ランサムウェアの被害者にならないためのガイド

組織とデータを保護するためにできる 15 の実用的なステップ

ウェブルート株式会社

2016 年 4 月

目次

背景

この二年半で、ランサムウェアの脅威と攻撃が大幅に増える中、ウェブルートでは多くのブログと記事で、この犯罪集団からどう防御するべきかを紹介してきました。企業または一般のユーザが、恐喝に応じるか、それとも重要なデータを全て無くしてしまうか、という選択をしないといけない状況になるべきではないと信じています。

「どのエンドポイント保護製品がランサムウェアから 100%保護することができるだろうか」という質問を受けることが多くなっていますが、簡単な答えは「そのような製品はない」です。最高のエンドポイント保護製品（ウェブルートは常にこれを目指しています）でも、多くの場合、100%に近い効果を実現できるだけです。その他の場合、サイバー犯罪者は、エンドポイント保護の防御をかいくぐり、攻撃が成功してしまうこともあります。

エンドポイント保護の提供会社として、例えウェブルートの高効率のセキュリティでも感染する可能性があると知っていながら、何もしないというスタンスを取ることはできません。例えば、保護されたバックアップなどの主要な軽減戦略によって、環境をよりセキュアにすることができるのです。

ランサムウェアに関するオンラインセミナーを数多く開催し、様々な質問を受けた結果、このガイドを提供し、ウェブルートのユーザとその他の組織に、どのようにランサムウェア対策を行うことができるかご紹介致します。「ランサムウェアの被害者にならないためのガイド」と名付け、IT 環境をセキュアにし、ランサムウェアに感染しないようにするための 15 の主要方法を説明します。また、これらの簡単な作業を行うことによって、増え続ける大変危険な犯罪脅威を軽減できるかを紹介します。

尚、このガイドは一般的なアプローチの一部を紹介することが目的です。場合によっては、企業の IT 環境にマッチしないこともあります。このガイドの内容を実行した場合、正しくインストールされない、または期待されたように機能しないプログラムが一部あるため、ご注意ください。

ランサムウェアの被害を低減するためのガイド

このガイドでは、いくつかの軽減化戦略を紹介し、どのように企業や組織のデータをランサムウェア攻撃から防御できるかを説明します。

ランサムウェアは時間と共に進化しており、エンドポイントの感染のみならず、企業ネットワークのローカルドライブ、割り当てされたドライブ、またマッピングされていないドライブまで感染することがあります。ランサムウェアは、単純に面倒なセキュリティリスクではなく、Ransomware as a Service（RaaS）のフル導入を中心とした、持続性が高く組織化された犯罪行為なのです。

適切な対策をしないで、軽減化戦略も行わずに、ランサムウェアの被害に遭ってしまうと、その影響は小さくはありません。実際の被害にあったロサンゼルスの病院では、生命の危険さえもありました。中小企業においては、企業の存続にも関わるほどの被害になる可能性があります。

1. 実績のあるマルチベクトルなエンドポイントセキュリティを実施

エンドポイント保護では、多くの選択肢があります。ランサムウェア対策では参考になる検知テストが公表されていますが、多くの検知テストは信頼できません。テストでは 100%の検知率を達成しているソフトウェアが多いのですが、実際のリアルな環境でそのテスト結果を再生することができない場合が多いのです。

ウェブルートは、ランサムウェア対策においては、高く評価されています。ウェブルートの目標は、まず 100%の効果を出すことです。ウェブルートは、アンチウイルス・アンチマルウェアのベンダーとしては、初めて標準のシグネチャベースのファイル検知手法から完全に移行したベンダーです。クラウドコンピューティングの性能を活用することによって、ウェブルートは従来の「問題が起きてから対応する」アンチウイルス対策から、プロアクティブなリアルタイムのエンドポイント監視と脅威インテリジェンスの活用に移行し、各エンドポイントを個別に保護すると同時に、脅威データの収集、分析、普及を総合的に行います。

この予測型感染保護モデルによって、ウェブルートのソリューションは正確に既存の変更された実行ファイルやプロセスの分類を行い、現在の状況を実行されるポイントで把握することができます。このアプローチで、ウェブルートはシグネチャベースのアプローチより多くの感染を確認しブロックすることができ、またランサムウェアの検知とブロックも高効率で行うことができます。

もちろん複数の脅威ベクトルに対応した保護が必要です。例えば、リアルタイムのアンチフィッシング機能でフィッシングサイトへのメールリンクをブロックしたり、ウェブブラウザの脅威を止めるブラウザ保護やウェブレピュテーションなどで、場合によっては安全ではないリスクが高いサイトへのアクセスをブロックすることができるなどです。

ウェブルートは 4 年間、このアプローチによって、デバイスが感染するときにリアルタイムにマルウェアをブロックし、暗号化プロセスが始まる前に止める事ができてきました。現時点でウェブルートは、大きなスケールで、実績があるエンドポイントでのマルウェア保護を提供している唯一のエンドポイント・セキュリティ・ベンダーであると言えます。

その結果、ウェブルートは従来のエンドポイント・アンチウイルス・ソリューションのリプレース候補として、大幅に導入が増えています。

どのエンドポイントセキュリティソリューションを選択するかに関係なく、マルウェアに対して多面の保護と予防を提供すること、そして外部の脅威と不審な振る舞いを認識することが重要です。ファイルベースの脅威の保護を行うだけではない、次世代型のエンドポイント保護ソリューションが必要なのです。

2. データバックアップの重要性

もしランサムウェアによるデータの暗号化を止められなかった場合、データの復旧と業務のダウンタイムを短縮することが、次に最適な保護対策です。バックアップ戦略を考えるときに、CryptoLocker のようなランサムウェアは割り当てされたドライブのファイルも暗号化するというリスクを考えてください。また、ランサムウェアの亜種にはマッピングされていないドライブにも影響することがあります。ランサムウェアは、USB ドライブのような外部ドライブも検索するほか、ドライブの文字を指定されているクラウド上のファイル保存場所も検索できてしまいます。

定期的なバックアップを設定し、最低でも外部ドライブまたはバックアップサービスにデータを保存するほかに、バックアップしてない時には、完全に切断された環境を構築する必要があります。

データとシステムのベストプラクティスとしては、最低でも異なる三ヵ所にバックアップする必要があります。

1. メインとなるストレージ（ファイルサーバ）
2. ローカルのディスクへのバックアップ

3. クラウド上の企業継続サービスへのミラーリング

ランサムウェアの被害にあった場合、このバックアップシステムでは、データ乗っ取りの影響を軽減し、重要な IT システムのフル機能を短時間で再構築することが可能となります。企業継続計画と災害復旧計画がない場合の最悪の事態を考えると、MSP と企業が自社のシステムを深く再検討し、保護するためのソリューションへの投資を検討することが必要です。

ランサムウェアは、バックアップを行わない企業に最も影響を与えますが、定期的なバックアップはどのような企業の IT インフラでも、まず中心に考えるべき事です。バックアップとリカバリのサービスはコストもあまりかからないため、企業が最適な計画を行わない理由はありません。

3. 一般的な保護のポイント

これらのポイントは、様々な企業で IT 環境を保護するため、そしてランサムウェアの脅威と攻撃をブロックするために活用されています。

3.1. 選択されたエンドポイント保護製品がインストールされて、正しく設定されていることを確認

適切な保護ポリシーが正しくユーザグループに適用されているかを確認する。

3.2. バックアップが正しく稼働しているかを定期的に確認する

バックアップが正しく稼働し、データの整合性がとれているか、そしてホストにデータを復旧できるかを確認するのは非常に重要な作業です。

3.3. 最新の Windows アップデートが適用されているか

もし Windows の最新アップデートが適用されていれば、マルウェアに感染するリスクをすぐに削減することができます。余計な作業を減らすために、最新のアップデートを適用し、パッチ当てをルーティン化するようにしましょう。バックアップと同様、パッチが最新ではないため、多くの組織が感染による大きな被害を受けることがあります。これはセキュリティの基本であり、最適なパッチ管理を行わないことに言い訳はできません。

3.4. 全てのプラグインを最新にアップデートする

全てのサードパーティのプラグインを最新のビルドにアップデートするのは、脆弱性のリスクを減らすために非常に重要です。こちらも最適な管理を行いましょう。

3.5. 最新のブラウザを活用し、広告をブロックするプラグインを使う

Chrome や Firefox のような最新ブラウザは、脆弱性を低減するために常にアップデートが行われています。また、これらのブラウザではオプションとして、BHO（Browser Helper Object）やプラグインを追加することによって、ユーザの安全を高める事ができます。最も基本的なこととして、ポップアップのブロック機能をインストールし、利用することによって、多くのユーザを感染から守ることができます。

