ソリューション概要

WannaCryとPetyaを阻止する

2017年5月、WannaCryマルウェア ファミリーによる大規模なサイバー攻撃が発生しました。WannaCryは、Microsoft Windowsの一部のバージョンに存在する脆弱性を攻撃しました。短時間で300,000台以上のコンピューターに感染し、身代金を請求しました。被害範囲は150か国に及んでいます。

最初の感染経路は不明ですが、ワームにより感染を拡大しています。このマルウェアが狙ったWindowsの脆弱性を解決するパッチは、3月にすでに公開されていましたが、多くの企業はこのパッチを適用していませんでした。

WannaCryの攻撃発生後、Microsoft はサポート対象外のWindows（Windows XP、Windows Server 2003）にもセキュリティ パッチを急きょリリースしました。

この6週間後、同じ脆弱性を悪用した別のサイバー攻撃が発生します。この攻撃ではPetyaというマルウェアが使用されましたが、WannaCryほどの被害は発生しませんでした。しかし、この2つのマルウェアによる攻撃で、重要な領域でいまだに古い、サポート対象外のオペレーティング システムが利用され、パッチ更新プロセスが徹底されていない組織が少なくないことが露呈しました。これらの攻撃の詳細な分析については、『McAfee脅威レポート: 2017年9月』をご覧ください。

WannaCryとPetyaを阻止するポリシーと手順

- **ファイルのバックアップ:** ランサムウェアに対する最も有効な対策は、データ ファイルのバックアップを定期的に行い、ネットワークの回復手順を確認しておくことです。
- **ネットワーク利用者への注意喚起:** 他のマルウェアと同様に、ランサムウェアもフィッシング攻撃でシステムに侵入を試みています。メールの添付ファイル、ダウンロード、Web閲覧は特に注意が必要です。
- **ネットワーク トラフィックの監視と調査:** これにより、ランサムウェアに関連する異常なトラフィックを検出できます。
- **脅威インテリジェンスのデータフィードの利用:** これにより、脅威をより迅速に検出できます。
- **コード実行の制限:** ランサムウェアの多くはオペレーティング システムのフォルダーで実行されます。これらのフォルダーに対するアクセスを制御することで、ランサムウェアによるデータの暗号化を防ぐことができます。
- **管理者権限によるシステム アクセスの制限:** デフォルトのアカウントを悪用するランサムウェアも存在します。このようなランサムウェアは、デフォルトのユーザー アカウント名を変更し、邪魔なアカウントを無効にすることで、攻撃を成功させようとします。
- **ローカル管理者権限の削除:** ローカル システムでのランサムウェアの実行と管理者権限を利用した拡散を防ぎましょう。ローカル管理者権限を削除することで、ランサムウェアが暗号化を試みる重要なシステム リソースやファイルへのアクセスをブロックできます。
- **権限関連のその他の対策:** ユーザーの書き込み権限を制限しましょう。ユーザー ディレクトリからの実行を阻止し、アプリケーションをホワイトリストに登録しましょう。ネットワーク ストレージや共有へのアクセス制限も検討する必要があります。自身のインストールや実行のために特定のファイル パスに対する書き込み権限を必要とするランサムウェアもあります。書き込み権限を特定のディレクトリ（ドキュメント、ダウンロードなど）に限定することで、このようなランサムウェアの実行を阻止できる可能性があります。これらのディレクトリから実行権限を削除するのも効果的な手段です。多くの企業では、仕事に使用できるアプリケーションを限定しています。これらのアプリケーションをホワイトリストに登録することで、ランサムウェアを含む他のアプリケーションの実行をブロックできます。また、ネットワーク フォルダーなどの共有リソースに対するログインも制限する必要があります。
- **ソフトウェアを常に最新の状態にする:** この他にも、ランサムウェア対策で重要となるがソフトウェアの更新です。ソフトウェア、特に、オペレーティング システム、セキュリティ、マルウェア対策ソフトウェアは常に最新の状態にしておく必要があります。

