

Forum:[Hack Forums](#)

Thread: [Why do almost all botnets use HTTP protocol?](#)

SIM-5411207 - May 20, 2025, 9:28 am

Wouldn't it be better to use HTTPS and add an additional layer of encryption, or to write your own socket server and create a more private structure even make these connections with SSL/TLS? Can you explain the differences between having HTTP or HTTPS on the server or using Socket or Socket + SSL/TLS instead? I think a socket program and custom encryption would be the cleanest. What is the best way?

DramaKing - May 20, 2025, 12:19 pm

(May 20, 2025 09:28 AM)SIM-5411207 Wrote: [\[CITE\]](#) Wouldn't it be better to use HTTPS and add an additional layer of encryption, or to write your own socket server and create a more private structure even make these connections with SSL/TLS? Can you explain the differences between having HTTP or HTTPS on the server or using Socket or Socket + SSL/TLS instead? I think a socket program and custom encryption would be the cleanest. What is the best way?

First of all, there's no HTTPS or SSL/TLS to be clear. HTTPS is HTTP over SSL/TLS. Applications use sockets to communicate on a network. Second, botnets should use encryption, but they might be old, or the developers might be lazy.

StinkButt420 - May 20, 2025, 7:57 pm

(May 20, 2025 12:19 PM)DramaKing Wrote: [\[CITE\]](#) First of all, there's no HTTPS or SSL/TLS to be clear. HTTPS is HTTP over SSL/TLS. Applications use sockets to communicate on a network. Second, botnets should use encryption, but they might be old, or the developers might be lazy.

This is a very high quality answer, I'm not upgraded, so I can't donate or give quick love, but I can at least TELL you I appreciate this. Good on you!

SIM-5411207 - May 20, 2025, 9:13 pm

(May 20, 2025 12:19 PM)DramaKing Wrote: [\[CITE\]](#) First of all, there's no HTTPS or SSL/TLS to be clear. HTTPS is HTTP over SSL/TLS. Applications use sockets to communicate on a network. Second, botnets should use encryption, but they might be old, or the developers might be lazy.

First of all, thank you for your comment. You said that every botnet should use encryption. For example, should we create our own custom encryption system in a TCP socket program, or would it be correct to via SSL/TLS with a self-signed certificate? Or we can do both. Which one would be better?

DramaKing - May 20, 2025, 11:12 pm

(May 20, 2025 09:13 PM)SIM-5411207 Wrote: [\[CITE\]](#) First of all, thank you for your comment. You said that every botnet should use encryption. For example, should we create our own custom encryption system in a TCP socket program, or would it be correct to via SSL/TLS with a self-signed certificate? Or we can do both. Which one would be better?

Using an existing SSL library would be the usual method, I think.

SIM-5411207 - May 21, 2025, 12:16 am

(May 20, 2025 11:12 PM)DramaKing Wrote: [\[CITE\]](#) Using an existing SSL library would be the usual

method, I think.

I have seen in some examples that self-signed 100-year certificates are created. Is this how it should be done?

SIM-5613027 - May 21, 2025, 3:41 am

(May 21, 2025 12:16 AM)SIM-5411207 Wrote: [\[CITE\]](#) I have seen in some examples that self-signed 100-year certificates are created. Is this how it should be done?

use openssl if you want to generate a self-signed cert

richmitchman - May 21, 2025, 11:51 pm

It would be a great project to build out. Open a TCP socket, wrap it in a TLS layer with OpenSSL, send your own framed messages over that encrypted channel. Or you could just run HTTP + TLS