技術概要

ランサムウェアを阻止する方法

現在のランサムウェアの脅威を阻止するIntel® Securityの製品

ランサムウェアは、非対称暗号で標的の情報を暗号化し、金銭を要求するマルウェアです。非対称暗号（公開鍵/秘密鍵）は、鍵のペアを使用してファイルの暗号化と復号を行う暗号化技術です。攻撃者は標的ごとに固有の鍵ペア（公開鍵/秘密鍵）を生成し、ファイルの復号に使用する秘密鍵をサーバーに格納します。攻撃者は身代金と引き換えに秘密鍵を渡すとしていますが、最近のランサムウェアを見ると、言葉どおり秘密鍵が渡されるとは限りません。秘密鍵がなければ、ファイルの復号はほぼ不可能です。

ランサムウェアには様々な種類があります。ランサムウェアなどのマルウェアの多くはスパム メールや標的型攻撃で配布されています。Intel® Securityの製品は様々な技術を使用してランサムウェアを阻止します。次のMcAfee®製品と構成を使用してランサムウェアを阻止してください。

McAfee VirusScan® Enterprise 8.8またはMcAfee Endpoint Security 10

- 常に最新のDATファイルを使用します。
- McAfee Global Threat Intelligence（McAfee GTI）を使用します。McAfee GTIは800万を超えるランサムウェアのシグネチャを保持しています。
- ランサムウェアのインストールを阻止するアクセス保護ルールを作成します。アクセス保護ルールについては、KnowledgeBaseの記事KB81095、KB54812をご覧ください。

McAfee Host Intrusion Prevention

- CryptoLockerのペイロードを阻止するようにHost Intrusion Preventionを設定する方法については、この動画をご覧ください。
- Host Intrusion Preventionのシグネチャ3894 Access Protection—Prevent svchost.exe executing non-Windows executables（アクセス保護－svchost.exeによるWindows以外の実行ファイルの実行阻止）を有効にします。
- Host Intrusion Preventionシグネチャ6010と6011を有効にして、インジェクションをすぐにブロックします。

intel Security

McAfee Host Intrusion Preventionルール
McAfee Host Intrusion Preventionは、ファイルの作成、読み取り、書き込み、実行、削除、名前の変更、属性の変更、ハードリンクの作成をモニタリングします。必要または不要なファイル パス/タイプを定義し、リストに追加した実行ファイル（既知の不正なソース）や除外した実行ファイル（誤検知の原因）を警告します。このルールは侵入型になる可能性があります。トライアル期間は、情報/ログ モードでルールを使用することを検討してください。ファイル保護ルールを使用する場合には、信頼されたアプリケーション データベースに接続する必要があります。

Rule:Cryptolocker—block EXE in AppData

Rule type: files

Operations: create, execute, write

Parameters:

- Include: Files:**\AppData*.exe
- Include: Files:**\AppData\Local*.exe
- Include: Files:**\AppData\Roaming*.exe

Executables:Include *.*

次の例では、スペースの関係から、多くのファイル拡張子を省略しています。アプリケーションに該当するファイルの拡張子をすべて確認してください。

Rule {

tag “Blocking a Non-Trusted program attempt to write to protected data file extensions”

Class Files

Id 4001

level 4

files {Include “**.3DS” “**.7Z” “**.AB4” “**.AC2” “**.ACCDB” “**.ACCDE” “**.ACCDR” “***.ACCDT” “**.ACR” “**.ADB” “**.AI” “**.AIT” “**.al” “**.APJ” “**.ARW” “**.ASM” “**.ASP” “**.BACKUP” “**.BAK” “**.BDB” “**.BGT” “**.BIK” “**.BKP” “**.BLEND” “**.BPW” “**.C” “**.CDF” “**.CDR” “**.CDX” “**.CE1” “**.CE2” “**.CER” “**.CFP” “**.SRF” “**.SRW” “**.ST4” “**.ST5” “**.ST6” “**.ST7” “**.ST8” “**.STC” “**.STD” “**.STI” “**.STW” “**.STX” “**.SXC” “**.SXD” “**.SXG” “**.SXI” “**.SXM” “**.SXW” “**.TXT” “**.WB2” “**.X3F” “**.XLA” “**.XLAM” “**.XLL” “**.XLM” “**.XLS” “**.XLSB” “**.XLSM” “**.XLSX” “**.XLT” “**.XLTM” “**.XLTX” “**.XLW” “**.XML” “**.ZIP”}

