Lecture Outline

- Feedback from Bill Marczak's lecture?
- A bit about Anonymity:
 - Brief look at Tor's evolution ...
 - … plus a "teachable moment"
- The problem of Spam
 - *Measurement* of a botmaster's spamming operations
 - DNSBLs and counter-intelligence
 - Spammer \$\$

Tor's Evolution

Directly connecting users



The Tor Project - https://metrics.torproject.org/

2013-11-03	<or> Relays</or>	Microsoft adds the Mevade/Sefnit botnet signative to their Malicious Software Removal Tool. Blog Post 6 000 000-
2013-10-27	<or> Relays</or>	Microsoft adds the Mevade/Sefnit botnet signature to various security scanners. Blog Post
2013-10-11	ipv4	geoip database updated to "October 2 2013 Maxmind GeoLite Country" (geoip+db-digest A28267CED18A1D80B4298796E9FE42EC755420 Ct.). C Commit
2013-09-23	flashproxy obfs2 obfs3	Release of the pluggable transports browser bundle 2.4.17-beta-2-pt3.
2013-09-10	ipv4	geoip database updated to "September 4 2013 Maxmind GeoLite Country" (geoip-db-digest CB632F60547F141E06FB0705D1F2012047165722014. 2016 2018 2020 Commit The Tor Project - https://metrics.torproject.org/
2013-08-19 to 2014-04-28	<or> Relays</or>	Relay users increase globally from about 800K to over 5M, when computers in the Mevade/Sefnit botnet began using Tor to communicate. The user count decreased in the following months through efforts to clean up the botnet. Sometime in 2014-04, the botnet switched from using Tor to using SSH.
2013-08-12	ipv4	geoip database updated to "August 7 2013 Maxmind GeoLite Country" (geoip-db-digest 83CCB5AF823A5CCF3C86C3CA33AF801D4E8996EC). C Commit
2013-08-10	flashproxy obfs2 obfs3	Release of the pluggable transports browser bundle 2.4.15-beta-2-pt1. Blog Post
2013-07-08	ipv4	geoip database updated to "July 3 2013 Maxmind GeoLite Country" (geoip-db-digest 4D558EA73DD91A0361DE3FA3E83171DCD38D1A2D). C Commit
2013-06-05	ipv4	geoip database updated to "June 5 2013 Maxmind GeoLite Country" (geoip-db-digest 5E570BB92DBEE1D517E35DAA4A52F58FDA6BB44E). C Commit
2013-06-02	flashproxy obfs2 obfs3	Release of the pluggable transports browser bundle 2.4.12-alpha-2-pt1.

2018-01-05 to present		Outage of the on-bk OnionPerfinstance
2010-01-03 to present		Op-Hk Graph
2018-01-01	United Arab Emirates Relays	User report that the UAE blocked Tor, bridges work.
		4 000 000 -
2017-12-28 to 2018-01-13	Iran	Protests in Iran, blocking of various services including Tor. Instagram was unblocked 2018-01-06.
		Telegram was unblocked 2018-01-13.
		C Wikipedia C OONI Report Relay Graph Breisen Graph C Twees C Spiphorn Isens
2017-12-21		Release of tor 0.3.2.8-rc, intended to fix the KIST bug that enabled a Dos on relays by running them
		out of memory.
		Announcement C Ticket
2017-12-20	inv4 inv6	geoin and geoin 6 databases updazoiz to "Decemzoiz 6 2017 Mazzoion Geolite 2018 uptry" (gezozon -
2011-12-20		db-digest 1D486694A710145631B295CC39ECC5682F75858C. a chi the might bling Westries torproject and
		F33231CAC761A71F7C19273DB1E11CEE01E2D982).
		C Commit
2017-12-16 to 2017-12-17	Bridges Unknown	Drop in the number of measured bridges
	onknown	Graph C Mailing List Post
2017-12-12 to 2018-01-18	meek	(former meek-azure, now unused) and grouploader meek barsoftware com (used by
		GAEuploader) bridges.
2017-12-12 to 2018-01-10	France <or> Relays Unknown</or>	Temporary tripling of relay users in France. Bridges not affected.
2017-12-10 to 2018-02-01	Germany <or> Relays</or>	Further, slow increase of relay users in Germany, from 500k to over 1.5M.
	Unknown	Graph 🖸 Reddit Thread 🖸 Ticket
2017-12-09	<or> ipv6 Relays</or>	Release of Tor Browser 7.0.11, containing tor 0.3.1.9, which adds an IPv6 address for the bridge
		authority bastet.
		Blog Post
2017-12-09	<or> ipv6 Relays</or>	Release of Tor Browser 7.5a9, containing for 0.3.2.6-alpha, which adds an IPv6 address for the
		bridge authority bastet.
		Image: State of the state o
		C. Blog Post

		Directly connecting users
2019-07-23	snowflake	The broker domain name snowflake-broker.bamsoftware.com is blocked by Google Safe Browsing,
		preventing the Snowflake web browser extension from working.
		C Ticket C Comment Noting Decrease In Proxies
2019-07-18 to 2019-08-07	Kazakhstan	The Kazakh ISP Kaz Telecom does man-in-the-middle of TLS connections. C Censored Planet Report Post About End
2019-07-03	snowflake	The Snowflake web browser extension for Chrome's published.
2019-07-02 to 2019-08-26	Iran <or> Relays Bridges</or>	Relays in Iran are reported to be unblocked once again, and user numbers recover to about 25% of the maximum they had reached buring trepprevious period of unblocking. They then druc precipitously, and bridge users increase.
2019-06-26	snowflake	The Snowflake web browser extension for Firefox is published. The Tor Project - https://metrics.torproject.org/
2019-06-21 to present	Burma	Internet shutdown in parts of Myanmar.
2019-06-20	obfs4	A call to set up new obfs4 bridges is posted to the tor-relays mailing list. Image: Continues Image: Continues
2019-05-28		Failure of network equipment at site of op-ab OnionPerf instance (equipment now replaced) Onionperf Timeouts Graph
2019-05-22	fte	Release of Tor Browser 9.0a1, removes support for FTE. Blog Post C Ticket
2019-05-17	ipv4 ipv6	geoip and geoip6 databases updated to "May 13 2019 Maxmind GeoLite2 Country" (geoip-db- digest 35DFDA2D06D2A0467EF37D60A67B438B11952B74, geoip6-db-digest C0193A1D086819353FABBF70AADB15866B7B2525). C Commit
2019-05-16 to 2019-06-23	Iran Relays	Tor becomes directly accessible in Iran, leading to an explosion in relay users up to about 1.5 million, before being blocked again.
		C Ticket C Comment About End C Tor-Talk Thread C Reddit Thread C Comment C Reddit Thread



This site can't provide a secure

connection

torproject.org sent an invalid response.

ERR_SSL_PROTOCOL_ERROR

None of my browsers can get to torproject.org from my home





This site can't provide a secure

connection

torproject.org sent an invalid response.

ERR_SSL_PROTOCOL_ERROR

But it works through campus VPN



••• <>		=	(Metrics.torp	roject.org		Ċ			1 O
				Users – Tor N	Metrics	News 📑 S	Sources 🕫 Ser	vices Development	â Research	+ [©] About
Táf Metri	cs									
😤 Home 🛛 😤 Users	🛱 Servers 🛛 🗚	Traffic 🛛 🚳 Performance	🕈 Onion Services 🗳	Applications						
	Home » Users									
	Users									
	We estimate the	number of users by analyzing	the requests induced by clie	ents to relays an	d bridges.					
	Relay users	Bridge users by country	Bridge users by transport	Bridge user	s by country and transport	Bridge use	ers by IP version			
	BridgeDB requ	lests by requested transport	BridgeDB requests by dis	stributor To	op-10 countries by relay user	ſS				
	Top-10 countri	ies by possible censorship eve	ents Top-10 countries by	/ bridge users	"The anonymous Interne	et"				
	6 000 000 -	Directly o	connecting users							
						Start date:	2010-01-01			
	4 000 000 -		- N	1		End date:	2020-04-07			
	2 000 000		we we have			Show		`		
	2 000 000 -	L	and the second sec	aar Va		censorship events if				
	0 -	2012 2014	2016 2018	2020		available:	Off	0		
	This graph shows	s the estimated number of dir	The Tor Project - https://m ectly-connecting clients; tha	netrics.torproject.org/ t is, it excludes	clients connecting via	Download gra	aph as PNG or PDF			



This site can't provide a secure connection

torproject.org sent an invalid response.

ERR_SSL_PROTOCOL_ERROR

How do we diagnose this failure?

									🗾 🗾 to	or-project-	-fail.trace)		
		۲		01010 01101 01110	×	Q		$\widehat{\mathbf{A}}$			÷	Θ		
Annh	, a displa	v filter	~											_

A	oply a display filter <쁐/>				Expression	+
No.	Time	Source	Destination	Protocol	l Length Info	
	1 1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64	
	2 1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=	
	3 1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…	
	4 1586234922.346904	10.0.0.119	95.216.163.36	TLSv1	583 Client Hello	
	5 1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310 [TCP ZeroWindow] , Ignored Unknown Record	
	6 1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…	
	7 1586234922.541524	95.216.163.36	10.0.0.119	TCP	66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…	
	8 1586234922.541555	10.0.0.119	95.216.163.36	TLSv1	73 Alert (Level: Fatal, Description: Protocol Version)	
	9 1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…	
	10 1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514 Ignored Unknown Record	
	11 1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266 Ignored Unknown Record	
	12 1586234922.559920	95.216.163.36	10.0.0.119	TLSv1	139 Ignored Unknown Record	
	13 1586234922.560036	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0	
	14 1586234922.560051	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0	
	15 1586234922.560056	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0	
	16 1586234922.560059	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0	
	17 1586234922.730475	95,216,163,36	10.0.0.119	TLSv1	90 Application Data	

Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)

▶ Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119

Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256

Secure Sockets Layer

Ignored Unknown Record

 [Expert Info (Warning/Protocol): Ignored Unknown Record] [Ignored Unknown Record] [Severity level: Warning] [Group: Protocol]

0000	8c	85	90	05	30	d7	48	1d	70	c4	c6	d2	08	00	45	00	E.
0010	01	28	00	00	40	00	40	06	2c	5d	5f	d8	a3	24	0a	00	.(@.@. ,]\$
0020	00	77	01	bb	d4	74	d5	88	6f	74	7d	4c	1d	0f	50	18	.wt ot}LP.
0030	00	00	eb	dØ	00	00	ff										
0040	ff																
0050	ff																
0060	ff																
0070	ff																
0080	ff																
0090	ff																
00a0	ff																
00b0	ff																
00c0	ff																
00d0	ff																

wireshark displaying a "pcap" packet capture made using tcpdump

							🧲 tor-proj	ect-fail.trac	e					
		01010	X	<u>)</u>	•	 <u>↓</u>		Ð	Θ	1				
Apply a	displav filter < ¥	/>											Expression	+

No.	Time	Source	Destination	Protocol	Ler gth Info
	1 1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
	2 1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
	3 1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18
-	4 1586234922.346904	10.0.0.119	95.216.163.36	TLSv1	503 Client Hello
	5 1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310 [TCP ZeroWindow] , Ignored Unknown Record
	6 1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
	7 1586234922.541524	95.216.163.36	10.0.0.119	ТСР	66 443 → 54388 [ACK] Seq 1 1 4 510 11 61700 1 0 70 1 5
	8 1586234922.541555	10.0.0.119	95.216.163.36	TLSv1	73 Alert (Level: Fatal, Decurrent TOD
	9 1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514 [TCP Retransmission]
	10 1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514 Ignored Unknown Recor
	11 1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266 Ignored Unknown Recor
	12 1586234922.559920	95.216.163.36	10.0.0.119	TLSv1	139 Ignored Unknown Recor
	13 1586234922.560036	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq
	14 1586234922.560051	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0
	15 1586234922.560056	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0
Τ_	16 1586234922.560059	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0
	17 1586234922.730475	95.216.163.36	10.0.0.119	TLSv1	90 Application Data

Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)

▶ Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119

▶ Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256

Secure Sockets Layer

▼ Ignored Unknown Record

[Expert Info (Warning/Protocol): Ignored Unknown Record]
 [Ignored Unknown Record]
 [Severity level: Warning]
 [Group: Protocol]

0000	8c	85	90	05	30	d7	48	1d	70	c4	c6	d2	08	00	45	00	0.H. pE.	
0010	01	28	00	00	40	00	40	06	2c	5d	5f	d8	a3	24	0a	00	.(@.@. ,]\$	
0020	00	77	01	bb	d4	74	d5	88	6f	74	7d	4c	1d	Øf	50	18	.wt ot}LP.	
0030	00	00	eb	dØ	00	00	ff											
0040	ff																	
0050	ff																	
0060	ff																	
0070	ff																	
0080	ff																	
0090	ff																	
00a0	ff																	
00b0	tf	ff	tf															
00c0	tf	ff	tf															
00d0	†f	†f	†f	†f	tf	†f	†f	†f	ff	tf	†f	†f	†f	†f	†f	†f		

🔵 🌠 tor-project-fail

_						
			tor-project-fail.tra	trace	9	
			E F	$(+)$ $(-)$ $(=)$ $\overline{++}$		
				4 4 4 ±		
	Apply a display filter <%/>			Expression		ion 🕂
No	. Time Ocure	Destination	Protocol	Length Info	ength Info	
	1 1586234922.150003 10.0.0.119	95.216.163.36	ТСР	78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …	78 54388 → 443 [SYN] Se	
	2 1586234922.346452 95.216.163.36	10.0.119	TCP	74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=	74 443 → 54388 [SYN, AC	=
	5 1500254922.540552 10.0.0.119	95.216.163.36	ТСР	66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…	66 54388 → 443 [ACK] Se	8
1	4 1586234922.346904 10.0.0.119	95.216.163.36	TLSv1	583 Client Hello	583 Client Hello	
	5 1586234922.353697 95.216.163.36	10.0.0.119	TLSv1	310 [TCP ZeroWindow] , Ignored Unknown Record	310 [TCP ZeroWindow] , I	
П		95.216.163.36	TCP	66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…	66 54388 → 443 [ACK] Se	a
	Pound_trin time	10.0.0.119	TCP	66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…	66 443 → 54388 [ACK] Se	5
		95.216.163.36	TLSv1	73 Alert (Level: Fatal, Description: Protocol Version)	73 Alert (Level: Fatal,	
	· · · · · · · · · · · · · · · · · · ·	10.0.0.119	ТСР	1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…	1514 [TCP Retransmission]	i
	(RTT) to convor	10.0.0.119	TLSv1	1514 Ignored Unknown Record	1514 Ignored Unknown Reco	
		10.0.0.119	TLSv1	1266 Ignored Unknown Record	1266 Ignored Unknown Reco	
		10.0.0.119	TLSv1	139 Ignored Unknown Record	139 Ignored Unknown Reco	
	$lis \sim 200 msec$	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0	54 54388 → 443 [RST] Se	
		95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0	54 54388 → 443 [RST] Se	
		95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0	54 54388 → 443 [RST] Se	
	16 1586234922.560059 10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0	54 54388 → 443 [RST] Se	
	17 1586234922.730475 95.216.163.36	10.0.119	TLSv1	90 Application Data	90 Application Data	
▶	Frame 5: 310 bytes on wire (2480 bits), 310	bytes captured (2480 bit	s) on interface	ace 0 (inbound)	0 (inbound)	
▶	Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:7	0:c4:c6:d2), Dst: Apple_	05:30:d7 (8c:8	:85:90:05:30:d7)	90:05:30:d7)	
▶	Internet Protocol Version 4, Src: 95.216.163	.36, Dst: 10.0.0.119				
▶	Transmission Control Protocol, Src Port: 443	, Dst Port: 54388, Seq:	1, Ack: 518, Le	Len: 256	: 256	
▼	Secure Sockets Layer					

Ignored Unknown Record

[Expert Info (Warning/Protocol): Ignored Unknown Record]
 [Ignored Unknown Record]
 [Severity level: Warning]
 [Group: Protocol]

0000	8c 85 90 05 30 d7 48 1d	70 c4 c6 d2 08 00 45 00	0.H. pE.
0010	01 28 00 00 40 00 40 06	2c 5d 5f d8 a3 24 0a 00	.(@.@.,]\$
0020	00 77 01 bb d4 74 d5 88	6f 74 7d 4c 1d 0f 50 18	.wt ot}LP.
0030	00 00 eb d0 00 00 ff ff	ff ff ff ff ff ff ff ff ff	
0040	ff ff ff ff ff ff ff ff	ff ff ff ff ff ff ff ff ff	
0050	ff ff ff ff ff ff ff ff	ff ff ff ff ff ff ff ff ff	
0060	ff ff ff ff ff ff ff ff	ff ff ff ff ff ff ff ff ff	
0070	ff ff ff ff ff ff ff ff	ff ff ff ff ff ff ff ff ff	••••••
0080	ff ff ff ff ff ff ff ff	ff ff ff ff ff ff ff ff ff	
0090	ff ff ff ff ff ff ff ff	ff ff ff ff ff ff ff ff ff	
00a0	ff ff ff ff ff ff ff ff	ff ff ff ff ff ff ff ff ff	
00b0	ff ff ff ff ff ff ff ff	ff ff ff ff ff ff ff ff ff	
00c0	ff ff ff ff ff ff ff ff	ff ff ff ff ff ff ff ff ff	
00d0	ff ff ff ff ff ff ff ff	ff ff ff ff ff ff ff ff	

	Image:												
🖉 📕 👩 💿 📄 🖺 🕱 🍯 🍳 🦛 🔿 🚈 🏹 🛃 🗐 🗐 🗨 Q. Q. T													
				• •									
	play litter < æ/>	Destination	Destant	ala lufa	Expression	T							
NO.	586234922 150003 10 0 0 119	05 216 163 36	TCP	$\frac{100}{78} = 54388 \rightarrow 443$	[SYN] Seg-0 Win-65535 Len-0 MSS-1460 WS-64	41							
2 15	586234922.346452 95.216.163.36	10.0.0.119	ТСР	70 54500 → 445 74 443 → 54388	[SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=								
5 1	0.0.2.74922.940332	95.216.163.36	ТСР	66 54388 → 443	[ACK] Seg=1 Ack=1 Win=131712 Len=0 TSval=18								
4 15	586234922.346904 10.0.0.119	95.216.163.36	TLSv1	583 Client Hello									
5 15	586234922.353697 95.216.163.36	10.0.0.119	TLSv1	310 [TCP ZeroWin	dow] , Ignored Unknown Record								
					ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva								
🖵 († r	raceroute confi	rms remo	te sei	ver is	ACK] Seq=1 ACK=518 Win=64/68 Len=0 ISval=5								
					ission] 443 \rightarrow 54388 [ACK] Seg=1 Ack=518 Wi								
h o	+	toppor	act	000	wn Record	1							
ne	rsuell-uerr-03	· Lorproj	ect.	org	wn Record								
		1 3		U	wn Record	l							
ll in	Furone)				RST] Seq=518 Win=0 Len=0								
					RST] Seq=518 Win=0 Len=0								
16 15	586234922 560059 10 0 0 119	95 216 163 36	тср	54 54388 → 443	RSIJ Seq=518 Win=0 Len=0								
17 15	586234922.730475 95.216.163.36	10.0.0.119	TLSv1	90 Application	Data	1							
▶ Frame 5:	310 bytes on wire (2480 bits), 310 bytes	captured (2480 bits) on	interface 0	(inbound)									
▶ Ethernet	II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:	c6:d2), Dst: Apple_05:30:	d7 (8c:85:90	:05:30:d7)									
▶ Internet	Protocol Version 4, Src: 95.216.163.36,	Dst: 10.0.0.119											
► Transmiss	sion Control Protocol, Src Port: 443, Dst	: Port: 54388, Seq: 1, Ack	k: 518, Len: 2	256									
Secure So	ockets Layer												
	ed UNKNOWN RECORD	(nown Record)											
	[Tanored Unknown Record]												
i i	[Severity level: Warning]												
[[Group: Protocol]												
0000 8c 85	5 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45	000.H. pE.											
0010 01 28	3 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a	00 .(@.@.,]\$				1							
0020 00 77	0 eb d0 00 00 ff	16 .WL. OL}LP. ff				1							
0040 ff ff	f ff f	ff				1							
0050 ff ff	f ff f	ff				1							
0000 TT TT 0070 ff ff	• •• •• •• •• •• •• •• •• •• •• •• •• •	ff											
0080 ff ff	f ff	ff											
0090 ff ff	f ff f	ff											
00a0 TT ff 00b0 ff ff	• •• •• •• •• •• •• •• •• •• •• •• •• •	ff											
00c0 ff ff	f ff f	ff											
00d0 ff ff	f ff f	ff											
😑 🍸 tor-p	project-fail			Pac	kets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.0 Profile: Defau	lt							

			tor-project-fail.tra	ace	
	📕 🧟 📄 🛅 🔀 🔇	(= _) 환 🚡 🕹			
					:
Appl	y a display filter <発/>			Expr	ession +
No.	Time Source	Destination	Protocol	Length Info	
	1 1586234922.150003 10.0.0.119	95.216.163.36	ТСР	$7854388 \rightarrow 443$ [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=	b4
	2 1580234922.340452 95.210.103.30		ТСР	$74 443 \rightarrow 54388$ [SIN, ACK] Seq=0 ACK=1 Win=05100 Len=0 M CC 54388 442 [ACK] Seq=1 Ack=1 Win=131712 Lon=0 TSval	-19
	4 1586234922 346904 10 0 0 119	95,216,163,36	TL Sv1	583 Client Hello	-10
	2 + 13002343221340304 + 1010101113	10.0.0.119		Ju [][P Zerowindow] . Ignored Unknown Record	
	6 1586234922.353811 10.0.0.119	95.216.163.36	ТСР	66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 T	Sva
	7 1586234922.541524 95.216 <u>.163.36</u>	10.0.0.119	ТСР	66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSva	l=5
	8 1586234922.541555 10.0.0			73 Alert (Level: Fatal, Description: Protocol Version)	
	9 1586234922.559911 95.216	rowser se	nds	1514 [TCP Retransmission] $443 \rightarrow 54388$ [ACK] Seq=1 Ack=518	Wi
	10 1586234922.559916 95.216 VIY N			1514 Ignored Unknown Record	
	11 1586234922.559918 95.216		.	1266 Ignored Unknown Record	
	12 1586234922.559920 95.210 The f	edular sta	rt ot	54 54388 \rightarrow 443 [RST] Seg=518 Win=0 Len=0	
	14 1586234922.560051 10.0.0	3		$54 + 54388 \rightarrow 443$ [RST] Seq=518 Win=0 Len=0	
	15 1586234922.560056 10.0.0 —	S handch	ako	54 54388 → 443 [RST] Seq=518 Win=0 Len=0	
	16 1586234922.560059 10.0.e 📿 I 🖵	Shahusha	ane	54 54388 → 443 [RST] Seq=518 Win=0 Len=0	
	17 1586234922.730475 95.216 <mark>.105.50</mark>	1010101115	12011	90 Application Data	
► Fran	ne 5: 310 bytes on wire (2480 bits), 310	bytes captured (2480 bits) on interfac	e 0 (inbound)	
► Ethe	ernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:7	0:c4:c6:d2), Dst: Apple_0	5:30:d7 (8c:8	5:90:05:30:d7)	
	ernet Protocol Version 4, Src: 95.216.163	.36, DST: 10.0.0.119	Ack: 519 L	on: 256	
	ire Sockets Laver	, DST POTT. 54588, Seq. 1	, ACK: 510, L	230	
	anored Unknown Record				
	[Expert Info (Warning/Protocol): Ignore	d Unknown Record]			
	[Ignored Unknown Record]				
	[Severity level: Warning]				
	[Group: Protocol]				
			_		
0000	8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 0 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 3	0045000.H.p 240a.00 (@@_]	.E.		
0020	00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d d	of 50 18 .wt ot}L	P.		
0030	00 00 eb d0 00 00 ff ff ff ff ff ff ff	f ff ff	•••		
0040	TT	T TT TT			
0060	ff	fffff			
0070	ff	f ff ff	•••		
0080	11 11 1T TT T	f ff ff			
00a0	ff	fffff	•••		
00b0	ff	fffff	•••		
0000					

.....

