Daxin Backdoor: In-Depth Analysis, Part Two

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage-analysis

Threat Hunter TeamSymantec

In the second of a two-part series of blogs, we examine the communications and networking features of Daxin.

This is the concluding part of our in-depth analysis of Backdoor. Daxin, advanced malware that is being used by a China-linked espionage group.

In this blog, we will analyze the communications and network features of the malware.

Communications protocol

In our previous blog, we set up a lab consisting of four separate networks and five machines. Some of the machines had two network interfaces to communicate with different networks, but all packet forwarding functionality was disabled. Each machine ran various network services that were reachable from its neighbors only.

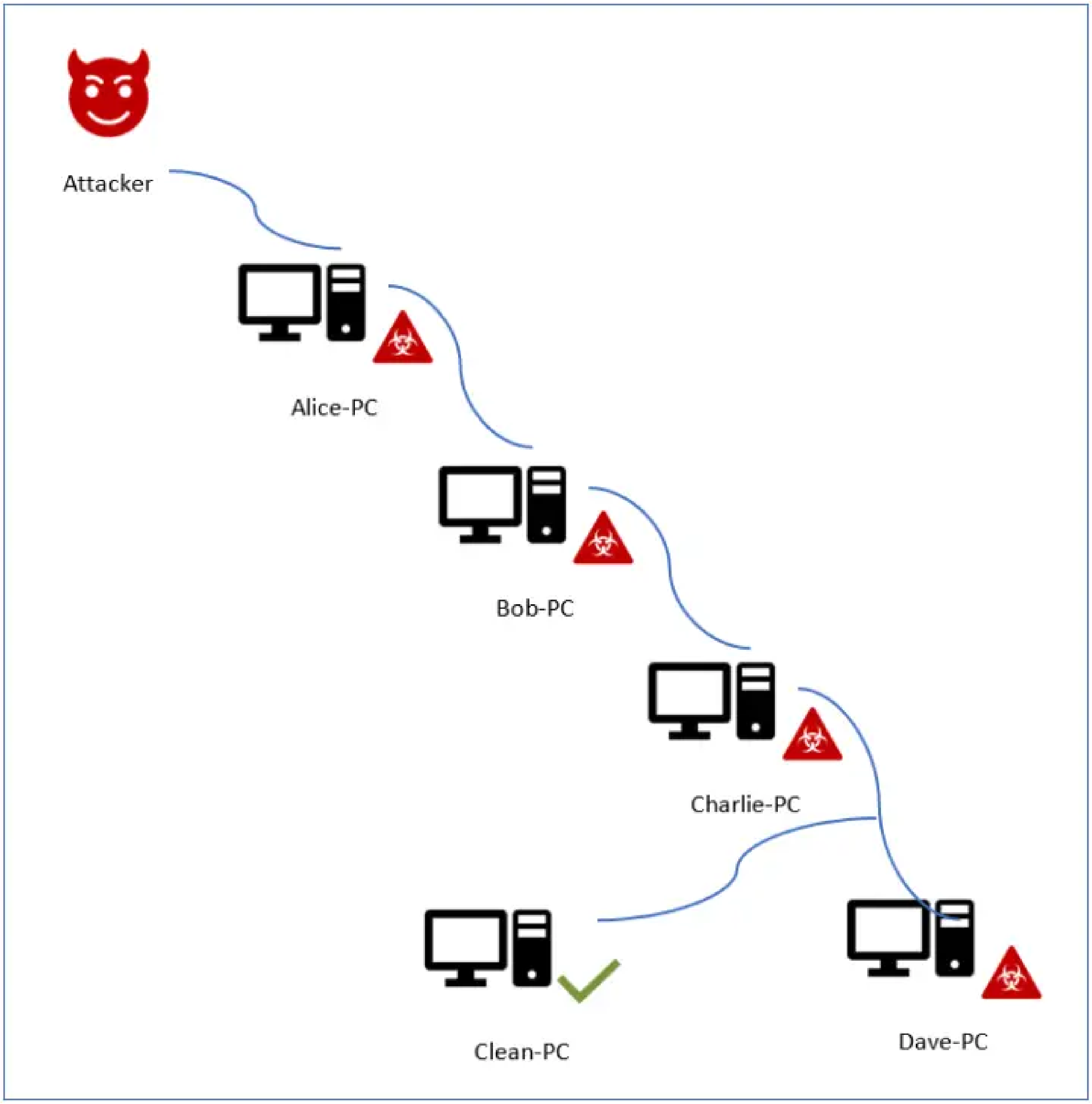
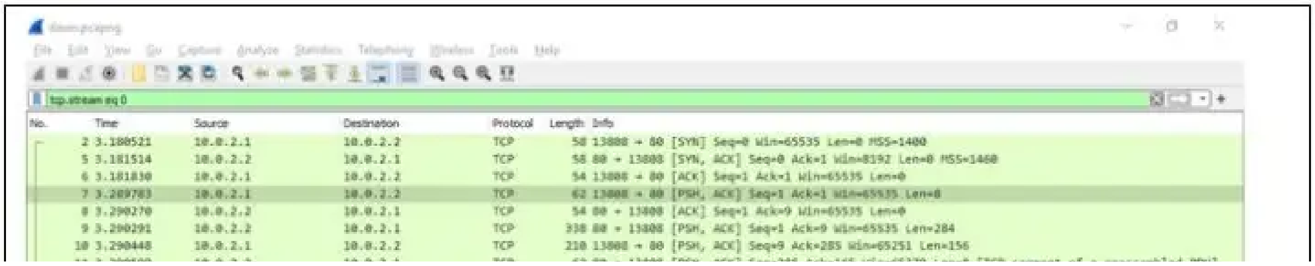


