IT@Intel 概要

インテル IT 部門

情報セキュリティーとステルスマルウェア保護

2013 年 2 月

企業向け McAfee* Deep Defender* の評価

- カーネルモードのルートキットに乗っ取られる前に、ルートキットをリアルタイムで防止
- ステルスマルウェア攻撃の特定、分析、攻撃への対応を迅速化
- システムの再構築を必要としない検出 / 修復機能
- McAfee* Host Intrusion Prevention for Desktops と McAfee* VirusScan* Enterprise の優れたコンパニオン製品

インテル IT 部門では、インテルにおいての McAfee* Deep Defender* の潜在的なビジネス価値を評価するために、初期試験導入を実施しました。この試験導入では、インテルが現在導入しているアンチマルウェア・アプリケーションではリアルタイムに防ぐことが不可能と思われていたステルスマルウェアの脅威を検出し、ブロックすることが可能であると判明しました。こうした価値のある結果に基づき、インテルでは、2013 年、社内組織を対象に Deep Defender* の実稼動環境への試験導入を行います。実稼動環境での試験導入が成功したあかつきには、さらに幅広い導入への可能性を検証する調査を実施する予定です。

Deep Defender* は、リアルタイム検出によってゼロデイマルウェア（コンピューターのアプリケーションや OS のこれまでに公表されていない脆弱性を悪用する脅威）を阻止します。具体的には、このソフトウェアは、カーネル・ルートキットを使用するステルスマルウェア攻撃を検出し、ブロックすることができます。このハードウェア支援型セキュリティーは、McAfee DeepSAFE* テクノロジーによって実現されます。

McAfee Labs の研究員は、370 万個以上の新種のステルス・ルートキットを確認しています。インテル IT 部門の脅威管理担当者は、Deep Defender* により、マルウェアの変種を検出し、分析するために必要な時間が削減できたことを確認しています。また、リアルタイム検出により、システムの修復が可能となり、システムの再構築が不要となるため、時間と労力が節約できることを期待しています。ステルスマルウェア攻撃をタイムリーに検出、ブロックし、修復する Deep Defender* は、インテルの既存の情報セキュリティー・ポートフォリオにとって新たな付加価値となります（図 1）。

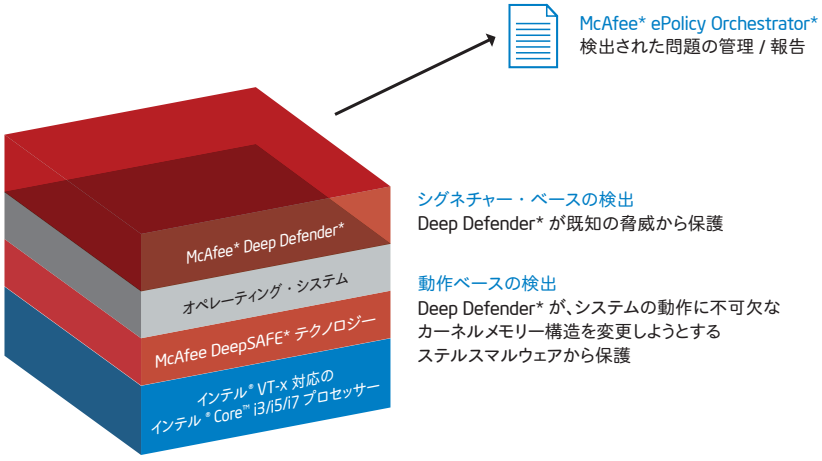

図 1. McAfee* Deep Defender* は、IA-32、インテル® 64、インテル® アーキテクチャーに対応したインテル® バーチャライゼーション・テクノロジー（インテル® VT-x）対応のインテル® Core ™ i3/i5/i7 プロセッサーで、シグネチャー・ベースの検出と動作ベースの検出の両方を使用して、ステルスマルウェアからのリアルタイム保護を実現します。

