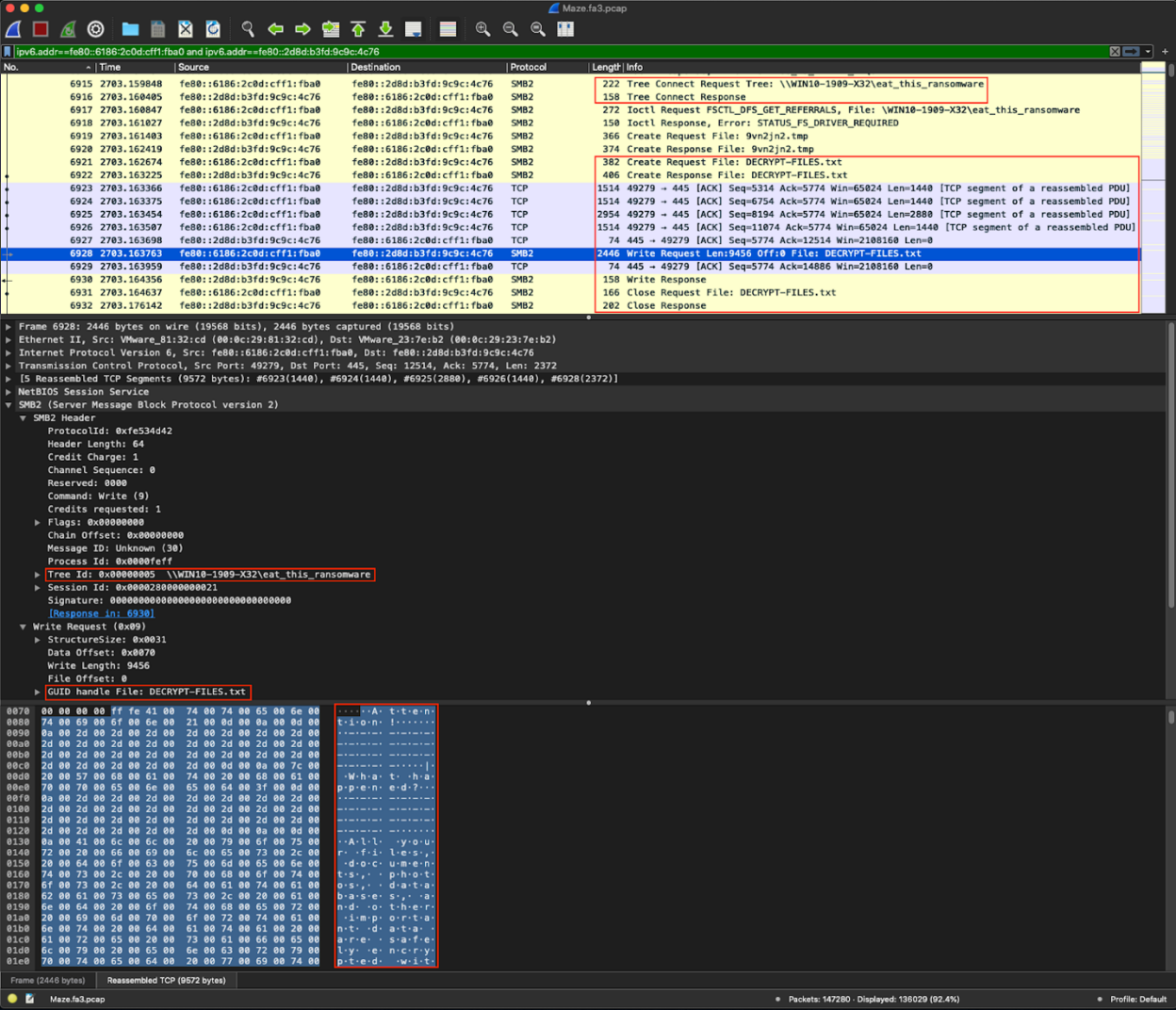
Maze.fa3.pcap
ipv6.addr==fe80::6186:2c0d:cff1:fba0 and ipv6.addr==fe80::2d8d:b3fd:9c9c:4c76
No. Time Source Destination Protocol Length Info
6915 2703.159848 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 222 Tree Connect Request Tree: \\WIN10-1909-X32\eat_this_ransomware
6916 2703.160405 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 158 Tree Connect Response
6917 2703.160847 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 272 Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \WIN10-1909-X32\eat_this_ransomware
6918 2703.161027 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 150 Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
6919 2703.161403 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 366 Create Request File: 9vn2jn2.tmp
6920 2703.162419 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 374 Create Response File: 9vn2jn2.tmp
6921 2703.162674 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 382 Create Request File: DECRYPT-FILES.txt
6922 2703.163225 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 406 Create Response File: DECRYPT-FILES.txt
6923 2703.163366 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 TCP 1514 49279 → 445 [ACK] Seq=5314 Ack=5774 Win=65024 Len=1440 [TCP segment of a reassembled PDU]
6924 2703.163375 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 TCP 1514 49279 → 445 [ACK] Seq=6754 Ack=5774 Win=65024 Len=1440 [TCP segment of a reassembled PDU]
6925 2703.163454 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 TCP 2954 49279 → 445 [ACK] Seq=8194 Ack=5774 Win=65024 Len=2880 [TCP segment of a reassembled PDU]
6926 2703.163507 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 TCP 1514 49279 → 445 [ACK] Seq=11074 Ack=5774 Win=65024 Len=1440 [TCP segment of a reassembled PDU]
6927 2703.163698 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 TCP 74 445 → 49279 [ACK] Seq=5774 Ack=12514 Win=2108160 Len=0
6928 2703.163763 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 2446 Write Request Len:9456 Off:0 File: DECRYPT-FILES.txt
6929 2703.163959 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 TCP 74 445 → 49279 [ACK] Seq=5774 Ack=14886 Win=2108160 Len=0
6930 2703.164356 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 158 Write Response
6931 2703.164637 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 166 Close Request File: DECRYPT-FILES.txt
6932 2703.176142 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 202 Close Response