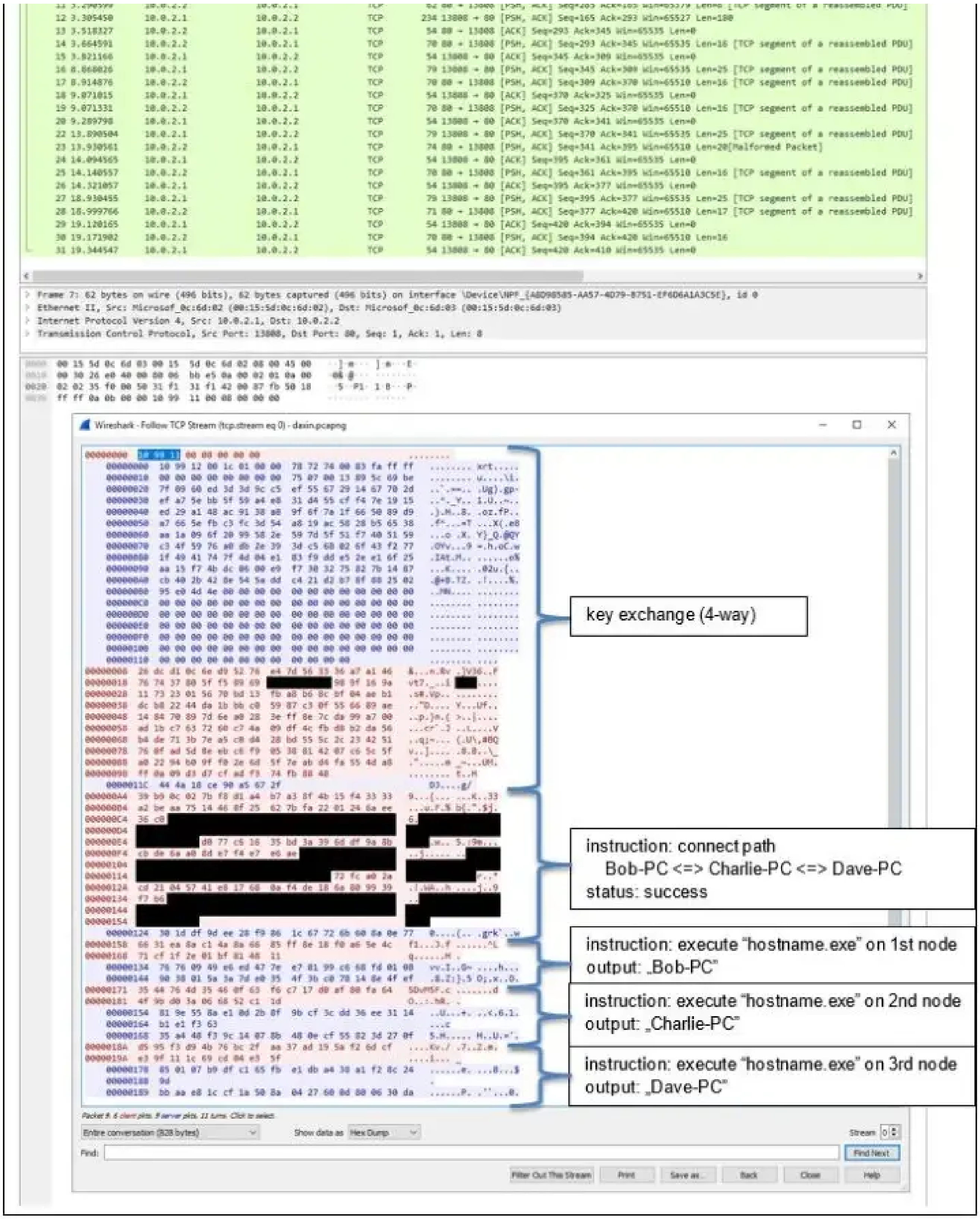
Figure 1. Test setup to illustrate Daxin's backdoor capabilities.

