

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
@inrt explr
@http://serv1.ec2-102-102-95-13-2-ubuntu.local
```

Initial Det:



Wireshark Packet Analysis

Wireshark packet capture showing a TCP connection. The interface displays packets 1 through 11. Packet 10 is highlighted, showing a TCP segment with Seq=65535, Win=1400, Len=256, SACK_PERM=1, and a payload of 256 bytes. The packet list on the left shows the sequence of packets, including the initial SYN, SYN-ACK, and subsequent data segments.

Time: 0.000000000 to 0.000000000
Destination: 10.0.2.8
Protocol: TCP
Length: 256
Seq: 65535
Win: 1400
Len: 256
SACK_PERM: 1
Payload: 256 bytes

Packet 10 details:

- Ethernet II, Src: Pci0000000000 (08:00:27:55:00:00), Dest: Pci0000000000 (08:00:27:55:00:00)
- Internet Protocol Version 4, Src: 10.0.2.15, Dest: 10.0.2.8
- Transmission Control Protocol, Src Port: 4444, Dest Port: 80, Seq: 1, Ack: 1, Len: 0
- TCP, Seq: 65535, Win: 1400, Len: 256, SACK_PERM: 1

Packet 11 details:

- Ethernet II, Src: Pci0000000000 (08:00:27:55:00:00), Dest: Pci0000000000 (08:00:27:55:00:00)
- Internet Protocol Version 4, Src: 10.0.2.15, Dest: 10.0.2.8
- Transmission Control Protocol, Src Port: 4444, Dest Port: 80, Seq: 1, Ack: 1, Len: 0
- TCP, Seq: 65535, Win: 1400, Len: 256, SACK_PERM: 1

