NBP

浅探百度网盘下载逻辑

01 基本准备

501P US PoorMan

○4 买一送 一> RESTful框架 双栈下载

01

基本准备

优雅使用wireshark:

https://zhuanlan.zhihu.com/p/36669377

对PC端抓包:

https://www.cnblogs.com/gancuimian/p/14010628.html





-	Cast II day II days					
	Tink	- James	becomes .	Pyrophist	louit lev	5540
	636.3.32889	231.310.10.00	\$8,38,265.00	109	82 888 - 888 (ACE) heg-220 bin-cell allevialit Lavia	
	330 0.308144	131.00.10.85	38.38.343.83	309	82 440 + 9364 (ACC) 3ep-326 Act=0003 HER-40403 Lamb	=
	546.3.329668	121-229-129-77	38,38,345.90	71.9(1.3	394 Server Mally, Change Cipher Spen, Concupted Extensions, Yanished	-
	541 5 398314	38,38,343.61	321-328-136-77	TUBUS.B	355 Shange Eigher Novo, Finished	
	542 3,100004	28.28.267.62	321.228.529.77	HTTPS	sec magic, settimen(e), admony penerg(e)	=
	149 3.338625	38.38,345.65	321.228.120.77	WITTER	44T #EADDIS[1]: OFTIONS / Nercodes/producedko-jik-vilk-vilk-vilk-vilk-vilk-vilk-vilk-vi	-
	544-3,336768	J21 330 19 95	38/28/263-03	707	82 445 - 9554 (ACE) 5ep-026 Acts 1714 Min-68652 Lanes	
	600 31,488622	220.228.128.77	36.38.243.65	TEP	SE BIS 4 WIND [ACC] REQUEST AND ADDRESS AN	-=
	AM: 3,333034	221.320.126.77	38,38,363.63	HITHE	iss serioss[e], socos_serie[e], serioss[e]	- 25
	947 3,1538W	20.28.247.61	333.339.130.77	HTTVL:	#S SETTINGS[#]	-
	548 5,355885	18,28,245,62	381.89.324.78	105	54 555 - 445 (ACE) Repulsive Acceptable storollilla Lerne	- 8
	509.0.365028	321.110.19.86	38.38.741.63	HTTPS:	NAX HEADERS[1] 284 No Combert	
	350 J. 00000	20,20,267,07	221.230.20.40	HITTEL	ser planted(A) mil /apl/getmoster/large-relication-lettrases	
	250 3 381422	121 136 19 35	38.38.345.65	HITEL:	240 MANUSCIT - 284 in Contact	_
	349 3/3KEN94	H-SEJO/H	EEE-200-39-84	TEP	90 NEXT - 440 (578) 160/8 H(4/04200 (201/0 PER/10/10/10/10/10/10/10/10/10/10/10/10/10/	
	962 3,380278	- 123.130.18.86	00.00.001.01	HULLUT :	Bay widehit(t): (but his content	-
	661.2 (36677)	28,28,245,61	321.130.19.36	308	SE NISA - 460 [ACE] Sep-2107 ACE-CTMR ASS-CITERS Lett-4	
	564.3.167678	38.38.343.65	321,130,19,65	HETPS:	188 MIADES[L1]: GET /api/top/list?lang=rrSis=188/MiADEShips-20	_
	565 5 349525	221, 230, 29, 95	38.29.243.63	HITTEL	\$42 HEADERS(7): 284 No Content	_
	300.1.10001	34.24.207.45	202:330.00.00	HITPL	per entremains). set /www.lefullang.ordfrom.lnunktu.tespensense	-
1 1979	Seri verismi I.I.40					_
	wer Longton 7					
	mer version					
	size congre: 6					
	wliw: 1.3.40					
	Descriped: 1.5.201					
	epresentation Literal	Header Field with In-	creserval bedeater +	Sent Asser		
	Ser: sec-ch-up-mobile: 1					
			b: Mieda; x84) April d	etilit/107.36	(000%, Libs Series) Chroma/129, 8.0.8 Sefara/517.18	
	her wormen't application					
	mer: Fg: ThysDecastraggs					BU UK
			VC29, vv1Fwi000132903	rysideceny/files/fi	0x200w/MAG WWGLC Langtot (Edward FASET Later Accident with region of Microsoft Accident (ASET ACCIDENT CONTROL OF ACCIDENT ACCIDENT CONTROL OF ACCIDENT ACCI	
	der: sec-th-se-platform					
1 Heat			rhochici Lighterlie			
	der: origin: strone-esta		OR OR OTHER PROPERTY.			
7, 1969	der: erigin: shrome-e-ta der: esc-fatch-site: ora	se-site				
1 190 1 100		na-cité				
- 100	der: eac-fittch-site; orv	sa-site				
7 1969 - Head	der: sac-fetch-süte: dru was length: 14	sse-site				
- Hab	der: sez-fetch-süte; orv une length: 14 www.:sez-fetch-site	us-site				
Hara	Ser: saz-fetch-site: srv bna length: 14 bnu: saz-fetch-site Wiwe Length: 18	ma-site				

	LEGISS - Cylvia				□ •
No	Time	Surre	Deprination:	Protocii	Length Tefs
1	38769 3.689526	2489 8749;715c;481 8999;;90	2488:8848:0518:6556:e551:389a:e584:65c7	TOP	1374 [TCP Out-Of-Order] 440 + 6329 [ACK] Seq=14733862 Ack=2784 Wine727
	38779 3.689525	2408:E746:72fc:481:8888::98	2488:8448:8518:0f66:e9f1:989ace58d:8fc7		1374 [TCP Dut-Of-Order] 443 + 8229 [ACK] Seq=14732562 Ack=2784 Win=725
ll .	38772 3:889526	2488:E748:73fc:483:5809::56	248818448185181856565671158991658d:6fc7		3374 [TCF Out-Of-Order] 443 + 8329 [ACK] Seq=54793262 Ack+2784 Win+727
	38772 3.689581	2488:8440:b510:6f66:e9f1:989a:e58d:6fc7	2488:8748:71fc:481:8888::58	TCP	74 6329 + 443 [ACK] 5eq+2784 ACK+14736462 Nin+2188736 Len+8
	38773 3.689687	192.168.76.123	181.69.194.222	TCP	54 6338 - 443 [ACK] Seq=2076 Ack=2569887 Win=527636 Len=0
	30774-3:449711	BIMI(491940222)	192.168.76.113	TL5V1.2	1414 [TCF Previous segment not deptimed] y Ignores Unknown Mecord
	30775 3.609711	181,49,394,222	192 168 76 323	†#	1414 [TCF Out-Of-Order] 441 + 6338 [ACK] Seq-2569887 Ack+2076 Min+7276
	38776 3.689757	192.168,76.123	101.69.194.222	TCP	54 6338 * 443 [ACK] Seq*2076 Ack*2572607 Win*527616 Len+0
_	38777 3,689911	181.69.194,322	192,168,76,123	TI SVI. 2	1414 Tenoned Jinkman Record
1	38778 3 689911	181.69.154.222	192,168,76,123	Ti.5y11	1414 [TCP Previous segment not captured] , Igeores Unknown Record
1	38779 1.369911	191,99494,222	194, 168, /6, 123	167	1414 [NCF OUT-OF-OFOSF] 448 4 8381 [MCK] SEQ-18211886 ACC42843 WINFIZA
	30788 3.589911	181,49,194,222	192,168,76,123		1414 [TCF Dut-CF-Order] 445 + 6331 [4CX] Seq=18289646 Act=2843 Win=727
l	39781 13: 509911	181,69,164,222	192,168,76,123		1414 [TCP Out-Of-Order] 441 + 6331 [ACK] Sep-18038236 Ack-2043 Win-727
1	38782 -3,609911	181.89 (94)222	192,169,76,123		1414 [TCF OVE-OF-Order] 443 + 6331 [ACX] Seq=58288926 ACE=2843 Win=723
H.	39783 -3: 699911	181.69.154.222	192,168,76,123		1414 [TCP Out-Of-Order] 441 + 6333 [ACK] Seq=10295566 Ack=2043 Min=727
Г	38784 3.689911	181,65,194,222	197,188,76,123	TL501.2	1434 [TCP Previous segment not captured] , Ignored Unknown Record
	39785 3.489911	181,85,134,222	192:180:76:123		1414 [TCP Out-Of-Order] 441 - 6338 [ACX] Seg-2573967 Ack+2876 kin+7276
	38705 31609911	191.69:194:222	192,188,76,123		1414 [TCP Out-Of-Order] 441 + 6338 [ACK] 540=2572687 Ack=2076 Win=7274

