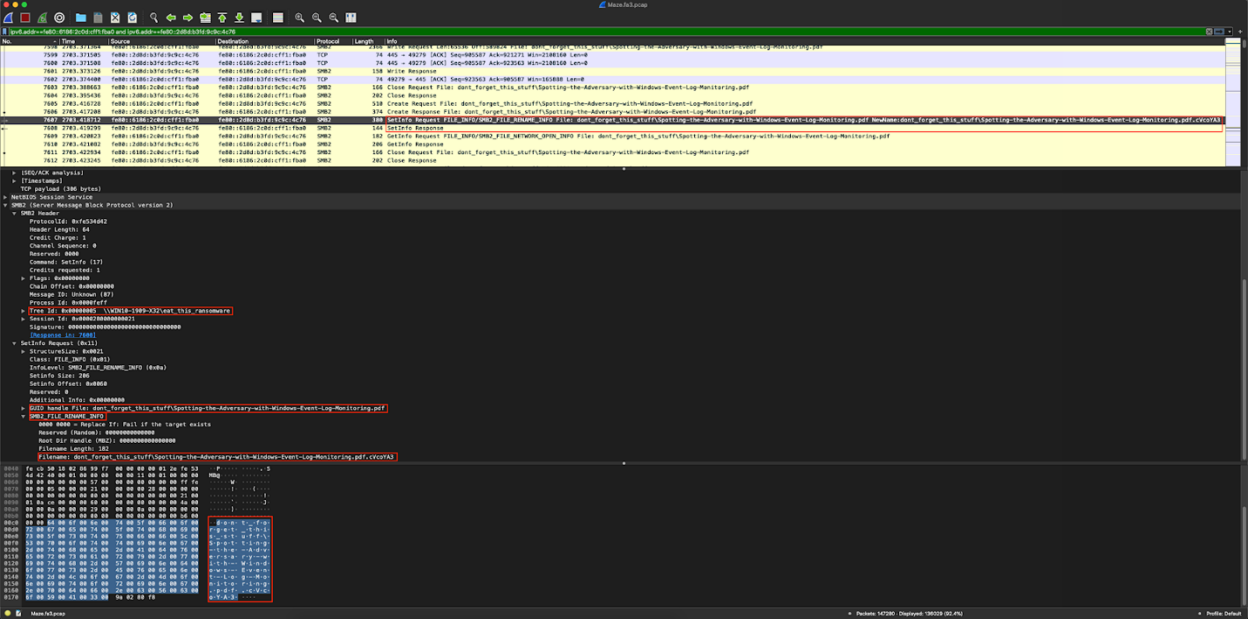
Maze.fs3.pcap
ipv6.addr==fe80::6186:2c0d:cff1:fba0 and ipv6.addr==fe80::2d8d:b3fd:9c9c:4c76
No. Time Source DestAddress Protocol Length Info
7599 2783.371585 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 214 Write Request Len:150 Off:0 File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
7599 2783.371585 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 TCP 74 445 → 49279 [ACK] Seq=905587 Ack=923571 Win=2180160 Len=0
7600 2783.371598 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 TCP 74 445 → 49279 [ACK] Seq=905587 Ack=923563 Win=2180160 Len=0
7601 2783.373126 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 158 Write Response
7602 2783.374408 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 TCP 74 49279 → 445 [ACK] Seq=923563 Ack=905587 Win=165888 Len=0
7603 2783.388663 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 166 Close Request File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
7604 2783.389430 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 202 Close Response
7605 2783.416728 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 510 Create Request File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
7606 2783.417280 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 374 Create Response File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
7607 2783.418712 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 380 SetInfo Request FILE_INFO/SMB2_FILE_RENAME_INFO File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf;NewName:dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf.cvcoYA3
7608 2783.419299 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 144 SetInfo Response
7609 2783.420823 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 182 GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
7610 2783.421402 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 206 GetInfo Response
7611 2783.422534 fe80::6186:2c0d:cff1:fba0 fe80::2d8d:b3fd:9c9c:4c76 SMB2 166 Close Request File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
7612 2783.423245 fe80::2d8d:b3fd:9c9c:4c76 fe80::6186:2c0d:cff1:fba0 SMB2 202 Close Response
[SEQ/ACK analysis]
[Timestamps]
TCP payload (306 bytes)
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: SetInfo (17)
Credits requested: 1
Flags: 0x00000000
Chain Offset: 0x00000000
Message ID: Unknown (87)
Process Id: 0x0000feff
Tree Id: 0x00000005 - \\WIN10-1909-X32\est_this_ransomware
Session Id: 0x0080210000000021
Signature: 00000000000000000000000000000000
[Response in: 7666]
SetInfo Request (0x11)
StructureSize: 0x0021
Class: FILE_INFO (0x01)
InfoLevel: SMB2_FILE_RENAME_INFO (0x0a)
SetInfo Size: 290
SetInfo Offset: 0x0060
Reserved: 0
Additional Info: 0x00000000
GUID handle File: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
SMB2_FILE_RENAME_INFO
0000 0000 = Replace If: Fail if the target exists
Reserved (Mustbe0): 0000000000000000
Root Dir Handle (MBZ): 0000000000000000
Filename Length: 182
Filename: dont_forget_this_stuff\Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf.cvcoYA3
0060 fe ub 50 18 02 08 89 f7 00 00 68 00 81 2a fe 53 ..P..... ..h..*.S
0070 4d 42 40 00 01 00 00 00 00 00 11 01 01 00 00 00 MB@..... ....
0080 00 00 00 00 00 00 37 00 00 00 00 00 00 00 ff fe ......7. ....
0090 00 00 05 00 00 00 21 00 00 00 00 00 00 00 00 00 ......!. ....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 21 00 ....!.
00b0 01 0a c0 00 00 00 60 00 00 00 00 00 00 00 6a 00 ......`. ......j.
00c0 00 00 0a 00 00 00 29 00 00 0a 00 00 00 00 00 00 ......). ....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b6 00 ....
00e0 64 00 6f 00 6e 00 27 00 74 00 5f 00 66 00 6f 00 d.o.n.'. t._.f.o.
00f0 72 00 67 00 65 00 74 00 5f 00 74 00 68 00 69 00 r.g.e.t._ .t.h.i.
0100 73 00 5f 00 73 00 74 00 75 00 66 00 66 00 5c 00 s._.s.t. u.f.f.\.
0110 53 00 70 00 6f 00 74 00 74 00 69 00 6e 00 67 00 S.p.o.t. t.i.n.g.
0120 2d 00 74 00 68 00 65 00 2d 00 41 00 64 00 76 00 -.t.h.e. -.A.d.v.
0130 65 00 72 00 73 00 61 00 72 00 79 00 2d 00 77 00 e.r.s.a. r.y.-.w.
0140 69 00 74 00 68 00 2d 00 57 00 69 00 6e 00 64 00 i.t.h.-. W.i.n.d.
0150 6f 00 77 00 73 00 2d 00 45 00 76 00 65 00 6e 00 o.w.s.-. E.v.e.n.
0160 74 00 2d 00 4c 00 6f 00 67 00 2d 00 4d 00 6f 00 t.-.L.o. g.-.M.o.
0170 6e 00 69 00 74 00 6f 00 72 00 69 00 6e 00 67 00 n.i.t.o. r.i.n.g.
0180 2e 00 70 00 64 00 66 00 2e 00 63 00 56 00 63 00 ..p.d.f. ..c.V.c.
0190 6f 00 59 00 41 00 33 00 0a 02 00 f8 o.Y.A.3. ....
Packets: 147280 · Displayed: 138039 (92.4%)
Profile: Default