本プレスリリースは、米 Webroot, Inc.が 2017 年 9 月 21 日（現地時間）米国コロラド州ブルームフィールド で発表したプレスリリースを翻訳したものです。

2017 年 10 月 5 日
ウェブルート株式会社

【プレスリリース】

毎月150万近くの新たなフィッシングサイトが誕生

ウェブルート、「ウェブルート四半期脅威情報アップデート」（2017 年 9 月版）で、
フィッシング攻撃が質・量ともに進化し続けていることを明らかに

次世代のエンドポイントセキュリティと脅威インテリジェンスでセキュリティ業界をリードするウェブルートは、2017 年 9 月版の「ウェブルート四半期脅威情報アップデート」において、毎月平均して 138.5 万のフィッシングサイトが新たに作られ、5 月にはその数が 230 万と高い発生率を記録したと報告しました。ウェブルートが収集したデータによると、現在のフィッシング攻撃はより巧妙化して検出が難しく、ターゲットを絞り込んで実行されているために、攻撃を防ぐことが極めて困難になっています。最新のフィッシングサイトでは本物そっくりのウェブページが使用されているため、Web クローラーを使って見つけることはほとんど不可能に近く、標的にされた個人や組織から機密情報を窃取しています。

「ウェブルート四半期脅威情報アップデート」は、業界で最も高度な機械学習技術によって得た脅威インテリジェンスに基づき迅速かつ正確な情報を提供しています。報告書の全文（英文）は以下でご覧いただけます。 www.webroot.com/trends

主な調査結果と分析

- **フィッシング攻撃は 2017 年に入り、かつてないペースで拡大** – フィッシングは依然として法人、個人のいずれにとっても、最も直面する危険性が高いセキュリティの脅威の 1 つであり、幅広くまん延しています。1 日平均 46,000 以上のフィッシングサイトが新たに出現し、世界的にセキュリティ侵害の最大の原因となっています。膨大な数のフィッシングサイトが次々に創り出されるために、企業にとってフィッシング攻撃からの防御は極めて困難になっています。

- **依然として極めて短い フィッシング攻撃の存続期間** –フィッシングサイトのライフサイクルは、2017 年上半期も引き続き極めて短い傾向で、大半の場合、オンライン上でアクティブな時間はわずか 4～8 時間程度しかありませんでした。こうしたサイトはブロックリストのような従来のアンチフィッシング手法による検出をかいくぐるよう設計されています。1 時間ごとにリストを更新したとしても、情報を入手してリストとして提供されるまでに一般的に 3～5 日経過しているため、発表される頃には既に問題のサイトはユーザーから情報をだまし取った上で消滅している可能性があります。

- **ますます高度化し巧妙化する騙しのテクニック** – 過去のフィッシング攻撃では、大勢の人がウィルスに感染した添付ファイルを開いたり、悪質なウェブサイトを訪問したりすることを期待して、できるだけ対象を広げてランダムに攻撃が行われていました。現在の手口はより洗練されています。ハッカーはソーシャルエンジニアリングを活用して予め必要な個人情報を入手し、個別に攻撃を仕掛けるようになっています。フィッシングサイトも良性なドメインに隠れたり、本物の URL との区別をつきにくくして、悪質なペイロードを運んだり、なりすましサイトにユーザーを誘い込んだりしています。

- **特定の企業のなりすましによる攻撃がさらに進化** — フィッシング攻撃に使われるゼロデイのウェブサイトは毎月数百万に上る可能性があるものの、なりすましの対象にされている企業の数はそれほど多くはありません。ウェブルートはなりすましの被害に遭ったウェブサイトごとに URL を分類し、金融機関や IT 企業が最も多く被害を受けていることを明らかにしました。また、2017 年上半期の 6 カ月間になりすましの多かった企業上位 10 社を以下の通り、特定しました。
  - Google 35%
  - Chase 15%
  - Dropbox 13%
  - PayPal 10%
  - Facebook 7%
  - Apple 6%
  - Yahoo 4%
  - Wells Fargo 4%
  - Citi 3%
  - Adobe 3%

業界動向

- 2017 年 5 月 4 日付けの FBI Public Service Announcement によると、米国企業のフィッシング詐欺による損害は年間 5 億ドルに上っています。
- Verizon によると、セキュリティ侵害などのセキュリティ関連インシデントの 90%がフィッシングによるものでした。
- ESG の最新レポートによると、調査対象となったセキュリティやネットワークにおけるインフルエンサーや意思決定者の 63%以上が、過去 2 年間のうちにフィッシング攻撃を受けたと回答しています。
- 同じく、ESG のレポートでは回答者の 46%が、過去 2 年間でマルウェアによる攻撃がより標的型攻撃化したと答え、45%が過去 2 年間を上回る量のマルウェアが存在していると答えています。

BrightCloud® リアルタイム・アンチフィッシングについて

ウェブルートはネットワーク/セキュリティベンダーパートナーに、蔓延するフィッシング攻撃に対抗する独自のリアルタイム・ソリューションを提供しています。

- パートナーのテクノロジーや製品に統合

- リアルタイムで URL を検証し、ネットワーク遅延を高めることなくゼロアワーのフィッシング攻撃に対する保護を提供
- 高度な機械学習やコンテンツ・クラシフィケーション機能を活用し、フィッシングサイトを自動的に検出
- オンデマンドで、クロールを実行し、数百のサイト特性とサイトに関連する外部情報を利用して、リクエストされたすべての URL を数ミリ秒で評価

コメント

ウェブルートの最高技術責任者であるハル・ロナス（Hal Lonas）は、次のように述べています。「昨今のフィッシング攻撃は驚くほど巧妙化しています。ハッカーたちは悪質な URL を見破られないようにして巧みに心理をつき、事前に収集した情報をうまく使ってリンクをクリックさせており、サイバーセキュリティに詳しい専門家でさえ騙されかねません。被害者を責める代わりに、業界としてユーザー教育とリアルタイム・インテリジェンスを用いた組織的な保護とを組み合わせ、変わり続ける脅威に対して常に先手を打てるような体制を整えていく必要があります」

関連リソース

- ウェブルートのソリューション：ウェブルート BrightCloud 脅威インテリジェンス・サービス
- 前回の報告書：四半期脅威情報アップデート 2017 年 6 月版（英文）

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）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。

SNS: Twitter | LinkedIn | YouTube | Facebook

###

©2017 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。

＜本件に関する報道関係からのお問い合わせ先＞

ウェブルート株式会社 マーケティング部 東田
Email: thigashida@webroot.com

ウェブルート 広報代理 株式会社プラップジャパン
担当 高橋、白谷、谷本
Tel: 03-4580-9109/ Fax: 03-4580-9135
Email: webroot_pr@ml.prap.co.jp