In this section we will dissect the network traffic between two backdoor instances running on the separate computers "Alice-PC" and "Bob-PC". The traffic was initiated by the Daxin backdoor running on "Alice-PC" when it was instructed to create a communication channel to "Dave-PC" passing via two intermediate nodes, "Bob-PC" and "Charlie-PC", as described previously.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.stream eq 0

No.   Time        Source      Destination   Protocol  Length  Info
   2 3.180521    10.0.2.1    10.0.2.2      TCP         58 13888 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1400
   5 3.181514    10.0.2.2    10.0.2.1      TCP         58 80 → 13888 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
   6 3.181830    10.0.2.1    10.0.2.2      TCP         54 13888 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   7 3.289783    10.0.2.1    10.0.2.2      TCP         62 13888 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=8
   8 3.290270    10.0.2.2    10.0.2.1      TCP         54 80 → 13888 [ACK] Seq=1 Ack=9 Win=65535 Len=0
   9 3.290291    10.0.2.2    10.0.2.1      TCP        338 80 → 13888 [PSH, ACK] Seq=1 Ack=9 Win=65535 Len=284
  10 3.290448    10.0.2.1    10.0.2.2      TCP        210 13888 → 80 [PSH, ACK] Seq=9 Ack=285 Win=65251 Len=156
```



key exchange (4-way)
instruction: connect path Bob-PC <=> Charlie-PC <=> Dave-PC status: success
instruction: execute "hostname.exe" on 1st node output: „Bob-PC"
instruction: execute "hostname.exe" on 2nd node output: „Charlie-PC"
instruction: execute "hostname.exe" on 3rd node output: „Dave-PC"
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

