

2016年9月2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

**チェック・ポイント、業界初となる Web ブラウザ向けリアルタイムのゼロデイ攻撃対策を発表**

SandBlast Agent for Browsers により、最新 Web ベースのマルウェアやフィッシングおよび認証情報の窃取を保護

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、代表取締役社長：ピーター・ハレット、以下 チェック・ポイント）は本日、ゼロデイ・フィッシング対策技術を強化した新製品、「SandBlast Agent for Browsers」を発表しました。先進の脅威対策を提供する SandBlast ソリューション・ファミリーの最新製品である SandBlast Agent for Browsers は、SandBlast の中核機能である高度なサンドボックスおよびファイルの無害化機能がブラウザにシームレスに組みこまれ Web ベースのマルウェアやフィッシング詐欺、ソーシャル・エンジニアリング攻撃など絶えず進化を遂げるセキュリティ脅威からユーザを保護することが可能になります。また、今日の巧妙な攻撃を防ぐために必要となるエンドポイントにおけるリソースを軽減しながらリアルタイムの保護を実現しています。

業務フローと安全性の両立を提供するこの保護性能は、企業組織および総務省が主導する自治体強靱性向上モデルにおいても外部からのファイル・ダウンロード、分離されたネットワーク間でのファイル受け渡しでの利用が期待されています。

業績の最大化、業務の効率化および技術革新に取り組む今日の組織環境においては、制約のないインターネット接続とダウンロードしたコンテンツや電子メールの即時な活用が求められています。その一方で、組織は、変化を続けるセキュリティ脅威動向にも対応しなければなりません。機密性の高い個人情報や組織の知的財産の窃取を防ぎながら、重要な業務システムの効率性も維持する必要があります。

Web 経由でダウンロードされるファイルは、今日のマルウェアにとって主要なエントリー・ポイントであり、このような脅威が増加傾向を示す事実も明らかになっています。組織を標的とする Web ベースのマルウェアやソーシャル・エンジニアリング攻撃は、ますます増加・高度化しています。サイバー攻撃者は、最新の検出回避手法や巧妙な詐欺の手口と組み合わせて、ターゲットへの感染を試みます。近日発表予定の SANS による調査「Exploits at the Endpoint: SANS 2016 Threat Landscape Study」のプレビュー版には、以下のような事実が述べられています。

- 回答者の 41%が、不正プログラムのドライブバイ・ダウンロードを使用した攻撃により大規模なセキュリティ被害に遭遇

- 組織の 80%が過去 12 か月間にフィッシング詐欺の被害に遭い、68%がこの種の攻撃の増加を目の当たりにしている

Verizon の「Data Breach Investigations Report (2016 年)」によると、データ侵害の 63%が、脆弱なパスワード、デフォルトまたは盗み出されたパスワードを介した何らかの認証情報の窃取と関連しています。こうした事実からも、企業のセキュリティを確保するためには、さまざまな Web ベースの攻撃からユーザを保護することが不可欠なのは明白です。

se2 のエンタープライズ・セキュリティ・マネージャを務める Saul Schwartz 氏は、「社員を標的とするソーシャル・エンジニアリング攻撃が巧妙化の一途を辿る今日、弊社が事業を拡大させていくうえで自社のエンドポイントのセキュリティ確保がとりわけ大きな課題となっています。今後、弊社のモバイルワーカー数が増加するのは確実です。社員の生産性を損なわずに攻撃を阻止できるシンプルで使いやすいブラウザの拡張機能があれば、フィッシング詐欺などの脅威にも優位に立てると思っています」と述べています。

自社のエンドポイントの保護という課題に直面するいずれの企業も、最大限のセキュリティを確保すると同時に、すべてのシステム上で複数のエンドポイント・ソリューションを運用、管理、導入するためのフットプリントを最小限に抑えたいと望んでいます。SandBlast Agent for Browsers は、下記の特長を備え、各種のニーズに対応します。

- プロアクティブなリアルタイムの保護機能: わずか数秒で再構成した安全なコンテンツをユーザへ転送することにより高度なマルウェアの配布を防止
- 動的な分析: ユーザの認証情報を狙う未知およびゼロデイのフィッシングを動的に分析し攻撃をブロック
- 容易に導入できるブラウザ・プラグイン: Internet Explorer および Chrome 向けのシンプルで容易に導入できるブラウザ・プラグインは、数分でインストールが完了し、最小限の負荷で動作可能
- 業界トップのマルウェア検出率: 高度なサンドボックス技術と特許取得済みの CPU レベルの検査技術により、高いマルウェア検出率を実現

チェック・ポイントの脅威対策部門責任者であるネイサン・シューカミ (Nathan Shuchami) は、「サイバー攻撃が巧妙化の一途を辿り、発生頻度も上昇し続けている今日、企業が幅広いブラウザ・ベースの攻撃に狙われるリスクはますます高まっています。既存の対策技術を利用する場合、ユーザはコンテンツごとに安全を確認するか、すべてのシステム上に複数のソフトウェアをそれぞれインストールする必要があります。今回発表した SandBlast Agent for Browsers は、世界最高レベルのセキュリティでユーザを保護します。シンプルなブラウザ・プラグインにより、Web からのダウンロードを介して拡散する未

知およびゼロデイのマルウェアをブロックしながら、安全なコンテンツを素早く転送することが可能です」と述べています。

## 受注開始時期

SandBlast Agent for Browser は、2016 年第 3 四半期に提供開始となる予定です。

詳細については、[www.checkpoint.co.jp/products/endpoint-sandblast-agent/](http://www.checkpoint.co.jp/products/endpoint-sandblast-agent/) をご覧ください。

## ■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 ( http://www.checkpoint.co.jp/ ) 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・溝口

Tel: 03-5367-2500 / Fax: 03-5367-2501

Email: info\_jp@checkpoint.com

広報代行 共同ピーアール株式会社

担当 中村・小林・上瀧

Tel: 03- 3571 – 5238 / Fax: 03- 3571-5380

Email: checkpoint-pr@kyodo-pr.co.jp