Press Release

平成31年4月16日

「ウェブルート脅威レポート2019」を発表

悪意あるURLの40%が安全なドメインから検出
家庭用デバイスの感染率は企業デバイスの2倍以上

セキュリティソフトをグローバルで展開し、セキュリティ業界をリードするウェブルート株式会社（本社：東京都港区、 代表取締役社長：伊藤 誉三、以下 ウェブルート）は、ウェブルート脅威研究チームによる2018年、1年間のサイバー脅威のデータを分析した「ウェブルート脅威レポート2019」を発表いたしました。レポートは、ウェブルートの最新クラウドベース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で取得・分析されました。このレポートでは、実証済みの攻撃が依然として脅威である一方で、新たな脅威が日々登場し、新たな犯行手口が展開されている実態が明らかになっています。

▼レポートの詳細はこちらをご参照ください。
https://wbrt.io/wmcaf

「ウェブルート脅威レポート2019」の注目点

悪意あるURLの40%が安全なドメインから検出

正当なウェブサイトは知らないうちに悪意あるコンテンツによって頻繁に侵害されています。ユーザの重要な情報を保護するためには、ウェブサイトの安全性を可視化し、サイトのレピュテーション（評判）をリアルタイムに入手することが必要です。

家庭用デバイスの感染率は企業デバイスの2倍以上

企業エンドポイントのウイルス感染率32%に対し、コンシューマーエンドポイントの感染率は68%と、2倍以上の差が見られました。

＜本件に関するお問合せ先＞
ウェブルート株式会社
マーケティング部　東田
Email: thigashida@webroot.com

＜報道関係者からのお問合せ先＞
ウェブルート広報事務局（カーツメディアワークス内）
担当：田口・佐藤・ジェレミー
Email: info@kartz.co.jp　Tel: 03-6427-1627

Press Release

WEBROOT®

フィッシング攻撃が36%増加、フィッシングサイトの数が220%増加

近年フィッシングサイトはSSL証明書やHTTPSを利用して訪問者に安全で正当なページだと信じ込ませています。しかしフィッシング攻撃の77%が金融機関になりすまし、HTTPSを利用する傾向が大きく見られます。実際に、標的となった金融機関のフィッシングページの80%以上でHTTPSが使用されていました。また、フィッシング全体で、偽装された企業の第1位はGoogleでした。

一度感染したデバイスの半数以上が年内に再感染

ウェブルートの調査によると、感染したデバイスの半数以上(53%）が１年以内に再感染していたことが判明しました。

マルウェアの3分の1近くが%appdata%フォルダへの潜伏を画策

マルウェアはどこにでも潜伏することができますが、主な潜伏先としては、%appdata%（29.4%）、%temp%（24.5%）、%cache%（17.5%）などが挙げられます。%temp%ディレクトリ、%cache%ディレクトリでの実行ファイルを禁止するだけで、IT管理者はマルウェアの起動率を4割以上減少させることができるのです。

仮想通貨の価格は下落、マイニングとクリプトジャッキングは増加

2018年ウェブルートが毎月観測したクリプトジャッキングのURL数は、9～12月にかけては2018年前半の2倍以上となりました。クリプトジャッキングは、サイバー犯罪者が身代金の支払いを待つ必要がなく、簡単なため、ランサムウェア攻撃よりも利益が高いのです。ウェブベースのクリプトジャッキングは依然として、Coinhiveが80%以上のシェアを持っていますが、類似するクリプトジャッキングツールがいくつか登場し、普及し始めています。

2018年はランサムウェアの脅威が減る一方、標的型が増加

主なランサムウェアは、2019年にさらに減少していくと予想されます。しかしマルウェア作成者は標的型攻撃にシフトし、多くの企業は引き続きランサムウェアの被害を受けることとなるでしょう。2018年のランサムウェア攻撃の多くは攻撃方法としてリモート・デスクトップ・プロトコル（RDP）を利用し、Shodanのようなツールを使ってシステムをスキャン、不適切なRDP設定のネットワークを見つけられます。このような安全性が低いRDP接続からシステムへアクセスし、すべてのシステムデータや共有ドライブを閲覧することで、ランサムウェアを展開するのか、他のマルウェアを使用するか、どちらがより儲かるのかと犯罪者は余裕をもって検討できるのです。

