BKDR_POISON.TUHB

マルウェアタイプ:	バックドア型	危険度:	低
破壊活動の有無:	なし	ダメージ度:	低
プラットフォーム:	Windows	感染力:	低
暗号化:	あり	情報漏えい:	低
感染報告の有無 :	あり	感染確認数:	低

概要

感染経路: インターネットからのダウンロード, 他のマルウェアからの作成

マルウェアは、他のマルウェアに作成されるか、悪意あるWebサイトからユーザが誤ってダウンロードすることによりコンピュータに侵入します。

マルウェアは、ワーム活動の機能を備えていません。

マルウェアは、不正リモートユーザからのコマンドを実行し、感染コンピュータを改ざんします。

詳細

ファイルサイズ: 34,304 bytes
タイプ: DLL
メモリ常駐: あり
発見日: 2017年1月19日
ペイロード: システムセキュリティへの感染活動

侵入方法

マルウェアは、他のマルウェアに作成されるか、悪意あるWebサイトからユーザが誤ってダウンロードすることによりコンピュータに侵入します。

インストール

マルウェアは、以下の Mutex を作成し、メモリ上で自身の重複実行を避けます。

- NlUJhUGIY

自動実行方法

マルウェアは、自身のコピーがWindows起動時に自動実行されるよう以下のレジストリ値を追加します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Active Setup\Installed Components\{GUID}
StubPath = "{malware path and filename}"
```

感染活動

マルウェアは、ワーム活動の機能を備えていません。

バックドア活動

マルウェアは、不正リモートユーザからの以下のコマンドを実行します。

- Send system information (Lan IP, Wan IP, Computer name, Username, Account Type, OS)
- Send hardware information (CPU speed, Memory)
- Manage Files (Search, Download, Upload, Execute, Rename, Delete)
- Manage Registries (Search, Modify, Delete, Rename, Create)
- Manage Processes (View, Kill, Suspend, Unload Module)
- Manage Services (View, Start, Stop, Edit, Install, Uninstall)
- Manage Devices (View, Enable, Disable, Remove)
- Manage Windows
- Relay server
- View,copy and uninstall applications
- View active ports
- Perform a shell command
- Download and inject remote codes to legitimate processes
- Log keystrokes and active window
- Capture screenshots
- View webcam activity
- Listen to microphone audio
- Update, Uninstall, Restart the malware
- Retrieve cached passwords and hashes

マルウェアは、以下のWebサイトにアクセスし、不正リモートユーザからのコマンドを送受信します。

- film.{BLOCKED}ayfilmlink.com:443

その他

マルウェアが自身の不正活動を実行するためには、以下のファイルが必要になります。

- {malware path}\McVsShld.exe - non malicious, used by the malware to load the malicious dll
- C:\Users\Public\Documents\yoshiDATA.dat - configuration file, also detected as BKDR_POISON.TUHB

不正リモートユーザから送信されるコマンドは以下のとおりです。

- システム情報の送信（LANのIPアドレス、WANのIPアドレス、コンピュータ名、ユーザ名、アカウントタイプおよびオペレーティングシステム（OS））
- ハードウェア情報の送信（CPUスピード、メモリ）
- ファイルの管理（検索、ダウンロード、アップロード、実行、改称および削除）
- レジストリの管理（検索、変更、削除、改称、作成）
- プロセスの管理（表示、終了、休止およびモジュールのアップロード）
- サービスの管理（表示、開始、終了、編集、インストールおよびアンインストール）
- デバイスの管理（表示、有効化、無効化および削除）
- ウィンドウの管理
- 中継サーバ
- アプリケーションの表示、コピーおよびアンインストール
- アクティブなポートの表示
- シェルコマンドの実行
- リモートコードのダウンロードおよび正規のプロセスへの挿入
- キー入力操作情報とアクティブウィンドウの収集
- スクリーンショットの取得
- Webカメラ活動の閲覧
- マイク音声の傍受
- マルウェアの更新、アンインストールおよび再起動
- キャッシュされたパスワードとハッシュの取得

マルウェアが自身の不正活動を実行するために必要な以下のファイルは、不正なDLLファイルを読み込みます。

- {malware path}\McVsShld.exe

マルウェアが自身の不正活動を実行するために必要な以下のファイルは、環境設定ファイルで、「BKDR_POISON.TUHB」として検出されます。

- {C:\Users\Public\Documents\yoshiDATA.dat

マルウェアは、以下のレジストリ値にアクセスすることで、標準ブラウザをクエリーします。