「カーネル下で Microsoft* Windows* を攻撃する脅威の頻度は増えつつあります。標的にされている重要資産の中には、BIOS、マスター・ブート・レコード（MBR）、ボリューム・ブート・レコード（VBR）、GUID パーティション・テーブル（GPT）、NTLoader などがあります。これらの脅威の数が、Windows* やアプリケーション上で実行される、非常にシンプルな攻撃の数に迫る可能性は低いとはいえ、こうした複雑な攻撃によって、はるかに破壊的な影響が生じるおそれがあります。McAfee Labs では、この領域の脅威は 2013 年中に増加すると見込んでいます。」

出典：『2013 年の脅威予測』
（2012 年に McAfee Labs が公開）

背景

2010 年にインテルがマカフィーを買収する以前から、インテルとマカフィーは、OS に対するステルスマルウェア攻撃を検出し、ブロックするテクノロジーの開発に共同で取り組んできました。ハッカーたちはマルウェアが販売できることに気づいており、ステルスマルウェア攻撃がさらに進化し続けることは予想された事態でした。インテルとマカフィーは、ソフトウェア・エージェントがハードウェア内の機能を利用して、OS 外部からの新しい独自の保護を実行できるようにするテクノロジーの共同開発を開始しました。この共同開発の成果が McAfee DeepSAFE* テクノロジーであり、McAfee* Deep Defender* に実装されています。

現在、新しいマルウェアの数は増え続けており、マルウェア作成者が機密情報の攻撃に使用する手法やツールは常に進化しています。サイバー犯罪者が PC やネットワークへアクセスするために使用するステルス型の手法は高度化し、実行しやすくなっています。サイバー犯罪者は、既存のセキュリティー保護をかいくぐることを目的としたステルスマルウェアを次々と作り出しています。

特に懸念されるのが、カーネルモードのステルス・ルートキットです。カーネルモードのルートキットは、コンピューターの OS やアプリケーションよりも先にロードされ、OS のカーネルレベルで動作します（図 2）。ルートキットは、コンピューターのアプリケーションや OS を標的とする他のマルウェア・コンポーネントを隠ぺいするために、ゼロデイ攻撃[1] で使用されます。

2012 年末の時点で、McAfee Labs の 30 カ国 500 名の総合研究員で構成されるチームが、370 万個以上の新種のステルス・ルートキットを確認しました。McAfee Labs では、Microsoft* Windows* の深部や下層に隠ぺいされた持続的な攻撃が増加すると予測しています。

リアルタイム検出による ゼロデイ脅威のブロック

Deep Defender* は、ハードウェア支援型のリアルタイムのメモリー監視機能と保護機能を各ユーザーデバイスに追加することで、インテル IT 部門の既存のアンチウイルス、セキュリティー監視、セキュリティー・インテリジェンスの各プラットフォームを補完します。

ステルスマルウェアは次の 2 種類の方法で検出できますが、Deep Defender* はこの両方を使用します。

- **シグネチャー・ベースの検出 - 既知の脅威の検出：**コードファイル内の静的文字列を検出し、該当するファイルをマルウェアと見なします。ほとんどのアンチウイルス・アプリケーションがこの方法を使用していますが、シグネチャー・ベースの検出だけでは、すでに特定され、検出テーブルに入力されている脅威に対する保護しか提供されません。また、この検出方法が実行される時点では、PC はステルスマルウェアにすでに感染し、被害を受けてしまっています。
- **動作ベースの検出 - ゼロデイ脅威のリアルタイムの検出：**システムメモリーを監視して、マルウェアがシステムの動作に不可欠なカーネルメモリー構造の変更を試みていないかどうかを確認します。この方法では、脅威が発生した時点でルートキットなどのゼロデイマルウェアを検出できます。

Deep Defender* では、既知の脅威に対処するシグネチャー・ベースの検出と、カーネル・ルートキットなどのゼロデイ脅威をブロックする動作ベースの検出とを組み合わせることで、ステルスマルウェアからのリアルタイム保護を実現します。従来のシグネチャーのみのセキュリティー手法に比べ、こうした保護方法の組み合わせは大きな進歩と言えます。Deep Defender* のハードウェア支援型セキュリティーは、McAfee DeepSAFE* テクノロジーによって実現されます。インテル® プロセッサーと直接やり取りを行う McAfee DeepSAFE* テクノロジーは、OS の外部というセキュリティーの新たな視点を提供します。

