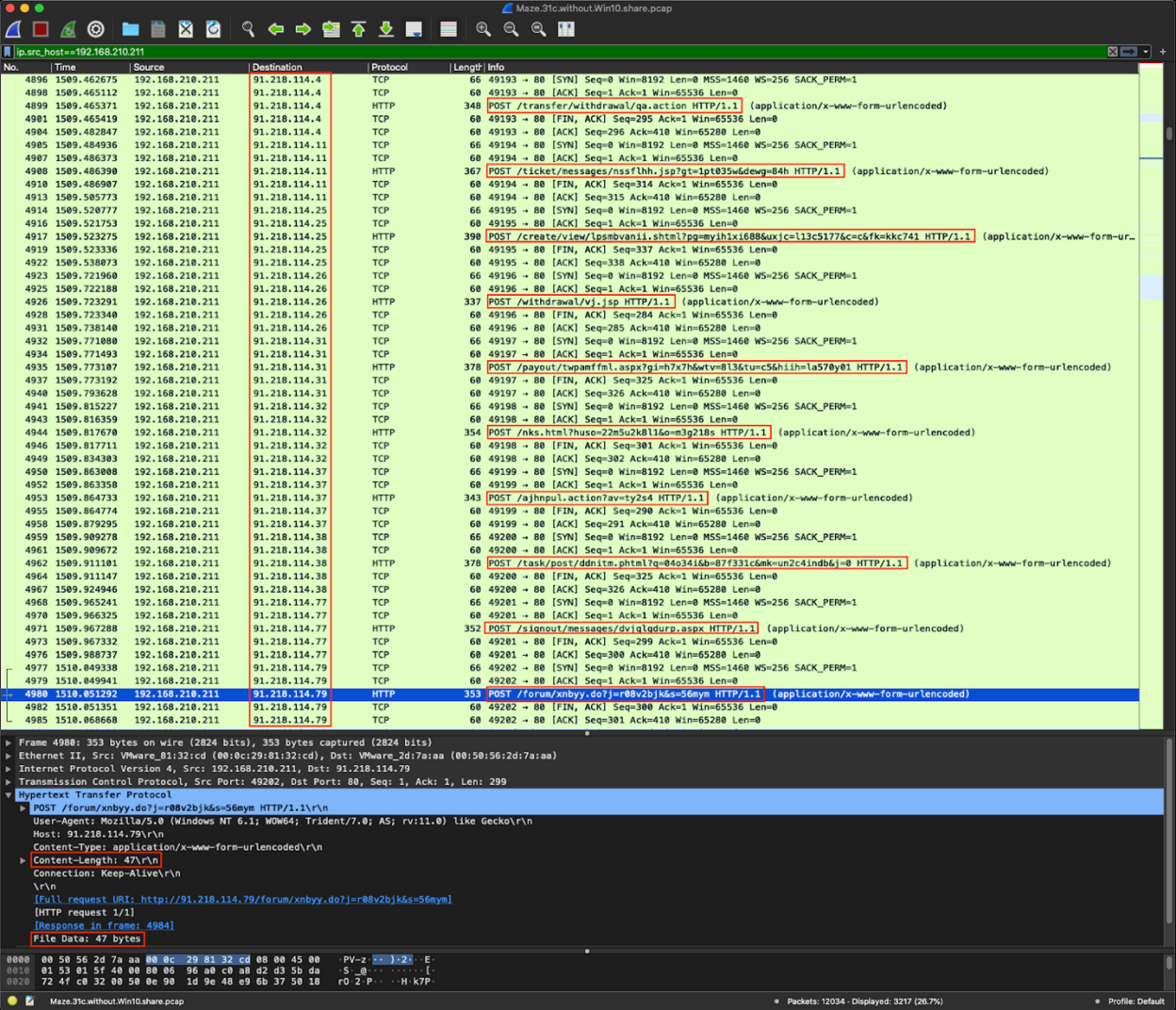
Maze.31c.without.Win10.share.pcap
ip.src_host==192.168.210.211
No. Time Source Destination Protocol Length Info
4896 1509.462675 192.168.210.211 91.218.114.4 TCP 66 49193 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4898 1509.465112 192.168.210.211 91.218.114.4 TCP 60 49193 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4899 1509.465371 192.168.210.211 91.218.114.4 HTTP 348 POST /transfer/withdrawal/qa.action HTTP/1.1 (application/x-www-form-urlencoded)
4901 1509.465419 192.168.210.211 91.218.114.4 TCP 60 49193 → 80 [FIN, ACK] Seq=295 Ack=1 Win=65536 Len=0
4904 1509.482847 192.168.210.211 91.218.114.4 TCP 60 49193 → 80 [ACK] Seq=296 Ack=410 Win=65280 Len=0
4905 1509.484936 192.168.210.211 91.218.114.11 TCP 66 49194 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4907 1509.486373 192.168.210.211 91.218.114.11 TCP 60 49194 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4908 1509.486390 192.168.210.211 91.218.114.11 HTTP 367 POST /ticket/messages/nssflhh.jsp?gt=1pt035w&dewg=84h HTTP/1.1 (application/x-www-form-urlencoded)
4910 1509.486907 192.168.210.211 91.218.114.11 TCP 60 49194 → 80 [FIN, ACK] Seq=314 Ack=1 Win=65536 Len=0
4913 1509.505773 192.168.210.211 91.218.114.11 TCP 60 49194 → 80 [ACK] Seq=315 Ack=410 Win=65280 Len=0
4914 1509.520777 192.168.210.211 91.218.114.25 TCP 66 49195 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4916 1509.521753 192.168.210.211 91.218.114.25 TCP 60 49195 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4917 1509.523275 192.168.210.211 91.218.114.25 HTTP 390 POST /create/view/ipsmbvanii.shtml?pg=myih1xi688&uxjc=l13c5177&c=c&fk=kkc741 HTTP/1.1 (application/x-www-form-ur…
4919 1509.523336 192.168.210.211 91.218.114.25 TCP 60 49195 → 80 [FIN, ACK] Seq=337 Ack=1 Win=65536 Len=0
4922 1509.538073 192.168.210.211 91.218.114.25 TCP 60 49195 → 80 [ACK] Seq=338 Ack=410 Win=65280 Len=0
4923 1509.721960 192.168.210.211 91.218.114.26 TCP 66 49196 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4925 1509.722188 192.168.210.211 91.218.114.26 TCP 60 49196 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4926 1509.723291 192.168.210.211 91.218.114.26 HTTP 337 POST /withdrawal/vj.jsp HTTP/1.1 (application/x-www-form-urlencoded)
