WEBROOT®
Smarter Cybersecurity™

2019 年 ウェブルート

脅威レポート

中間アップデート

2019 年 9 月

目次

はじめに

予測の行為自体は、何かが起こる確率を適用したものです。適用したものです。たとえば、ある人がある行動を一度行った場合、あなたはその人が再び同じ行動をすると期待するかもしれません。しかし、その行動が良くない、またはマイナスの結果を引き起こした場合、その人がその行動を繰り返さないと期待する可能性が高いでしょう。それでは、もう少し複雑にしてみましょう。その人が、ある状況ではその行動をとったものの、他の状況ではその行動をとっていないとしましょう。それぞれの状況の詳細を分析し、それぞれの状況の違いと要因を判断することにより、特定の文脈においてその人が取る可能性のある行動を予想し始めることができるでしょう。それゆえ、将来の合理的な予測を行うには、文脈と共に過去の出来事に対する明確な洞察を得ることが必要です。

つまり、それこそウェブルートが脅威インテリジェンスで実行しようとしていることです。インターネットのデータとオブジェクトを調べて脅威の傾向を判断することにより、将来の脅威の挙動の確率を計算できます。数百万のウェブサイト、ドメインおよび IP アドレスの状態が害のないものから悪意のあるものに変化し戻るにつれ、当社は傾向を分析し、それらの関係だけでなく、ファイルやアプリケーションなどの他のインターネットオブジェクトとの関係をマッピングできます。これにより、害のないウェブサイトや IP が悪意のあるものに変化する可能性、将来の攻撃がどこから発生するかをよりよく予測できるようにもなります。

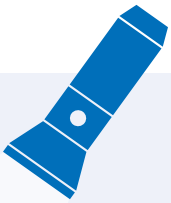
2019 年上半期の脅威インテリジェンスデータを調べると、過去数年間に当社が観察した傾向が依然として強いことが明白です。特に、ポリモーフィズム、フィッシングおよび革新的な攻撃が全体的に増加し続けています。

年次ウェブルート脅威レポートを更新した本中間レポートは、当社の先進的な機械学習ベースの脅威分析アーキテクチャである Webroot® プラットフォームで使用しているデータと、ウェブルート脅威調査チームからの傾向、洞察および予測をご紹介するものです。

エンドポイント マルウェアの変化

総じて、マルウェアで見られる比較的大きな傾向の1つは、より偵察機能を強めたものへの移行です。攻撃者はこれまで同様、多数のマルウェアキャンペーンをローンチしていますが、システムから得られる価値を判断するため、犯罪者が事前により多くの偵察を行っていることがわかりました。たとえば、優れた速度と処理能力を備えたシステム、またはシステムネットワークを検出した場合、それらのシステムを利用して暗号通貨をマイニングする攻撃をローンチすることを選択できます。または、重要なインフラストラクチャのはるかに広いネットワークに接続するエンドポイントデバイスを侵害した場合、ランサムウェアを起動してビジネスに不可欠なシステムを暗号化し、被害者から金銭を強要する可能性があります。

> *多数の感染は依然として価値がありますが、攻撃者は被害者の価値のプロファイリングを選択することにより、実質的に量よりも質を求めています。*
>
> **ジェイソン・デイヴィソン、高度脅威調査アナリスト**



注目される脅威：
DANABOT とその進化形

最近のマルウェアシーンでランサムウェアが優勢であることから、古き良きバンキング型トロイの木馬がフィッシングメールを介して配信される聞けば、懐かしく思われるかもしれません。しかし、サイバー犯罪者は常に検出を回避し成功の可能性を高めようと戦術を変更しているため、昔よく使った手法を基に新たに構築することは理にかなっています。

DanaBot と呼ばれるトロイの木馬は、2018 年 4 月にセミプライベートのフォーラムで初めて販売されました。基本的なトロイの木馬に情報を盗む機能を備えた DanaBot は、詐欺やその他の犯罪行為について疑いを持たないユーザーから機密の銀行情報を収集します。これらの活動自体は新しいものではありませんが、このトロイの木馬は進化を続けています。