「不審」のフラグが付けられた動作が、ドライバーのアップグレードなどの正当な動作であることが判明した場合、そのドライバーをホワイトリストに追加することで、Deep Defender* によるユーザーへの警告を停止できます。ホワイトリストとブラックリストの両方を作成することで、さまざまなセキュリティー環境に合わせて Deep Defender* を調整し、パフォーマンスとセキュリティー保護を向上させることが可能になります。

共同での取り組み

Deep Defender* の開発は、インテルとマカフィーの継続的な共同事業です。McAfee DeepSAFE* テクノロジーでは、IA-32、インテル® 64、インテル® アーキテクチャーに

[1] ゼロデイ攻撃の詳細については、http://www.mcafee.com/japan/media/mcafeeb2b/international/japan/pdf/enterprise/wp_stealth-crimeware.pdf を参照してください。

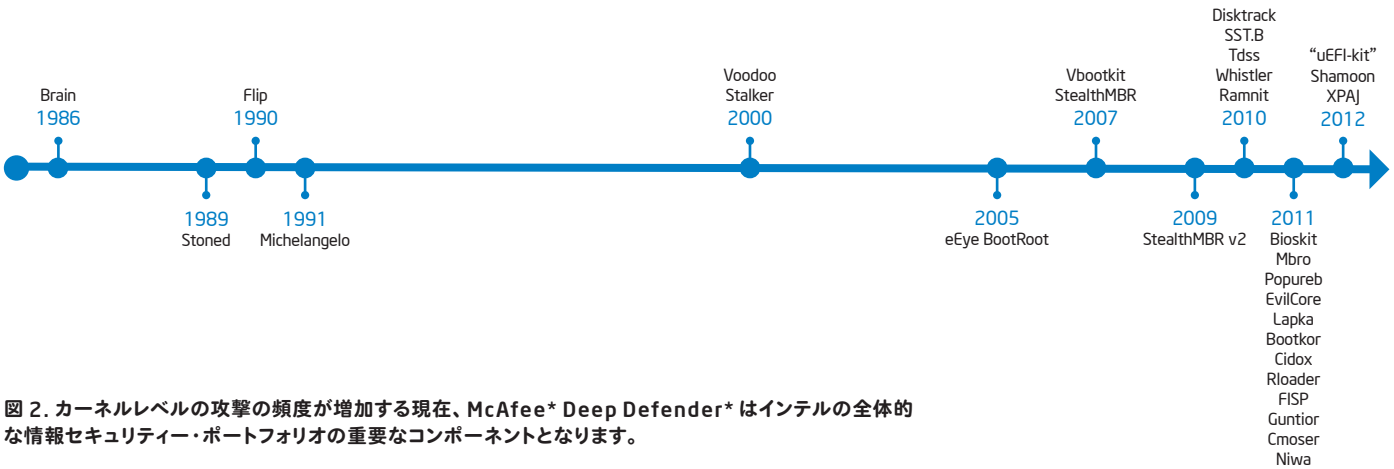

図 2. カーネルレベルの攻撃の頻度が増加する現在、McAfee* Deep Defender* はインテルの全体的な情報セキュリティー・ポートフォリオの重要なコンポーネントとなります。

対応したインテル® バーチャライゼーション・テクノロジー（インテル® VT-x）が利用されます。インテル® アーキテクチャーの専門家はマカフィーの製品開発者と共に、インテル® プロセッサーの機能を使用してカーネルを保護する製品の開発を進める共同作業に取り組んできました。

さらに、インテルは、製品の開発にあたって、次に示すようないくつかの領域においても知識を共有し、開発支援を行いました。

- パフォーマンス・オーバーヘッドの大幅な削減
- マカフィーのセキュリティー管理プラットフォームである McAfee* ePolicy Orchestrator*（McAfee ePO*）と Deep Defender* の統合の強化
- 不具合の特定と解決
- 32 ビットと 64 ビットのステルスマルウェアの変種に対する保護機能の開発による、サイバー犯罪者の活動への対策支援

