BrightCloud® リアルタイム アンチフィッシング サービス

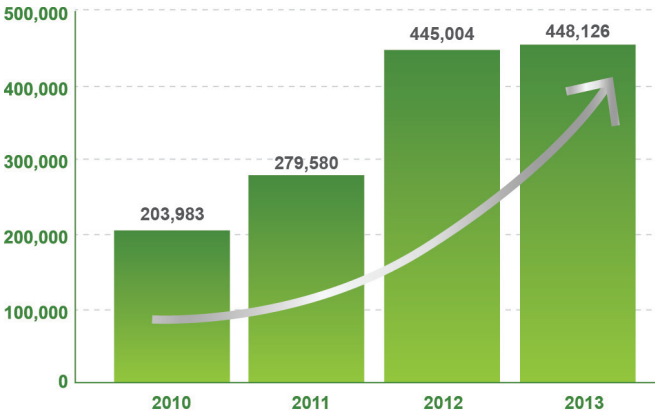
概要

- 最も危険なフィッシング サイトの存続期間は短く、日単位ではなく、分単位または時間単位であると考えられている
- 静的なフィッシング リストでは今日の攻撃のスピードに対応できない
- セキュリティ ベンダーは、BrightCloud® リアルタイム アンチフィッシング サービスにより、適時のサイト スキャンを利用して、悪意のあるサイトへのユーザーのアクセスを回避できる

インターネットには、数百万の新しいフィッシング サイトが散在しており、瞬く間に出現しては、消えていきます。ユーザーを保護するためには、検出時間を日単位ではなくミリ秒単位で考える必要があります。BrightCloud リアルタイム アンチフィッシング サービスを使用すると、パートナーは、ゼロ アワー フィッシングの脅威に対して、静的なフィッシング ブラックリストよりはるかに効果的な保護を提供できます。業界で最も高度な機械学習テクノロジーとリアルタイムの ウェブルート インテリジェンス ネットワーク（Webroot® Intelligence Network, WIN）によってサポートされているこのサービスでは、今日企業が直面しており、最も広く蔓延している脅威の 1 つに対する優れた保護を提供します。現在では、不正対策サービス、電子メール セキュリティ、電子メール インフラストラクチャ、ソーシャル メディア、SMS、Web ブラウザ、エンドポイント セキュリティ、DNS、境界セキュリティ アプライアンス、検索エンジン、モバイル アプリなどのベンダー、および携帯電話会社は、ユーザーを保護するために包括的なソリューションを使用しています。

米国および英国で IT ディレクターに行った Webroot® の最新の調査では、回答者の 55% が一番件数の多いセキュリティ侵害はフィッシングであると回答しています。[1] フィッシング攻撃およびスピア フィッシング攻撃は、今日、あらゆる規模の企業をターゲットにしており、サイバー犯罪者による、ネットワーク侵害を目的としたこれらの攻撃が急激に増えています。現在、フィッシング攻撃は、非常に巧妙化されており、多くの場合、IT セキュリティの専門家でさえ見破ることができません。RSA の最新の調査では、2013 年の世界全体での損失は 59 億ドルと見積もられています。[2]2012 年から 2013 年のフィッシング サイトの増加は比較的少ない一方で、フィッシング サイトは常に消えては現れ、より効率的になっており、財政損失は 2012 年より約 400% (15 億ドル) 増えています [3]。これは、高度な標的型の攻撃が有効であることと、従来のフィッシング対策ソリューションで検出される可能性が最も低いこの攻撃をより集中的に行われるようになったことを示しています。

フィッシングの増加数 (前年比)
2010 ～ 2013 年のフィッシング数



[1] Webroot Web セキュリティ調査。2012 年 12 月　[2] RSA「2013 年を振り返る (2013 A Year in Review)」2014 年 1 月　[3] RSA「フィッシングの年 (The Year in Phishing)」2013 年 1 月

フィッシング対策の静的なブラックリストは、毎時間更新されたとしても、多くの場合、現在のフィッシング攻撃には効果がありません。リアルタイムの URL 検証は、ゼロ アワー攻撃、偽装リダイレクト、最近ハイジャックされた Web サイトに対して真に効果のある唯一の保護です。BrightCloud® リアルタイム アンチフィッシング サービスでは、ユーザーがアクセスを試みている Web サイトのみに確実にアクセスできるようにすることで、ユーザーを保護します。サイトは、リクエスト時に検証され、適切かつ安全なサイトであることが保証されます。

