

njRAT - Remote Access Trojan

njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it is capable of accessing a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing the process and file manipulations, and viewing the victim's desktop.

RATs help an attacker to remotely access complete GUI, control victim's computer without his or her awareness and are capable of performing screening and camera capture, code execution, keylogging, file access, password sniffing, registry management, and so on. It infects victims via phishing attacks and drive by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

The njRAT Trojan can be used to control Botnets (network of computers), allowing the attacker to update, uninstall, disconnect, restart, close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the Command and Control server software.

Objectives

- Create a server using njRAT.
- Access the target machine remotely.

Requisites

- Windows 10 (Attacker).
- Windows 7, 8 or Server (Target).
- **please apply this on VMs only**

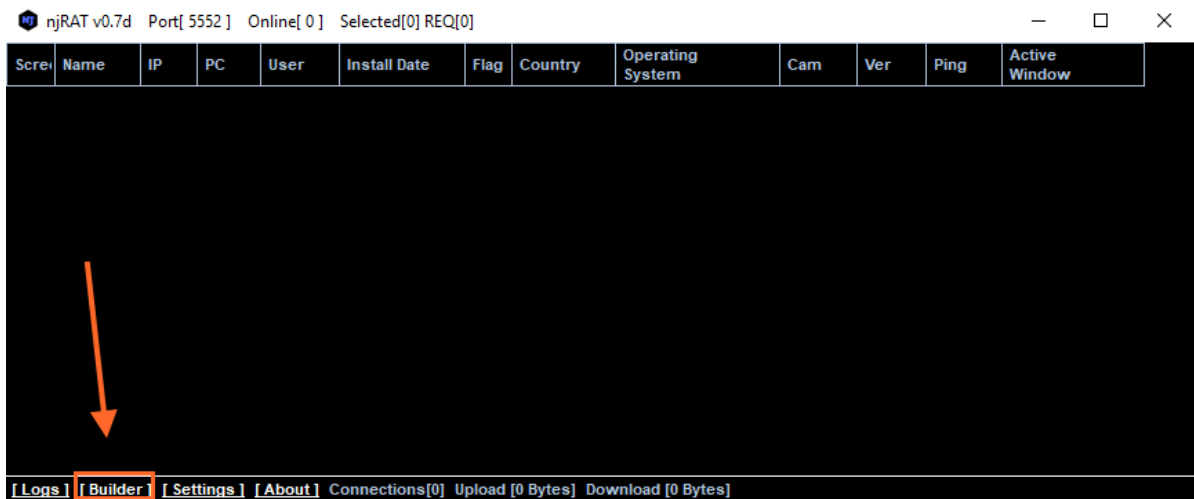
Create an Executable Server with njRAT

1. Log in to the **Windows 10** and install the **njRAT**.
2. Launch the njRAT, the GUI appears along with a pop-up, where you need to specify the port you want to use to interact with the target machine. Use the

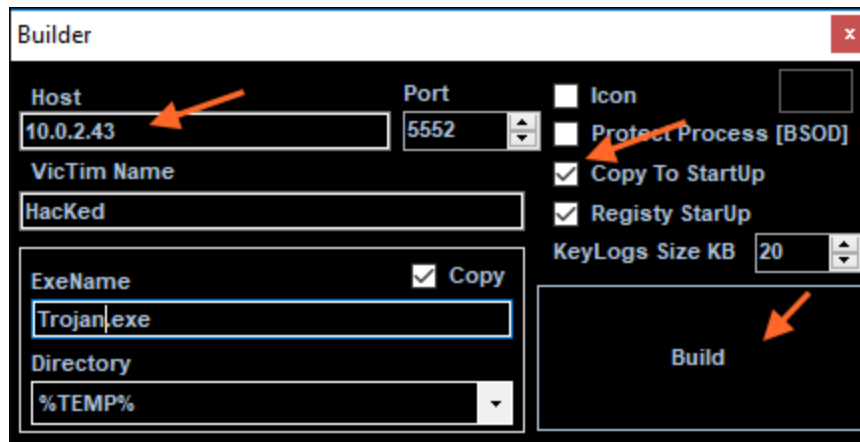
default port number **5552**, and click **Start**.



3. Click on **Builder** at lower-left corner.



4. On the **Builder** dialog-box, enter the IP address of the **Attacker machine - Windows 10**, check the option **Copy to StartUp and Registry StarUp**, then click **Build** as shown below:



5. **Save** the file on the **Desktop** and name as **Example.exe**.
6. Now, we need to use any technique to send this server to the intended target through mail or any other way.