基本准备

优雅使用wireshark:

https://zhuanlan.zhihu.com/p/36669377

对尸[端抓包:

https://www.cnblogs.com/gancuimian/p/14010628.html



Wireshark

Fiddler+proxifier



基本准备

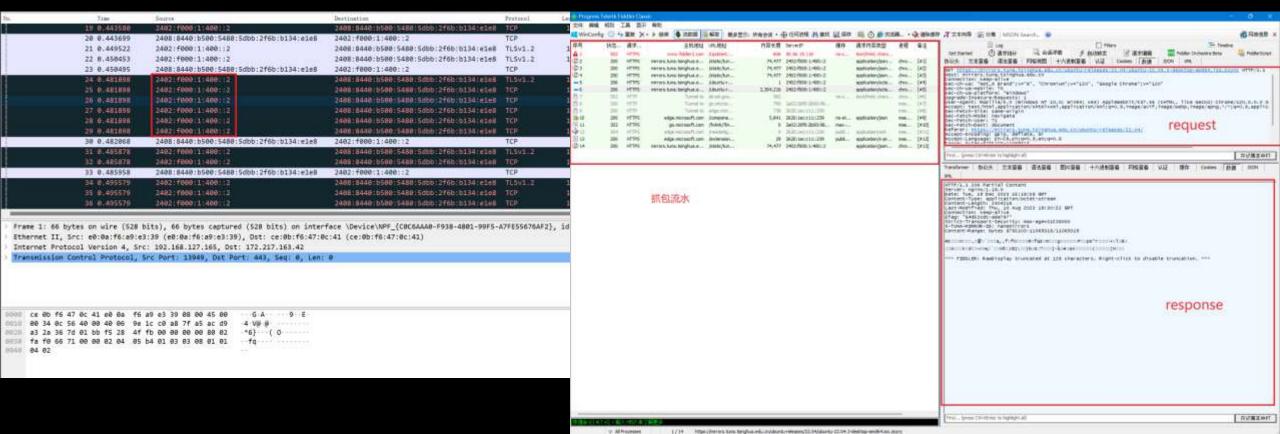
优雅使用wireshark:

https://zhuanlan.zhihu.com/p/36669377

对尸[端抓包:

https://www.cnblogs.com/gancuimian/p/14010628.html





网页端 US 客户端

- 01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx
- 02 从清华镜像网站下载 4167029 字节 ubuntu-22.04.3-live-server-amd64.iso.zsync
- 03 从百度客户端登录并下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

12对比,观察百度网盘 (PanBD) 网页端和一般下载网站的下载区别

13对比,观察PanBD网页端和客户端的下载区别

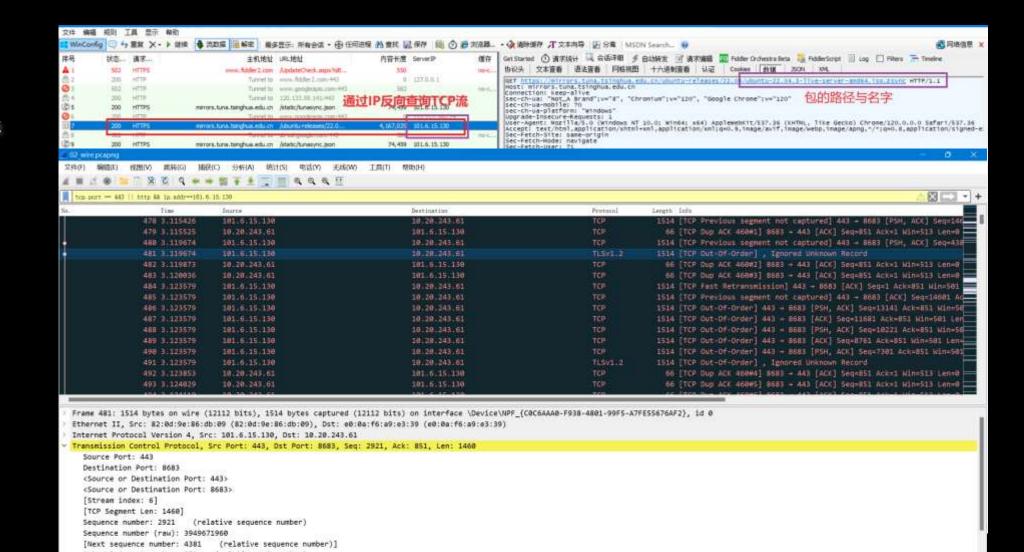
01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