4928 1509.723340 192.168.210.211 91.218.114.26 TCP 60 49196 → 80 [FIN, ACK] Seq=284 Ack=1 Win=65536 Len=0
4931 1509.738140 192.168.210.211 91.218.114.26 TCP 60 49196 → 80 [ACK] Seq=285 Ack=410 Win=65280 Len=0
4932 1509.771080 192.168.210.211 91.218.114.31 TCP 66 49197 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4934 1509.771493 192.168.210.211 91.218.114.31 TCP 60 49197 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4935 1509.773107 192.168.210.211 91.218.114.31 HTTP 378 POST /payout/twpamffml.aspx?gi=h7x7h&wtv=8l3&tu=c5&hiih=la570y01 HTTP/1.1 (application/x-www-form-urlencoded)
4937 1509.773192 192.168.210.211 91.218.114.31 TCP 60 49197 → 80 [FIN, ACK] Seq=325 Ack=1 Win=65536 Len=0
4940 1509.793628 192.168.210.211 91.218.114.31 TCP 60 49197 → 80 [ACK] Seq=326 Ack=410 Win=65280 Len=0
4941 1509.815227 192.168.210.211 91.218.114.32 TCP 66 49198 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4943 1509.816359 192.168.210.211 91.218.114.32 TCP 60 49198 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4944 1509.817670 192.168.210.211 91.218.114.32 HTTP 354 POST /nks.html?huso=22m5u2k8l1&o=m3g218s HTTP/1.1 (application/x-www-form-urlencoded)
4946 1509.817711 192.168.210.211 91.218.114.32 TCP 60 49198 → 80 [FIN, ACK] Seq=301 Ack=1 Win=65536 Len=0
4949 1509.834303 192.168.210.211 91.218.114.32 TCP 60 49198 → 80 [ACK] Seq=302 Ack=410 Win=65280 Len=0
4950 1509.863008 192.168.210.211 91.218.114.37 TCP 66 49199 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4952 1509.863358 192.168.210.211 91.218.114.37 TCP 60 49199 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4953 1509.864733 192.168.210.211 91.218.114.37 HTTP 343 POST /ajhnpul.action?av=ty2s4 HTTP/1.1 (application/x-www-form-urlencoded)
4955 1509.864774 192.168.210.211 91.218.114.37 TCP 60 49199 → 80 [FIN, ACK] Seq=290 Ack=1 Win=65536 Len=0
4958 1509.879295 192.168.210.211 91.218.114.37 TCP 60 49199 → 80 [ACK] Seq=291 Ack=410 Win=65280 Len=0
4959 1509.909278 192.168.210.211 91.218.114.38 TCP 66 49200 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4961 1509.909672 192.168.210.211 91.218.114.38 TCP 60 49200 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4962 1509.911101 192.168.210.211 91.218.114.38 HTTP 378 POST /task/post/ddnitm.phtml?q=04o34i&b=87f331c&mk=un2c4indb&j=0 HTTP/1.1 (application/x-www-form-urlencoded)
