

Dns Resolver Analysis

Martin Fracker

March 6, 2017

In figure 1 we can see that packet indicates a jump into fixed header. This is essentially an occurrence of the byte 0xc0 followed by a byte equal to or less than 0x0b.

In figure 2 the server returned a packet smaller than 12 bytes, the size of the fixed header.

In figure 3 the packet indicated a jump that would result in a location past the end of the packet.

In figure 4 the packet indicates a jump with byte 0xc0 at some position x within the packet, followed by another byte which indicated an offset of x . This results in an infinite jump loop.

In figure 5 the packet indicated a huge amount of additional records. This inevitably results in the program eventually expecting a jump offset past the boundary of the packet.

In figure 6 the packet intends to indicate an answer by jumping. This is indicated by the last byte of the packet, 0xc0. However, because the jump indicator is the last byte of the packet, the packet offset is truncated.

In figure 7 the packet indicates an answer length that is longer than the amount of bytes left in the rest of the packet.

In figure 8 the packet indicates that its one question is x amount of bytes long which is larger than the amount of bytes in the rest of the packet. For this case, since questions are handled differently in code and are displayed differently than answers, authorities, and additional answers, they were special enough to have their own error category.

In figure 9 the packet ends before the next name is finished being specified. That is, not only is there no trailing null byte, but the name length, indicates a name longer than there are bytes left in the rest of the packet.

```
C:\Windows\system32\cmd.exe
Lookup : random0.irl
Query  : random0.irl, type 1, TXID 0x338C
Server  : 128.194.135.82
*****
Attempt 0 with 29 bytes... response in 2 ms with 82 bytes
TXID 0x338C flags 0x33792 questions 1 answers 2 authority 0 additional 0
succeeded with Rcode = 0
----- [questions] -----
      random0.irl type 1 class 1
----- [answers] -----

** invalid record: jump into fixed header
Press any key to continue . . . _
```

Figure 1: Jump into fixed header

```
C:\Windows\system32\cmd.exe
Lookup : random3.irl
Query  : random3.irl, type 1, TXID 0x354E
Server  : 128.194.135.82
*****
Attempt 0 with 29 bytes... response in 1 ms with 5 bytes
TXID 0x354E flags 0x33792 questions 0 answers 0 authority 0 additional 0

** invalid reply: smaller than fixed header
Press any key to continue . . . _
```

Figure 2: Smaller than fixed header

```
C:\Windows\system32\cmd.exe
Lookup : random5.irl
Query : random5.irl, type 1, TXID 0x48E9
Server : 128.194.135.82
*****
Attempt 0 with 29 bytes... response in 2 ms with 71 bytes
TXID 0x48E9 flags 0x33792 questions 1 answers 2 authority 0 additional 0
succeeded with Rcode = 0
----- [questions] -----
random5.irl type 1 class 1
----- [answers] -----
random.irl A 1.1.1.1 TTL = 30

++ invalid record: jump beyond packet boundary
Press any key to continue . . . _
```

Figure 3: Jump beyond packet boundary

```
C:\Windows\system32\cmd.exe
Lookup : random6.irl
Query : random6.irl, type 1, TXID 0x496C
Server : 128.194.135.82
*****
Attempt 0 with 29 bytes... response in 2 ms with 59 bytes
TXID 0x496C flags 0x33792 questions 1 answers 2 authority 0 additional 0
succeeded with Rcode = 0
----- [questions] -----
random6.irl type 1 class 1
----- [answers] -----
random6.irl CNAME
++ invalid record: jump loop
Press any key to continue . . . _
```

Figure 4: Jump loop

```
C:\Windows\system32\cmd.exe
Query : random1.irl, type 1, TXID 0x4A57
Server : 128.194.135.82
*****
Attempt 0 with 29 bytes... response in 1 ms with 468 bytes
TXID 0x4A57 flags 0x34304 questions 1 answers 1 authority 0 additional 65535
succeeded with Rcode = 0
----- [questions] -----
random1.irl type 1 class 1
----- [answers] -----
random.irl A 1.1.1.1 TTL = 30
----- [additional] -----
Episode.IV A 2.2.2.2 TTL = 30
A.NEW.HOPE A 2.2.2.2 TTL = 30
It.is.a.period.of.civil.war A 2.2.2.2 TTL = 30
Rebel.spaceships A 2.2.2.2 TTL = 30
striking.from.a.hidden.base A 2.2.2.2 TTL = 30
have.won.their.first.victory A 2.2.2.2 TTL = 30
against.the.evill.Galactic.Empire A 2.2.2.2 TTL = 30
During.the.battle A 2.2.2.2 TTL = 30
Rebel.spies.managed A 2.2.2.2 TTL = 30
to.steal.secret.plans A 2.2.2.2 TTL = 30
to.the.Empires.ultimate.weapon A 2.2.2.2 TTL = 30

** invalid record: truncated jump offset
Press any key to continue . . . _
```

Figure 5: Truncated jump offset

```
C:\Windows\system32\cmd.exe
Lookup : random7.irl
Query : random7.irl, type 1, TXID 0x4ABC
Server : 128.194.135.82
*****
Attempt 0 with 29 bytes... response in 2 ms with 42 bytes
TXID 0x4ABC flags 0x33792 questions 1 answers 2 authority 0 additional 0
succeeded with Rcode = 0
----- [questions] -----
random7.irl type 1 class 1
----- [answers] -----
random7.irl CNAME
** invalid record: truncated jump offset
Press any key to continue . . . _
```

Figure 6: Truncated jump offset

```
C:\Windows\system32\cmd.exe
Lookup : random4.irl
Query : random4.irl, type 1, TXID 0x4D7E
Server : 128.194.135.82
*****
Attempt 0 with 29 bytes... response in 1 ms with 53 bytes
TXID 0x4D7E flags 0x33792 questions 1 answers 1 authority 0 additional 11
succeeded with Rcode = 0
----- [questions] -----
random4.irl type 1 class 1
----- [answers] -----
random.irl 0
++ invalid record: RR value length beyond packet
Press any key to continue . . . _
```

Figure 7: RR value length beyond packet

```
C:\Windows\system32\cmd.exe
Lookup : random4.irl
Query : random4.irl, type 1, TXID 0x64AB
Server : 128.194.135.82
*****
Attempt 0 with 29 bytes... response in 1 ms with 20 bytes
TXID 0x64AB flags 0x33792 questions 1 answers 1 authority 0 additional 11
succeeded with Rcode = 0
----- [questions] -----

++ invalid query: truncated label
Press any key to continue . . . _
```

Figure 8: Truncated label

```
C:\Windows\system32\cmd.exe
Lookup : random4.irl
Query : random4.irl, type 1, TXID 0x4BC8
Server : 128.194.135.82
*****
Attempt 0 with 29 bytes... response in 1 ms with 281 bytes
TXID 0x4BC8 flags 0x33792 questions 1 answers 1 authority 0 additional 11
succeeded with Rcode = 0
----- [questions] -----
random4.irl type 1 class 1
----- [answers] -----
random.irl A 1.1.1.1 TTL = 30
----- [additional] -----
Episode.IV A 2.2.2.2 TTL = 30
A.NEW.HOPE A 2.2.2.2 TTL = 30
It.is.a.period.of.civil.war A 2.2.2.2 TTL = 30
Rebel.spaceships A 2.2.2.2 TTL = 30
striking.from.a.hidden.base A 2.2.2.2 TTL = 30
have.won.their.first.victory A 2.2.2.2 TTL = 30

** invalid record: truncated name
Press any key to continue . . . _
```

Figure 9: Truncated name