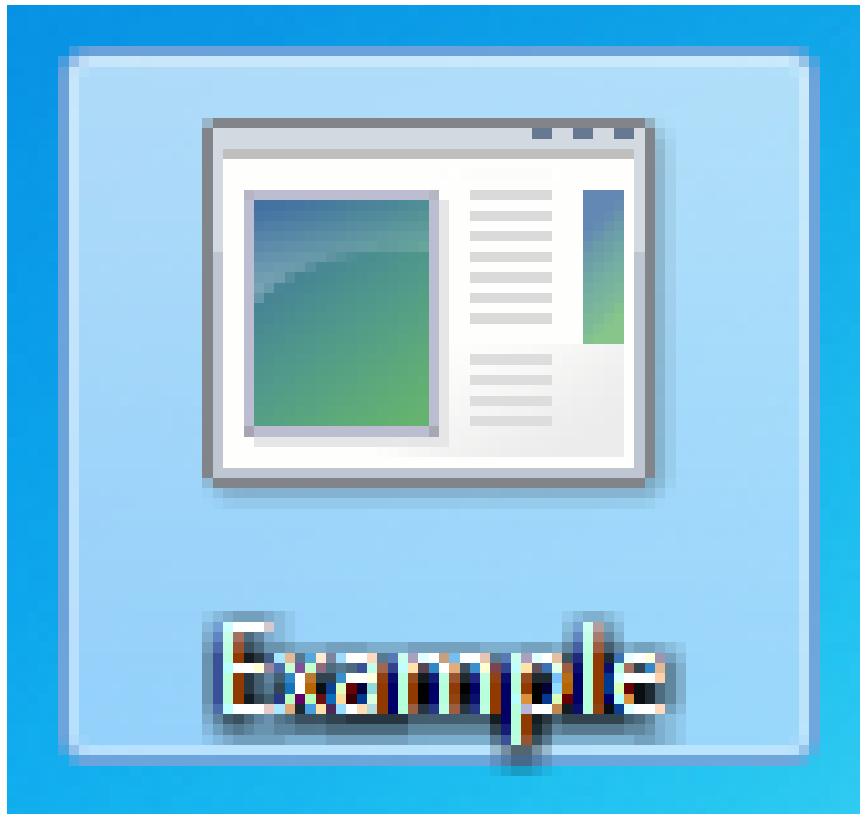
To make this easier in this lab, I copied the **Example.exe** file in the **shared network location**.

Execute the Server on the Target Machine

In this Lab I'm using Windows 7 SP1 virtual machine.

Note: Make sure to **enable** the Firewall on the target machine.

1. Drag the **Example.exe** file to your Desktop and double-click it.



As you can see below, the connection was successfully established.

```
C:\Windows\system32>netstat
```

Active Connections			
Proto	Local Address	Foreign Address	State
TCP	10.0.2.43:49176	10.0.2.45:5552	ESTABLISHED

2. Switch back to the **Windows 10** (Attacker). When the target double-clicks the server, the executable starts running and the njRAT GUI running on the Windows 10 establishes a persistent connection with the Target machine as show below:

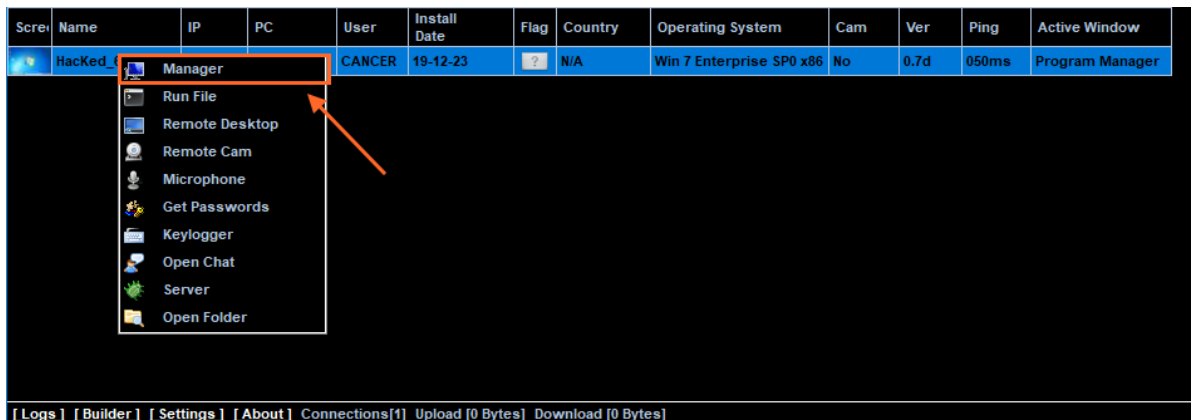


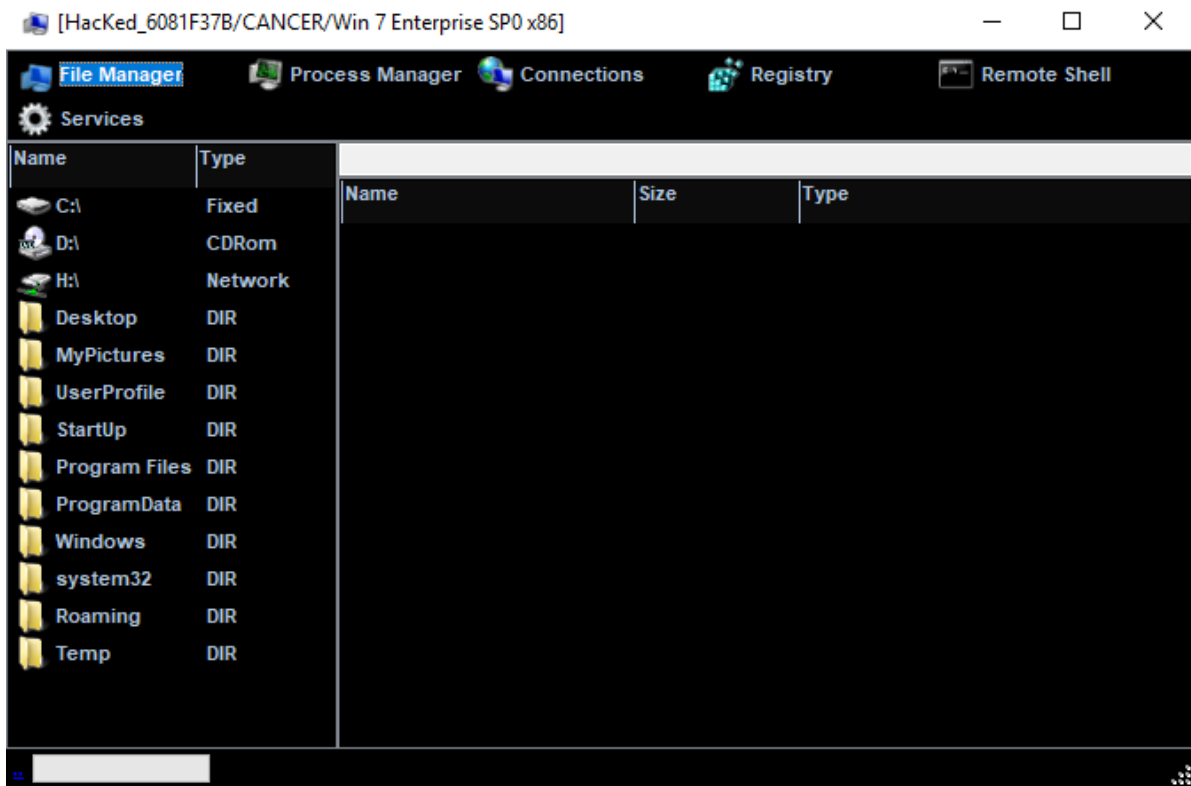
The GUI displays the machine's basic details such as the IP address, OS, user name and so on.