「Webroot の機能を RSA の自動フィッシング検出と組み合わせると、より迅速に疑わしいフィッシング サイトを特定し、詳しい調査が必要な URL をすばやく特定できます。」

RSA、詐欺サイト対策ソリューション ディレクター、Avi Rosen 氏

フィッシング攻撃を直ちに止めさせる

BrightCloud リアルタイム アンチフィッシング サービスでは、高度なフィッシング攻撃を特定して阻止することで、セキュリティ侵害とデータ損失を回避できます。このサービスでは高度な機械学習およびコンテンツ分類を利用して、フィッシング サイトの検出を自動化します。Webroot では、判定の精度を向上させるため、確実性の高い判定を行うことができない場合に、まれに人間による評価を使用することがあります。この評価はシステムに反映され、これにより以降の判定の精度が上がります。

この新しいアプローチを幅広く検証したところ、このアプローチでは、競合製品の 3 ～ 5 日前にフィッシング サイトが検出されています。これは、フィッシング攻撃に対する防御での大きな進歩です。フィッシング サイトは、通常、他のフィッシング対策テクノロジーでは検出できないほど、存続期間が極めて短いため、迅速に検出することが、非常に重要です。

このサービスでは、クロールを実行し、数百のサイトの特性だけでなく、サイトに関連する外部要因を使用して、要求された URL を数ミリ秒で評価します。この外部要因には、Web 評価、IP 評価、サイトの存続期間、最新の脅威の履歴などの WIN のコンテキスト分析エンジンの関連付けられた情報があります。このサービスでは、要求された各 URL のリスク スコアを表示します。

パートナーの利点

- **競合他社から自社を差別化**
  フィッシング攻撃に対する極めて正確な、次世代のリアルタイムの保護を提供できる
- **WIN の利用**
  世界で最も強力なクラウド ベースのセキュリティ分析エンジンを利用できる
- **統合および使用が簡単**
  RESTful API および SDK を使用してソリューションに容易に統合できる
- **ユーザー エクスペリエンスへの影響が最小限で済む**
  サイトをリアルタイムにスキャンして、高度な保護を提供すると同時に、ユーザーの介入を最小限に抑えることができる

BRIGHTCLOUD® リアルタイム アンチフィッシング サービスの活用

ユーザーがインターネットにアクセスするたびに、BrightCloud リアルタイム アンチフィッシング サービスは、オンライン アカウントが意図せず侵害されたり、悪意のあるサイトで不要なマルウェアを入手したりしないようにユーザーを保護できます。さらに、このサービスを統合すると、次のことが可能になります。

- ネットワーク アプライアンスの Web セキュリティを向上させる
- 不正対策サービスのために新しいゼロ アワー脅威を特定する
- Web ブラウザおよびプグインに安全な閲覧を提供する
- 電子メール フィルタリング ソフトウェアおよびエンドポイント セキュリティ製品を強化する
- ソーシャル ネットワーク、ブログ、およびメッセージング アプリでユーザーが生成したコンテンツをフィルタリングする

統合オプション

Webroot では、RESTful Web サービスおよび SDK を提供しており、パートナーは BrightCloud リアルタイム アンチフィッシング サービスを自社のソリューションに簡単に組み込むことができます。また、他の BrightCloud サービスと同じ SDK を使用して、このサービスを既存のセキュリティ ソリューションと組み合わせることで、統合を可能な限りシンプルにできます。

ウェブルートについて
ウェブルートは、サイバー セキュリティに焦点を当て、個人および企業向けのソリューションである Webroot SecureAnywhere® の一連の製品群および、テクノロジー パートナー向けの BrightCloud® セキュリティ インテリジェンス ソリューションを通じて Software-as-a-service(SaaS) がもつパワーをインターネット セキュリティの世界にもたらしています。その結果、Net PromoterScore による顧客満足度ではナンバー 1 を誇っています。詳細については、http://www.webroot.co.jp をご覧ください。

ウェブルート株式会社
〒107-0062
東京都港区南青山 3-13-18
313 南青山 8F
+81 3 4588 6500