NEWS RELEASE

2010 年 1 月 22 日
株式会社ブロードバンドセキュリティ

BBSec が、「Gumblar（ガンブラー）対策トータルソリューション」の販売を開始

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、「Gumblar（ガンブラー）対策トータルソリューション」の販売、サービスの提供を開始します。

2009 年 12 月から 2010 年 1 月にかけてガンブラー（Gumblar、別名 GENO ウイルス）と呼ばれる攻撃手法による Web 改ざん被害が急拡大しています。特に 2009 年年末から 2010 年年始にかけては、国内大手企業が Web サイト改ざんの被害を受け、そのサイトを閲覧したユーザが不正なサイトへと誘導され、ウイルスに感染する等の被害が多発しています。ガンブラーの脅威は、パターンを変えた新しい攻撃スクリプトが大量に登場してきていることにあり、この攻撃手法によるウイルス感染の強力な連鎖性は昨今、類を見ないものとなっております。

BBSec では、こうした背景のもと、「Gumblar（ガンブラー）対策トータルソリューション」のサービスを開始し、改ざん検知から事後対策、未然防止までをワンストップで提供します。

【猛威をふるうガンブラーの特徴】

ガンブラーとは 2009 年 5 月頃より急激に広まったドライブ・バイ・ダウンロード攻撃の一種で、当初攻撃者が用意したマルウェア配布サイトのドメインが gumblar.cn であったことからこの名前が付けられました。

ガンブラーの特徴は、改ざんされた Web サイトを閲覧したユーザを不正なサイトへと誘導し、不正プログラム(FTP アカウントを盗み出すトロイの木馬や外部からの操作を可能にするバックドア、偽セキュリティソフトなど)を自動的にダウンロードさせる攻撃手法のことです。ガンブラーの場合は、一連の攻撃の中でダウンロードされるウイルスが OS の脆弱性や Adobe Reader/Acrobat/Flash Player 等アプリケーションの脆弱性を突くため、これら脆弱性が対策されていない PC から改ざんサイトを訪問した場合に影響を受けます。

ウイルスに感染したユーザを別サイトへ誘導してさらに別のウイルスに感染させたり、ボットに感染させたりする攻撃は以前より存在していましたが、ガンブラーがこれほどまでに被害を拡大した原因には、FTP アカウントの盗用が大きく関連しています。攻撃者はウイルスに感染したコンピュータから盗んだ FTP アカウント情報を使用して“正面”から Web サイトへ侵入し、サイトの内容を改ざんすることで新たな「ガンブラー誘導サイト」をネズミ算式に増やしていったのです。

2009 年年末から 2010 年年始にかけて行われた攻撃では、誘導先の攻撃サイトが頻繁に変更されていること、また攻撃コードやダウンロードされる不正プログラムも多岐に渡ることから、攻撃手法は類似していても当初のガンブラーとは、全く別のものであると考えられます。昨今見られる攻撃では、「GNU GPL」「CODE1」「LGPL」等の記述が含まれており、難読化や著名なドメインを使用するなど、ウイルス対策ソフトの検知を回避しようとするのが特徴となっています。

企業の Web サイトが改ざんの被害を受け、そのサイトを閲覧したユーザがさらにウイルスに感染する等の被害が多発しており、Web サイトの改ざんを受けた企業は被害者であるだけでなく、第三者に感染を拡げる

NEWS RELEASE

加害者ともなりえるため、深刻な問題であることはもちろんのこと、適切な対策が求められています。

このように、ガンブラーの脅威は、パターンを変えた新しい攻撃が大量に登場し、閲覧者を通じて感染の被害を拡大させるものであり、今後における徹底的な対策が必要なのです。

【Gumblar（ガンブラー）対策トータルソリューション　サービス概要】

ガンブラー対策については、お客様の抱える不安要素は様々です。自社 Web サイトの改ざん被害の確認から、PC 対策、未然防止対策など、BBSec では、様々なソリューションをご提案いたします。

BBSec の Web 改ざん検知サービス「Cracker Detect」の特徴は、改変された Web ファイルの差分を比較し、未知の攻撃手法であっても検知が可能となっております。

ガンブラーは、パターンを変化させ、複雑かつ巧妙な攻撃に進化を続けています。
企業におけるリスク対策としては、様々な攻撃に対する定期的な監視と検知が必要であり、「Cracker Detect」では、その機能を実現しております。

また、お客様のご要望にあわせ、「Cracker Detect +（プラス）」では、セキュリティエンジニアによる現地オンサイトでの確認調査も行います。

ケース別課題	サービス内容
Case1 **Web サイトの改ざんチェック**	***Cracker Detect +（プラス）*** ①サーバ上のすべてのテキストファイルをダウンロード ②コンテンツ作成者が作成した元ファイルを準備 ③双方のファイル内容を比較し差分を抽出 ④抽出した内容から Gumblar（及び亜種）との関連性を分析 ※セキュリティエンジニアによる現地オンサイトあり。
Case2 **Web サイト及びコンテンツの管理者 PC の感染チェック**	***Cracker Detect for PC*** ①複数のアンチウイルスソフトで対象の PC をチェック ②公開された情報を基にレジストリ、システムファイル等の改ざんをチェック ③パケット解析ツールを導入し不審なパケットの有無を分析（パケット分析サービス）
Case3 **改ざんされた Web サイトの復旧**	***Cracker Restore for Web*** ①ネットワークから隔離しサイトを停止（別サーバでの仮運用は可能） ②設定情報等のバックアップ ③OS、ミドルウェア等のクリーンインストール ④設定情報の投入 ⑤各種ログイン ID／Password の再設定（旧 ID／Password の再利用禁止） ⑥コンテンツの元ファイルをアップロード
Case4 **未改ざんまたは復旧後の Web サイトへの予防措置**	***Cracker Protection for Web*** ①改ざん検知の仕組みを導入（Cracker Detect） ②Web アプリケーションのソースコード診断（S.Q.A.T. Core） ③Web アプリケーション、ネットワークの脆弱性診断（S.Q.A.T. A&P） ④Internet 以外のネットワークのバックドア調査
Case5 **感染した PC の復旧**	***Cracker Restore for PC*** ①ネットワークから隔離

NEWS RELEASE

	②設定情報等のバックアップ ③OS、アプリケーションのクリーンインストール ④最新のセキュリティパッチの適用（当社指定ソフトウェアのみ） ⑤アンチウイルスソフトの最新の定義ファイルを適用 ⑥設定情報の投入
Case6 **未感染または復旧後の PC への予防措置**	***Cracker Protection for PC*** ①最新のセキュリティパッチの適用（当社指定ソフトウェアのみ） ②アンチウイルスソフトの最新の定義ファイルの適用

【サービスサイト】

（Gumblar 対策トータルソリューション） http://www.bbsec.co.jp/solution/gumblar.html

（Cracker Detect～Web 改ざん検知サービス） http://www.bbsec.co.jp/solution/crackerdetect.html

【BBSec が提供するセキュリティサービスについて】

BBSec では、最新のセキュリティノウハウと豊富なセキュリティ監査経験を持ったセキュリティエキスパートが今後もお客様の課題・要望に応じて対応し、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/

【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