特に、DanaBot はアフィリエイトを追加し、ジオターゲティングを増やし、プロキシモジュール（注入に使用）、スティーラーモジュール、Tor モジュール

のマルウェアは単一の PC に独特なもの。

などの新しいモジュールを含むように全体的に機能性を拡張しました。ランサムウェアの配信もできるよう拡張されています。

総じて、マルウェアの発生率は 2018 年の実績値からほぼ横ばいでしたが、注意すべき重要な点がいくつかあります。まず、当社のデータでは、遭遇したマルウェアのサンプルの 95% が単一マシンに固有なものでした (昨年実績の 92% から増加)。これは即ち、今日の脅威のほぼすべてがポリモーフィック型であり、シグネチャベースのテクノロジーでそれらを検出することはほぼ不可能になっています。

第二に、マルウェアの感染数に大きな変化はありませんでしたが、感染しているWindows®バージョンと、感染したデバイスの地理的位置を見ると、顕著な変化が確認されました。

ウェブルートで保護された PC 上で検出されたマルウェアサンプルの割合

PC 1 台	95.2%
2-100 台	3.9%
11-100 台	0.8%
101-500 台	0.12%
501-1000 台	0.01%

感染した WINDOWS® デバイスの地域分布

中東	11.0%
アジア	10.1%
アフリカ	8.8%
南米	8.0%
欧州	4.4%
北米	3.2%
オーストラリア/ニュージーランド	2.5%
日本	2.2%
英国	2.3%
その他	2.8%

ウェブルートで保護されたデバイス、オペレーティングシステム及び地域分布

	Windows® 8 およびそれ以前	Windows® 10
中東	53%	47%
アジア	49%	51%
アフリカ	51%	49%
南米	39%	61%
欧州	45%	55%
北米	34%	66%
オーストラリア/ニュージーランド	43%	57%
日本	56%	44%
英国	44%	56%
その他	50%	50%

データを並べて調べると、中東、アジア、アフリカに影響を与える感染の増加は、比較的古い、またはパッチが適用されていないオペレーティングシステムの使用と相関していると考えられます。

第三に、比較的古いオペレーティングシステムを攻撃するマルウェアの増加が見られました。2018 年と比較すると、Windows® 7 マシンをターゲットとするマルウェアは 71% 増加しています。一般に、Windows 7 オペレーティングシステムを使用しているコンピューターは、Windows® 10 を実行しているコンピューターの倍感染する可能性が高く、2019 年年初来、Windows 7 デバイスあたりの感染が約 0.12 であったのに対し、Windows 10 デバイスは 0.05 でした。

すべてのマルウェアの 76% は WINDOWS® システム上の 3 箇所のうちの 1 つに隠れています。

専門家のヒント

企業にとっては、一時フォルダとキャッシュフォルダからの実行を阻止する Windows® ポリシーを策定することで、多くの脅威が特定のエンドポイントデバイスの感染に成功するのを阻止できるでしょう。

WINDOWS® 7 システムをターゲットとするマルウェアが増加

71%

> *「旧式のオペレーティングシステムの使用頻度は減っていますが、その 1台でさえ侵害されれば企業のネットワーク全体がダウンする可能性があります。それこそ、2017 年に WannaCry やNotPetya のような感染が急速に広まった方法です。それらは、パッチが適用されていない旧式のオペレーティングシステムの脆弱性を利用したのです」*
>
> **– ブリアナ・バトラー、シニア エンジニアリング データ アナリスト**

[1] Webroot Inc. “Hook, Line and Sinker: Why Phishing Attacks Work.” (2019 年 9 月)