3.6. オートランを無効にする

オートランは便利な機能ですが、多くのマルウェアがこの機能を悪用し、企業環境の中に拡散していきます。USB メモリの増加に伴い、マルウェアがオートラン機能を悪用することが増えています。Visual Basic Script（VBS）マルウェアやウォームが主に悪用する機能なので、ポリシーとして無効にすることが最適です。

3.7. Windows Scripting Host を無効にする

マルウェア開発者はマイクロソフトのスクリプトである VBS を悪用し、環境への破壊活動を行ったり、より先進的なマルウェアをダウンロードするための処理を行います。しかし、VBS ファイルが稼働する Windows Scripting Host エンジンを無効にすることによって、VBS ファイルを無効にすることが可能です。

3.8. ユーザが管理者権限ではなく制限ユーザとして PC を利用

これはセキュリティの観点では非常に望ましいのですが、パワーユーザにとっては、難しいことかもしれません。しかし、現在のランサムウェア脅威は、エンドユーザがアクセスできるマッピングされたドライブのデータを閲覧し暗号化することができるため、これは非常に重要なことです。ユーザ権限を制限し、共有フォルダやマッピングされたドライブへのアクセスを制限することによって、暗号化できるファイルを減らすことができます。

3.9. 隠されたファイル拡張子を表示する

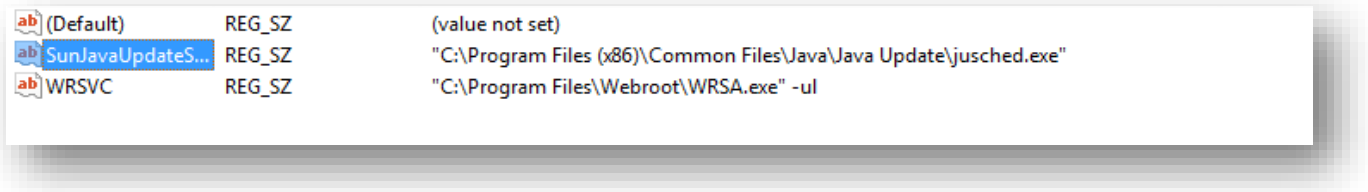
CryptoLocker やその他のランサムウェアは、「.PDF.EXE」のような拡張子が付いたファイル名で送られてくることがあります。マルウェア開発者は Windows の標準機能である既知の拡張子を表示しないという機能を悪用し、不正なファイルの信頼度を高めようとします。もし拡張子を表示するように設定すれば、ユーザと管理者が不審なファイルを簡単に見つけることが可能です。

4. ランサムウェア対策のために Windows のポリシーを作成する

ランサムウェア対策のために Windows のポリシーを作成し、パスやファイル拡張子の稼働をブロックすることができます。

脆弱性のあるソフトウェアとして Java が一番有名ですが、一般的に利用されている全てのプラグインに言えることです。もし特定のプラグインを利用することがないのであれば、インストールしないことをお薦めします。

もし利用するのであれば、最新版にアップデートすることを推奨します。また、Java アップデーターのランキーを無効にしないようにしましょう。



Java アップデータサービスの例

コモンパス

このガイドでは、パスとファイル形式を取り上げているので、簡単な説明が必要かもしれません。マルウェアは、一般的に少数のコモンパスに侵入してきます。侵入後、マルウェアは PC およびネットワーク内を自由に移動します。

マルウェアが侵入するコモンパスは：

- ユーザのテンポラリフォルダ（%localusertemp%の場合が多い）
- アプリデータとそのサブフォルダ（ローミング、ローカルアプリデータ）
- ユーザプロファイル
- Temp フォルダ（%temp% または C:¥Windows¥temp）
- ブラウザのキャッシュフォルダ（ブラウザによって異なる%cache。下の例を参照）
- c:¥users¥admin¥appdata¥local¥microsoft¥windows¥temporaryinternet files¥content.ie5¥
- デスクトップフォルダ

%が付いているパスに異動するには、フレーズを「run window」または「windows start search」に入力。例えば、「%temp%」を入力すると、**「C:¥Users¥admin¥AppData¥Local¥Temp」**へ移動します。

マルウェアが PC に感染しアクティブになった場合、マルウェアは自由に PC 内を移動し、検知することがより難しくなります。または、自身を拡散しやすい場所に移動することもあります。さらに先進的なマルウェアであれば、ネットワークパスへ拡散することもあります。レジストリのエントリで自動実行したり、タスクサービスとして時間で起動するように行動することもあります。

- C:¥program data¥（標準で非表示のフォルダ）
- C:¥Windows
- C:¥Windows¥System32
- C:¥Recylcer¥ （非表示フォルダ、ゴミ箱）
- c:¥のルート
- C:¥Program files¥ （32 および 64 ビットのパス、PUA がこのフォルダに見つかることが多い）

マルウェアは認知度の高いファイル名を使ったり、Windows のシステム名を使うなどして、ユーザを騙そうとすることが少なくありません。例えば、 Winlogon.exe は Windows のコアコンポーネントであり、**c:¥windows¥system32¥winlogon.exe** で見つかり、通常のファイルサイズは約 450kb です。

もしユーザのテンポラリフォルダで WinLogon.exe ファイルを見つけて、ファイルサイズが通常の倍以上であれば、そのファイルを確認するべきです。多くの場合、アンチマルウェアソフトがそのファイルを処理していますが、しかしこのガイドで紹介しようとしている内容の一つの例となります。ここからは、ポリシーをどのように設定し、特定のファイル形式とパスへのアクセスを制限できるかを紹介していきます。

より制限が多いほど、IT 環境を安全にすることができますが、その結果、いくつかのプログラムが正しく機能しない可能性もあります。

5. 二つ目のブラウザを活用する

PC で二つ目のブラウザを利用することには、大きなメリットがあります：

5.1. もし主要ブラウザに被害があった場合、リモート接続ができなくなります。全員が RDP を使っていることはなく、また RDP は無効にすることを推奨しています。
5.2. PUA またはマルウェアはブラウザのスピードを遅くし、その結果、不安定になり使えなくなります。
5.3. IEの古いバージョンでは正しいレンダリングが行われない。FirefoxとChromeを利用して、テストができます。
5.4. Windows の古いバージョンでは、最新の IE をインストールできない場合がある。
5.5. 新しいブラウザはプラグインを利用できる

ブラウザの選択肢は多数ありますが、現時点で Chrome と Firefox が一番人気が高いブラウザです。また、Chrome と Firefox の便利な機能が、プラグインを活用できることです。先に書いたとおり、プラグインを利用して、マルウェアをブロックすることができます。

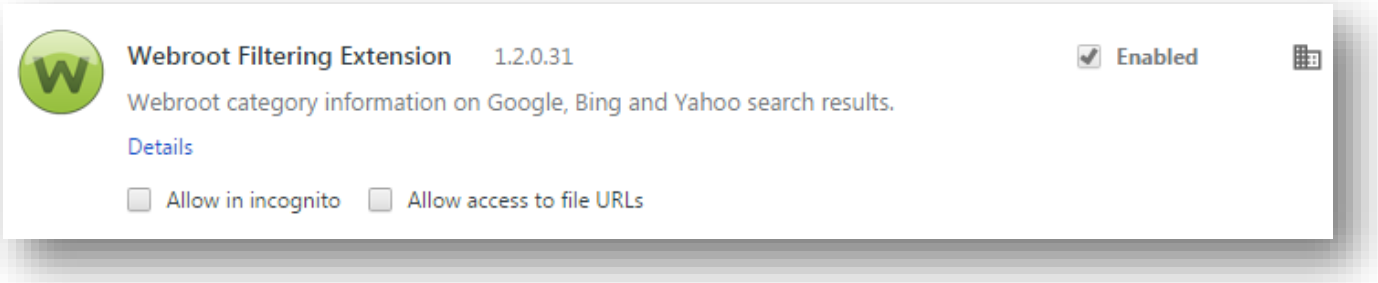
便利なブラウザプラグイン種類：

» アドブロッカー
» スクリプトブロッカー
» ウェブフィルター

多くのウェブサイトはオンライン上で生き残るために広告が必要ですが、しかし人気のあるウェブサイト（例えば、年間で 100 万人以上の訪問者がある）の多くがウェブサイト上のサードパーティホストされた広告経由でユーザをマルウェア感染させています。これが「マルバタイジング」です。最近、アメリカ国内の人気が高いニュースサイトのいくつかがハイジャック被害に遭い、ある日曜日に訪問したユーザ全員にマルバタイジング感染してしまったこともありました。アドブロッカーをインストールし、ユーザ情報を入力しないまま利用したとしても、IT 知識が低いユーザによる感染を止めることに効果があります。

