McAfee Advanced Threat Defense

高度なマルウェアを検出

McAfee® Advanced Threat Defenseを使用すると、セキュリティ対策を回避する高度なマルウェアを検出し、収集した脅威情報から迅速にアクションを実行して組織を保護できます。従来のサンドボックスと異なり、高度な検査機能により、回避技術を駆使した脅威も検出します。ネットワークからエンドポイントまでの様々なセキュリティ ソリューションと緊密に統合され、環境全体で脅威情報を迅速に共有し、保護機能と検査機能を強化できます。柔軟な配備オプションが用意されているため、様々なネットワークに配備できます。

ネットワークからエンドポイントまでの保護対策に高度なマルウェア分析機能を統合し、IT環境全体で脅威情報を共有することで、脅威の検出方法が大きく変わります。エコシステムで脅威インテリジェンスを共有することで、統合されたセキュリティ ソリューションが連携して指令サーバーとの通信を速やかに遮断し、感染システムを隔離します。同一または類似した脅威を阻止するだけでなく、影響を評価して必要な対策を講じることができます。

McAfee Advanced Threat Defense: 高度脅威の検出

McAfee Advanced Threat Defenseは、多層型の革新的なアプローチで現在のステルス型攻撃やゼロデイ マルウェアを検出します。ウイルス対策のシグネチャ、レピュテーション、リアルタイム エミュレーションなどの分析エンジンと動的な分析（サンドボックス）を組み合わせ、実際の動作を分析します。詳細なコードの静的分析でファイルの属性と命令セットを調査し、意図と動作を特定して既知のマルウェア ファミリとの類似性を評価します。分析の最終段階で、McAfee Advanced Threat Defenseはディープ ニューラル ネットワークの機械学習を利用し、不正な兆候を確認します。このソリューションは市場で最も強力で高度なマルウェア対策技術を提供し、パフォーマンスを低下させずに高度な調査を行います。既知のマルウェアは、シグネチャとリアルタイム エミュレーションで検出し、パフォーマンスを向上させています。回避技術を駆使した巧妙な脅威は詳細な静的コード分析、機械学習から取得した情報、サンドボックスにより阻止します。動的な環境で実行されない不正な兆候は、詳細な静的コード分析と機械学習の結果から特定します。

McAfee Advanced Threat Defenseの主な差別化要因

様々なソリューションと統合

- 既存のMcAfeeソリューション、オープン規格に対応しているサードパーティのメール ゲートウェイなどの製品と統合
- 検出から封じ込めまでの時間を短縮し、組織全体を保護
- ワークフローが簡素化され、対応と修復にかかる時間を短縮
- 自動化に対応

強力な分析機能

- 詳細な静的コード分析と動的分析、機械学習により、豊富な分析データに基づいて検出精度を向上
- SOCで対応している高度な機能と調査能力

McAfeeとつながる

マルウェアの作成者はパッキングでコードの構成を変更したり、検出を回避しようとします。大半の製品は元の実行コードを正しく解凍できません。McAfee Advanced Threat Defenseには高度な解凍機能が搭載されています。これにより、難読化を解除し、元の実行コードを展開することができます。また、詳細な静的コード分析では、ファイル属性と命令セットを解析してコードの挙動を特定します。

詳細な静的コード分析、機械学習、動的分析により、マルウェアの疑いがあるコードを正確に評価します。高度な分析結果から生成されたサマリー レポートにより、状況を確認し、優先度に従ってアクションを実行できます。また、詳細レポートにより、マルウェアの詳しい分析結果を確認できます。

保護の強化

McAfee Advanced Threat Defenseは、ネットワークからエンドポイントまでのセキュリティ デバイスと緊密に統合されているので、McAfee Advanced Threat Defenseが不審なファイルを検出するとすぐにアクションを実行できます。このように検出と保護が緊密かつ自動的に統合されている点が非常に重要です。