インテル IT 部門は、Deep Defender* によるパフォーマンスへの影響をさらに減らし、製品全体の改善を行うために、引き続きマカフィーと協力していきます。例えば、インテルとマカフィーは、インテルのテクノロジーを利用して BIOS 攻撃などの他の種類の脅威を検出する追加機能の開発にも積極的に取り組んでいます。

初期試験導入

インテル IT 部門では、インテルが McAfee* Deep Defender* を利用することで得られる潜在的なビジネス価値を評価するために、初期試験導入を実施しました。10 週間の試験導入期間を設け、320 名の参加者が同製品のバージョン 1.0.1 を使用しました。社内のソフトウェア配布システムを使用してソフトウェアを導入し、McAfee ePO* サーバーを使用して検出された問題の管理と報告を行いました。試験導入の実施後に参加者を対象とした調査を行い、試験導入の結果を分析しました。

手 法

サンプルとして抽出する従業員に多様性を持たせるために、世界各国のさまざまなビジネスグループの従業員に対して試験導入への参加を呼びかけました。参加者には、マルウェアを受ける危険性やステルスマルウェア攻撃の標的になる危険性が一般的に高い、次のような人々が含まれていました。

- 以前にマルウェアによる影響を受けたことがある
- 機密データにアクセスする
- 出張先で接続するためにホテルやホットスポットを利用する
- 顧客や供給メーカーと頻繁にやり取りする
- 会社での物品購入にクレジットカードを使用し、財務データを処理する

試験導入に参加するにあたり、従業員の PC は次の条件を満たす必要がありました。

- インテル® VT 対応のインテル® Core ™ i3/i5/i7 プロセッサーを搭載していること
- McAfee* Agent 4.6 を使用できること
- 互換性のないハイパーバイザーがインストールされていないこと [2]

対象となる従業員に、ソフトウェアのインストールと有効化の手順を記載した電子メールを送りました。

試験導入の参加者向けに、3 つのコンポーネントが含まれたクライアント・パッケージを作成しました。

- PC の BIOS 設定がインテル® VT-x とエグゼキュート・ディスエーブル・ビット用に正しく設定されていることを検証するコンポーネント
- McAfee* Agent 4.6 ソフトウェア
- McAfee* Deep Defender* 1.0.1 ソフトウェア

BIOS チェックによって不適切な設定が検出された場合、ほとんどの設定のリセットは自動的に実行されました。ただし、手動で変更する必要がある設定については、従業員にリセットの手順を詳細に示しました。

テスト用の McAfee ePO* サーバーで動作するように McAfee* Agent 4.6 を構成しました。テスト用の McAfee ePO* サーバーですべてのマルウェア検出イベントが記録されるように、McAfee ePO* サーバーの構成に McAfee* Deep Defender* 1.0.1 の拡張機能を含めました。また、McAfee ePO* ポリシー設定を作成し、McAfee ePO* サーバーに適用しました。例えば、ゼロデイマルウェアが検出された場合は、Deep Defender* がそのマルウェアをブロックし、修復するようにしました。インテルでは、今後 Deep Defender* を導入する際には、このクライアント・パッケージをベースにする予定です。

主な結果とビジネス価値

インテル IT 部門は、初期試験導入の実施前に、Deep Defender* によってマルウェアの変種の脅威分析を迅速化できること、さらには攻撃を受けた後に事後対応でシステムを再構築するのではなく、リアルタイムで脅威を検出し、修復できる可能性があることを予想していました。