専門家の洞察：マルウェアの傾向

ジェイソン・デイヴィソン (ウェブルートの高度脅威調査アナリスト) が 2019 年年初来のマルウェアのエコシステムについて以下のようにまとめています。

1

猿真似。

あまり洗練されていないサイバー犯罪者は比較的規模の大きい組織的なグループが用いて成功した戦略を監視し真似しようと試みます。

2

データが増えれば問題も増える。

比較的規模が大きく、組織的なサイバー犯罪者はビッグデータの問題を抱えています。手に余るほどの感染を抱えていると、追求するのに十分価値がある感染を見極めるためにすべての情報を効率的かつ効果的に選別しなければなりません。

3

企業のみ。

犯罪者は、どの攻撃の成功率と収益性が最も高いかを判断した後、ランサムウェア ペイロードをデプロイする前に、ラテラルムーブメント (横方向の移動) と特権昇格を通じてネットワーク全体をターゲットにすることができます。彼らは意図的に、学校、州政府および各部門、病院など閉鎖する余裕のない被害者を標的にします。攻撃を受けた場合、これらの組織は一般に、安全なバックアップが整備されていない限り、支払わざるを得ません。

予測

> 大規模で組織化された脅威の運用を取り巻く効率は改善し続けるでしょう。すでにかなりの量の自動化が行われていると思いますが、特にラテラルムーブメントや高価値のターゲットから次のターゲットへのジャンプについて特に自動化が進む可能性が高いでしょう。
>
> **– ジェイソン・デイヴィソン、高度脅威調査アナリスト**

7

URL および IP ベースの脅威

4分の1の

悪意のある URLの ホストは信頼されたドメイン。

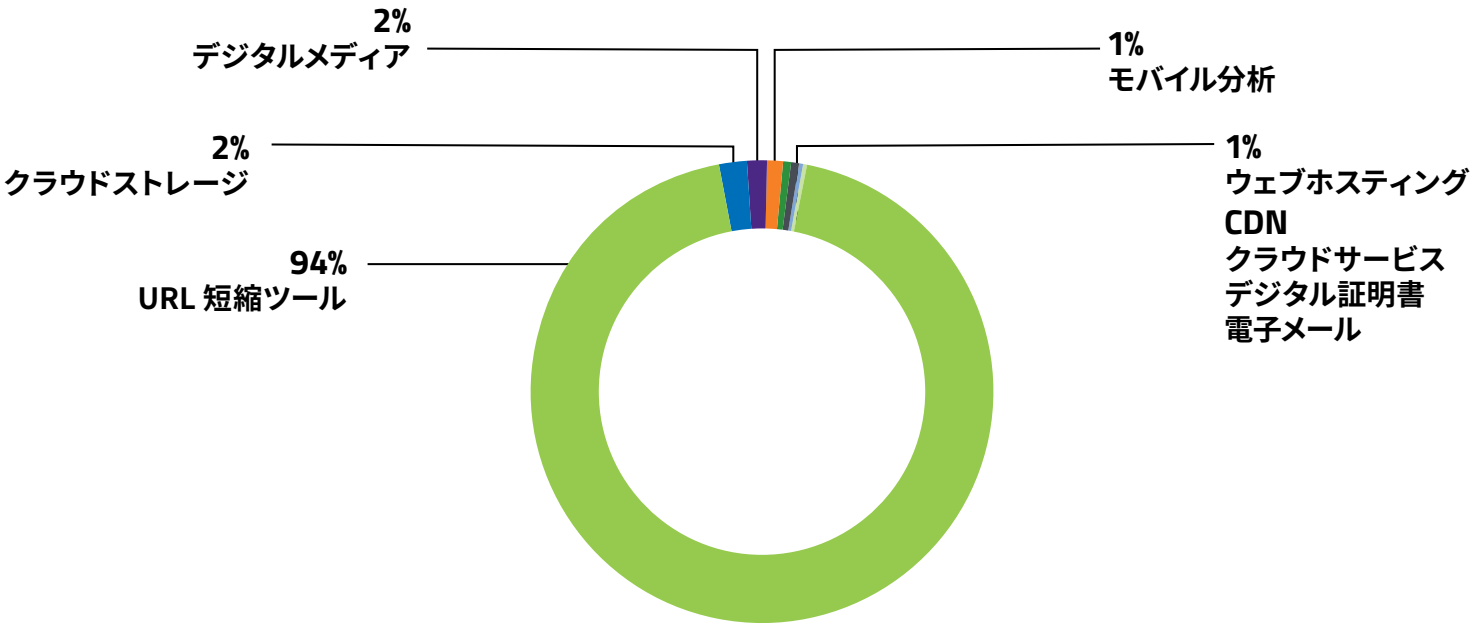
最後に、検出されたすべてのマルウェアのうち、ホームユーザーの PC は、引き続きビジネス PC の約 2 倍 (それぞれ 64% と 36%) 感染する可能性が高くなっています。この乖離にはさまざまな要因があります。特に、ほとんどの企業のデバイスはビジネスファイアウォールと必須のセキュリティで保護されていますが、ホームユーザーはデバイスの保護が比較的緩いと考えられます。第二に、平均的な人は雇用主が所有する仕事用デバイスでウェブを閲覧する際により慎重になる傾向があります。[1]

