

Cobalt Strike | Beacon原理浅析

Ms08067安全实验室 3天前

以下文章来源于物联网IOT安全，作者lmnmn



物联网IOT安全

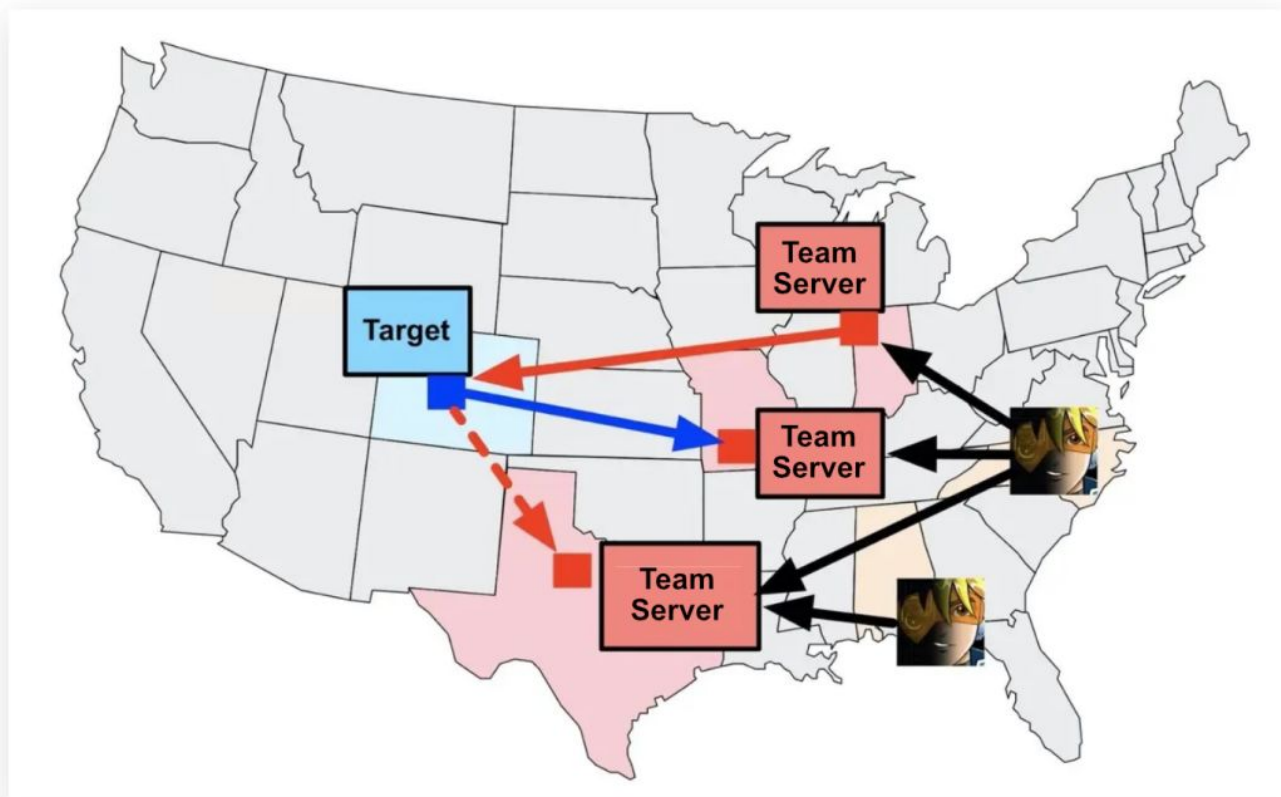
我们是一个专注于物联网IOT安全 固件逆向 近源攻击 硬件破解的公众号，与我们一起学习...



Hello大家好哇，我是你们可爱的lmn小姐姐，今天我们来研究一下Beacon的一些基础知识,如果有师傅没有看过这个系列之前的文章，可以点击下方图片阅读。



Cobalt Strike 作为一种**后渗透工具**，可以完成**侦察**、**鱼叉式钓鱼**、**浏览器代理**等攻击。上文中我们介绍了Cobalt Strike 分为**客户端**和**服务器**两部分，服务器端被称之为Team Server。Team Server既是Beacon payload的**控制器**，也是Cobalt Strike提供**社工功能的主机**。Team Server还存储了Cobalt Strike**收集的数据**以及**日志记录**。工作模式如下图所示：



很多同学在Cobalt Strike教程中见到最多的词就是Beacon，我们今天主要来介绍一下Beacon和Listener。

0x00 Beacon简介

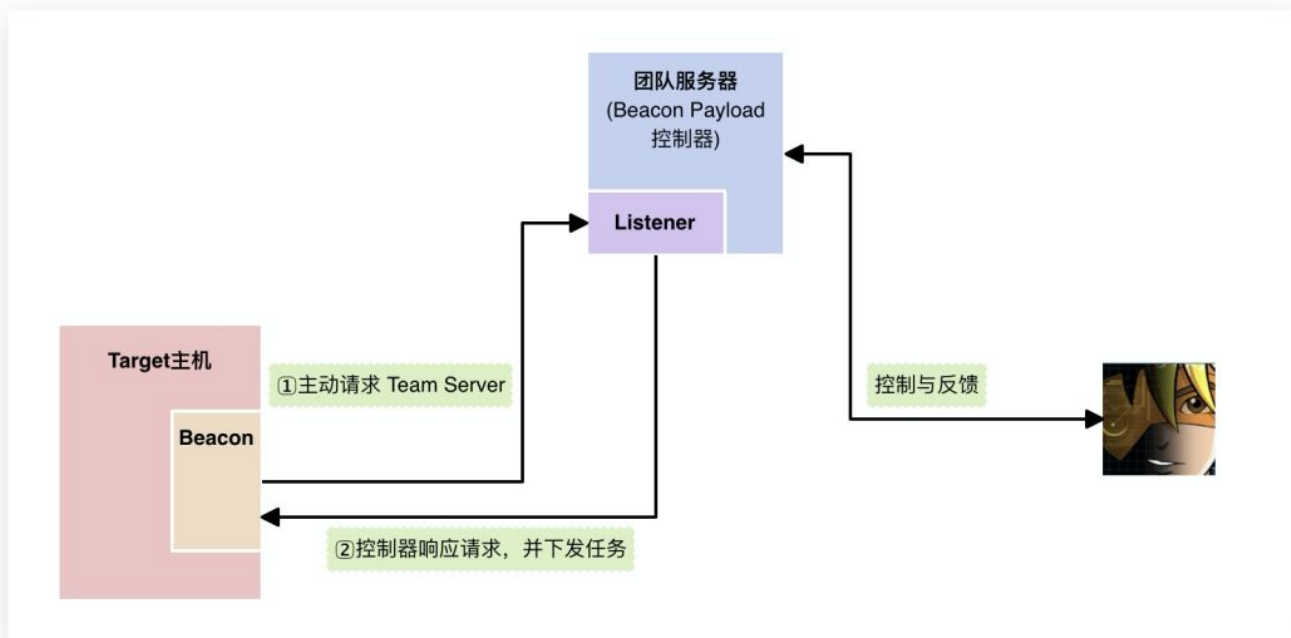
Beacon是Cobalt Strike运行在目标主机上的payload，Beacon在隐蔽信道上我们提供服务，用于长期控制受感染主机。它的工作方式与Metasploit Framework Payload类似。在实际渗透过程中，我们可以将其嵌入到可执行文件、添加到Word文档或者通过利用主机漏洞来传递Beacon。

