





# PUA.Win32.Adload.AI

 [trendmicro.com/vinfo/us/threat-encyclopedia/malware/pua.win32.adload.ai/](https://trendmicro.com/vinfo/us/threat-encyclopedia/malware/pua.win32.adload.ai/)

Analysis by: Maria Emreen Viray

-  Threat Type: Potentially Unwanted Application
-  Destructiveness: No
-  Encrypted:
-  In the wild: Yes

## OVERVIEW

This Potentially Unwanted Application arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

## TECHNICAL DETAILS

### Arrival Details

This Potentially Unwanted Application arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

### Installation

This Potentially Unwanted Application drops the following files:

- %User Temp%\main.ini
- %Application Data%\DataRecovery\api-ms-win-core-console-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-datetime-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-debug-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-errorhandling-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-file-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-file-l1-2-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-file-l2-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-handle-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-heap-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-interlocked-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-libraryloader-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-localization-l1-2-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-memory-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-namedpipe-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-processenvironment-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-processthreads-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-processthreads-l1-1-1.dll

- %Application Data%\DataRecovery\api-ms-win-core-profile-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-rtlsupport-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-string-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-synch-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-synch-l1-2-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-sysinfo-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-timezone-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-core-util-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-conio-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-convert-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-environment-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-filesystem-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-heap-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-locale-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-math-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-multibyte-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-private-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-process-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-runtime-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-stdio-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-string-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-time-l1-1-0.dll
- %Application Data%\DataRecovery\api-ms-win-crt-utility-l1-1-0.dll
- %Application Data%\DataRecovery\Aspose.Words.dll
- %Application Data%\DataRecovery\Common.lcc
- %Application Data%\DataRecovery\DataPreview.exe
- %Application Data%\DataRecovery\dnhfzj.dll
- %Application Data%\DataRecovery\dnhfzj64.dll
- %Application Data%\DataRecovery\dnhfzjctrl.exe
- %Application Data%\DataRecovery\dnhfzjsvr.exe
- %Application Data%\DataRecovery\DuiLib.dll
- %Application Data%\DataRecovery\FreeImage.dll
- %Application Data%\DataRecovery\libcommon.dll
- %Application Data%\DataRecovery\main.ini
- %Application Data%\DataRecovery\MaskRoate.png
- %Application Data%\DataRecovery\msvcpl140.dll
- %Application Data%\DataRecovery\OpenWordDll.dll
- %Application Data%\DataRecovery\Refresh.png
- %Application Data%\DataRecovery\System.Runtime.InteropServices.RuntimeInformation.dll
- %Application Data%\DataRecovery\Thumbs.db
- %Application Data%\DataRecovery\Uninst.exe
- %Application Data%\DataRecovery\vcruntime140.dll
- %Application Data%\DataRecovery\wDataRecovery.exe
- %Application Data%\Microsoft\Windows\Start Menu\Programs\DataRecovery\DataRecovery.Ink
- %Application Data%\Microsoft\Windows\Start Menu\Programs\DataRecovery\Uninstall.Ink
- %Desktop%\DataRecovery.Ink
- %User Temp%\com{random digits}.dlcc
- Added after uninstallation through ControlPanel/running %Application Data%\DataRecovery\Uninst.exe:
  - %User Temp%\Uninst.exe
  - %User Temp%\dnhfzj.dll

(Note: %User Temp% is the current user's Temp folder, which is usually C:\Documents and Settings\{user name}\Local Settings\Temp on Windows 2000(32-bit), XP, and Server 2003(32-bit), or C:\Users\{user name}\AppData\Local\Temp on Windows Vista, 7, 8, 8.1, 2008(64-bit), 2012(64-bit) and 10(64-bit).. %Application Data% is the current user's Application

Data folder, which is usually C:\Documents and Settings\{user name}\Application Data on Windows 2000(32-bit), XP, and Server 2003(32-bit), or C:\Users\{user name}\AppData\Roaming on Windows Vista, 7, 8, 8.1, 2008(64-bit), 2012(64-bit) and 10(64-bit).. %Desktop% is the current user's desktop, which is usually C:\Documents and Settings\{User Name}\Desktop on Windows 2000(32-bit), XP, and Server 2003(32-bit), or C:\Users\{user name}\Desktop on Windows Vista, 7, 8, 8.1, 2008(64-bit), 2012(64-bit) and 10(64-bit).)

