



Ele

📅 2021-09-01 | 📁 Challenge , 2021 , 工业信息安全技能大赛 , 巡回赛-杭州站

Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-杭州站 | Ele

[点击此处](#)获得更好的阅读体验

WriteUp来源

来自 **Venom** 战队

题目描述

工程师发现电力网络中存在异常流量，尝试通过分析流量包，分析出流量中的异常数据，并拿到FLAG，flag形式为 flag{}

题目考点

- 流量分析
- GOOSE协议

解题思路

分离出goose包，发现所有PDU 的data值都是 **VBfMWV**

goose.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
351	28.306296	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	167	
352	28.306300	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	167	
353	28.306385	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	161	
354	28.306392	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	161	
355	28.306590	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
356	28.306593	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
357	28.307132	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	163	
358	28.307136	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	163	
359	28.307212	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	153	
360	28.307216	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	153	
361	29.315427	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	167	
362	29.315431	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	167	

<

timeAllowedtoLive: 2000
datSet: SHR_UDM5LD0/LLN0\$dsGOOSE0
goID: SHR_UDM5LD0/LLN0\$GO\$gocb0
t: Jul 20, 2021 12:45:32.568999946 UTC
stNum: 3
sqNum: 800
test: True
confRev: 1
ndsCom: False
numDatSetEntries: 6
▼ allData: 6 items
 > Data: integer (5)
 > Data: integer (5)
 > Data: integer (5)
 > Data: integer (5)
 > Data: integer (5)
 > Data: integer (5)

0000	00 ff 1a 67 87 f4 e8 7a 64 45 1f 26 81 00 00 00	...g...z dE.&...
0010	88 b8 00 08 00 92 00 00 00 00 61 82 00 86 80 19a.....
0020	53 48 52 5f 55 44 4d 35 4c 44 30 2f 4c 4c 4e 30	SHR_UDM5 LD0/LLN0
0030	24 47 4f 24 67 6f 63 62 30 81 02 07 d0 82 19 53	\$GO\$gocb 0.....S
0040	48 52 5f 55 44 4d 35 4c 44 30 2f 4c 4c 4e 30 24	HR_UDM5L D0/LLN0\$
0050	64 73 47 4f 4f 53 45 30 83 19 53 48 52 5f 55 44	dsGOOSE0 ..SHR_UD
0060	4d 35 4c 44 30 2f 4c 4c 4e 30 24 47 4f 24 67 6f	M5LD0/LL N0\$GO\$go
0070	63 62 30 84 08 60 f6 c5 6c 91 a9 fb 00 85 01 03	cb0...`.. 1.....
0080	86 02 03 20 87 01 01 88 01 01 89 01 00 8a 01 06
0090	ab 12 85 01 56 85 01 42 85 01 66 85 01 4d 85 01	...V...B ..f..M..
00a0	57 85 01 56	W..V

当 `goose.apid==8` 时，Data有变化

https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/巡回赛-杭州站/7jmwXGJMU6jmwZufRyQEZu.html

2/6

goose.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

goose.apid=8

o.	Time	Source	Destination	Protocol	Length	Info
1232	118.758244	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1241	119.768446	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1242	119.768452	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1251	120.780666	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1252	120.780669	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1261	121.687199	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1262	121.687204	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1271	121.804186	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1272	121.804191	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1281	122.815750	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1282	122.815754	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1291	123.825776	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	

```
timeAllowedtoLive: 2000
datSet: SHR_UDM3LD0/LLN0$dsGOOSE0
goID: SHR_UDM3LD0/LLN0$GO$gocb2
t: Jul 20, 2021 14:36:23.122999966 UTC
stNum: 31
sqNum: 385
test: True
confRev: 1
ndsCom: False
numDatSetEntries: 6
```

allData: 6 items

- > Data: integer (5)
- > Data: integer (5)
- > Data: integer (5)
- > Data: integer (5)
- > Data: integer (5)
- > Data: integer (5)

```
0000 00 ff 1a 67 87 f4 e8 7a 64 45 1f 26 81 00 00 00 ...g...z dE.&...
0010 88 b8 00 08 00 92 00 00 00 00 61 82 00 86 80 19 .....a.....
0020 53 48 52 5f 55 44 4d 33 4c 44 30 2f 4c 4c 4e 30 SHR_UDM3 LD0/LLN0
0030 24 47 4f 24 67 6f 63 62 32 81 02 07 d0 82 19 53 $GO$gocb 2.....S
0040 48 52 5f 55 44 4d 33 4c 44 30 2f 4c 4c 4e 30 24 HR_UDM3L D0/LLN0$
0050 64 73 47 4f 4f 53 45 30 83 19 53 48 52 5f 55 44 dsGOOSE0 ..SHR_UD
0060 4d 33 4c 44 30 2f 4c 4c 4e 30 24 47 4f 24 67 6f M3LD0/LL N0$GO$go
0070 63 62 32 84 08 60 f6 df 67 1f 7c ed 00 85 01 1f cb2...`.. g.|.....
0080 86 02 01 81 87 01 01 88 01 01 89 01 00 8a 01 06 .....
0090 ab 12 85 01 4d 85 01 5a 85 01 57 85 01 47 85 01 ..M..Z ..W..G..
00a0 43 85 01 5a C..Z
```