Beacon的功能包括以下几点：

1. 使用HTTP或DNS检查是否有待执行任务
2. 可连接到多个C2域名

3. 能够在分段传输后自动迁移
4. 与Cobalt Strike紧密集成，通过社工、主机漏洞和会话来传递Beacon

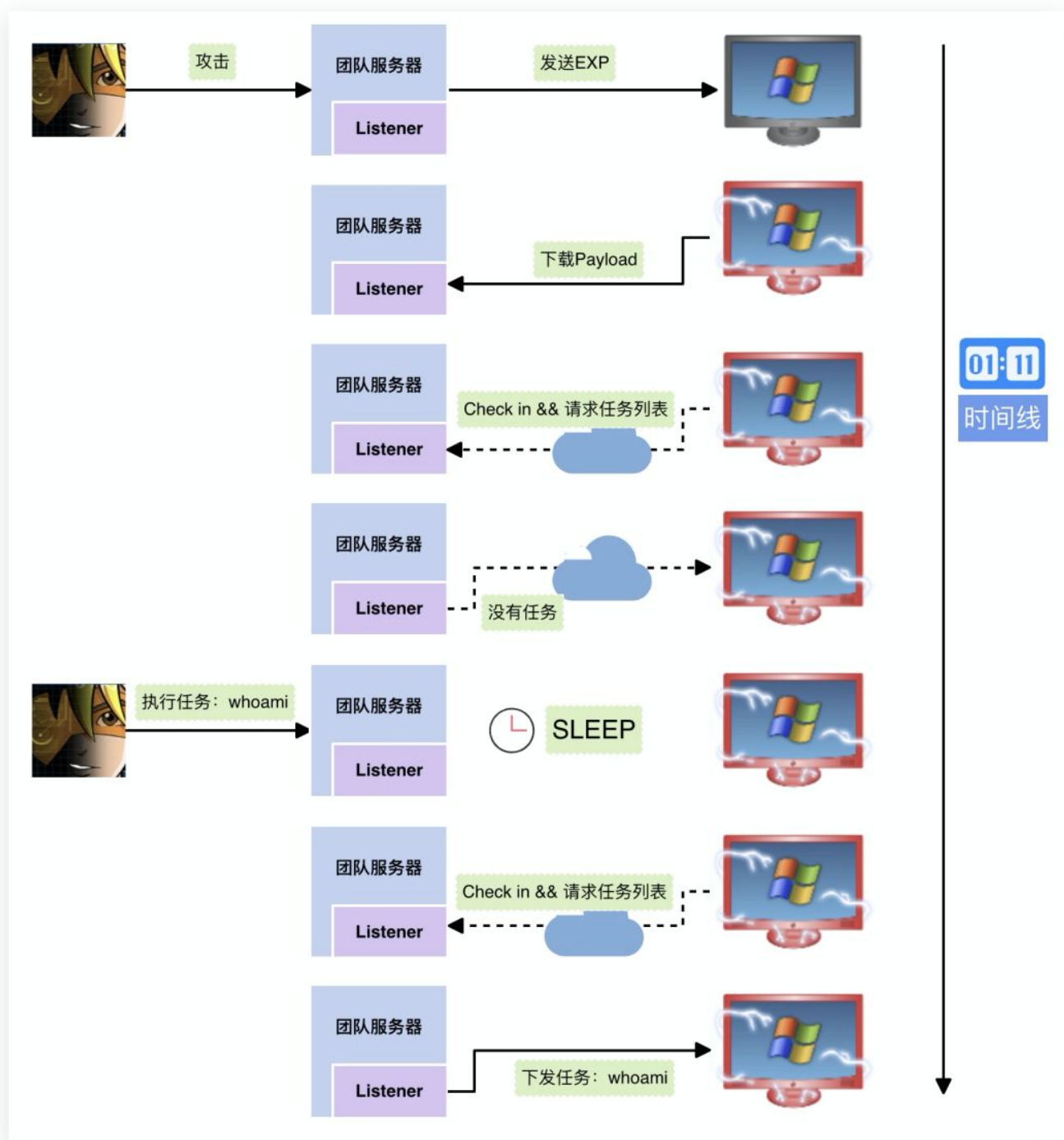
Beacon的中文名为信标，像是在网络中告诉我们：“嘿，我是肉鸡，我在这...”。我们可以通过下图来看Beacon的工作原理：



