CLR Injection 通用托管注入

http://chengchen.cnblogs.com

chengchencici@163.com

软件版本

软件版本	说明	更新日期
V2.0.1511.07	*超级灰色按钮克星，正式更名为：CLR Injection 通用托管注入器。将原先功能使用插件的形式合并到新的工具中。 *提供插件以及插件编写的 SDK 和参考源代码。用户可以自己编写插件扩展注入功能。 *默认提供两个插件，第一个是原来的属性修改插件，第二个是可以注入进取查看 IL 代码的插件。 *系统可以自动识别并注入 DOTNET2.0/3.0/3.5/4.0/4.5/4.6 等版本，无需人工选择。 *增加进程列表注入，这样针对无界面的程序也可以实现注入操作。 *支持 Win10 平台。 *使用了全新的皮肤和全新界面。 *取消对传统 Win32 平台的按钮激活，本程序将只关注 DOTNET 平台。 *因为 DOTNET1.1 实际使用的人太少，因此取消对 DOTNET1.1 的支持。	2015-11-07
V1.4.1309.13	*修复在部分 64 位操作系统上无法执行对 win32 程序无权限注入的操作。 *增加了 UAC 认证。 *支持 DOTNET4.5 平台。	2013-09-13
V1.4.1212.03	*紧急修复在 x86 平台上的 bug	2012-12-03
V1.4.1212.02	*增加了对 x64 位 DOTNET 程序的支持。 *区分 x86 和 x64 位平台。 *完善对 Win8 操作系统的支持。 *至少需要 WinXP SP2 以上版本。	2012-12-02
v1.3.1112.40	*根据某网友需求，新增支持 DOTNET Framework 1.1，克服种种困难终于实现了对目前所有 DOTNET FrameWork 平台的支持！	2010-11-12
v1.2.814.40	*新增支持 DOTNET Framework 4.0	2010-8-14

v1.1.324.40	*可以多次注入同一程序。 *使用了新的引擎，不再操作注册表。 *使用了新技术，只需要一个 DLL 文件就可以完成托管注入。 *使用了新的皮肤。	2010-3-24
V1.0	*实现托管注入的伟大创举。	2007-10-25

1 简介

这款软件可以将任意托管 DLL 使用插件的形式，注入到正在运行中的.net 托管程序集中去。提供插件编写的 SDK 和参考源代码。用户可以自己编写插件扩展注入功能。支持 DOTNET Framework 2.0/3.0/3.5/4.0/4.5/4.6 版本。

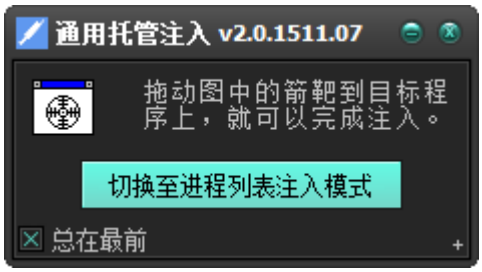
支持 XP SP2,SP3/Vista/Win7/Win8/Win10/Win2003 Sp1/Win2008/Win2012 操作系统。