McAfee Advanced Threat Defenseは様々な方法で統合できます。特定のセキュリティ ソリューションに直接統合することも、McAfee Threat Intelligence ExchangeやMcAfee Advanced Threat Defense Email Connectorを介して統合することもできます。

直接統合した場合、McAfee Advanced Threat Defenseが検出したファイルに他のセキュリティ ソリューションがアクションをすぐに実行します。脅威情報を既存のポリシー施行プロセスに組み込み、同一または類似したファイルをネットワーク全体でブロックできます。

McAfee Advanced Threat Defenseの検出結果が統合製品のログとダッシュボードに表示されるので、分析全体が一つの環境で実行されているように見えます。これにより、ワークフローが簡素化されるので、1つのインターフェースでアラートを効率よく管理できます。

McAfee Threat Intelligence Exchangeとの統合により、McAfee Endpoint Protectionなどの保護対策とMcAfee Advanced Threat Defenseが連動し、分析結果と侵入の痕跡が共有されます。McAfee Advanced Threat Defenseが不審なファイルを検出すると、McAfee Threat Intelligence Exchangeがレピュテーションを更新し、最新の脅威情報を組織内の統合セキュリティに配信します。

柔軟で一元管理された配備

- 複数のプロトコルに対応した集中配備でコストを削減
- 柔軟な配備オプションが用意され、様々なネットワークに配備可能

統合ソリューション

- McAfee® Active Response
- McAfee® Advanced Threat Defense Email Connector
- McAfee® Enterprise Security Manager
- McAfee® ePolicy Orchestrator®
- McAfee® Network Security Platform
- McAfee® Threat Intelligence Exchange
  - McAfee® Application Control
  - McAfee® Endpoint Protection
  - McAfee® Security for Email Servers
  - McAfee® Server Security
- McAfee® Web Gateway
- Bro Network Security Monitor
- TAXII (Trusted Automated eXchange of Indicator Information)

McAfee Threat Intelligence Exchangeを使用するエンドポイントは、新しいマルウェアの感染をブロックし、同じファイルによる攻撃を未然に防ぎます。McAfee Threat Intelligence Exchangeに統合されたゲートウェイは不審なファイルの侵入を阻止します。また、McAfee Threat Intelligence Exchangeを使用するエンドポイントは、社内ネットワークに接続していない場合でもファイルの検出情報を受信し、ペイロードの拡散を防ぎます。

McAfee Advanced Threat Defense Email Connectorを利用すると、McAfee Advanced Threat Defenseはメール ゲートウェイからメールの添付ファイルを受信し、分析することができます。McAfee Advanced Threat Defenseは添付ファイルを分析し、メッセージのヘッダーに分析結果を追加してアクティブなすべてのメール ゲートウェイに戻します。メール ゲートウェイは、ポリシーに従ってアクション（添付メールの削除や隔離など）を実行し、内部ネットワークへのマルウェアの侵入を阻止します。オフライン モードでは、添付ファイルを含むメールがMcAfee Advanced Threat Defenseでスキャンされ、エンドユーザーに配信されます。メール ゲートウェイによる添付ファイルの評価は待ちません。管理者は、McAfee Advanced Threat DefenseまたはMcAfee Threat Intelligence Exchangeによる添付ファイルのスキャン結果を確認できます。McAfee Threat Intelligence Exchangeを介してMcAfee Advanced Threat DefenseとMcAfee Security for Email Serversを統合することで、メール サーバーで高度な検出を行います。

脅威情報の共有で調査を自動化

攻撃に対して適切な判断と対応を行うには、実用的な情報を取得し、組織全体を可視化する必要があります。McAfee Advanced Threat Defenseは、環境全体で簡単に共有し、自動的な調査を可能にする詳細な脅威情報を生成します。Data Exchange Layer（DXL）とREST APIのサポートにより、他の製品との統合が容易になり、STIX（Structured Threat Information eXpression）/TAXII（Trusted Automated eXchange of Indicator Information）などの脅威情報の共有規格を採用することで、効果的なセキュリティ エコシステムの構築と強化が可能にしています。