```
11 3.290599   10.0.2.2   10.0.2.1   TCP   62 80 → 13808 [PSH, ACK] Seq=285 Ack=165 Win=65379 Len=8 [TCP segment of a reassembled PDU]
12 3.305450   10.0.2.1   10.0.2.2   TCP  234 13808 → 80 [PSH, ACK] Seq=165 Ack=293 Win=65527 Len=180
13 3.518327   10.0.2.2   10.0.2.1   TCP   54 80 → 13808 [ACK] Seq=293 Ack=345 Win=65535 Len=0
14 3.664591   10.0.2.2   10.0.2.1   TCP   70 80 → 13808 [PSH, ACK] Seq=293 Ack=345 Win=65535 Len=16 [TCP segment of a reassembled PDU]
15 3.821166   10.0.2.1   10.0.2.2   TCP   54 13808 → 80 [ACK] Seq=345 Ack=309 Win=65535 Len=0
16 8.868026   10.0.2.1   10.0.2.2   TCP   79 13808 → 80 [PSH, ACK] Seq=345 Ack=309 Win=65535 Len=25 [TCP segment of a reassembled PDU]
17 8.914876   10.0.2.2   10.0.2.1   TCP   70 80 → 13808 [PSH, ACK] Seq=309 Ack=370 Win=65510 Len=16 [TCP segment of a reassembled PDU]
18 9.071015   10.0.2.1   10.0.2.2   TCP   54 13808 → 80 [ACK] Seq=370 Ack=325 Win=65535 Len=0
19 9.071331   10.0.2.2   10.0.2.1   TCP   70 80 → 13808 [PSH, ACK] Seq=325 Ack=370 Win=65510 Len=16 [TCP segment of a reassembled PDU]
20 9.289798   10.0.2.1   10.0.2.2   TCP   54 13808 → 80 [ACK] Seq=370 Ack=341 Win=65535 Len=0
22 13.890504  10.0.2.1   10.0.2.2   TCP   79 13808 → 80 [PSH, ACK] Seq=370 Ack=341 Win=65535 Len=25 [TCP segment of a reassembled PDU]
23 13.930561  10.0.2.2   10.0.2.1   TCP   74 80 → 13808 [PSH, ACK] Seq=341 Ack=395 Win=65510 Len=20[Malformed Packet]
24 14.094565  10.0.2.1   10.0.2.2   TCP   54 13808 → 80 [ACK] Seq=395 Ack=361 Win=65535 Len=0
25 14.140557  10.0.2.2   10.0.2.1   TCP   70 80 → 13808 [PSH, ACK] Seq=361 Ack=395 Win=65510 Len=16 [TCP segment of a reassembled PDU]
26 14.321057  10.0.2.1   10.0.2.2   TCP   54 13808 → 80 [ACK] Seq=395 Ack=377 Win=65535 Len=0
27 18.930455  10.0.2.1   10.0.2.2   TCP   79 13808 → 80 [PSH, ACK] Seq=395 Ack=377 Win=65535 Len=25 [TCP segment of a reassembled PDU]
28 18.999766  10.0.2.2   10.0.2.1   TCP   71 80 → 13808 [PSH, ACK] Seq=377 Ack=420 Win=65510 Len=17 [TCP segment of a reassembled PDU]
29 19.120165  10.0.2.1   10.0.2.2   TCP   54 13808 → 80 [ACK] Seq=420 Ack=394 Win=65535 Len=0
30 19.171982  10.0.2.2   10.0.2.1   TCP   70 80 → 13808 [PSH, ACK] Seq=394 Ack=420 Win=65510 Len=16
31 19.344547  10.0.2.1   10.0.2.2   TCP   54 13808 → 80 [ACK] Seq=420 Ack=410 Win=65535 Len=0
```

```
> Frame 7: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface \Device\NPF_{A8D98585-AA57-4D79-8751-EF6D6A1A3C5E}, id 0
> Ethernet II, Src: Microsof_0c:6d:02 (00:15:5d:0c:6d:02), Dst: Microsof_0c:6d:03 (00:15:5d:0c:6d:03)
> Internet Protocol Version 4, Src: 10.0.2.1, Dst: 10.0.2.2
> Transmission Control Protocol, Src Port: 13808, Dst Port: 80, Seq: 1, Ack: 1, Len: 8
```

```
0000  00 15 5d 0c 6d 03 00 15  5d 0c 6d 02 08 00 45 00   ··]·m··· ]·m···E·
0010  00 30 26 e0 40 00 80 06  bb e5 0a 00 02 01 0a 00   ·0&·@··· ········
0020  02 02 35 f0 00 50 31 f1  31 f1 42 00 87 fb 50 18   ··5··P1· 1·B···P·
0030  ff ff 0a 0b 00 00 10 99  11 00 08 00 00 00         ········ ······
```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · daxin.pcapng