スクリプトブロッカーは、ウェブサイト上での Java スクリプトの稼働を止める事ができます（Java スクリプトの稼働を許可することも可能）。これはユーザ側でテクニカル知識が必要であるため、全てのユーザには推奨できません。多くのウェブサイトではFlashとJavaプラグインを利用しており、もしユーザがその状況をわからなければ、社内でITサポートへの要請をしてしまうかもしれません。

ウェブフィルターは、一般的に多くインストールされているアンチウイルス製品であり、脅威に対する最前線になることもあります。ユーザが閲覧する前にウェブサイトをスキャンし、脅威の実行をブロックすることができます。



Chrome* にインストールされた *Webroot Filtering Extension

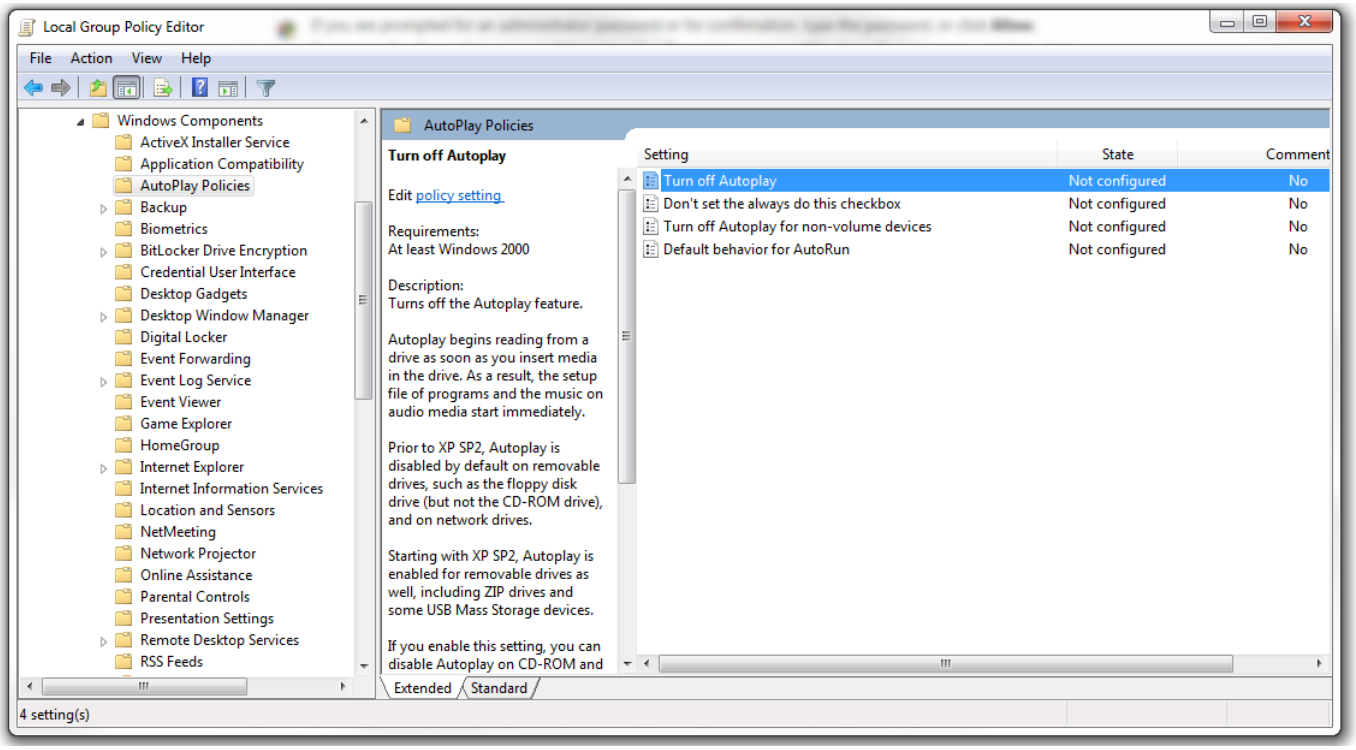
ウェブルートフィルタはウェブサイトのレピュテーションを確認し、もしサイトが安全でなければ、ユーザに警告します。

6. オートランを無効にする

オートランは便利な機能でありますが、マルウェアはこの機能を悪用し、企業環境の中に自身を拡散していきます。オートランは Local Group Policy Editor を利用して無効にすることができます。（これは USB ドライブの機能には影響しません）

- **Start** をクリックして、**gpedit.msc** を入力。**Enter** キーを押す
- **Computer Configuration** の中から、 **Administrative Templates** を展開、**Windows Components** を展開、そして **Autoplay Policies** を選択
- **Details** の中から、**Turn off Autoplay** をダブルクリック

» **Enabled** を選択し、**Turn off Autoplay** の中から **all drives** を選択し、全てのドライブでのオートランを無効化



オートプレイを無効にする

7. Policy Editor を利用してパスをブロックする

ポリシーは様々な目的に活用できる強力なツールです。ユーザによる特定のソフトウェアのインストールや稼働を止めることができるほか、様々な管理を行うこともできます。下の例はローカルポリシーを利用していますが、これらはネットワークグループポリシーにも適用することができます。このガイドでは簡単な紹介しかできませんが、もしより詳細な情報が必要であれば、このマイクロソフトのリンクを参照してください：

https://technet.microsoft.com/en-us/library/bb457006.aspx

ポリシーはグループで設定することができるので、グループ毎に合わせた最適なポリシーを設定することができます。もしより多くのアクセスが必要であったり、またはテクニカル知識が高いグループがいる場合には、制限が低いポリシーを設定することも可能です。

尚、これらのポリシーをまずミッションクリティカルではないテスト用 PC でテストすることをお薦めします。

便利なポリシー例：

» Temp 内の実行ファイルを開くのをブロック
» VSS サービスの変更をブロック
» Temp＋appdata の実行ファイルを開くのをブロック
» スタートアップエントリの生成をブロック

現実として、次のファイル形式は次のディレクトリでは稼働するべきではありません：

» SCR、PIF、CPL ファイルを users temp、program data、または desktop ディレクトリ

上記に対するポリシーは比較的安全です。ランサムウェアは、ポータブル実行（PE）ファイルとしてあまり認識されていない「SCR」ファイルを悪用することがあります。また追加で、マルウェアドロッパーがよく侵入するコモンパスの PE ファイル形式をブロックするポリシーを作成することもできます。

