UnHackMe Corporative Edition について

UnHackMe は強力なルートキット検出・駆除ツールです。

ルートキットとは、ハッカーがその侵入を隠して、コンピュータやネットワークに対する管理者レベルのアクセス権限を得るために使用する一連のプログラムです。ハッカーがコンピュータにルートキットをインストールする手段としては、ユーザの操作を利用する、既知の脆弱性を悪用する、パスワードを解読する、などが挙げられます。ルートキットが一度インストールされると、バックドア技術によって、ハッカーがコンピュータを完全に支配できるようになってしまいます。ルートキットは、ユーザによって発見されないように、自身のファイル、レジストリ キー、プロセス名、ネットワーク接続などを隠しています。

UnHackMe Corporative Edition を使用すると、ローカル ネットワーク上のすべてのコンピュータを保護することができます。

利点

1)インストール/更新が簡単 – 通常のインストールのほかにも、サイレント インストールにも対応しています。

2)完全アラート – ルートキットが検出された場合、電子メール、ネットワーク メッセンジャ、または Web スクリプトを使用して、システム管理者に通知されます。

3)自動駆除 – ルートキットを自動的に駆除したり、コンピュータをネットワークから切断したりして、ルートキットの伝播を防止することができます。

4)操作がシンプル – 簡単で使いやすいインターフェイスが採用されています。

コンピュータを安全に保護するためにも、UnHackMe をぜひお試しください。

システム要件

UnHackMe を使用するには、以下の要件を満たしている必要があります。

· コンピュータに Windows NT4/2000/XP/2003 (32 ビットまたは 64 ビット) 以上のオペレーティングシステムがインストールされている必要があります。

· UnHackMe を使用するには、管理者権限が必要になります。

· UnHackMe のインストールには、約 4MB のハード ディスク空き容量が必要です。

· UnHackMe のメモリ要件は、オペレーティング システム (Windows NT4/2000/XP) のメモリ要件と同様です。

起動

1. UnHackMeCorporative.exe を実行します。
2. [共通パラメータ] タブを開きます。
3. [チェック間隔] を分および秒で設定します。
4. UnHackMe を非表示モードで実行するには、[アイコンを隠す] チェック ボックスをオンにします。
   UnHackMe がバックグラウンドで実行され、システム トレイの UnHackMe アイコンからはプログラムを終了できなくなります。
   ただし、タスク マネージャから UnHackMe モニタ (hackmon.exe) を終了することは可能です。
5. [除外リスト] セクションで [開く] をクリックして、必要に応じて、誤検出アイテムを設定します。
   除外リスト内のアイテムは UnHackMe の検出対象から除外されます。

ルートキット検出時の処理

[対処] タブを開きます。

1. 検出されたルートキットのレコードがアプリケーション ジャーナルに追加されるようにするには、[イベント ログに書き込む] チェック ボックスをオンにします。
2. ネットワーク接続を無効にして、ルートキットの伝播を防止するには、[ネットワークをロック] チェック ボックスをオンにします。
   ネットワーク接続を再び有効にするには、[ネットワーク接続] ウィンドウ ([コントロール パネル] -> [ネットワーク接続]) を開き、対象の接続の右クリック メニューで [有効にする] をクリックする必要があります。
3. Web フォームにログを送信するには、[Web フォームに送信] チェック ボックスをオンにします。
   この場合、Web サーバ上に特別な CGI スクリプトを設定する必要があります。
   [Web 送信 (POST)] タブを参照してください。
4. ローカル ネットワーク管理者にアラートを送信するには、[管理者にアラートを送信] チェック ボックスをオンにします。
   この場合、[管理者連絡先] タブで管理者のコンピュータを指定する必要があります。
   なお、メッセージの送信には "net send" が使用されます。
5. アラートを電子メールで送信するには、[アラートをメールで送信] チェック ボックスをオンにします。
   この場合、[管理者連絡先] タブで管理者の電子メール アドレスを指定する必要があります。
6. 特定のプログラムを実行するには、[プログラムを実行] チェック ボックスをオンにして、編集ボックスにプログラムのフルパスと名前を入力します。
7. ルートキットを自動的に停止するには、[ルートキットを自動的に停止] チェック ボックスをオンにします。
   ルートキットを停止する際に確認メッセージは表示されませんので、このオプションは慎重に使用してください。また、このオプションを有効にするには、再起動が必要になります。

[OK] をクリックして、設定内容を保存し、UnHackMe Corporative を終了します。
UnHackMe Corporatuve フォルダに "corp.ini" ファイルが作成されます。