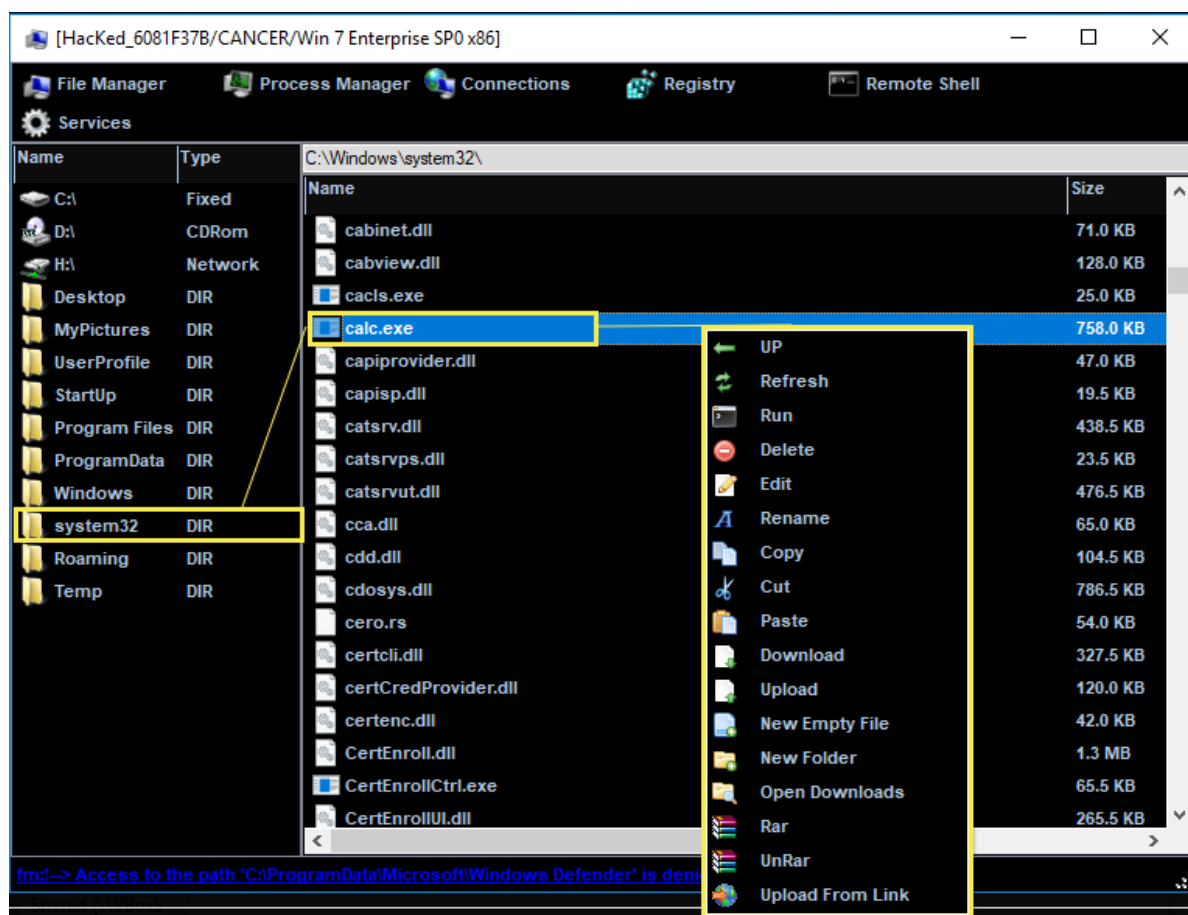
Note: Unless the attacker disconnects the server on his own, the victim machine remains under his control.

