BrightCloud® IP レピュテーション サービス

概要

- インターネット上のすべてのパケットに、発信元 IP アドレスと宛先 IP アドレスがある
- 悪意のある IP との通信の無効化は効果的であるが、包括的なインテリジェンスなしでは困難
- BrightCloud® IP レピュテーション サービスでは、最新の IP インテリジェンスを提供しており、パートナーはユーザーのネットワークの保護を強化できる

現在、サイバー犯罪者が利用できるエクスプロイトや攻撃手法は莫大な数に上ります。また、サイバー犯罪者は暗号化通信、DNS キャッシュ ポイズニング、URL リダイレクション、ハイパーリンクの難読化など、数えきれないほどの手法を駆使して、自分の個人情報や活動を隠ぺいします。ただし、インターネット上のすべてのパケットには、発信元 IP アドレスと宛先 IP アドレスがあるため、既知の悪意のある IP が発信元または宛先である通信を無効にすると、非常に効果的です。では、ブロックする IP はどのように判別したらよいでしょうか。

公開されている IP リストの多くは、静的なもので、最新ではありません。つまり、このようなリストでは、動的な IP アドレスに対応できず、新しい未知の脅威をブロックすることができません。また、正しい IP が悪意があるものとしてリストされていることも多々あります。

BrightCloud IP レピュテーション サービスにより、ネットワーク ベンダーおよびセキュリティ ベンダーは、動的な IP レピュテーション サービスを自社の防御に追加することで、ユーザーのセキュリティを強化することができます。Webroot では、既知の悪意のある IP アドレスを、継続的に更新されるフィードでパートナーに提供します。これにより、パートナーのユーザーの IT セキュリティ管理者は、容易に脅威を特定して、ネットワークを保護できます。

このサービスを使用すると、新規および既存の IP 脅威の特定にかかる時間が大幅に短縮されるため、セキュリティの有効性と効率性が飛躍的に向上します。BrightCloud IP レピュテーション サービスでは、IP アドレスの調査にかかる時間が短縮されるだけでなく、脅威の種類や、脅威の履歴データおよび地理位置情報データが視覚化されるため、セキュリティ管理者は、より適切に脅威を特定できます。

BrightCloud IP レピュテーション サービスでは、ウェブルート インテリジェンス ネットワーク（Webroot® Intelligence Network, WIN）を使用しています。WIN では、ビッグ データ アーキテクチャを使用して、現在利用できるものの中で最も包括的かつ正確な脅威インテリジェンス（新たに出現した脅威の IP に関する最新のインテリジェンスを含む）を提供します。これには、約 1,200 万個の危険な IP で構成される動的なリストが含まれており、主要な IP 脅威にも対応しています。主要な IP 脅威には、スパム発信元、Windows エクスプロイト、Web 攻撃、ボットネット、スキャナ攻撃、サービス拒否、評価への脅威、フィッシング、プロキシ攻撃、およびモバイル脅威などがあります。また、ユーザーは、IP レピュテーション サービスの監視対象である約 43 億の IP アドレスに関する一連の豊富なメタデータにアクセスすることもできます。

WIN では、非常に多くの要素にわたってデータの分析および関連付けを行い、予測リスク スコアを作成します。このスコアは、信頼可能なものから悪意のあるものまでの 5 つの評価ランクのいずれかになります。すぐに最新ではなくなってしまう静的な公開されたブラックリストを使用するのではなく、BrightCloud IP レピュテーション サービスでは、動的な IP 評価データをほぼリアルタイムに（5 分ごと）ネットワーク デバイスに提供します。パートナーは、このサービスを統合することで豊富な IP フィルタリング ポリシーを介してユーザーを保護することができます。BrightCloud IP 評価指標では、1 ～ 100 の範囲のスコアが提供されます。このスコアは、「信頼できる」、「危険度 - 低」、「危険度 - 中」、「疑わしい」、および「危険度 - 高」のランクに分けられます。