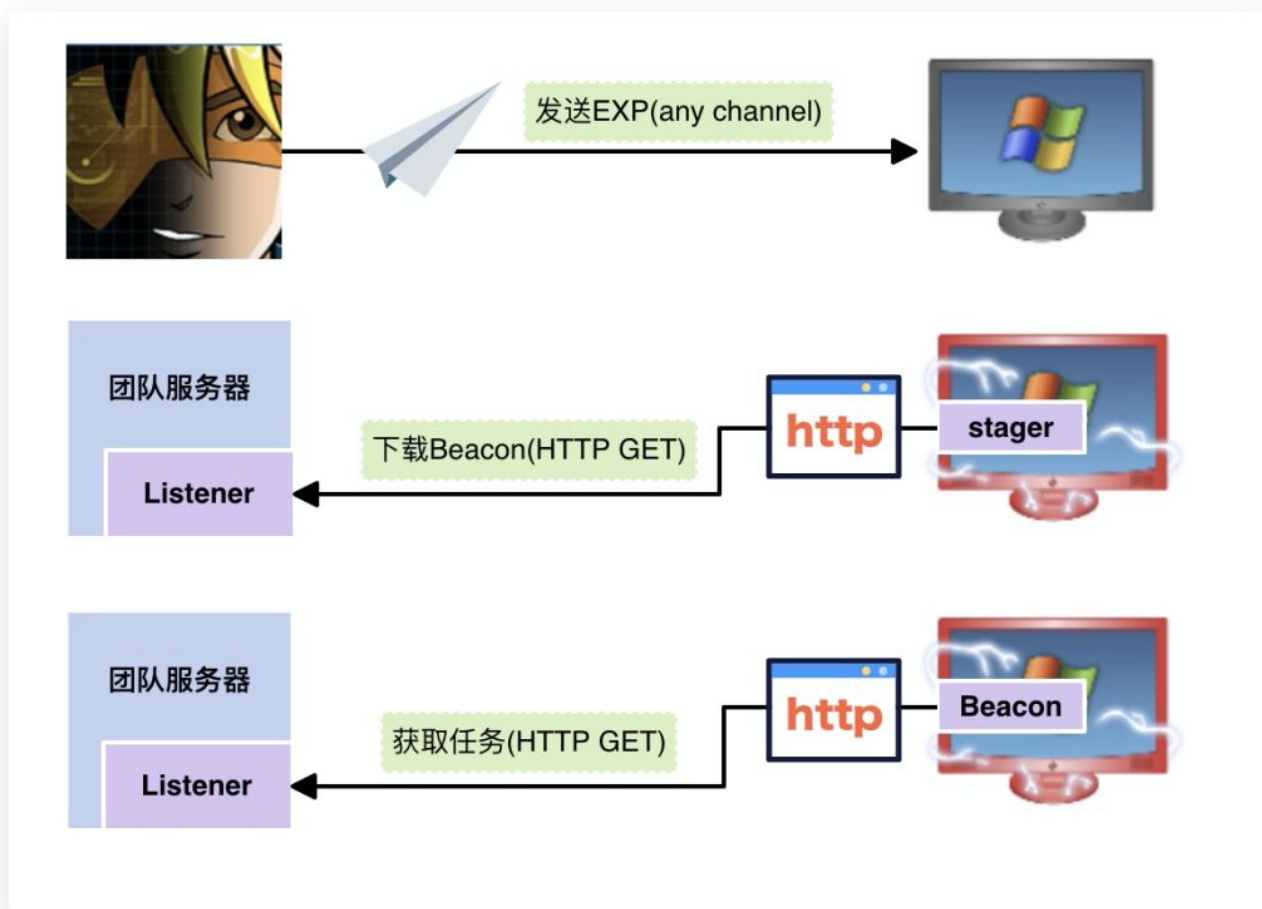
Beacon在目标主机上运行之后，会**主动**向我们提前设置好的Listener发送请求信息(叮，您有新的主机已上线)。

```
02/19 10:17:16 *** : [REDACTED] has joined.
02/19 10:18:41 *** [REDACTED] hosted Scripted Web Delivery (powershell) @ http://120.92.112.219:80/a
02/19 10:19:37 *** initial beacon from [REDACTED]@172.16.161.150 (WINDOWS10)
```

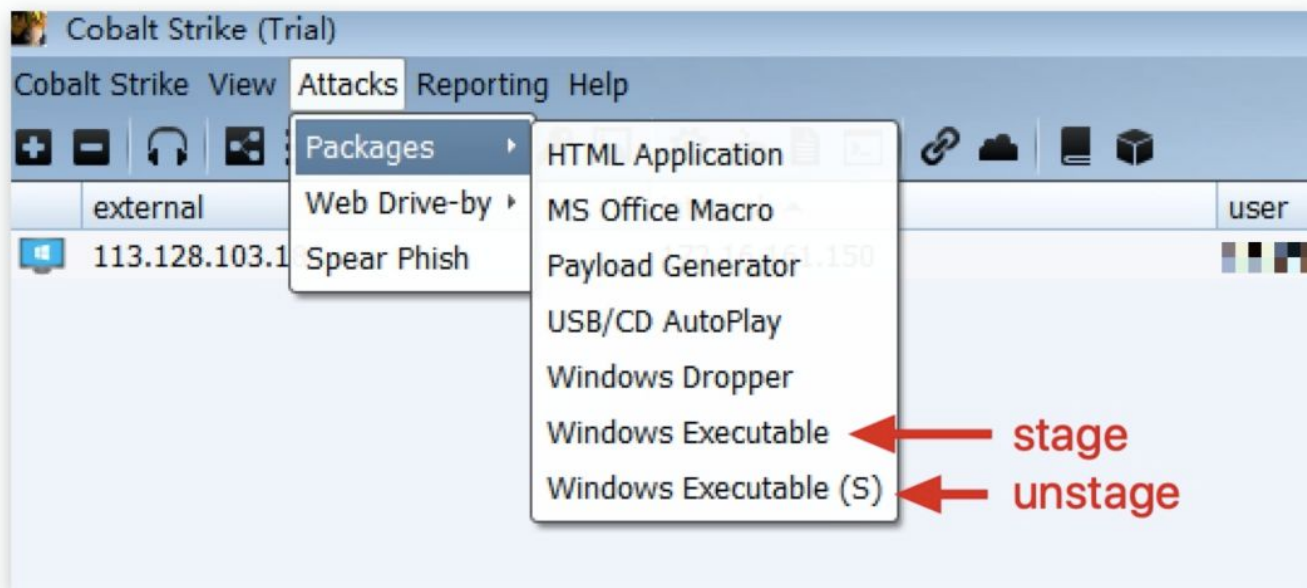
Team Server控制器接收到请求后会**检查是否有待执行的任务**，如果有就会将任务下发到Beacon。