» EXE、DLL、SYS、FON、EFI、OCX、 SCR
» Temp、Appdata、ProgramData など

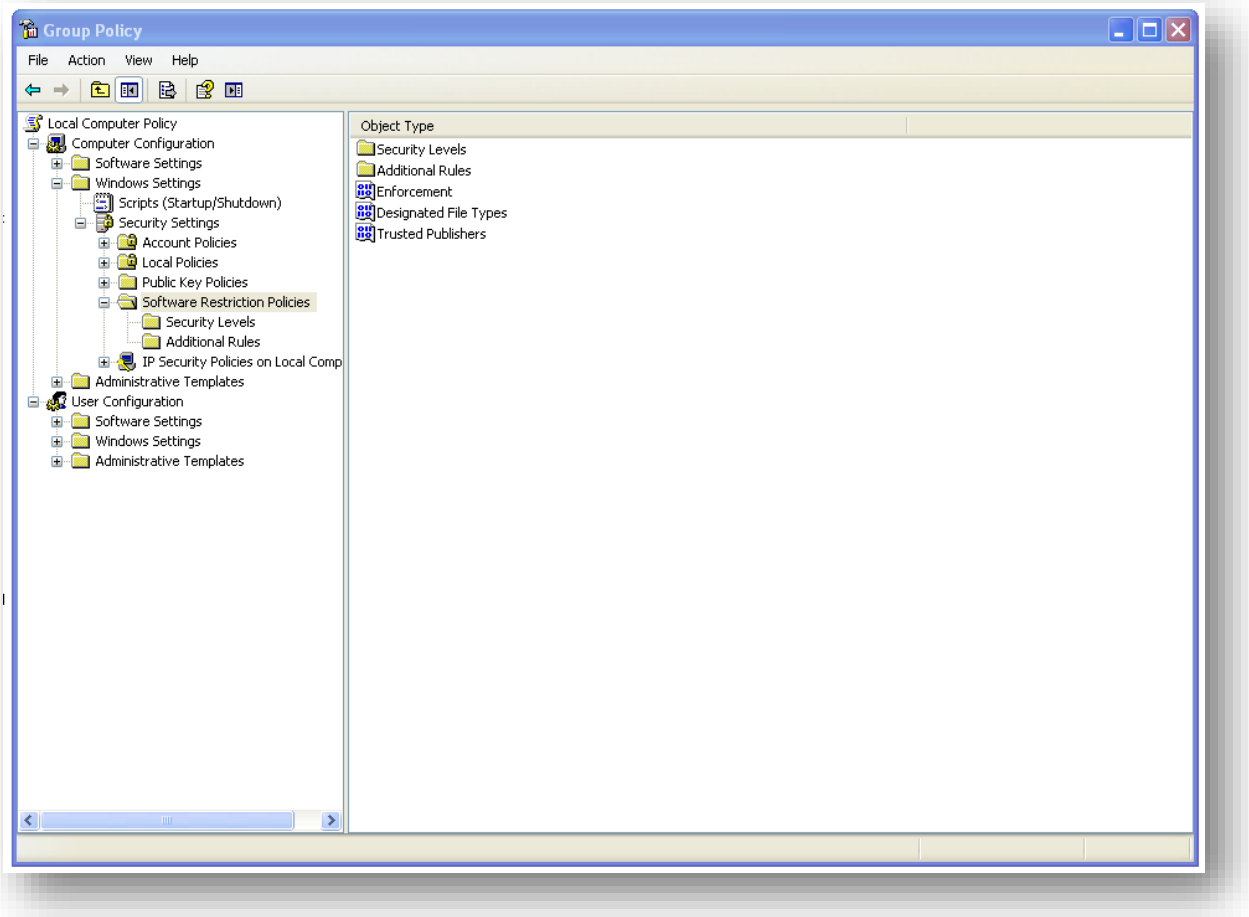
次のプロセスで Local Group Policy Editor を開くことができます。コマンドラインから Local Group Policy Editor を開くには：

» **Start** をクリックし, **msc** を **Start Search** 欄に入力。エンターキーを押す。

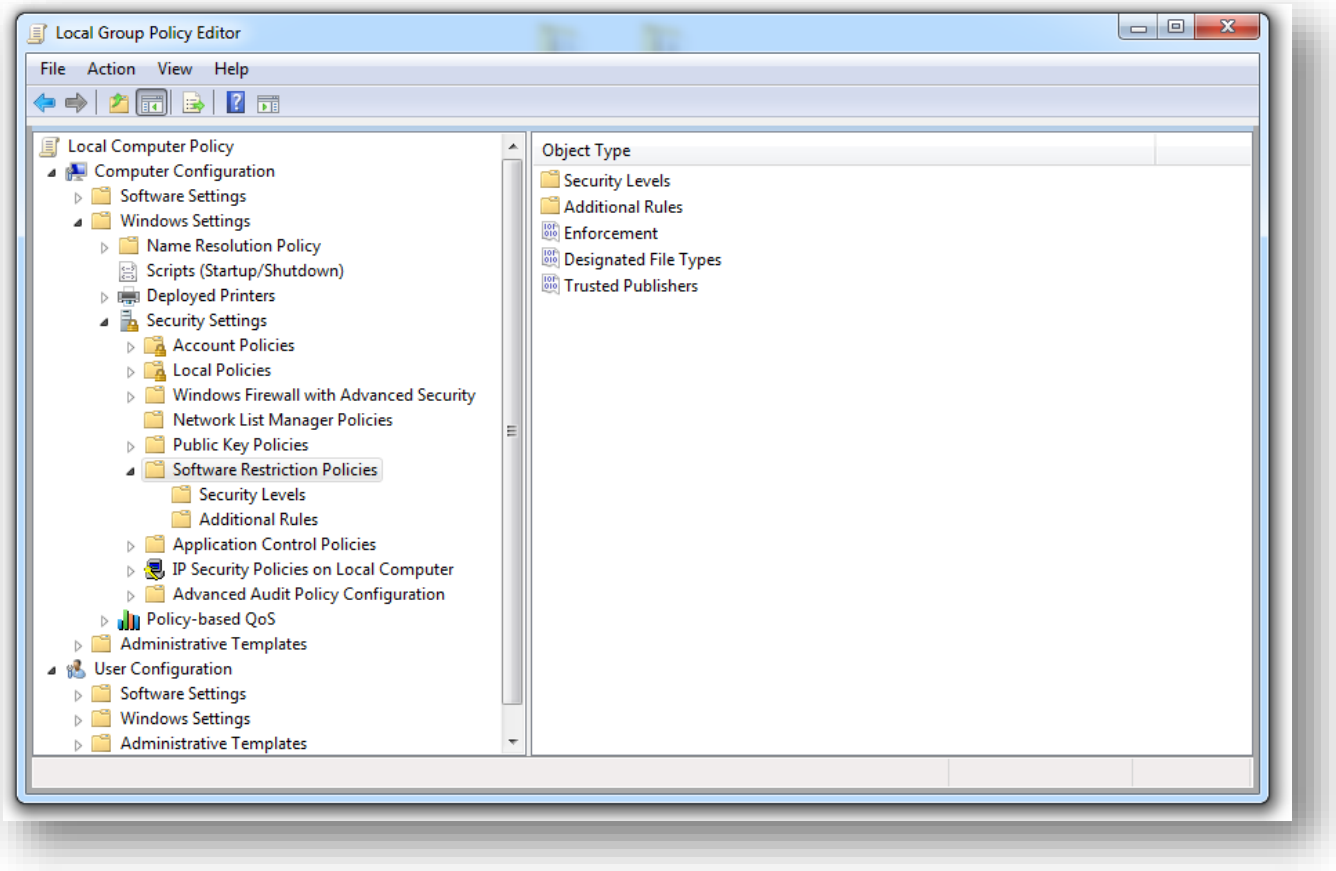
MMC スナップインとして、 Local Group Policy Editor を開くには：

1. **Start** をクリックし, **Start Search** 欄をクリック。**mmc** を入力後、エンターキーを押す。
2. **File** メニューから、**Add/Remove Snap-in** を選択
3. **Add or Remove Snap-ins** のダイアログボックスから、**Group Policy Object Editor** を選択し、**Add** をクリックする
4. **Select Group Policy Object** ダイアログボックスから、**Browse** を選択
5. **This Computer** をクリックし、Local Group Policy Object を編集する、または **Users を選択し、** Administrator、Non-Administrator、またはユーザ別の Local Group Policy オブジェクトを編集する

6. **Finish** で終了する



グループポリシーへのアクセス



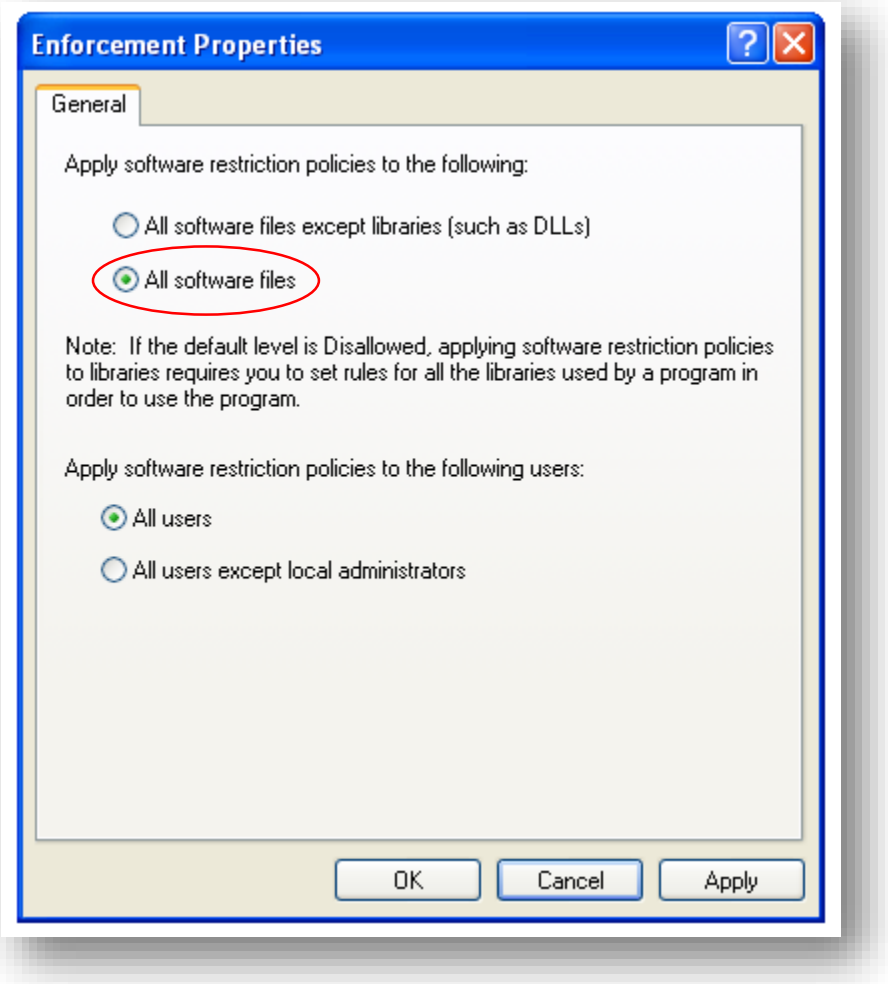
ローカルグループポリシーエディター

8. ポリシーをテストする

ポリシーを作成するには、ツリー構成を展開し、次を行います：

» **Computer Configuration -> Windows Settings -> Security Settings -> Software Restriction Policies**