🔵 🍸 tor-project-fail

		🚄 tor-pi	roject-fail.trac	e		
	👩 💿 💼 🗂 🕱 🏹 🔍 🦛	🔿 🕸 🏹 🤳	Ð	Θ Θ $\overline{\bullet}$		
				•••		Fypression +
	Time Source	Destination	Protocol	ength Info		
1	1586234922.150003 10.0.0.119	95.216.163.36	TCP	78 54388 → 443 [SYI	N] Seq=0 Win=65535 Len=0 MSS=1	460 WS=64
2	1586234922.346452 95.216.163.36	10.0.0.119	ТСР	74 443 → 54388 [SYI	N, ACK] Seq=0 Ack=1 Win=65160	Len=0 MSS=
3	3 1586234922.346532 10.0.0.119	95.216.163.36	TCP	66 54388 → 443 [AC	K] Seq=1 Ack=1 Win=131712 Len=	0 TSval=18
4	1586234922.346904 10.0.0.119 1586234922 353697 95 216 163 36	95.216.163.36 10 0 0 110	TLSV1	583 Client Hello	1 Tanored Unknown Record	
	1560234922.555697 95.210.105.56	95.210.103.30		00 54388 → 443 IAU	KI Seg=518 ACK=257 WIN=131456	Len=0 TSva
7	1586234922.541524 95.216.163.36	10.0.0.119	ТСР	66 443 → 54388 [AC	K] Seq=1 Ack=518 Win=64768 Len	=0 TSval=5
8	1586234922 541555 10 0 0 110	05 046 460 06	TL 04	70 11	ich Description: Protocol Ve	rsion)
9	1586234922 Back comes	on linuer	T lei	CD roch	BRCO BREAK Seq=1	Ack=518 Wi…
10	1586234922 DACK CONICS	s an unusu		CI IESPU		
12	1586234922.559920 95.216.163.36	10.0.0.119	TLSv1	139 Ignored Unknown	Record	
13	1586234922.560036 10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RS	T] Seq=518 Win=0 Len=0	
14	1586234922.560051 10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RS]	T] Seq=518 Win=0 Len=0	
15		95.216.163.36	TCP	54 54388 → 443 [RS]	T] Seq=518 Win=0 Len=0	
10	1586234922.500059 10.0.119	95.210.103.30 10.0.0.119	TL Sv1	90 Application Data	a	
► Frame	5: 310 bytes on wire (2480 bits), 310 byte	s captured (2480 bits) on	interface	0 (inbound)		
▶ Ether	net II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4	:c6:d2), Dst: Apple_05:30	d7 (8c:85:	90:05:30:d7)		
▶ Inter	net Protocol Version 4, Src: 95.216.163.36,	Dst: 10.0.0.119				
► Trans	mission Control Protocol, Src Port: 443, Ds	t Port: 54388, Seq: 1, Ac	:k: 518, Len	: 256		
v Secure	e Sockets Layer Jored Unknown Record					
v Igi	[Expert Info (Warning/Protocol): Ignored Un	known Record]				
· · ·	[Ignored Unknown Record]					
	[Severity level: Warning]					
	[Group: Protocol]					
0000 80	85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45	5 000.H. pE.				
0010 01	28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a	a 00 .(@.@. ,]\$				
0020 00) 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50) 18 .wt ot}LP.				
0040 ff	f ff f	f ff				
0050 ff	ff	ff				
0060 ff	• 11 11 11 11 11 11 11 11 11 11 11 11 11	f ff				
0080 ff	ff	f ff				
0090 ff	·	f ff				
00b0 ff	ff	f ff				
00c0 ff	· ff	f ff				
0000						

😑 🏹 tor-project-fail

-				🚄 tor-pro	oject-fail.tra	ace		
L			È 🔀 🍯 🤇 🖛 🛛	🔶 😫 🐔 👱 属	÷			
	Apply a	display filter <発/>					Expression 🕂	
٢	lo.	Time	Source	Destination	Protocol	Length	Info	Ī
	_ 1	1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78	54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64	
	2	1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74	443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=	
	3	1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18	
~	- 4	1586234922.346904	10.0.0.119	95.216.163.36	TLSv1	583	Client Hello	
	5	1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310	[TCP ZeroWindow] , Ignored Unknown Record	
	6	1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66	54500 → 445 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva	
	7	1586234922 541524	95 216 163 36	10 0 0 119	TCP	66	443 → 54388 [ACK] Seg=1 Ack=518 Win=64768 Len=0 TSval=5	

TLSv1

TLSv1

TLSv1

TLSv1

TCP

TCP

TCP

TCP

TCP

 10
 1300234922.7300039
 10.0.0.119
 95.210.103.36
 10.0.119
 10.0.0.119

 17
 1586234922.730475
 95.216.163.36
 10.0.0.119
 TLSv1
 from sending any data

 Frame 5:
 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits) on interface
 from sending any data

Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)

95.216.163.36

10.0.0.119

10.0.0.119

10.0.0.119

10.0.0.119

95.216.163.36

95.216.163.36

95.216.163.36

95.216.163.36

▶ Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119

Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256

Secure Sockets Layer

Ignored Unknown Record

8 1586234922.541555 10.0.0.119

9 1586234922.559911 95.216.163.36

10 1586234922.559916 95.216.163.36

11 1586234922.559918 95.216.163.36

12 1586234922.559920 95.216.163.36

13 1586234922.560036 10.0.0.119

14 1586234922.560051 10.0.0.119

15 1586234922.560056 10.0.0.119

16 1586234922.560059 10.0.0.119

[Expert Info (Warning/Protocol): Ignored Unknown Record]
 [Ignored Unknown Record]
 [Severity level: Warning]
 [Group: Protocol]

0000	8c	85	90	05	30	d7	48	1d	70	c4	c6	d2	08	00	45	00	0.H.	pE.	
0010	01	28	00	00	40	00	40	06	2c	5d	5f	d8	a3	24	0a	00	.(@.@.	.]\$	
0020	00	77	01	bb	d4	74	d5	88	6f	74	7d	4c	1d	0f	50	18	.wt	ot}LP.	
0030	00	00	eb	dØ	00	00	ff												
0040	ff																		
0050	ff																		
0060	ff																		
0070	ff																		
0080	ff																		
0090	ff																		
00a0	ff																		
00b0	ff																		
00c0	ff																		
00d0	ff																		

🔵 🌠 tor-project-fail

73 Alert (Level: Fatal, Description: Protocol Version)

preventing my browser

Offered window is **0**,

[TCP Retransmission] 443 - 54388 [ACK] Seg-1 Ack-518

					🚄 tor-project-fail	.trace			
	(1 🛞 🖿 📑		2 🔶 🏟 🔨 🏹		÷ • •			
		display filter < \%/>				• •	•		 Expression
No	1 1 2 7 2	Time 9	Source	Destination	Protocol	Length Ir	nfo		
140.	1	1586234922.150003 1	10.0.0.119	95.216.163.3	6 TCP	78 5	54388 → 443 [SYN	1] Seg=0 Win=65535 Len=0 MSS=14	60 WS=64
	2	1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74 4	443 → 54388 [SYN	I. ACK] Seq=0 Ack=1 Win=65160 I	en=0 MSS=
	- 3	1586234922.346532	10.0.0.119	95,216,163,3	6 TCP	66 5	54388 → 443 [ACK	[] Seg=1 Ack=1 Win=131712 Len=0	TSval=18
	4	1586234922.346904	10.0.0.119	95.216.163.3	6 TLSv1	583 (Client Hello	() bed 1 men 1 men 101/12 20m 0	
М.	5	1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310	[TCP ZeroWindow]	. Ignored Unknown Record	
	6	1586234922.353811	10.0.0.119	95,216,163,3	6 TCP	66 5	54388 → 443 [ACK	(] Several ACK=227 WHU=121456 L	en=0 TSva
	7	1586234922.541524	95.216.163.36	10.0.0.119	ТСР	66 4	443 → 54388 [ACK	(] Seg=1 Ack=518 Win=64768 Len=	0 TSval=5
	8	1586234922.541555	L0.0.0.119	95.216.163.3	6 TLSv1	73 A	Alert (Level: Fa	atal. Description: Protocol Ver	sion)
	9	1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514	[TCP Retransmiss	sion] 443 → 54388 [ACK] Seg=1 A	ck=518 Wi
	10	1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514 1	Ignored Unknown	Record	
	11	1586234922.559918	95.216.163.36	10.0.0.119			9	Record	
	12	1586234922.559920	95.216.163.36	10.0.0.119	Doopor	noo id	o not	Record	
	13	1586234922.560036	10.0.0.119	95.216.163	RESPUI	150 13	5 1101 1] Seg=518 Win=0 Len=0	
	14	1586234922.560051 1	L0.0.0.119	95.216.163			Г] Seq=518 Win=0 Len=0	
	15	1586234922.560056 1	L0.0.0.119	95.216.163	wall for	mod	TIC] Seq=518 Win=0 Len=0	
	16	1586234922.560059 1	L0.0.0.119	95.216.163	WEII-IUI	meu] Seq=518 Win=0 Len=0	
	17	1586234922.730475	95.216.163.36	10.0.0.119			a	3	
	Frame	5: 310 bytes on wire	e (2480 bits),	310 bytes captured (24	80 bits) on interf	ace 0 (inbou	und)		
	Ethern	et II, Src: CiscoSpv	_c4:c6:d2 (48:	1d:70:c4:c6:d2), Dst:	Apple_05:30:d7 (8c	:85:90:05:30	0:d7)		
	Intern	et Protocol Version	4, Src: 95.216	.163.36, Dst: 10.0.0.1	.19				
	Trancm	iccion Control Broto	Src Port.	112, Det Dort. 51288,	Seq: 1, Ack: 518,	Len: 256			
	Secure	Sockets Layer							
	🔻 Igno	ored Unknown Record							
	. ▼ [Expert Info (Warning	g/Protocol): Ig	nored Unknown Record]					
		[Ignored Unknown R	ecord]						
		[Severity level: W	arning]						
		[Group: Protocol]							
00	00 8c	85 90 05 30 d7 48 1	d 70 c4 c6 d2	08 00 45 000.H	. pE.				
00	10 01	28 00 00 40 00 40 0	6 2c 5d 5f d8	a3 24 0a 00 .(@.@.	. ,]\$				
002	20 00	77 01 bb d4 74 d5 8	8 6f 74 7d 4c	1d 0f 50 18 .wt.	. ot}LP.				
00	30 00	00 eb d0 00 00 ff f	f ff ff ff ff	ff ff ff ff					
004	40 TT 50 ff	TT	T TT TT TT TT TT f ff ff ff ff	TT TT TT TT					
00	50 ff	ff ff ff ff ff ff ff ff	f ff ff ff ff	ff ff ff ff					
00	70 ff	ff ff ff ff ff ff ff	f ff ff ff ff	ff ff ff ff					

..... 😑 🏹 tor-project-fail

		🥖 tor-project-fail.trace
	🗎 🔀 🔇 ፍ 🌩	🖄 🚡 🛃 🔳 🔍 Q, Q, 🎹
Apply a display filter < %/>		

	Apply a	display filter <೫/>					Expression +
No.		Time	Source	Destination	Protocol	Length	Info
	1	1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78	54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64
	2	1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74 -	443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=
	3	1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
-	4	1586234922.346904	10.0.0.119	95.216.163.36	TLSv1	583	Client Hello
	5	1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310	[TCP ZeroWindow] , Ignored Unknown Record
	6	1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
	7	1586234922.541524	95.216.163.36	10.0.0.119	ТСР	66	443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
	8	1586234922.541555	10.0.0.119	95.216.163.36	TLSv1	73	Alert (Level: Fatal, Description: Protocol Version)
	9	1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514	[TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
	10	1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514	Ignored Unknown Record
	11	1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266	Ignored Unknown Record
	12	1586234922.559920	95.216.163.36	10.0.0.119	TLSv1	139	Ignored Unknown Record
	13	1586234922.560036	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0
	14	1586234922.560051	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0
	15	1586234922.560056	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0
	16	1586234922.560059	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0
	17	1586234922.730475	95.216.163.36	10.0.0.119	TLSv1	90	Application Data
	Frame	5: 310 bytes on wi	re (2480 bits), 310 bytes	captured (2480 bits) on	interfac	e 0 (inho	und)
	Ethern	et II, Src: CiscoS	ov_c4:c6:d2 (48:1d:70:c4:	c6:d2), Dst: Apple_05:30:	d7 (8c:8	5:90:05:3	30:d7)
	Intern	et Protocol Version	4. Src: 95.216.163.36.	Dst: 10.0.0.119			

▶ Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256

Secure Sockets Layer

0000	8c	85	90	05	30	d7	48	1d	70	c4	c6	d2	08	00	45	00	Ø.H. pE.
0010	01	28	00	00	40	00	40	06	2c	5d	5†	d8	aЗ	24	0a	00	.(@.@. ,]\$
0020	00	77	01	bb	d4	74	d5	88	6f	74	7d	4c	1d	Øf	50	18	.wt. ot}LP.
0030	00	00	eb	dØ	00	00	ff										
0040	ff																
0050	ff																
0060	ff																
0070	ff																
0080	ff																
0090	ff																
00a0	ff																
00b0	ff																
00c0	ff																
00d0	ff																

Ethernet frame

Ethernet (eth), 14 bytes

	🚄 tor-project-fail.trace	
	C 🔍 🔶 🚔 🚰 🛃 📃 🗮 🔍 Q Q) (
Apply a display filter < \%/>		

A	oply a	display filter <郑/>					Expression
No.		Time	Source	Destination	Protocol	Length	Info
	1	1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78	54388 \rightarrow 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64
	2	1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74	443 \rightarrow 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=
	3	1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18
-	4	1586234922.346904	10.0.0.119	95.216.163.36	TLSv1	583	Client Hello
	5	1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310	[TCP ZeroWindow] , Ignored Unknown Record
	6	1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
	7	1586234922.541524	95.216.163.36	10.0.0.119	ТСР	66	443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5
	8	1586234922.541555	10.0.0.119	95.216.163.36	TLSv1	73	Alert (Level: Fatal, Description: Protocol Version)
	9	1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514	[TCP Retransmission] 443 \rightarrow 54388 [ACK] Seq=1 Ack=518 Wi
	10	1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514	Ignored Unknown Record
	11	1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266	Ignored Unknown Record
	12	1586234922.559920	95.216.163.36	10.0.0.119	TLSv1	139	Ignored Unknown Record
	13	1586234922.560036	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0
	14	1586234922.560051	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0
	15	1586234922.560056	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0
Г	16	1586234922.560059	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0
	17	1586234922.730475	95.216.163.36	10.0.0.119	TLSv1	90	Application Data

Ethernet II, Src: CiscoSpy_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)

▶ Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119

▶ Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256

Secure Sockets Layer

0000	8c	85	90	05	30	d7	48	1d	70	c4	c6	d2	08	00	45	00	0.H. p <mark>E.</mark>
0010	01	28	00	00	40	00	40	06	2c	5d	5f	d8	a3	24	٧a	שש	.(@.@.,]\$
0020	00	77	01	bb	d4	74	d5	88	6f	74	7d	4c	1d	Øf	50	18	.wt ot}LP.
0030	00	00	eb	dØ	00	00	ff										
0040	ff																
0050	ff																
0060	ff																
0070	ff																
0080	ff																
0090	ff																
00a0	ff																
00b0	ff																
00c0	ff																
00d0	ff																

IP header

🔵 🌠 🛛 Internet Protocol Version 4 (ip), 20 bytes

	🚄 tor-project-fail.trace	
	🙆 🤇 🗢 🔿 🖄 🖉 🛃 🗐 🔍 Q Q 🏾	
Apply a display filter < \%/>		

	1 1 1 2		1						4
No).		Time	Source	Destination	Protocol	Length	Info	
		1	1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78	54388 \rightarrow 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64	
		2	1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74	$443 \rightarrow 54388$ [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=	
Т		3	1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…	
+		4	1586234922.346904	10.0.0.119	95.216.163.36	TLSv1	583	Client Hello	
		5	1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310	[TCP ZeroWindow] , Ignored Unknown Record	
		6	1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…	
		7	1586234922.541524	95.216.163.36	10.0.0.119	ТСР	66	443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5	
		8	1586234922.541555	10.0.0.119	95.216.163.36	TLSv1	73	Alert (Level: Fatal, Description: Protocol Version)	
Т		9	1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514	[TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…	
		10	1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514	Ignored Unknown Record	
		11	1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266	Ignored Unknown Record	
		12	1586234922.559920	95.216.163.36	10.0.0.119	TLSv1	139	Ignored Unknown Record	
		13	1586234922.560036	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	_
		14	1586234922.560051	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
		15	1586234922.560056	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
		16	1586234922.560059	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
		17	1586234922.730475	95.216.163.36	10.0.0.119	TLSv1	90	Application Data	

Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)

▶ Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119

▶ Transmission Control Protocol Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256

Secure Sockets Layer

0000	8c	85	90	05	30	d7	48	1d	70	c4	c6	d2	08	00	45	00	0.H. pE.
0010	01	28	00	00	40	00	40	06	2c	5d	5f	d8	a3	24	0a	00	.(@.@. ,]\$
0020	00	77	01	bb	d4	74	d5	88	6f	74	7d	4c	1d	0f	50	18	.wt ot}LP.
0030	00	00	cu	uv	00	00	ff	· · · · · · · · · · · · · · · · · · ·									
0040	ff																
0050	ff																
0060	ff																
0070	ff																
0080	ff																
0090	ff																
00a0	ff																
00b0	ff																
00c0	ff																
00d0	ff																

TCP header (0x1bb = 443)

Expression...

• • •		🚄 tor-project-fail.trace	
	🖹 🍯 🤇 🔶 🍝		
Apply a display filter $< \frac{2}{3}$			

Ар	oly a (display filter <೫/>					Expression	÷
No.		Time	Source	Destination	Protocol	Length	Info	ĺ
	1	1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78	54388 \rightarrow 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64	
	2	1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74	443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=	
	3	1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18	ł
-	4	1586234922.346904	10.0.0.119	95.216.163.36	TLSv1	583	Client Hello	
	5	1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310	[TCP ZeroWindow] , Ignored Unknown Record	ł
	6	1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…	i
	7	1586234922.541524	95.216.163.36	10.0.0.119	ТСР	66	443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5	1
	8	1586234922.541555	10.0.0.119	95.216.163.36	TLSv1	73	Alert (Level: Fatal, Description: Protocol Version)	
	9	1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514	[TCP Retransmission] 443 \rightarrow 54388 [ACK] Seq=1 Ack=518 Wi	
	10	1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514	Ignored Unknown Record	I
	11	1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266	Ignored Unknown Record	l
	12	1586234922.559920	95.216.163.36	10.0.0.119	TLSv1	139	Ignored Unknown Record	I
	13	1586234922.560036	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	ł
	14	1586234922.560051	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	í.
	15	1586234922.560056	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	l
	16	1586234922.560059	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	l
	17	1586234922.730475	95.216.163.36	10.0.0.119	TLSv1	90	Application Data	1

Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)

▶ Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119

Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 256

▶ Secure Sockets Layer

			Payload is	
0000 0010	8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00 01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00	0.H. pE. .(@.@. ,]\$	256 Oxff's	
0020	00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18	.wt ot}LP.	200 0/11 3	
0030	ff	· · · · · · · · · · · · · · · · · · ·		
0050	ff	•••••		
0000	ff			
0080	ff			
0090 00a0	ff	•••••		
00b0	ff			
00c0 00d0	tt tt tt tt tt tt tt tt tt ff ff ff ff f			

								_ +											
		:						tor-proj	ect-fail.t	race									
		۵ ک			२ 🔶 🗖		A	2		Ð Ð		E							
Ap	ply a d	lisplay filter	、<郑/>														Exp	ression	+
No.		Time	So	ource		Destination			Protocol	Length	Info								
	1	1586234922	.150003 10	0.0.0.119		95.216.1	163.36		ТСР	78	54388	→ 443	[SYN]	Seq=0 Win=	=65535	Len=0 MS	S=1460 WS=	=64	
	2	1586234922	.346452 95	5.216.163.36		10.0.0.1	L19		ТСР	74	443 →	54388	[SYN,	ACK] Seq=0) Ack=1	Win=651	60 Len=0 №	1SS=	
	2	1596224022	.346533 10	2.0.0.110		95.216.1	163.36		ТСР	66	54388	→ 443	[ACK]	Seq=1 Ack=	=1 Win=	131712 L	en=0 TSval	l=18	
	4	1586234922	.346904 10	0.0.0.119		95.216.1	163.36		TLSv1	583	Clien	t Hello)						
	5	1586234922	.353697 95	5.216.163.36		10.0.0.1	19		TLSv1	310	[TCP	ZeroWi	ndow]	Ignored L	Jnknown	Record			
	U	1300234922		0.0.0.119		95.216.1	L63.36		ТСР	66	54388	→ 443	[ACK]	Seq=518 Ac	ck=257	Win=1314	56 Len=0 T	rSva	
	7	1586234922	.541524 95	5.216.163.36		10.0.0.1	L19		ТСР	66	443 →	54388	[ACK]	Seq=1 Ack=	=518 Wi	n=64768	Len=0 TSva	al=5	
	8	1506224022	E41EEE 10	0 0 110		<mark>05 2</mark> 16.1	163.36		TLSv1	73	Alert	(Leve	l: Fata	al, Descrip	otion:	Protocol	Version)		
	9					.0.1	119		ТСР	1514	[TCP	Retrans	smissio	on] 443 → 5	54388 [ACK] Seq	=1 Ack=518	3 Wi	
	10	Red	ΟΙΛ Γ	OOK O		.0.1	L19		TLSv1	1514	Ignor	ed Unkı	nown Re	ecord					
	11		- j -		J	.0.1	L19		TLSv1	1266	Ignor	ed Unkı	nown Re	ecord					
	12	7 100		+		.0.1	L19		TLSv1	139	Ignor	ed Unkı	nown Re	ecord					
	13		isec	io ar	rive	16.1	163.36		ТСР	54	54388	→ 443	[RST]	Seq=518 Wi	in=0 Le	n=0			
	14					16.1	163.36		ТСР	54	54388	→ 443	[RST]	Seq=518 Wi	in=0 Le	n=0			
	15	1586234922	.560056 10	0.0.0.119		95.216.1	163.36		ТСР	54	54388	→ 443	[RST]	Seq=518 Wi	in=0 Le	n=0			
	16	1586234922	.560059 10	0.0.0.119		95.216.1	163.36		ТСР	54	54388	→ 443	[RST]	Seq=518 Wi	in=0 Le	n=0			
	17	1586234922	.730475 95	5.216.163.36		10.0.0.1	L19		TLSv1	90	Appli	cation	Data						
▶ Fr	ame !	5: 310 byte	s on wire	(2480 bits),	310 bytes	capture	d (2480 b	oits) on i	Interfa	ce 0 (in	oound)								
► Et	hern	et II, Src:	CiscoSpv_	_c4:c6:d2 (48:	1d:70:c4:c	6:d2), [Ost: Appl	le_05:30:c	17 (8c:	85:90:05	30:d7)								
▶ Ir	nterne	et Protocol	Version 4	4, Src: 95.216	5.163.36, D	st: 10.0	0.0.119												
▶ <mark>T</mark> I	ansm	ission Cont	rol Protoc	col, Src Port:	443, Dst	Port: 54	4388, Sec	q: 1, Ack:	518,	Len: 256									
Se Se	ecure	Sockets La	yer																
▼	Igno	red Unknow	n Record																

[Expert Info (Warning/Protocol): Ignored Unknown Record]
 [Ignored Unknown Record]
 [Severity level: Warning]
 [Group: Protocol]

0000	8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00	0.H. pE.
0010	01 28 00 00 40 00 40 06 2c 5d 5f d8 a3 24 0a 00	.(@.@. ,]\$
0020	00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 50 18	.wt. ot}LP.
0030	00 00 eb d0 00 00 ff	
0040	ff	
0050	ff	
0060	ff	
0070	ff	
0080	ff	
0090	ff	
00a0	ff	
00b0	ff	
00c0	ff	
00d0	ff	