goose.appid=8

No.	Time	Source	Destination	Protocol	Length	Info
1522	147.145858	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1531	148.155830	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1532	148.155833	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1541	149.167352	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1542	149.167355	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1551	150.177995	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1552	150.177998	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1561	150.493773	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1562	150.493779	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1571	151.188059	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1572	151.188062	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	
1581	152.263621	e8:7a:64:45:1f:26	00:ff:1a:67:87:f4	GOOSE	164	

timeAllowedtoLive: 2000
 datSet: SHR_UDM3LD0/LLN0\$dsGOOSE0
 goID: SHR_UDM3LD0/LLN0\$GO\$gocb2
 t: Jul 20, 2021 14:36:23.122999966 UTC
 stNum: 31
 sqNum: 385
 test: True
 confRev: 1
 ndsCom: False
 numDatSetEntries: 6

▼ allData: 6 items

- > Data: integer (5)
- > Data: integer (5)
- > Data: integer (5)
- > Data: integer (5)
- > Data: integer (5)
- > Data: integer (5)

0000	00 ff 1a 67 87 f4 e8 7a 64 45 1f 26 81 00 00 00	...g...z dE-&....
0010	88 b8 00 08 00 92 00 00 00 00 61 82 00 86 80 19a.....
0020	53 48 52 5f 55 44 4d 33 4c 44 30 2f 4c 4c 4e 30	SHR_UDM3 LD0/LLN0
0030	24 47 4f 24 67 6f 63 62 32 81 02 07 d0 82 19 53	\$GO\$gocb 2.....S
0040	48 52 5f 55 44 4d 33 4c 44 30 2f 4c 4c 4e 30 24	HR_UDM3L D0/LLN0\$
0050	64 73 47 4f 4f 53 45 30 83 19 53 48 52 5f 55 44	dsGOOSE0 ..SHR_UD
0060	4d 33 4c 44 30 2f 4c 4c 4e 30 24 47 4f 24 67 6f	M3LD0/LL N0\$GO\$go
0070	63 62 32 84 08 60 f6 df 67 1f 7c ed 00 85 01 1f	cb2...`.. g.
0080	86 02 01 81 87 01 01 88 01 01 89 01 00 8a 01 06
0090	ab 12 85 01 33 85 01 33 85 01 4d 85 01 5a 85 01	...3..3 ..M..Z..
00a0	4e 85 01 44	N..D


```
>>> import base64
>>> base64.b32decode("MZWGCZ33MZNDsv2SKZYGGM
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
  File "D:\Python27\lib\base64.py", line 205
    raise TypeError('Incorrect padding')
TypeError: Incorrect padding
>>> base64.b32decode("MZWGCZ33MZNDsv2SKZYGGM
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
  File "D:\Python27\lib\base64.py", line 205
    raise TypeError('Incorrect padding')
TypeError: Incorrect padding
>>> base64.b32decode("MZWGCZ33MZNDsv2SKZYGGM
'flag{fZ9WRVpc0FL0xt1U}'
```



提取得到字符串：`MZWGCZ33MZNDsv2SKZYGGMCGJQYFQ5DMKV6Q`，解三次base32就可以得到flag了

Flag



```
1  flag{fZ9WRVPC0FL0XT1U}
```

本文作者： CTFHub


本文链接： <https://writeup.ctfhub.com/Challenge/2021/工业信息安全技能大赛/巡回赛-杭州站/7jmwXGJMU6jmwZufRyQEZu.html>

版权声明： 本博客所有文章除特别声明外，均采用 [CC BY-NC-SA](#) 许可协议。转载请注明出处！

[# Challenge](#) [# 2021](#) [# 工业信息安全技能大赛](#) [# 巡回赛-杭州站](#)

[< PCZ](#)

[mod traffic >](#)

© 2019 – 2022  CTFHub
由 [Hexo](#) & [NexT.Gemini](#) 强力驱动