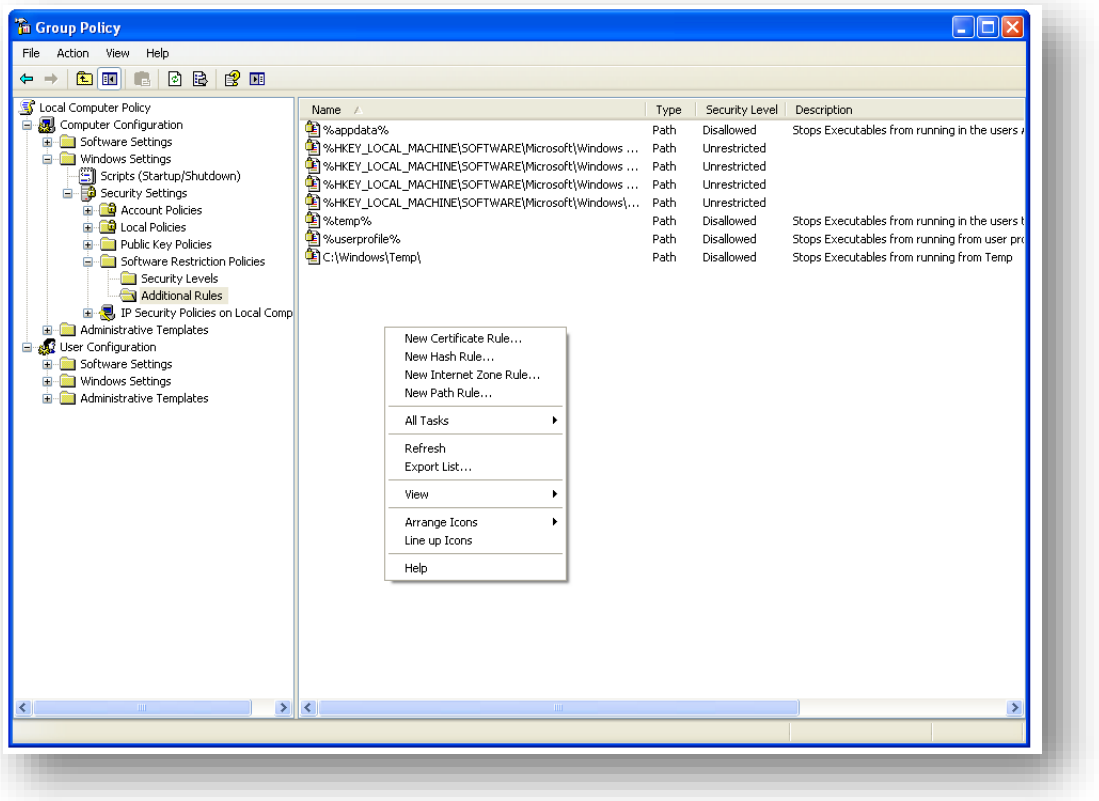
まず Enforcement Properties の設定を変更します。「All software files except libraries」から「All software files」へ変更します。



Enforcement Properties の設定を変更する

9. ポリシーを作成する

ポリシーを作成するには、Policy ウィンドウの右側を右クリックして、「New Path Rule」を選択



ポリシーを作成する

新しいルールを作成できる小さいウィンドウが開きます。このウィンドウ内で、特定のフォルダを参照したり、一般的な Windows のワイルドカードパスを利用することができます。下の例では、C:¥Windows¥Temp で実行ファイルの起動をブロックするポリシーを作成しています。

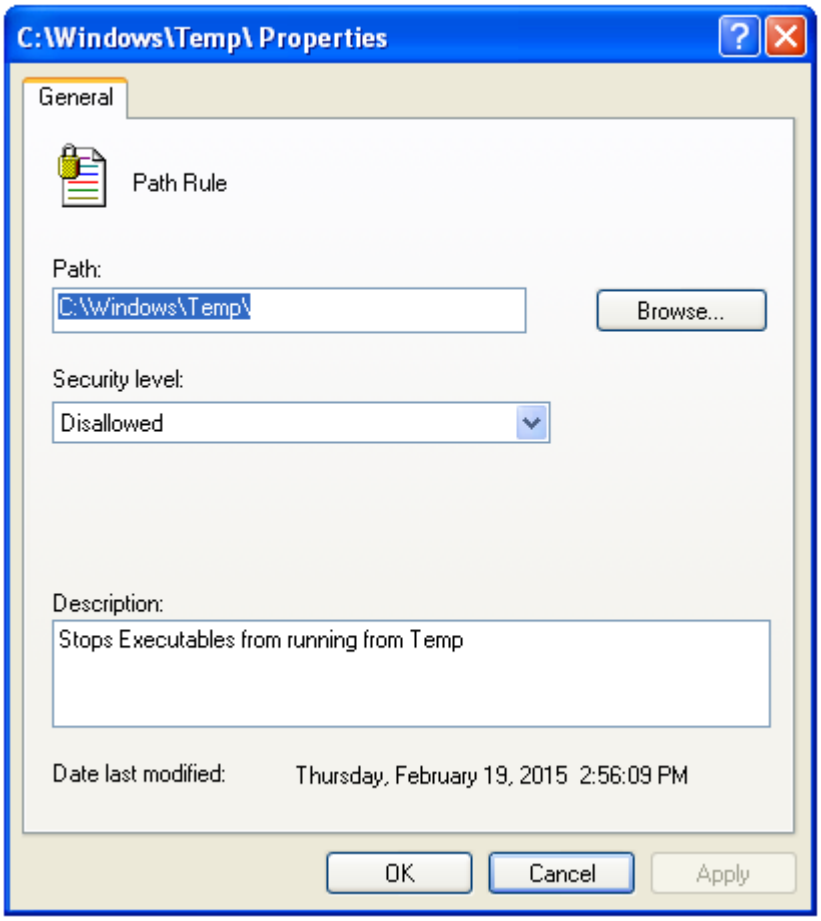
これは Windows のテンポラリフォルダ（多くのプログラムやインストーラーで利用）ですので、このポリシーを適用することによって、いくつかの問題が発生することが予測できます。しかし、デモンストレーションのためには最適なフォルダです。定義するパスではクリエイティブに考えることもできます。（下のスクリーンショットを参照）

