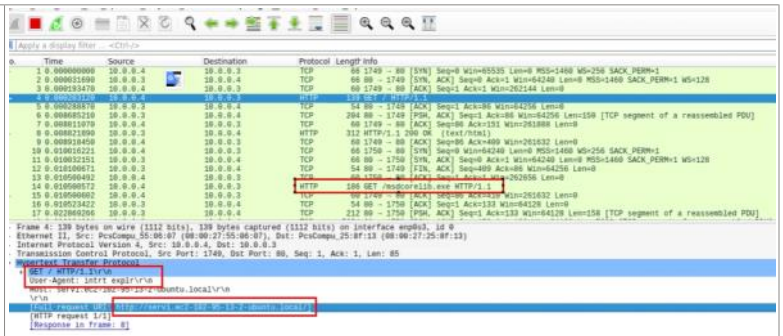
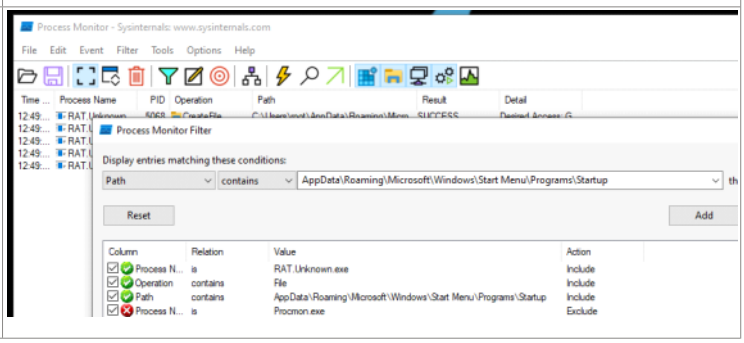
RAT.CmdSocket.exe.malz