It adds the following processes:

- %Application Data%\DataRecovery\dnhfzjsvr.exe -install
- %Application Data%\DataRecovery\dnhfzjctrl.exe regdll=%Application Data%\DataRecovery\dnhfzj.dll
- %System%\regsvr32.exe /s "%Application Data%\DataRecovery\dnhfzj.dll"
- %Application Data%\DataRecovery\wDataRecovery.exe

(Note: %Application Data% is the current user's Application Data folder, which is usually C:\Documents and Settings\{user name}\Application Data on Windows 2000(32-bit), XP, and Server 2003(32-bit), or C:\Users\{user name}\AppData\Roaming on Windows Vista, 7, 8, 8.1, 2008(64-bit), 2012(64-bit) and 10(64-bit).. %System% is the Windows system folder, where it usually is C:\Windows\System32 on all Windows operating system versions.)

### Autostart Technique

This Potentially Unwanted Application registers itself as a system service to ensure its automatic execution at every system startup by adding the following registry entries:

HKEY\_LOCAL\_MACHINE\SYSTEM\{ControlSet001 or CurrentControlSet}\services\dnhfzjsvr  
Description = Data Recovery File Stream Control Serve

HKEY\_LOCAL\_MACHINE\SYSTEM\{ControlSet001 or CurrentControlSet}\services\dnhfzjsvr  
DisplayName = Data Recovery File Stream Control Server

HKEY\_LOCAL\_MACHINE\SYSTEM\{ControlSet001 or CurrentControlSet}\services\dnhfzjsvr  
ErrorControl = 1

HKEY\_LOCAL\_MACHINE\SYSTEM\{ControlSet001 or CurrentControlSet}\services\dnhfzjsvr  
ImagePath = %Application Data%\DataRecovery\dnhfzjsvr.exe

HKEY\_LOCAL\_MACHINE\SYSTEM\{ControlSet001 or CurrentControlSet}\services\dnhfzjsvr  
ObjectName = LocalSystem

HKEY\_LOCAL\_MACHINE\SYSTEM\{ControlSet001 or CurrentControlSet}\services\dnhfzjsvr  
Start = 2

HKEY\_LOCAL\_MACHINE\SYSTEM\{ControlSet001 or CurrentControlSet}\services\dnhfzjsvr  
Type = 272

### Other System Modifications

This Potentially Unwanted Application adds the following registry entries:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\App Paths\wDataRecovery.exe

(Default) = %Application Data%\DataRecovery\wDataRecovery.exe

HKEY\_CURRENT\_USER\Software\Microsoft\  
Windows\CurrentVersion\Uninstall\  
wDataRecovery  
DisplayName = wDataRecovery

HKEY\_CURRENT\_USER\Software\Microsoft\  
Windows\CurrentVersion\Uninstall\  
wDataRecovery  
UninstallString = %Application Data%\DataRecovery\uninst.exe

HKEY\_CURRENT\_USER\Software\Microsoft\  
Windows\CurrentVersion\Uninstall\  
wDataRecovery  
DisplayIcon = %Application Data%\DataRecovery\wDataRecovery.exe

HKEY\_CURRENT\_USER\Software\Microsoft\  
Windows\CurrentVersion\Uninstall\  
wDataRecovery  
DisplayVersion = 2.0.0.1

HKEY\_CURRENT\_USER\Software\Microsoft\  
Windows\CurrentVersion\Uninstall\  
wDataRecovery  
Publisher = ShangHai Yingshuang

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B60}  
(Default) = dnhfzj

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B60}\InprocServer32  
(Default) = %Application Data%\DataRecovery\dnhfzj.dll

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B60}\InprocServer32  
ThreadingModel = Apartment

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B60}\Settings  
Title = Data Recovery

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B60}\Settings  
Path = %Application Data%\DataRecovery\wDataRecovery.exe

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B60}\Settings  
Custom =

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B60}\Settings  
ShowIcon = 1

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\Settings  
Dynamic = 1

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\Settings  
Maxtext = 25

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
\*\shellex\ContextMenuHandlers\  
dnhfzj  
(Default) = {BF73DE8F-608F-479F-ACE5-01199DBC6B0}

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
Directory\shellex\ContextMenuHandlers\  
dnhfzj  
(Default) = {BF73DE8F-608F-479F-ACE5-01199DBC6B0}

