NEWS RELEASE

2010 年 3 月 31 日
株式会社ブロードバンドセキュリティ

BBSec が、クラウドマークのレピュテーション DB を搭載した Web コンテンツ改ざん防止ソリューション「Cracker Detect EXOCET」のサービスを開始
～「ドライブバイダウンロード攻撃の連鎖を食い止めろ！」～

株式会社ブロードバンドセキュリティ（本社：東京都新宿区　代表取締役社長　持塚　朗　以下 BBSec）は、Web サイトコンテンツ改ざん防止ソリューションとして新サービス「Cracker Detect EXOCET」（クラッカーディテクトエグゾセ）のサービスを開始しました。

ドライブバイダウンロード攻撃の脅威～進化するガンブラー亜種

2009 年 12 月からガンブラーと呼ばれるドライブバイダウンロード攻撃手法による Web 改ざん被害が急拡大しており、連日のように国内企業においても Web サイト改ざん被害のニュースが報道されております。

また、さらなる亜種が増加、進化を続け新たな脅威を生んでおります。
最新の攻撃では、パターンマッチングなどでの検出を回避するため、動的に生成される高度に難読化された JavaScript 内に悪意のあるプログラム（マルウェア）へのリンクを埋め込む攻撃手法が主流になっています。
また、「.htaccess」ファイル内に不正なリダイレクトを埋め込む事例が発見されています。単なる、外部からの HTTP アクセスによる Web ページスキャンでは「.htaccess」ファイル内の記述まで確認することができません。
こうした進化する攻撃に対して BBSec では、新サービス「Cracker Detect EXOCET」にて防御を実践いたします。

Cracker Detect EXOCET サービス概要 （特許出願中）

■改ざんコンテンツの公開を水際で阻止
業界初の FTP プロキシー型のリアルタイム改ざん検知により改ざんコンテンツの公開を防ぎます

■リンク評価にクラウドマーク社のレピュテーション DB を採用
SNS だけで 1 億 3000 万アカウントを守る「Cloudmark Sender Intelligence」を採用しました
レピュテーション DB の情報更新が圧倒的に高速です

■難読化リンクも.htaccess の改ざんも未然に防ぎます
HTTP 経由の改ざん検知ソリューションの弱点は EXOCET（エグゾセ）には存在しません

■フィッシングサイト等へ向けたリンクの埋め込みも未然に防ぎます
レピュテーションは犯罪サイト全般を網羅しています

■改ざんに使用された FTP アカウントもお知らせします
事後処理のための完璧な情報を提供致します

■大規模サイトでは検出用アプライアンスを設置・運用
必要最小限の稼働コストで余計な設備投資や回線負荷を生じさせません
LDAP でのユーザ認証に対応しています（各種 DB に対応予定）

■小規模サイトでは FTP プロキシーの ASP を提供致します
FTP アカウント情報は弊社側で LDAP に登録致します

Cracker Detect EXOCET では、ガンブラー等の攻撃手法により FTP の ID、パスワードなどが入手され第三者による悪意のある不正なリダイレクトの付加されたコンテンツやコンテンツ制御ファイルが

NEWS RELEASE

アップロードされようとした際に、当該ファイルをチェックし、問題があると判定された場合はコンテンツのアップロードを抑止し、お客様のシステム担当者にメールで通知します。FTP アカウントを盗用され、第三者による改ざんコンテンツがアップロードされた場合、即座にその注意喚起と対策を可能にします。

・ **難読化されたスクリプトを解読して URL を抽出**

最新の攻撃では、パターンマッチングなどでの検出を回避するため、動的に生成される高度に難読化された JavaScript 内にマルウェアへのリンクを埋め込む手法が主流になっています。
当システムでは、難読化を解除し、以下の分析手法を利用し、危険なリンクの付加されたコンテンツがアップロードされることを防ぎます。

1. クラウドマーク社のレピュテーション DB※によりリンク先の信用度を分析

世界で 1 億 3,000 万人が利用する最大規模の SNS サイトでも採用された、クラウドマーク社（Cloudmark, Inc. 本社:米カリフォルニア州、日本事務所:東京都千代田区 代表者 小島國照）の IP レピュテーションサービス「Cloudmark Sender Intelligence (以下 CSI)」を採用し、リンク先サイトの信用度を分析します。この CSI は、全世界で 10 億人を超す Cloudmark ユーザコミュニティからのトラフィック・パターン、フィンガープリント、フィードバック情報などによりリアルタイムで更新され、これらの相関を解析、レピュテーションスコアをリアルタイムに算出します。分析の結果、信用度が低いと判断されたサイトへのリンクを含むコンテンツは、アップロードをブロックします。

※レピュテーションとは、スパムメールを受け取らないようにしたり、悪意ある Web サイトからウイルスをダウンロードしないようにするために、通信相手の“評判”(reputation)を事前に調べて通信を制限する技術を意味します。レピュテーションによって脅威に対するフィルタリング効果が高まり、スパムメールの受信やウイルスの感染を未然に防ぐ効果が実現されます。