02 从清华镜像网站下载 4167029 字节 ubuntu-22.04.3-live-server-amd64.iso.zsync

02

网页端 US 客户端

TCP下载证明: 以包02为例 找到下载的包的报文, 通过IP反向观察wireshark数据流



02

网页端 US 客户端

01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

02 从清华镜像网站下载 4167029 字节 ubuntu-22.04.3-live-server-amd64.iso.zsync

TCP下载证明: 对01包和03包做相同处理, 结果一致 证毕

	ping				- o x
文件(f) 编	BIE) BURNY) IRRO(G) MIRRY	O SHIA MESS MESS ES	(W) IM(f) ##00·f)		
4 1 4 4	8 2 2 8 2 4 + +	報子主言 医电电压			
trp 8t	up Attp5 tup.port == 443 AA	ip. e62:=119.167.143,94			<u> </u>
No.	Tine :	Fourte .	Pestination	Frotocol	Length Info
	4429 24.646388	10.20.243.61	119.167.143.56	TLSv1.2	180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess
	4432 24.684881	119.167.143.56	18.28.243.61	TLSv1.2	328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Messa
	4433 24.684081	119,167,143,56	18.28.243.61	TCP	60 443 = 5889 [ACK] Seq=3461 Ack=308 Win=30464 Len=0
	4436 241695511	18.26.343.61	119.167.143.56	TCP	458 [TCF Previous segment not captured] \$800 - 443 [PSH, ACK] Seg-174
	4448 24:785709	119,167,143,55	10.20.243:61	TCP	60 [TCP ACKed unseen segment] 443 - 5800 [ACK] Seg-3735 Ack-2164 Wir
	4458 25.148397	119.167.143.56	18.20.243.61	TEP	1514 443 + 5889 [ACK] Seq=3735 Ack=2164 Min=34848 Len=1468 [TCP segmen
	4459 25,148631	119.167.143.56	18,28,243.61	TCP	1514 [TCP Previous segment not captured] 443 - 5889 [ACK] Seq=16875 Ac
	4468-25,148631	119.167.148.56	10.20.243.61	TCP	1514 [TCP Out-Of-Order] 445 - 5889 [ACK] Seq=15415 Ack=2168 Min=34848 -
	4461 25,148631	119.567.143.56	10.20.243.61		1534 [TCP Out-Of-Order] 443 - 5889 [ACK] Seq=15955 Ack=2164 Min=34848
l wreper	ping				= 9 3
Chiff and	BIE) RASSION MERCIGO MIGRA	SHIA MINS MEN THE	(W) IB(I) ##0H		
CHT(F) MA					
	THE PERSON WAS SELECTION	# * * 3 = 4 4 4 E			
M 25 6	THE PERSON WAS SELECTION	据事业 <u>录量</u> 电电电阻			
H 25 6	* * * P 3 8 = #	据事业 <u>录量</u> 电电电阻		Tratoosi	Length Tofo
m it e	8 12	#####################################		Fratoccil TCP	
m it e	8 = 7 R & Q + + to trap5 top poet = 443 in The-	報 本 ま 및 豊 鬼 鬼 鬼 旺 (a. allo-till, ill, ill, left Postre	Bestization		Leverth Torto 66 13525 - 443 [ACK] Seq=152 Ack=3457 Min=132896 Len=8 SLE=2921 SRE=
H 25 6	8 1	## # # ## ## ## ## ## ## ### #########	Destination 113:137.57.249	TCP	Leverth Torto 66 13525 - 443 [ACK] Seq=152 Ack=3457 Min=132896 Len=8 SLE=2921 SRE=
H 25 6	8 10 7 2 8 9 4 40 14 10 11 targe 11 tee peer = 440 84 Time 51644 98.853615 51645 98.855482	in add—111 107, 07, 248 Fearre 18.28, 243, 61 19.28, 243, 61	Bestination 113:137.57.249 113:137.57.249	TCP TLSv1.2	Leverh Info 66 13525 + 443 [ACK] Seq=152 Ack=3457 Min=132896 Len=8 SLE=2921 SRE= 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess
H 25 6	8 12 2 2 4 4 1	6 4 4 5 4 4 4 11 10 44/-111 137 37 248 Fearre 10 .20 .243 .61 113 .137 .57 .249	Destination 113:137.57.249 113:137.57.249 18:28:243.61	TCP TLSv1.2 TLSv1.2	Leverh Info 66 13525 * 443 [ACK] Seq=152 Ack=3457 Min=132896 Len=8 SLE=2921 SRE= 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess 196 New Session Ticket, Change Cipher Spec, Encrypted Handshake Messa
H 25 6	51644 98.053615 51645 98.055482 51646 98.86583 51647 98.88683	in elf=U1 137, 157, 245 Fourse 10, 20, 243, 61 10, 20, 243, 61 113, 137, 57, 249 113, 137, 57, 249	Destination 113.137.57.249 113.137.57.249 18.26.243.61 16.26.243.61	TCP TLSV1.2 TLSV1.2 TCP	Lmarii Info 66 13525 - 443 [ACK] Seq=152 Ack=3457 Min=132896 Len=8 SLE=2921 SRE= 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess 296 Mew Session Ticket, Change Cipher Spec, Encrypted Handshake Mess 68 443 - 13525 [ACK] Seq=3457 Ack=278 Min=38464 Len=8
H 25 6	8 1 2 2 2 43 44 The 51644 98.853615 51645 98.853615 51646 98.85683 51647 98.88683 51648 98.89683	in abt=111 137.37.24# Fearte 18.28.243.61 18.38.243.61 113.137.57.249 18.28.243.61	Decitation 113:137:57:249 113:137:57:249 18:28:243:61 18:28:243:61 113:137:57:249	TCP TLSvi.2 TLSvi.2 TCP TCP	Lmarh Info 66 13525 + 443 [ACK] Seq+152 Ack=3457 Min=132896 Len=8 SLE=2921 SRE= 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess 196 New Session Ticket, Change Cipher Spec, Encrypted Handshake Mess 66 443 = 13525 [ACK] Seq=3457 Ack=278 Min=34464 Len=8 54 13825 + 443 [FIN, ACK] Seq=278 Ack=3690 Min=131848 Len=0
H 25 6	8 12 2 2 4 43 44 Time 51644 98.853615 51645 98.855482 51646 98.866883 51647 98.886883 51648 98.64633 51648 98.64633 51668 98.115787	is add=111 137, 37, 248 le 26, 243, 61 10, 26, 243, 61 113, 137, 57, 249 113, 137, 57, 249 113, 137, 57, 249 113, 137, 57, 249 113, 137, 57, 249	Destination 113:137.57.249 113:137.57.249 18:28:243.61 18:28:243.61 113:137.57.249 18:28:243.61	TCP TLSv1.2 TLSv1.2 TCP TCP TCP	Learn Info 66 13525 + 443 [ACK] Seq=152 Ack=3457 Min=132896 Len=8 SLE=2921 SRE= 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess 196 New Session Ticket, Change Cipher Spec, Encrypted Handshake Mess 68 443 = 13525 [ACK] Seq=3457 Ack=278 Min=38464 Len=8 54 13825 = 443 [FIN, Ack] Seq=278 Ack=279 Min=33484 Len=8 68 443 = 13525 [ACK] Seq=3698 Ack=279 Min=38464 Len=8
H 25 6	8 1 2 2 2 4 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1	10. 267-111 137. 37.248 Fearre 10. 20. 243. 61 10. 20. 243. 61 113. 137. 57. 249 113. 137. 57. 249 113. 137. 57. 249 113. 137. 57. 249	Destination 113:137:57:249 113:137:57:249 18:26:243:61 16:26:243:61 113:137:57:249 18:26:243:61 18:20:243:61	TCP TLSv1.2 TLSv1.2 TCP TCP TCP TCP	LmarN Info 66 13525 ~ 443 [ACK] Seq=152 Ack=3457 Min=132896 Len=8 SLE=2921 SRE= 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess 196 New Session Ticket, Change Cipher Spec, Encrypted Handshake Mess 68 443 ~ 13525 [ACK] Seq=3457 Ack=278 Min=38464 Len=8 54 13825 ~ 443 [FIN, ACK] Seq=278 Ack=3600 Min=1384e Len=0 68 443 ~ 13525 [ACK] Seq=3690 Ack=279 Min=38464 Len=8 50 443 ~ 13525 [FIN, ACK] Seq=3690 Ack=279 Min=38464 Len=8
H 25 6	8	in wir-til 17. 17.24f Forme 19.29.243.61 19.28.243.61 113.137.57.249 113.137.57.249 113.137.57.249 113.137.57.249 113.137.57.249 113.137.57.249 113.137.57.249	Pertination 113:137:57:249 113:137:57:249 18:26:243:61 16:26:243:61 113:137:57:249 18:26:243:61 18:28:243:61 113:137:57:249	TCP TLSv1.2 TLSv1.2 TCP TCP TCP TCP	LmarN Info 66 13525 ~ 443 [ACK] Seq=152 Ack=3457 Min=132896 Len=0 SLE=2921 SRE= 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess 296 Mew Session Ticket, Change Cipher Spec, Encrypted Handshake Mess 60 443 ~ 13525 [ACK] Seq=3457 Ack=278 Min=38464 Len=0 54 13525 * 443 [FIN, ACK] Seq=278 Ack=3620 Min=131848 Len=0 60 443 ~ 13525 [ACK] Seq=3699 Ack=279 Min=38464 Len=0 60 443 ~ 13525 [ACK] Seq=279 Ack=3700 Min=31848 Len=0 54 13525 ~ 443 [ACK] Seq=279 Ack=3700 Min=131848 Len=0
H 25 6	8	Forme 18.28.243.61 18.28.243.61 18.37.57.249 18.28.243.61 113.137.57.249 18.28.243.61 113.137.57.249 18.28.243.61 113.137.57.249 18.28.243.61 113.147.57.240 18.28.243.63	Destitation 113:137:57:249 113:137:57:249 18:28:243:61 18:28:243:61 113:137:57:249 18:28:243:61 113:137:57:249 113:137:57:249 113:137:57:249	TCP TLSv1.2 TLSv1.2 TCP TCP TCP TCP TCP TCP TCP TCP	Lmarn Info 66 13525 + 443 [ACK] Seq=152 Ack=3457 Min=132896 Len=8 SLE=2921 SRE= 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess 296 New Session Ticket, Change Cipher Spec, Encrypted Handshake Mess 60 443 = 13525 [ACK] Seq=3457 Ack=278 Min=38464 Len=8 54 13525 + 443 [FIN, ACK] Seq=278 Ack=1690 Min=131848 Len=0 60 443 = 13525 [ACK] Seq=3699 Ack=279 Min=38464 Len=8 60 443 = 13525 [FIN, ACK] Seq=2899 Ack=279 Min=38464 Len=8 54 13525 = 443 [ACK] Seq=299 Ack=3706 Min=131848 Len=8 65 13542 = 88 [SVN] Seq=8 Win=64248 Len=8 MSS=1668 MS=256 SACK PERM=
H & 6	5 1644 98.053615 51645 98.053615 51646 98.055482 51646 98.086883 51647 98.086883 51648 96.04633 51668 98.125707 51661 98.126270 51662 98.125707 51663 98.125707 51663 98.125707 51664 98.12670 51664 98.12670 51664 98.12670	is abi	Decidation 113:137:57:249 113:137:57:249 18:28:243:61 18:28:243:61 113:137:57:249 18:28:243:61 18:28:243:61 18:3137:57:249 113:137:57:249 113:137:57:249 18:28:243:61	TCP TLSv1.2 TLSv1.2 TCP	Learn Info 66 13525 + 443 [ACX] Seq=152 Ack=3457 Min=132896 Len=8 SLE=2921 SRE= 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess 196 New Session Ticket, Change Cipher Spec, Encrypted Handshake Mess 60 443 - 13525 [ACX] Seq=3457 Ack=278 Min=38464 Len=8 54 13525 + 443 [FIN, ACX] Seq=278 Ack=1690 Min=131848 Len=8 60 443 - 13525 [ACX] Seq=3698 Ack=279 Min=38464 Len=8 60 443 + 13525 [ACX] Seq=3698 Ack=279 Min=38464 Len=8 54 13525 + 443 [ACX] Seq=279 Ack=3788 Min=31848 Len=8 66 13542 + 88 [SVN] Seq=8 Win=64248 Len=8 VISS=1468 WS=256 SACX_PERV= 66 88 - 13542 [SVN, ACX] Seq=8 Ack=1 Min=8192 Len=8 VSS=1452 MS=32 S
H & 6	51644 98.853615 51645 98.855482 51646 98.865883 51647 98.886883 51647 98.886883 51648 98.826883 51648 98.125787 51661 98.126278 51662 99.126339 52946 186.383571 52947 186.334935 52948 186.335101	In addr=U1 137.17.24f Fearte 19.26.243.61 19.26.243.61 113.137.57.249 113.137.57.249 113.137.57.249 113.137.57.249 113.137.57.249 113.137.57.249 113.137.57.249 113.137.57.249 113.137.57.249	Destination 113.137.57.249 113.137.57.249 18.26.243.61 18.26.243.61 113.137.57.249 18.26.243.61 113.137.57.249 113.137.57.249 113.137.57.249 113.137.57.249 113.137.57.249	TCP TLSv1.2 TLSv1.2 TCP	Lmarn Info 66 13525 = 443 [ACK] Seq=152 Ack=3457 Min=132896 Len=8 SLE=2921 SRE= 188 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messl 196 New Session Ticket, Change Cipher Spec, Encrypted Handshake Messl 60 443 = 13525 [ACK] Seq=3457 Ack=278 Min=38464 Len=8 54 13825 = 443 [FIN, ACK] Seq=278 Ack=3600 Min=131848 Len=0 60 443 = 13525 [ACK] Seq=3699 Ack=279 Min=38464 Len=8 60 443 = 13525 [FIN, ACK] Seq=2898 Ack=279 Min=38464 Len=8 54 13525 = 443 [ACK] Seq=279 Ack=3780 Min=131848 Len=8 65 13542 = 88 [SVN] Seq=8 Min=64248 Len=8 NSS=1460 NS=256 SACK_PERM= 66 80 = 13542 [SVN, ACK] Seq=8 Ack=1 Min=8102 Len=8 NSS=1452 WS=32 S 54 13542 = 88 [ACK] Seq=1 Ack=1 Win=110006 Len=8