Manipulate Files on Target machine

- Right-click on the detected Target machine and click **Manager**. Double-click on any directory in the left pane. You can right-click any selected directory and manipulate it using the contextual options:

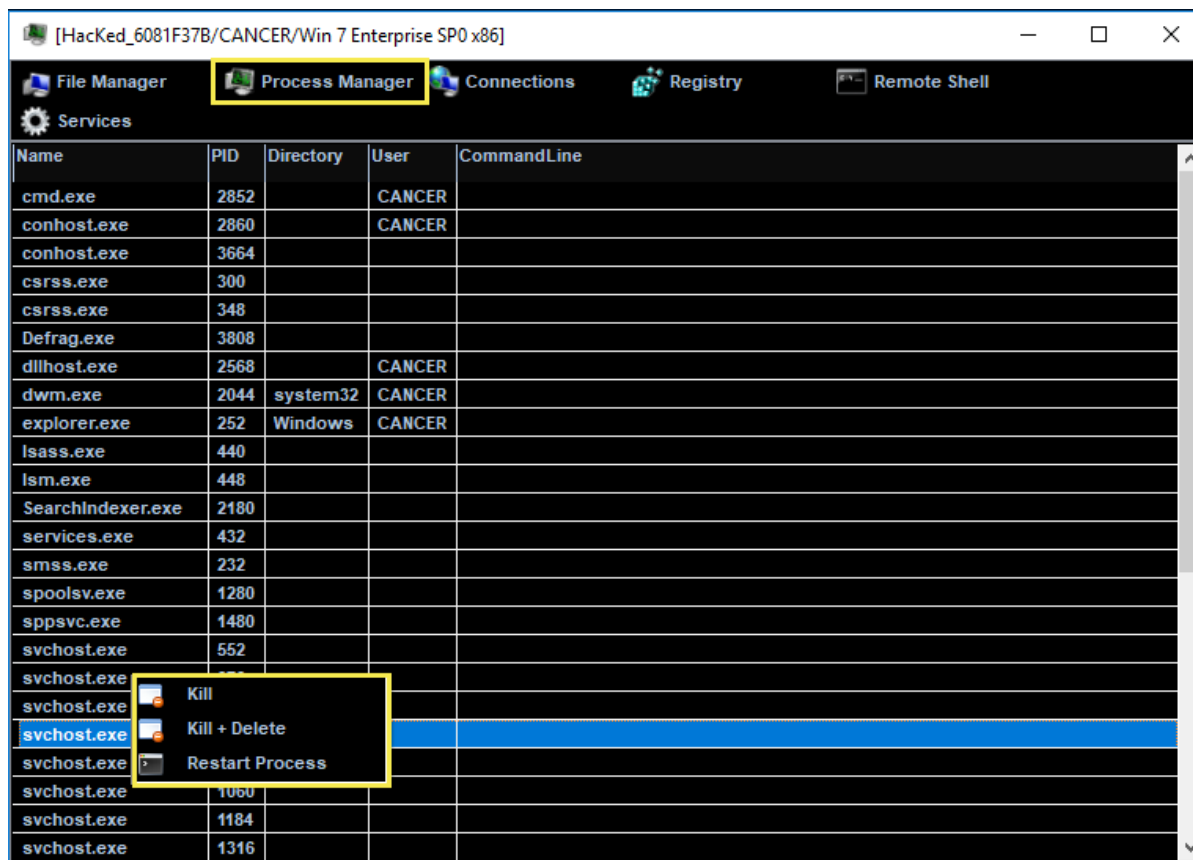






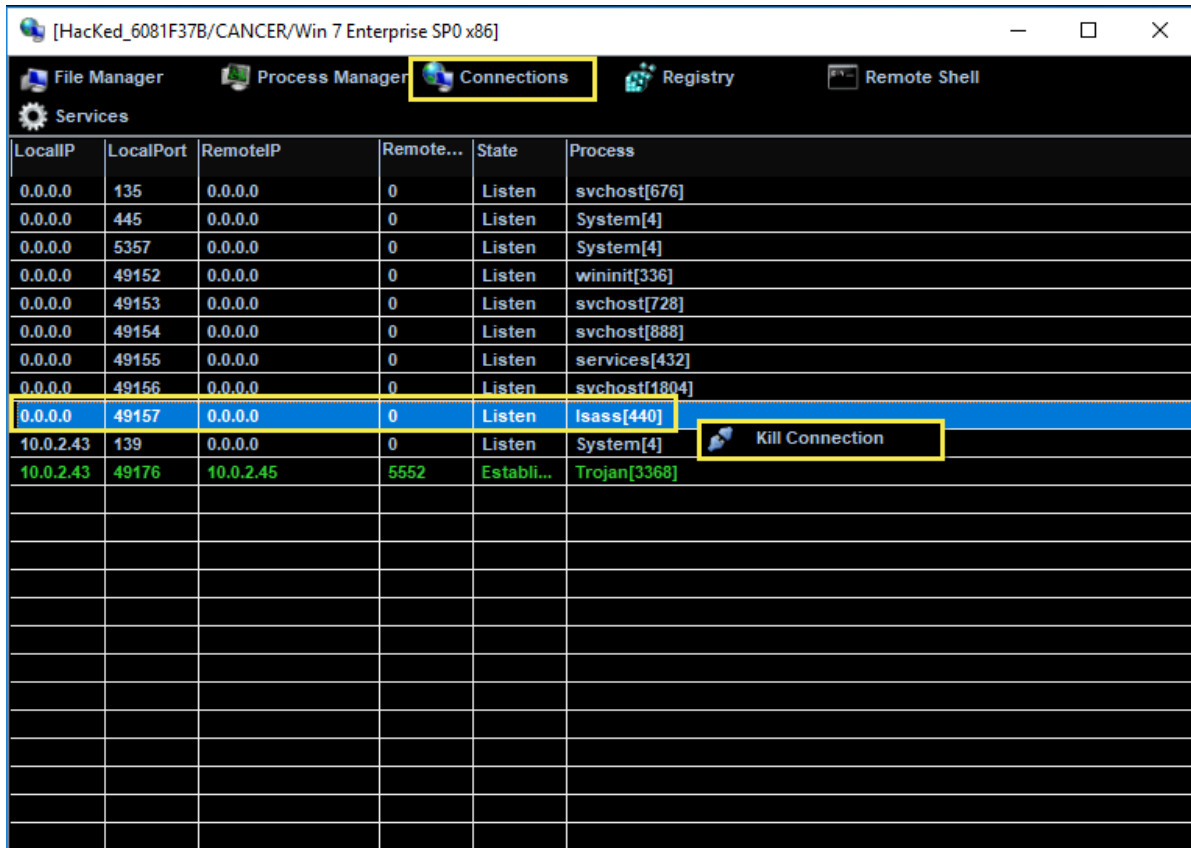
Manage the Processes

- Click on **Process Manager** on the top menu. You will be redirected to the Process Manager, where you can right-click any process and perform actions such as **Kill**, **Delete**, and **Restart**.