最高技術責任者ハル・ロナス（Hal Lonas）による総括

「私たちはサイバーセキュリティ領域における技術革新の重要性をよく語りますが、今年のレポートのデータを見れば、真の革新者はサイバー犯罪者であることが分かるでしょう。彼らは様々な攻撃手法を組み合わせ、最大の成果を得るため新たな方法を模索し、既存の攻撃方法と不正に組みあわせているのです。
企業の皆さまに今伝えたいことは、自社のリスクを認識・評価し、複数の攻撃方法から自社を保護できる「複層アプローチ」を生み出すことです。ウェブルートのソリューションは、その最適なアプローチの一つです。」

＜本件に関するお問合せ先＞
ウェブルート株式会社
マーケティング部　東田
Email: thigashida@webroot.com

＜報道関係者からのお問合せ先＞
ウェブルート広報事務局（カーツメディアワークス内）
担当：田口・佐藤・ジェレミー
Email: info@kartz.co.jp　Tel: 03-6427-1627

Press Release

WEBROOT®

ウェブルート株式会社セールスエンジニア　セバスチャン・アミゴによるコメント

昨年より、日本ではフィッシング対策のソリューションに関して、当社のパートナー様だけでなく、新規のお客様からも高い関心を寄せいただいております。現在、サイバーセキュリティ対策に関する情報が多くでまわっており、その中には誤った情報も混在しているようです。当社は、お客様のデバイスを保護するため、階層型セキュリティアプローチの採用をお勧めしております。
Windows 10のように、OS自体がより安全になったとしても、近年の複雑化したサイバー攻撃から身を守るためには、ネットワークやエンドポイントに特化した専用のセキュリティ対策が必要となります。

「ウェブルート脅威レポート2019」について

「ウェブルート脅威レポート2019」は、ウェブルート脅威研究チームによるサイバー脅威の現状の分析や知見、インサイトを示すものです。本レポートでは320億以上のURL、7億5,000万以上のドメイン、IPv4および使用中のIPv6の全42億アドレス、6,200万以上のモバイルアプリ、310億以上のファイル動作記録を分析しました。この年次レポートに含まれている数値は、弊社の最新クラウドベース機械学習アーキテクチャであるWebroot® プラットフォームで自動的に取り込まれ、分析された指標によるものです。このシステムは既知・ゼロデイ・未知・最新の永続的脅威に対し、ユーザーやネットワークを積極的に保護します。このプラットフォームから生み出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に使用され、また BrightCloud® 脅威インテリジェンスサービスを通じてテクノロジーパートナーにも使用されています。

ウェブルートについて

ウェブルートは Smarter Cybersecurity®のソリューションプロバイダです。インテリジェントなエンドポイント保護および脅威インテリジェンス・サービスによって「モノのインターネット」（IoT=Internet of Things／モノのインターネット）のセキュリティを実現。
クラウドベースで予測型の総合脅威インテリジェンス・プラットフォームを活用することによって、コンピュータ、タブレット、スマートフォン、そしてあらゆるデバイスをマルウェアや他のサイバー攻撃から保護しています。高い評価を受けているSecureAnywhere®インテリジェント・エンドポイント保護とBrightCloud®脅威インテリジェンス・サービスは、世界中で数千万台以上のエンドユーザ、企業、エンタープライズ機器を守っています。ウェブルートのテクノロジーは、業界トップリーダーである Cisco、F5 Networks、HP、Microsoft、Palo Alto Networks、RSA、Arubaなどのソリューションに採用され、高い信頼を得ています。本社を米国コロラド州に置き、北米、欧州、アジア環太平洋、日本でビジネス展開しています。
Smarter Cybersecurity®の詳細はウェブサイトhttp://www.webroot.com/jp/ja/ をご参照ください。

公式Facebookページ： https://www.facebook.com/WebrootJapan/
公式Twitterアカウント：https://twitter.com/Webroot_JP

＜本件に関するお問合せ先＞
ウェブルート株式会社
マーケティング部　東田
Email: thigashida@webroot.com

＜報道関係者からのお問合せ先＞
ウェブルート広報事務局（カーツメディアワークス内）
担当：田口・佐藤・ジェレミー
Email: info@kartz.co.jp　Tel: 03-6427-1627