頻度が増加するにつれて、サイバー犯罪者は信頼を利用するためにできる限りのことを行っています。2019 年年初来、悪意のある URL の 4 分の 1 (24%) は信頼できるドメインで発見されました。犯罪者は正式なサイトのページをハイジャックして悪意のあるコンテンツをホストします。セキュリティ措置でこれらのドメインの URL をブロックすることが比較的困難であり、エンドユーザーが認識しているドメインのページを疑う可能性が低いことを知っているからです。 URL 短縮サービス (bit.ly、TinyURL、tiny.cc など) 、クラウドストレージ (Dropbox、SharePoint、Google™Drive など) 、デジタルメディア (Tumblr、Imgur など) 、(最も人気のある上位 1,000 ドメインのうち) 9 つの異なるドメインコンテンツカテゴリーでこの動作の殆どを確認しました。

悪意のある URL は非常に動的で頻繁に変化しますが、当社が遭遇した総数は前年実績と比べてほぼ横ばいで、存在するすべてのウェブサイトの約 2% を占めています。

URL の 50 に 1 つは 悪意のあるもの

それ自体、その数は特に目を見張るほどではないかもしれませんが、実際には重大なリスクを表しています。本質的に、50 の URL のうち 1 つは悪意のあるものです。クリックするリンクの数や毎日アクセスするウェブサイトの数を考えると、実際に存在するリスクの量を把握し始めることができるでしょう。実際、世界の人々の 85% が、1 日平均仕事関連のリンクを最大 50、個人的な生活関連のリンクを最大 50 クリックすることを認めています。[2]



[2] Webroot Inc. “Hook, Line and Sinker: Why Phishing Attacks Work.” (2019 年 9 月)

注目される脅威：

クリプトジャッキングは忘れ去られることはない

クリプトジャッキングとは、ウェブ 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。

記録上初の暗号通貨マイニング スクリプトである CoinHive の発案者は 2019 年 3 月 8 日にサービスを終了しました。しかし、DeepMiner、DeepMinerAnonymous、JSECoin、CryptoLoot、CoinImp など多数の模倣者が登場しています。

ブラウザベースのセキュリティ対策はこの脅威を阻止するために改善されていますが、この脅威がすぐに消えることはありません。当社の検出によると、現在 87,000 以上のドメインがクリプトジャッキング スクリプトをホストしています。実際、この数は 7 月に過去最高値を記録し、その間にウェブルートはクリプトジャッキング スクリプトをホストしているページに対する 100 万を超える URL リクエストをブロックしました。

専門家の洞察：

タイラー・モフィット、セキュリティ アナリスト兼常駐暗号通貨スペシャリストは、クリプトジャッキングの減少についてさらなる洞察を提供します。

彼の説明によると、「クリプトジャッキングの問題は、通常のウェブ訪問の典型的な滞在時間ではうまく作用しないということと、収益性の面では広告のほうがスクリプトマイニングよりも割がいいということです。ターゲットとなるサイトのほぼすべては、ユーザーが多くの時間を費やすストリーミングサイトです。これにより、犯罪者によるこの攻撃ベクトルの採用率が大幅に低下します」