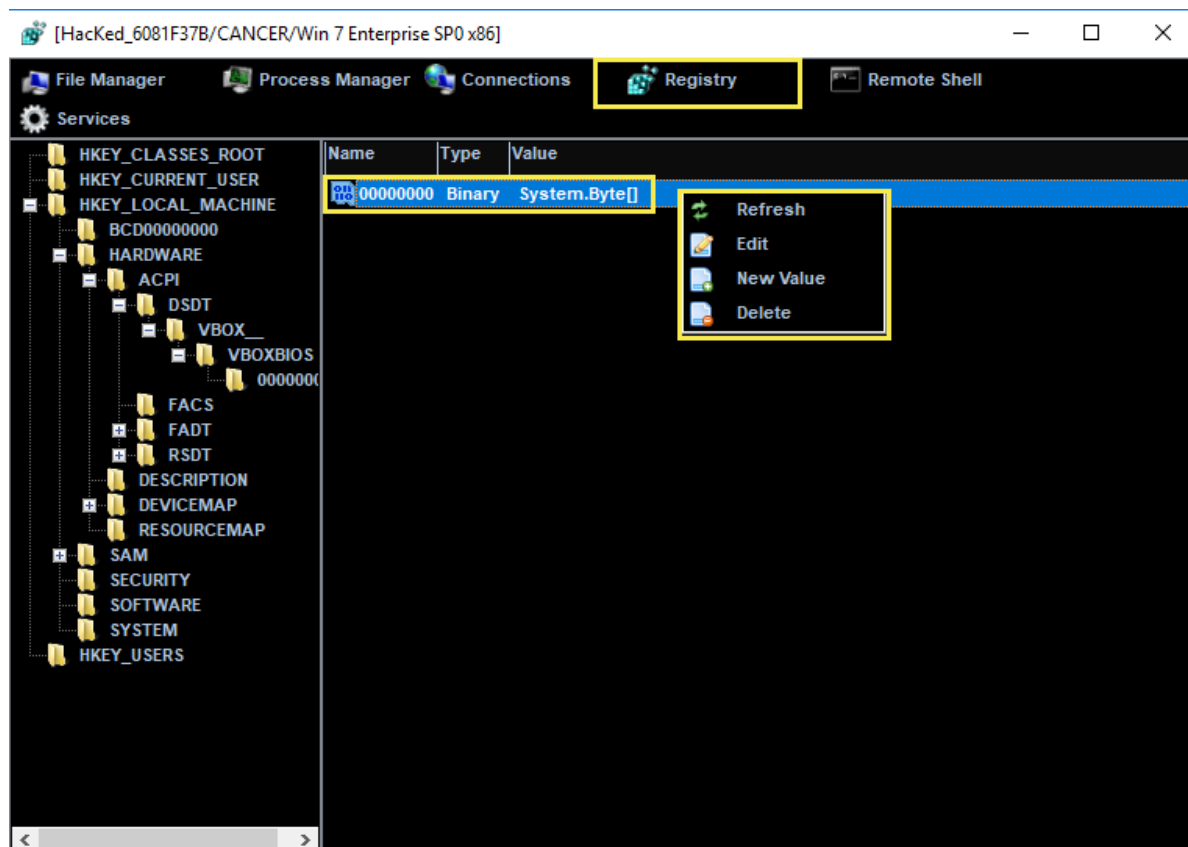
Manage the Connections

- Click on **Connections** on the top menu and select a specific connection, right-click on it, and click **Kill Connection**. This action kills the connection between two machines communicating through a particular port.



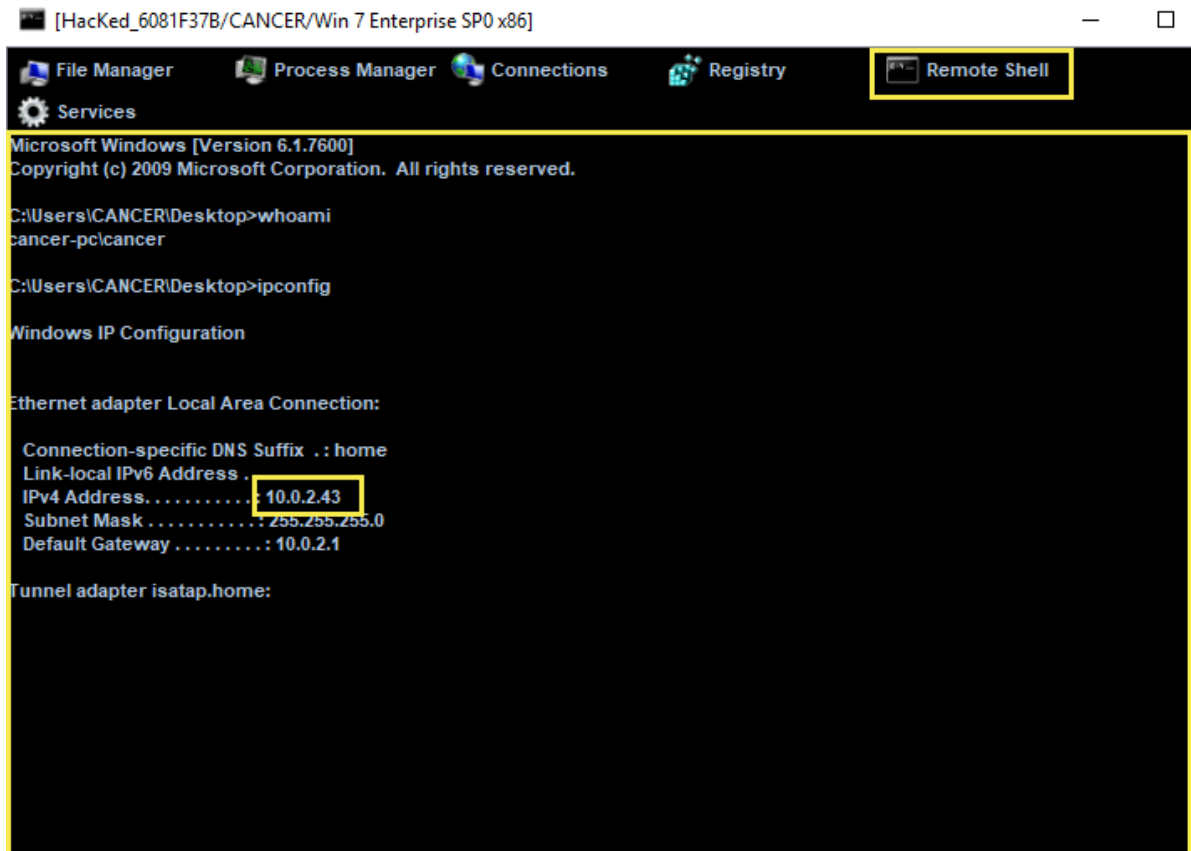
Manage the Registries

- Click on **Registry** on the top menu and choose a registry from the left pane, right-click on its associated registry files, a few options appear to manipulate them.



