



16

📅 2021-08-30 | 📁 Challenge , 2021 , 工业信息安全技能大赛 , 巡回赛-兰州站

Challenge | 2021 | 工业信息安全技能大赛 | 巡回赛-兰州站 | 16

[点击此处](#)获得更好的阅读体验

WriteUp来源

来自 M01N 战队

题目描述

在某次对某工业企业进行检查评估工作时，发现了疑似感染恶意软件的上位机。现已提取出上位机的网络通信流量，通过数据包分析找到其中的隐藏信息。

题目考点

- 流量分析

解题思路

找到可疑字符串：666c61677b3768464d32536c596764507a7d 直接解hex即可

16.cap

应用显示过滤器: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
630	0.081632905	Universa_f7:ca:39	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.243
631	0.082632600	Universa_f7:ca:39	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.243
632	0.086537671	0001	00a8	SNA	602	Subarea Node <--> PU2
633	0.086537771	0001	00a8	SNA	602	Subarea Node <--> PU2
634	0.086537771	00:e2:36:0b:19:2b	Broadcast	ARP	60	ARP Announcement for 192.168.1.181
635	0.091014434	192.168.1.123	192.168.1.181	UDP	60	64406 -> 11000 Len=18
636	0.091178704	192.168.1.181	192.168.1.123	UDP	60	11000 -> 64406 Len=10
637	0.091178998	192.168.1.123	192.168.1.181	UDP	60	64406 -> 11000 Len=18
638	0.091360677	192.168.1.181	192.168.1.123	UDP	60	11000 -> 64406 Len=10
639	0.091360935	192.168.1.123	192.168.1.181	UDP	59	64406 -> 11000 Len=17
640	0.091511214	192.168.1.181	192.168.1.123	UDP	60	11000 -> 64406 Len=10
641	0.091511595	192.168.1.123	192.168.1.181	UDP	62	64406 -> 11000 Len=20
642	0.091661607	192.168.1.181	192.168.1.123	UDP	60	11000 -> 64406 Len=10
643	0.091661962	192.168.1.123	192.168.1.181	UDP	62	64406 -> 11000 Len=20
644	0.091662638	0001	00a8	SNA	602	Subarea Node <--> PU2
645	0.091662872	0001	00a8	SNA	602	Subarea Node <--> PU2
646	0.091662872	00:e2:36:0b:19:2b	Broadcast	ARP	60	ARP Announcement for 192.168.1.181
647	0.091812274	192.168.1.181	192.168.1.123	UDP	60	11000 -> 64406 Len=10
648	0.091813108	192.168.1.123	192.168.1.181	UDP	180	64406 -> 11000 Len=137

> Frame 648: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface 0

> Ethernet II, Src: VMware_0a:63:9f (00:0c:29:0a:63:9f), Dst: 00:e2:36:0b:19:2b

> Internet Protocol Version 4, Src: 192.168.1.123, Dst: 192.168.1.181

> User Datagram Protocol, Src Port: 64406, Dst Port: 11000

> Data (137 bytes)

Data: 0d00d73f8900240026272527000077000000110062000000... [Length: 137]

> VSS Monitoring Ethernet trailer, Source Port: 0

分组: 1665 · 已显示: 1665 (100.0%)

Last build: 5 months ago

Recipe

From Hex

Delimiter: Auto

Input

666c61677b3768464d32536c596764507a7d

Output

flag{7hFM2SlYgdPz}

CTFHub

Flag



1 flag{7hFM2SlYgdPz}

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-兰州站/vBT5FpGpF7g3CXHJc3X4ap.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-兰州站](#)

< 08

msbackdoor >

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