コンピュータへの UnHackMe のインストール

1. 以下の Web サイトから UnHackMe の最新バージョンをダウンロードします。
http://www.unhackme.com (英語)
http://www.shareedge.com (日本語)
2. コンピュータに UnHackMe をインストールします。
デフォルトのインストール先フォルダは "C:¥Program Files¥UnHackMe" です。このユーザ ガイドでは、このフォルダを UnHackMe フォルダと呼んでいます。
3. すべてのユーザが共通のネットワーク ドライブにアクセスできる場合、そのドライブ上に UnHackMe corp.ini 用のフォルダを作成します。管理者にはフル アクセス権限、管理者以外のユーザには読み取り権限を設定します。作成したフォルダに "corp.ini" ファイルをコピーします。
たとえば、"s:¥programs¥unhackme" のようなマップ ドライブを指定し、
"¥¥server¥programs¥unhackme" のような UNC パスは使用しません。
共通のドライブを使用していない場合は、"corp.ini" を UnHackMe フォルダにコピーします。
4. Greatis Software またはその販売代理店 (日本国内は nextEDGE Technology) から受け取った **"aspr_keys.ini" ファイル (ロック解除コード)** を UnHackMe フォルダにコピーします。
5. "Compil32.exe" (インストーラ作成用の **Inno Setup** コンパイラ) を実行します。
6. [File (ファイル)] メニューの [Open (開く)] をクリックして、"**unhackmecorp.iss**" ファイルを探します。

7. 必要に応じて、ファイル内のパス名を変更します。
8. ネットワーク ドライブ上の "corp.ini" を使用する場合、ファイルの末尾に移動して、[Registy] セクションの以下の行を探します。
Root: HKCU; Subkey: Software¥Greatis¥Unhackme; ValueType: string; ValueName: "UnHackMeCorp"; ValueData: "{app}¥corp.ini"
9. "ValueData" をネットワーク パスに変更します。
コンピュータのすべてのユーザで UnHackMe を使用する場合、Root を "HKLM" に設定します。
10. F9 キーを押して、インストーラを作成します。

サイレント インストール

UnHackMe は、ログオン スクリプトまたは SMS ソフトウェアを使用して、自動的にインストール (サイレント インストール) することができます。使用可能なコマンドライン オプションは以下のとおりです。
/SILENT、/VERYSILENT - "/SILENT" を使用した場合、ウィザードと背景ウィンドウは表示されなくなりますが、インストール進捗ウィンドウは表示されます。"/VERYSILENT" を使用した場合、インストール進捗ウィンドウも表示されなくなります。他に特別なオプションを使用していなければ、インストール中のエラー メッセージ、およびスタートアップ プロンプトは表示されます (DisableStartupPrompt または "/SP-" コマンドライン オプションで無効にしていない場合)。
/SP- - セットアップの最初に表示される "このセットアップ プログラムは ... をインストールします。続行しますか?" というようなプロンプトを無効にします。DisableStartupPrompt [Setup] セクション ディレクティブを "yes" に設定している場合、このオプションを使用しても効果はありません。
/SUPPRESSMSGBOXES - メッセージ ボックスが表示されなくなります。"/SILENT" または "/VERYSILENT" と組み合わせて使用した場合にのみ効果があります。
/NOCANCEL - [キャンセル] ボタンおよび [×(閉じる)] ボタンを無効にします。ユーザはインストール処理をキャンセルできなくなります。"/SILENT" または "/VERYSILENT" と組み合わせて使用すると便利です。
/NORESTART - 必要に場合でも再起動されなくなります。

例
unhackmecorp300.exe /SP- /VERYSILENT /SUPPRESSMSGBOXES /NOCANCEL

新機能

バージョン 3.0
- UnHackMe Corporative Edition の最初のパブリック リリース

テクニカル サポート

プログラムの操作上何らかの問題 (バグ) を発見した場合は、以下のサポート センターまでご連絡ください。
オンライン フォーム
http://www.greatis.com/support (英語)
https://www.shareedge.com/cs/ (日本語)
電子メール
support@greatis.com または ateam@greatis.com (英語)

contact@nextEDGEtech.com（日本語）
書面でのご連絡の際は、氏名と電子メール アドレスを明記してください。
問題の再現手順は可能な限り詳しくご報告ください。ご報告いただいた内容の調査が完了しましたら、推奨する解決方法をご提示させていただきます。