より低いスコア（危険性がより高い）は、その IP が悪意のある IP である可能性が高いか、悪意のある IP になる可能性が高く、信頼できる IP より高い頻度で監視されます。この評価のランクを使用すると、企業は、リスクの許容度およびビジネス ニーズに基づいて、セキュリティ設定を詳細に調整できます。これにより、危険な IP または危険性の高い IP と自社のネットワークとの通信を制限することで、攻撃を前もって防止することができます。たとえば、セキュリティ要件が非常に高いある銀行では、80 未満のスコアの IP をすべてブロックすることを選択し、ある企業では、アクセスされるサイトがパートナーと提携している場合はスコアが 60 より高い IP からのトラフィックを受け入れることを選択します。

BrightCloud IP 評価指標

01-20 危険度 - 高		**危険度が高い IP アドレスです。この IP がインフラストラクチャおよびエンドポイントに悪意のあるペイロード、サービス妨害攻撃などの攻撃を行う可能性が高いことが予測されます。**
21-40 疑わしい		**疑わしい IP です。この IP がインフラストラクチャおよびエンドポイントに攻撃を行う可能性が平均より高いことが予測されます。**
41-60 危険度 - 中		**概して無害な IP ですが、セキュリティ リスクを示唆するいくつかの特性を示しています。この IP がインフラストラクチャおよびエンドポイントに攻撃を行う可能性がある程度あります。**
61-80 危険度 - 低		**無害の IP で、ユーザーがセキュリティ リスクにさらされる特性はほとんど示されていません。攻撃を受ける危険性はほぼないことが予測されます。**
81-100 信頼できる		**クリーンな IP であり、セキュリティ上の危険はありません。インフラストラクチャおよびエンドポイントが攻撃を受ける危険性が極めて低いことが予測されます。**

BrightCloud® IP レピュテーション サービス

BRIGHTCLOUD WEB レピュテーション サービスによるパートナーの利点

» **競合他社から自社を差別化**
業界最先端の悪意のある IP に対する保護を、ほぼリアルタイムでユーザーに提供できる

» **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

» **ネットワークに影響が少ない**
ネットワーク デバイス経由で保護し、不要なトラフィックをなくすことによりユーザーのキャパシティを増やすことができる

BRIGHTCLOUD IP レピュテーションの活用

リストを最新かつ正確に保つため、Webroot では、保留手法を使用して IP を評価します。このサービスでは、次のことを実行します。

» 疑わしい IP を特定する自動化アルゴリズムを導入
» IP を調査して関連付けを行う
» 組み込み型のルールを適用して、IP をテストする
» IP を制限するかどうかと、制限を行う期間を決定する
» IP に関する制限を解除する。ただし、監視は継続する

このサービスでは、企業ユーザーが IP 脅威に対抗する能力を向上できるだけでなく、他の多くの IP レピュテーション サービスで必要な、面倒なセキュリティ処理を回避できます。このサービスを使用することで、ネットワーク境界アプライアンスの IP インテリジェンス サービスを強化し、悪意のあるアドレスが送信元または宛先であるトラフィックをブロックすることで、機密データを保護します。また、このサービスを使用すると、既知のフィッシング プロキシを追跡し、ユーザーが中間者攻撃などのフィッシング サイトからの悪意のあるリクエストを回避したり、警告で応答したりすることもできます。

統合が容易

直観的に使用できるソフトウェア開発キット (SDK)、REST サービス、および API を使用すると、パートナーは BrightCloud セキュリティ サービスを簡単に自分のソリューションに統合できます。また、他の BrightCloud サービスと同じ SDK を使用して、BrightCloud IP レピュテーション サービスを既存のセキュリティ ソリューションに組み込むことで、複数のサービスの統合がより簡単になります。BrightCloud IP レピュテーションでは、エンドポイントにフル データベースがダウンロードされ、5 分ごとに更新されます。

世界中の戦略的パートナーが、次世代のファイアウォールからネットワーク ロード バランサまで、ネットワーク ソリューションへの Webroot の統合に成功しています。Webroot が提供する統合は複雑でないため、世界中のネットワーク ベンダーおよびセキュリティ ベンダーが、このソリューションをシンプルかつ容易に実装できます。

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