

【米国報道発表資料抄訳】

2016年3月4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

サーバ・ルームから空港まで、あらゆる場所のシステムに チェック・ポイントのゼロデイ・セキュリティ機能を拡張

新しい保護機能と先進的なフォレンジックが統合された SandBlast Agent が、
エンドポイント・デバイスのセキュリティ確保と迅速なインシデント対応を実現

2016年2月9日カリフォルニア州サンカルロス発 — 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 Check Point® Software Technologies Ltd. (NASDAQ: CHKP、インターナショナル本社: イスラエル、会長兼 CEO: ギル・シュエッド) は、同社の先進的な境界セキュリティおよびゼロデイ保護テクノロジーである SandBlast を進化させた Check Point SandBlast™ Agent を発表しました。SandBlast Agent は、エンドポイント・デバイスおよび保存されているデータの保護を、場所を問わず確保するよう設計されています。SandBlast Agent には、サンドボックス技術とファイルに含まれる潜在的脅威を無害化する技術に基づくプロアクティブな保護に加え、インシデント分析を自動化するフォレンジックの機能も組み込まれています。これにより、すでに存在する脅威および今後起こりうる両方の脅威に対し、効果的に対応できる信頼性をさまざまな組織へ提供します。

あらゆる人やモノ、機器がつながりをますます強めるコネクテッド・ワールドでは、社員が社内ネットワークに接続しているか、リモート・サイトから接続しているかを問わず、さまざまなデバイスを使用して企業の情報にアクセスできるようにすることで、イノベーション、生産性、および成長の機会を飛躍的に向上させることが可能となります。しかし、これらのデバイスは重要であるにもかかわらず、防御効果に限界がある既知の脅威しか検出できない、シグネチャ・ベースの従来型アンチウイルス・エージェントが利用されています。ハッカーはこの現状を利用し、より高度なゼロデイ攻撃(例: CryptoWall や CryptoLocker などのマルウェアの新しい回避型変種)を仕掛けて、特にエンドポイント・デバイスを標的にしています。

Community Newspaper Group のインフラストラクチャ・マネージャー、マイケル・ブライン (Michael Brine) 氏は次のように述べています。「エンタープライズ・セキュリティの前線に対応する立場で最新のハッキング手口の現実を見ると、アンチウイルス・ソリューションは、これらの新種の脅威を防ぐ手段としては頼りにできなくなってきています。最新のマルウェアを検出するために最善を尽くすことはもちろん、イベントが発生したときに迅速に対応することが非常に重要です。攻撃がこれ以上ユーザに到達するのを防いだうえで、セキュリティ・チームが脅威をすばやく抑制し、かつ業務への影響を未然に防げるようにすると、モバイル・ワーカーは安心して各自の業務を管理できるようになります。」

これらの最新式の攻撃を阻止するには、これまでとは違うアプローチでエンドポイント・セキュリティの強化に取り組む必要があります。SandBlast Agent は、エンドポイント向けゼロデイ保護機能と自動化されたフォレンジック/インシデント対応機能を統合した唯一のソリューションです。このソリューションの主な機能は以下のとおりです。

- **今日のビジネス要件を満たすよう設計されたエンドポイント・セキュリティ** — SandBlast Agent は、エンドポイント上に保護機能を直接実装して、高度な攻撃やウェブ・ベースの脅威(スパイ・フィッシングやウォータリング・ホールなど)を電子メールやリムーバブル・メディアから検出し阻止します。リモート・サンドボックス・モデルに基づく、非侵入型かつ低オーバーヘッドの導入環境は、ローカル・パフォーマンスに対する影響を最小限に抑えると同時に、インストール済みアプリケーションとの完全な互換性も維持します。ファイルに対し厳密なセキュリティ分析の実行中も、標準のファイル形式へ無害化した安全なドキュメントで作業を継続することが可能です。

- **感染を特定して封じ込める次世代テクノロジー** — SandBlast Agent は、チェック・ポイントの次世代脅威阻止ソリューションである SandBlast をベースにしており、感染したデバイスによる疑わしい通信活動を検出して、機密データを組織から引き出そうとする動きを阻止し、感染したエンドポイントを隔離することによって感染の拡大を防ぎます。SandBlast は、NSS Labs が最近実施した侵害検知システム(BDS)グループ・テストにおいて、「Recommended」として評価されるほか、セキュリティの有効性と価値においても最高評価を獲得しています。
- **包括的な自動分析機能に基づく実践的なレポート** — SandBlast Agent の自動インシデント分析機能により、セキュリティ・イベントを完全に可視化して、潜在的な損害とそれに伴う修復コストを最小限に抑えることができます。SandBlast Agent では、自動化されたフォレンジック機能に基づいて、実践的で対話型のレポートが即座に生成されるため、根本原因、マルウェアのエントリー・ポイント、損害の規模を完全に把握できます。これにより、迅速な修正が可能になるとともに、マルウェアの拡散とそれによる損害が制限されます。

チェック・ポイントの脅威阻止部門の責任者、ネイサン・シューカミは、次のように述べています。「ハッカーがエンド・ユーザのシステムに標的を絞り、シグネチャ・ベースのアンチウイルス・セキュリティ製品をバイパスすることを目的とした高度な脅威が登場するなど、組織は今、さまざまな重大な課題に直面しています。SandBlast Agent により、ユーザがネットワーク境界の内側にいるか外側にいるかにかかわらず、最新の高度なマルウェア手法に基づく攻撃を防ぐことが可能になります。」

■チェック・ポイントについて WE SECURE THE FUTURE.

チェック・ポイント・ソフトウェア・テクノロジーズ(www.checkpoint.com)は、あらゆる規模の組織に対応する世界トップクラスのセキュリティ・リーディング・カンパニーです。業界随一の検出率を誇る先進のセキュリティ対策により、お客様のネットワークをマルウェアなどの多岐にわたるサイバー攻撃から保護します。大規模ネットワークからモバイル・デバイスまでを保護する包括的なセキュリティ・アーキテクチャに加え、直感的で使いやすい総合的なセキュリティ管理ソリューションを提供しています。世界の 10 万以上の組織・企業がチェック・ポイントのセキュリティ製品を利用しています。

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。

©2016 Check Point Software Technologies Ltd. All rights reserved

####

《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 石黒佐知子
 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 高橋・南宮
 Tel: 03-4580-9109 / Fax: 03-4580-9135
 Email: CheckPoint_pr@ml.prap.co.jp