BKDR_ANDROM

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

概要

感染経路: 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、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

タイプ: EXE
メモリ常駐: あり
ペイロード: ファイルのダウンロード, ファイルの実行

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、以下のファイルを作成します。

- %User Temp%\cdo{random numbers}.dll

(註：%User Temp%フォルダは、ユーザの一時フォルダで、Windows 2000、XP および Server 2003 の場合、通常、"C:\Documents and Settings\＜ユーザー名＞\Local Settings\Temp"、Windows Vista 、7 、8、8.1 、Server 2008 および Server 2012の場合、"C:\Users\＜ユーザ名＞\AppData\Local\Temp" です。.)

マルウェアは、感染したコンピュータ内に以下のように自身のコピーを作成します。

- %ProgramData%\ms{random}.exe
- %All Users Profile%\ms{random}.exe

(註：%ProgramData%フォルダは、Windows Vista および 7 の場合、通常、"C:\ProgramData"、Windows 2000、XP (32ビット)、Server 2003 の場合、"C:\Program Files"、Windows XP (64ビット) の場合、"C:\Program Files (x86)" です。. %All Users Profile%フォルダは、Windows 2000、XP および Server 2003 の場合、通常、"C:\Documents and Settings\All Users”、Windows Vista 、7 、8、8.1 、Server 2008 および Server 2012の場合、"C:\ProgramData” です。.)

マルウェアは、以下のプロセスを追加します。

- msiexec.exe

マルウェアは、以下のプロセスに自身を組み込み、システムのプロセスに常駐します。

- created msiexec.exe

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\
Windows\CurrentVersion\policies\
Explorer\Run
{random number} = "%ProgramData%\ms{random}.exe"
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\policies\
Explorer\Run
{random number} = "%All Users Profile%\ms{random}.exe"
```

他のシステム変更

マルウェアは、以下のレジストリ値を変更します。

```
HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Explorer\
Advanced
Hidden = "2"
```

(註：変更前の上記レジストリ値は、「1」となります。)