不支持 XP Sp1，Win2003 原版

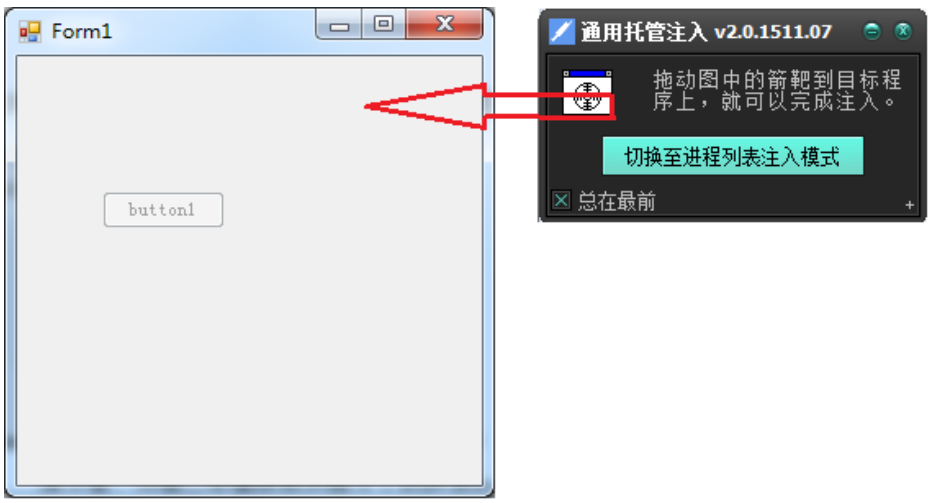
2 使用说明

2.1 通用托管程序注入

1、根据被注入程序的执行平台，相应选择 x86 或 x64 程序，打开 CLR_Injection.exe

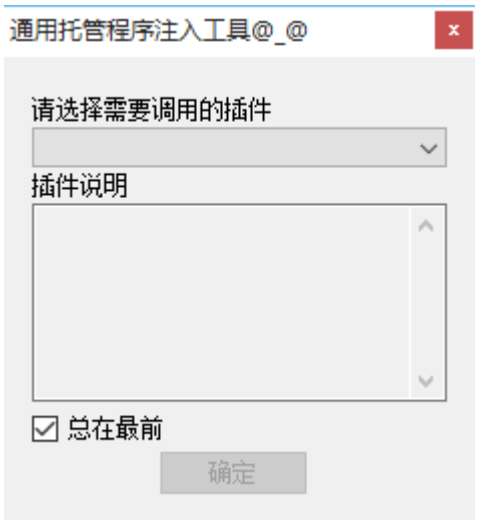


2、将箭靶拖动到目标程序中去：