		🚄 tor	-project-fail.trace	
	🔬 💿 🖿 🗋 🕱 🔇	◆ ◆ 🖄 🛉 🛓 📃		
Apply a	display filter <೫/>			Expression +
No.	Time Source	Destination	Protocol Length	Info
_ 1	1586234922.150003 10.0.0.119	95.216.163.36	TCP 7	8 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64
2	1586234922.346452 95.216.163.36	10.0.0.119	TCP 7	4 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=
3	1586234922.346532 10.0.0.119	95.216.163.36	TCP 6	6 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18
4	1586234922.346904 10.0.0.119	95.216.163.36	TLSV1 21	3 Ullent Hello
7	1586234922.541524 95.216.163.36	10.0.0.119	TCP 6	$6 443 \rightarrow 54388$ [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5
8	1586234922.541555 10.0.0.119	95.216.163.36	TLSv1 7	3 Alert (Level: Fatal. Description: Protocol Version)
9	1586234922.559911 95.216.163.36	10.0.0.119	TCP 151	4 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10	1586234922.559916 95.216.163.36	10.0.119	TLSv1 151	4 Ignored Unknown Record
11	1586234922.559918 95.216.163.36	10.0.119	TLSv1 126	6 Ignored Unknown Record
12	1586234922.559920 95.216.163.36	10.0.119	TLSv1 13	9 Ignored Unknown Record
13 14 15 16 17	¹⁵⁸⁶ ¹⁵⁸⁶ Was this res ¹⁵⁸⁶ Or was it <i>in</i>	ponse from	n an <i>in</i> -	path middlebox?
▶ Frame	5: 31 OI Was IL III			
▶ Ethern	net II,			
▶ Intern	net Protocol Version 4, Src: 95.216.16	3.36, Dst: 10.0.0.119	Asks E10 Lans DE	
	Alssion Control Protocol, Src Port: 44	-3, DST POFT: 54388, Seq: 1,	ACK: 518, Len: 250	
	ored Unknown Record			
v Ign	[Expert Info (Warning/Protocol): Igno	ed Unknown Record]		
	[Ignored Unknown Record]			
	[Severity level: Warning]			
	[Group: Protocol]			
0000 8c	85 90 05 30 d7 48 1d 70 c4 c6 d2 08	00 45 000.H. pE.		
0010 01	28 00 00 40 00 40 06 2c 5d 5f d8 a3	24 0a 00 .(@.@.,]\$		
0020 00	77 01 DD 04 74 05 88 61 74 70 4C 10 00 eb d0 00 00 ff ff ff ff ff ff ff	ff ff ff		
0040 ff	ff	ff ff ff		
0050 ff	ff	ff ff ff		
0060 ff		ft tt tt		
0080 ff	ff	ff ff ff		
0090 ff	ff	ff ff ff		
00a0 ff	ff	ff ff ff		
0000 ff	TT	TT TT TT		
00d0 ff	ff	ff ff ff		
O ℤ 1	tor-project-fail			Packets: 20 · Displayed: 20 (100.0%) · Load time: 0:0.0 Profile: Default

		🚄 tor-p	project-fail.tra	ce
	🔬 💿 📄 🗋 🏹 🕥 🦛	⇒ 😤 주 👱 📃	Œ	
Apply a	display filter <%/>		:	Expression +
No.	Time Source	Destination	Protocol	Length Info
1	1586234922.150003 10.0.0.119	95.216.163.36	ТСР	78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
2	1586234922.346452 95.216.163.36	10.0.0.119	ТСР	74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
3	1586234922.346532 10.0.0.119	95.216.163.36	ТСР	66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4	1586234922.346904 10.0.0.119	95.216.163.36	TLSv1	583 Client Hello
• 5	1586234922.353697 95.216.163.36	10.0.0.119	TLSv1	310 [TCP ZeroWindow] , Ignored Unknown Record
6	1586234922.353811 10.0.0.119	95.216.163.36	ТСР	66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7	1586234922.541524 95.216.163.36	10.0.0.119	ТСР	66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8	1586234922.541555 10.0.0.119	95.216.163.36	TLSv1	73 Alert (Level: Fatal, Description: Protocol Version)
9	1586234922.559911 95.216.163.36	10.0.0.119	ТСР	1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10	1586234922.559916 95.216.163.36	10.0.0.119	TLSv1	1514 Ignored Unknown Record
11	1586234922.559918 95.216.163.36	10.0.0.119	TLSv1	1266 Ignored Unknown Record
12	1586234922.559920 95.216.163.36	10.0.0.119	TLSv1	139 Ignored Unknown Record
13	1586234922.560036 10.0.0.119	95.216.163.36	ТСР	E4 E4289 . 442 [DET] Cog=E19 Win=0 Lon=0
14	1586234922.560051 10.0.0.119	95.216.163.36	ТСР	
15	1586234922.560056 10.0.0.119	95.216.163.36	ТСР	
16	1586234922.560059 10.0.0.119	95.216.163.36	ТСР	
17	1586234922.730475 95.216.163.36	10.0.0.119	TLSv1	
▶ Frame	9: 1514 bytes on wire (12112 bits), 1514 k	oytes captured (12112 bits	s) on inte	another reply with
▶ Ethern	net II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4		0:d7 (8c:8	
▶ Intern	net Protocol Version 4, Src: 95.216.163.36,	Dst: 10.0.0.119		<i>// 1</i>
▶ Transm	nission Control Protocol, Src Port: 443, De	st Port: 54388 Seq: 1, A	ck: 518	same sequence # !
				came coquerios in .
0000 8c	85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 4	5 000.H. pE.		
0000 8c 0010 05	85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 4 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0	5 000.H. pE. a 00@.+\$		0
0000 8c 0010 05 0020 00	85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 4 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 8	5 000.H. pE. a 00@.+\$ 0 10 .wt ot}L		
0000 8c 0010 05 0020 00 0030 01	85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 4 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 8 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6 91 16 03 04 74 22 02 00 00 21 5	5 000.H. pE. a 00@.+\$ 0 10 .wt. ot}L b 73Cvks b d9 d z v. ([0
0000 8c 0010 05 0020 00 0030 01 0040 34 0050 40	85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 4 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 8 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6 91 16 03 03 00 7a 02 00 00 76 03 2f 5 7a 14 5d bd 36 38 27 4e 40 df 91 5d dd dd <td< td=""><td>5 000.H. pE. a 00@.+\$ 0 10 .wt ot}L b 73Cv/[. b 56 @z.l.68' N@.lV</td><td></td><td></td></td<>	5 000.H. pE. a 00@.+\$ 0 10 .wt ot}L b 73Cv/[. b 56 @z.l.68' N@.lV		
0000 8c 0010 05 0020 00 0030 01 0040 34 0050 40 0060 45	85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 4 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 8 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6 91 16 03 03 00 7a 02 00 00 76 03 32 f<5	5 000.H. pE. a 00@.+\$ 0 10 .wt ot}L b 73C"vks b d9 4zv/[. b 56 @z.].68' N@]V 9 c5 Ez		
0000 8c 0010 05 0020 00 0030 01 0040 34 0050 40 0060 45 0070 70	85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 4 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 8 fa 43 f6 00 01 01 08 0a 22 76 c1 c4 6 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 04 04 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f 6d 20 c9 2e 2e 5f ea <t< td=""><td>5 000.H. pE. a 00@.+\$ 0 10 .wt. ot}L b 73Cvks b d9 4zv/[. b 56 @z.].68' N@]V 9 c5 Ez 2 6a pmlQ.yj</td><td></td><td></td></t<>	5 000.H. pE. a 00@.+\$ 0 10 .wt. ot}L b 73Cvks b d9 4zv/[. b 56 @z.].68' N@]V 9 c5 Ez 2 6a pmlQ.yj		
0000 8c 0010 05 0020 00 0030 01 0040 34 0050 40 0060 45 0070 70 0080 24	85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 4 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 8 fa 43 f6 00 01 01 08 0a 22 76 c1 c4 6 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0d 0a aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f 6d 20 c9 2e 2e 5f ea <t< td=""><td>5 000.H. pE. a 00@.+\$ 0 10 .wt. ot}L b 73Cvks b d9 4zv/[. b 56 @z.].68' N@]V 9 c5 Ez 2 6a pmlQ.yj 3 02 \$V]cP.</td><td></td><td></td></t<>	5 000.H. pE. a 00@.+\$ 0 10 .wt. ot}L b 73Cvks b d9 4zv/[. b 56 @z.].68' N@]V 9 c5 Ez 2 6a pmlQ.yj 3 02 \$V]cP.		
0000 8c 0010 05 0020 00 0030 01 0040 34 0050 40 0060 45 0070 70 0080 24 0090 00	85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 4 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 8 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0 aa 99 b0 b6 off 88 a1 20 15 b3 7a 1a 20 f 6d 20 c9 2e bc 5f ea <t< td=""><td>5 000.H. pE. a 00@.+\$ 0 10 .wt. ot}L b 73Cvks b d9 4zv/[. b 56 @z.].68' N@]V 9 c5 Ez. 2 6a pmlQ.yj 3 02 \$V].cP d 00+3.\$</td><td></td><td></td></t<>	5 000.H. pE. a 00@.+\$ 0 10 .wt. ot}L b 73Cvks b d9 4zv/[. b 56 @z.].68' N@]V 9 c5 Ez. 2 6a pmlQ.yj 3 02 \$V].cP d 00+3.\$		
0000 8c 0010 05 0020 00 0030 01 0040 34 0050 40 0060 45 0070 70 0080 24 0090 00 00a0 20	85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 4 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 8 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0 0a aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f 6d 20 c9 2e bc 5f <td< td=""><td>5 000.H. pE. a 00@.+\$ 0 10 .wt. ot}L b 73Cv/[. b 56 @z.].68' N@]V 9 c5 Ez 2 6a pmlQ.yj 3 02 \$V].cP d 00+3.\$ f e3J.W K.je?.</td><td></td><td></td></td<>	5 000.H. pE. a 00@.+\$ 0 10 .wt. ot}L b 73Cv/[. b 56 @z.].68' N@]V 9 c5 Ez 2 6a pmlQ.yj 3 02 \$V].cP d 00+3.\$ f e3J.W K.je?.		
0000 8c 0010 05 0020 00 0030 01 0040 34 0050 40 0060 45 0070 70 0080 24 0090 00 0080 24 0090 00 00b0 f3 00c0 4b	85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 4 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 8 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0 0 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f 6 20 c9 2 2e bc 5f	5 000.H. pE. a 00@.+\$ 0 10 .wt. ot}L b 73C"vks b d9 4zv/[. b 56 @z.].68' N@.]V 9 c5 Ez 2 6a pmlQ.yj 3 02 \$V].cP d 00+3.\$ f e3J.W. K.j.e?. f cc		

🔵 🏹 tor-project-fail

		🗾 tor-project-fail.trace	
A O A A A	📄 🔝 🕅 9	🔶 🌩 警 🚡 🛓 📃 🔍	
Apply a display filter	< %/>		

	1177						
Nc		Time	Source	Destination	Protocol	ength Info	
	1	1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78 54388 → 443	3 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64
	2	1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74 443 → 54388	3 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=
	3	1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66 54388 → 443	3 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18
	4	1586234922.346904	10.0.0.119	95.216.163.36	TLSv1	583 Client Hell	lo
•	5	1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310 [TCP ZeroWi	indow] , Ignored Unknown Record
	6	1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66 54388 → 443	3 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
	7	1586234922.541524	95.216.163.36	10.0.0.119	ТСР	66 443 → 54388	3 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5
	8	1586234922.541555	10.0.0.119	95.216.163.36	TLSv1	73 Alert (Leve	el: Fatal, Description: Protocol Version)
Т	9	1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514 [TCP Retrar	nsmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
	10	1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514 Ignored Un	known Record
	11	1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266 Ignored Un	known Record
	12	1586234922.559920	95.216.163.36	10.0.0.119	TLSv1	139 Ignored Un	known Record
T	13	1586234922.560036	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443	3 [RST] Seq=518 Win=0 Len=0
	14	1586234922.560051	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443	3 [RST] Seq=518 Win=0 Len=0
	15	1586234922.560056	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443	3 [RST] Seq=518 Win=0 Len=0
	16	1586234922.560059	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443	3 [RST] Seq=518 Win=0 Len=0
	17	1586234922.730475	95.216.163.36	10.0.0.119	TLSv1	90 Applicatior	n Data

▶ Frame 9: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0 (inbound)

Ethernet II, Src: CiscoSpv_c4:c6:d2 (48:1d:70:c4:c6:d2), Dst: Apple_05:30:d7 (8c:85:90:05:30:d7)

▶ Internet Protocol Version 4, Src: 95.216.163.36, Dst: 10.0.0.119

▶ Transmission Control Protocol, Src Port: 443, Dst Port: 54388, Seq: 1, Ack: 518, Len: 1448

But more data ...

