

2011年10月13日

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

【報道資料】

チェック・ポイント、革新的なボット防御ソリューションを発表

先進の検出技術によりゲートウェイ上でボット攻撃を阻止する「Anti-Bot Software Blade」

ゲートウェイからエンドポイントまでの包括的セキュリティを提供するチェック・ポイント・ソフトウェア・テクノロジーズ株式会社（本社：東京都新宿区、代表取締役社長 藤岡健）は本日、ボットやAPT（Advanced Persistent Threats）への防御機能を提供する新製品、「[Anti-Bot Software Blade](#)」を発表しました。サイバー犯罪者がコンピュータを乗っ取るために使用する不正ソフトウェアの一種であるボットは、データを盗み出す、ネットワーク・リソースに不正アクセスする、サービス妨害（DoS）攻撃を仕掛ける、スパム・メールを送信するなどの違法行為を行うために使用されます。また、遠隔操作されているため、その多くはユーザに気付かれることなく秘密裏に活動します。今回発表された「[Anti-Bot Software Blade](#)」を使用すると、コンピュータに感染しているボットを検出し、そのコンピュータと遠隔地にいるボット管理者との間の通信を遮断して、ボットによる被害を防ぐことができます。この新ソリューションはゲートウェイに統合され、ボットの脅威に対する多層防御を提供します。最大 40 Gbps超という優れたトラフィック・パフォーマンスを実現しているため、企業で使用するすべてのコミュニケーション・チャネルを確実に保護することが可能です。

ボットは大規模なマルウェア攻撃を行うことが可能なため、組織のコンピュータがボットに感染すると、社会的信用の低下やデータ漏洩、金銭的損害などの被害が生じるおそれがあります。ZeusやMariposaに代表されるボットネット（ボットに感染したコンピュータで構成されるネットワーク）は、口座情報を盗み出したりDoS攻撃を仕掛けたりといった犯罪活動を行うマルウェアとして知られています。このようにすでに知られているボットネットもありますが、ほとんどの場合はその把握が困難であり、誰にも気付かれず秘密裏に増殖している場合があります。サイバー犯罪者は、ボットの検出を免れるためにさまざまなステルス技術を駆使しており、アンチウイルス・ソフトウェアの機能を無効にしてボットの存在を隠蔽する、暗号化などの技術によってボットのトラフィックを正当なトラフィックに偽装する、などの手法がその代表例です。またボットは、StuxnetやOperation Auroraなどで知られるAPT（Advanced Persistent Threats）と呼ばれる標的型攻撃の手段としても使用されます。

チェック・ポイントの「[Anti-Bot Software Blade](#)」は、ボットの検出や駆除、将来的な被害予防などのボット対策を可能にする高度な技術を備えています。このソリューションの核となる、Multi-tier ThreatSpect™と呼ばれるチェック・ポイント独自の検出エンジンは、各ゲートウェイを通過するトラフィックを分析して、数百万通りのアウトブレイク・タイプを検知します。その後、ボットネットのパターンやボットに対する指令の発信元、攻撃時の行動予測など複数のリスク要因を相関分析してボットを見つけ出します。検出された場合は、ボットや

そのビジネスへの影響(データの漏洩や詐欺的なスパム・メールの送信など)が分かりやすく表示されるダッシュボードを使用し、ボットのリスク・レベルを素早く分析することが可能です。管理者はこれらの情報に基づき、多彩なフォレンジック機能を使用してボットの感染状況を調査し、その結果を多層防御態勢の構築や迅速な問題解決に役立てることができます。

「Anti-Bot Software Blade」は、先進の検出技術を備えるだけでなく、[IPS](#)や[Antivirus & Anti-Malware](#)、[URL Filtering](#)などチェック・ポイントの既存のセキュリティ技術と統合することが可能です。これにより、各ゲートウェイ上で多層防御態勢を構築し、ボットに対する革新的な防御を実現できます。「Anti-Bot Software Blade」は、最大 40 Gbpsという優れたトラフィック・パフォーマンスを実現する業界初の統合型ボット防御ソリューションです。

「Anti-Bot Software Blade」の主な機能と利点:

- **多層型の革新的なボット検出技術:** チェック・ポイントの Multi-tier ThreatSpect™ エンジンが、インラインの防御としてゲートウェイを通過するネットワーク・トラフィックを分析し、複数のリスク要因を相関分析してボットを検出します。また、「Anti-Bot Software Blade」にアップデートを自動配信するリポジトリである ThreatCloud™ により、ボットに関する情報が随時提供されるため、新しいタイプの脅威にも容易に対応できます。
- **事前防御:** ボットに感染したコンピュータとボットの指令(C&C)サーバとの間の通信を遮断し、サイバー犯罪者によるネットワークの乗っ取りを未然に防ぐことで、ボットによる被害を予防します。
- **フォレンジック機能とレポート機能:** 感染状況の概要を通知するマルウェア・レポートとダッシュボードを使用して、ボットがもたらすリスクを分析できます。ボットに関連する特定のインシデントをドリルダウンしながら、多彩なフォレンジック機能を用いて感染状況を調査し、想定される被害を素早く把握できます。
- **複数の技術による統合型の防御:** 「Anti-Bot Software Blade」は、チェック・ポイントの既存のセキュリティ技術と容易に統合することができます。例えば、最新の脆弱性に対する防御を提供する[IPS](#)、ウイルスの送信を防止する[Antivirus & Anti-Malware](#)、不正サイトへのアクセスを遮断する[URL Filtering](#)などと組み合わせて使用できます。複数の技術を統合して多層防御ソリューションを構成することにより、セキュリティ環境を集約しながら、ネットワークのあらゆるレイヤにわたってボット対策を行うことができます。
- **集中管理:** [Software Bladeアーキテクチャ](#)に基づくポリシーの集中管理により、ネットワークの全体像を把握できるため、複雑な管理作業の負担が軽減されます。

参考資料:

- 解説画像: ボットネット - ステルス型のオンライン脅威(英語)

<http://bit.ly/oHvrij>

- 動画: ボットとボットネットの脅威(英語)

<http://www.youtube.com/watch?v=6495O71W5iE>

- ・ 動画: Anti-Bot Software Blade (英語)

<http://www.youtube.com/watch?v=PaykuZZhujc>

- ・ ボット対策に関する最新のニュースを紹介するチェック・ポイントのボットネット・リソース・ページ (英語)

<http://www.checkpoint.com/products/anti-bot-software-blade/anti-bot-software-blade-landing-page.html>

- ・ - チェック・ポイント セキュリティ調査レポート -

欧米大企業の約半数がソーシャル・エンジニアリング攻撃の被害に

http://www.checkpoint.co.jp/pr/2011/20110928_social_engineering_survey.html

- ・ Software Blade アーキテクチャ

<http://www.checkpoint.co.jp/products/softwareblades/architecture/index.html>

受注出荷時期

「Anti-Bot Software Blade」は、2012年第1四半期より各国のチェック・ポイント正規販売代理店を通じて購入可能となる予定です。チェック・ポイントのパートナーについては、

<http://partners.us.checkpoint.com/partnerlocator/> をご覧ください。

Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド (www.checkpoint.com) は、インターネット・セキュリティにおけるトップ企業として、セキュリティの複雑さと総所有コスト (TCO) を低減しつつ、あらゆるタイプの脅威からお客様のネットワーク環境を確実に保護するための妥協のないセキュリティ機能を実現しています。チェック・ポイントは、FireWall-1 と特許技術のステートフル・インスペクションを開発した業界のパイオニアです。チェック・ポイントは、革新的セキュリティ技術である Software Blade アーキテクチャをベースとした一層の技術革新に努めています。Software Blade アーキテクチャは、導入先に合わせカスタマイズすることで、あらゆる組織のセキュリティ・ニーズにも的確に対応できる、柔軟でシンプルなソリューションの構築を可能にします。チェック・ポイントは、技術偏重から脱却してセキュリティをビジネス・プロセスの一環として定義する唯一のベンダーです。チェック・ポイント独自のビジョン 3D Security は、ポリシー、ユーザ、実施という3つの要素を統合して情報資産の保護を強化し、導入環境のニーズに合わせて高度なセキュリティを確保できるようにします。チェック・ポイントは、Fortune 100 社および Global 100 企業の全社を含む、何万ものあらゆる規模の企業や組織を顧客としています。数々の受賞歴のあるチェック・ポイントの ZoneAlarm ソリューションは、世界中で何百万にも及ぶお客様の PC をハッカー、スパイウェア、および情報窃盗から未然に保護しています。

チェック・ポイント・ソフトウェア・テクノロジーズの全額出資日本法人、チェック・ポイント・ソフトウェア・テクノロジーズ株式会社は、1997年10月1日設立、東京都新宿区に拠点を置いています。

####

《本件に関するお問い合わせ先》

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
担当 マーケティング 溝口
Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: info_jp@checkpoint.com

広報代行 株式会社プラップジャパン
担当 矢畑
Tel: 03-4570-3191/ Fax: 03-4570-3189