- HKEY_CLASSES_ROOT\http\shell\open\command

そして、マルウェアは、ブラウザのプロセス（例　iexplore.exe）を非表示で実行します。その後、マルウェアは、そのプロセスに、自身のバックドア活動に関する情報を含むコードを組み込みます。

マルウェアは、ルートキット機能を備えていません。

マルウェアは、脆弱性を利用した感染活動を行いません。

対応方法

対応検索エンジン: 9.8
初回 VSAPI パターンバージョン: 13.166.06
初回 VSAPI パターンリリース日: 2017年1月19日
VSAPI OPR パターンバージョン: 13.167.00
VSAPI OPR パターンリリース日:2017年1月20日

手順 1

Windows XP、Windows Vista および Windows 7 のユーザは、コンピュータからマルウェアもしくはアドウェア等を完全に削除するために、ウイルス検索の実行前には必ず「システムの復元」を無効にしてください。

手順 2

Windowsをセーフモードで再起動します。
詳細

セーフモードでの起動:

- **Windows 2000 の場合**:
  1. コンピュータを起動させます。
  2. 「Windows **** を起動しています・・・」のメッセージが表示されている間に[F8]を押します。
  3. 「Windows 拡張オプション メニュー」が表示されるので、[↓][↑]キーを使って[セーフモード]を選択し、[Enter]を押します。

- **Windows XP の場合**:
  1. コンピュータを起動させます。
  2. 「Windows **** を起動しています・・・」のメッセージが表示されている間に[F8]を押します。
  3. 「Windows 拡張オプション メニュー」が表示されるので、[↓][↑]キーを使って[セーフモード]を選択し、[Enter]を押します。

- **Windows Server 2003 の場合**:
  1. コンピュータを起動させます。

2. 「Windows **** を起動しています・・・」のメッセージが表示されている間に[F8]を押します。
3. 「Windows 拡張オプション メニュー」が表示されるので、[↓][↑]キーを使って[セーフモード]を選択し、[Enter]を押します。

• Windows Vista、Windows 7 および Windows Server 2008 の場合:

1. コンピュータを起動させます。
2. 「Windows **** を起動しています・・・」のメッセージが表示されている間に[F8]を押します。
3. 「詳細ブート オプション」が表示されるので、[↓][↑]キーを使って[セーフモード]を選択し、[Enter]を押します。

• Windows 8、8.1 および Server 2012の場合:

1. 画面の右上隅へマウスポインタを移動し、[チャーム]バーを表示します。
2. マウスで、[設定]ー[PC設定の変更]を選択します。
3. 左側のパネルで、[全般]を選択します。
4. 右側のパネルで、[PCの起動をカスタマイズする]が表示されるまで下にスクロールし、[今すぐ再起動]をクリック。コンピュータが再起動するまで待ちます。
5. [オプションの選択]メニューで、[トラブルシューティング]ー[詳細オプション]ー[スタートアップ設定]ー[再起動]をクリックします。
6. [スタートアップ設定]メニューで、[4]キーを押し、「4）セーフモードを有効にする」を選択します。

手順 3

このレジストリキーを削除します。
詳細

警告: レジストリはWindowsの構成情報が格納されているデータベースであり、レジストリの編集内容に問題があると、システムが正常に動作しなくなる場合があります。
レジストリの編集はお客様の責任で行っていただくようお願いいたします。弊社ではレジストリの編集による如何なる問題に対しても補償いたしかねます。
レジストリの編集前にこちらをご参照ください。

- In *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{GUID}*
  - **StubPath = "{malware path and filename}"**

このマルウェアが追加したレジストリキーの削除:

1. 「レジストリエディタ」を起動します。
   - Windows 2000、XP および Server 2003 の場合:
   [スタート]-[ファイル名を指定して実行]を選択し、**regedit** と入力し、Enter を押します。
   - Windows Vista、7 および Server 2008 の場合:
   [スタート]をクリックし、検索入力欄に **regedit** と入力し、Enter を押します。
   - Windows 8、8.1 および Server 2012 の場合:
   画面の左下隅を右クリックし、[ファイル名を指定して実行]を選択します。入力ボックスに **regedit** と入力し、Enter を押します。

   Iregedit は半角英数字で入力する必要があります（大文字／小文字は区別されません）。
2. 「レジストリエディタ」の左側のパネルにある以下のフォルダをダブルクリックします。
   HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Active Setup>Installed Components>{GUID}
3. 上記フォルダの左にあるプラスをクリックし、以下のキーを検索し、削除します。
   StubPath = "{malware path and filename}"
4. 「レジストリエディタ」を閉じます。

手順 4

コンピュータを通常モードで再起動し、最新のバージョン（エンジン、パターンファイル）を導入したウイルス対策製品を用い、「BKDR_POISON.TUHB」と検出したファイルの検索を実行してください。検出されたファイルが、弊社ウイルス対策製品により既に駆除、隔離またはファイル削除の処理が実行された場合、ウイルスの処理は完了しており、他の削除手順は特にありません。