そして試験導入の結果、この予想が実証されました。試験導入期間中において、マルウェアが 3 回も検出されたことで、大きなビジネス価値の存在が実証されました。

インテルが現在導入しているマルウェア検出アプリケーションでは、これらの脅威をリアルタイムで検出したりブロックすることはできなかったと考えられます。事実、現在導入されているアンチウイルス・アプリケーションは、いずれの脅威も検出しませんでした。新しいソフトウェアは、ルートキットがロードされようとしていることを検出し、このマルウェアをブロックして修復することで、カーネルレベルの侵害を阻止しました。この脅威がブロックされていなければ、システムの再構築が必要となり、IT 部門の何時間もの労力が消費され、従業員の生産性の損失が生じていたことでしょう。

マルウェアが検出されていなかった場合、影響を受けた各システム上では財務情報やドキュメントが盗まれ、ファイル共有操作によって他の従業員のシステムにも被害が及んでいた可能性があります。

ドライバーが正当な方法でカーネルレベルの情報を変更するという、ドライバー検出イベントもいくつか発生しました。こうしたイベント情報を使用し、対象となるドライバーをホワイトリストに登録することで、以後、該当するドライバーがイベントを発生させないようにすることができます。

インテル IT 部門は、試験導入期間に実証されたビジネス価値に基づいて、ステルスマルウェアの影響を受ける危険性の高い従業員の使用状況やシステムを特定しています。Deep Defender* は、アンチウイルス・アプリケーションやホスト侵入防止アプリケーションなど、インテルがすでに使用している既存の情報セキュリティー保護に新たな付加価値をもたらします。

インテルは、試験導入期間に、ネットワーク上でのセキュリティー・イベントをリアルタイムで監視し、解釈する既存の機能に Deep Defender* を統合するプロセスを開発しました。一例を挙げると、Deep Defender* は McAfee ePO* で動作するようになりました。McAfee ePO* は、エンドポイント、ネットワーク、コンテンツ・セキュリティー、コンプライアンスの各ソリューションの管理を一元化し、簡素化するセキュリティー管理プラットフォームです。また、インテルは、セキュリティー情報イベント管理ツールと Deep Defender* の統合にも取り組んでいます。

調査結果

試験導入の終わりに参加者を対象に調査を行い、222 件の回答が得られました。図 3 に示す

---

[2] インテル® バーチャライゼーション・テクノロジー（インテル® VT）を利用するソフトウェア製品間に互換性はありません。したがって、インテル® VT を利用するハイパーバイザーを実行しているシステムは、McAfee* Deep Defender* の実行候補にはなりません。

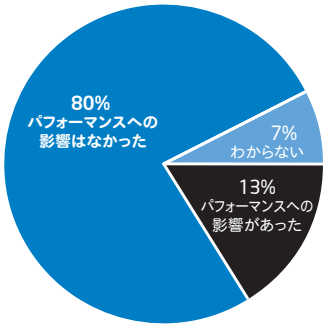

図 3. 初期試験導入後の調査では、回答者の 80% が McAfee* Deep Defender* ソフトウェアの実行時にパフォーマンスへの影響はなかったと回答しており、価値ある答えが得られました。

McAfee* Deep Defender* と Microsoft* Windows* 8

インテル IT 部門は、ビジネス向け Ultrabook™ デバイスとインテル® アーキテクチャー搭載タブレットの主要 OS として、Windows* 8 Enterprise の標準化を進めており、最終的にノートブック PC とデスクトップ PC で、この新しい OS を利用できるようにする予定です。

Windows* 8 では、起動時マルウェア対策 (ELAM) ドライバーと Unified Extensible Firmware Interface (UEFI) セキュアブートのサポートにより、起動プロセスでのセキュリティーが強化されますが、これらのセキュリティー対策はブラックリストにすでに登録されているドライバーにしか適用されません。McAfee* Deep Defender* は、Windows* 8 上のゼロデイマルウェアに対しても、次のような独自の利点を持ちます。

- 保護されたメモリー・ロケーションへのマルウェアのアクセスをプロファイルし、悪意のある動作に対処します。
- OS の前にロードされ、カーネルメモリーをリアルタイムで監視します。
- 実行時、つまり脅威がロードされようとする時点でマルウェアを検出します。これに対して、Windows* 8 の内蔵機能では、再起動時にのみ保護が行われます。そのため、感染から次の再起動までの間隔が数日または数週間開くこともあり、その間にステルスマルウェアが潜み、伝播する可能性が拡大します。