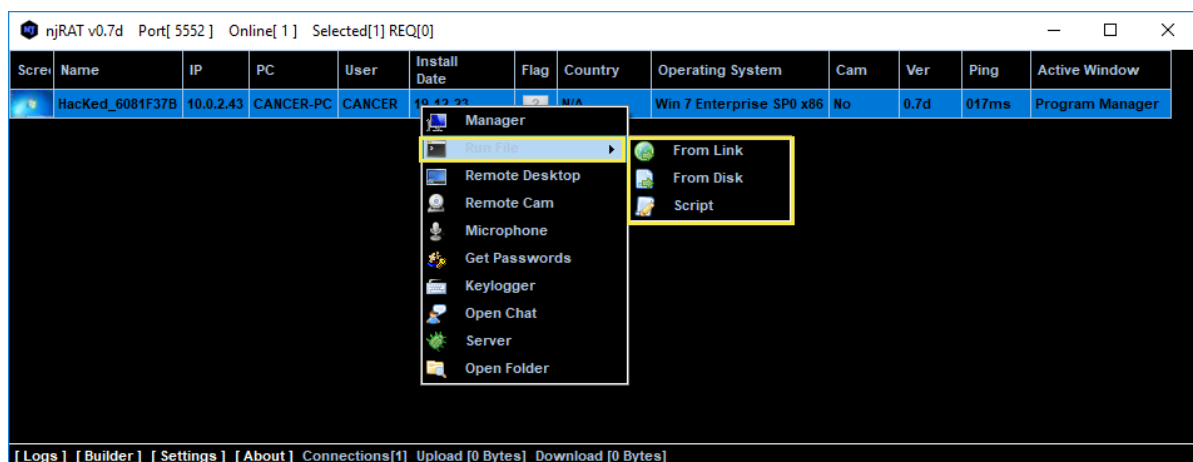
Launch a Remote Shell

- Click on **Remote Shell** on the top menu. This action launches a remote command prompt of the target machine. Similarly, you can issue all the other commands that can be executed in the command prompt of the target.



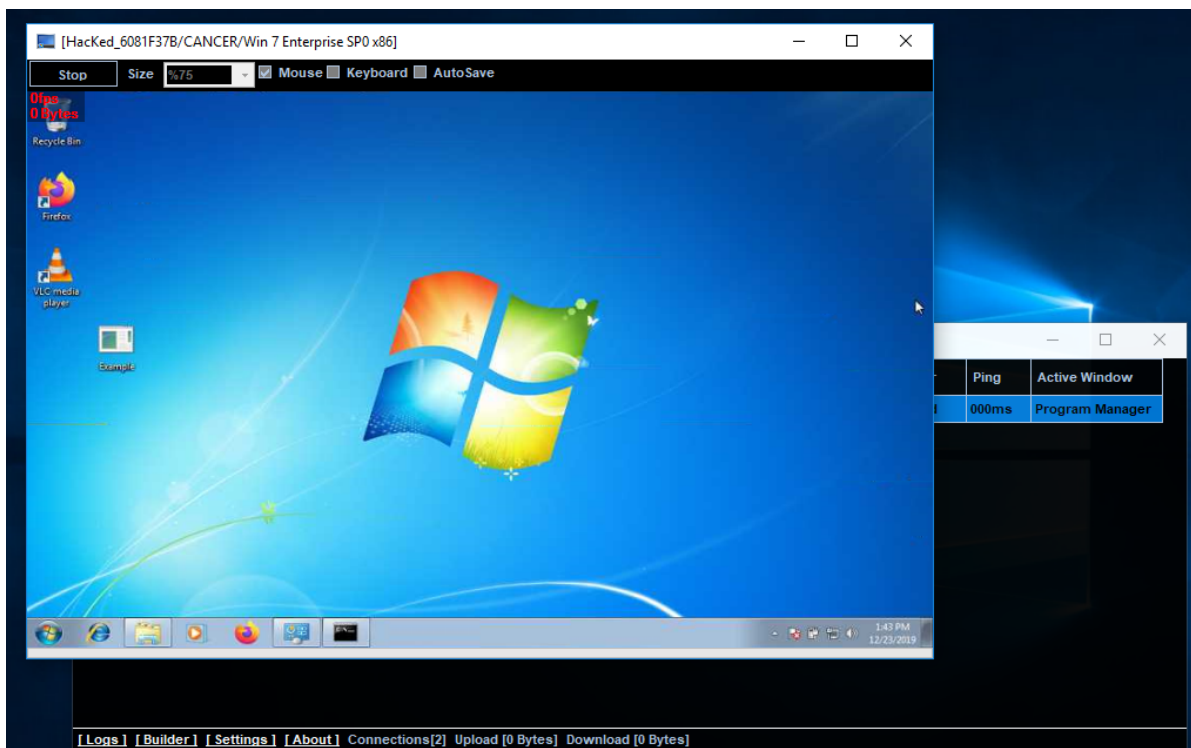
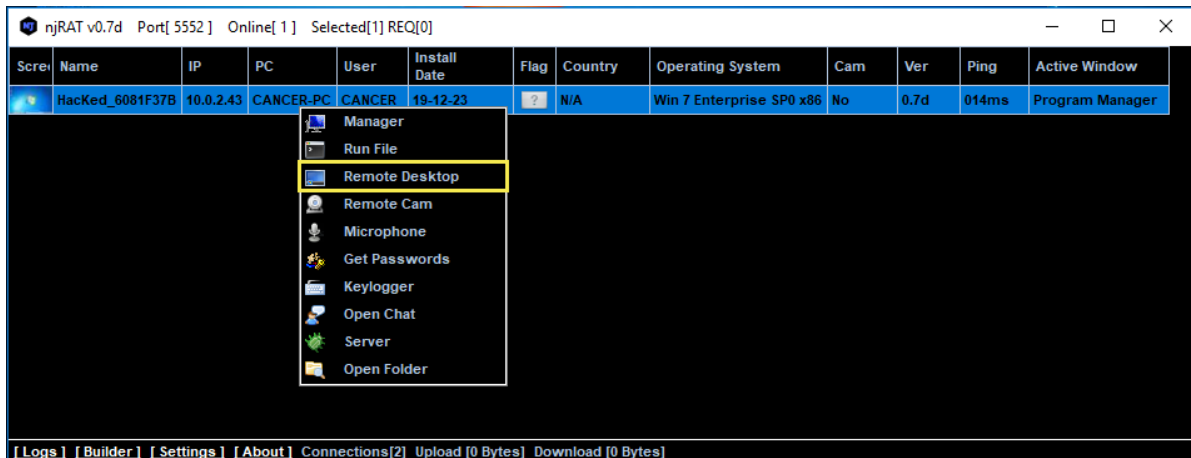
Run File