02

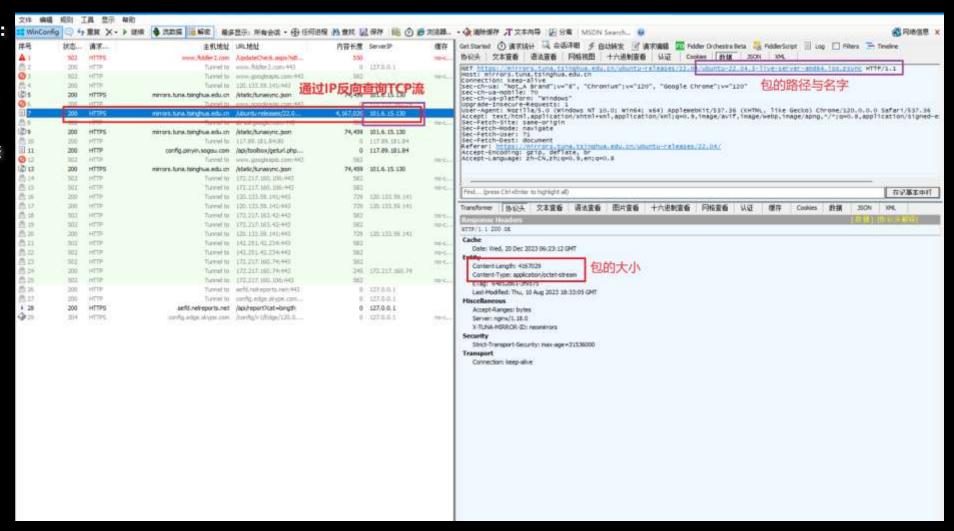
网页端 US 客户端

01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

02 从清华镜像网站下载 4167029 字节 ubuntu-22.04.3-live-server-amd64.iso.zsync

一般下载网站 VS PanBD网页端:

先看一般网站的下载,可以发现来往报文 http首部相对简洁,自定义字段并不多,也 没有cookies或者request URL 自定义字段在图中给出了说明 当然,这只是个例网站,仍有以偏概全之嫌



网页端 US 客户端

01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

02 从清华镜像网站下载 4167029 字节 ubuntu-22.04.3-live-server-amd64.iso.zsync

一般下载网站 VS PanBD网页端:

先看一般网站的下载,可以发现来往报文 http首部相对简洁,自定义字段并不多,也 没有cookies或者request URL 自定义字段在图中给出了说明 当然,这只是个例网站,仍有以偏概全之嫌



文件 領領 総則 工具 景示 報助 WinCorfig ① 子皇教 メ・ト 徳宗 🌘 田政宗 🍱 秘密 ಿ 長を思示。所有会話・ 函 任可出程 約 査成 🖳 保存 🐻 🕥 源 同語器 ・ 🚱 清極原存 . 丌 文本内号 (旧 分集) MSDN Soarch ... 🕸 高 网络信息 X Get Started 🕜 直家接计 👊 企送年租 🔌 自动转发 📝 直求機構 🌃 Middler Orthestra Seta 🚟 Middler Script 🔢 Liop 🗔 Piltera 🚍 Tendine 协议头 文本查看 遊去查看 网络视图 十六进制管备 认证 Cookes 数据 25CH 1945. GET https://mirrors.tuna.tsinghua.edu.cn/ubuntu-releases/22.04/ubuntu-22.04.3-live-server-amd64.iso.zsync HTTP/1.1 Host: mirrofs.tuna.tsinghua.edu.cn Connection: keep-alive sec-ch-ua: Not_A Brand"; v="8", "Chromium"; v="120", "Google Chrome"; v="120" 表示浏览器的品牌和版本。Not A Brand是一个用于防止服务器端指纹识别的标记 sec-ch-ua-mobile: ?0 浏览器是否在移动算 sec-ch-ua-platform: "Windows Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) ApplewebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Accept: text/html,application/shtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Sec-Fetch-Site: same-origin 表示请求的来源和资源的来源之间的关系 Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 是否由用户激活发起 Sec-Fetch-Dest: document
Referer: https://mirrors.tuna.tsinghua.edu.cn/ubuntu-releases/22.04/
Accept-Encoding: gzip, deflate, br Accept-Language: zh-CN,zh;q=0.9,en;q=0.8 Find ... (press Ctrl+Briter to Nighton); all) 在記事本中打 Transformer 协议头 文本宣春 语主宣春 图片宣春 十六进制酒香 网络夏春 认证 维存 Cookes 数据 2509 204. HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Wed, 20 Dec 2023 06:23:12 GMT 绿框内为常见字段 Content-Type: application/octet-stream Content-Length: 4167029 Last-Modified: Thu, 10 Aug 2023 18:33:05 GMT Connection: keep-alive ETag: "64d52d61-3f9575" Strict-Transport-Security: max-age=31536000 X-TUNA-MIRROR-ID: neomirrors 标识了请求发送到的铜像站点,用于负载均衡和银存目的 zsync: 0.6.2 Filename: ubuntu-22.04.3-live-server-amd64.iso MTime: Thu, 10 Aug 2023 05:06:27 +0000 Blocksize: 4096 Length: 21333 *** FIDDLER: RawDisplay truncated at 128 characters. Right-click to disable truncation. ***

02

网页端 US 客户端

01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

02 从清华镜像网站下载 4167029 字节 ubuntu-22.04.3-live-server-amd64.iso.zsync

一般下载网站 VS PanBD网页端:

再看PanBD,我们发现复杂度激增,连接请求逻辑和自定义首部数量与一般下载网站截然不同

我们将从下载服务器开始,尽可能的梳理出 网页端下载时的服务器请求链与特殊字段

从右图可见,下载服务器并不是 pan.baidu.com, 他们似乎都是baidupcs.com 的子域名服务器,命名也都有迹可循

同时,不像一般网站的下载,网盘并不是在 点击下载时直接跳转到该服务器,我们也看 见了如d.pcs.baidu.com/mbd.baidu.com等等 服务器,他们的作用也是我们感兴趣的地方

下面, 我们以d.pcs.baidu.com这 一服务器为例,带大家从http首部 剖析其作用

259	200	HTTPS:	pan baidu com	/api/enelytics?clienttyp	45	182,61,200,162	no-c	image/ipeg: chis	chro	[#257]	
(2) 260	200	HTTPS		/api/list?dienttype=08	4,883	182.61.200.162	no-c	application/ison	diro	200	
261	200	HTTPS	trumbnal0 badupcs.com	/thumbnal/34e0573cg	3,538	182.61.200.152	max-	image/peg	rjan-		
(2) 262	200	HTTPS	mao.baidu.com	/abdr?data=%76%22d	2	180,97,107,3		application/json	chro	[#260]	
fft 263	200	HITP	Turnel to	103.30.235.171:443	729	103.30.235.171			200	[#261]	
254	200	HTTPS	pan.badu.com	/act/analytics?clienttyp	43	182.61.700.162	no-c	image/peg; chs	thro	[#202]	
265	200	HETPS	pan-bedu-com	/api/analytics?clienttyp	43	182,61,200,162	no-c	іпаредреді гла	dws	(#263)	
266	200	HTTPS.	pan baidu com	/api/analytics?clienttyp	-63	182.61.200.162	no-c	image/peg: cha	ularo	[#264]	
267	200	HTTPS	pan.baidu.com	/wpi/analytics?stienttyp	43	182,61,200,162	no-c	image/peg: cha	dva	[#265]	
208	200	HEIP	Turviel to	mbd.baldu.com; 443	1,569	153.3.237.224			dwo	[#266]	
[m] 269	200	HTTPS	pan.baidu.com	/disk/cmsdata?clienttyp	206	182.61.200.162		application/json	chro	[#267]	
(m) 270	200	HTTPS	pan.baldu.com	/dsk/cnsdata?clenttyp	3,228	182.61.200.162		application/json	dwo	[#268]	
◆ 271	304	HTTPS	startovou cán boebos cum	Jinks-program%2Finag	Ď.	60.188.66.25	Expr.	image/png	abro	[#269]	
101272	200	HTTPS	pan baidy com	/api/gettemplatevariabl	545	182.61.200.162	no-c	application/json	chro	[#270]	
((273	200	HTTPS	mbd.baidu.com	/ztbox?action=zpblog&	44	153.3.237.224		application/json	chro	[#271]	
(6) 274	200	HTTPS:	pan.backu.com	/api/download?clientty	393	182,61,200,162	no-c	application/json	thro	[#272]	
西 275	200	HITP	Turvel to	d.pcs.badu.com/40	815	182,61,200,15			zhvo	[#273]	
276	302	HTTPS	d.pcs.baidu.com	/file/34e0571ccj2db543	50	182.61.200.15		text/plain; char	diro	[#274]	
(f) 277	200	HTTP	Turnel to	Naff-ct11.berdupos.com	815	113,137,57,111		25 (2)	thro	[#275]	
Z 276	200	HTTPS	xefj-ct11.bedupcs.com	/fie/34e0571ccj2db543	-21,386	113.137.57.111	max	Image/png	dvo	[#276]	
279	- 200	HITPS	paribadu com	/api/analytics/dienttyp	10	102.61.200.182	no-c	inage/peg: dis	2770	[#117]	
200	200	HTTPS:	pan.bedu.com	/api/analysics?identtyp	45	182,61,200,162	RP-C-	image/greg; cha	dwa	[#270]	1
Z 291	200	HTTPS	pan.badu.com	/api/analytics/identtyp	-43	182.61.200.162	100 C	inage/peg; cha	120.0	[#229]	1
292	200	HITTPS	pan.badu.com	/aci/analytics?clienttyp	45	182.61.200.162	00-C.,	image/peg; it's	ibro	[#280]	1
Q 283	200	HITP	Turnel to	mbd.baldu.com; 443	1,569	153.3.237.224			ithre	[#201]	
(例 254	200	HTTPS	pan.baidu.com	/disk/cmsdata?clienttyp	3,228	182.61.200.162		application/json	chro	[#282]	文件下载
(数 285	200	HTTPS	pan baidu com	/apy/download?clientty	391	182.61.200.162	110-C	application/json	chro	[#283]	1
(8) 286	200	HTTPS	mbd.baidu.com	/ztflox?action=zpblogils	44	153.3.237.224		application/json	chro	[#284]	
债 287	200	HITP	_	d.ocs_bedu.com:=43	815	182,61,200,15			ifwn	[#205]	1
S 288	302	HTTPS	d.pcs.baidu.com	/fie/ Beb81f1cp13cb8f	50	182.61.200.15		text/plan; char	dro	[#286]	1
(f) 289	200	HITP	Turnel to	alal02.badupcs.com;#43	815	119/107/143/56			thro	[#207]	J
290	200	HTTPS	allali02.baidupcs.com	/fie/15eb81f1cp13cb8f	26,014,284	119.167.143.56	max	application/ynd	chro	[#288]	
西201	502	HITP	Turnel to	sb-ist google.zum:443	382		no-c-	text/htm; chars	ihra	[#289]	
Ø 292	200	HTTP	Turnel to	www.googleaptr.com; 443	0	172,717,160,74			170	[#290]	
ff 293	200	HILL	Turnel to	103.50.235.171:443	729	103.50.236.171			9/0	[#291]	
西 294	200	HTTP	Turnel to	sufer Jenovomm.com: 443	729	103.30.235.171			leno	[#293]	
@ 295	406	HTTPS	oufur Jenoyamm.com	/report2	512	103.30.235.171	no-C-H	text/htm; chars	end.	#293	
ff) 296	200	HEIP	Turnel to	103.30.235-171:443	729	103.30.235.171			\$110	[#294]	
fft 297	200	HITP	Turnel to	103.50.235.171.443	729	303-30-235-171			pro	[#295]	
(f) 298	502	HTTP	Tunnel to	172.217.163.42:443	582		RP-C	text/html; chars	pro	[#296]	
而 299	502	HEIP	Turnel to	172.217.163.42:443	582		NO-C	text/html; chars	pro	[#297]	
200	200	HITP	Turnel to	61.170.98.116:80	- 0	61.179.98.116			pra	[#298]	
301	403	HITP	cd.huoying666.com	/static/profiles.pro	330	175.6.29.181		application/invi	pro	[#299]	
(5) 302	200	HTTP	Turnel to	180, 162-249-205:80	0	180, 163, 249, 205			pro	[#300]	
303	200	HTTP	profile.se.360.on	/proxyerr.php	0	180.163.249.205		application/octe	pro	[#301]	

02

网页端 US 客户端

01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

02 从清华镜像网站下载 4167029 字节 ubuntu-22.04.3-live-server-amd64.iso.zsync

一般下载网站 VS PanBD网页端:

让我们先回到wireshark的抓包流,将IP锁定为下载服务器的IP(这里指xafj-ct11服务器)可以看见下方 113段IP为下载服务器。而在此之前紧跟着的是IP182.61.200.15的tcp握手与数据传输。图中没有显示的是在于182交流完毕后主机马上就利用DNS寻找113服务器,说明d.pcs.baidu.com可能是一个响应传输请求的服务器让我们回到fiddler去实锤

01_wire_pcapng				- 0 X
The second secon	(C) 分析(A) 廃計(S) 用语(Y) 无线(V	W) 工順(T) 標準(H)		
	MF + S = QQQE			
top http://http2 tep-poet == 443				₩ - +
No. Time	Source	Destination	Frutucal	Length Info
3748 15.761846	182.61.180:162	10:20:243.61	TCP	66 [TCP Dup ACK 3738#1] 443 - 5693 [ACK] 5eq=22378 Ack=64482 Win=159
3744 15.789673	182.61.280.162	10.20.243.61	TCP	60 [TCP ACKed unseen segment] 443 - 5693 [ACK] Seq=22370 Ack=65854 k
3745 15.792298	182.61.200.162	10.20.243.61	TCP	68 443 + 5693 [ACK] Seg=22370 Ack=68509 Win=167936 Len=0
3746 15.877428	182.61.200.162	10.20.243.61	TLSv1.2	792 /apilisation Data
3747 15.894367	10.20,243.51	182.61,200.15	TCP	66 5797 + 443 [SYN] Seq=0 WIN=64240 Len=0 MSS=1460 WS>256 SACK_PERM=
3748 15.919047	10.20.243.61	182,61,280,162	TCP	54 5693 + 443 [ACK] Seq=68500 Ack=23100 Win=131320 Len=0
3749 15.935986	182,61,290,15	10,20,243.61	TCP	66 443 - 5797 [SYN, ACK] Seq 0 Ack=1 Win=8192 Len=0 MSS=1452 WS=32 S
3750 15,936130	10.20.243.61	182,61,200,15	TCP	54 5797 + 443 [ACK] Seq=1 Acd=1 Win=132096 Len=0
3751 15.939343	10.20.243.61	182.61.200.15	TLSV1.2	229 Client Hello
3757 16.079630	182.61,200.15	18.28.243.61	TCP	68 443 + 5797 [ACK] Seq=1 Ack=176 Win=30336 Len=0
3758 16.0R2686	182,61,200,15	10.20.241.61	TCP	1514 [TCP Previous segment not captured] 443 - 5797 [ACK] Seq=1461 Ack
3759 16.082686	182,61,288,15	10:20:243:61	TCP	1514 [TCP Out-Of-Order] 443 + 5797 [ACK] Seq=1 Ack=176 Win=38336 Len=1
3760 16.082780	10,20,243.61	182,61,200,15	TCP	54 5797 + 443 [ACK] Seq=176 Ack=2921 Win=132096 Len=0
3761 16.082892	182.61.280.15	18.28,243.61	TL5V1.2	SSS Server Hello, Certificate, Server Key Exchange, Server Hello Done
3762 16,082892	182,61,290.15	10.20.243.61	TCP	555 [TCP Retransmission] 443 - 5797 [PSH, ACK] Seq=2921 Ack=176 Hin=3
3763 16.882958	10.20.243.61	182,61,200,15	TCP	66 5797 + 443 [ACK] Seq=176 Ack=3422 Win=131584 Len=8 SLE=2921 SRE=3
3764 16.885677	10.20.243.61	182.61.200.15	TLSv1.2	147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mess
3765 16.185542	182.61.280.15	10.20,243.61	TLSV1,2	224 New Session Ticket, Change Cipher Spec, Encrypted Handshake Messa
3766 16.185542	182.61.200.15	10.20.243.61	TCP	60 443 + 5797 [ACK] Seq=3422 Ack=269 Win=38336 Len=8
3767 16.189363	10.20.243.61	182.61.200.15	TCP	832 [TCP Previous segment not captured] 5797 - 443 [PSH, ACK] Seg=317
3768 16.198328	10:20:243:51	13,107,21,239	TCP	56 [TCP Retransmission] 5780 + 443 [5VN] Seq=0 Nin=64240 Len=0 MSS=1
3778 16.288258	182.61.290.15	10.26.243.61	TCP	60 [TCP ACKed unseen segment] 443 - 5797 [ACK] Seq=3592 Ack=1721 Wir
9771 16,288898	182.61.200.15	10.20.243.61	TCP	50 443 + 5797 [ACK] Seq=3592 Ack+3951 Min=37760 Len=0
3772 16.389201	182.61.280.15	10.20.243.61	TLSv1.2	1262 Application Data
3773 16.389392	182.61.200.15	10.20.243.61	TCP	139 [TCP Previous segment not captured] 443 - 5797 [PSH, ACK] Seq+547
3774 16.389392	182.61.280.15	10.20.241.61	TL5V1:2	724 [TCP Out-Of-Order] , Application Data, Application Data
3775 16.389470	10.20,243,61	182.61.200.15	TCP	54 5797 + 443 [ACK] Seq=3951 Ack=5555 Min=132096 Len=0
3776 16,389808	182.61.200.15	10.20.243.61	TLSv1.2	88 Application Data
3777 16.389880	10.20.243.61	182.61.288.15	TCP	54 5797 - 443 [ACK] 500-3051 Ack-5589 Win=132096 Len=0
3780 16,473979	10.28.243.61	(113.137.57.111	TCD	66 5799 + 443 [SYN] Seq=0 Win=64240 Len=0 #55=1450 WS+256 SACK_PERH+
3781 16,424794	182, 63 280, 15	10/20/243/61	TL591 12	#8 [TCP Spurious Retransmission] , Application Data
3782 16.424843	10.20.243.51	182,61,280,15	TCP	66 [TCP Dup ACK 3777W1] 5797 + 443 [ACK] 5eg+3951 Ack+5589 M1n+13209
3783 15,498492	113.137.57.111	10.20.243.61	TCP	66 443 - 5799 [SYN, ACK] Seg-8 Ack-1 Win-8192 Len-8 MSS-1452 WS-32 S
3784 16,490732	10.20.243.61	113.137.57.111	TCP	54 5799 + 443 (ACK) Seq=1 Ack=1 Win=132896 Len=0
3785 16.493682	10.20.243.61	113.137.57.111	TL5V1.2	236 Client Hello

