August 19, 2017

Command and Control – PowerShell

netbiosX | Red Team | C&C, C2, Penetration Testing, Pentesting, PoshC2, PowerShell, Red Team | 4 Comments

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 give 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\
[+] Sucessfully installed PoshC2
PS C:\PoshC2> _
```

PoshC2 – Installation

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

```
 ___________                 ._.      ___________  ___________
 \_____   \ ____   _____   | |__   \_   ____  \ \_____   \
  |     ___/  _ \ /  ___/   |  \  /    \  \/  /  ____/
  |    |  (  <_> )___ \|   Y  \ \     \____/       \
  |____|   \____/____  >___|  /  \______  /\_______ \
                     \/     \/          \/         \/
=============== 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

Recent Posts

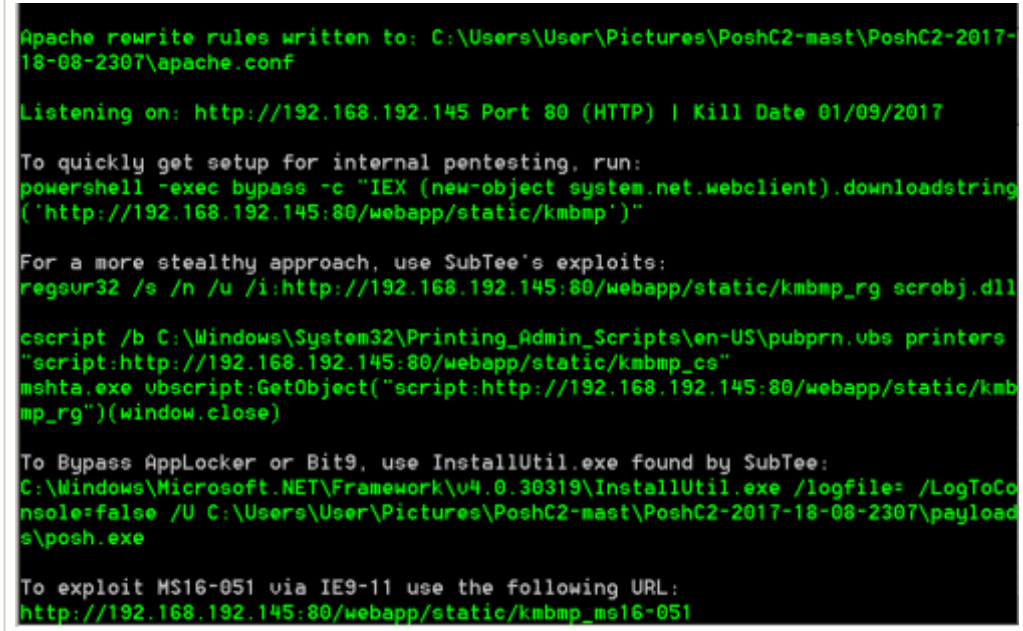
- Situational Awareness
- Lateral Movement – WinRM
- AppLocker Bypass – CMSTP
- PDF – NTLM Hashes
- NBNS Spoofing

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)

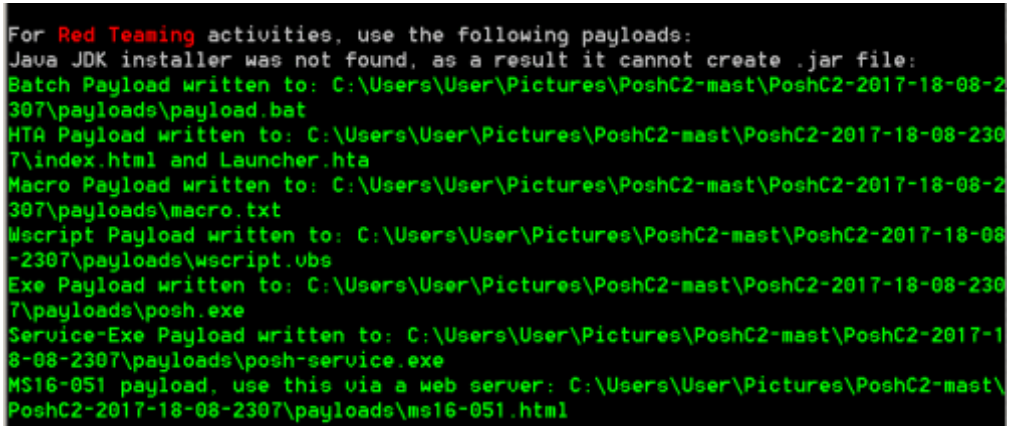
Archives

host via PowerShell.



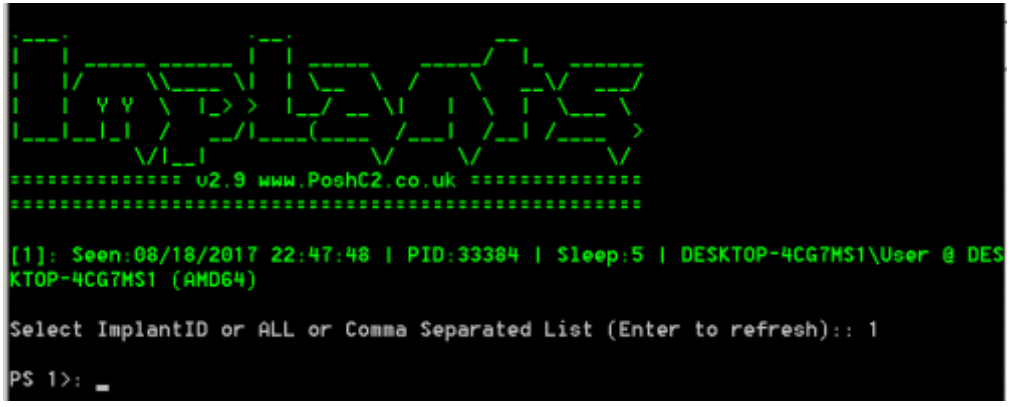
PoshC2 – Techniques

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



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.



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:

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

@ Twitter

- RT **@sensepost**: If you liked **@NeomindMusic**'s series on head exploitation (see **twitter.com/sensepost/stat…** for links). Make sure to check out his… **47 minutes ago**
- I don't get often into lists but always glad to get some unofficial recognition **blog.feedspot.com/pentest_blogs/** **56 minutes ago**
- **@jaysonstreet @hackinparis @winnschwartau @mjmasucci @gscarp12** I will be there for another year! Looking forward to catch up! **5 hours ago**
- RT **@notsosecure**: New blog by the **#NotSoSecure** team: Data Ex filtration via formula injection **notsosecure.com/data-exfiltrat… 6 hours ago**
- GyoiThon - A growing penetration test tool using Machine Learning **github.com/gyoisamurai/Gy… 12 hours ago**

Follow @netbiosX

Pen Test Lab Stats

- 3,008,481 hits

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:

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
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0

```
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

Advertisements

Older posts