КОМПАНИЯ ТТК

Практические аспекты противодействия DDOS атакам

Емельянов Роман Сергеевич
Директор Дирекции информационной безопасности
30.09.2010

DDoS #1

Жертва: оператор связи

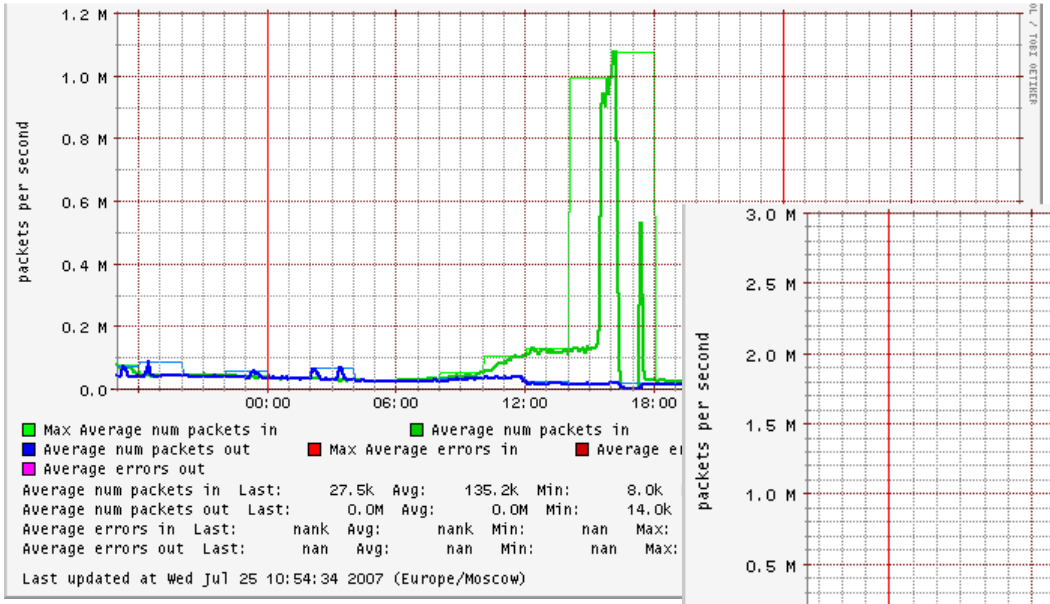
Профиль трафика: icmp echo-request

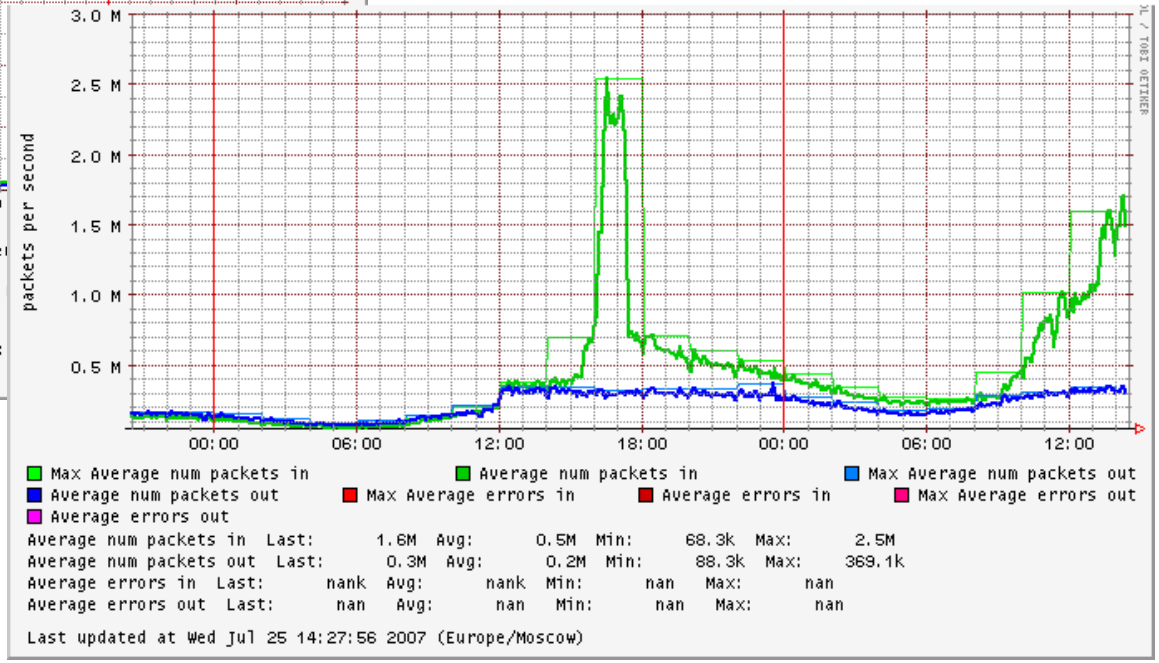
Сеть: /14, /16, /19

Год: 2007

Меры: acl drop icmp permit any
локализация в рамках одного канала

DDoS #1


packets per second
1.2 M
1.0 M
0.8 M
0.6 M
0.4 M
0.2 M
0.0
00:00
06:00
12:00
18:00
Max Average num packets in
Average num packets in
Average num packets out
Max Average errors in
Average errors out
Average num packets in Last: 27.5k Avg: 135.2k Min: 8.0k
Average num packets out Last: 0.0M Avg: 0.0M Min: 14.0k
Average errors in Last: nank Avg: nank Min: nan Max:
Average errors out Last: nan Avg: nan Min: nan Max:
Last updated at Wed Jul 25 10:54:34 2007 (Europe/Moscow)


packets per second
3.0 M
2.5 M
2.0 M
1.5 M
1.0 M
0.5 M
00:00
06:00
12:00
18:00
00:00
06:00
12:00
Max Average num packets in
Average num packets in
Max Average num packets out
Average num packets out
Max Average errors in
Average errors in
Max Average errors out
Average errors out
Average num packets in Last: 1.6M Avg: 0.5M Min: 68.3k Max: 2.5M
Average num packets out Last: 0.3M Avg: 0.2M Min: 88.3k Max: 369.1k
Average errors in Last: nank Avg: nank Min: nan Max: nan
Average errors out Last: nan Avg: nan Min: nan Max: nan
Last updated at Wed Jul 25 14:27:58 2007 (Europe/Moscow)

