# 渗透测试名词解析：Beacon、Payload、Shellcode有啥区别

安全运营 (https://www.secrss.com/articles?tag=安全运营) · 我需要的是坚持 (https://www.secrss.com/articles?author=我需要的是坚持) · 2020-12-13



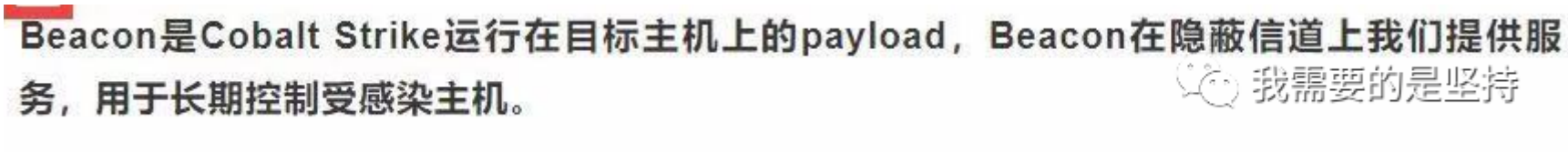
许多人分不清楚C2工具中的一些名词，包括：Beacon、Payload、Shellcode、Loader、Stager、Stagerless等。然后就出现了相互交流的时候鸡同鸭讲的情况。

## 1. 前言

有一段时间我发现好多安全从业者，也包括我，分不清楚C2工具中的一些名词，包括：Beacon、Payload、Shellcode、Loader、Stager、Stagerless等。没办法都是舶来品，洋大人的文章中有时候也是乱用的，更不要说国内的相关文章，导致大家对以上词汇的理解出现了分歧。然后就出现了相互交流的时候鸡同鸭讲的情况，以下是我对这些词汇的理解，有分歧欢迎讨论。

## 2. Beacon和Payload

前段时间看见这么一段话：



没有任何贬低和攻击的意思，我私信作者讨论了下，关于什么是Beacon。

- Beacon字面意思是**信标**，主要功能有：心跳和执行方法。你可以把它理解成一个灯塔，在不停的闪烁，发出“我在这儿、我在这儿”的信号。
    - 心跳：按照设定的时间周期和抖动不断的发送基本信息回控制端。
    - 执行方法：接受具体功能代码后，执行这些代码的方法。
- Payload字面意思是**有效载荷**（卫星或航天器携带的仪器设备等）。Payload被用在了很多地方，也是最让人傻傻分不清的名词。所有**被承载的物品**都能叫做Payload，因此：
    - 用Loader执行Shellcode，Shellcode可以被叫做Payload
    - 用DLL反射方法执行一个反射DLL文件，反射DLL文件可以叫做Payload
    - 在CS中你使用键盘记录功能，传给Beacon一个键盘记录的反射DLL，这个反射DLL可以叫做Payload

所以，说Beacon是一个Payload也没有多大问题。

**3. Shellcode和Loader**

这俩经常组合在一起，在CS中有一个“**Payload Generator**”的选项，主要生成的就是Shellcode。这些Shellcode没法作为可执行程序执行，需要Loader来执行它们。

- Shellcode维基上被定义为**一段用于利用软件漏洞而执行的代码，**这段代码通常的功能是获得一个shell，因此得名Shellcode。但是现在意义被扩大了很多。主要是以下2个特点：
    - 与位置无关的代码（PIC）
    - 无法独立执行
- Loader就是字面意思加载器。通常被用来对抗杀软，从静态特征到动态沙盒。Loader的实现也是千奇百怪，从不同语言到不同执行方法，根据加载的内容的不同，有PE Loader、Shellcode Loader、反射DLL Loader等等。