攻撃の侵入経路を塞ぐことも重要です。ランサムウェアでよく利用される侵入手段はフィッシング詐欺です。メールに対して次の対策を行いましょう。

- **コンテンツをフィルタリングする:** メールの保護は重要なポイントです。悪質なコンテンツを含む可能性があるスパムメールの受信量を減らすことで、攻撃の成功率が低くなります。
- **添付ファイルをブロックする:** 攻撃の侵入経路を塞ぐために、添付ファイルの検査は欠かせない作業です。ランサムウェアの多くは実行可能な添付ファイルとして散布されています。特定の拡張子のファイルをメールで送信できないようにポリシーを施行しましょう。これらの添付ファイルは、サンドボックス ソリューションで分析し、メール セキュリティ アプライアンスで削除できます。

WannaCryを阻止するMcAfee製品

McAfee Network Security Platform (NSP)

McAfee NSPは、エクスプロイトに迅速に対応し、ネットワーク内の資産を保護します。McAfee NSPチームは、重大な問題に対してユーザー定義シグネチャ (UDS) を迅速に開発し、配布しています。WannaCryの攻撃でも、攻撃発生から24時間以内にエクスプロイト ツールのEternalBlue、Eternal Romance SMB Remote Code Execution、DoublePulsarを対象にしたUDSを作成し、顧客のネットワーク センサーに配備しました。McAfeeは、元のトロイの木馬に関連する脅威をブロックできるように、関連する痕跡も公開しました。

NSPシグネチャの詳細については、こちらをご覧ください。

McAfee Host Intrusion Prevention (HIPS)

McAfee HIPS 8.0とNIPSシグネチャ6095を使用すると、現在確認されている4種類のWannaCryの亜種すべてに対応できます。この構成の最新情報については、KB89335をご覧ください。

カスタム シグネチャ#1:
WannaCryレジストリ ブロック ルール
標準サブルールを使用
ルール タイプ = レジストリ
操作 = 作成、変更、変幻の変更
レジストリ キーを含むパラメーター
レジストリ キー = \REGISTRY\MACHINE\SOFTWARE\WanaCrypt0r
実行ファイル = *

カスタム シグネチャ#2:
ファイル/フォルダー ブロック ルール
標準サブルールを使用
ルール タイプ = ファイル
操作 = 作成、書き込み、名前の変更、読み取り専用/隠し属性の変更、ファイルを含むパラメーター
ファイル = *.wnry
実行ファイル = *

McAfee Endpoint Protection（ENS）とMcAfee VirusScan Enterprise（VSE）適応脅威対策を使用する

McAfee Endpoint Security 10.5 — 適応脅威対策

McAfee Endpoint Security 10.5適用脅威対策のReal Protectとアプリケーションの動的隔離（DAC）を使用することにより、WannaCryが使用する既知または未知のエクスプロイトに対応できます。

- 適応脅威対策のオプション ポリシーで次の設定を行います。
  - ルールの割り当て = セキュリティ（デフォルトの設定は「バランス」です）
- 適応脅威対策のアプリケーションの動的隔離ポリシーで次のルールを設定します。
  - アプリケーションの動的隔離 — 隔離ルール

「KB87843: Endpoint SecurityのDynamic Application Containmentルールのリストとベストプラクティス」を参照して、推奨のDACルールを「ブロック」に設定してください。

McAfee Endpoint Security 10.1、10.2、10.5 — 脅威対策

McAfee Endpoint Security 10.x脅威対策とAMCoreコンテンツ バージョン2978以降を使用すると、現在確認されている4種類のWannaCryの亜種すべてに対応できます。

McAfee VirusScan Enterprise 8.8

McAfee VirusScan Enterprise 8.8とDATコンテンツ8527以降を使用すると、現在確認されている4種類のWannaCryの亜種すべてに対応できます。

