Offense and Defense – A Tale of Two Sides: PowerShell

PowerShell allows you to download a file by using Invoke-WebRequest, System.Net.WebClient, and Start-BitsTransfer. You can then use Start-Process, Invoke-item, or Invoke-Expression to run the downloaded file. If you ever see this combination, and you know your admins don't use these tools to download and execute files, it could be malicious and something worth checking out.

System.Net.Webclient also lets you download the contents of a file directly into a running process in memory and then run it. This is better known as "fileless malware," and is used to try and bypass traditional AV products.

It's normal or typical to see powershell.exe spawned by explorer.exe, but if cmd.exe is the parent process for powershell.exe, that might be a bit more suspicious, as many of the malicious attacks come through the command line process. We can then go back to the process that spawned cmd.exe.

If it's being called by an MS office program, such as Word or Excel, there is a very good chance it's malicious. In addition to MS Office programs spawning cmd.exe and then powershell.exe, some other ones you may want to pay attention to are mshta, tasking, wuapp, wscript, and script.

Other signs to look for to detect malicious PowerShell activities are the flag options. Below are a few to look out for.

- Exec Bypass – This allows you to get around the execution policy after it has been set. Even if you have restrictions set for better security, this flag can bypass some of them.
- WindowsStyle hidden – As you can tell, this one will make hide operations from the user.
- Nop or Noprofile – This flag will ignore the commands in the profile that you have set.
- Enc /Encode– This will encode using base64 encoding.
- Mixed Case – Text is mixed between upper and lower case.

As you go through the process of testing each PowerShell attack technique, it is important to understand the technique, simulate the attack technique, monitor your security controls, evaluate if any gaps exist, and document and make improvements needed for coverage.