02

网页端 US 客户端

01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

02 从清华镜像网站下载 4167029 字节 ubuntu-22.04.3-live-server-amd64.iso.zsync

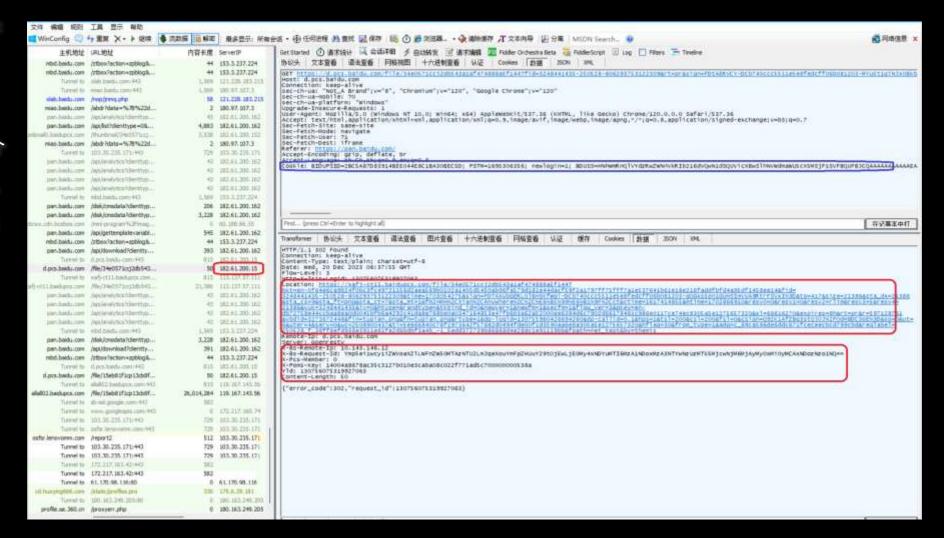
一般下载网站 VS PanBD网页端:

182段IP证实刚刚看见的tcp握手确实是d.pcs.baidu.com

再看应答与请求

应答中的Location字段纯纯显眼包,仔细一看开头正是xafj下载服务器,这说明就是这个服务器给host提供了下载的地址。同时下面也有一些自定义的X字段,推测是认证信息,此处不予证明。

而请求报文看起来则是风平浪静,与一般网站相差无几。但仔细看它超出屏幕的cookie就知道事情不简单



02

网页端 US 客户端

01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

02 从清华镜像网站下载 4167029 字节 ubuntu-22.04.3-live-server-amd64.iso.zsync

一般下载网站 VS PanBD网页端:

上方的requestURL传递了文件信息,最瞩目的 就是VIP字段了

下方的cookie则传递了用户的认证信息。从很多 很长的ID中能感觉出PanBD的安全性还是不错的

研究到这,我们进一步明确了方向,即 网页端和客户端在登录、运行、下载文件 时与百度的各类服务器的交互逻辑链有什 么异同,与下载时携带的http首部有什么 区别





02

网页端 US 客户端

PanBD网页端:

故接下去我们按照分析d.pcs.baidu.com的逻辑 将网页端主要(出现频率高)的子域名服务器作 了分析

因时长有限,我们直接给出结论

其中

请求服务器用于处理所有的动作请求并给出下一 指令应答

推送服务器用于建立全双工通信以实时获取数据 交互

略缩图服务器用于预览图片,子域名中的X代表数字

静态资源服务器负责存储框架类web前端文件 埋点服务器在特定动作埋伏,获取用户特征画像 以优化运营策略

文件传输服务器分为专线和通用,每次连接的服 务器为host发送请求时的相对最优解。专线服务 器的前四位'aabb'代表地区和用

途, 'cu/cm/ct'代表三大运营商,XX代表number

通用服务器一般以allall或者 地区+all为域名,所在地服务器规模一般较大

具体的结构框图会在本节最后给出

01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

02 从清华镜像网站下载 4167029 字节 ubuntu-22.04.3-live-server-amd64.iso.zsync

'根'服务器:pan.baidu.com/pcs.baidu.com/baidupcs.com

百度账号登录服务器:passport.baidu.com

账号数据云服务器:pcsdata.Baidu.com

请求服务器:d.pcs.baidu.com

推送服务器:webpush.pan.baidu.com //websocket 全双工通信

略缩图服务器:thumbnailX.baidupcs.com

静态资源服务器:bdstatic.com

埋点服务器 mbd.baidu.com Mobile Big Data / hm.baidu.com hao123 monitor

文件传输服务器

专线服务器 aabb-cu/ct/cmXX.baidupcs.com通用服务器: allall/地点all01.baidupcs.com

02

网页端 US 客户端

01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

03 从百度客户端登录并下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

PanBD客户端:

同理(省略-万字),我们整理出客户端从登录到下载所接触的服务器,并与网页端对比

右图中黑色为增添服务器, 白色为保留服务器, 灰色为不可见服务器

其中,host会规律性的向更新服务器发送用户状态,包括签名,传输沟道,VIP信息等

与P2P服务器的连接出现在登录初始化时,可能用于所谓"高速下载"?

插件服务器提供内核、基础库、升级程序等插件, 封装了web端的一些功能服务器

我们会发现相比于网页端,客户端在下载服务器上 并无太大区别,而功能服务器似乎更加集中密闭, 从某一程度上确实提高了安全性。

找到了交互服务器的区别,接着再聚焦于下载时的 字段有无明显区别 '根'服务器

更新服务器:update.pan.baidu.com

P2P连接服务器:aa.t.bcsp2p.baidu.com

百度账号登录服务器

账号数据云服务器

请求服务器

推送服务器

略缩图服务器

静态资源服务器

埋点服务器

插件服务器:wppkg.baidupcs.com 文件传输服务器

□ JSON wppkq服务器传的文件 md5=75412f1adb02efe4b6513cff9c69242a name kernelbasis.dl url=http://ssuecdn.baidupcs.com/issue/netdisk/p2p-pc/kernelbasis/kernelbasis.21518.gz version=2.1.5.18 基础库文件,用于提供一些基本的功能和接口,如 md5=28b5ed=12587eb1c5bde8029b75b9e63 url=http://issuecan.baidupcs.com/issue/netdisk/p2p-pc/kernelpromote/kernelpromote.22606.gz version=2,2,60.6 助亦福德库文件、用于提供一册、知多级程下程、新点提供、文件校验的功能 md5=5735134ha63f30f53522821fa01664c2 name kernelUpdate.exe | III NATION INTERNATION PROFINENCE url=http://d8.baidupcs.com/issue/netdisk/p2p-pc/kernelUpdate/kernelUpdate.3003.gz ⊞-KUInfo md5=194080d16405365bb979f21e5c8cba66 提供核心功能的文件、加上传下载。分享管理、同步看份等 url=http://d8.baidupcs.com/issue/netdisk/p2p-pc/kernel/kernel.300226.gz version=3.0.0.226 version=3.0.0.226

01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

03 从百度客户端登录并下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

02

网页端 US 客户端

PanBD 网页端 VS PanBD客户端:

下面我们对两者的来往报文与requestURL作对比 先看报文:

```
GET https://x8fi-ctil.baidupcs.com/file/34e057icci2db543a1af474B88a5f1447bkt=en-0f64e6ca9b24f0bc5fc49721156d2aea569bb102a1405d5450ab96fa579d181e44dacf59f2a1797
Host: xafj-ctil.baidupcs.com
connection: keep-alive
upgrade-insecure-Requests: 1
User-Agent: Mozilla/5.0 (windows NT 10.0; win64; x64) Applewebkit/S37.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/S37.36
Accept: text/html, application/xhtml+xml, application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-User: 71
Sec-Fetch-User: 71
Sec-Fetch-User: 1frame
Sec-Ch-ua-Mobile: 70
Sec-
```

```
GET http://xafi-cti0.baidupcs.com/file/34e0571cci2db543mlaf474888m5fl447bktmen-0f64e6ca9b24f0bc3fc49721156d2aea569b0102a1405d5450mb96fa579d181e44dmcf59f2m1797fHost: xafj-cti0.baidupcs.com
Connection: Keep-Alive
Content-Length: 0
Accept: #/*
Accept: #/*
Accept: #/*
Accept: #/*
Accept: elmguage: zh-CN
Range: bytes=0-21385
User-Agent: netdisk;P2SP;3.0.0.236
Accept: Encoding: identity
```

