Press Release

WEBROOT®

平成30年6月27日

高度化するサイバー攻撃にどう対応すべきか

「ウェブルート脅威レポート2018」を発表

～「Windows 10はWindows 7の2倍安全」「亜種・ポリモーフィック型マルウェアの広がり」など～

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、2017年の1月から12月を通じて収集したデータを分析した、年次レポート「ウェブルート脅威レポート2018」を発表いたしました。当調査をとおして、サイバー攻撃が年々高度化しており、既存のアンチウイルスソフトでは脅威に対抗できないことが分かりました。危険でダイナミックな脅威の状況が示され、リアルタイムの脅威インテリジェンスを利用した複層型の防御システムが企業や組織に求められています。

「ウェブルート脅威レポート2018」の注目すべき点

クリプトジャッキングの脅威が急速に増加

クリプトジャッキングは、標的となるPCやスマートフォンのCPU の処理能力を盗んで暗号通貨の採掘に使用するサイバー攻撃です。2017年9月以降、5,000以上のウェブサイトがJavaScriptの仮想通貨マルウェア「CoinHive」を通じてモネロ（仮想通貨）の採掘手法の被害に遭っています。

より安全なWindows 10への移行　企業では32%にとどまる

本調査によって、Windows 10はWindows 7と比較し約2倍安全なことが分かりました。しかし、企業におけるOS移行率はかなり低く、2017年末時点でWindows 10を利用している企業は32%にとどまっています。

ポリモーフィック型ウイルスの蔓延

自己複製の際に、プログラムのコードをわずかに変化させ亜種を作り出すことで検出を回避する「ポリモーフィック型ウイルス」が主流となりつつあります。2017年には、検出したマルウェアの93%、有害なアプリケーション（PUA）の95%が単一デバイス上で作られていました。残念ながら現在、既存のセキュリティソフトでは「ポリモーフィック型ウイルス」の検出はできません。

Press Release

WEBROOT®

ランサムウェア新型亜種の脅威

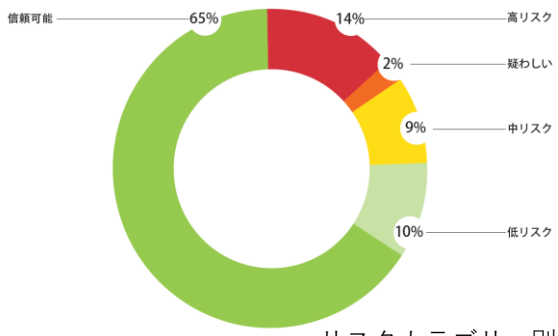
ランサムウェアとその亜種はさらに深刻な脅威となっています。過去1年間に、新規もしくは再利用されたランサムウェアの亜種が様々な目的でばらまかれ、たった24時間で、100か国以上で20万台以上の端末が「WannaCry」や「NotPetya」といったランサムウェアに感染しました。

悪質なIPアドレスの継続的な再利用

2017年には、感染によりスパムメールを送ったり、マルウェアの配布を行うなどした1万件の悪質なIPアドレスが平均18回再利用されていました。悪質なIPアドレスの65%はスパムサイト、次いでスキャナーが19%、Windowsのエクスプロイト（脆弱性を攻撃する）が9%となっています。

高リスクURLの増加拡大

2017年には、1日に数十万のウェブサイトが新たに立ち上げられ、そのうち、25%が悪質または疑わしいURL、もしくは中程度のリスクがあると判断されました。高リスクのURLは、33%がマルウェアサイト、プロキシ回避・アノニマイザーが40%と、2大カテゴリーに分類されます。



リスクカテゴリー別URL

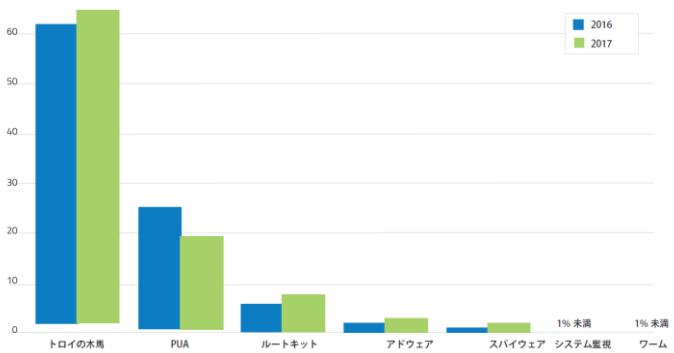
危険性が増した標的型フィッシング攻撃

フィッシング攻撃は標的型が増加しており、大きな成果をあげるためにソーシャルエンジニアリングやIPマスキングを利用しています。フィッシングサイトのオンライン時間は平均で4〜8時間となっており、従来のフィッシング対策を回避する設計となっていることが分かります。2017年に検知されたフィッシング攻撃の90%が、わずか62のドメインから発生していました。

また、2017年に最も偽装された企業は、52%が貨物運送会社「UPS」、23%が送金サービス会社の「Ria」となります。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、今後の標的として狙われる可能性が高くなると予測されます。

悪質なモバイルアプリによる世界的な脅威

モバイル機器も引き続き主要な標的となっています。調査の結果、32%のモバイルアプリが悪質なものと分かりました。悪質なモバイルアプリは、依然として悪質ではないプログラムを装った「トロイの木馬」が67%、次いで有害なアプリケーション（PUA）が20%と多くの割合を占めています。



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

▼レポートの詳細はこちらをご参照ください。
https://bit.ly/2KnW4sb

Press Release

最高技術責任者ハル・ロナス（Hal Lonas）の総括

過去1年間、サイバー攻撃はより攻撃的になり、独創性も非常に高まっています。当社のレポートにおいて、今年はじめてクリプトジャッキングが新たな脅威として登場しました。匿名性、展開の容易さ、低リスク、高い見返りといった攻撃者（犯罪者）が望むすべての要素を含んだ脅威です。企業や団体はリアルタイムに展開できるセキュリティシステムを利用して、新たな脅威を検知し、攻撃前に阻止する必要があります。

「ウェブルート脅威レポート2018」について

「ウェブルート脅威レポート2018」は、Webroot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、6,200万以上のモバイルアプリ、150億以上のファイル動作記録、520億以上の接続サーバーを分析しました。レポートに含まれている数値は、数百万の実世界のグローバルセンサーやサードパーティソースで自動的に取り込まれ、Webroot® 脅威インテリジェンス・プラットフォームで分析された脅威インテリジェンスの指標によるものです。Webroot脅威インテリジェンス・プラットフォームは高度なクラウドベース型機械学習ネットワークです。生成された脅威インテリジェンスはWebroot SecureAnywhere® エンドポイントやネットワークセキュリティ製品で利用され、またWebroot BrightCloud® 脅威インテリジェンスサービスを通じてウェブルートのパートナーにも利用されています。従来のリストベースやシングルベンダーの脅威インテリジェンスとは異なり、ウェブルートの脅威インテリジェンスは非常に高度なゼロデイ攻撃や、これまでにないAPT攻撃の特定・阻止に非常に効果的です。

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/

＜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