減少はしているものの、彼は私たちに思い出させます。「でもクリプトジャッキングは無くなっていません。 Coinhive は 3 月に暗号通貨が史上最安値でサービスを停止しましたが、CryptoLoot と CoinImp は 4 月から 6 月の強気相場で若干成長しました。彼らは Twitter で Coinhive の終焉後は彼らが新しい 1 位のサービスであると自慢しました」

予測

> “クリプトジャッキングのウェブサイトが減少しているものの、クリプトマイニングのペイロードは引き続き堅調であると見込まれます。犯罪者にとって、非常に効率的かつ低リスクな選択肢であるからです。ほぼすべてのオペレーティングシステムをターゲットにすることができる上、被害者が感染に気付くこともありません。少量のクリプトは、被害者にとってのパワーコストの形で徴収されます。ランサムウェアよりも収益性は低いものの、徴収は楽でかつ保証されています。今後もかなりの間存在し続けると思います。”
>
> **タイラー・モフィット、セキュリティ アナリスト**

フィッシング アップデート

おそらく、年初来で見られた最も印象的な傾向はフィッシングに関するものでした。フィッシングサイトは大幅に成長し、 4 月上旬にはウェブルートで保護された顧客がアクセスを阻止されたサイトの数が 1 日で約 6 万と急激に増加しました。2019 年上半期、ウェブルートはエンドユーザーのブラウジングを通じて 150 万種以上のフィッシング ウェブサイトを検出しました。さらに、自社のプロアクティブなクロールとインターネット分析により、340 万種を検出しました。

> *特に、新しいドメイン登録の綿密な監視と検査、およびホスティング割り当ての変更は、可能性のあるフィッシング活動の予測をゼロデイ (脆弱性が発見されて修正プログラムが提供される日より前) 検知に変えるために不可欠です。*
>
> **— キャシー・ヤング、プロダクト・マネージャー、Threat Intelligence Partnerships**

フィッシングのターゲットも変化しています。伝統的にフィッシング攻撃は金融機関になりすます傾向がありました。今や攻撃者は Amazon や FedEx など比較的重要度の低いアカウントの資格情報を取得しようとしているようです。ウェブルートのセキュリティ インテリジェンス ディレクターであるグレイソン・ミルボーンウェブルートのセキュリティ インテリジェンス ディレクターであるグレイソン・ミルボーンは、これがさまざまな要因による可能性が高いとしています。まず、金融口座をハッキングすると、より多くのデジタル痕跡が残る可能性があります。また、金融機関の詐欺対策が詐欺的な銀行活動にフラグを立てたり拒否したりする可能性があるため、努力に見合う価値がないかもしれません。犯罪者が比較的重要度の低いアカウントをターゲットにしているもう 1 つの理由は、パスワードの再利用に関係しています。犯罪者が Amazon や eBay など重要でないアカウントの個人のパスワードを入手した場合、それだけでは価値がないかもしれないとグレイソンは説明します。しかし、その人が別のアカウントのためにそのパスワードを再利用し、犯罪者がその人のオンライン習慣を判断するために何らかの偵察を行ったなら、犯罪者はそのパスワードを使用して他のアカウントに侵入するかもしれません。さらに、当該アカウントの 1 つが仕事関係のものであれば、発覚したパスワードを使って攻撃者は被害者の雇用主のネットワークにアクセスすることができるでしょう。

さらに、犯罪者は、侵害したあまり重要でないアカウントの情報を使用して、より確実なフィッシングの釣り餌を考案するかもしれません。たとえば、Amazon のメールをまねて、