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\  
Windows\CurrentVersion\Explorer\  
ShellIconOverlayIdentifiers\dnhfzj  
(Default) = {BF73DE8F-608F-479F-ACE5-01199DBC6B0}

#### Other Details

This Potentially Unwanted Application adds the following registry keys:

HKEY\_LOCAL\_MACHINE\SYSTEM\{ControlSet001 or CurrentControlSet}\  
services\dnhfzjsvr

HKEY\_CURRENT\_USER\Software\Microsoft\  
Windows\CurrentVersion\App Paths\  
wDataRecovery.exe

HKEY\_CURRENT\_USER\Software\Microsoft\  
Windows\CurrentVersion\Uninstall\  
wDataRecovery

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\InprocServer32

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\Settings

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
\*\shellex\ContextMenuHandlers\  
dnhfzj

HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\  
Directory\shellex\ContextMenuHandlers\  
dnhfzj

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\  
Windows\CurrentVersion\Explorer\  
ShellIconOverlayIdentifiers\dnhfzj

It connects to the following possibly malicious URL:

- <http://softlog.tw{BLOCKED}.cn/api/data/sync>
- <http://i.tw{BLOCKED}.cn/api/pure/get>

## SOLUTION

---

### Step 1

Trend Micro Predictive Machine Learning detects and blocks malware at the first sign of its existence, before it executes on your system. When enabled, your Trend Micro product detects this malware under the following machine learning name:

Troj.Win32.TRX.XXPE50FFF049

### Step 2

Before doing any scans, Windows 7, Windows 8, Windows 8.1, and Windows 10 users must disable *System Restore* to allow full scanning of their computers.

### Step 3

Note that not all files, folders, and registry keys and entries are installed on your computer during this malware's/spyware's/grayware's execution. This may be due to incomplete installation or other operating system conditions. If you do not find the same files/folders/registry information, please proceed to the next step.

### Step 4

Remove PUA.Win32.Adload.AI by using its own Uninstall option

[ Learn More ]

To uninstall the grayware process

### Step 5

Delete this registry value

[ Learn More ]

**Important:** Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this step only if you know how or you can ask assistance from your system administrator. Else, check this [Microsoft article](#) first before modifying your computer's registry.

- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}`  
**(Default) = dnhfzj**
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\InprocServer32`  
**(Default) = %Application Data%\DataRecovery\dnhfzj.dll**
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\InprocServer32`  
**ThreadingModel = Apartment**
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\Settings`  
**Title = Data Recovery**
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\Settings`  
**Path = %Application Data%\DataRecovery\wDataRecovery.exe**

- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\Settings`  
**Custom =**
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\Settings`  
**ShowIcon = 1**
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\Settings`  
**Dynamic = 1**
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\Settings`  
**Maxtext = 25**
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\*\shellex\ContextMenuHandlers\dnhfzj`  
**(Default) = {BF73DE8F-608F-479F-ACE5-01199DBC6B0}**
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\shellex\ContextMenuHandlers\dnhfzj`  
**(Default) = {BF73DE8F-608F-479F-ACE5-01199DBC6B0}**
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\dnhfzj`  
**(Default) = {BF73DE8F-608F-479F-ACE5-01199DBC6B0}**

### Step 6

Delete this registry key

[ Learn More ]

**Important:** Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this step only if you know how or you can ask assistance from your system administrator. Else, check this [Microsoft article](#) first before modifying your computer's registry.

- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}`
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\InprocServer32`
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{BF73DE8F-608F-479F-ACE5-01199DBC6B0}\Settings`
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\*\shellex\ContextMenuHandlers\dnhfzj`
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\shellex\ContextMenuHandlers\dnhfzj`
- In `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers\dnhfzj`

### Step 7

Search and delete this file

[ Learn More ]

There may be some files that are hidden. Please make sure you check the *Search Hidden Files and Folders* checkbox in the "More advanced options" option to include all hidden files and folders in the search result.

- %User Temp%\Uninst.exe
- %User Temp%\main.ini
- %User Temp%\dnhfzj.dll
- %User Temp%\com{random digits}.dlcc

### Step 8

Scan your computer with your Trend Micro product to delete files detected as PUA.Win32.Adload.AI. If the detected files have already been cleaned, deleted, or quarantined by your Trend Micro product, no further step is required. You may opt to simply delete the quarantined files. Please check the following Trend Micro Support pages for more information:

[Did this description help? Tell us how we did.](#)