0000	8c	85	90	05	30	d7	48	1d	70	c4	c6	d2	08	00	45	00	0.H. pE.
0010	05	dc	9b	9b	40	00	2b	06	a1	0d	5f	d8	a3	24	0a	00	@.+\$
0020	00	77	01	bb	d4	74	d5	88	6f	74	7d	4c	1d	0f	80	10	.wt ot}L
0030	01	fa	43	f6	00	00	01	01	08	0a	22	76	c1	c4	6b	73	C"vks
0040	34	91	16	03	03	00	7a	02	00	00	76	03	03	2f	5b	d9	4zv/[.
0050	40	7a	14	5d	bd	36	38	27	4e	40	df	91	5d	0d	0b	56	@z.].68' N@]V
0060	45	aa	99	b0	b6	0f	88	a1	20	15	b3	7a	1a	20	f9	c5	Ez
0070	70	6d	20	с9	2e	2e	bc	5f	ea	6c	51	1f	79	b4	12	6a	pmlQ.yj
0080	24	f5	86	83	56	13	14	fc	a5	5d	d8	81	63	50	13	02	\$V]cP
0090	00	00	2e	00	2b	00	02	03	04	00	33	00	24	00	1d	00	+3.\$
00a0	20	bb	d2	4a	8d	57	df	ec	4b	01	6a	13	81	65	3f	e3	J.W K.je?.
00b0	f3	d4	0a	37	ac	e7	82	09	b7	d1	c5	be	e4	86	0f	сс	7
00c0	4b	14	03	03	00	01	01	17	03	03	00	2a	6d	33	28	8c	K*m3(.
00d0	2a	e5	39	91	df	b3	1e	ee	ac	8f	af	df	07	a7	1f	1c	*.9

Expression...

									【 tor-project-fai	l.trace			
	J	۲	01010 01101 01110	×	9		$\mathbf{\widehat{\uparrow}}$	<u> </u>		Ð	Θ) (
Annly	a display	filtor 2	₩/~										

 <i> </i>	Apply a	display filter <郑/>					Expression	
No.		Time	Source	Destination	Protocol	Length	Info	
	1	1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78	54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64	
	2	1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74	443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=	
	3	1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…	
	4	1586234922.346904	10.0.0.119	95.216.163.36	TLSv1	583	Client Hello	
ł	5	1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310	[TCP ZeroWindow] , Ignored Unknown Record	
	6	1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…	
	7	1586234922.541524	95.216.163.36	10.0.0.119	ТСР	66	443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5	
	8	1586234922.541555	10.0.0.119	95.216.163.36	TLSv1	73	Alert (Level: Fatal, Description: Protocol Version)	
	9	1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514	[TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…	
	10	1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514	Ignored Unknown Record	
	11	1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266	Ignored Unknown Record	
	12	1586234922.559920	95.216.163.36	10.0.0.119	TLSv1	139	Ignored Unknown Record	
	13	1586234922.560036	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
	14	1586234922.560051	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
	15	1586234922.560056	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
	16	1586234922.560059	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
	17	1586234922.730475	95.216.163.36	10.0.0.119	TLSv1	90	Application Data	

[Next sequence number: 1449 (relative sequence number)]

Acknowledgment number: 518 (relative ack number)

1000 \dots = Header Length: 32 bytes (8)

▶ Flags: 0x010 (ACK)

Window size value: 506 [Calculated window size: 64768] [Window size scaling factor: 128] Checksum: 0x43f6 [unverified] [Checksum Status: Unverified] Urgent pointer: 0

▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

[SEQ/ACK analysis]

TCP payload (1448 bytes)

Retransmitted TCP segment data (1448 bytes)

8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00E. 0000 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 0010 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 .w...t.. ot}L.... 0020 0030 P1 1a 45 10 00 00 01 01 00 0a 22 70 C1 C4 0D 75 IICIIII II VIIN 0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[. 0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V 0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E..... ...z. ... 0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm_ .lQ.y..j 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 \$...V... .l..cP.. 0080 0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?. 00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc7..... 00c0 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c 00d0 🔽a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9....

And it's meaningful data

D	()																					🚺 to	or-p	oro	ject	-fa	il.tr	ace	9				
						J							01010 01101 01110	×	2	2	 (2)				<u>.</u>		-				(+	2	Θ	=			
П	Δ	n	əlv	а	di	spl	av	fil	ter	< 3	₩/>	>																								

No.		Time	Source	Destination	Protocol	Length Info
	1	1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78 54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 …
	2	1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=…
	3	1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
	4	1586234922.346904	10.0.0.119	95.216.163.36	TLSv1	583 Client Hello
ł	5	1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310 [TCP ZeroWindow] , Ignored Unknown Record
	6	1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
	7	1586234922.541524	95.216.163.36	10.0.0.119	ТСР	66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
	8	1586234922.541555	10.0.0.119	95.216.163.36	TLSv1	73 Alert (Level: Fatal, Description: Protocol Version)
	9	1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
	10	1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514 Ignored Unknown Record
	11	1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266 Ignored Unknown Record
	12	1586234922.559920	95.216.163.36	10.0.0.119	TLSv1	139 Ignored Unknown Record
	13	1586234922.560036	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0
	14	1586234922.560051	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0
	15	1586234922.560056	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0
	16	1586234922.560059	10.0.0.119	95.216.163.36	ТСР	54 54388 → 443 [RST] Seq=518 Win=0 Len=0
	17	1586234922.730475	95.216.163.36	10.0.0.119	TLSv1	90 Application Data

[Next sequence number: 1449 (relative sequence number)] Acknowledgment number: 518 (relative ack number)

1000 \dots = Header Length: 32 bytes (8)

▶ Flags: 0x010 (ACK)

Window size value: 506 [Calculated window size: 64768] [Window size scaling factor: 128] Checksum: 0x43f6 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 Followed by additional meaningful data

▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

[SEQ/ACK analysis]

TCP payload (1448 bytes)

Retransmitted TCP segment data (1448 bytes)

8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00E. 0000 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 0010 .w...t.. ot}L.... 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 0020 ..C.... .."v..ks 0030 01 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6b 73 0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[. 0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V 0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E..... ...z. ... 0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm_ .lQ.y..j 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 \$...V... .l..cP.. 0080 0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?. 00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc7..... 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c 00c0 00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9.....

Expression...

					tor-project-fail.trac	Э		
				ヽ 🌩 🚔 春 👱	.	Θ		
	Арр	ly a d	lisplay filter <発/>				Expression +	
No).		Time Source	Destination	Protocol L	ength	Info	Ī
		1	1586234922.150003 10.0.0.119	95.216.163.36	ТСР	78	$354388 \rightarrow 443$ [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64	
		2	1500254922.540452 95.210.105.50	95,216,163,36	ТСР	66	$4 + 443 \rightarrow 54366$ [STN, ACK] Seq=0 ACK=1 Win=05160 Len=0 MSS=	
		4	1586234922.346904 10.0.0.119	95.216.163.36	TLSv1	583	3 Client Hello	
ł		5	1586234922.353697 95.216.163.36	10.0.0.119	TLSv1	310	0 [TCP ZeroWindow] , Ignored Unknown Record	
		6	1586234922.353811 10.0.0.119	95.216.163.36	ТСР	66	5 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…	
		7	1586234922.541524 95.216.163.36	10.0.0.119	TCP	66	5 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5	
		0	1586774077 541555 14 H H H H	95.216.163.36	TLSV1	1514	Alert (Level: Fatal, Description: Protocol Version)	
		9	1386234922.339911 93.210.103.30	10.0.0.119	TL Sv1	1514	4 [ICP Retrainsmission] 443 \rightarrow 54366 [ACR] 584=1 ACR=516 Wi	
		11	1586234922.559918 95.216.163.36	10.0.0.119	TLSv1	1266	5 Ignored Unknown Record	
		12	1586234922.559920 95.216.163.36	10.0.0.119	TLSv1	139	9 Ignored Unknown Record	J
		13	1586234922.560036 10.0.0.119	95.216.163.36	ТСР	54	4 54388 → 443 [RST] Seq=518 Win=0 Len=0	
		14	1586234922.560051 10.0.0.119	95.216.163.36	TCP	54	4 54388 → 443 [RST] Seq=518 Win=0 Len=0	
		15 16	1586234922.560056 10.0.0.119	95.216.163.30		54 54	4 54388 → 443 [RST] Seq=518 Win=0 Len=0	
		17	1586234922.730475 95.216.163.36	10.0.0.119	TLSv1	90	0 Application Data	
		[Nex	t sequence number: 1449 (relati	ve sequence number)]				
		Ackn	owledgment number: 518 (relativ	ve ack number)	This c	lat	to started arriving	
		1000	\dots = Header Length: 32 bytes (8	3)	11115 0	αι	la starteu arriviriy	
		rtag Wind	S: 0X010 (ACK) ow size value: 506		000			
		[Cal	culated window size: 64768]		~ 200	m	sec after my browser's	
		[Win	dow size scaling factor: 128]					
		Chec	ksum: 0x43f6 [unverified]		hande	h	aka initiation	
		[Che	cksum Status: Unverified]		TIATIUS			
		Urge Onti	nt pointer: 0 and: (12 bytes) No Operation (NO) No Operation (NOD) Time	stamps			
		[SE0	/ACK analysisl	, NO-Operation (NOP), Time	scallips			
		TCP	payload (1448 bytes)					
		Retr	ansmitted TCP segment data (1448 k	ytes)				
0	000	8c	85 90 05 30 d7 48 1d 70 c4 c6 d2	08 00 45 000.H. p	E.			ŕ
0	010	05	dc 9b 9b 40 00 2b 06 a1 0d 5f d8	a3 24 0a 00@.+	.\$			J
0	020 030	00 01	// 01 bb d4 /4 d5 88 6t /4 /d 4c fa 43 f6 00 00 01 01 08 0a 22 76	1d 0f 80 10 .wt ot}L	ks			
0	040	34	91 16 03 03 00 7a 02 00 00 76 03	03 2f 5b d9 4zv.	./[.			
0	050	40	7a 14 5d bd 36 38 27 4e 40 df 91	5d 0d 0b 56 @z.].68' N@]V			
0	070	45 70	6d 20 c9 2e 2e bc 5f ea 6c 51 1f	79 b4 12 6a pml0.	 yj			
0	080	24	f5 86 83 56 13 14 fc a5 5d d8 81	63 50 13 02 \$V]	cP			
0	090 0a0	00 20	00 2e 00 2b 00 02 03 04 00 33 00 bb d2 4a 8d 57 df ec 4b 01 6a 13	24 00 1d 00+	\$			
0	0b0	f3	d4 0a 37 ac e7 82 09 b7 d1 c5 be	e4 86 0f cc7				
0	0c0	4b	14 03 03 00 01 01 17 03 03 00 2a	6d 33 28 8c K *r	m3(.			

*.9....