Executable {Include “*”}

user_name{Include “*”}

directives files:writefiles:renamefiles:delete

}

- アクセス保護ルール: アクセス保護ルールでは、ワイルドカードを使用してHost Intrusion Preventionルールを強化できます。
  \Users\AppData***.exe

注: McAfee VirusScan Enterprise、McAfee Agent, Host Intrusion Prevention、Data Loss Preventionの更新バージョンでSYSCoreの新しいバージョンが提供されている場合、[File or folder name to block] (ブロックするファイルまたはフォルダーの名前) フィールドの先頭に**は使用できません。新しいバージョンでは、次の形式を使用する必要があります。

```
C:\**\AppData\**.exe
```

このルールは、C:ドライブのAppDataフォルダーのルートとサブディレクトリにある任意の.exeをブロックします。

この種類のルールは制限なく繰り返し実行される可能性があります。ルールのすべての部分を検討してください。ルールのすべての部分、特定の機能で使用可能な項目、ルールの設定方法の確認が必要になる場合があります (以下に例を示します)。

```
Process to include: *

Process to exclude: [空白にする]

File or folder name to block: <パスまたはディレクトリ>

File actions to prevent: [必要なアクション。エンドポイントに対する被害を最小限に抑えるため、攻撃性の少ないアクションから始めることをお勧めします。]
```

McAfee SiteAdvisor® EnterpriseまたはEndpoint Security/Web Protection

- Webサイトのレピュテーションを使用して、ランサムウェアを配布するサイトの利用を阻止または警告します。

McAfee Threat Intelligence ExchangeとAdvanced Threat Defense

- Threat Intelligence Exchangeのポリシー設定:
  - 監視モードから開始します。エンドポイントで不審なプロセスを検出したときに、システム タグを使用してThreat Intelligence Exchange施行ポリシーを適用します。
  - 駆除: 既知の不正な項目
  - ブロック: 不正である可能性が非常に高い項目。レピュテーションが不明なファイルをブロックすると、保護対策は強化されますが、初期の管理作業が増えます。
  - レピュテーション レベルが不明以下の場合、McAfee Advanced Threat Defenseにファイルを送信します。
  - Threat Intelligence Exchangeサーバーのポリシー: Threat Intelligence Exchangeが未確認のファイルは、Advanced Threat Defenseのレピュテーションを使用します。
- Threat Intelligence Exchangeの手動操作:
  - ファイル レピュテーションの施行 (動作モードによります)
    不正な可能性が非常に高い: 駆除/削除
  - 不正な可能性がある: ブロック

- エンタープライズ レピュテーションでMcAfee GTIのレピュテーションを上書きできます。
  - たとえば、非対応または脆弱なアプリケーションをブロックできます。
  - ファイルに「不正な可能性がある」というマークを付けます。
- テストでは不要なプロセスを許可できます。
  - ファイルに「信頼できる可能性がある」というマークを付けます。

McAfee Advanced Threat Protection

- すぐに使える検出機能:
  - シグネチャ ベースの検出 ― McAfee Labsでは、800万件を超えるランサムウェア シグネチャ（CTB-Locker、CryptoWallの亜種を含む）を登録しています。
  - レピュテーション ベースの検出 ― McAfee GTI
  - リアルタイムの静的分析とエミュレーション ― シグネチャを使用しない検出
  - カスタムYARAルール
  - 完全な静的コード分析 ― リバース エンジニアリングでファイルのコードを解析し、その属性と機能セットを特定します。ファイルを実行せずにソース コードを分析します。
  - 動的なサンドボックス分析
- 分析用のプロファイルを作成し、ランサムウェアが実行される可能性が高い場所を特定します
  - 一般的なOS、Windows 7、8、XP
  - Windowsアプリケーション（Word、Excel）をインストールしてマクロを有効にします。
- 分析用プロファイルでインターネット アクセスを許可します。
  - サンプルの多くは、Microsoftドキュメントに含まれるスクリプトを実行し、外部に接続してマルウェアを実行します。インターネットに接続する分析用プロファイルを作成すると、検出率が高くなります。