此
处值得一提的是payloading staging，很多攻击框架都是使用**分段**的shellcode，以**防止shellcode过长**，覆盖到了上一函数栈帧的数据，导致引发异常。要说分段shellcode就不得不提stager，stager是一段很精短的代码，它可以**连接下载真正的payload并将其注入内存**。我们使用stager就可以解决shellcode过长的问題。



Cobalt Strike中也支持**分段**payload:



关于**分段payload优势与劣势**的问题，本文不予讨论，这就像是选择鸡还是鸡蛋一样，Cobalt Strike的作者最终选择了鸡蛋，所以.....在Cobalt Strike 3.5.1后的版本可以通过在Malleable C2中添加host_stage选项，以限制分段payload。

在Cobalt Strike 4中应该尽可能多的使用unstage，一方面以**保证安全性**（因为你无法确保stager下载的stage是否受到中间人攻击，除非像MSF一样使用SSL保证安全性）。另一方面如果我们通过层层代理，在内网进行漫游，这个时候使用分段的payload如果**网络传输出现问题**，stage没有加载过去，可能就会**错失一个Beacon**，unstage的payload会让人放心不少。

更多关于stage的参考资料：

```
1 https://cloud.tencent.com/developer/news/335831
2 https://blog.cobaltstrike.com/2016/06/22/talk-to-your-children-about-payload-stag
3 https://blog.cobaltstrike.com/2016/06/15/what-is-a-stageless-payload-artifact/
```

Beacon有两种通信策略（与团队服务器通信-CS 中以团队服务器作为 C2）

1. **异步式通信** = 异步模式下通信频率低、速度慢，如上图所示：Beacon会主动请求任务列表、然后进入SLEEP状态。
2. **交互式通信** = C2 对 Beacon 实时控制

摘抄(Plagiarism)雪师傅文章😁

0x01 Beacon分类

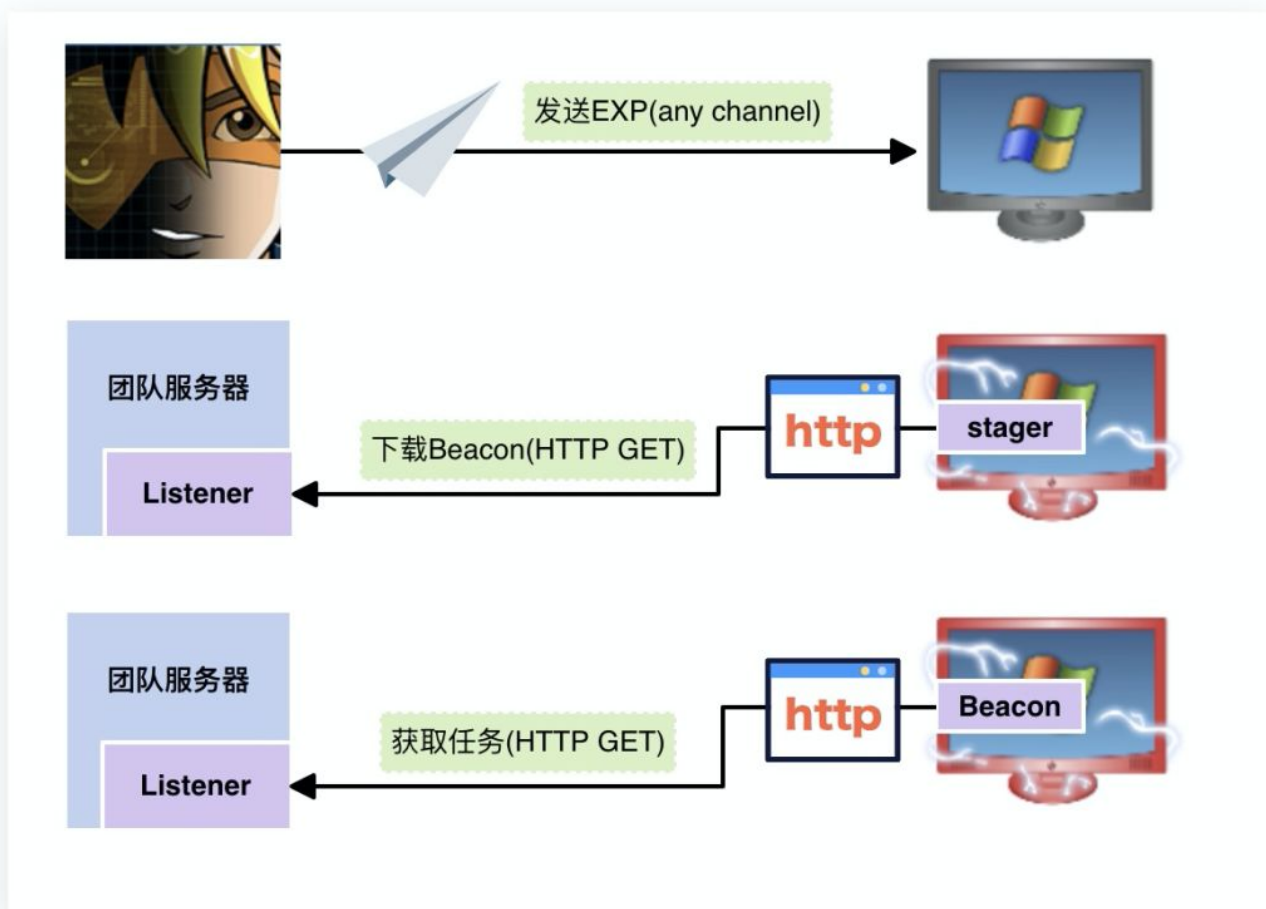
根据内置Listener的分类可以将Beacon分为：

1. HTTP and HTTPS Beacon
2. DNS Beacon
3. SMB Beacon

Listener是用来接收Beacon请求信息的Cobalt Strike模块，本文仅介绍Cobalt Strike 内置Listener。

1. HTTP and HTTPS Beacon

HTTP and HTTPS Beacon非常简单，关键是Beacon通过GET请求来下载任务。



需要强调的一点是这两个窗口中输入的地址作用并不相同。

The "New Listener" dialog box shows the following fields:

- Name: EC2 - HTTP Beacon
- Payload: windows/beacon_http/reverse_http
- Host: ads.loosenolove.com
- Port: 80

A "Save" button is located at the bottom right.

这里填写的是Stager下载Beacon的地址

The "Input" dialog box contains the following text:

This beacon uses HTTP to check for taskings. Please provide the domains to use for beaconing. The A record for these domains must be OK.

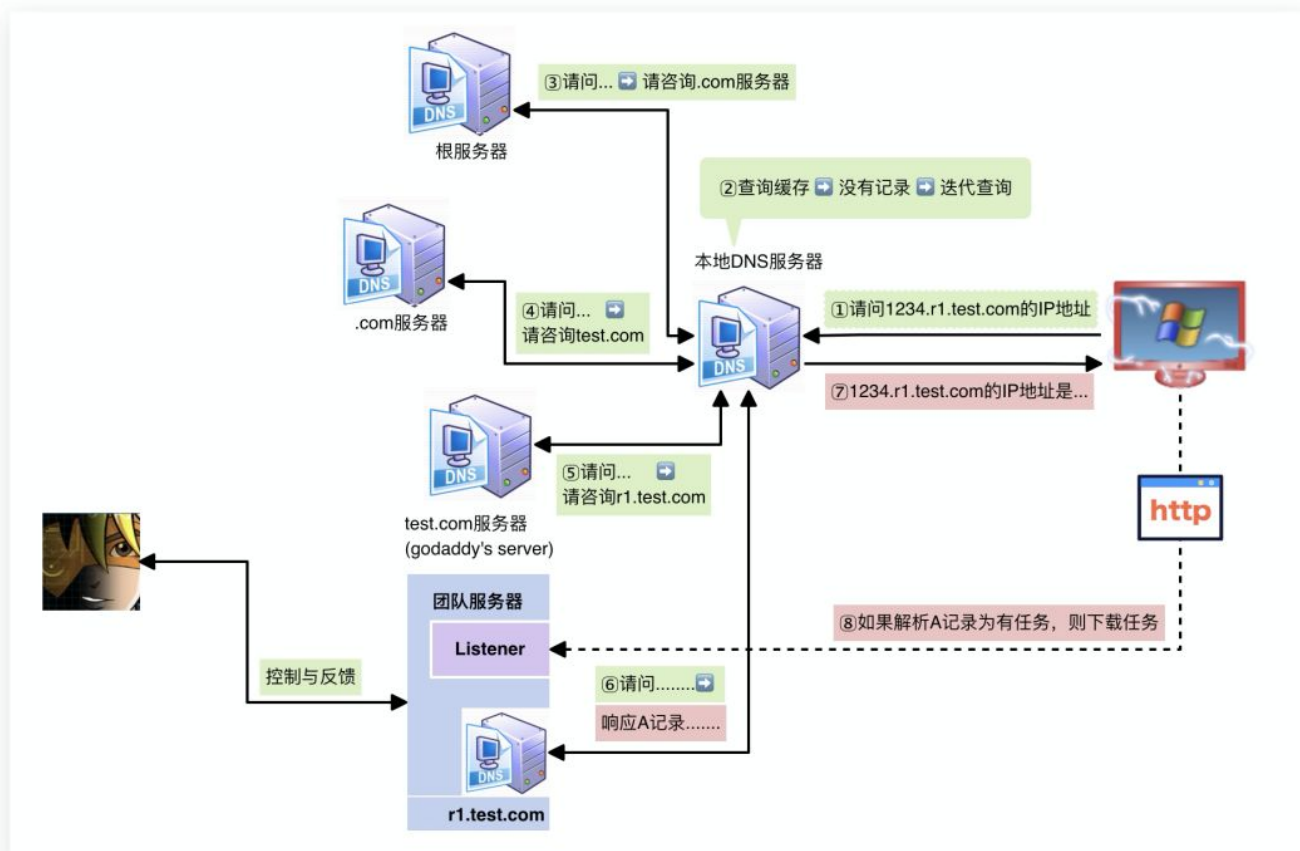
这里填写Beacon check in的地址

The input field contains the domain: ads.loosenolove.com

Buttons: OK, Cancel

2. DNS Beacon

