)。「適度」なアプリの割合は 2016 年 (19%) よりも 2017 年 (16%) の方が低かったものの、すべてのモバイルアプリの 1/4 以上を占める「無害」なアプリについては 2017 年には 26% と評価され、2016 年の 20% から上昇しました。

月ごとの調査では、「悪質」なアプリの割合が最も高かったのは 4 月で (ウェブルートによりその月に確認されたすべてのモバイルアプリの 60% 以上が悪質と判断)、次に高かったのが 12 月 (41%) でした。逆に、最も低かったのは 1 月 (14%) と 2 月 (25%) でした。「疑わしい」モバイルアプリの割合は 10 月と 11 月にやや高くなったものの (それぞれ 25% と 23%)、その他の月は 15 ～ 18% にとどまり、年間を通して比較的一定した数値を示しました。絶対数を見てみると、悪質なアプリのインシデント件数が最も多かったのは 2017 年 5 月と 7 月でした。これは、5 月に初めて確認されてその後数か月にわたって猛威を振るった Android デバイスを標的とした Cloak and Dagger (外套と短剣) 攻撃や、5 月に発見されたマルウェア Judy と相関関係がある可能性があります。

ウェブルートでは 2017 年に検出した悪質アプリをその主なアクティビティに基づいて分類しました。図 12 にはその結果が 2016 年と比較する形で示されています。悪質モバイルアプリの用途として最も多かったアクティビティが、引き続きトロイの木馬であることがわかりました。図で 60% 強を示している前の年を超えて 2017 年には 67% となり、マルウェアの他のタイプとの間には引き続き大きな差が見られます。次に最も多かったのは PUA であり、2016 年の 26% からは低下したものの、2017 年には分析されたモバイルアプリの 1/5 を占めています。これらの PUA は一緒に読み込まれる広告が面倒な場合がありますが、少なくともアプリ自体は正常に機能します。しかしながらウェブルートでは、一見迷惑なだけに見えるアプリが実は複数の目的を持つマルウェアである可能性も確認しました。たとえば、トロイの木馬として知られる Loapi では無限に広告が表示され、これにユーザーの注意が引き付けられている間に、マルウェアによって DDoS 攻撃が行われたり、メッセージを送信したり、さらには有料サービスに加入したりしてしまう可能性まで確認されています。

特に情報窃盗またはランサムエアのダウンロードが行われた場合、悪質なアプリによって引き起こされる被害は深刻なものになる可能性があります。2017 年には、Booster & Cleaner Pro および Wallpapers Blur HD という 2 つの Android アプリ内に LeakerLocker ランサムウェアが隠されていることが明らかになりました。このマルウェアはファイルを暗号化するのではなく、個人情報を拡散しないことと引き換えに被害者に金銭の支払いを要求します。クリプトジャッキングもモバイルデバイスを標的として攻撃し、スマートフォンの能力を著しく低下させて、場合によってはハードウェアに過剰な負荷がかかり、デバイスが損傷することもあります。