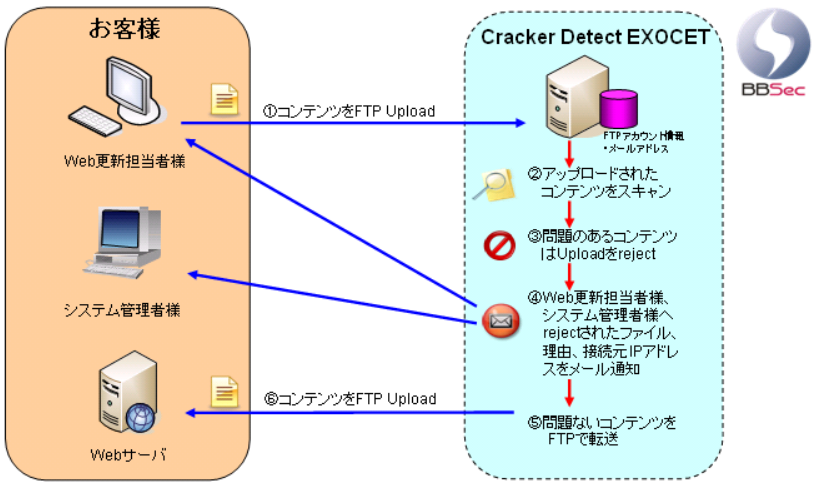
2. さらにホワイトリスト、ブラックリストにより、レピュテーションによる制御を補完

上記1の判定に加え、お客様にてホワイトリスト、ブラックリスト※の定義が可能です。
レピュテーション分析を補完した、お客様環境に合わせた柔軟な運用が可能になります。

※ホワイトリスト、ブラックリスト登録 URL はお客様よりご指定いただきます。

・ **最新のドライブバイダウンロード攻撃への対応**

最新の攻撃では、「.htaccess」ファイル内に不正なリダイレクトを埋め込む事例が発見されています。
外部からの Web ページスキャンでは、「.htaccess」ファイル内の記述まで確認することができません。
アップロードされたファイル全てをスキャンできる、当システムだけがこうした最新の攻撃手法に対応することができます。



NEWS RELEASE

・ 感染 PC、FTP アカウントの特定、注意喚起が可能

多く企業は、自身が不正なマルウェア等に感染していることには気付かずにコンテンツのアップロードを行なっている場合があります。当システムでは、アップロードを reject するだけではなく、LDAP でディレクトリサーバを参照することにより FTP アカウントと連絡先メールアドレスを紐付け、なぜアップロードが reject されたのかを連絡先に通知することができます。
この機能により、万が一改ざんコンテンツがアップロードされた時にどの FTP アカウントが利用されたかを認識することができ、二次的な改ざん被害を食い止めることができます。

・ 既存システムへの負荷影響を最小に

ファイルの受付からスキャン、access/reject 処理や警告メール送付など、全ての機能は当システム上で対応します。そのため、既存システムに対して本サービスの利用による大きな負荷上昇などはなく、逆に不要なコンテンツのアップロード処理などを削減できるため、既存システムの安定運用にも寄与します。

【サービスサイト】

（Cracker Detect EXOCET ご紹介ホームページ）http://www.bbsec.co.jp/solution/exocet.html

【BBSec が提供するセキュリティソリューションについて】

BBSec は、「セキュリティの本質」にこだわった本格的なセキュリティビジネスを展開する上で最も必要なセキュリティプロフェッショナルによる体制を強化しております。PCI SSC が認定する PCI DSS 監査資格者「QSA」、国際システムセキュリティ認証コンソーシアムが認定する CISSP など国際的なセキュリティ資格を数多く取得し、最新のセキュリティノウハウとセキュリティにおける高い意識をもったエキスパートを育成しております。今後も、これらのセキュリティエキスパートがお客様の情報システムの安全性を高めていくサービスを企画提供してまいります。

〔会社概要〕

企業名：株式会社ブロードバンドセキュリティ
本社所在地：東京都新宿区西新宿 8-5-1 野村不動産西新宿共同ビル 4 階
サービス内容：1. セキュリティ診断／コンサルティングサービス
2. セキュアメールサービス 3. マネジメントサービス
4. ネットワークインテグレーションサービス 5. Web ホスティングサービス
設立：2000 年 11 月 30 日
代表者：代表取締役社長 持塚 朗
ホームページ：http://www.BBSec.co.jp/

企業名：クラウドマーク ジャパン
所在地：〒101-0032 東京都千代田区岩本町 2-5-9 パステルコート神田岩本町 501
サービス内容：クラウドマークの代表的な製品は、世界中の 10 億人以上の登録ユーザが「スパムか」「正規メールか」をリアルタイムにレポートする「コラボレーション方式」のスパムフィルタとしています。メールに含まれる変更不可能な情報(フィンガープリント)をスパム判定に利用するため、スパムかどうか判断をユーザに委ねる必要があるグレーゾーンのメールも適切に判定でき、メールの文書内容や言語に依存せず、PDF スパムや SNS スパムのような新種や亜種への対応も実現しています。
クラウドマークのソリューションには、キャリアグレードのスパム/フィッシング/ウィルス対策フィルタ「Cloudmark Authority」、メールストア用フィルタ「Cloudmark ActiveFilter for Mail Stores」、エッジメール転送エージェント「Cloudmark Gateway」、メールクライアントプラグイン「Cloudmark Desktop」などがあり、リアルタイムデータを使用し、業界で最も精度が高く包括的な送信者プロファイルを作成する「Cloudmark Data Services」も提供しております。
代表者：小島國照
ホームページ：http://www.cloudmark.jp/

NEWS RELEASE

【サービスについてのお問合せ】
株式会社ブロードバンドセキュリティ
営業部
TEL：03-5338-7425
E-mail:sales@BBSec.co.jp

【本リリースに関するお問合せ】
株式会社ブロードバンドセキュリティ　広報担当　田中
TEL：03-5338-7430
E-mail：press@BBSec.co.jp