尚、この場合では、デスクトップ上からプログラムを起動することができなくなるので、注意が必要です。

1. %appdata%
2. %temp%
3. %userprofile%

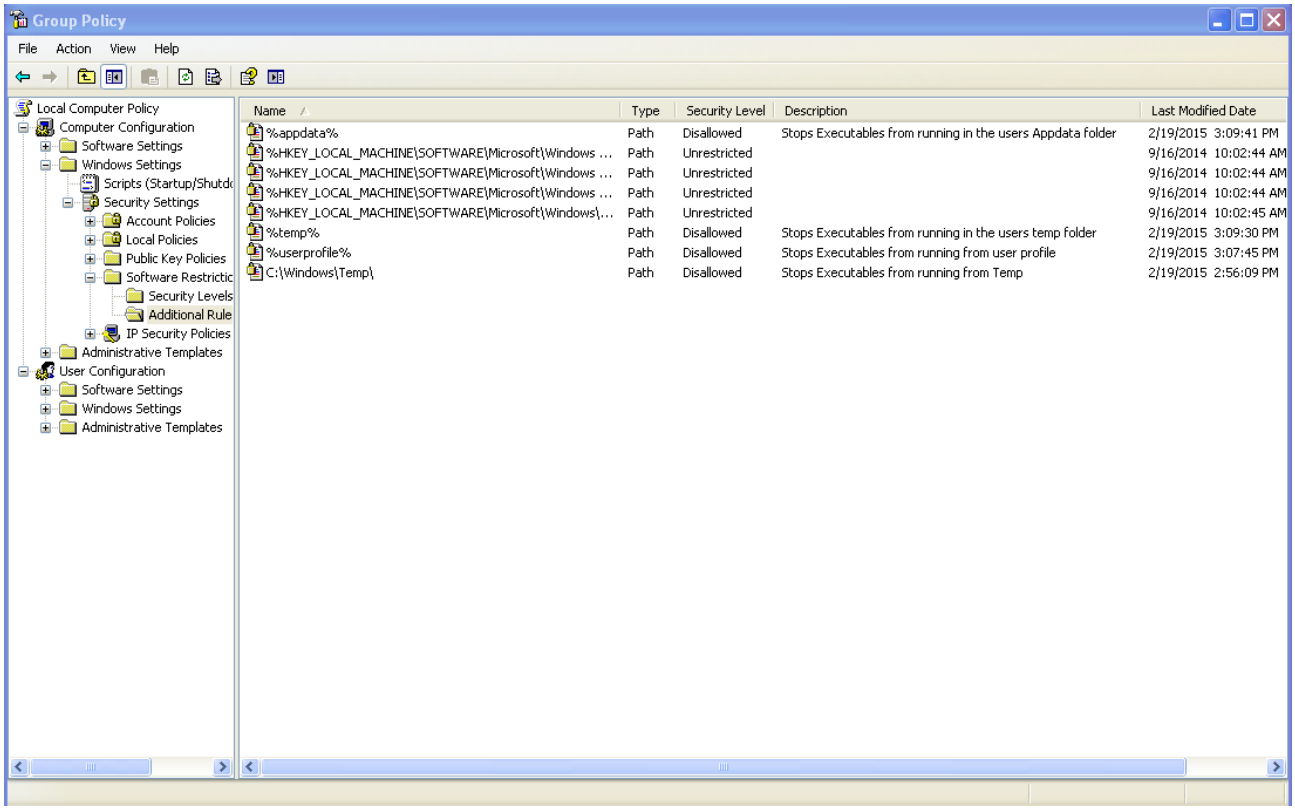
4. %localappdata%
5. %programdata%
6. C:¥Windows¥Temp

また、いくつかの正規プログラムやアップデータがユーザの appdata から起動することがあります。もし何かの理由で正規ソフトウェアが通常の Program Files フォルダではなく、appdata フォルダから起動するということが分かっているのであれば、そのソフトウェアをルールから除外する必要があります。除外しない場合は、起動しません。



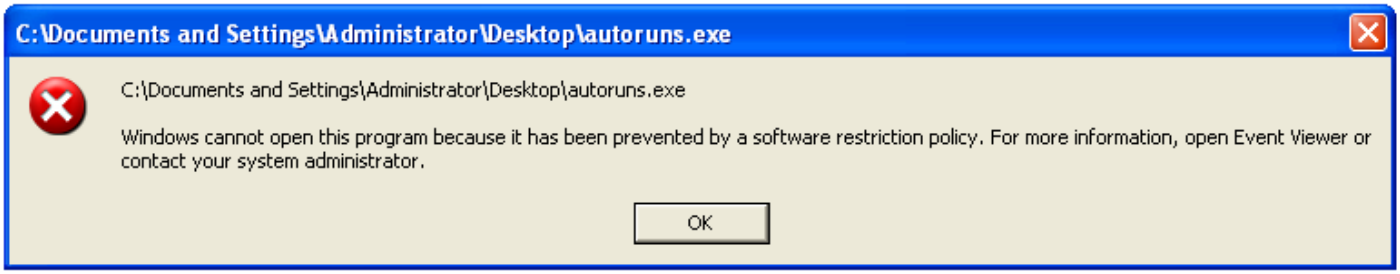
Temp フォルダ内の実行ファイルを止める

下の例では、次の名前/パスの中で実行ファイルの起動をブロックしているポリシーをいくつか作成しています。



パスによる実行ファイルのブロック

下のスクリーンショットでは、ローカル管理者のデスクトップにある実行ファイルを起動しようとしています。ご覧の通り、Windows から自動的にポップアップ画面で警告が表示され、プログラムは起動しません。制限されていないパスにファイルを移動した場合、プログラムは問題なく起動します。

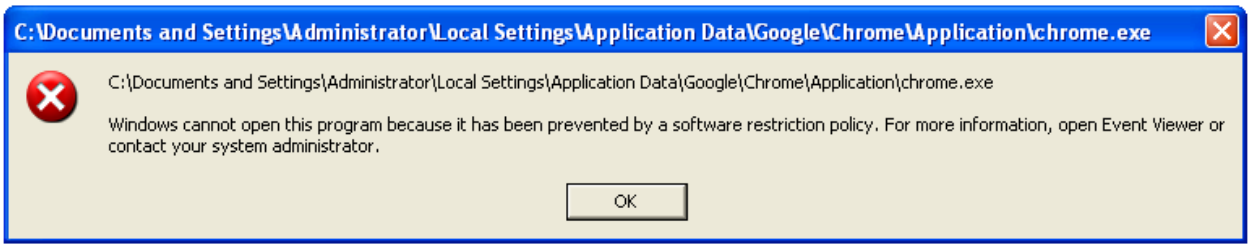


実行ファイルブロックの警告

10.ブロックされたプログラムの問題を修正する

ローカルユーザの appdata と temp フォルダにポリシーを適用すると、いくつかのプログラムが正しく起動しなくなります。

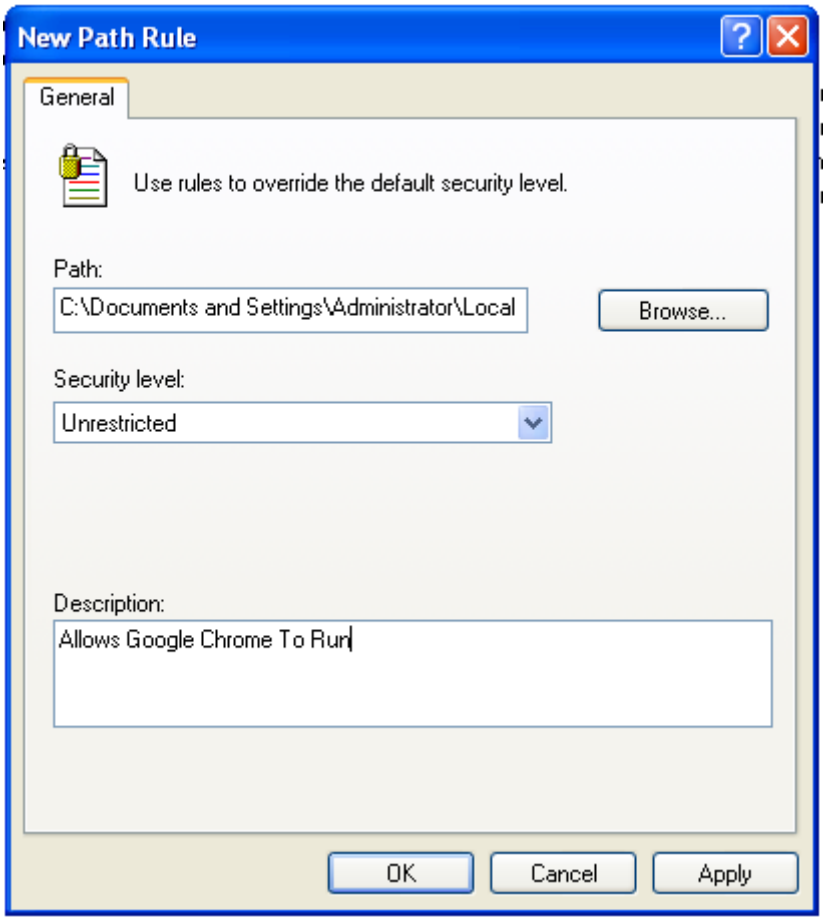
例えば、人気が高い Chrome ブラウザは、PC 上で起動できなくなります。これはユーザのプロファイルフォルダ内の実行ファイルをブロックするポリシーが原因です。しかし、Mozilla Firefox は、C:¥Program Files¥Mozilla¥にインストールされているので、問題なく起動します。また、Internet Explorer もプログラムファイルのパス内にあるため、開くことができます。



