**Windows Forensic Investigation Notes**

**System Information**

Computername:   
Registry: HKLM\System\CurrentControlSet\Control\Computername\

Windows Version:   
Registry: HKLM\Software\Microsoft\Windows NT\Currentversion\

Timezone:  
Registry: HKLM\System\CurrentControlSet\Control\TimeZoneInformation\

Network Information:   
Registry: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{interface-name}

Shutdown time:   
Registry: HKLM\System\ControlSet001\Control\Windows\ShutdownTime

Defender settings:  
Registry: HKLM\Software\Microsoft\Windows Defender\

**Users, Groups and User Profiles**

Active accounts during the attack timeframe?

Which account(s) were created?

Which accounts are Administrator group members?

Which users have profiles?

**User Behavior**

UserAssist: Applications opened ( NTUSER)

RecentDocs: Files and folders opened (NTUSER.dat\Software\Microsoft\WindowsCurrentVersion\Explorer\RecentDocs

Shellbags: Locations browsed by the user -- userclass.dat  
Open / Save MRU: Files that were opened  
Last-Visited MRU: Applications used to open files

**NTFS - File System Analysis**

MFT

USN Journal - $Extend\$J ( usnjrnl -- $max $j ) parce $j through mftecmd

**Execution Artifacts**

**Background Activity Moderator (BAM)**Registry*: HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings*

Which executables (.exe files) did the BAM record for the IEUser (RID 1000) incl. their last execution date and time?

**Application Compatibility Cache ("AppCompatCache") / Shimcache**  
Registry: *SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache*

To determine whether the executable executed or not , or to prove the existancce of a exe

**AmCache**  
Registry: *C:\Windows\AppCompat\Programs\Amcache.hve*

Amcacheparcer

**Prefetch**  
Path: *C:\Windows\Prefetch\\*.pf*

*PECmd*

**Shortcut (LNK) Files**Path:*C:\users\<username>\AppData\Roaming\Microsoft\Windows\Recent*Path*: C:\users\<username>\AppData\Roaming\Microsoft\Office\Recent*

**Persistence Mechanisms**

**Auto-Run Keys**Registry*:   
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce  
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce*

**Startup Folder**Paths:  
*C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup  
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp*

**Windows Services**  
Registry: *HKLM\SYSTEM\CurrentControlSet\Services*

**Scheduled Tasks**Registry:   
*HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks  
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree*

Path:  
*C:\Windows\System32\Tasks*

**Windows Event Log Analysis**

Path: *C:\Windows\System32\winevt\logs*

**Source Event IDs Description**

Microsoft-Windows-Windows Defender 5000 Defender enabled  
 5001 Defender disabled

System 7045 A new service was installed

Security 4624 An account was successfully logged on

Windows PowerShell 400 Engine state is changed from None to Available

Microsoft-Windows-Sysmon 1 Process creation  
 3 Network connection  
 11 File create  
 12, 13 Registry events  
 22 DNS query

**Memory Analysis**

with Volatility3

**Important memory related artifacts:**

Memory (volatile data)  
hiberfil.sys  
pagefile.sys  
swapfile.sys

PID of suspicious processes?

powershell.exe <PID>  
notepad.exe <PID>  
AtomicService.exe <PID>

Suspicious registry key in HKCU?