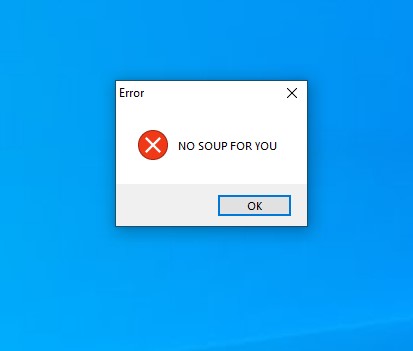
**Rat.CmdSocket.exe.malz**

|  |  |
| --- | --- |
| **Strings/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**](http://serv1.ec2-102-95-13-2-ubuntu.local/) |

# Initial Detonation



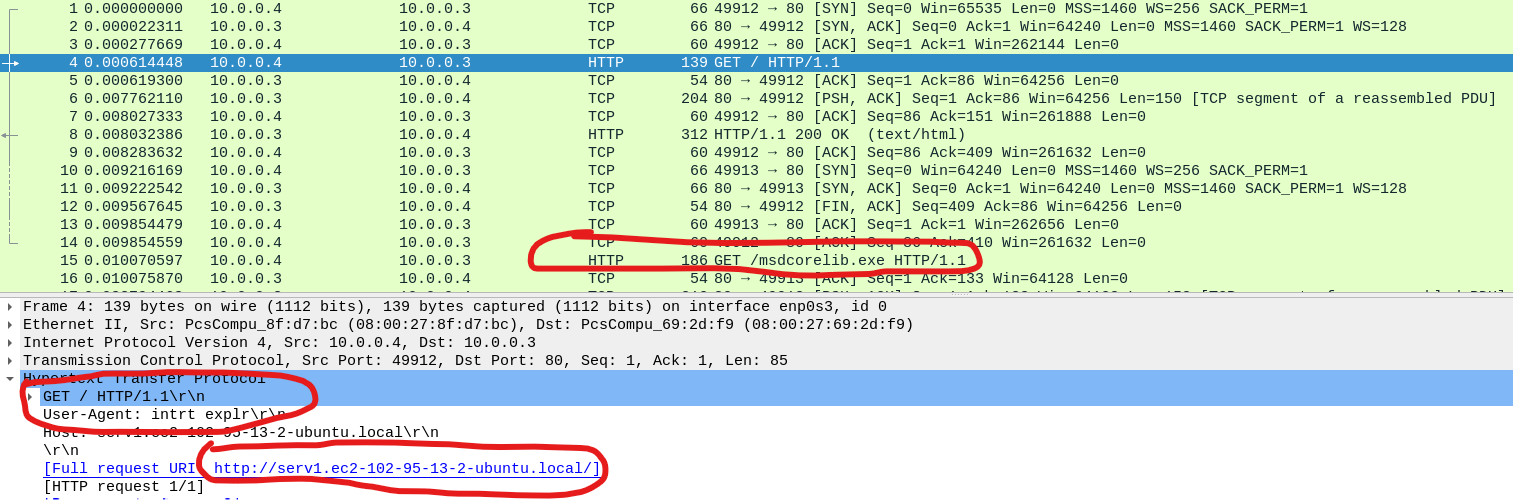
Just a box that says "NO SOUP FOR YOU." That's not fair.

# Network Indicators

Wireshark Packet Analysis

Head over to REMnux, and open a new terminal. Enter Wireshark. This will prompt Wireshark to execute.

Time to bust open Wireshark and run Rat.Unknown.exe.