- On the main window of njRAT, right-click on the Target machine and select **Run File**. An attacker makes use of these options to execute scripts or files remotely from his/her machine.



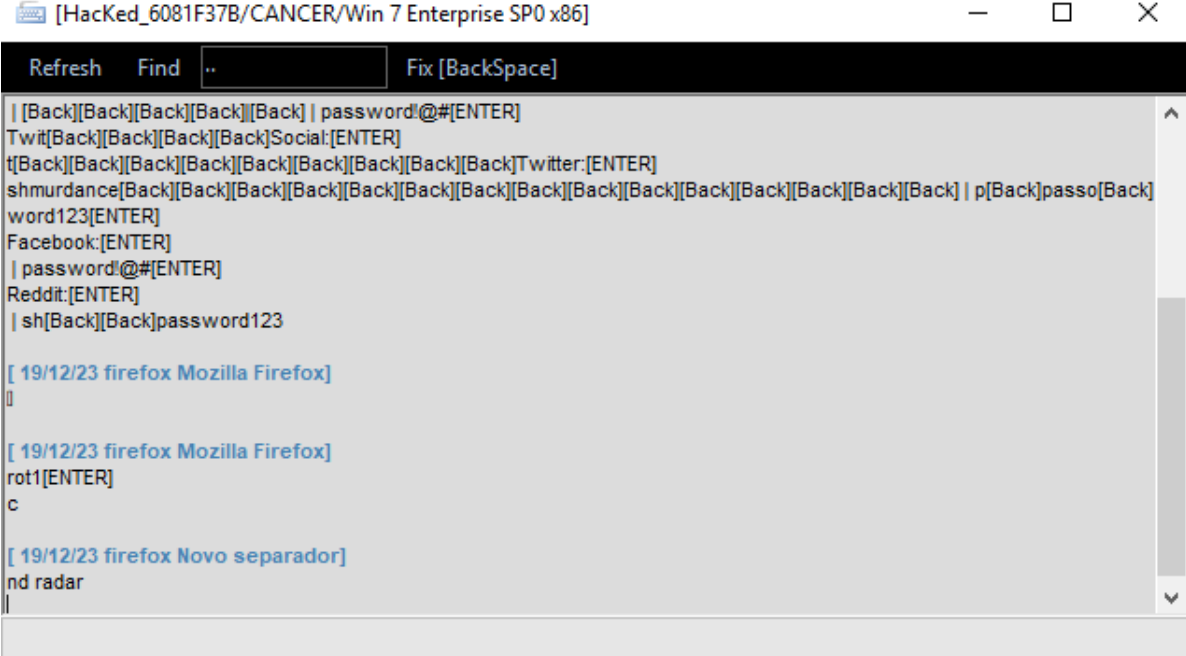
Launch a Remote Desktop Connection

- Right-click on the Target machine and select **Remote Desktop Connection**. This launches a remote desktop connection without target's consent. You will be able to remotely interact with the victim machine using the mouse or keyboard. In the same way, you can select the **Remote Cam** and **Microphone** to spy on the target and track voice conversations.



Perform Key Logging

- Switch to the **Windows 7 (Target machine)**. Let's assume that you are a legitimate user and perform a few activities such as logging into any websites or typing text in some documents.
- Now, switch back to **Windows 10** machine / njRAT GUI and right-click on the target machine, select the **Keylogger** option.



The screenshot shows a window titled "[HacKed_6081F37B/CANCER/Win 7 Enterprise SP0 x86]". Inside the window is a text area displaying captured keystrokes. The text area has a toolbar with "Refresh", "Find", and "Fix [BackSpace]". The captured text includes:

```
| [Back][Back][Back][Back][Back] | password!@#[ENTER]
Twit[Back][Back][Back][Back]Social:[ENTER]
t[Back][Back][Back][Back][Back][Back][Back][Back]Twitter:[ENTER]
shmurdance[Back][Back][Back][Back][Back][Back][Back][Back][Back][Back][Back][Back][Back] | p[Back]passo[Back]
word123[ENTER]
Facebook:[ENTER]
| password!@#[ENTER]
Reddit:[ENTER]
| sh[Back][Back]password123

[ 19/12/23 firefox Mozilla Firefox]
|

[ 19/12/23 firefox Mozilla Firefox]
rot1[ENTER]
c

[ 19/12/23 firefox Novo separador]
nd radar
|
```

The keylogger window appears, displaying all the keystrokes performed by the target.