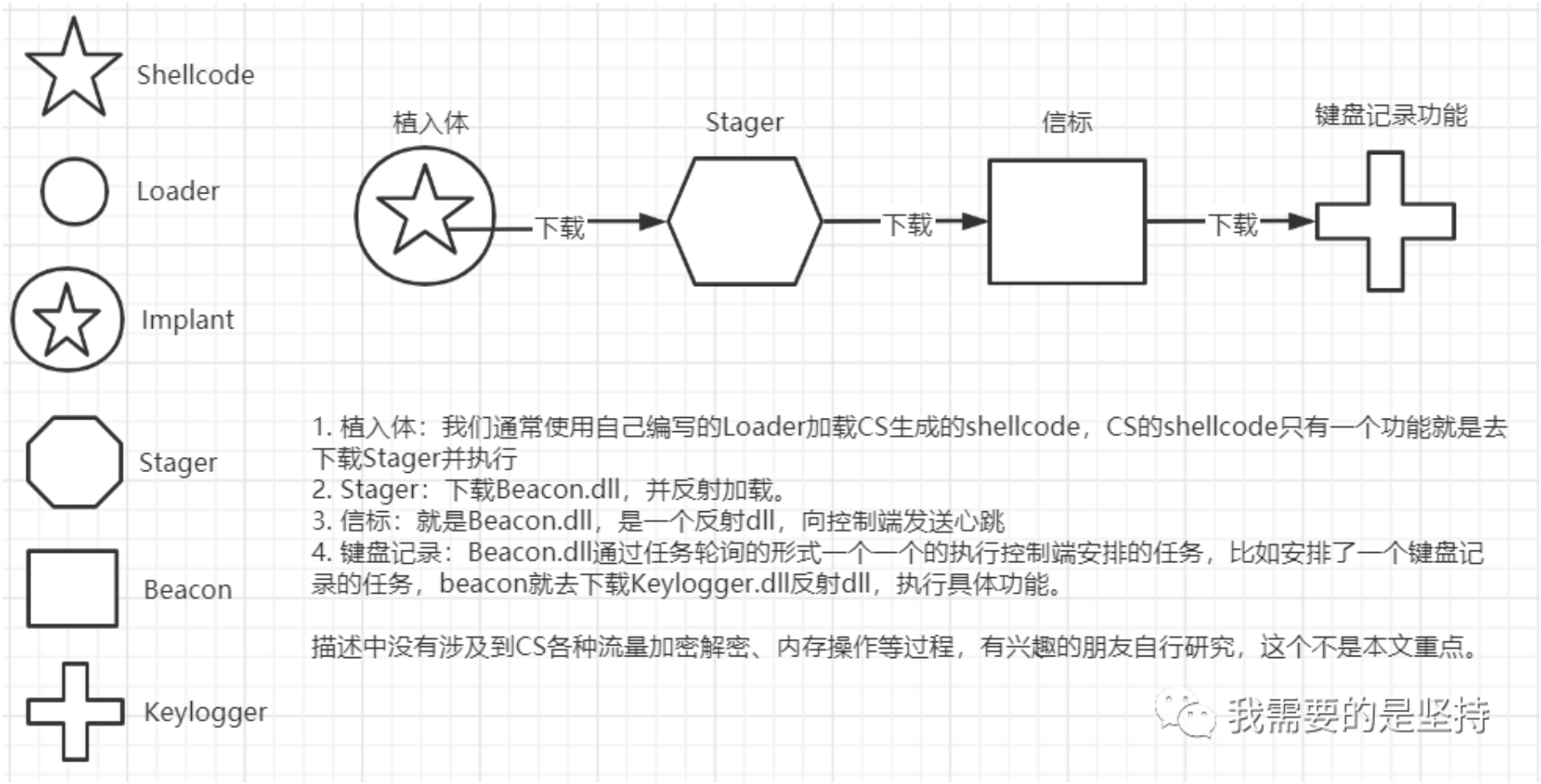
**4. Stage、Stageless**

分阶段和不分阶段，在实际红队工作中，很多时候不能在目标上执行过大的代码和文件，因此出现了，用一个小一点的代码去拉取更大的功能代码的情况。我们把这个一段一段的拉去代码执行的过程叫分阶段执行，因此出现了Stage(分阶段)和Stageless(不分阶段)这两个词。这其实很好理解，但伴随出现的Stager、Stagerless，让人有点傻傻分不清了。

- Stager，主要指用于执行下一阶段代码的相关代码，有点拗口。
- Stagerless，这个词语应该是国人创造的，我想说用Stageless就好。

**5. 以CobalStrike为例**

CS的分阶段加载过程：




总的来说：“**能用中文说清楚的别抖英文**”。全文到此了，最后是个题外话。

**6. CobaltStrike是不是远控、木马**

文章开头截图中的后半段“Beacon在隐蔽信道上为我们提供服务，用于长期控制受感染主机”，顿时我心中出现了一个疑问，大家是怎么看CobaltStrike的呢？

---

安全运营 (https://www.secrss.com/articles?tag=安全运营)