

Forum:[Hack Forums](#)

Thread: [Custom SSL/TLS C++ Reverse Shell \(HTTPS\) + AES](#)

Vixx - December 15, 2024, 5:26 am

When it comes to SSL/TLS reverse shells, the publicly available options are often limited to:

- Using msfvenom to generate an HTTPS reverse shell (signed).
- Using a PowerShell / python payload (high level languages).
- Using known tools like nc.exe

Using a standard reverse shell often results in unencrypted traffic, which can be easily flagged by Network Detection and Response (NDR) systems or firewalls. These tools inspect network traffic and can identify remote code execution patterns, blocking the binary and alerting defenders.

An encrypted reverse shell helps evade such detection by:

- Encrypting all communication, making it harder for network tools to inspect the traffic.
- Using SSL to blend in with legitimate HTTPS traffic.

To address this gap, I created a C++ SSL Reverse Shell POC (commented and explained):

- Undetected by Microsoft Defender and other AV solutions at the time of publishing (the ones I tested on).
- Enables secure communication via SSL, reducing the chance of detection.
- Using AES Encryption / Decryption and embedding the results and commands within HTTP headers to bypass deep packet inspection (Added)

More Info and POC: github.com/V-i-x-x/SSL-AES-Reverse-Shell/tree/main

Shapeless - December 15, 2024, 5:22 pm

Im interested more, how hard would it be implement something like this in my application, I am building an app that acts like a small very lightweight rat, where i have a pulse and a screenshot function. Would you be willing talking about setting this up for me for a fee? Also since i am doing a very lightweight rat with very limited , i repeat VERY limited functionality, wouldnt the encryption make my program more suspect than if i had it maybe sent to a http in webserver post functions instead? interested in your thoughts since you made this.

SIM-5600039 - December 17, 2024, 3:05 am

Please go ahead and share I want to see it. :)

Vixx - December 17, 2024, 3:35 am

It is already shared and public @bistratdbelay, you can access the github repo that i included.

@Shapeless, it would help bypass network detection tools / Firewalls which will detect based on the traffic that you have Remote Code Execution and trying to execute commands.

You can just reapply what I did in your application. it's a pretty simple c++ project (well commented and explained) that I did for everyone to be able to implement it easily, that's the intention.

The only difference or changes you have to make is:

- Send the command or whatever you're sending to the target encrypted and through an SSL Tunnel and get the response (the communication between the server and the client needs to be through an SSL Tunnel and encrypted so the network tools don't see anything suspicious)

I can check it out but not at the moment, I am currently training a client, I will have some free time starting next week, you can message me discord => on my github profile its visible.

dm8173675 - February 10, 2025, 12:29 am

Greetings to Everyone. Anyone got .php shell script I can upload in WordPress and Convert it into Shell.. I need to turn my WordPress into shell

Shapeless - February 11, 2025, 12:46 pm

@Shapeless, it would help bypass network detection tools / Firewalls which will detect based on the traffic that you have Remote Code Execution and trying to execute commands.

Would it really? use post / get from a webserver only with cloudflare, they would not know the contents of the data being sent, just as im communicating with a web. But yeah i thought it would mostly help with high end network detections yes this much should be true.