上方左右两图分别是网页端的来往报文,下方为客户端 报文上二者无明显区别,除了前者的agent为浏览器,而后者netdisk 再试图分析requestURL首部

02

网页端 US 客户端

01 从网页端下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

03 从百度客户端登录并下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

PanBD 网页端 VS PanBD客户端:

字段对比如下, 有颜色的字段代表该端的特殊字段

因能力有限,我们无法透过字段实锤结论,只能做出猜测:

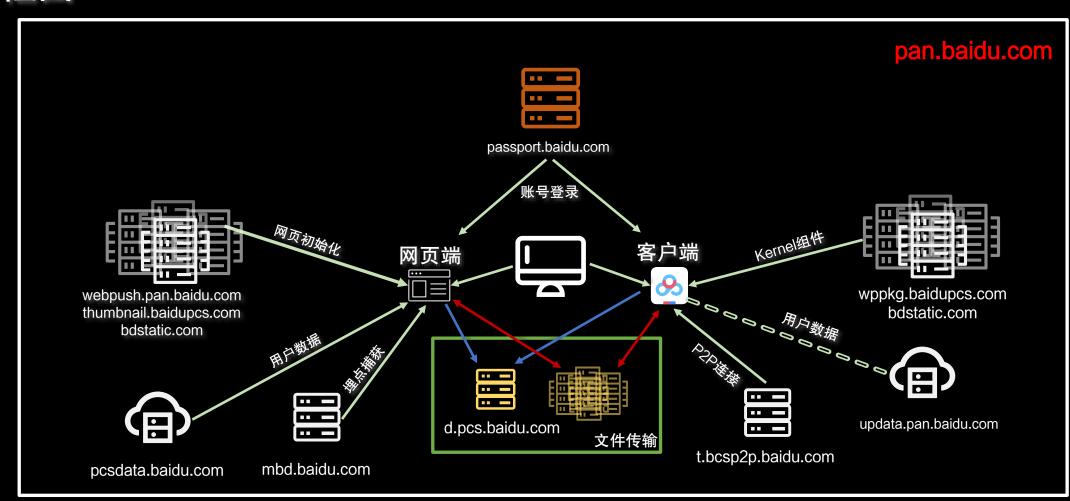
总体上二者的requestURL首部数量相差不大且都远远大于纯粹下载网址,再者rt字段都为pr,应为private,故推断下载时二者的逻辑本质上是没有差别的

网页端因通过browser这一媒介,故 可能部分用于认证的字段可以略去

ten fiel	cri- 0964-6-a6b;2409c3h48721156d2aea6689x0102 a1,005d5450a1665y79c181e44dac5667a17079 75977a1637641b63e18e216faddb44a95e714 68ac44	nès	6ft- 0f64e6ca9b24f0bc3fc49721156d2aea569b010					en-			
fiel	The state of the s		2a1406d5490at66fb67bd183a44dbcf59f2a378 7ff75fff7a3a537643b63a18a236taddfbf54a85 aff16f6aa17		30 #	88816270	pkey	0572758e44xxbas8es040045b7b6s4292x 61da8e768be0a0347354853e477b6b1s62 a52000ee5384e6c7962d85178483c586e0	- 19	adg	a_313±0:7102917-0:090±154±09965 f3235f3
	3248441435-250528-806393753122309	fed	3248441435-250528-898283753322309		31 sopres	Eh	al .	117-078-0-E1646-01758672791 88616270	60	rectabel	250528 38HBertsSSBc0911a8 18268xdbf3a4t - 1,295xdb4cf8x684x5343e5ed4 ete78e8
time.	1703054275	time	3709073122		mu.	Or.	expires		41	ibo.	
starr	FDTAXU66ERLQIBHSKNVqi- DC6740ce5511e5e8tedet08681208- g0Gestpm1GUHSknvVLMRRtrFSVx1=	sign	FDTAXUBGERLQIBHSKTWG- DCb740cc5611e5e8fedcf06b081283- +8b500xb6712Dhs1pPo6+45MiQ=		22 e	58712876L	et	pr	-	Speth	net lest
to	417	10	218		Si yodid	1273672448		679421727	-83	De.	Demin
size:	21396	size	21386		88 Re	tupian peg	vodid	, or or a contract of			USCHOOL .
eta et		sta.de	21380		26 m:	tusion prog	ñn	tuplan.prig			
sta o		sta cx	11		IT rtype	1	frilling:	416.79.214.18-216			
Ma ft		sta ft	IND		35 dp-loged	1.307586+17	eret veer				
sta e		sta et	programme and a second		39 dp-callid	0.1	check liture				
			1		40 hps			-			
sta it		sta_mt			40 Hps.	1	rtype	armateur.			
tm2	MH,Xion,Anyothere,,WIT,ct	tm2	MH.Xian,Anywhere, IRIZ.et		AL Isl	200	denid	BURNAVI- O 305 DESSONSFINAFF286-409C39817173C 3-C D-O 9025-3853-2101-218F- M-ERRALEARITH - II BURNOSETE			
ctime	1617414895	ctime	3817414855		42 cal	200	stientype				
entire	e 1702899910	mone	1702866610		43 fM	0	channel	0			
resvo	a a	rew0	0	į.	At calgn	QR3x1A/ZBu3xrQjQJ/Od HBDC3bE=	dp-logid	1.35835£+17			
cesv1	0	#esv1	0	i i	45 50	0	dp-callid	0.1			
regy2		169/2	rlim		46 ut	6	tsi.	200			
reev3		Ten/I			67 uter	4	cui	200			
(may-)		rese4	21306		45 very		tel				
wide	3248441435	. Walk	1248441435		40.ue	2508800437	csign	Q92k1Af28kj3rtQj03/OdH8DC3cE=			
N	0	N.	0		58 W	5e666840c78f1973642f57 882d94948ce007Lt3590a e6e6a305a5e1275657320	10	1			
htype		htype			DI Integ	30	Mt				
mid		randtype			52 from type	1	uter				
	7.0				The contract of	c 89ca586deGdddc673fpec					
tkbie	d id 0	fishind,id	0		SE adg	exerbes/799ctsd	serv				
newv		est	i		54 register	250528 1899645038629 116916248545934b - 1 56843727396868864 62846169111965	lac .	3853345400			
nesid	n 1	DEWAYEE	1		SE Queta	net less	16	3d549898w0139656347a2889039620286c5 d275867aa7dslc			
1.						\$2000 b	DAY DOWN	G2/300/Margon			
uncte		newtre	,		50 by	Uvernes	sta_sck	.4			
flow.	we 3	sector	1		57		hring	30			
pkasy	un- db/12758e44xcbes8es0d9945bfb944292e41ds8 e789se6s0547164853e47f98b506265090ee63	flow yer			70		From type				

网页端 US 客户端

总结框图



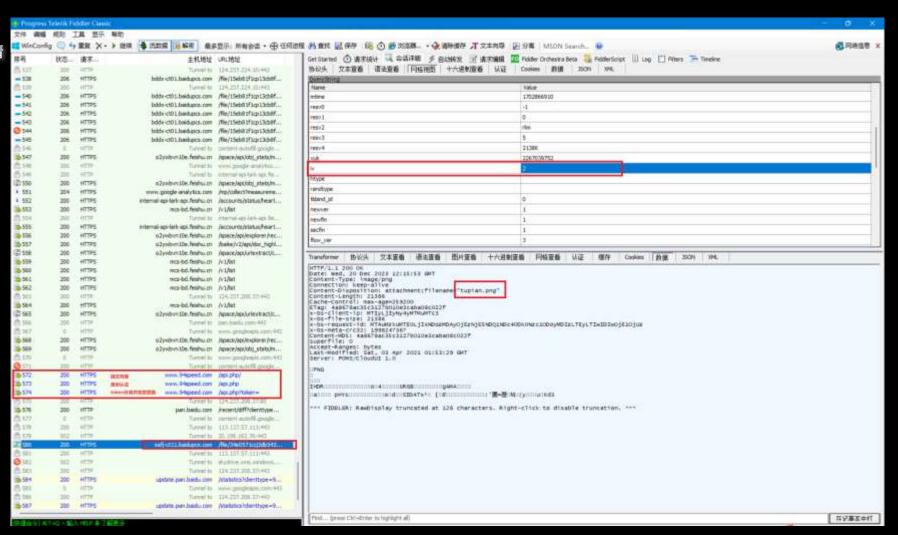
SVIP VS PoorMan

04 用第三方工具下载 21386 字节 tupian.png 和 26014284 字节 testppt.pptx

这里我们采用拿他人API接口获取SVIP直链的方法可以看见原本的d.pcs.baidu.com变成了三个api的请求,分别为数据列表提交、身份认证和token验证

普通用户和SVIP用户所用的服务器是一样的 从requestURL的角度,除了iv字段从0变成2,还有 一些随机数的不同以外几乎没有差别。

而后,我们开始怀疑tcp的窗口限制



优雅提速直链获取网站:94speed.com

NBP-NETWORK

03

SVIP VS PoorMan

但事实上,两者的实际窗口大小相差无几,怀疑不成立

接着我们想到了线程的控制,并对比了网页端、客户端和SVIP的区别,有了一些发现:

先看网页端, 网页端用浏览器下载只有单线程, 难怪恁慢

Window size value: 1040 SVIP
[Calculated window size: 33280]

[Window size scaling factor: 32]

Checksum: 0xd846 [unverified]

Window size value: 952

[Calculated window size: 30464]

[Window size scaling factor: 32]

Checksum: 0xb2aa [unverified]

200	НТТР		/api/filediff?block_list= /file/15eb81f1cp13cb8f	467	110.242.69.174
200	HTTP	Tunnel to	110.242.69.174:80	0	110.242.69.174
200	HTTP	Tunnel to	allall02.baidupcs.com:443	815	119.167.143.56
302	HTTPS	d.pcs.baidu.com	/file/15eb81f1cp13cb8f	50	182.61.200.15
200	HTTP	Tunnel to	d.pcs.baidu.com:443	815	182.61,200,15
200	HTTPS	mbd.baidu.com	/ztbox?action=zpblog&	44	153.3.237.224
200	HTTPS	pan.baidu.com	/api/download?clientty	391	182.61.200.162
状态	请求	主机地址	URL地址	内容长度	ServerIP
	200 200 302 200 200	200 HTTPS 200 HTTPS 200 HTTP 302 HTTPS 200 HTTP 200 HTTP	200 HTTPS pan.baidu.com 200 HTTPS mbd.baidu.com 200 HTTP Tunnel to 302 HTTPS d.pcs.baidu.com 200 HTTP Tunnel to 200 HTTP Tunnel to	200 HTTPS pan.baidu.com /api/download?clientty 200 HTTPS mbd.baidu.com /ztbox?action=zpblog& 200 HTTP Tunnel to d.pcs.baidu.com:443 302 HTTPS d.pcs.baidu.com /file/15eb81f1cp13cb8f 200 HTTP Tunnel to allall02.baidupcs.com:443 200 HTTP Tunnel to 110.242.69.174:80	200 HTTPS pan.baidu.com /api/download?dientty 391 200 HTTPS mbd.baidu.com /ztbox?action=zpblog& 44 200 HTTP Tunnel to d.pcs.baidu.com:443 815 302 HTTPS d.pcs.baidu.com /file/15eb81f1cp13cb8f 50 200 HTTP Tunnel to allall02.baidupcs.com:443 815 200 HTTP Tunnel to 110.242.69.174:80 0

appell01.beidupcs.com /file/15ebil1f1cp13cbilf...

2,097,152

03

SVIP VS PoorMan

左图为小文件客户端下载,速度在5M/s左右,已经是 飞速了

可以看见网盘对线程数量并没有作过多的限制,而是对 每个线程的下载上限作出约束,像左图都是2097152封

小文件封顶影响不显著,但一旦下载较大文件就要命了, 上限掉到原来的1/4, 意味着与服务器连接所花费的时 间激增,自然速度就下来了

再看SVIP,在截图所在时间的网速下并没有触碰到上 限,这样能让网络自己调整到最高效的下载节奏上 即不限速

综上,我们得出结论,网盘是通过对每一 线程的上限作出限制而达成限速的目的~

- 56 206 HTTP - 58 206 HTTP - 59 206 HTTP - 60 200 HTTP - 60 200 HTTP	app801.bedupcs.com /fie/15eb81 app801.bedupcs.com /fie/15eb81 app801.bedupcs.com /fie/15eb81 Turnel to 113.137.57. Turnel to 113.137.57.	75:80
主机地址	URLHEIL	内容长度
bddv-ct01.baidupcs.com	/file/15eb81f1cp13cb8f	26,014,284
Turnel to	124.237.224.10:443	815
bddx-ct01 baidupcs.com	/file/15eb81f1cp13cb8f	25,248,344
Tunnel to	124.237.224.10:443	815
Turnel to	124.237.224.10:443	815
bddx-ct01.baidupcs.com		12,534,402
bddx-ct01.baidupcs.com		6,267,202
Turnel to	124.237.224.10:443	815
bddx-ct01.baidupcs.com	/file/15eb81f1cp13cb8f	5,988,396
Turnel to	124.237.224.10:443	815
Tunnel to	124.237,224.10:443	815
Tunnel to	124.237.224.10:443	815
Turnel to	124.237.224.10:443	815
bddx-ct01.baidupcs.com	/file/15eb81f1cp13cb8f	2,920,844
bddx-ct01.baidupcs.com	/file/15eb81f1cp13cb8f	2,658,529
bddx-ct01.baidupcs.com	/file/15eb81f1cp13cb8f	2,322,486
bddx-ct01.baidupcs.com	/file/15eb81f1cp13cb8f	2,128,167
Turnel to	124.237.224.10:443	815
Tunnel to	124.237,224.10:443	815
Tunnel to	124.237.224.10:443	815
Tunnel to	124.237,224.10:443	815
Turnel to	124.237.224.10:443	9.15
Tunnel to	124.237,224.10:443	815
Turnel to	124.237.224.10:443	815
Tunnel to	124.237,224,10:443	815
bddx-ct01.baidupcs.com	/file/15eb81f1cp13cb8f	1,280,230
bddx-ct01.baidupcs.com		915,856
bddx-ct01.baidupcs.com	/file/15eb81f1cp13cb8f	714,983
bddx-ct01.baidupcs.com	/file/15eb81f1cp13cb8f	640,148
bddx-ct01.baidupcs.com	/file/15eb81f1cp13cb8f	1,911,780
bddx-ct01.baidupcs.com		559,248
bddx-ct01-baidupcs-com	/file/15eb81f1cp13cb8f	510,097
Tunnel to	124.237.224.10:443	815
bddx-ct01.baidupcs.com	/file/15eb81f1cp13cb8f	457,961
Turnel to	124.237.224.10:443	8.15
bddx-ct01.baidupcs.com	/file/15eb81f1cp13cb8f	1,291,492
Turnel to	124.237.224.10:443	815

See					
商 57	200	HULE	Tunnel to	119.167.143.118:80	0
= 58	206	нттр	qdbh-cu00.baidupcs.com	/fie/89f160ed5n246b1	524,288
- 59	206	HTTP	qdbh-cu00.baidupcs.com	/file/89f160ed5n246b1	524,288
60	206	HTTP	qdbh-cu00.baidupcs.com	/file/89f160ed5n246b1	524,288
-61	206	HTTP	qdbh-cu00.baidupcs.com	/file/89f160ed5n246b1	524,288
- 52	206	HTTP	gdbh-cu00.baidupcs.com	/file/89f160ed5n246b1	524,288
63	200	HTTP	pan.baidu.com	/rest/2.0/membership/	14
3 64	200	HTTP	pan.baidu.com	/rest/2.0/membership/	14
65	206	HTTP	qdbh-cu00.baidupcs.com	/file/89f160ed5n246b1	524,288
- 66	206	HTTP	qdbh-cu00.baidupcs.com	/file/89f160ed5n246b1	524,288
2 67.	403	HITP	pan.baidu.com	/rest/2,0/membership/	80
商 68	200	HTTP	Turvel to	update.pan.badu.com:	0
2 69	200	HTTPS	update.pan.baidu.com	/statistics?clienttype=8	11
- 70	206	HTTP	qdbh-cu00.baidupcs.com	/file/89f160ed5n246b1	524,288
-71	206	нттр	qdbh-cu00.baidupcs.com	/file/89f160ed5n246b1	524,288
- 72	206	HTTP	adoh-cu00.baidupcs.com	/file/89f160ed5n246b1	524,288

买一送二

我们在研究的过程中了解了RESTful框架统一接口,并在抓包中发现了IPv6、IPv4的双栈传输,本欲详细说明,怎奈时间有限,只能贴出网址了T.T

优雅提速直链获取网站: 94speed. com

什么是RESTful API:

https://zhuanlan.zhihu.com/p/334809573

什么是双栈结构:

https://zhuanlan.zhihu.com/p/569641486

05 〉 总结

基于wireshark和fiddler+proxifier两个平台,我们抓取了网页端和客户端、普通用户和SVIP用户的下载流程链,作出对比分析,最终得到了下载逻辑框图和限速原因,并给出了科学合法有效的提速方法,浅显地解决了自己的问题。 当然,我们仍未清晰的弄明一些请求字段的含义与作用,这是我们此次研究的遗憾。

最后,这里是NBP-宁波小学队,希望我们的调查能给你一些收获~