您也可以使用进程列表选择被注入进程，这个主要适用于没有 GUI 的 DOTNET 程序。

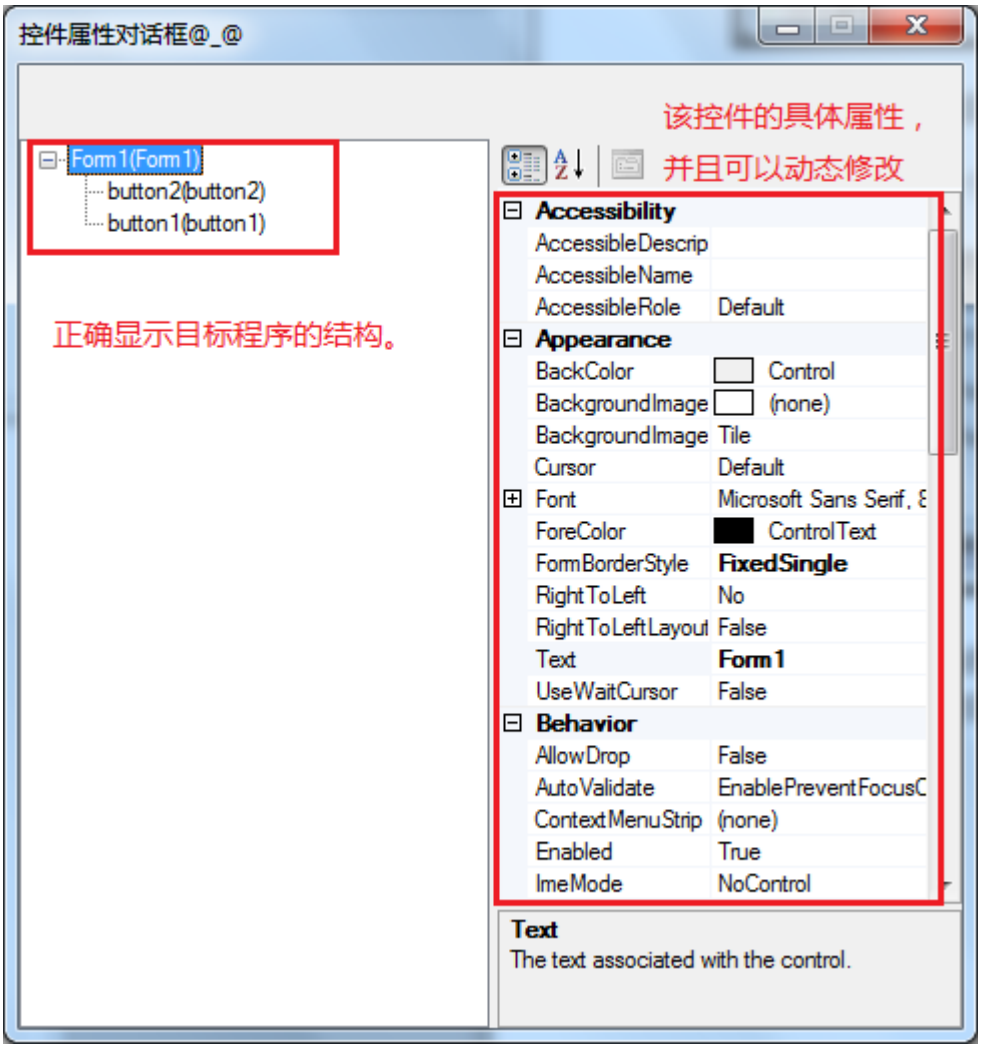
此时会弹出一个对话框，可以选择相应的插件。



目前系统自带两个插件

1) PropertyView

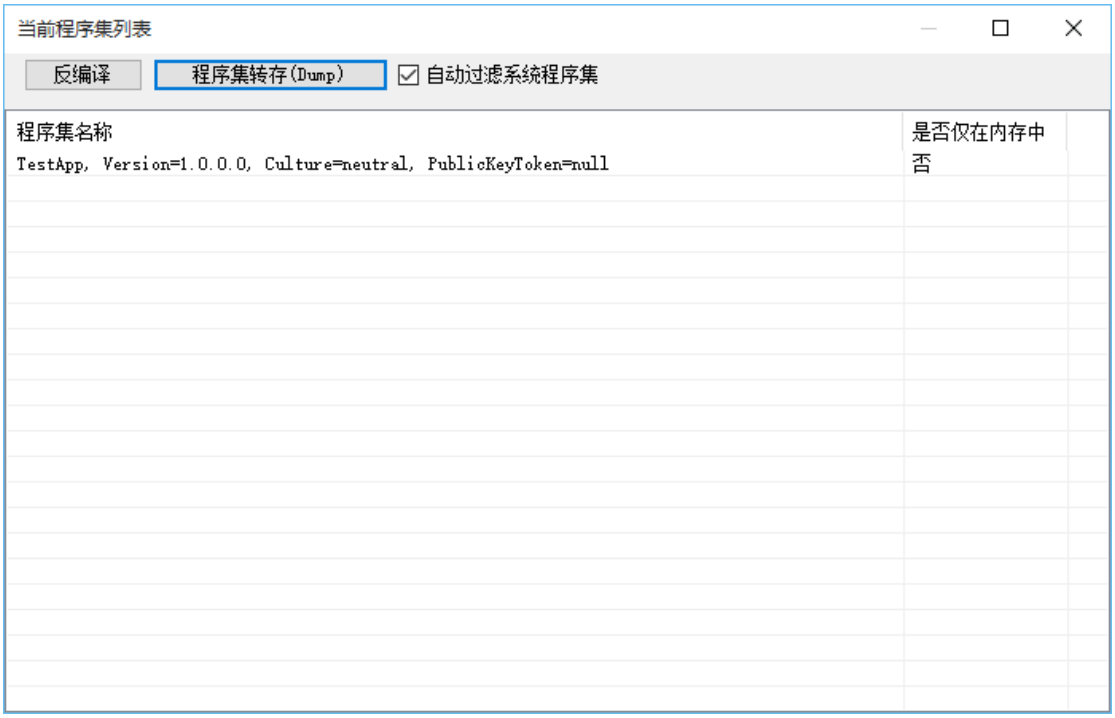
简介：这个插件就是原来的超级灰色按钮克星。可以显示当前所有窗体的属性，用户可以随时修改。