DDoS #2

Жертва: веб портал

Профиль трафика: смешанный

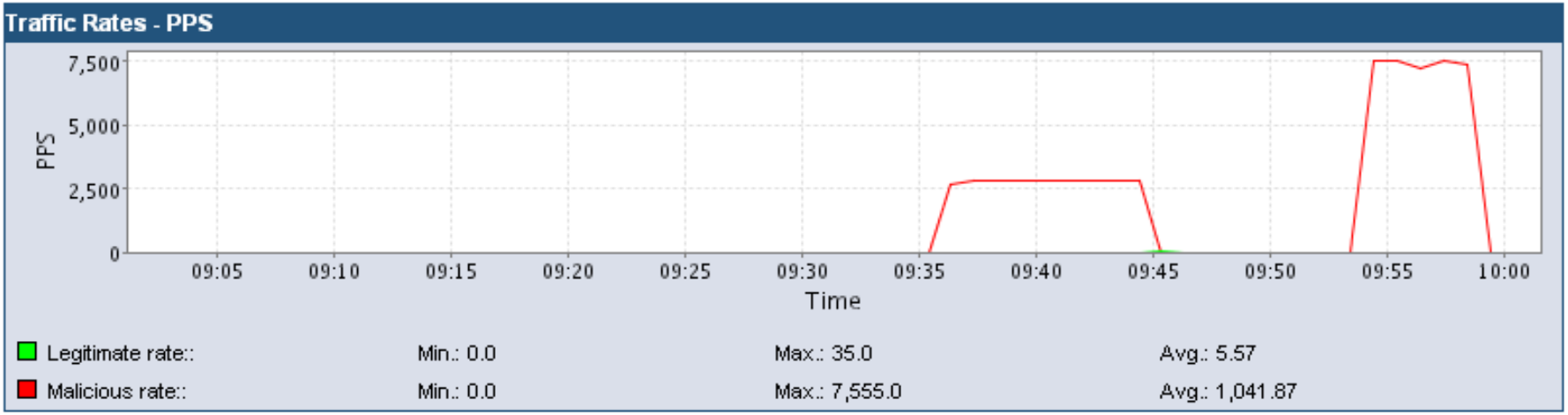
Сеть: /32

Год: 2008

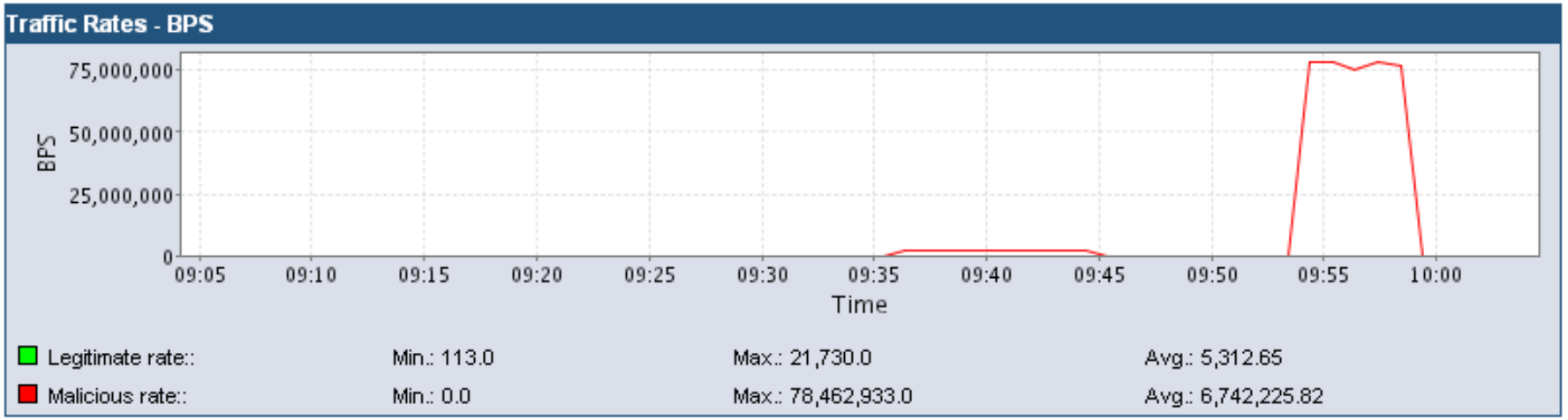
Меры: acl permit http drop any,
http-redirect,
javascript-redirect