McAfee Network Security Platform

- Network Security Platformのデフォルト ポリシーに含まれるシグネチャで検出を行います。
  - シグネチャ ID=0x4880f900（ランサムウェア用）があることを確認します。
  - Network Security Platformのシグネチャでは、マルウェア関連のファイル転送に使用される可能性があるTORも識別できます。
- Advanced Threat Defenseとの統合で攻撃の新しい亜種を検出:
  - 詳細なマルウェア ポリシーでAdvanced Threat Defenseとの統合を設定します。
  - Network Security Platformが.exe、Microsoft Officeファイル、Javaアーカイブ、PDFファイルをAdvanced Threat Protectionに送信し、検査するように設定します。
  - Advanced Threat Protectionの設定がセンサー レベルで適用されていることを確認します。
- コールバック検出ルール（ボットネット用）を更新します。

McAfee Web Gateway

- McAfee Gateway Anti-Malwareによる検査を有効にします。
- McAfee GTIを有効にして、URLとファイルのレピュテーションを取得します。
- Advanced Threat Defenseと統合し、サンドボックスでゼロデイ脅威を検出します。

VirusTotal Convicter: 自動処理

- ConvicterはPythonスクリプトです。McAfee ePolicy Orchestrator®（McAfee ePO™）の自動応答システムで実行されます。McAfee Threat Intelligence Exchange脅威イベントを生成したファイルをVirusTotalで調査できます。
- GetSuspなど、他の脅威情報交換を参照するようにスクリプトを変更できます。
- コミュニティの信頼しきい値を満たしていれば、スクリプトはエンタープライズ レピュテーションを自動的に設定します。
- 推奨のしきい値: ベンダーの30%と大手2社の同意が必要
- フィルター: 対象のファイル名に次の項目を入れない: McAfeeTestSample.exe
- これは無料のコミュニティ ツールです（McAfee/Intel Securityのサポートはありません）。

McAfee Active Response

Active Responseは、高度な脅威を検出して対応します。McAfee GTI、Dell SecureWorks、ThreatConnectなどの脅威フィードと関連付けると、広範囲に拡散する前に新しい脅威（ランサムウェアを含む）を検出し、被害を未然に防ぐことができます。

- カスタム コレクターにより、ランサムウェアの侵害兆候を検出し、識別する特定のツールを作成できます。
- トリガーや対応はユーザーが作成し、特定の条件下で実行されるアクションを定義します。たとえば、ハッシュまたはファイル名が見つかったときに、削除アクションを自動的に実行します。

詳細情報

Protecting Against Ransomware（ランサムウェアから保護する）
このKnowledgeBaseの記事では、Intel Security環境でランサムウェアを阻止する方法を詳しく説明しています。

CryptoLockerランサムウェアの亜種、兆候、攻撃方法、防止策については、次の動画をご覧ください。

- CrytpoLocker Malware Session（CrytpoLockerマルウェア セッション）
- CryptoLocker Update（CryptoLockerの最新情報）

McAfee Labs脅威アドバイザリ: X97M/Downloader
この記事では、最新のランサムウェアを詳しく分析しています。

ランサムウェアから大切なデータを守る
この4ページのソリューション概要では、ランサムウェアの概要とIntel Securityのソリューションがこの脅威を阻止する方法を説明しています。

Advice for Unfastening CryptoLocker Ransomware（CryptoLockerランサムウェアから復旧するためのアドバイス）
このブログでは、ランサムウェアによる攻撃を受けた後の対処方法を説明しています。

ランサムウェア: 巧妙さを増した新しいファミリの出現
McAfee Labs脅威レポートの記事（14ページ）。進化を続けるマルウェアについて解説しています。

McAfee. Part of Intel Security.
マカフィー株式会社
東京本社　〒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）FAX 03-5428-1480
西日本支店　〒530- 0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233（代）FAX 052-551-6236
福岡営業所　〒810- 0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com