McAfee Endpoint Security（ENS）とMcAfee VirusScan Enterprise（VSE）アクセス保護でプロアクティブな対策を実施する

McAfee ENSとMcAfee VSEのアクセス保護ルールで、.wnryファイルの作成を阻止します。このルールにより、.wncryt、.wncryまたは.wcryファイルを含む暗号化ファイルを作成する暗号化ルーチンの実行を阻止できます。.wnryファイルに対するブロックを実装するだけで、他の種類の暗号化ファイルをブロックする必要はありません。

McAfee VSEアクセス保護ルールの詳細については、こちらをご覧ください。

エンドポイント セキュリティ システムを設定してWannaCry（今後発生する亜種）によるファイルの暗号化を阻止する

McAfee ENSの適応型脅威対策を使用していない場合、McAfee定義のコンテンツ保護で未知の亜種に対応することはできません。リポジトリ更新タスクの実行間隔を最短にし、McAfeeからリリース後すぐに最新のコンテンツが適用されるように.設定することを推奨します。

暗号化ルーチンに対する追加の保護対策として、McAfee VSE/ENSのアクセス保護ルールやMcAfee HIPSカスタム ルールも使用できます。この構成の最新情報については、KB89335をご覧ください。

McAfee VSEとMcAfee ENSのアクセス保護ルール、McAfee HIPSカスタム シグネチャを使用して.wnryファイルの作成を防ぎます。

このルールにより、.wncryt、.wncryまたは.wcryファイルを含む暗号化ファイルを作成する暗号化ルーチンの実行を阻止できます。

.wnryファイルに対するブロックを実装するだけで、他の種類の暗号化ファイルをブロックする必要はありません。

この構成の最新情報については、KB89335をご覧ください（記事を参照するには、McAfeeへのユーザー登録が必要です）。

McAfee Advanced Threat Defense（ATD）

McAfee ATDの機械学習により、重大度中の分析でサンプルを特定できます。

McAfee ATDは次のことを行います。

動作の分類:

- 難読化されたファイル
- 拡散
- シェルコードによる攻撃
- ネットワーク伝播

動的分析:

- ランサムウェアの誘発行動
- ファイルの暗号化
- 不審なスクリプト コンテンツの作成と実行
- トロイの木馬マクロ ドロッパーなどの動作

WannaCryに関して、McAfee ATDは現在までに22のプロセスを監視しています。この中には、5個のランタイムDLL、58個のファイル操作、レジストリの変更、ファイルの変更、ファイルの作成（dll.exe）、DLLインジェクション、34個のネットワーク操作が含まれます。

McAfee Web Gateway（MWG）

McAfee Web Gateway（MWG）はWebプロキシの製品ファミリー（アプライアンス、クラウド、ハイブリッド）で、複数のリアルタイム スキャン エンジンを使用して、Web（HTTP/HTTPS）からのWannaCryの侵入を阻止します。

プロキシでWebトラフィックが処理されるときに、既知の亜種は、McAfee Global Threat Intelligence（GTI）のレピュテーションとマルウェア スキャンでブロックされます。

MWGのGateway Anti-Malware（GAM）Engineは、ファイル、HTML、JavaScriptに対して動作エミュレーションを実行し、シグネチャで未対応の亜種（ゼロデイ脅威）を阻止します。このエミュレーターには、機械学習モデルにより定期的に脅威情報が提供されます。トラフィックを処理するときに、GTIレピュテーション、マルウェア対策と一緒にGAMが実行されます。

MWGとATDを使用することで、脅威を効率的に検出し、防止することができます。

McAfee Threat Intelligence Exchange（TIE）

McAfee Threat Intelligence Exchange（TIE）により、セキュリティをさらに強化できます。TIEは、ENS、VSE、MWG、NSPからレピュテーション情報を収集し、統合環境内で情報を共有します。WannaCry関連の情報も迅速に共有できます。GTIでグローバルなレピュテーション情報を照会できるので、ランサムウェアが実行される前に、TIEデータベースのレピュテーション情報を利用して対策を講じることができます。