```
00000000  10 99 11 00 00 00 00 00                            ........
    00000000  10 99 12 00 1c 01 00 00  78 72 74 00 03 fa ff ff   ........ xrt.....
    00000010  00 00 00 00 00 00 00 00  75 07 00 13 89 5c 69 be   ........ u....\i.
    00000020  7f 09 60 ed 3d 3d 9c c5  ef 55 67 29 14 67 70 2d   ..`.==.. .Ug).gp-
    00000030  ef a7 5e bb 5f 59 a4 e8  31 d4 55 cf f4 7e 19 15   ..^._Y.. 1.U..~..
    00000040  ed 29 a1 48 ac 91 38 a8  9f 6f 7a 1f 66 50 89 d9   .).H..8. .oz.fP..
    00000050  a7 66 5e fb c3 fc 3d 54  a8 19 ac 58 28 b5 65 38   .f^...=T ...X(.e8
    00000060  aa 1a 09 6f 20 99 58 2e  59 7d 5f 51 f7 40 51 59   ...o .X. Y}_Q.@QY
    00000070  c3 4f 59 76 a0 db 2e 39  3d c5 68 02 6f 43 f2 77   .OYv...9 =.h.oC.w
    00000080  1f 49 41 74 7f 4d 04 e1  83 f9 dd e5 2e e1 6f 25   .IAt.M.. ......o%
    00000090  aa 15 f7 4b dc 06 00 e9  f7 30 32 75 82 7b 14 87   ...K.... .02u.{..
    000000A0  cb 40 2b 42 8e 54 5a dd  c4 21 d2 b7 8f 08 25 02   .@+B.TZ. .!....%.
    000000B0  95 e0 4d 4e 00 00 00 00  00 00 00 00 00 00 00 00   ..MN.... ........
    000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
    000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
    000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
    000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
    00000100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
    00000110  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
00000008  26 dc d1 0c 6e d9 52 76  e4 7d 56 33 36 a7 a1 46   &...n.Rv .}V36..F
00000018  76 74 37 80 5f f5 89 69  [redacted] 98 9f 16 9a   vt7._..i [redacted]....
00000028  11 73 23 01 56 70 bd 13  fb a8 b6 8c bf 04 ae b1   .s#.Vp.. ........
00000038  dc b8 22 44 da 1b bb c8  59 87 c3 0f 55 66 89 ae   .."D.... Y...Uf..
00000048  14 84 70 89 7d 6e a0 28  3e ff 8e 7c da 99 a7 00   ..p.}n.( >..|....
00000058  ad 1b c7 63 72 60 c7 4a  09 df 4c fb d8 b2 da 56   ...cr`.J ..L....V
00000068  b4 de 71 3b 7e a5 c8 d8  28 bd 55 5c 2c 23 42 51   ..q;~... (.U\,#BQ
00000078  76 0f ad 5d 8e eb c6 f9  05 38 81 42 07 c6 5c 5f   v..].... .8.B..\_
00000088  a0 22 94 b0 9f f8 2e 6d  5f 7e ab d4 fa 55 4d a8   ."....m _~...UM.
00000098  ff 0a 09 d3 d7 cf ad f3  74 fb 88 48               ........ t..H
    0000011C  44 4a 18 ce 90 a5 67 2f                            DJ....g/
000000A4  39 b9 0c 02 7b f8 d1 a4  b7 a3 8f 4b 15 f4 33 33   9...{... ...K..33
000000B4  a2 be aa 75 14 46 8f 25  62 7b fa 22 01 24 6a ee   ...u.F.% b{.".$j.
000000C4  36 c8 [redacted]                                   6. [redacted]
000000D4  [redacted]
000000E4  [redacted] d8 77 c6 16  35 bd 3a 39 6d df 9a 8b    [redacted] .w.. 5.:9m...
000000F4  cb de 6a a0 8d e7 f4 e7  e6 ae [redacted]          ..j..... .. [redacted]
00000104  [redacted]
00000114  [redacted] 72 fc a0 2a                             [redacted] r..*
00000124  cd 21 04 57 41 e8 17 68  8a f4 de 18 6a 80 99 39   .!.WA..h ....j..9
00000134  f7 b6 [redacted]                                   .. [redacted]
00000144  [redacted]
00000154  [redacted]
    00000124  30 1d df 9d ee 28 f9 86  1c 67 72 6b 60 8a 0e 77   0....(.. .grk`..w
00000158  66 31 ea 8a c1 4a 8a 66  85 ff 8e 18 f0 a6 5e 4c   f1...J.f ......^L
00000168  71 cf 1f 2e 01 bf 81 48  11                        q......H .