00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c

🗧 🕒 🖉 🖉	
Apply a display filter <\%/>	Express

No.		Time	Source	Destination	Protocol	Length	Info	
	1	1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78	54388 \rightarrow 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64	
	2	1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74	443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=	
	3	1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18	
	4	1586234922.346904	10.0.0.119	95.216.163.36	TLSv1	583	Client Hello	
•	5	1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310	[TCP ZeroWindow] , Ignored Unknown Record	
	6	1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…	
	7	1596224022 541524	05 216 162 26	10 0 0 110	TCD	66	442 . 54288 [ACK] Sog-1 Ack-518 Win-64768 Lon-0 TSvo]=5	
	8	1586234922.541555	10.0.0.119	95.216.163.36	TLSv1	73	Alert (Level: Fatal, Description: Protocol Version)	
	У	1280234922.229911	95.210.103.30	10.0.119	TCP	1514	[ICP RETRANSMISSION] 443 → 54388 [ACK] SEQ=1 ACK=518 Wi…	
	10	1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514	Ignored Unknown Record	
	11	1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266	Ignored Unknown Record	
	12	1586234922.559920	95.216.163.36	10.0.0.119	TLSv1	139	Ignored Unknown Record	
	13	1586234922.560036	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
	14	1586234922.560051	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
	15	1586234922.560056	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
	16	1586234922.560059	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
	17	1586234922.730475	95.216.163.36	10.0.0.119	TLSv1	90	Application Data	

[Next sequence number: 1449 (relative sequence number)] Acknowledgment number: 518 (relative ack number)

1000 \dots = Header Length: 32 bytes (8)

▶ Flags: 0x010 (ACK)

Window size value: 506 [Calculated window size: 64768] [Window size scaling factor: 128] Checksum: 0x43f6 [unverified] [Checksum Status: Unverified] But by then, my browser had already given up

▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

[SEQ/ACK analysis]

Urgent pointer: 0

TCP payload (1448 bytes)

Retransmitted TCP segment data (1448 bytes)

8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00E. 0000 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 0010 .w...t.. ot}L.... 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 0020 01 fa 43 f6 00 00 01 01 ..C.... .."v..ks 0030 08 0a 22 76 c1 c4 6b 73 0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[. 0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V 0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 pm_ .lQ.y..j 0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 \$...V... .l..cP.. 0080 0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?. 00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc7..... 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c 00c0 00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9.....

											tor-pro	ject-fail.	trace			
		J	۲		01010 01101 01110	×	6	 Q		$\widehat{\mathbf{r}}$			Ð	Θ		
Ar	nlv a	display	/ filter	< \#/>												

_		J 0. 4							
Ν	lo.		Time	Source	Destination	Protocol	Length	Info	
		1	1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78	54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64	
		2	1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74	443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=	
Ι		3	1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…	
	_	4	1586234922 346904	10 0 0 119	95 216 163 36	TLSv1	583	Client Hello	
ł		5	1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310	[TCP ZeroWindow] , Ignored Unknown Record	
		6	1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…	
		7	1586234922.541524	95.216.163.36	10.0.0.119	ТСР	66	443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5	
		8	1586234922.541555	10.0.0.119	95.216.163.36	TLSv1	73	Alert (Level: Fatal, Description: Protocol Version)	
Ι		9	1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514	[TCP Retransmission] 443 \rightarrow 54388 [ACK] Seq=1 Ack=518 Wi	
		10	1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514	Ignored Unknown Record	
		11	1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266	Ignored Unknown Record	
		12	1586234922.559920	95.216.163.36	10.0.0.119	TLSv1	139	Ignored Unknown Record	
1		13	1586234922.560036	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	-
		14	1586234922.560051	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
		15	1586234922.560056	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
		16	1586234922.560059	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
		17	1586234922.730475	95,216,163,36	10.0.0.119	TLSv1	90	Application Data	_

[Next sequence number: 1449 (relative sequence number)]

Acknowledgment number: 518 (relative ack number)

1000 \dots = Header Length: 32 bytes (8)

▶ Flags: 0x010 (ACK)

Window size value: 506 [Calculated window size: 64768] [Window size scaling factor: 128] Checksum: 0x43f6 [unverified] [Checksum Status: Unverified] Urgent pointer: 0

Verdict:

▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

[SEQ/ACK analysis]

TCP payload (1448 bytes)

Retransmitted TCP segment data (1448 bytes)

8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00E. 0000 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24 0a 00 0010 .w...t.. ot}L.... 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 0020 ..C.... .."v..ks 0030 01 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6b 73 0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[. 0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V 0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E..... ...z. ... 0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm_ .lQ.y..j \$...V....]..cP.. 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 0080 0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?. 00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc7..... 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c 00c0 00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9....

Expression.

										【 tor-p	roject-fa	ail.trace	2		
		٦	۲		01010	×	9		$\overline{\mathbf{A}}$			+	Θ	9	
An	nlv a	dienlay	/ filtor	~ \L/>											

	pryat							
No.		Time	Source	Destination	Protocol	Length	Info	
	1	1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78	54388 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64	
	2	1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74	443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=	
	3	1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…	
	4	1586234922 346904	10 0 0 119	95 216 163 36	TI Sv1	583	Client Hello	
ł	5	1586234922.353697	95.216.163.36	10.0.0.119	TLSv1	310	[TCP ZeroWindow] , Ignored Unknown Record	
	6	1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66	54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…	
	7	1586234922.541524	95.216.163.36	10.0.0.119	ТСР	66	443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5	
	8	1586234922.541555	10.0.0.119	95.216.163.36	TLSv1	73	Alert (Level: Fatal, Description: Protocol Version)	
	9	1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514	[TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…	
	10	1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514	Ignored Unknown Record	
	11	1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266	Ignored Unknown Record	
	12	1586234922.559920	95.216.163.36	10.0.0.119	TLSv1	139	Ignored Unknown Record	
	13	1586234922.560036	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	-
	14	1586234922.560051	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
	15	1586234922.560056	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
	16	1586234922.560059	10.0.0.119	95.216.163.36	ТСР	54	54388 → 443 [RST] Seq=518 Win=0 Len=0	
	17	1586234922.730475	95.216.163.36	10.0.0.119	TLSv1	90	Application Data	

[Next sequence number: 1449 (relative sequence number)]

Acknowledgment number: 518 (relative ack number)

1000 = Header Length: 32 bytes (8)

Flags: 0x010 (ACK) Window size value: 506

[Calculated window size: 64768] [Window size scaling factor: 128] Checksum: 0x43f6 [unverified] [Checksum Status: Unverified] Urgent pointer: 0

Verdict: injection! And apparently courtesy of Comcast!

▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

[SEQ/ACK analysis]

TCP payload (1448 bytes)

Retransmitted TCP segment data (1448 bytes)

8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00 45 00E. 0000 05 dc 9b 9b 40 00 2b 06 0010 a1 0d 5f d8 a3 24 0a 00 .w...t.. ot}L.... 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0f 80 10 0020 ..C.... .."v..ks 0030 01 fa 43 f6 00 00 01 01 08 0a 22 76 c1 c4 6b 73 0040 34 91 16 03 03 00 7a 02 00 00 76 03 03 2f 5b d9 4.....z. ..v../[. 0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 0d 0b 56 @z.].68' N@..]..V 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20 f9 c5 E..... ...z. ... 0060 0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 b4 12 6a pm_ .lQ.y..j 24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02 \$...V... .l..cP.. 0080 0090 00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00 00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3 ..J.W.. K.j..e?.7..... 00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86 0f cc 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 33 28 8c 00c0 00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c *.9.....

Expression



lold.reddit.com

C

Comcast's XFi advanced security is autoblocking torproject.org (ERR_SSL_PROTOCOL_ERROR) : TOR



	📕 1	tor-project-fail.tra	ce		
	🗅 🔿 😟 🏹 🎝		Θ Θ $\overline{\Psi}$		
Apply a display filter <%/>				Expression	ł.
No. Time Source	Destination	Protocol	Length Info		
	95.216.163.36	TCP	78 54388 → 443 [SYN] Seq=0 Win=6	5535 Len=0 MSS=1460 WS=64	
2 1586234922.346452 95.216.163.36	10.0.0.119	TCP	74 443 → 54388 [SYN, ACK] Seq=0	Ack=1 Win=65160 Len=0 MSS=	i I
3 1586234922.346532 10.0.0.119	95.216.163.36	TCP	$66 54388 \rightarrow 443 \text{ [ACK] Seq=1 ACK=1}$	Win=131/12 Len=0 ISval=18	1
		TI SV1	583 (Lient Hello		
5 1580234922.353097 95.210.103.30		TLSV1	310 [TCP Zerowindow] , Ignored Un	known Record	
7 1596224922.555611 10.0.0.119	10 0 0 110		$00 54300 \rightarrow 445 [ACK] 580=10 ACK = 66 442 + 54299 [ACK] 500=1 Ack=5$	-257 WIN-151450 Len=0 TSVa	I.
2 1586234922.541524 95.210.105.50 9 1586234022 541555 10 0 0 110	05 216 163 36		73 Alert (level: Estal Descript)	ion: Protocol Version)	
0 1586234022 550011 05 216 163 36	10 0 0 110	TCP	1514 [TCP Petransmission] 443 - 54	388 [ACK] Seg-1 Ack-518 Wi	
10 1586234922 559916 95 216 163 36	10.0.0.119	TL Sv1	1514 [ICF RecFallShirtssion] $443 \rightarrow 54$ 1514 Tanored Unknown Record	566 [ACK] 564-1 ACK-516 WI	1
11 1586234922.559918 95.216.163.36	10.0.0.119	TLSV1	1266 Ignored Unknown Record		
12 1586234922.559920 95.210105150	1010101115				
13 1586234922,560036 10.0				•	Ľ
14 1586234922.560051 10.0. D OC	neral can	dete	ct packet inject	ion —	
15 1586234922.560056 10.0.	iorai, cari		er paener nijeer		
16 1586234922.560059 10.0.		- 1	line a multiple for a		
17 1586234922.730475 95.21 DECA	lse origina	ai reb	lies arrive too.		1
[Next sequence number: 1449	<u></u>				
Acknowledgment number: 518					
1000 = Header Length:					
▶ Flags: 0x010 (ACK)					
Window size value: 506					
[Calculated window size: 64					
[Window size scaling factor					
Checksum: 0x43f6 [unverifie					
[Checksum Status: Unverifie					
Urgent pointer: 0					
Options: (12 bytes), No-Operation (NOP), No	-Operation (NOP), Times	tamps			
[SEQ/ACK analysis]					
TCP payload (1448 bytes)					L
Retransmitted TCP segment data (1448 bytes)					
0000 8c 85 90 05 30 d7 48 1d 70 c4 c6 d2 08 00) 45 000.H. p	.Ε.			ň
0010 05 dc 9b 9b 40 00 2b 06 a1 0d 5f d8 a3 24	4 0a 00@.+\$	5			
0020 00 77 01 bb d4 74 d5 88 6f 74 7d 4c 1d 0	80 10 .wt ot}L				
	-5b d9 4 z v d				
0050 40 7a 14 5d bd 36 38 27 4e 40 df 91 5d 00	1 0b 56 @z.].68' N@]	. V			
0060 45 aa 99 b0 b6 0f 88 a1 20 15 b3 7a 1a 20) f9 c5 Ez.				
0070 70 6d 20 c9 2e 2e bc 5f ea 6c 51 1f 79 be	12 6a pmlQ.y.	. j			
) 13 02 \$V]Ch) 1d 00 + 3 ¢	•••			
00a0 20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 6	5 3f e3J.W K.ie	?			
00b0 f3 d4 0a 37 ac e7 82 09 b7 d1 c5 be e4 86	6 0f cc7				
00c0 4b 14 03 03 00 01 01 17 03 03 00 2a 6d 3	3 28 8c K*m3	3(.			
00d0 2a e5 39 91 df b3 1e ee ac 8f af df 07 a	/ 1† 1c *.9				

🔘 🍸 🛛 The TCP payload of this packet (tcp.payload), 1448 bytes

				🧲 tor-project-fail.trace			
			🕨 🌩 警 春 👱				
	ly a display filter <発/>					~	Expression
No.	Time	Source	Destination	Protocol Length	Info		
	1 100000 10000 10000	2 10 0 0 110	05 010 100 00	TCD 70	F 4200 442 [C	FEDE 1 0 MCC 14CO	110 04

1 1586234922.150003	10.0.0.119	95.216.163.36	ТСР	78 54388 \rightarrow 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64
2 1586234922.346452	95.216.163.36	10.0.0.119	ТСР	74 443 → 54388 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=
3 1586234922.346532	10.0.0.119	95.216.163.36	ТСР	66 54388 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=18…
4 1586234922 346904	10 0 0 119	95 216 163 36	TLSv1	583 Client Hello
5 1586234922 . 353697	95.216.163.36	10.0.0.119	TLSv1	310 [TCP ZeroWindow] , Ignored Unknown Record
6 1586234922.353811	10.0.0.119	95.216.163.36	ТСР	66 54388 → 443 [ACK] Seq=518 Ack=257 Win=131456 Len=0 TSva…
7 1586234922.541524	95.216.163.36	10.0.0.119	ТСР	66 443 → 54388 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=5…
8 1586234922 541555	10.0.0.119	95-216-163-36	TI Sv1	73 Alert (Level: Fatal Description: Protocol Version)
9 1586234922.559911	95.216.163.36	10.0.0.119	ТСР	1514 [TCP Retransmission] 443 → 54388 [ACK] Seq=1 Ack=518 Wi…
10 1586234922.559916	95.216.163.36	10.0.0.119	TLSv1	1514 Ignored Unknown Record
11 1586234922.559918	95.216.163.36	10.0.0.119	TLSv1	1266 Ignored Unknown Record

13 1586234922.560036 10.0. In general, can detect packet injection 14 1586234922.560051 10.0. 15 1586234922.560056 10.0 16 1586234922.560059 10.0 because original replies arrive too. 17 1586234922.730475 95.21 [Next sequence number: 1449

This includes detecting **RST injection** [Calculated window size: 64 [Window size scaling factor Checksum: 0x43f6 [unverifie used to censor/control traffic. [Checksum Status: Unverifie

▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

[SEQ/ACK analysis]

Urgent pointer: 0

▶ Flags: 0x010 (ACK) Window size value: 506

TCP payload (1448 bytes)

12 1586234922.559920 95.21

Acknowledgment number: 518 1000 = Header Length:

Retransmitted TCP segment data (1448 bytes)

```
8c 85 90 05 30 d7 48 1d
                                                    0000
                            70 c4 c6 d2 08 00 45 00
0010
     05 dc 9b 9b 40 00 2b 06
                            a1 0d 5f d8 a3 24 0a 00
                                                    00 77 01 bb d4 74 d5 88
                            6f 74 7d 4c 1d 0f 80 10
                                                    .w...t.. ot}L....
0020
                                                    ..C.... .."v..ks
0030
     01 fa 43 f6 00 00 01 01
                            08 0a 22 76 c1 c4 6b 73
0040
     34 91 16 03 03 00 7a 02
                            00 00 76 03 03 2f 5b d9
                                                    4.....z. ..v../[.
0050
     40 7a 14 5d bd 36 38 27
                            4e 40 df 91 5d 0d 0b 56
                                                    @z.].68' N@..]..V
     45 aa 99 b0 b6 0f 88 a1
                            20 15 b3 7a 1a 20 f9 c5
0060
                                                    0070
     70 6d 20 c9 2e 2e bc 5f
                            ea 6c 51 1f 79 b4 12 6a
                                                    pm ...._ .lQ.y..j
0080
     24 f5 86 83 56 13 14 fc a5 5d d8 81 63 50 13 02
                                                    $...V... .]..cP..
0090
     00 00 2e 00 2b 00 02 03 04 00 33 00 24 00 1d 00
                                                    00a0
     20 bb d2 4a 8d 57 df ec 4b 01 6a 13 81 65 3f e3
                                                     ..J.W.. K.j..e?.
00b0
     f3 d4 0a 37 ac e7 82 09
                            b7 d1 c5 be e4 86 0f cc
                                                    ...7.... .....
     4b 14 03 03 00 01 01 17
                            03 03 00 2a 6d 33 28 8c
                                                    K....*m3(,
00c0
     2a e5 39 91 df b3 1e ee ac 8f af df 07 a7 1f 1c
00d0
                                                    *.9.....
```

The Problem of Spam
Spam: Unwanted Messages

- Endemic networking problem:
 - If network is open & sending is cheap, miscreants will abuse to transmit low-value messages at massive scale
 - Scale means low value still reaps benefits

Spam: Unwanted Messages

- Endemic networking problem:
 - If network is open & sending is cheap, miscreants will abuse to transmit low-value messages at massive scale
 - Scale means low value still reaps benefits
- Old as the hills
 - Telegram spam in 1864!
 - Energetic arms race
- You probably don't care ...
- ... but you should:
 - Bankrolls development of botnets (*incentivizes attacks*)
 - Gateway drug to more serious cybercrime
 - Today's bane: ransomware





Run captive bot binaries in VMs (repurposed worm *honeyfarm*)



Make sure they can't send any actual spam (but think they are)





Crawler pretends to be a worker and relentlessly asks Storm proxies for work ("**milking**")





Types of Storm C&C Messages

- Activation (report from bot to botmaster)
- Email address harvests
- Spamming instructions
- Delivery reports
- DDoS instructions
- FastFlux instructions
- HTTP proxy instructions
- Sniffed passwords report
- IFRAME injection/report

Campaign mechanics: harvest



Campaign mechanics: harvest



Campaign mechanics: spamming



MACRO	SEEN LIVE	FUNCTIONALITY	
(0)	\checkmark	Spam target email address.	
(A)	\checkmark	FQDN of sending bot, as reported to the bot as part of the preceding C&C exchange.	
(B)		Creates content-boundary strings for multi-part messages.	
(Cnum)	\checkmark	Labels a field's resulting content, so it can be used elsewhere through (V); see below.	
(D)	\checkmark	Date and time, formatted per RFC 2822.	
(E)		ROT-3-encodes the target email address.	
(Fstring)	\checkmark	Random value from the dictionary named string. ²	
(Gstring)	\checkmark	Line-wrap string into 72 characters per line.	
(Hstring)		Defines hidden text snippets with substitutions, for use in HTML- and plain-text parts.	
(I)	\checkmark	Random number between 1 and 255, used to generate fake IP addresses.	
(Jstring)		Produces quoted-printable "=20" linewrapping.	
(K)		IP address of SMTP client.	
(M)	\checkmark	6-character string compatible with Exim's message identifiers (keyed on time).	
(N)		16-bit prefix of SMTP client's IP address.	
(Ostring:num)	\checkmark	Randomized message identifier element compatible with Microsoft SMTPSVC.	
(Pnum ₁ [-num ₂]:string)	\checkmark	Random string of num_1 (up to num_2 , if provided) characters taken from <i>string</i> .	
(Qstring)		Quoted-printable "=" linewrapping.	
$(Rnum_1-num_2)$	\checkmark	Random number between num_1 and num_2 . Note, special-cased when used with (D).	
(Ustring)		Randomized percent-encoding of string.	
(Vnum)	\checkmark	Inserts the value of the field identified by (Cnum).	
(W)		Time and date as plain numbers, e.g. "20080225190434".	
(X)		Previously selected member of the "names" dictionary.	
(Ynum)	\checkmark	8-character alphanumeric string, compatible with Sendmail message identifiers.	
(Z)	\checkmark	Another Sendmail-compatible generator for message identifiers.	

Table 2: Storm's spam-generation templating language.

```
Received: from auz.xwzww ([132.233.197.74]) by dsl-189-188-79-63.prod-infinitum.com.mx with ▷
Microsoft SMTPSVC(5.0.2195.6713); Wed, 6 Feb 2008 16:33:44 -0800
Message-ID: <002e01c86921$18919350$4ac5e984@auz.xwzww>
From: <katiera@experimentalist.org>
To: <voelker@cs.ucsd.edu>
Subject: JOB $1800/WEEK - CANADIANS WANTED!
Date: Wed, 6 Feb 2008 16:33:44 -0800
```

Figure 2: Snippet of a spam template, showing the transformation of an email header from template (top) to resulting content (bottom). The \triangleright -symbol indicates line continuations. Bold text corresponds to the formatting macros and their evaluation.

Campaign mechanics: spamming



Money mule scam Attemps to enroll the victim in money laundering schemes	V
	V
Personal ad scam Fake dating/matchmaking invitations intended to convince victim to advance money	/
Job ads Variant of money-mule scams, new "employee" is asked to forward money or goods	S
Self-propagation Tricks or lures victims into executing malicious binaries ¹	
Phishing Entices victims to enter sensitive information at fake bank sites or similars	
Pharmaceutical Pointers to web sites selling Viagra, Cialis, and other "male enhancement" products	\$
Stock scam Tries to convince victim to buy a particular stock suppsedly about to increase in value	ue
Other ads Other kinds of advertising	
Image spam Image-based spam ²	
Other Broken or empty templates, noise-only templates, etc. ³	

Table 3: Meanings of campaign classes.



Figure 5: Classes and instances of spaming campaigns identified over time.

Storm did a wide variety of shortlived spam campaigns likely for hire



Figure 5: Classes and instances of spaming campaigns identified over time.

Plus steady pharma spam ... likely botmaster's own



Figure 5: Classes and instances of spaming campaigns identified over time.

And occasional *stupid Postcards* spam to freshen the bot army

Campaign mechanics: reporting



Measurements: delivery efficacy



Measurements: delivery efficacy



DNS Blacklists (DNSBL)

- Spammer vulnerability: activities broadly visible
 Defenders with large "telescopes" can view early ...
 - and distill & disseminate signatures for blocking
- Easy signature: IP address of sender
- Easy way to disseminate signatures: DNS





-			
-	-	_	0
_	=		
=		-	
			0

Mail Server A

If B forwards the mail, or when B originates mail

DNSBL Server Z "Is B a spammer" Mail Server B SMTP: "I have some email for you" Z will see that B both makes a lot of lookups over time, and gets Mail Server C looked up a lot over time

DNSBL Counter-Intelligence

- Counter-intelligence: learning about your adversary via their own attempts to gather intel
- The utility of a bot plummets if on a DNSBL
- For a spammer considering buying a set of bots, they <u>need to determine this</u>
 - Need to look up the bots themselves ...
 - ... often using an existing bot to proxy their lookup



Idea: operator of Z *seeds* analysis with list of Known Bad addresses. For any such system, *which other addresses* A_i did it look up in a burst? Add A_i to Known Bad addresses list and *recurse* \Rightarrow **enumerate botnet**.

Can also seed with systems that do bursts of lookups and aren't themselves looked up in non-bursts.

Counter-Intelligence, con't

- Bill M. probes spyware C&C using set of scanning hosts S_i
- C&C operators noticed some of these S_j and blacklisted them (TCP RST reply) ...
- ... but didn't find $\frac{a}{o}$ of them (S_k)
- So: Bill scans entire Internet from S_j system and from S_k system
 - System replying to latter but not to former ⇒
 managed by the C&C operator
 - Allows enumeration!

How Much \$\$ Do Spammers Make?

We drive cash your way.

PARINERS	Site map Server Time: 2011	-11-10 16:10 Tickets Logout
Affiliate ID: 17788 Balance:	Home / FAQ	
\$0.00 Payments:	Frequently Asked Questions	Help for this Section: Eng / Rus
\$0.00 Hold	How do you pay?	
Stats	What are your payment plans?	
Creatives	What should I do to join you?	
Settings	What do you sell? What if I don't live in the US&2 May I become your affiliate?	
Payments	Where can I monitor the statistics of my site?	
Advanced	When do you ship the orders? Can Ladvertise a specific product, not the whole pharmacy?	
Info	What is the commission on the refill orders?	
Contacts	I need help configuring my templates what do I do? I lost my password, what do I do? Are you accepting call centers?	

How do you pay?

Skype: 🕄 mark affiliate

Skype: 😡 vanessa-affiliate

mary_ryan_affiliate

Skype: 🚫 liza affiliate

Vanessa 🐨 644

Sandra 356

Skype: 🔝

Liza 634

Mary Ryan 608

We pay every week on Thursday with a 2 weeks' holdback. \$50 minimum on stormpay and wires. If you require larger amounts sent at one time you can set the minimum yourself.

Payment by request is now available. Effective from 07.17.2006

Our loyal affiliates now have the chance to minimize the hold period and to get the money when they need it. Even though it will be handled individually in every case the guidelines are simple.

You should have the steady sales record for the last 3 months (that is your daily average should be at least 3 sales for the above mentioned period) and your traffic source can be easily tracked. This will not apply to the commission earned during special promotions and we won't be able to pay to PayPal earlier than scheduled. You are welcome to use Bank Wire, Epass, Egold, Webmoney and

What are your payment plans?

Our affiliate program offers 3 levels of RevShare.

You can choose to receive 30, 40 or 50% from sale. Prices of products increase with each new level of Revshare. You can set ANY price provided that it is higher than the base price (price of product at 30%).

For example, viagra 100mg x 10 pills, has the following prices:

- \$29.95 (30%)
- \$35.95 (40%)
- \$49.95 (50%)
- You cannot set the price lower than \$29.95
- Any price between \$29.95 and \$35.95 will give you Revshare of 30%
- Any price between \$35.95 and \$49.95 will give you Revshare of 40%
- Any price higher than \$49.95 will give you Revshare of 50%

To change the price enter the new figure in "Your Price" window and click on the arrow next to it. The forcast of price per pill and your commission will be shown. Click on the Save button at the buttom of the screen to enable the new prices. (If you don't click on the arrow the "Save" button won't work)

You can also change all prices by setting a needed percentage in "Value", (in the upper part of interface), or by coping the prices from another Tracking id.

Please note that some products may have only one or two levels of Revshare.

How do you know that this is "my" customer?

First, your affiliate id is clearly visible in the site's url. Our program leaves a cookie at a customer's computer to identify him at the return. And finally the customer creates an account at our site. He is sure to remember his original login name as we offer great bonuses for the returning customers.



These folks seem trustworthy ...



... how about these?





Kirill Levchenko

klevchen@cs.ucsd.edu

I am a project scientist with the <u>Systems and Networking</u> group in the Computer Science department at the University of California, San Diego. My current research