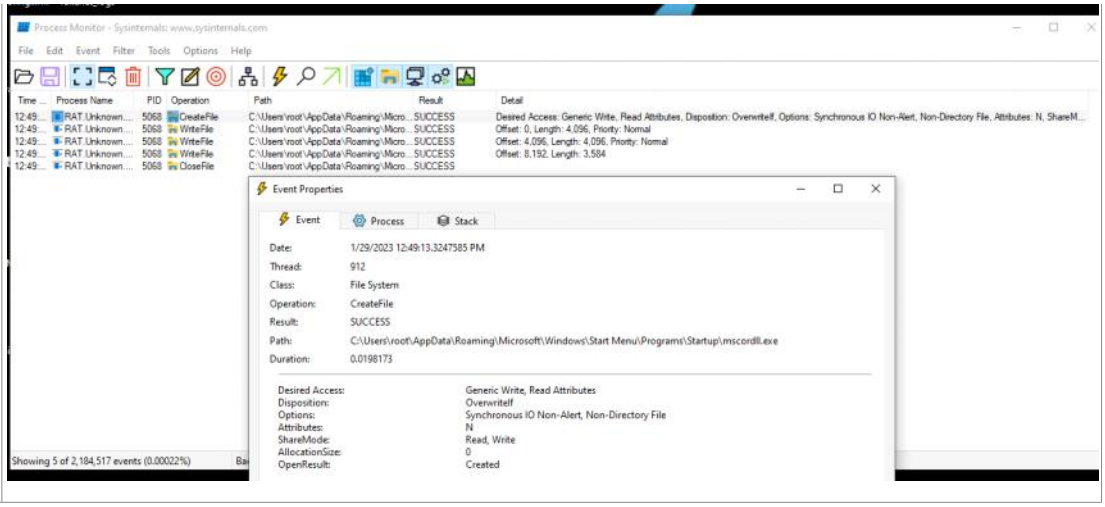
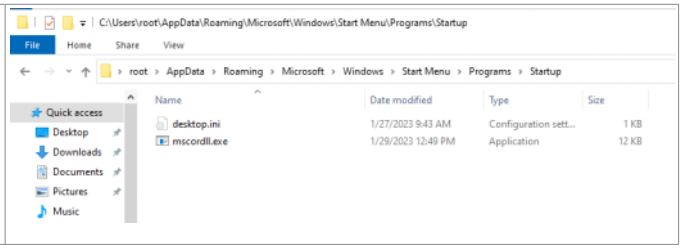
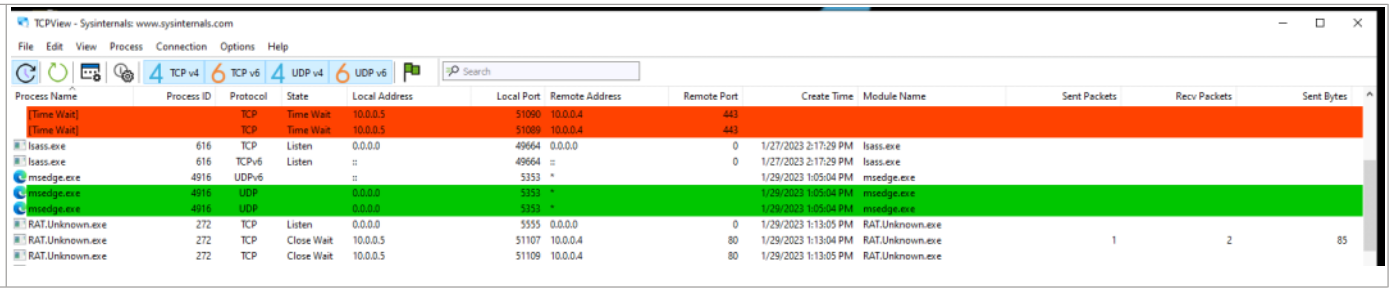
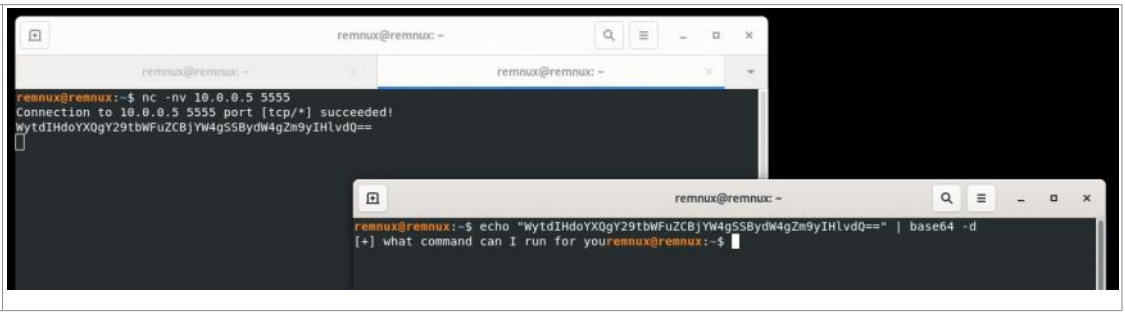
niedziela, 29 stycznia 2023 02:34

String/**FLOSS** output	@SSL support is not available. Cannot connect over SSL. Compile with -d:ssl to enable. @https @No uri scheme supplied. InternetOpenW InternetOpenUrlW @wininet @wininet MultiByteToWideChar @kernel32 @kernel32 MessageBoxW @user32 @user32 @[+] what command can I run for you @[+] online @NO SOUP FOR YOU @\mscordll.exe @Nim httpclient/1.0.6 @/msdcorelib.exe @AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup @intrt explr @http://serv1.ec2-102-95-13-2-ubuntu.local

Initial Det:	

Wireshark Packet Analysis	

Potential file download	msdcorelib.exe
Filters:	

Host Based Indicators	
Persistence binary	
TCP Socket in listening state	
Base64 encoded data from socket on TCP 5555	
Command injection capability: