X-Cleaner コマンド ライン ユーザ ガイド

概要

X-Cleaner コマンド ライン スキャナは、それ自身が実行可能であり、SMS などの既存のデプロイメント システムを利用している企業に対して最適なソリューションを提供します。また、デプロイメント サーバやクライアントで追加のエージェントを実行することを避けたいと考えている企業にとっても有効です。X-Cleaner コマンド ライン バージョンには、非常に柔軟性に優れたレポート オプションが用意されています。

システム要件

- XP Professional/Home、2000、2000 Server、2003 Server、Windows 98、Windows 98 SE
- 128 MB RAM
- 2MB の空きディスク容量
- TCP/IP の利用可能なネットワーク
- クライアント側での必要最小限のリソース: スキャン環境に応じて、10～15MB のメモリ、2～20% の CPU 負荷

機能

- エージェント不要 ― サーバやクライアントでエージェントを実行する必要がないため、システム リソースを最小限に抑えられ、生産性の向上を図れます。
- インストール不要 ― スキャナ自身が実行可能形式であるため、インストール作業は必要ありません。
- 設定不要 ― 中央のサーバからインストールなしで直接実行することができます。
- クイック スキャン ― X-Cleaner では、隠れたスパイウェアを検出するための非常に高速なスキャン技術を採用しています。
- ディープ スキャン – X-Cleaner には、個々のファイルをくまなくスキャンすることでクイック スキャンでは検出できないスパイウェアを検出するための機能も備わっています。
- レポート機能 – X-Cleaner には、検出されたスパイウェアの情報を詳細分析するためのレポート機能が備わっています。レポートには、ファイル、CLSID、ディレクトリ位置、およびレジストリ キーの情報が含まれます。このレポートは、XML、電子メール、HTTP Post などを利用して、任意の Web サーバに送信することができます。

X-Cleaner コマンド ライン スキャナのセットアップ

1. パッケージの内容を解凍します。パッケージには、以下の 3 つのファイルが含まれています。
    a. xcl_cmd.exe (X-Cleaner コマンド ライン スキャナ)
    b. xc_sigs.dat (シグネチャ ファイル)
    c. settings.ini (レポート機能用の設定ファイル)
2. 簡単な設定方法については、本ユーザ ガイドの「レポートとスキャン オプションの設定」を参照してください。

推奨する利用方法

中央に設置

1. 設置先とするファイル サーバ上に読み取り専用の共有領域を作成します。
2. 作成した共有領域にファイルをコピーします。

ログイン スクリプトを利用したスキャン

以下の Microsoft のドキュメントを参照してください。
通常のネットワーク セットアップの場合
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_CreateLogonScripts.asp

"Active Directory" セットアップの場合
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_assign_LScripts_user_AD.asp

共有領域を設定したサーバからコマンド ラインでスキャナを呼び出すには、以下を実行します。
\\<サーバ名>\<共有ディレクトリ名>\xcl_cmd.exe /autostart /reportonly /silent

スキャンのスケジュール

管理者は、Windows Job ファイルを管理者権限で作成し、そのファイルを基に、ログイン スクリプトやデプロイメント機能を利用してスキェンをスケジュールすることができます。
以下の Microsoft のドキュメントを参照してください。
http://windows.about.com/od/ customizationsforwindows/l/aa001022b.htm

http://www.microsoft.com/technet/prodtechnol/windows2000serv/maintain/featusability/tsksched.mspx

カスタム利用

X-Cleaner コマンド ラインは、既存のどんなデプロイメント システムとも統合することが可能です。これにより、管理者は豊富なコマンド ライン オプションを利用することができるようになります。詳細については、以下を参照してください。

レポートとスキャン オプションの設定

メモ:キーワードは、大文字と小文字を区別しません。また、"/" は、必要に応じて "-" で置き換えることができます。
/AUTOSTART (実行するには、このスイッチが必要です)
スキャンを自動的に開始し、停止します。
このオプションは "/UPDATE" を除くその他すべてのオプションと一緒に利用する必要があります。

/INOCULATE (推奨)

レジストリを検疫し、悪意のある既知の CLSID がインストールされるのを回避します。これは、再感染を回避するために最も有効な方法です。

/DEBUGLOG (推奨)
X-Cleaner コマンド ライン スキャナでは、ログを作成し、問題が発生した場合のトラブルシューティングに役立てることができます。

/DSCANHD (推奨)
すべてのローカル ドライブをファイル単位でディープ スキャンします。このオプションを利用すると、すべてのファイルを走査するため終了するまでに時間がかかります。しかし、これはディスク上のすべてのファイルを検査するため大変効果があります。このスキャンは、毎週実行することをお薦めします。

/NOREBOOT
X-Cleaner では、スパイウェアを完全除去するために再起動が必要になる場合があります。このスイッチでは、スパイウェアの除去後、再起動のための問い合わせをユーザに行わないようにします。

/ALWAYSRESTOREPOINT (推奨)
安全性を高めるために、X-Cleaner は、スパイウェアを除去する前に "システム回復ポイント" を生成します。このスイッチを利用すると、システム回復ポイントの生成についてユーザに問い合わせすることなく、常に "はい" として処理します。

/TURBO (推奨)
ユーザへの GUI アップデートを表示することなく、スキャンを最速で実行します。このオプションにより、3 秒程度の非常に高速なスキャンを実行することができます。Turbo スイッチでは、90～95% のスパイウェアを検出することができます。このスキャンは、毎日実行することをお薦めします。

/REPORTONLY
このオプションを利用すると、すべての除去処理が無効化され、(ログ ファイルまたはその他の設定オプションで) 報告のみを行います。このオプションは、X-Cleaner をすべてのコンピュータに展開する前に、"スパイウェア インベントリ チェック" を行うために有効です。

/SILENT
画面への出力を無効にします。ただし、スパイウェアを検出した際の警告は表示します。

/UPDATE
開始時に、インターネット経由で新しいバージョンをチェックします。確認および問い合わせは、"SILENT" スイッチを共に利用することで無効化することができます。

/SNIPER
このオプションを利用すると、管理者は、X-Cleaner でのスパイウェアの検出および除去をユーザの介在なしに実行することができます。つまり、ユーザには、除去に関する選択をさせることはありません。

/NORESTOREPOINT
安全性を高めるために、X-Cleaner は、スパイウェアを除去する前に "システム回復ポイント" を生成します。このスイッチでは、この機能を無効化し、すべての除去処理を可能な限り "undo" することができます。
/NOUNINSTALLER
製品の一部分を完全に (合法的にも、技術的にも) 除去するには、専用のアンインストーラ (存在する場合) を実行する必要があります。そのため、X-Cleaner スキャン エンジンは、除去要求が発生すると、ア

ンインストーラを実行するよう試みます。この方法の唯一の欠点は、アンインストーラを制御することができず、また、ユーザの介在が必要になるということです。このスイッチを利用すると、製品のアンインストーラが実行されることを防止できます。

/FORCEREBOOT
通常の再起動動作では、ユーザに未保存のデータを保存することを促すオプションや、再起動をキャンセルするためのオプションがあります。このスイッチを利用すると、アンアテンデット（無人）処理をより確実に行えます。ユーザは、数秒間のみ上記のオプションを選択することは可能ですが、再起動はキャンセルすることはできません。このスイッチを利用した場合、ユーザの未保存のドキュメントなどのデータを喪失する可能性があるので注意してください。

レポート オプション – settings.ini ファイルの設定

スパイウェアが検出された場合の通知を受信するための各種オプションが準備されています。
各設定は、個別にオン/オフを切り替えることができます。
同時に複数の種類のレポート方法を利用することも可能です。
レポート機能は、"ノンブロッキング" です。つまり、レポート機能は、一定時間の間に処理できないとしても、後の処理は中断されることなく実行されます。
電子メールによるレポート機能
メール設定は、テストや小さなネットワーク環境で最適です。このオプションは、ネットワーク上で検出されたスパイウェアの通知のみをすぐに受け取りたい管理者にとって有効です。通知の配信は、既存のメール サーバを利用して行われるため、追加のセットアップは一切必要ありません。このオプションはまた、リモート設定でノートブック コンピュータなどを利用している "road warrior(外出の多い方)" にとって最適なソリューションとなります。ユーザがインターネットに接続し、メール サーバに接続可能であれば、警告はオフィスにいる場合と同じように受信することができます。
;--------------------メール送信設定
; スイッチのオン/オフ。
mailactive=on
; メールを送信するためのサーバ（SMTP サーバ）のホスト名。必須。
mailserver=smtp.yourdomain.com
; レポートのメール受信アドレス。必須。
mailto=admin@yourdomain.com
; メールの "From" アドレス。省略可能。省略した場合、送信先が使用されます。
;mailfrom=admin@yourdomain.com
HTTP によるレポート機能
規模の大きいネットワーク（例えば 100 台以上の PC）では、中央のデータベースにレポートを蓄えることで効果が得られます（必要であれば、サーバのセットアップに関するドキュメントを参照してください）。この目的のために "Management Console" を利用する場合、設定ファイルのこの部分は自動的に適切な URL 設定で記述されます。

このレポート オプションは標準HTTP 呼び出しを利用していることから、簡単に情報を収集するカスタム構築ソリューションとすることが可能です。これには、開発技術が必要になりますが、このドキュメントでは解説を省略します。弊社では、Management Console を利用して早期の段階でこのソリューションを導入することを強くお薦めしています。詳細については、contact@nextEDGEtech.com までお問い合わせください。
;--------------------HTTP POST 設定
; スイッチのオン/オフ。

httpactive=on
; 検出の詳細を POST するフル URL。必須。
httpurl=http://yourservername/yourdir/postresult.asp

テクニカル ノート

– "活動している" スパイウェアを検出するために、X-Cleaner を可能な限り Windows スタートアップの終わりに実行するように設定してください。

– このプログラムは、DOS モードでは実行できません。

– 実行可能ファイルは、自動展開が可能なようにコードは証明書付きです。

– プログラムはどんな場所からでも実行可能です。
例: 読み取り専用の共有ディレクトリ

– ステータス メッセージは、標準出力に送信されます。すべての確認要求と警告は、ダイアログ ボックスに表示されます。

これにより、ステータス メッセージは必要に応じてリダイレクトすることができます。
例: xcl_cmd.exe –autostart –turbo > NUL

– このアプリケーションは、XBlock System LLC に著作権があります。
利用するには、コンピュータ毎にライセンスが必要になります。
詳細については、contact@nextEDGEtech.com までお問い合わせください。