McAfeeのエコシステム内で、McAfee Enterprise Security Managerは、McAfee Advanced Threat Defenseなどからファイル レピュテーションと実行イベントを収集し、相関分析を行います。高度なアラートと履歴ビューにより、詳細な情報からセキュリティ状況をリアルタイムで把握し、リスクの優先度を判断できます。McAfee Advanced Threat Defenseが検出した痕跡データはMcAfee Enterprise Security Managerが6か月間管理し、ネットワークやシステムの分析に使用されます。これにより、新たに識別されたマルウェアの発生源と以前に通信を行っていたシステムを特定できます。McAfee Endpoint Protection、McAfee Threat Intelligence Exchange、McAfee Active Responseの緊密な統合により、的確なセキュリティ オペレーションを実施できます。新しい構成の送信、新しいポリシーの実装、ファイルの削除、ソフトウェア更新の配備などを行い、リスクを回避できます。ネットワー

ク内で感染したエンドポイントはMcAfee Active Responseによって自動的に識別され、McAfee Advanced Threat Defenseレポートに表示されるので、的確なアクションをすぐに実行できます。アナリストは、McAfee Active Response内の1つのワークスペースで、詳細なレポートを見ながら効率的に作業を行うことができます。

調査をサポートする高度な機能

McAfee Advanced Threat Defenseは次のような高度な機能を提供します。

- **設定可能なオペレーティング システム/アプリケーション サポート:** 特定の環境変数で分析を調整し、脅威の検証と調査のサポートを行うことができます。
- **ユーザー対話モード:** マルウェアのサンプルを直接使用しながら分析を行うことができます。
- **高度な解凍機能:** 数日かかっていた調査も数分で終わります。
- **完全な論理パス:** 標準的なサンドボックス環境で休眠状態のサンプルを追加の論理パスで強制的に実行し、詳しい分析を行うことができます。
- **複数の仮想環境へのサンプルの送信:** ファイルの実行に必要な環境変数を特定し、調査にかかる時間を短縮できます。
- **詳細なレポート:** MITRE ATT&CK™マッピング、逆アセンブリの出力、関数呼び出しの関係図、埋め込みファイルやドロップされたファイルの情報、ユーザー APIのログ、PCAP情報など、調査に必要な重要な情報を提供します。脅威タイムラインにより、攻撃の実行段階を視覚的に確認できます。
- **Bro Network Security Monitorの統合:** 不審なネットワーク セグメントにBroセンサーを配備し、トラフィックのモニタリングと収集を行い、不審なファイルをMcAfee Advanced Threat Defenseに転送して分析できます。

配備

高度な脅威分析には柔軟な配備オプションが用意され、様々なネットワークに配備できます。McAfee Advanced Threat Defenseは、オンプレミス アプライアンスまたは仮想のフォーム ファクターとして使用できます。また、Azure Marketplaceのプライベート クラウドやパブリック クラウドにも対応しています。