Frame 6928: 2446 bytes on wire (19568 bits), 2446 bytes captured (19568 bits)
Ethernet II, Src: VMware_81:32:cd (00:0c:29:81:32:cd), Dst: VMware_23:7e:b2 (00:0c:29:23:7e:b2)
Internet Protocol Version 6, Src: fe80::6186:2c0d:cff1:fba0, Dst: fe80::2d8d:b3fd:9c9c:4c76
Transmission Control Protocol, Src Port: 49279, Dst Port: 445, Seq: 12514, Ack: 5774, Len: 2372
[5 Reassembled TCP Segments (9572 bytes): #6923(1440), #6924(1440), #6925(2880), #6926(1440), #6928(2372)]
NetBIOS Session Service
SMB2 (Server Message Block Protocol version 2)
SMB2 Header
ProtocolId: 0xfe534d42
Header Length: 64
Credit Charge: 1
Channel Sequence: 0
Reserved: 0000
Command: Write (9)
Credits requested: 1
Flags: 0x00000000
Chain Offset: 0x00000000
Message ID: Unknown (30)
Process Id: 0x0000feff
Tree Id: 0x00000005 \\WIN10-1909-X32\eat_this_ransomware
Session Id: 0x0000280000000021
Signature: 00000000000000000000000000000000
[Response in: 6930]
Write Request (0x09)
StructureSize: 0x0031
Data Offset: 0x0070
Write Length: 9456
File Offset: 0
GUID handle File: DECRYPT-FILES.txt
0070 00 00 00 00 ff fe 41 00 74 00 74 00 65 00 6e 00
0080 74 00 69 00 6f 00 6e 00 21 00 0d 00 0a 00 0d 00
0090 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00
00a0 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00
00b0 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00
00c0 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00 7c 00
00d0 20 00 57 00 68 00 61 00 74 00 20 00 68 00 61 00
00e0 70 00 70 00 65 00 6e 00 65 00 64 00 3f 00 0d 00
00f0 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00
0100 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00
0110 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00
0120 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00 0d 00
0130 0a 00 41 00 6c 00 6c 00 20 00 79 00 6f 00 75 00
0140 72 00 20 00 66 00 69 00 6c 00 65 00 73 00 2c 00
0150 20 00 64 00 6f 00 63 00 75 00 6d 00 65 00 6e 00
0160 74 00 73 00 2c 00 20 00 70 00 68 00 6f 00 74 00
0170 6f 00 73 00 2c 00 20 00 64 00 61 00 74 00 61 00
0180 62 00 61 00 73 00 65 00 73 00 2c 00 20 00 61 00
0190 6e 00 64 00 20 00 6f 00 74 00 68 00 65 00 72 00
01a0 20 00 69 00 6d 00 70 00 6f 00 72 00 74 00 61 00
01b0 6e 00 74 00 20 00 64 00 61 00 74 00 61 00 20 00
01c0 61 00 72 00 65 00 20 00 73 00 61 00 66 00 65 00
01d0 6c 00 79 00 20 00 65 00 6e 00 63 00 72 00 79 00
01e0 70 00 74 00 65 00 64 00 20 00 77 00 69 00 74 00
Frame (2446 bytes)
Reassembled TCP (9572 bytes)
Maze.fa3.pcap
Packets: 147280 · Displayed: 138029 (92.4%)
Profile: Default