1つのエンドポイントが亜種を検出して侵入を阻止し、レピュテーション スコアを更新してTIEに送信すると、TIEで接続されているすべてのエンドポイントにこの情報が提供されます。MWGとNSPでも脅威インテリジェンスが双方向で共有されます。ネットワークやWebに脅威が侵入を試みると、MWGとNSPが脅威を検出して阻止し、この情報をTIEと共有します。これにより、他のエンドポイントへの攻撃を未然に防ぎ、環境を保護することができます。

Petyaを阻止するMcAfee製品

McAfee Advanced Threat Defenseの高度なマルウェア動作分析、Real Protect Cloud、Dynamic Neural Network（DNN）を使用すると、Petyaの攻撃を初期段階で阻止することができます。

ATD 4.0では、半教師付き学習を行う多層型の逆伝播ニューラル ネットワーク（DNN）を使用する新しい検出機能が導入されました。DNNは、マルウェアの特定の特徴を検出し、その評価結果から不正なコードかどうかを判断します。

ATDは単独で使用することも、McAfeeのエンドポイントやネットワーク センサーに接続することもできます。いずれの場合も、ATDはサンドボックスの動作分析と高度な機械学習で脅威情報を処理し、ゼロデイの適応型保護対策を提供します。Dynamic Endpointソリューションに含まれるReal Protectは、機械学習とリンク分析により、シグネチャを使わずにマルウェアを阻止します。また、Dynamic EndpointとMcAfeeエコシステムの残りの部分に豊富な情報を提供します。Real Protectとアプリケーションの動的隔離を使用すると、Petyaを早期に検出し、攻撃を未然に防ぐことができます。