DDOS #2: DNS amplification

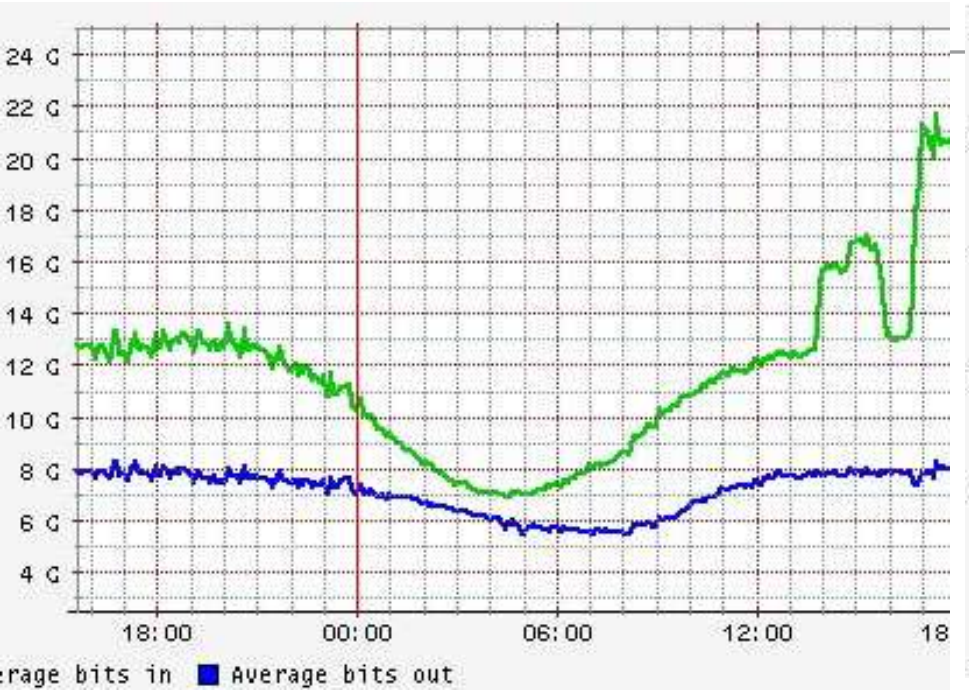
7500 / 2500 = 3

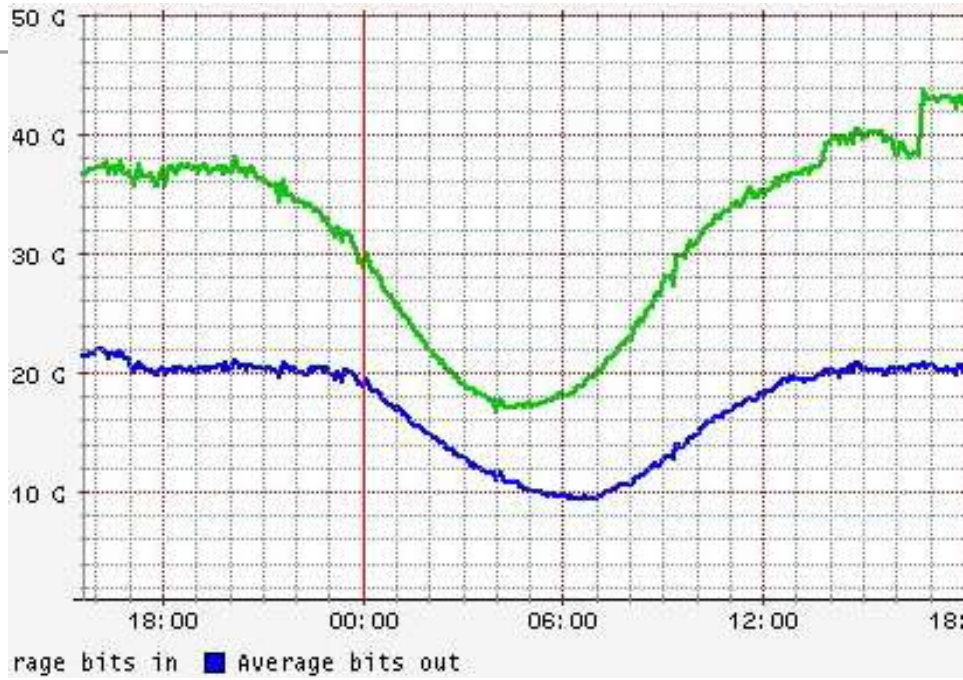


75000000 / 1500000 = 50



DDOS #2: DNS amplification





(21−13)+(45−38)=15 Gbps

DDoS #3