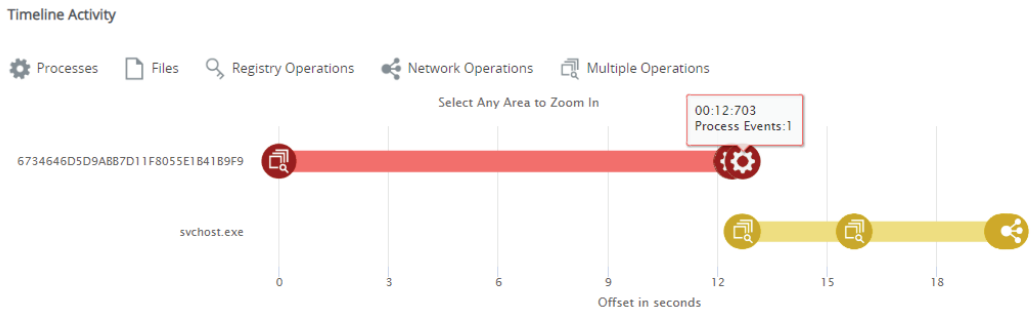

図 1. タイムライン アクティビティにより、分析した脅威の実行手順を視覚的に確認できる

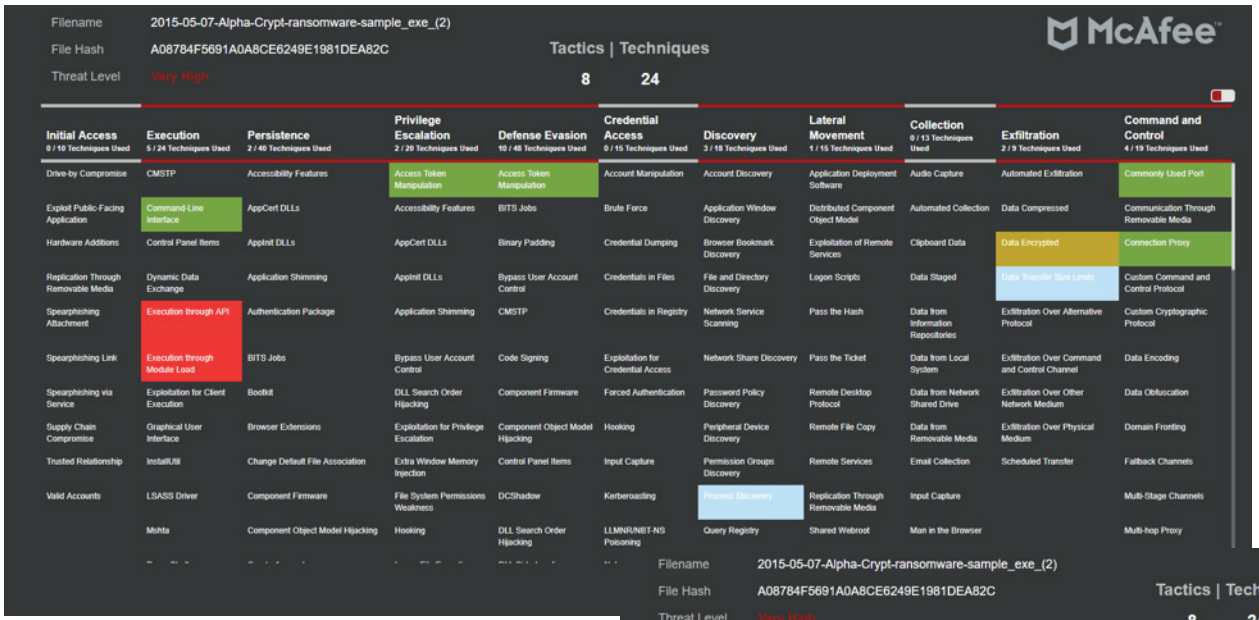

図 2. MITRE ATT&CK™フレームワークの結果マップ

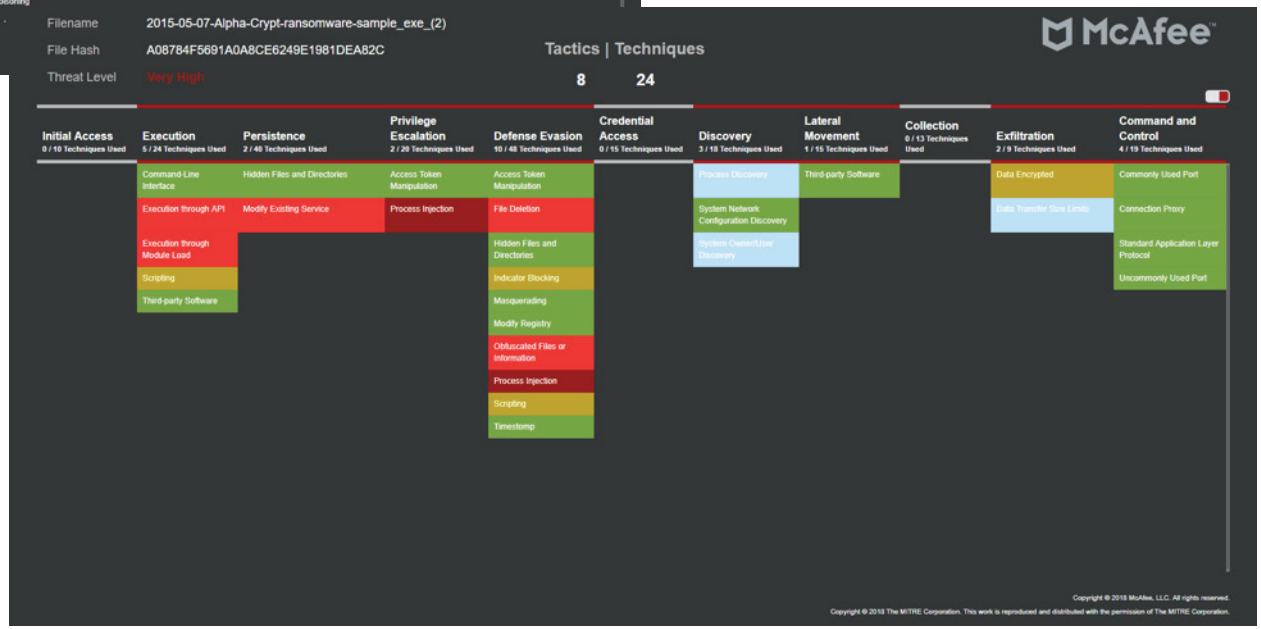

図 3. 図2の結果をフィルタリングし、確認した技術のみを表示

McAfee Advanced Threat Defenseの仕様		
物理フォーム ファクター	ATD-3200 1Uラックマウント	ATD-6200 1Uラックマウント
仮想フォーム ファクター	v1008 ESXi 5.5、6.0、6.5、6.7 Hyper-V Windows Server 2012 R2、Windows Server 2016	
検出		
対応のファイル/サンプル タイプ	PEファイル、Adobeファイル、Microsoft Officeファイル、イメージ ファイル、アーカイブ、Java、Androidアプリケーション パッケージ、URL	
分析方法	McAfee Anti-Malware Engine、GTIレピュテーション（ファイル/URL/IP）、Gateway Anti-Malware（エミュレーションと動作分析）、動的分析（サンドボックス）、詳細なコード分析、カスタムYARAルール、機械学習	
対応OS	Windows 10（64ビット）、Windows 8.1（64ビット）、Windows 8（32ビット/64ビット）、Windows 7（32ビット/64ビット）、Windows XP（32ビット/64ビット）、Windows Server 2016、Windows Server 2012、Windows Server 2012 R2、Windows Server 2008、Windows Server 2003、Android すべての言語のWindowsオペレーティング システム。	
出力形式	STIX、OpenIOC、XML、JSON、HTML、PDF、テキスト	
送信方法	ポイント製品との統合、RESTful API、手動送信、McAfee Advanced Threat Defense Email Connector（SMTP）	

詳細情報

McAfee Advanced Threat Defenseの評価をご希望の方は、弊社の営業担当までご連絡いただくか、次のサイトをご覧ください。

www.mcafee.com/enterprise/ja-jp/products/advanced-threat-defense.html

〒150-0043
東京都渋谷区道玄坂 1-12-1
渋谷マークシティ ウエスト 20F
Tel. 03-5428-1100（代表）
www.mcafee.com/jp