Potential file
download

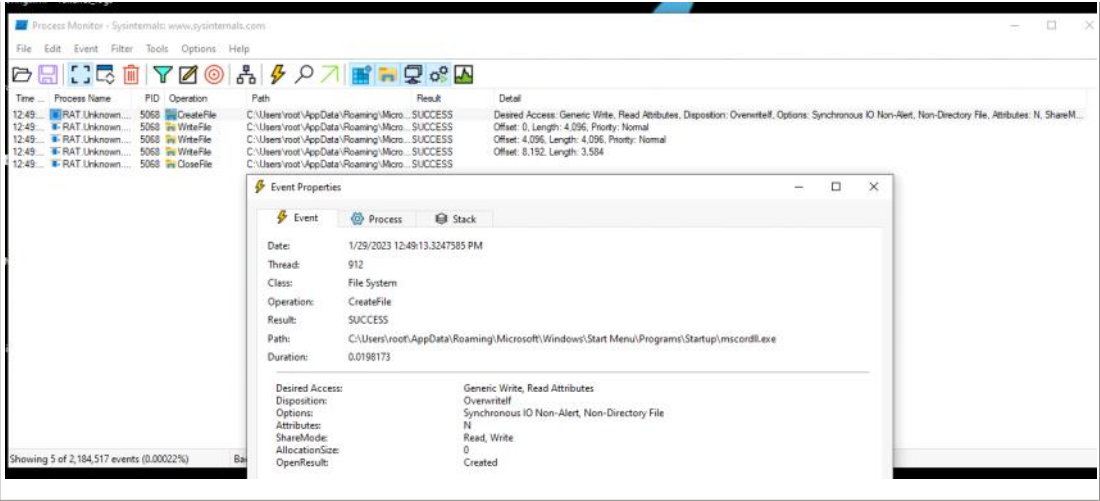
msdcorelib.exe

Filters:

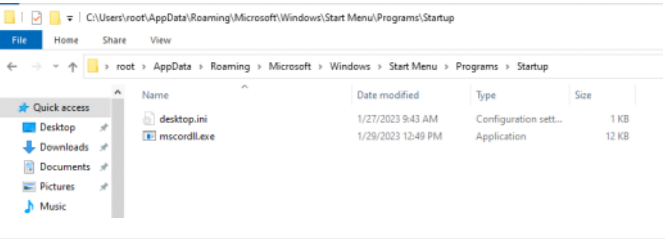
The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Edit", "Event", "Filter", "Tools", "Options", and "Help". The toolbar contains various icons for file operations, viewing, and filtering. The main window displays a list of events, with the selected event being a "Create File" operation by "Process N." at 12:49. The "Process Monitor Filter" dialog is open, showing a list of filters. The "Path" filter is selected, and the "Reset" button is highlighted. The filter list includes:

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Process N.	is	RAT Unknown.exe	Include
<input checked="" type="checkbox"/> Operation	contains	File	Include
<input checked="" type="checkbox"/> Path	contains	AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	Include
<input checked="" type="checkbox"/> Process N.	is	Process N.	Exclude

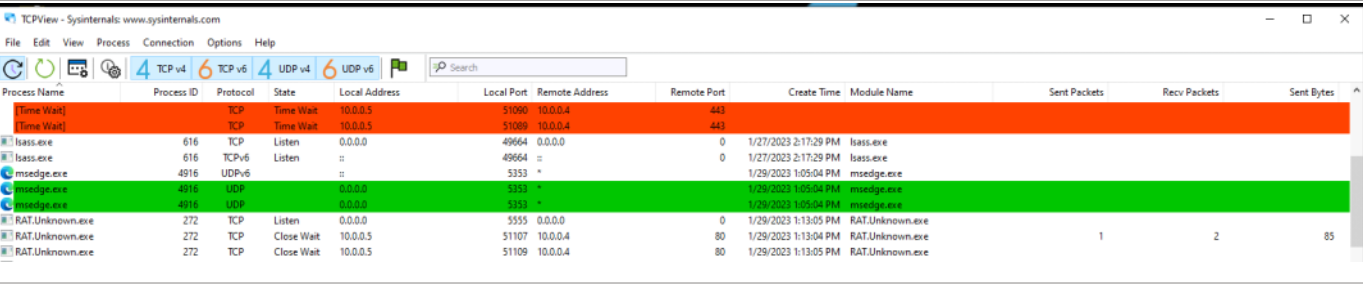
Host Based Indicators



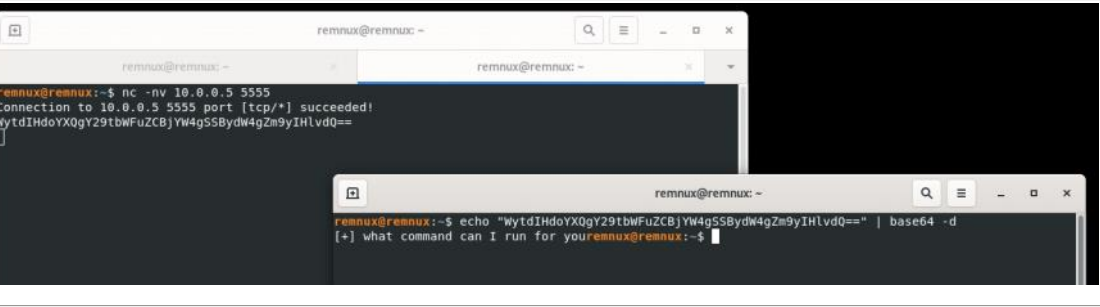
Persistence binary



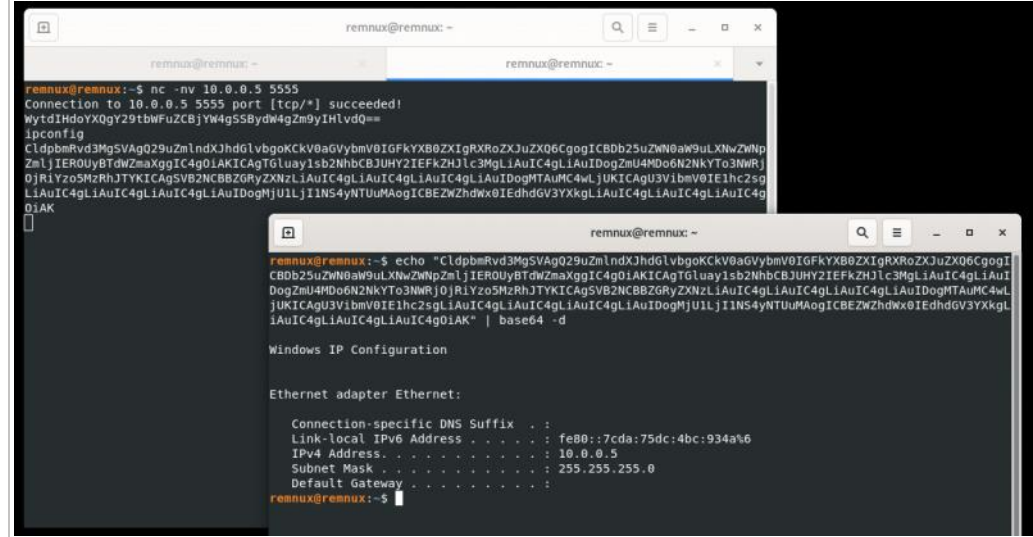
TCP Socket in listening state



Base64 encoded data from socket on TCP 5555



Command injection capability:



--	--