```
HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Explorer\
Advanced
ShowSuperHidden = "0"
```

(註：変更前の上記レジストリ値は、「1」となります。)

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。

- Download a file directed by C&C server, save it as %User Temp%\KB{8 random numbers}.exe and execute it
- Download a file directed by C&C server, save it as %All User Profile%\ms{random number}.dat and load it
- Download a file directed by C&C server, save it as %All User Profile%\ms{random}.exe:{random number}
- Copy %System%\cdosys.dll to %User Temp%\cdo{random number}.dll and load it
- Start a process
- Uninstall itself
- Perform remote shell commands
- Restart system

(註：%User Temp%フォルダは、ユーザの一時フォルダで、Windows 2000、XP および Server 2003 の場合、通常、"C:\Documents and Settings\＜ユーザー名＞\Local Settings\Temp"、Windows Vista 、7 、8、8.1 、Server 2008 および Server 2012の場合、"C:\Users\＜ユーザ名＞\AppData\Local\Temp" です。.. %System%フォルダは、システムフォルダで、いずれのオペレーティングシステム(OS)でも通常、"C:\Windows\System32" です。.)

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。

- http://{BLOCKED}rderstatus.ru/order.php
- http://{BLOCKED}erentia.ru/diff.php

情報漏えい

マルウェアは、以下の情報を収集します。

- Operating system information
- Local IP address
- Root volume serial number

その他

マルウェアは、以下のWebサイトにアクセスしてインターネット接続を確認します。

- update.microsoft.com
- microsoft.com
- google.com
- bing.com
- yahoo.com

対応方法

対応検索エンジン: 9.750

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

このマルウェアもしくはアドウェア等の実行により、手順中に記載されたすべてのファイル、フォルダおよびレジストリキーや値がコンピュータにインストールされるとは限りません。インストールが不完全である場合の他、オペレーティングシステム（OS）の条件によりインストールがされない場合が考えられます。手順中に記載されたファイル／フォルダ／レジストリ情報が確認されない場合、該当の手順の操作は不要ですので、次の手順に進んでください。

手順 3

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 4

このレジストリ値を削除します。
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\Windows\CurrentVersion\policies\Explorer\Run*
  - **{random number} = "%All Users Profile%\ms{random}.exe"**
- In *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run*
  - **{random number} = "%ProgramData%\ms{random}.exe"**

このマルウェアが追加したレジストリ値の削除:

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、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>Windows>CurrentVersion>policies>Explorer>Run
3. 右側のパネルで以下のレジストリ値を検索し、削除します。
   {random number} = "%All Users Profile%\ms{random}.exe"
4. 右側のパネルで以下のレジストリ値を検索し、削除します。
   {random number} = "%ProgramData%\ms{random}.exe"
5. 「レジストリエディタ」を閉じます。

手順 5

変更されたレジストリ値を修正します。
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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced*
  - From: **Hidden = "2"**
    To: **Hidden = 1**
- In *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced*
  - From: **ShowSuperHidden = "0"**
    To: **ShowSuperHidden = 1**

変更されたレジストリ値の修正:

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_CURRENT_USER>Software>Microsoft>Windows>CurrentVersion>Explorer>Advanced
3. 右側のパネルで以下のレジストリ値を検索します。
   Hidden = "2"
4. [値の名前]上で右クリックし、[修正]または[変更]を選択します。[文字列の編集]ダイアログボックスが表示されたら、[値のデータ]を以下に変更します。

Hidden = 1

5. 再び、右側のパネルで以下のレジストリ値を検索します。

ShowSuperHidden = "0"

6. [値の名前]上で右クリックし、[修正]または[変更]を選択します。[文字列の編集]ダイアログボックスが表示されたら、[値のデータ]を以下に変更します。

ShowSuperHidden = 1

7. レジストリエディタを閉じます。

手順 6

以下のファイルを検索し削除します。

詳細

コンポーネントファイルが隠しファイル属性に設定されている場合があります。[詳細設定オプション]をクリックし、[隠しファイルとフォルダの検索]のチェックボックスをオンにし、検索結果に隠しファイルとフォルダが含まれるようにしてください。

- %All User Profile%\ms{random}.exe
- %All User Profile%\ms{random number}.dat
- %User Temp%\KB{8 random numbers}.exe
- %User Temp%\cdo{random number}.dll

マルウェアのコンポーネントファイルの削除:

- Windows 2000、XP および Server 2003 の場合:

  1. [スタート]-[検索]-[ファイルとフォルダすべて]を選択します。
  2. [ファイル名のすべてまたは一部]に以下のファイル名を入力してください。
     - **%All User Profile%\ms{random}.exe**
     - **%All User Profile%\ms{random number}.dat**
     - **%User Temp%\KB{8 random numbers}.exe**
     - **%User Temp%\cdo{random number}.dll**
  3. [探す場所]の一覧から[マイコンピュータ]を選択し、[検索]を押します。
  4. 検索が終了したら、ファイルを選択し、SHIFT+DELETE を押します。これにより、ファイルが完全に削除されます。

  註: ファイル名の入力欄のタイトルは、Windowsのバージョンによって異なります。(例:ファイルやフォルダ名の検索の場合やファイル名のすべてまたは一部での検索)

- Windows Vista、7、Server 2008、8、8.1 および Server 2012 の場合:

  1. Windowsエクスプローラ画面を開きます。
     - Windows Vista、7 および Server 2008 の場合:
       - [スタート]-[コンピューター]を選択します。
     - 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、[エクスプローラー]を選択します。
  2. [コンピューターの検索]に、以下を入力します。
     - **%All User Profile%\ms{random}.exe**
     - **%All User Profile%\ms{random number}.dat**
     - **%User Temp%\KB{8 random numbers}.exe**
     - **%User Temp%\cdo{random number}.dll**
  3. ファイルが表示されたら、そのファイルを選択し、SHIFT+DELETE を押します。これにより、ファイルが完全に削除されます。

  註: Windows 7 において上記の手順が正しく行われない場合、マイクロソフトのWebサイトをご確認ください。

手順 7

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_ANDROM」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。