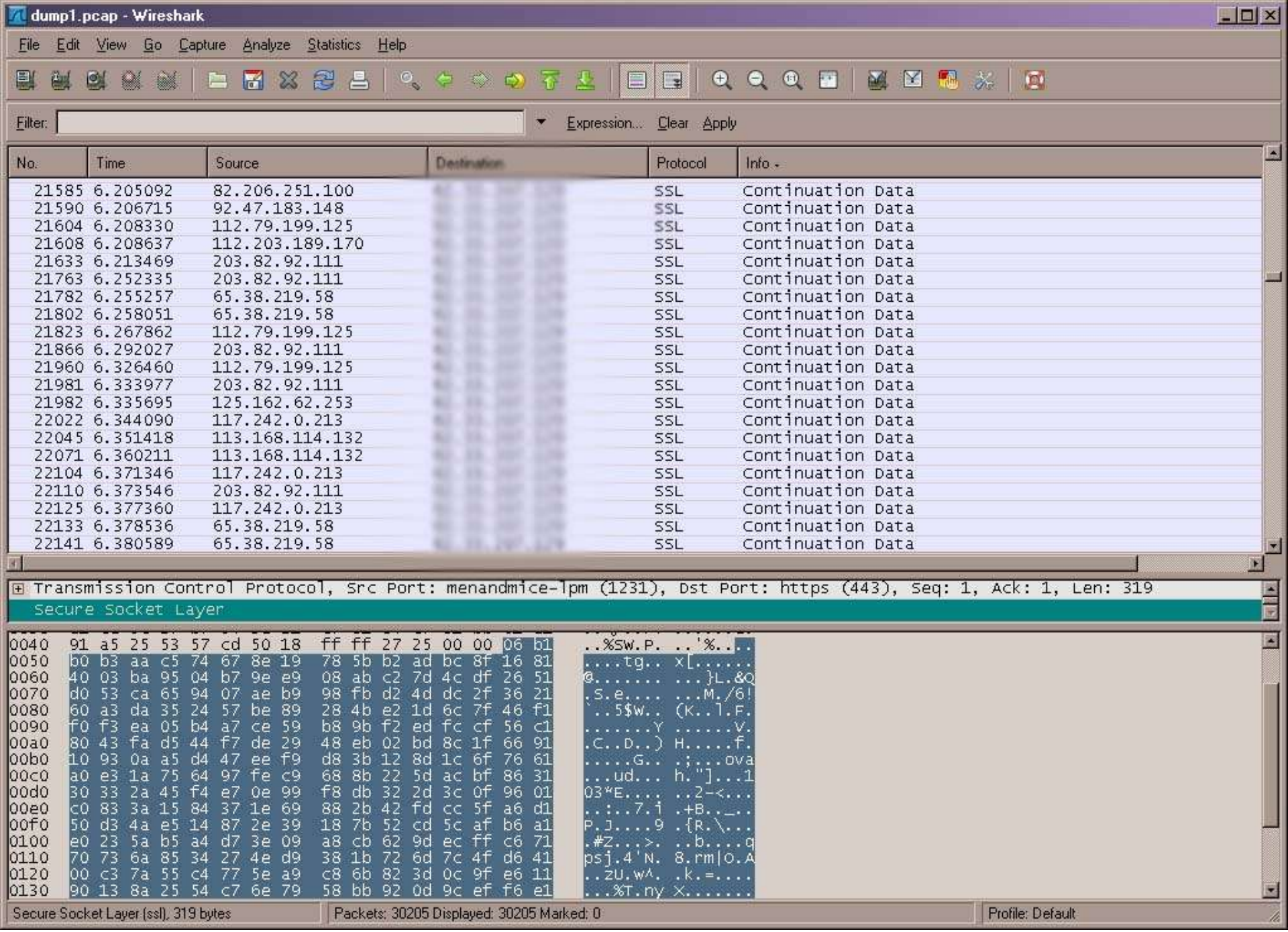
Жертва: платёжная система

Профиль трафика: HTTPS

Сеть: /30

Год: 2010

Меры: acl permit https drop any,
ограничение количества соединений,
географическое разделение,
TCP payload inspection