ように、回答者の 80% が、Deep Defender* ソフトウェアの実行時にパフォーマンスへの影響はなかったと答えています。「わからない」と答えた回答者も 7% いますが、これは彼らがパフォーマンスへの影響を基本的に意識していなかったことを示しています。一般的に、マルウェア検出 / 修復ソフトウェアを実行すると、ユーザーはパフォーマンスへの影響を感じることが少なくありません。その点を考えると、これは目覚ましい結果と言えるでしょう。実稼動環境への試験導入時にも、パフォーマンスへの影響に関する調査は引き続き行われる予定です。

次のステップ

Deep Defender* は、インテルの情報セキュリティー・ポートフォリオに付加価値をもたらすことがわかりました。現在、インテルで使用されている PC のうち、Deep Defender* を導入して使用することでメリットが得られる PC の数は約 7 万台と推測されています。Deep Defender* は進化を続けているため、その価値は今後さらに高まると考えられます。2013 年第 2 四半期にリリース予定のリリース 1.6 では、次の主要機能が提供される予定です。

- **BIOS の監視 :** PC の起動時の動作の変更を防ぎます。
- **インテル® Xeon® プロセッサーのサポート :** サーバーおよびその重要なビジネス機能とデータを保護できる、リアルタイムのマルウェア防止機能を提供します。
- **Microsoft* Windows* 8 のサポート :** Windows* 8 OS で発生するステルスマルウェアの脅威に対してカーネルと BIOS を保護します。
- **最新のインテル® アーキテクチャーのサポート :** McAfee* ソフトウェアでは、インテル® マイクロアーキテクチャーが提供するハードウェア支援型の高度なセキュリティー機能を引き続き利用します。

今後の計画として、初期試験導入の参加者のリリース 1.5 へのアップグレード、リリース 1.6 の評価、実稼動環境への試験導入での社内組織を対象とした Deep Defender* の導入などを予定しています。

まとめ

McAfee* Deep Defender* は、リアルタイム検出によって、カーネルモードのルートキットを使用した攻撃など、いわゆるゼロデイマルウェアがシステムに損害を与えたり、他の PC に拡散したりする前にマルウェアを阻止します。インテルでの初期試験導入では、このソフトウェアは、インテルで使用中の他のアンチマルウェア・アプリケーションではタイムリーに検出または防止できなかったステルスマルウェアの脅威を検出し、ブロックできました。

また、この試験導入の結果、Deep Defender* が提供するイベントデータを利用することで、インテル IT 部門の脅威管理担当者がマルウェアの変種を検出し、解析するために必要な時間を削減できるという予想も実証されました。さらに、リアルタイム検出により、ほとんどの場合、システムの修復が可能となり、システムの再構築の必要がなくなるため、時間と労力を大幅に節約できます。

ステルスマルウェアを検出し、ブロックすることができる Deep Defender* は、アンチウイルス・アプリケーションやホスト侵入防止アプリケーションなど、インテルがすでに使用している情報セキュリティー保護製品の有効なコンパニオン製品となります。インテルでは、2013 年、社内組織を対象に Deep Defender* の実稼動環境への試験導入を行います。実稼動環境への試験導入が成功した後は、さらに幅広い導入の可能性に関する調査を実施する予定です。

著 者

Greg Bassett
インテル IT 部門
セキュリティー・エンジニア

Albert Gutierrez
インテル IT 部門
クライアント・セキュリティー・エンジニア

Stephanie Mahvi
インテル IT 部門
プロジェクト・マネージャー

最新トピックに関するインテルの IT リーダーのコメントについては、http://www.intel.co.jp/itatintel/ を参照してください。

インテル株式会社
〒 100-0005 東京都千代田区丸の内 3-1-1
http://www.intel.co.jp/

2013 年 6 月

327765-001JA
JPN/1306/1K/SE/IT/TC