4964 1509.911147 192.168.210.211 91.218.114.38 TCP 60 49200 → 80 [FIN, ACK] Seq=325 Ack=1 Win=65536 Len=0
4967 1509.924946 192.168.210.211 91.218.114.38 TCP 60 49200 → 80 [ACK] Seq=326 Ack=410 Win=65280 Len=0
4968 1509.965241 192.168.210.211 91.218.114.77 TCP 66 49201 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4970 1509.966325 192.168.210.211 91.218.114.77 TCP 60 49201 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4971 1509.967288 192.168.210.211 91.218.114.77 HTTP 352 POST /signout/messages/dviqlqdurp.aspx HTTP/1.1 (application/x-www-form-urlencoded)
4973 1509.967332 192.168.210.211 91.218.114.77 TCP 60 49201 → 80 [FIN, ACK] Seq=299 Ack=1 Win=65536 Len=0
4976 1509.988737 192.168.210.211 91.218.114.77 TCP 60 49201 → 80 [ACK] Seq=300 Ack=410 Win=65280 Len=0
4977 1510.049338 192.168.210.211 91.218.114.79 TCP 66 49202 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4979 1510.049941 192.168.210.211 91.218.114.79 TCP 60 49202 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4980 1510.051292 192.168.210.211 91.218.114.79 HTTP 353 POST /forum/xnbyy.do?j=r08v2bjk&s=56mym HTTP/1.1 (application/x-www-form-urlencoded)
4982 1510.051351 192.168.210.211 91.218.114.79 TCP 60 49202 → 80 [FIN, ACK] Seq=300 Ack=1 Win=65536 Len=0
4985 1510.068668 192.168.210.211 91.218.114.79 TCP 60 49202 → 80 [ACK] Seq=301 Ack=410 Win=65280 Len=0
Frame 4980: 353 bytes on wire (2824 bits), 353 bytes captured (2824 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: 49202, Dst Port: 80, Seq: 1, Ack: 1, Len: 299
Hypertext Transfer Protocol
POST /forum/xnbyy.do?j=r08v2bjk&s=56mym 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: 47\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://91.218.114.79/forum/xnbyy.do?j=r08v2bjk&s=56mym]
[HTTP request 1/1]
[Response in frame: 4984]
File Data: 47 bytes
0000 00 50 56 2d 7a aa 00 0c 29 81 32 cd 08 00 45 00 ·PV-z··· )·2···E·
0010 01 53 01 5f 40 00 80 06 96 a0 c0 a8 d2 d3 5b da ·S·_@··· ·····[·
0020 72 4f c0 32 00 50 0e 90 1d 9e 48 e9 6b 37 50 18 rO·2·P·· ··H·k7P·
Maze.31c.without.Win10.share.pcap
Packets: 12034 · Displayed: 3217 (26.7%)
Profile: Default