また、複数のMcAfee製品を組み合わせることで、攻撃を封じ込め、更なる攻撃を防ぐことができます。

McAfee Endpoint Security

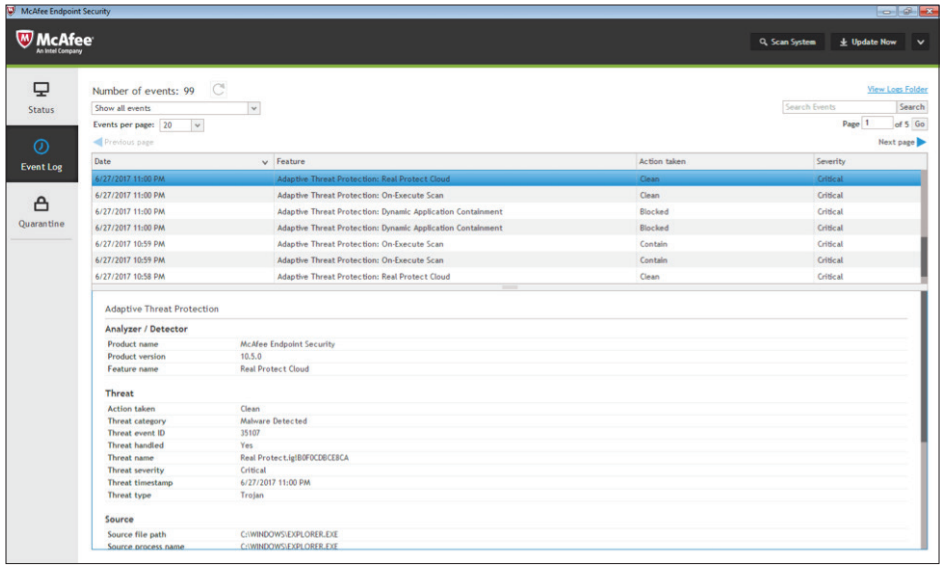
脅威対策

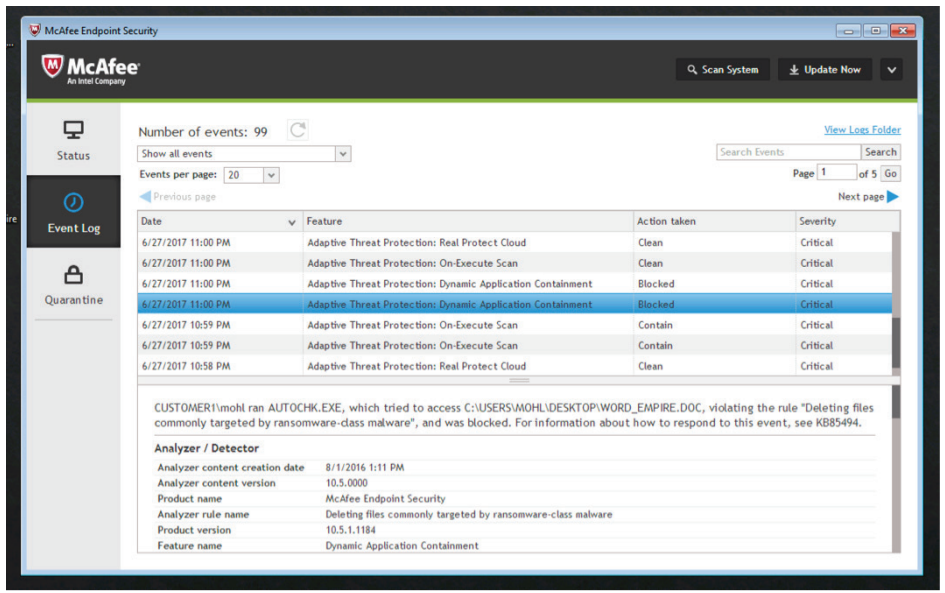
- McAfee Endpoint Security、McAfee Global Threat Intelligence、感度レベル「低」のオンアクセス スキャン ポリシーにより、既知のサンプルと亜種を阻止できます。
- McAfee GTI ファイル レピュテーションの推奨設定については、KB74983をご覧ください。詳細については、KB53735をご覧ください。
- McAfee Threat Intelligence ExchangeとGTIで、既知のサンプルと亜種を阻止できます。

McAfee ENS 10のシステムは、シグネチャと脅威インテリジェンスの両方を使用して既知のサンプルと亜種から保護されます。

適応脅威対策

- 適応脅威対策（ATP）をバランス モード（[ATP]、[オプション]、[ルールの割り当て]で設定されているデフォルト）で使用すると、Petyaランサムウェアの既知と未知の亜種を阻止できます。
- ATPモジュールが複数の防御機能で未知の脅威を阻止します。
  - ATPのReal Protect Staticが、クライアント側で実行前の動作分析を行い、未知の脅威を監視します。
  - ATPのReal Protect Cloudが、クラウドの機械学習を使用して脅威を識別し、駆除します（右の上の図）。
- ATPのアプリケーションの動的隔離（DAC）が脅威を封じ込め、被害を未然に防ぎます（右の下の図はDACイベントを表しています）。