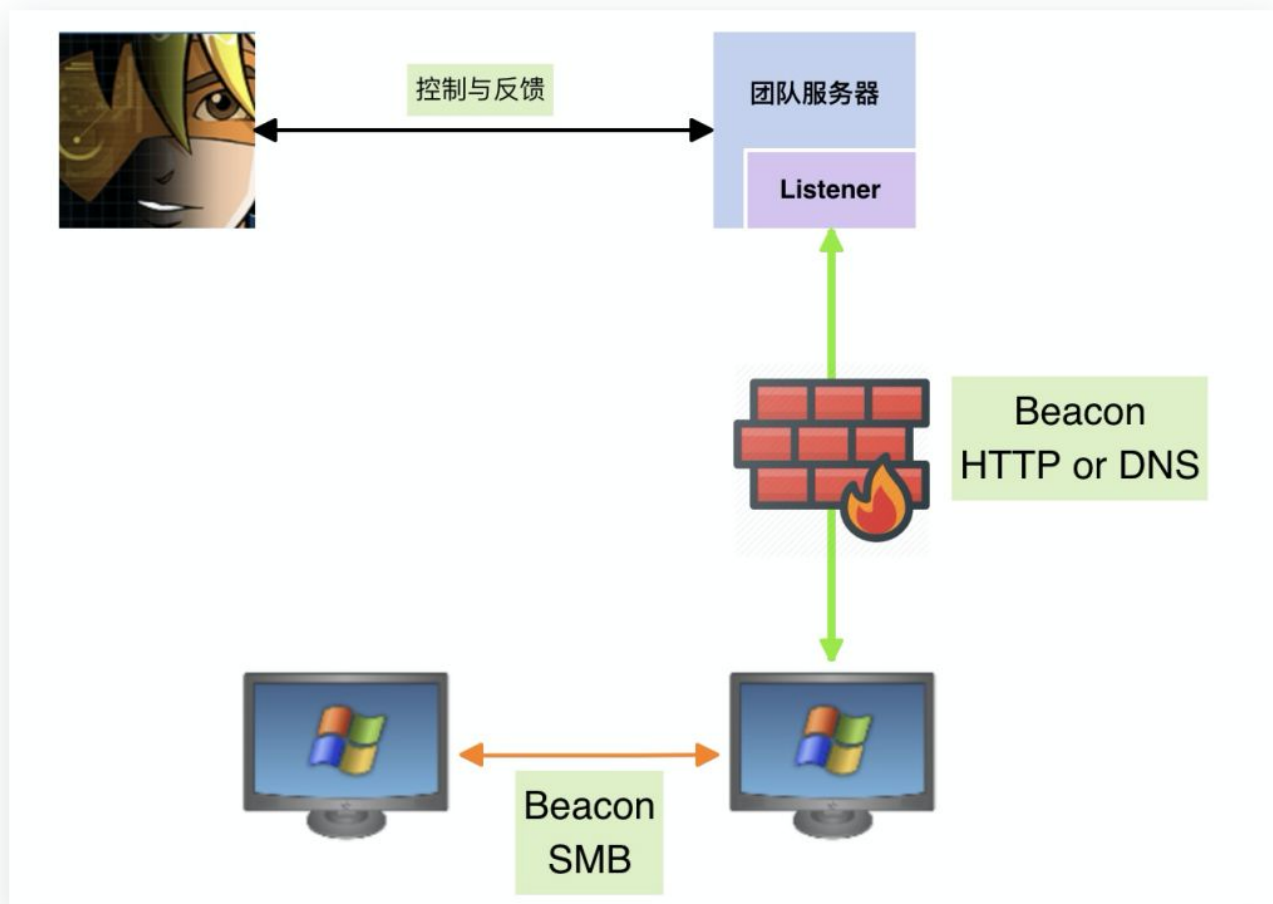
DNS Beacon是我最喜欢的方式，没有之一。Cobalt Strike使用DNS来完成Beacon check in的工作，如果DNS返回的记录解析为有需要执行的任务，那Beacon会使用HTTP来完成获取任务这一过程。具体原理参看下图：



需要注意的是DNS Beacon现在已经有两种方式(第二种方式是使用TXT记录)传输Beacon和task list，关于此内容后期的DNS Beacon文章中会特别强调，欢迎师傅关注后续文章。

3. SMB Beacon

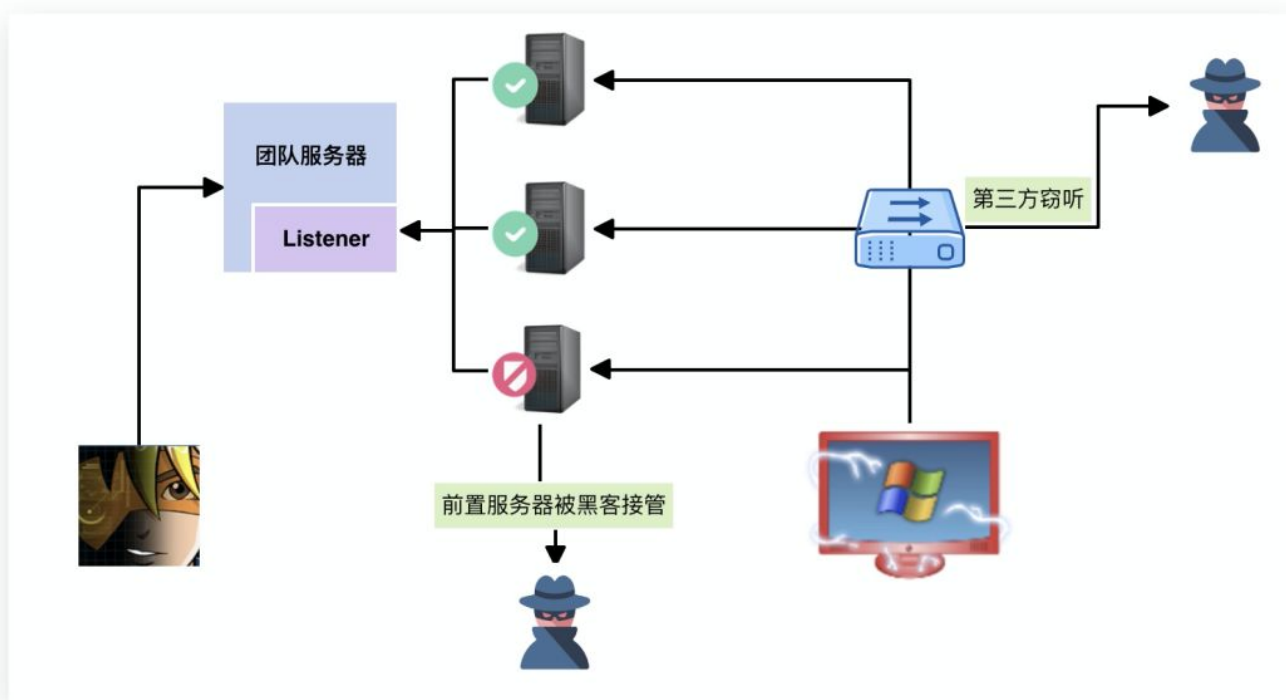
SMB Beacon需要连接到Parent Beacon使用，所有任务均从parent Beacon接收，并通过parent Beacon返回任务结果。它使用了Windows的命名管道，命名管道是Windows进程间通信机制，允许两者间通信、互相查看和操作对方的文件。Cobalt Strike使用这种方式在进程与进程或主机与主机之间通信，因为基于SMB协议所以被称之为SMB Beacon。



本文对SMB Beacon不详细展开，欢迎师傅关注下一篇文章，专门讲解SMB Beacon。

0x02 Beacon安全性

设想这样一个问题，如果**有人劫持了你的通信流量**，并可以监听到你的Beacon向Team Server传回的数据，这时**会发生什么呢**？

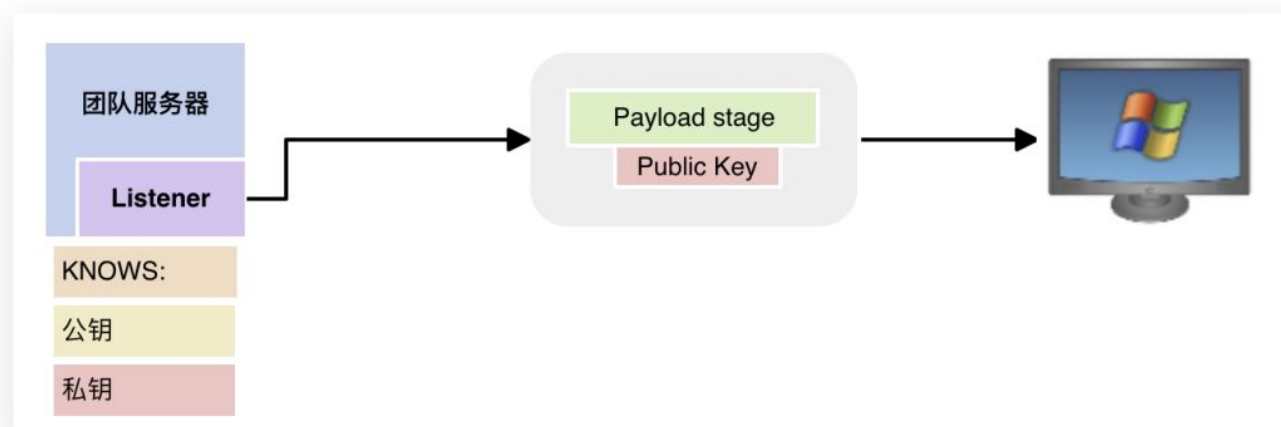


答案是什么都不会发生。因为Beacon内置了多种安全特性（除了第四条）：

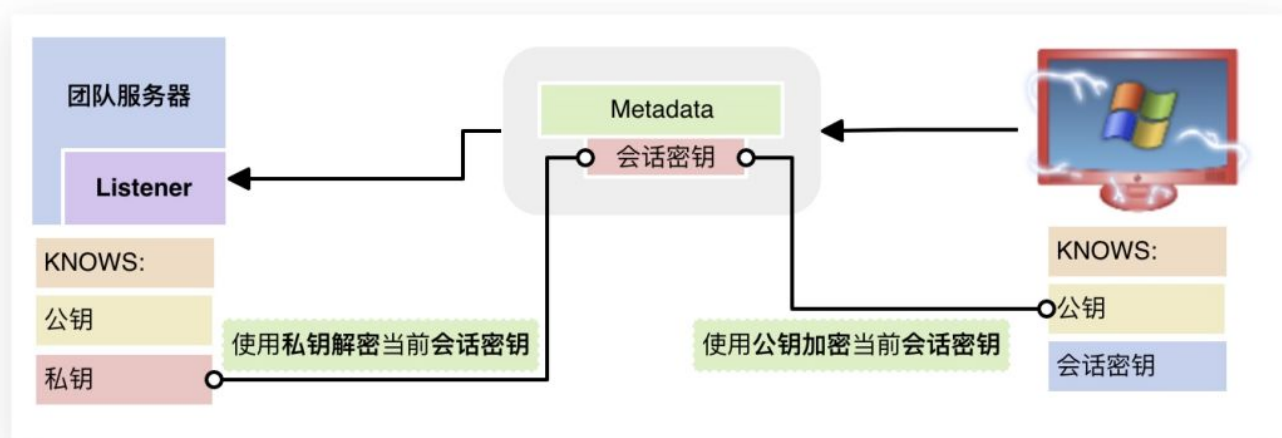
1. Beacon stage 在连接时会验证Team Server
2. Beacon 的任务请求和任务输出都是被加密的
3. Beacon 有重放保护机制
4. Beacon stagers 没有任何安全机制

当你启动Team Server并创建了Beacon Listener时，Team Server就会**创建公钥对**来保证后续传输过程的安全性。我们以分段传输payload为例，详细讲解一下Cobalt Strike的安全特性。

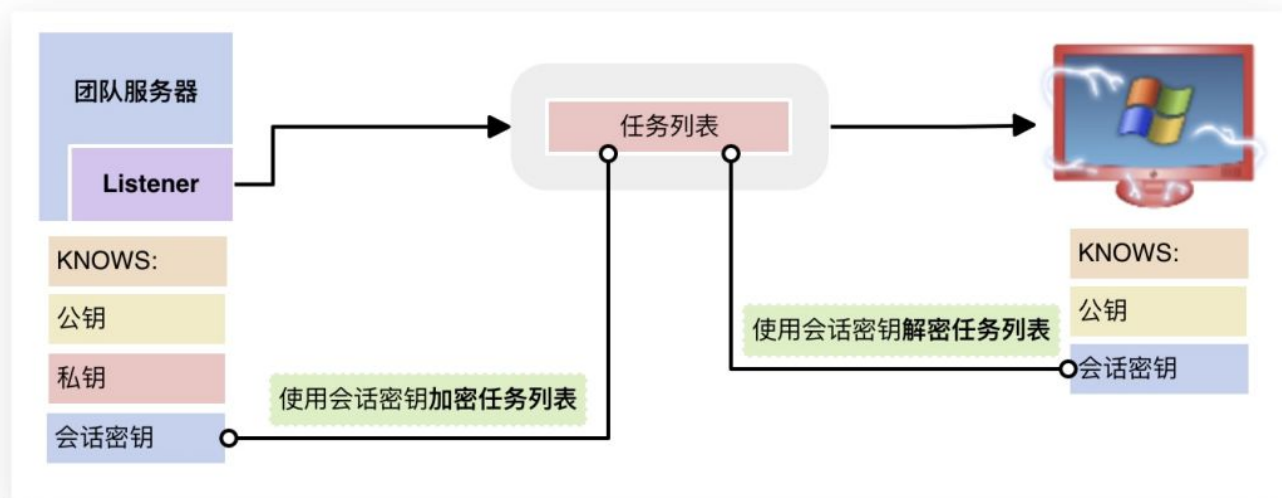
1. 当stager**下载stage**时，**公钥**也会被一起发送：



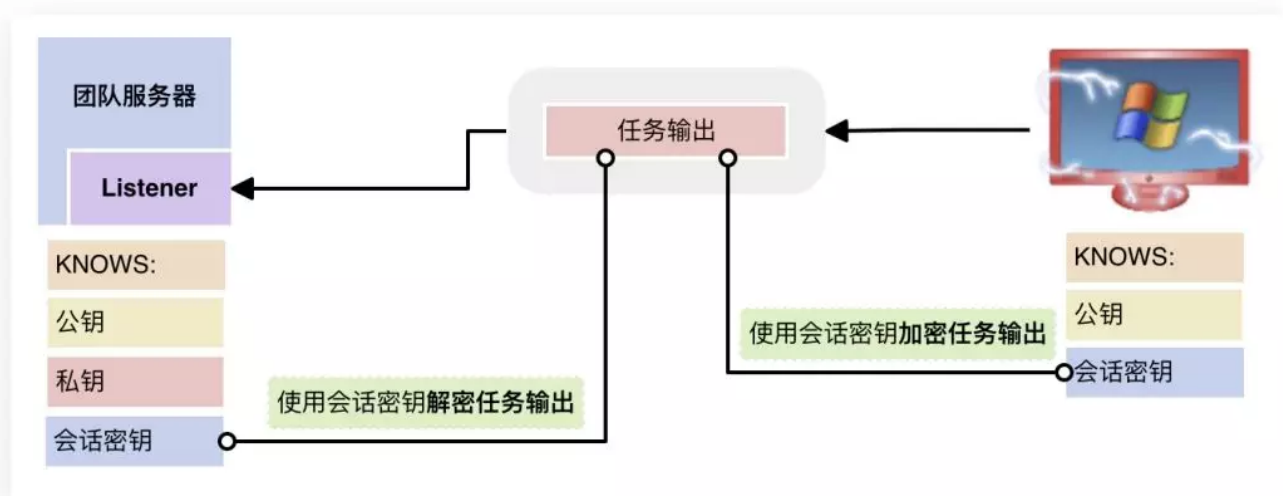
2. 当Beacon stage准备check in的时候，第一步就是要发送关于beacon session的元数据(Metadata)元数据中包含了用户、PID、电脑名称、IP地址等等基础信息，同时元数据中也包括了Beacon stage**创建的一个随机会话密钥**。为了保证安全性，Beacon stage会使用**公钥加密元数据(含会话密钥)**，这意味着只有Team Server才能够解密该数据包。



3. 当Beacon从Team Server下载任务的时候，团队服务器会使用**会话密钥加密**这些任务，Beacon stage也会使用**会话密钥来解密**任务列表。



4. 同样在返回任务结果的时候，Beacon stage也会使用**会话密钥**对任务输出加密。



可以看到Raphael在设计Cobalt Strike的时候已经充分的考虑到了它的安全性问题，所以..师傅放心用吧，wink~

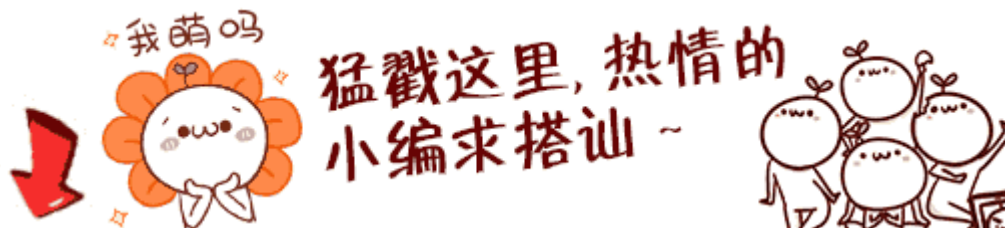
0x03 致谢

本文参考引用修改了以下文章的部分或节选内容，感谢各位师傅。

- 1 强烈推荐雪师傅的CS硬文: <http://blog.leanote.com/post/snowming/62ec1132a2c9>
- 2 探寻Metasploit Payload模式背后的秘密: <https://cloud.tencent.com/developer/news/33583>
- 3 Out of the Blue: <https://www.recordedfuture.com/identifying-cobalt-strike-servers/>
- 4 Cobalt Strike系列2listener与payload: https://blog.csdn.net/weixin_42140534/article/details/103444444
- 5 SMB Beacon Setup and Use: <https://www.youtube.com/watch?v=J3BEeIx6Xzk>
- 6 Volatility Plugin for Detecting Cobalt Strike Beacon: <https://blogs.jpcert.or.jp/en/2019/07/25/volatility-plugin-for-detecting-cobalt-strike-beacon/>
- 7 Meterpreter载荷执行原理分析: <https://xz.aliyun.com/t/1709/>
- 8 CobaltStrike基本功能与使用: <https://www.jianshu.com/p/8d823adbc6b5>



长按二维码 关注我们





END

广告时间

