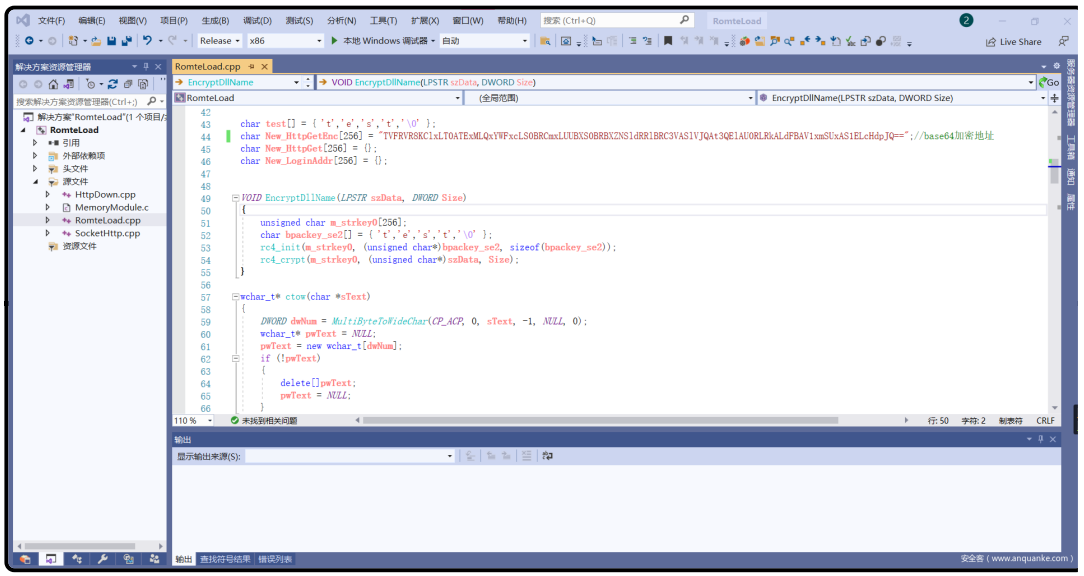
以看到是经过加密且Bypass。

接下来笔者把加密好的Shellcode.dll放到Http下载地址里。（Http下载服务器搭建，笔者在这里就不详细说明）

将URL: http://URL/ShellCode.dll 加密，得到加密过后的下载地址：TVFRVR8KClxLT0ATExMLQxYWFxcLS0BRCmxLUUBXS0BRBXZNSldRRlBRC3VASlVJQAt3QElAU0RLRkALdFBAV1xmSUxAS1ELcHdpJQ==

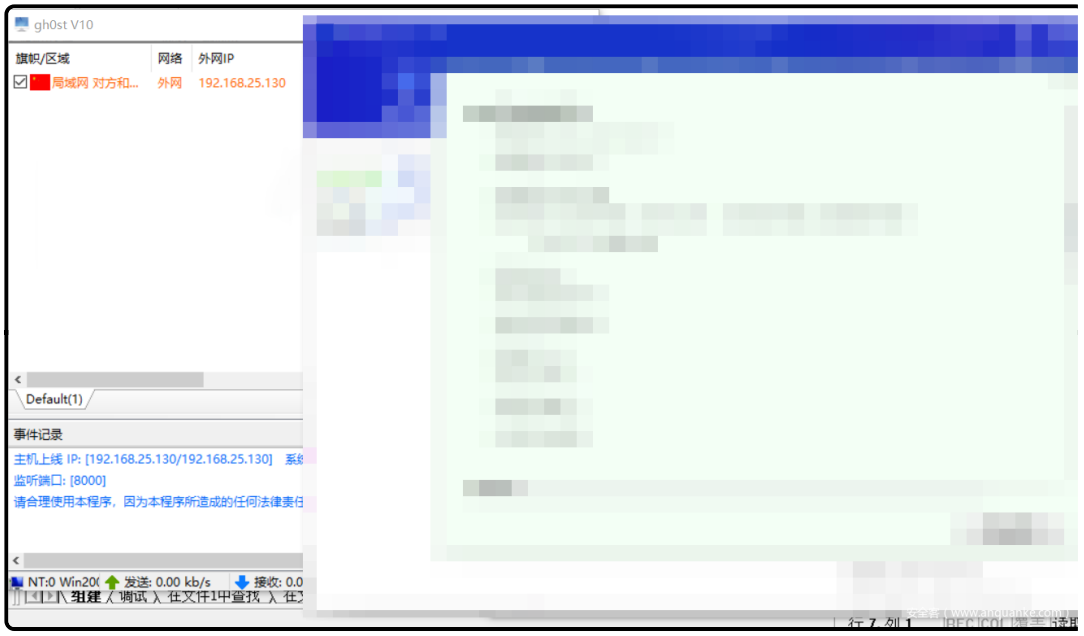
在这里有一个注意点，笔者用的这个地址加密不只有Base64，还有Rc4，所以大家解不开是正常的。



这就是上面提到的思路，他是一个加载器（或者通俗点下载者），其作用是：

解密 ==> 加密后的地址 ==> 下载文件到内存 ==> 执行

测试上线，这里选择虚拟机测试，懂得都懂，毕竟后门或者啥的我也没仔细去看。



经测试，国内企业杀软，以及Tinder无感执行。至于微步云沙箱或者别的沙箱，笔者就不上传了，免得被记录特征导致代码失效。