> *現在のフィッシング攻撃は単なるユーザー名やパスワードを盗むだけにとどまりません。攻撃者は、あなたの最初のペットの名前であるとか、あなたが育った通りのような「秘密の質問」の答えにつながる事柄もターゲットにしています。これらの質問の答えをデータ侵害によって収集した情報と組み合わせることで、なりすまし犯罪はいとも簡単に実行できるようになります。*
>
> **—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**

2019 年年初来、当社は

150 万種類を超える

フィッシング URL を発見し、

335 万エンドポイント

デバイス

を保護してきました。

注目される脅威：

HTTPS の解決困難な状況

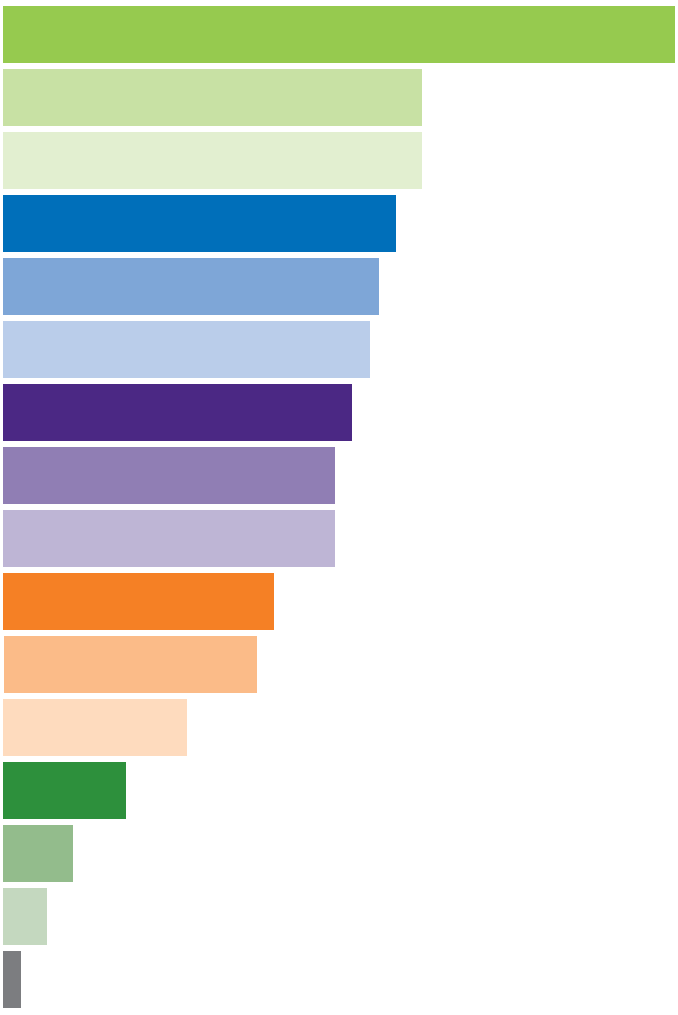
フィッシングサイトの 3 件に 1 件は HTTPS を使用しています。

HTTPS プロトコルは誤ったセキュリティ感覚を与えている、とウェブルートの CTO (最高技術責任者) であるハル・ロナスは述べます。 「S」 はセキュア (安全) を指しますが、問題は HTTPS が実際にセキュリティに関するものではないことです。それはプライバシーについてなのです。 ハルは、「ブラウザに小さな鍵アイコンが表示されている時は、そのサイトで送信する情報が暗号化され、目的の場所に安全に配信されていることを意味するだけなのです。目的のサイトが安全であるという保証はありません」

ハルによると、我々はみなそのアイコンを探すよう訓練されているため、悪意のある攻撃者は HTTP の使用を増やすことにより、悪意のある彼らのウェブサイトに合法的な印象を作り出そうとしています。セキュリティ証書を取得するのはもはや特別難しいことではないため、そうすることにより犯罪者は簡単にユーザーの信頼を利用することができるのです。実際、当社が検知したフィッシングサイトの約 3 分の 1 (29%) は HTTPS を使用しています。

HTTPS を使用しているフィッシングサイトの割合 (カテゴリー別)