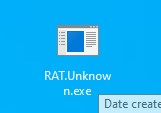


As we can tell above, we can see the 3-way handshake, and an HTTP request was made. We also know that it has downloaded something served up by INETSIM, possibly a second stage payload.

|  |  |
| --- | --- |
| **Potential File Download** | **msdcorelib.exe** |

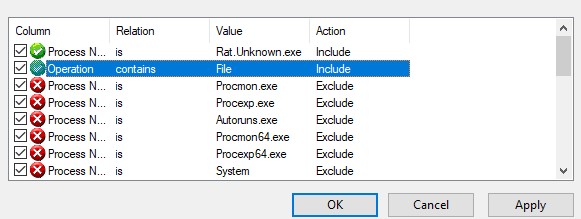
# Host Based Indicators

Let's revert back then re-arm the malware by renaming it. Please ensure it ends with .exe.



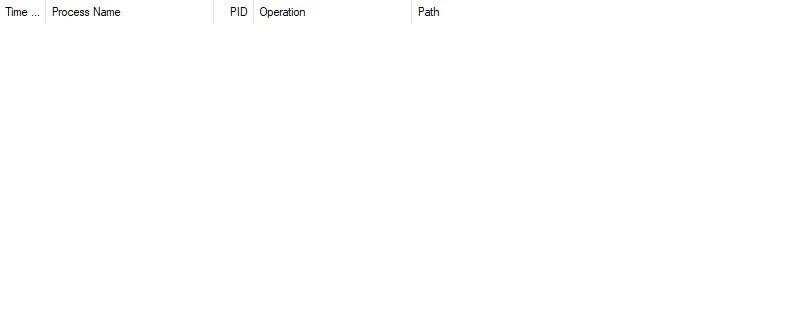
Let's open up Procmon and agree to the license agreement. Then let's head on over to filters, and add two filters.

1. Process Name is Rat.Unknown.exe
2. Operation contains File

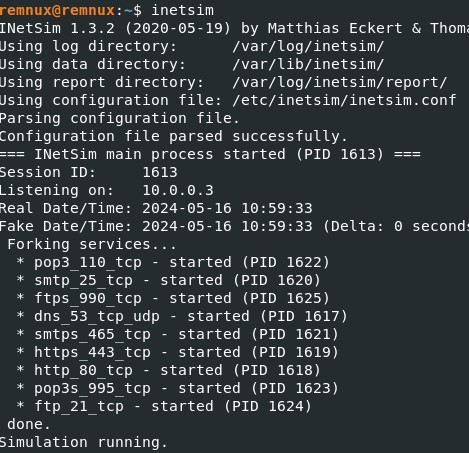


Make sure to click Add, Apply and then OK.

At first, nothing will populate.



Head over to REMnux and make sure INETSIM is still running.



Now we are observing host based indicators at this point. We don't need to worry about Wireshark anymore, so it can be closed.

Let's move back over and detonate Rat.Unknown.exe.



Navigate back over to Procmon. Wow! That's a ton of information.

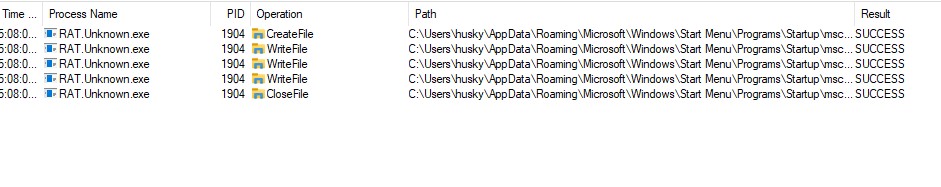
Let's look back at our notes and see if we can find something else to add to filters in Procmon.

AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

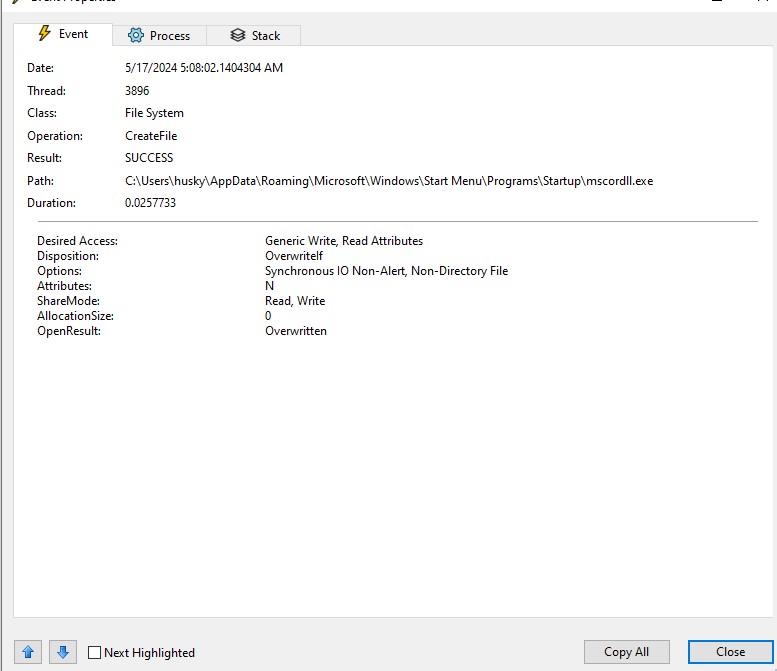
The Startup directory is often abused and utilized by malware to install itself as persistent, or install a second payload. Let's copy that, and navigate back to Procmon to create a new filter.

This filter will be PATH CONTAINS AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup. Click Add, then Apply, and finally OK.

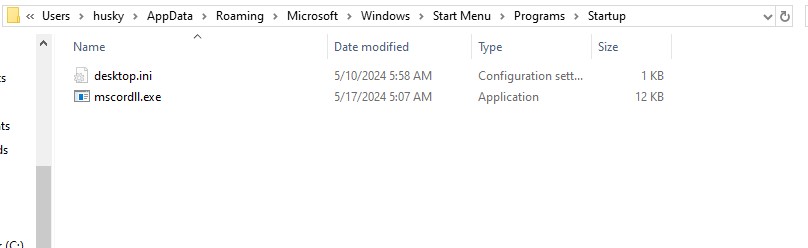
Wow! This is much more digestible now.



Lets expand the details pane. Click on The top process called "Create File".



The mscordll.exe looks might sus. Let's navigate there in file explorer to see if it actually wrote anything.



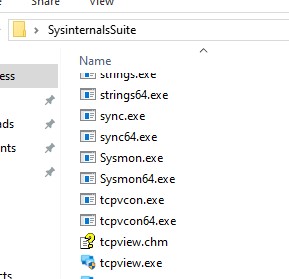
Mighty sus indeed. This shows that if you logout, and then log back in, whatever is right here is going to be executed at the time of login.

We need to do some further analysis. Let's reset our VM, and restore current snapshot from before we detonated.

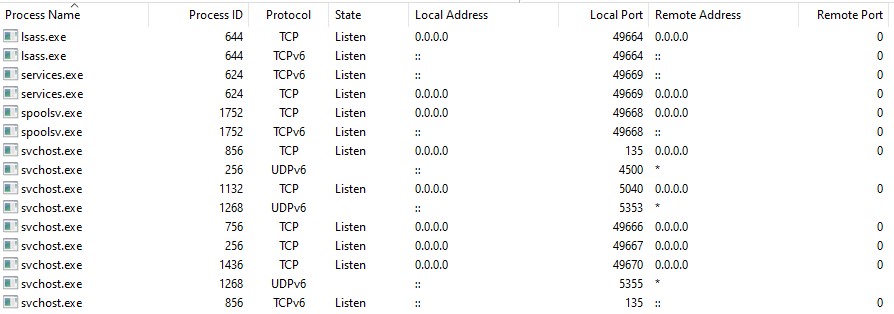
Once restored, we need to rearm our malware.