制限が厳しすぎるポリシーの例

このポリシーはそんなに強いものではありません。次の例では、このポリシーを無効にして、より強調されたパスとファイルのポリシーを生成しています。

まずそれぞれのパスとフィあるポリシールールを次のように設定します。



パスとファイルのポリシールール

11.Volume Shadow コピーサービスへのアクセスをブロックする

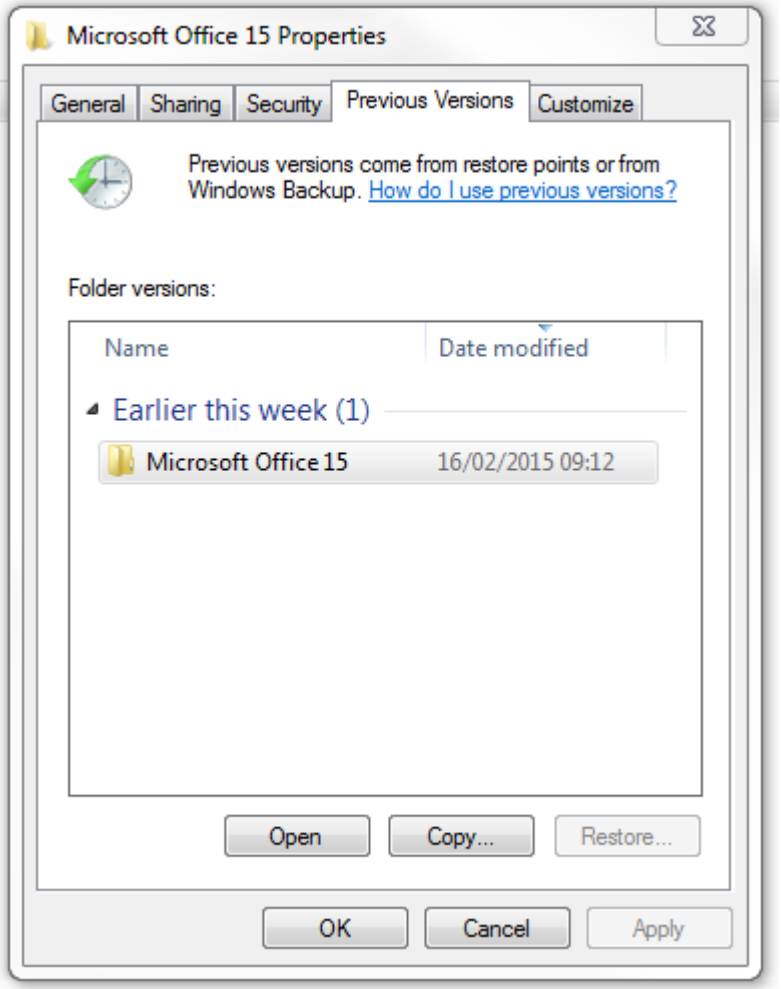
Windows XP 以上では、Windows が VSS コピーサービスを活用して、ファイルのローカルコピーを生成します。

次のパスにあります：

C:¥Windows¥System32¥VSSAdmin.exe

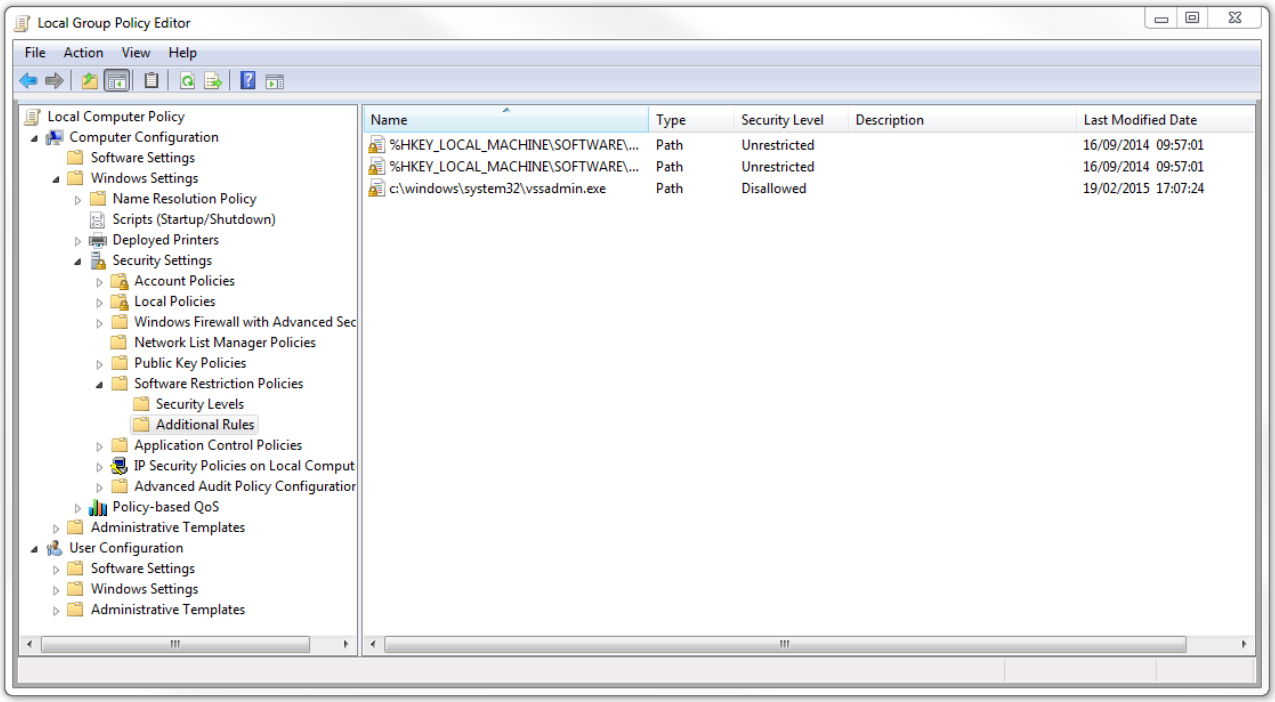
古いバージョンの CryptoLocker は VSS コピーを止めることなく、また削除することもありませんでした。その結果、データを復旧することができました。データ復旧の人気ツールの一つが Shadow Explorer でしたが、Windows の機能を使って、データを復旧することも可能でした。尚、VSS コピはローカルドライブ（通常だと C:¥ドライブ）のみ適用されています。

VSS サービスは現実的には Vista 以上でのみ有効で、暗号化されたファイルを救済する最後の手段です。



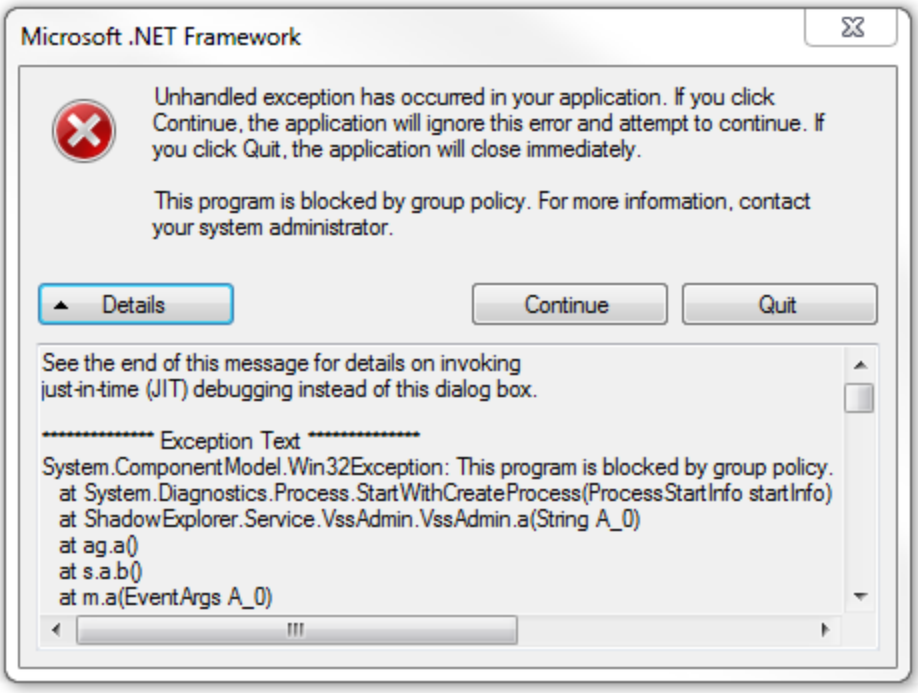
重要なノート：VSS はバックアップの替わりではありません。保護するのはローカルドライブのみです。

