

ウェブルート 「2019年脅威動向予測」を発表

～生体認証システムの増加・IoT機器／接続デバイス認証団体など最新トピックスを紹介～

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、「2019年セキュリティ脅威動向予測」を発表しました。2018年は、サイバー攻撃や脅威に関する事件が多く発生し、大手IT企業から航空会社まで被害が相次いだ一方、個人のパソコン、デバイスを標的としたクリプトジャッキング詐欺も世界各地で発生しました。常に進化し続けるサイバーセキュリティ業界では2019年にどのような脅威やトレンドが予測されるのでしょうか。

生体認証システムの増加

スマートフォン利用時や様々なサービスなどの生体認証システムの導入が増加しており、2019年にはシステムの導入・利用がさらに増加するとみられており、ユーザー名とパスワードを使用しているログインはレガシーな選択となるかもしれません。

IoT機器／接続デバイス認証団体の発足

電化製品の浸透にともない、電気用品安全法が施行され、家電安全認証が進んだことと同様に、消費者向けIoT機器／接続デバイスの認証団体の発足が考えられます。スマート製品メーカーに『セキュリティ・バイ・デザイン』という概念が義務付けられます。

無料Wi-Fiの需要増加

日本国内では携帯キャリア大手3社が利用料金の値下げを発表しており、今後通信料の値下げにより、新規契約台数が増えると考えられます。また、2019年にはラグビーワールドカップ、2020年東京オリンピック・パラリンピックなど世界最大級のスポーツイベント、さらに2025年には大阪万博が開催されるため、無料Wi-Fiの需要は増加すると考えられ、利用者情報を守る安全な無料Wi-Fiが求められます。

標的型攻撃の広がり

2019年、サイバー攻撃はより高い精度でターゲティングされる可能性があります。2018年、ランサムウェアはクリプトジャッキングやバンキング型トロイの木馬と比較し、存在感が希薄でしたが、**Dridexグループ***の事例のように、標的を絞った計画的なサイバー攻撃が今後も発生すると考えられています。

クリプトジャッキング（仮想通貨採掘）とランサムウェア間の割合はビットコインなどで知られる仮想通貨の価格により変動が予測されますが、クリプトジャッキングの収益モデルは今後も利用を継続するでしょう。

*Dridexグループ: ヨーロッパを拠点とする主要銀行や金融機関の顧客を標的しているハッカー団体

ゼロデイ攻撃の減少

過去10年間でサイバー攻撃の金銭的コスト物理コストが劇的に高まっているため、ゼロデイ攻撃や個人情報の搾取は減少するとみられています。しかし、国家レベルの個人情報・機密情報の価値は下がることなく非常に高いままであり、今後も間違いなくターゲットにされますが、**Shadowbrokers***のような大規模ハッキング事件は少なくなることが予想されます。

*Shadowbrokers: アメリカ国家安全保障局の機密情報を公に漏洩させ、大手企業のファイアウォールやセキュリティソフトへのゼロデイ攻撃で有名なハッカー団体

ランサムウェアからクリプトジャッキングへ

一般的なランサムウェアの流行は減少傾向にあります。ランサムウェアが消えることはありませんが、エンドポイント対策の向上により疑わしいランサムウェアの動きからデバイスを保護する体制が整いつつあります。そのためマルウェア開発者は、さらに標的を絞った攻撃や、より巧妙なクリプトジャッキングなど代替手段へと切り替えていくと考えられています。

2019年脅威動向予測について

下記ウェブルートのサイバーセキュリティ担当による分析。

- ・ Jason Davison (上位脅威リサーチアナリスト)
- ・ Paul Barnes (製品戦略シニアディレクター)
- ・ Eric Klonowski (主席脅威リサーチアナリスト)
- ・ 池田 憲司 (ウェブルート日本法人)

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、業界トップライダーである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

©2018 Webroot Inc. All rights reserved. Webroot、SecureAnywhere、Webroot SecureAnywhere、Webroot BrightCloud、BrightCloud、Smarter CybersecurityはWebroot Inc.の米国その他の国における商標または登録商標です。その他の商標はすべてそれぞれの所有者に帰属します。

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