教育	77%
暗号通貨	48%
ストリーミング	48%
金融機関	45%
ゲーム	43%
SaaS/ウェブメール	42%
ISP	40%
支払いサービス	38%
政府機関	38%
ファイル ホスティング	31%
小売	29%
ソーシャルメディア	21%
配送サービス	14%
ヘルスケア	8%
行政サービス	5%
ニュース	2%



あなたが無意識に自分の銀行の非常によくできた偽のフィッシングサイトにたどり着き、鍵アイコンを見れば、正しいサイトに接続していて問題がないとみなすのは当然です。あなたがログインしようとしている時を除けば、あなたが実際にしていることはあなたのログイン情報を攻撃者にプライベートに送信しているのです。この場合、あなたをだますために HTTPS が使われるでしょう。

— ハル・ロナス、CTO (最高技術責任者)

予測

フィッシングキットは今後も進化し続け、自動検出方法を回避するためさらなる技術が追加されると見込まれます。フィッシングページの配信もより動的になる可能性が高く、さまざまな条件を使用して、よりターゲットを絞ったフィッシングページを配信し、キャンペーンの成功の可能性を高めるでしょう。

ダン・パラ、シニア高度脅威調査アナリスト

結論および重要なポイント

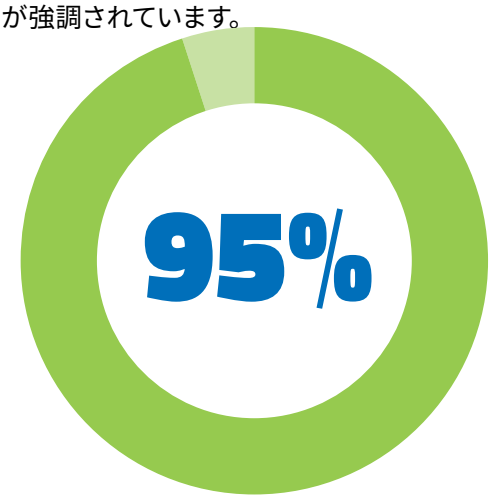
結論

年次脅威レポートを更新した本中間レポートで使用されたデータは、ウェブルート プラットフォームと、世界中の何百万もの当社の顧客が経験し、ウェブルート脅威調査チームが確認した傾向と変化の詳細をご紹介するものです。2019 年上半期には、マルウェア開発者がいかに技術を進化させ、ターゲットを変更してきたかを示しています。

サイバー犯罪の戦術が進化し続けるにつれて、発生する前に予防的に脅威を阻止できる予測的保護が重要であることは明らかです。さらに、フィッシングやその他のオンラインリスクを回避するようエンドユーザーが教育されれば、エンドユーザーが強力な初期防衛となるよりよい準備が整うでしょう。フィッシングの継続的な進化から、企業が自社と顧客を保護するには予測セキュリティ製品と関連する継続的なサイバーセキュリティ認識トレーニングを組み合わせることが唯一の方法であることが示唆されています。

重要ポイント

マルウェアの統計は比較的横ばいでしたが、当社がこれまで検知したマルウェアの **ほぼすべて (95%) は単独の PC に固有のもので、**ポリモーフィックな脅威を阻止できる行動保護の必要性が強調されています。



WINDOWS® 7 システムをターゲットとするマルウェアが増加

71%

Windows 7 PC をターゲットとする感染件数は大幅に増加し、**悪意のある攻撃者がパッチの適用されていない脆弱性をエクスプロイトしようと比較的古いオペレーティングシステムを特にターゲットとしていることが示唆されています** (これらのエクスプロイトは 2017 年に WannaCry が NSA を使って EternalBlue を攻撃した際のように大きな攻撃につながっています。)

犯罪者は引き続きオペレーティングシステムの脆弱性を利用するうちに、人間の脆弱性、すなわち我々の信頼をも利用するようになっています。

悪意のある URL の約 4 件に 1 件 (24%) は信頼されたドメインにホストされ、馴染みのあるブランドやウェブサイトに対するサイト訪問者の信頼を当てにしています。