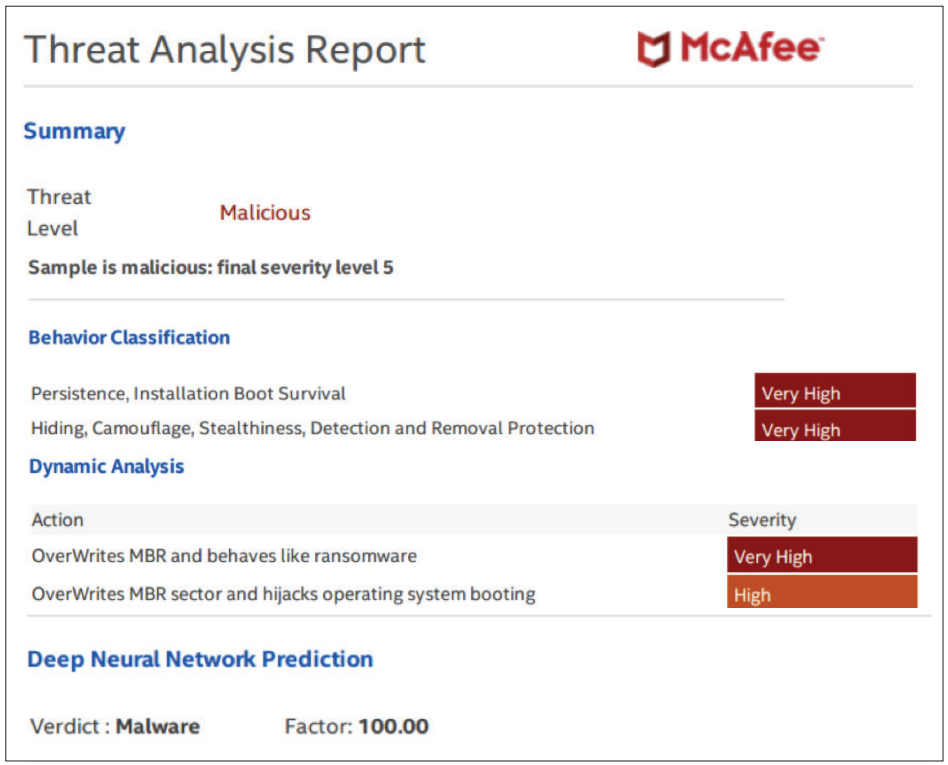
McAfee Advanced Threat Defense

- McAfee Advanced Threat Defense 4.0とDeep Neural Network、Dynamic Sandboxにより、脅威を識別し、攻撃が発生する前にサイバー防御のエコシステムを更新します（以下を参照）。

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager（ESM）は、セキュリティ情報/イベント管理ソリューションです。有益な情報に基づいて脅威の優先度を判別し、調査、対応を行うことができます。McAfee ESMのSuspicious Activity Content PackとExploit Content Packが更新され、WannaCry用のルール、アラーム、ウォッチリストが追加されています。これにより、感染の有無を確認できます。これらの更新はPetyaにも有効です。いずれのコンテンツ パックも無料でMcAfee ESMコンソールからダウンロードできます。McAfee ESMのデフォルトの相関ルールでもユーザーにアラートを送信し、SMBスキャンのレベルを向上できます。

WannaCryと同様に、Petyaの攻撃も学習によってセキュリティ オペレーション センターの分析能力を向上できます。『ベストプラクティスとその自動化』で今後の攻撃に対応する方法をご確認ください。



McAfee Web Gateway

McAfee Web Gateway（MWG）はWebプロキシの製品ファミリー（アプライアンス、クラウド、ハイブリッド）で、複数のリアルタイム スキャン エンジンを使用して、Web（HTTP/HTTPS）からのPetyaの侵入を阻止します。プロキシでWebトラフィックが処理されるときに、既知の亜種はGTIのレピュテーションとマルウェア スキャンでブロックされます。

MWGのGateway Anti-Malware Engineは、ファイル、HTML、JavaScriptに対して動作エミュレーションを実行し、シグネチャが未対応のゼロデイ脅威を阻止します。このエミュレーターには、機械学習モデルにより定期的に脅威情報が提供されます。トラフィックを処理するときに、GTIレピュテーション、マルウェア対策と一緒にGAMが実行されます。

MWGとATDを使用することで、脅威を効率的に検出し、防止することができます。

DATファイルを使用するMcAfee製品

McAfeeは、Petyaに対応するためExtra.DATをリリースしました。また、この脅威用の緊急DATもリリースしています。このコンテンツは今後のDATに組み込まれます。最新のDATファイルについては、Knowledge Centerの記事KB89540をご覧ください。

詳細情報

技術情報は頻繁に更新されています。最新の情報については、McAfee Knowledge Centerの記事KB89335、KB87843、KB74983、KB53735、KB89540をご覧ください。

〒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
www.mcafee.com/jp