サービスへのアクセスをロックすることによって、CryptoLocker のようなランサムウェアがバックアップファイルを削除しようとすることを止めることができます。ポリシーを作成し、VSSAdmin の実行ファイルを対象にします。



***VSSadmin* をローカルグループポリシーエディターでブロックする**

このサービスにアクセスまたは止めようとする行動をブロックします。



***VSSAdmin* をブロックするポリシー警告**

12.Windows Script Hosting の無効化 - VBS スクリプトをブロックする

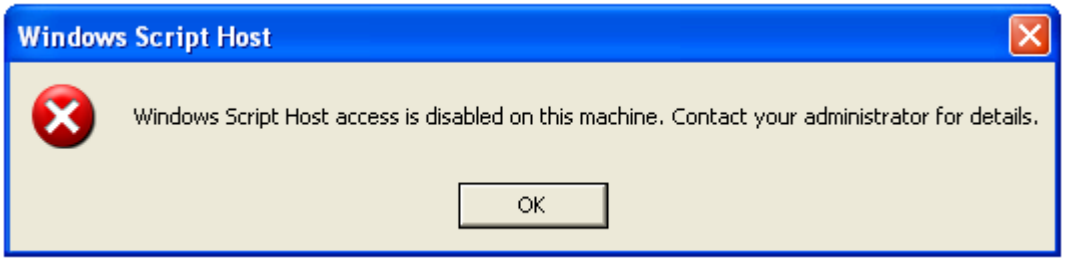
VBS スクリプトはマルウェア開発者によって悪用され、環境内での破壊活動を起こすか、またはより多くの先進的なマルウェアをダウンロードするプロセスを起動することに使われます。2000 年代の前半には、ILOVEYOU VBS マルウェアが流行り、大きな被害を残しました。現在では、多くの VBS スクリプトはフォルダを隠したり、ファイルを移動したりすることに悪用されています。しかし、VBS ファイルが起動する Windows Script Host エンジンを無効にすることによって、VBS スクリプトを無効化することができます。

警告：もし企業でログインスクリプトを利用している場合、そのスクリプトが起動できなくなります。尚、ポリシーを利用して、*VBS* ファイルの利用を停止することもできます。（項目 *7* でのリンクを参照ください）

次の二つのレジストリのエントリが、Windows Script Hosting Engine Executable の実行をブロックされるために使われる二つのエントリです。(Wcscript.exe)

- » HKEY_CURRENT_USER¥Software¥Microsoft¥Windows Script Host¥Settings¥Enabled
- » HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows Script Host¥Settings¥Enabled

これらのレジストリキーが有効化された後に、VBS ファイルを実行しようとすると、次のエラーメッセージが表示されます：



Windows Script Hosting ブロックの警告

これらをブロックするには簡単な方法があります。次のレジストリキーをダウンロードして利用してください。もしスクリプトを起動する必要があれば、ポリシーエディターでよりカスタマイズされたバージョンを作成することもできます。

http://download.webroot.com/VBSDisable.zip

http://download.webroot.com/VBSEnable.zip

13.メールサーバで EXE ファイルをフィルタリングする

もしメールゲートウェイで、ファイル拡張子でのフィルタリングが可能であれば、EXE ファイルが添付されているメールを拒否する、または二つの拡張子があるファイルが添付されているメールを拒否などのルールを設定すれば最適です。二つ目の拡張子が実行ファイル（“*.*.EXE” ファイル）となる形式が、ランサムウェアでは一般的です。

14.RDP を無効にする

CryptoLocker や Filecoder マルウェアは、攻撃対象の PC に Remote Desktop Protocol（RDP）を悪用してアクセスしようとします。RDP は、Windows のツールでリモート環境からのデスクトップへのアクセスを提供しています。もし RDP 機能が不要であれば、RDP を無効にすることによって、Filecoder や他の RDP 脆弱性を狙ったマルウェアから PC を保護することができます。Windows 7 以上のバージョンでは、RDP は標準で無効になっていますが、念のために保護する OS の設定を確認することをお勧めします。

15.ユーザ教育

セキュリティのリンクで一番弱いのは、ユーザである「人的ファイアウォール」だとよく言われます。ユーザのセキュリティ教育は重要であり、自分の都合のいい時間帯に行えるオンライン教育が増える中で、これらのツールを活用してユーザにオフィスでの脅威、または自宅でインターネットを利用する際のリスクなどを教育しない言い訳はもうできません。

これらの簡単なことを行うだけで、ユーザにより安全な環境を提供することができます：

15.1. 可能であれば、二段階認証を行う

ネットワークへのアクセスで活用するほかに、ユーザがオフィスから VPN 経由のリモート環境で働く場合にも活用しましょう。二段階認証でパスワードリセットとウェブベースのビジネスツールへのアクセスを提供しましょう。

15.2. セキュアパスワードの利用を強制する

デスクトップおよびその他のアプリケーションへのログインではまだパスワード認証に頼っています。強制的にストロングパスワードのルールを作り、そしてユーザに簡単なトレーニングを行

い、簡単で覚えやすい強力なパスワードを作ることによって、よりセキュアで安全な職場を作り上げることができます。

15.3. ジャンクのフィルタリングを設定しメールでのクリックスルーを制限する

ユーザがまず騙されて感染の被害にあってしまう最も多い手法が、フィッシングとスピアフィッシングです。ユーザに対してリンクを容易にクリックしない（知っている人、信頼している人から送信されるように見えた場合でも）と教育するのは非常に有効です。また、リンクつきのメールを検疫する、またはリンクを無効にするなどが、唯一、強力なスピアフィッシング攻撃をブロックできる方法かもしれません。

16.もし感染してしまったら

もし企業が残念なことにマルウェアに感染してしまった場合、次の対策を講じることをお薦めします。

16.1. 感染した PC を至急ネットワークから切断し、感染の拡大を止める

16.2. 感染の原因を把握できるまで、PC のリイメージなどを行わない

16.3. エンドポイント・セキュリティ・ベンダーのサポートスタッフに連絡し、感染のクリーンナップを開始する。ベンダーのサポートには、クリーンアップの支援、感染が完全に修復できているかを確認してもらう。

16.4. ベンダーのサポートスタッフと、なにがどのように感染したかを追求する。

16.5. ユーザのデータが暗号化されたかチェックする。これもできるだけ早急に行う

16.6. 他の社員に警告を出し、これが標的型攻撃だったか、または脅威ベクトルについて、適切な情報を伝える。

17.結論

このガイドは究極のリファレンスとしての位置づけが目標ではありません。ウェブルートが今まで経験した中から得た知見によって、ランサムウェアの被害に遭わないように、どのような行動が最適かを紹介したドキュメントです。身代金要求はひどい犯罪行為であり、お金を払うことは犯罪者を喜ばせ、ユーザを悲しめるだけです。

簡単なステップをいくつか行うだけで、組織をこのような攻撃から保護し、データを復旧してもらうために犯罪者に頼り、会社の生産性を犯罪者に元に戻してもらうという不要な行為が不要になるのです。

18.詳細情報

18.1. ランサムウェアの詳細な情報は、ICIT は発行した ICIT のランサムウェアレポート「2016 Will Be The Year Ransomware Holds America Hostage」に掲載されています。PDF はこちらからダウンロードできます:
http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report.pdf

18.2. このドキュメントは、ウェブルートのブログと Threat Research and Support チームが執筆した記事からまとめています。このガイドにご協力いただき、感謝します。関連するウェブルートの最新ブログ記事（英語）は、次の URL をご参照ください：

KeRanger: http://www.webroot.com/blog/2016/03/07/18611/
Locky: http://www.webroot.com/blog/2016/02/22/locky-ransomware/
Padcrypt: http://www.webroot.com/blog/2016/02/18/new-ransomware-padcrypt-first-live-chat-support/
RaaS Ransomware As A Service: http://www.webroot.com/blog/2015/07/28/encryptor-raas-ransomware-as-a-service/
TeslaCrypt: http://www.webroot.com/blog/2015/03/12/teslacrypt-encrypting-ransomware-that-now-grabs-your-games/
Critroni: http://www.webroot.com/blog/2014/07/25/critroni-new-encrypting-ransomware/
A Typical Macro Infection: http://www.webroot.com/blog/2016/01/14/a-look-at-a-typical-macro-infection/
Best practices for securing your environment against CryptoLocker and ransomware https://community.webroot.com/t5/Webroot-Education/Best-practices-for-securing-your-environment-against/ta-p/191172