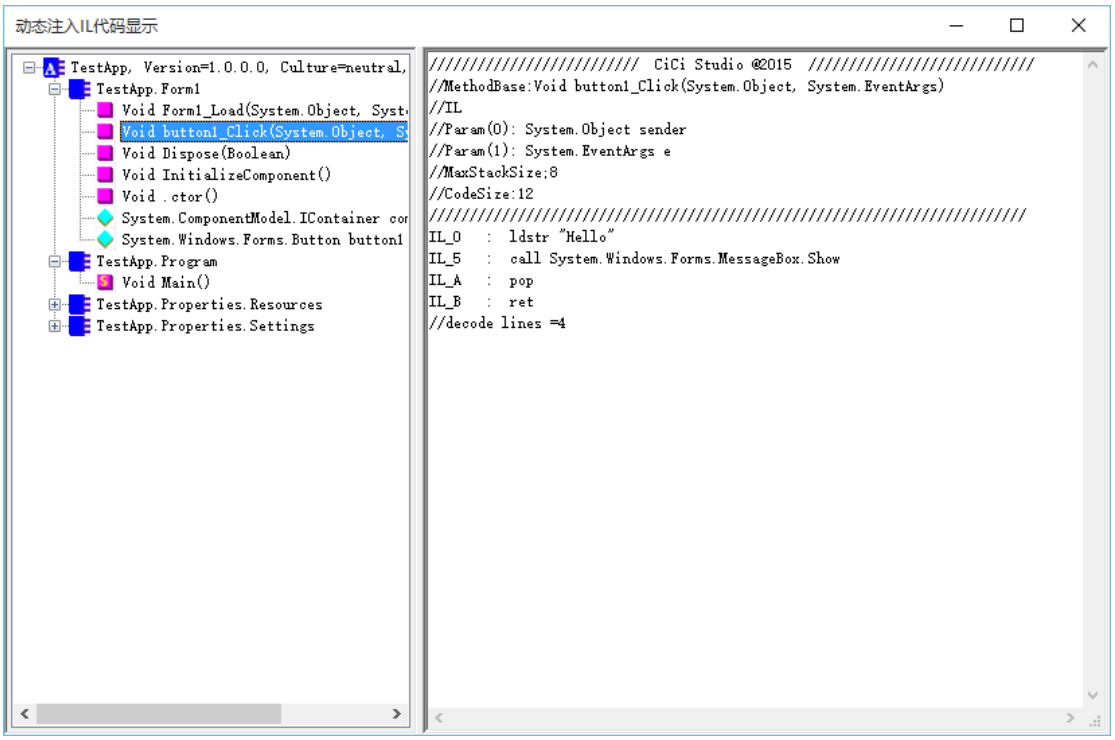
这个插件已经开源，可以在”程序根目录\SDK\Plugin_Source\PropertyView 找到完整代码。

2) InjectReflector

简介：这是一个可以查看程序集中的类、方法、属性、IL 代码的插件，使用者甚至可以 Dump 已经加载进来的程序集。因为这个插件已经被注入进目标程序，因此可以躲避部分目标程序特定检测和加密。



用户可以在内存中反编译程序集，甚至可以自己 dump 程序集，系统会自动尝试修复被加密的程序集，但不能保证所有 dump 后的程序集可以完美运行。一些程序会在内存中使用 byte[]数组的形式加载程序集，这样的程序集也可以从内存中直接 dump 下来，这个 dump 功能适用于整体加密的 DOTNET 程序。



2.2 SDK 编写

SDK 编写请参考“程序根目录\SDK\SDK 编写指南.pdf“。