dump1.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
21585 6.205092 82.206.251.100 SSL Continuation Data
21590 6.206715 92.47.183.148 SSL Continuation Data
21604 6.208330 112.79.199.125 SSL Continuation Data
21608 6.208637 112.203.189.170 SSL Continuation Data
21633 6.213469 203.82.92.111 SSL Continuation Data
21763 6.252335 203.82.92.111 SSL Continuation Data
21782 6.255257 65.38.219.58 SSL Continuation Data
21802 6.258051 65.38.219.58 SSL Continuation Data
21823 6.267862 112.79.199.125 SSL Continuation Data
21866 6.292027 203.82.92.111 SSL Continuation Data
21960 6.326460 112.79.199.125 SSL Continuation Data
21981 6.333977 203.82.92.111 SSL Continuation Data
21982 6.335695 125.162.62.253 SSL Continuation Data
22022 6.344090 117.242.0.213 SSL Continuation Data
22045 6.351418 113.168.114.132 SSL Continuation Data
22071 6.360211 113.168.114.132 SSL Continuation Data
22104 6.371346 117.242.0.213 SSL Continuation Data
22110 6.373546 203.82.92.111 SSL Continuation Data
22125 6.377360 117.242.0.213 SSL Continuation Data
22133 6.378536 65.38.219.58 SSL Continuation Data
22141 6.380589 65.38.219.58 SSL Continuation Data
Transmission Control Protocol, Src Port: menandmice-lpm (1231), Dst Port: https (443), Seq: 1, Ack: 1, Len: 319
Secure Socket Layer
0040 91 a5 25 53 57 cd 50 18 ff ff 27 25 00 00 06 b1
0050 b0 b3 aa c5 74 67 8e 19 78 5b b2 ad bc 8f 16 81
0060 40 03 ba 95 04 b7 9e e9 08 ab c2 7d 4c df 26 51
0070 d0 53 ca 65 94 07 ae b9 98 fb d2 4d dc 2f 36 21
0080 60 a3 da 35 24 57 be 89 28 4b e2 1d 6c 7f 46 f1
0090 f0 f3 ea 05 b4 a7 ce 59 b8 9b f2 ed fc cf 56 c1
00a0 80 43 fa d5 44 f7 de 29 48 eb 02 bd 8c 1f 66 91
00b0 10 93 0a a5 d4 47 ee f9 d8 3b 12 8d 1c 6f 76 61
00c0 a0 e3 1a 75 64 97 fe c9 68 8b 22 5d ac bf 86 31
00d0 30 33 2a 45 f4 e7 0e 99 f8 db 32 2d 3c 0f 96 01
00e0 c0 83 3a 15 84 37 1e 69 88 2b 42 fd cc 5f a6 d1
00f0 50 d3 4a e5 14 87 2e 39 18 7b 52 cd 5c af b6 a1
0100 e0 23 5a b5 a4 d7 3e 09 a8 cb 62 9d ec ff c6 71
0110 70 73 6a 85 34 27 4e d9 38 1b 72 6d 7c 4f d6 41
0120 00 c3 7a 55 c4 77 5e a9 c8 6b 82 3d 0c 9f e6 11
0130 90 13 8a 25 54 c7 6e 79 58 bb 92 0d 9c ef f6 e1
Secure Socket Layer (ssl), 319 bytes
Packets: 30205 Displayed: 30205 Marked: 0
Profile: Default

Контакты

Емельянов Роман Сергеевич
Директор дирекции
информационной безопасности

Компания ТТК
Тел: +7 (495) 784 66 70 ext. 6737
Факс: +7 (495) 784 66 71
www.ttk.ru
R.Emelyanov@ttk.ru