検知されたフィッシングサイトの約 3 件に 1 件 (29%) は HTTPS を使用し、「セキュア」なプロトコルを使用するサイトを探して信頼することに慣れているインターネット利用者をだまそうと期待しています。

データについて

本中間アップデートは、ウェブルートの年次脅威レポートの延長として作成されたものです。年次脅威レポートでは、前年の新たな脅威やサイバー犯罪の傾向を分析し、今後の見通しや予測をご紹介しています。ウェブルートの年次脅威レポートは、webroot.com/2019ThreatReport でご覧になれます。

この年次脅威レポートで提示された統計は、当社の高度なクラウドベースの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って自動的に取り込まれ分析されたメトリックに基づいています。このシステムは、既知およびゼロデイ、これまでに見られなかった高度な持続的脅威などからユーザーとネットワークを予防的に保護します。プラットフォームによって生成された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通じテクノロジーパートナーによって使用されます。当社の脅威インテリジェンスは、IPv4 および使用中の IPv6 スペース時間の経過とともに全体、数十億のURL、数千万の新規および更新されたモバイルアプリ、およびウェブルートで保護された世界中のすべての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、信頼度を使用したリアルタイムスコアリングおよび継続的な更新により、ウェブルート脅威インテリジェンスは、最も洗練された脅威であっても特定および阻止するのに非常に効果的です。ウェブルートは、膨大なデータ処理能力、利用可能な最も高度な技術の独自の実装、および強力なコンテキスト分析エンジンに基づいて、機械学習に独自のアプローチを採用しています。コンテキスト化は、インターネットオブジェクトをリンクする「関連付けによる罪悪感」モデルです。観測された各インターネットオブジェクトの広範な特性（オブジェクトあたり最大 1,000 万個の特性）を取り込むことにより、ウェブルートは、正確な分析時にオブジェクトが脅威をもたらすかどうかを判断できます。当社の特許取得済みのアプローチは、攻撃と脅威の行動をベクター全体にマッピングし、URL、IP、ファイル、モバイルアプリ間の関係を分析します。たとえば、ユーザーが連絡先リストにアクセスして IP アドレスに転送しようとするモバイルアプリを実行すると、当該アプリの悪意のある動作が IP アドレスの評価スコアに影響を与えます。オブジェクト間の現在の関連付けを、何百万ものオブジェクトが経時的にどのように動作したかについての履歴と相関させるこの機能ゆえに、ウェブルート脅威インテリジェンスは本質的に予測可能になるのです。

Carbonite について

Carbonite は企業向けにバックアップ、障害回復、高度な可用性と業務移行の技術など力強いデータ保護プラットフォームを提供しています。Carbonite データ保護プラットフォームはセキュア クラウド インフラストラクチャで世界的規模で企業をサポートします。詳細は www.carbonite.com または Twitter のアカウント @Carbonite でご覧になれます。

Carbonite, Inc. は Carbonite データプロテクション、 ウェブルート サイバーセキュリティおよび MailStore 電子メールアーカイブの 3 つのブランドでお客様にサービスを提供しています。

ウェブルートについて

Carbonite の子会社であるウェブルートはクラウドや人工知能 (AI) を活用し、企業や個人のお客様をサイバー脅威から保護しています。管理サービスプロバイダーおよび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、およびセキュリティ認識トレーニングソリューションを提供します。 Webroot BrightCloud®脅威インテリジェンス・サービスは、シスコ、F5 ネットワークス、シトリックス、アルーバ、パロ・アルト・ネットワークス、A10 ネットワークスなどの市場をリードする企業で使用されています。ウェブルートは機械学習の力を活用して何百万もの企業や個人を保護し、接続された世界を保護します。ウェブルートは、北米、欧州、オーストラリア、アジアにかけてグローバルに運営されています。webroot.com で Smarter Cybersecurity®ソリューションについての詳細をご覧ください。

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