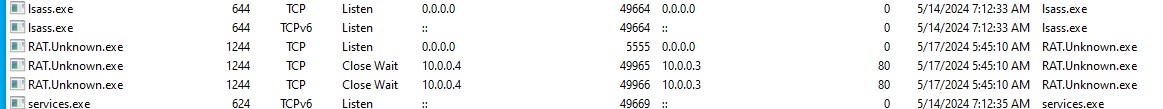
Navigate to SysinternalsSuite. If you do not have it, you can grab it off the Microsoft website. It's FREE!!!! <https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>Let's run TCP View (.exe).



Let's sort Process Name in Alphabetical order. You might have to click Process Name a few times. Take note of the Process name we are searching for Rat.Unknown.exe.



Detonate Rat.Unknown.exe. Navigate back to TCP View, and we can observe what we are looking for.

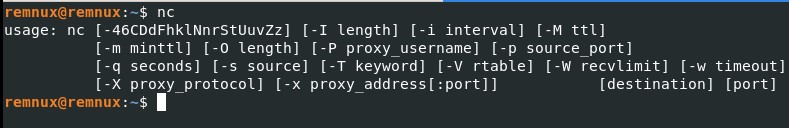


We can deduce that Rat has the TCP Socket set to a Listen state. The local address for that is

0.0.0.0. This means give me any IP Address. Also, the port is 5555.

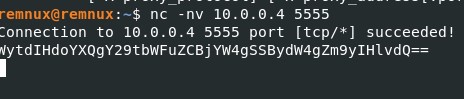
Navigate back to REMnux, and open a new terminal. Let's run a pretty cool tool called Netcat.

This can be done by entering "nc".



Let's type in "nc -nv 10.0.0.4 5555".

*N means no DNS, and V translates to Verbose. 10.0.0.4 happens to be our Flare VM host. The port we observed earlier is 5555.*

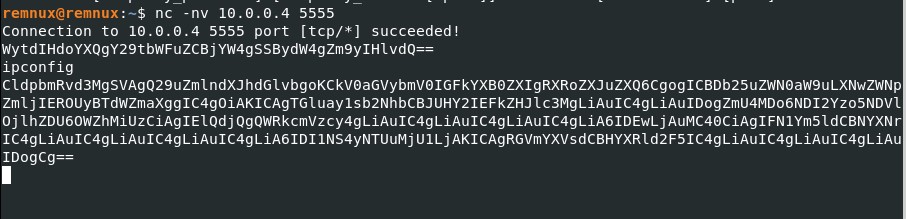


Copy this code, and open another terminal and type echo followed by the code piped with base 64 -d.

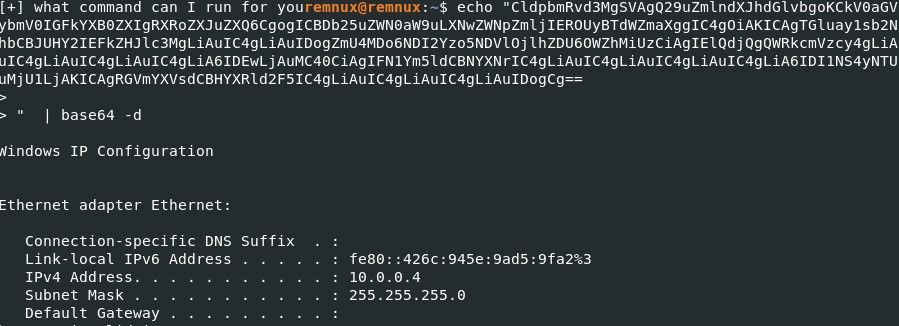


|  |  |
| --- | --- |
| **Base encoded data from Socket on TCP**  **5555** |  |

Navigate back to the terminal which you copied the code from, and type in "ipconfig".



We can observe some information populate and ipconfig is ran. Lets copy this new information. Head back over to our echo terminal, and enter replace the prior information we copied with the new information and run.



Looks like command injection is viable.

|  |  |
| --- | --- |
| **Command**  **injection capability** |  |

Based upon all of the information, this appears to be a full-blown command execution remote access trojan. It opens on port 5555 to the file system. It has command injection capabilities, and it writes something to the Startup directory.