**PWF - Investigation #001**

*Disclaimer: This template has been provided by Blue Cape Security, LLC through the Practical Windows Forensic (PWF) course. The purpose is to guide the student through the course and the process of performing digital forensic analysis of various Windows artifacts. It does not represent an actual template of a forensic report.*

**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  
RecentDocs: Files and folders opened  
Shellbags: Locations browsed by the user  
Open / Save MRU: Files that were opened  
Last-Visited MRU: Applications used to open files

**NTFS - File System Analysis**

Which files are located in My Computer\CLSID\_Desktop\PWF-main\PWF-main\AtomicRedTeam?

What is the MFT Entry Number for the file "ART-attack.ps1"?

What are the MACB timestamps for "ART-attack.ps1"?

Was "ART-attack.ps1" timestomped?

When was the file "deleteme\_T1551.004" created and deleted?

What was the Entry number for "deleteme\_T1551.004" and does it still exist in the MFT?

**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*

Determine the cache entry position for:

* AtomicService.exe:
* mavinject.exe:

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

What SHA-1 hash did Amcache record for AtomicService.exe?

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

Use the Prefetch-Timeline output to produce a timeline of suspicious execution events in the Eric Zimmerman Timeline Explorer:  
*POWERSHELL.exe  
cmd.exe  
NET.exe  
REG.exe  
SCHTASKS.exe  
SC.exe  
ATOMICSERVICE.EXE  
MAVINJECT.exe  
NOTEPAD.exe*

**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*

What is the full path of the AtomicService.exe that was added to the run keys?

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

What is the name of the suspicious script in the StartUp folder?

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

When was the suspicious atomic service installed?

**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*

Which tasks were created by the IEUser and what's the creation time?

How many times did they execute?

**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?