PowerShell Commands to look for

NOTE:
Taken from Windows+PowerShell+Logging+Cheat+Sheet+ver+Sept+2018+v2.2.pdf

POWERSHELL MODULES:
The following is a list of PowerShell module calls that you should monitor for executing using either Sysmon, WLS or the enhanced module logging of PowerShell. This is by no means a complete list.

Any “Set-“, “Get-“, “Invoke-“, “Out-”, “Write-“ and all PowerShell arguments can be shortened like “iex”, “ex”, etc so be careful and look for these too. Then filter out your normal modules and look for malicious ones such as:

** Set-ExecutionPolicy, Set-MasterBootRecord

** Get-WMIObject, Get-GPPPassword, Get-Keystrokes, Get-TimedScreenshot, Get-VaultCredential, Get-ServiceUnquoted, Get-ServiceEXEPerms, Get-ServicePerms, Get-RegAlwaysInstallElevated, Get-RegAutoLogon, Get-UnattendedInstallFiles, Get-Webconfig, Get-ApplicationHost, Get-PassHashes, Get-LsaSecret, Get-Information, Get-PSADForestInfo, Get-KerberosPolicy, Get-PSADForestKRBTGTInfo, Get-PSADForestInfo, Get-KerberosPolicy

** Invoke-Command, Invoke-Expression, iex, Invoke-Shellcode, Invoke--Shellcode, Invoke-ShellcodeMSIL, Invoke-MimikatzWDigestDowngrade, Invoke-NinjaCopy, Invoke-CredentialInjection, Invoke-TokenManipulation, Invoke-CallbackIEX, Invoke-PSInject, Invoke-DllEncode, Invoke-ServiceUserAdd, Invoke-ServiceCMD, Invoke-ServiceStart, Invoke-ServiceStop, Invoke-ServiceEnable, Invoke-ServiceDisable, Invoke-FindDLLHijack, Invoke-FindPathHijack, Invoke-AllChecks, Invoke-MassCommand, Invoke-MassMimikatz, Invoke-MassSearch, Invoke-MassTemplate, Invoke-MassTokens, Invoke-ADSBackdoor, Invoke-CredentialsPhish, Invoke-BruteForce, Invoke-PowerShellIcmp, Invoke-PowerShellUdp, Invoke-PsGcatAgent, Invoke-PoshRatHttps, Invoke-PowerShellTcp, Invoke-PoshRatHttp, Invoke-PowerShellWmi, Invoke-PSGcat, Invoke-Encode, Invoke-Decode, Invoke-CreateCertificate, Invoke-NetworkRelay

** EncodedCommand, New-ElevatedPersistenceOption, wsman, Enter-PSSession, DownloadString, DownloadFile

** Out-Word, Out-Excel, Out-Java, Out-Shortcut, Out-CHM, Out-HTA, Out-Minidump, HTTP-Backdoor, Find-AVSignature, DllInjection, ReflectivePEInjection, Base64, System.Reflection, System.Management

** Restore-ServiceEXE, Add-ScrnSaveBackdoor, Gupt-Backdoor, Execute-OnTime, DNS_TXT_Pwnage, Write-UserAddServiceBinary, Write-CMDServiceBinary, Write-UserAddMSI, Write-ServiceEXE, Write-ServiceEXECMD

** Enable-DuplicateToken , Remove-Update, Execute-DNSTXT-Code, Download-Execute-PS, Execute-Command- SSQL, Download_Execute, Copy-VSS, Check-VM, Create-MultipleSessions, Run-EXEonRemote, Port-Scan, Remove-PoshRat, TexttoEXE, Base64ToString, StringtoBase64, Do-Exfiltration, Parse_Keys, Add-Exfiltration, Add-Persistence, Remove-Persistence, Find-PSServiceAccounts, Discover-PSMSSQLServers,

Discover-PSMSExchangeServers, Discover-PSInterestingServices, Discover-PSMSExchangeServers, Discover-PSInterestingServices

** Mimikatz, powercat, powersploit, PowershellEmpire, Payload, GetProcAddress

** And any other commands found in any PowerShell exploit kits