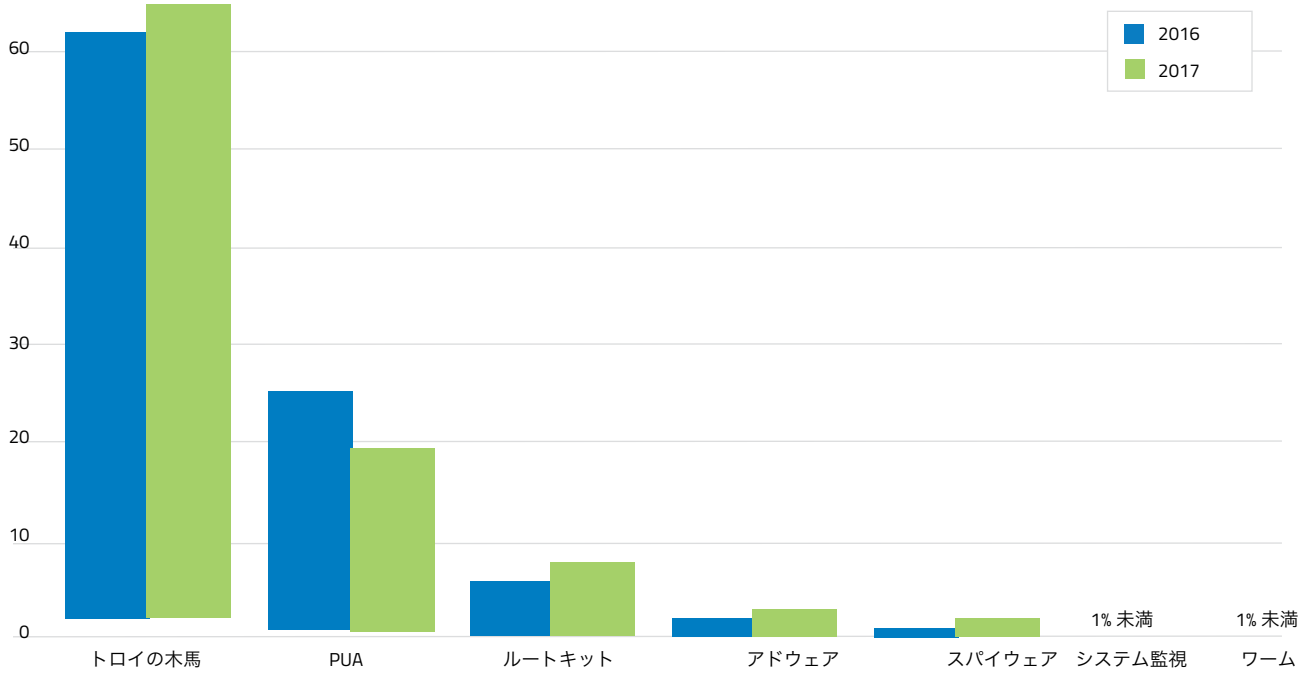


図 12: 過去 2 年間における主なアクティビティ別の悪質なアプリ

まとめ

ウェブルートが 2017 年を通して収集・分析したデータにより、サイバー脅威の状況が急速に変化し続けていることがわかりました。攻撃者は攻撃の効果をすばやく学習し、既存の防御を回避すべく新しい手法を常に考え出しています。

» 亜種戦略攻撃がマルウェアにとって最良の攻撃手法である状況が継続(ウェブルートによって確認されたすべての悪質な実行可能ファイルの 94% 以上)。

» 2017 年にはランサムウェアが増加。今までで最大規模の 2 つの攻撃では、新たな手法が使用されて企業ネットワーク全体が感染し、数十億ドルもの被害を引き起こしました。

» クリプトジャッキングの脅威が急速に増加中。CPU の処理能力を盗んで暗号通貨の採掘に使用することで、攻撃者は容易に収益を上げることができます。

» 高リスク IP アドレスはレピュテーションの状態が頻繁に変わる傾向が継続。2017 年にウェブルートでは、10,000 もの悪質な IP アドレスが継続的に再利用されており、それぞれ平均で 18 回もレピュテーションのステータスを変えていることを確認しました。動的に更新される IP アドレスのリストおよびコンテキスト分析なしでは検出が困難なスパムサイトがその大多数を占めています (67%)。

» 2017 年に監視した URL の 1/4 は、企業や組織、個人にとって同様に深刻なリスクとなる「高リスク」、「疑わしい」、「中リスク」に分類。

» 標的をより絞ったフィッシング攻撃では、標的を騙すためにソーシャルエンジニアリングおよび IP マスキングを使用。確認したフィッシング攻撃の 90% はわずか 62 個のドメインから行われました。

» 引き続き深刻な脅威とされる悪質なモバイルアプリ。2017 年にウェブルートが分析したアプリの 32% は悪質なものでした。

亜種戦略、ランサムウェア、およびクリプトジャッキングの新たな増加傾向、悪質な URL の増加、より高度なフィッシング攻撃および悪質なモバイルアプリなど、多くの要因によって危険で動的な脅威にさらされているサイバー環境では、複数の層からなる防御策が求められます。Windows 10 などのセキュリティ機能が強化されたオペレーティングシステムへの移行は脅威の緩和に役立ちますが、あくまでも対策の一部にすぎません。今日では、継続的に更新される脅威インテリジェンス、コンテキスト分析、高度なエンドポイントおよび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の意思決定システムを採用することが企業や組織にとって不可欠です。さらに、ユーザー向けの強力なセキュリティトレーニングを実施することで、企業や組織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ます。

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 脅威インテリジェンス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 SecureAnywhere® 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 Webroot SecureAnywhere 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]「Why Enterprises Are Upgrading to Windows 10 Faster Than Expected.」 CIO、2017 年 4 月。https://www.cio.com/article/3187503/windows/why-enterprises-are-upgrading-to-windows-10-faster-than-expected.html

[ii]「"WannaCry" ransomware attack losses could reach $4 billion.」 Moneywatch、2017 年 5 月。https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

[iii]「NotPetya Still Roils Company's Finances, Costing Organizations $1.2 Billion in Revenue.」 Cyberreason、2017 年 11 月。https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue

[iv]「Hackers are using YouTube Ads to Mine Monero Cryptocurrenty.」 HackRead.com、2018 年 1 月。https://www.hackread.com/hackers-using-youtube-ads-to-mine-monero-cryptocurrency/

[v]「October 2017 Web Server Survey」 Netcraft、2017 年。https://news.netcraft.com/archives/2017/10/26/october-2017-web-server-survey-13.html

[vi]「Number of smartphone users worldwide from 2014 to 2020 (in billions).」 Statista、2018 年。https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

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。弊社では、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、およびセキュリティ意識向上トレーニングで弊社を必要とするマネージドサービスプロバイダーおよび小規模ビジネスのお客様に向けて、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、および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。

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