Subject: Re: wwnet
Posted by [EE]pickle-jucer on Fri, 01 Jul 2016 23:47:06 GMT
View Forum Message <> Reply to Message

Okay, so 1 and 1/2 years later and I've made some tiny progress . But I do have a few open questions if anybody would be willing answer them.

When I'm parsing raw packets sent between the client and server, this is the basic logic I'm following:

Step 1: Read in the CRC32 and compare it to the rest of the packet
Step 2: Read in the 2 byte header and bitmask out the PacketLength and IsMorePackets bit fields.
Step 3: Read in PacketLength many bytes and save them to later parse into Type, ID, SenderID, BitLength, etc.
Step 4: If(IsMorePackets == true){ goto Step 2 }

The 2 byte header is like such:
(1){1111111111}[11111]

() = (data >> 15) & 0x1 = IsMorePackets (Signifies if there is another packet after it.)
{} = (data >> 5) & 0x3FF = PacketLength (Packet length in bytes)
[] = (data >> 0) & 0x1F = Unknown (Somehow relates to decompression of repeated data?)

The question I have about this is about a function called when (Unknown - 1 > 0). The function in question, which is at ".text:0061BD90" (client address), seems to relate decompression of repeated data, but is too large for me to understand with my current knowledge of ASM. Does anybody know how this works, what it's supposed to do, or even its original name?

Also, while comparing the client<->server communication of the original client with a client running with TT scripts, I noticed a new packet type (8). This made me wonder, does TT hijack any fields that would make a client with TT scripts NOT be able to play on a server without TT scripts?