    00000134  76 76 09 49 e6 ed 47 7e  e7 81 99 c6 68 fd 01 08   vv.I..G~ ....h...
    00000144  90 38 01 5a 3a 7d e0 35  4f 3b c0 78 14 0e 4f ef   .8.Z:}.5 O;.x..O.
00000171  35 44 76 4d 35 46 0f 63  f6 c7 17 d0 af 80 fa 64   5DvM5F.c .......d
00000181  4f 9b d0 3a 06 68 52 c1  1d                        O..:.hR. .
    00000154  81 9e 55 8a e1 0d 2b 0f  9b cf 3c dd 36 ee 31 14   ..U...+. ..<.6.1.
    00000164  b1 e1 f3 63                                        ...c
    00000168  35 a4 48 f3 9c 14 07 8b  48 0e cf 55 82 3d 27 0f   5.H..... H..U.='.
0000018A  d5 95 f3 d9 4b 76 bc 2f  aa 37 ad 19 5a f2 6d cf   ....Kv./ .7..Z.m.
0000019A  e3 9f 11 1c 69 cd 04 e3  5f                        ....i... _
    00000178  85 01 07 b9 df c1 65 fb  e1 db a4 30 a1 f2 8c 24   ......e. ...0...$
    00000188  9d                                                 .
    00000189  bb aa e8 1c cf 1a 50 8a  04 27 60 8d 80 06 30 da   ......P. .'`...0.
```

Packet 9. 6 client pkts, 5 server pkts, 11 turns. Click to select.

Entire conversation (828 bytes)   Show data as: Hex Dump   Stream: 0

Find:

Figure 2. Wireshark capture of traffic between two backdoor instances. The screenshot and examples below are reused from a private report prepared by us that discussed an earlier sample, so certain details may not match.

Using Wireshark, we captured traffic between two backdoor instances, one running on "Alice-PC" and the other on "Bob-PC", as shown in Figure 2.

Starting with the key exchange, all backdoor communication is carried out by exchanging messages that follow the same underlying format:

The *magic* value is always 0x9910 or 0x9911.

The *kind* value identifies the state transition during key exchange. Then, once the encrypted communication channel is established, it encodes the purpose of each message and determines the formatting of the data that follows the fixed-size header.

The initial message of the key exchange in the Wireshark capture is not encrypted:

It can be decoded as follows:

The fields *magic* and *kind* correspond to the first three bytes of TCP data, 0x10 0x99 0x11. On the target computer, in case it is infected with a copy of the malicious driver, this sequence causes the TCP connection to be hijacked, as explained in part one of this blog series.

The target checks that the received message is valid according to the session state machine, ensuring that *magic* is the expected constant 0x9910 and *kind* matches any of two supported values: 0x10 or 0x11. Next, it generates a nonce to use when encrypting any future incoming messages. Finally, it sends a response message with the nonce, its own details, and the information about the infected machine.

Parts of the response message are encrypted using a combination of the following algorithms:

The details of this response message are as follows:

The message includes the backdoor login that is recognized during the following key exchange step, and what looks like malware build and version numbers.

Looking at the decoded message, we find references to “XRT” and these reassemble the hardcoded Name “NDISXRPT” that we documented when discussing the *NdisRegisterProtocol()* call during driver initialization:

The initiator responds with the backdoor login and hashed password:

Want to comment on this post?