**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: **DESKTOP-ODLQEI9**  
Registry: HKLM\System\CurrentControlSet\Control\Computername\

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

**ProductName Windows 10 Enterprise Evaluation**

**ReleaseID 2009**

**BuildLab 19041.vb\_release.191206-1406**

**BuildLabEx 19041.1.amd64fre.vb\_release.191206-1406**

**CompositionEditionID EnterpriseEval**

**RegisteredOrganization**

**RegisteredOwner IEUser**

**UBR 2006**

**InstallDate 2023-10-23 22:05:23Z**

**InstallTime 2023-10-23 22:05:23Z**

**UBR 2006**

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

**Pacific Standard Time**

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

**DhcpIPAddress 10.0.2.15**

**DhcpSubnetMask 255.255.255.0**

**DhcpServer 10.0.2.2**

**DhcpNameServer 192.168.0.1**

**DhcpDefaultGateway 10.0.2.2**

**DhcpSubnetMaskOpt 255.255.255.0**

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

**ShutdownTime : 2023-10-24 02:22:10Z**

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

**Key path: Microsoft\Windows Defender\Real-Time Protection**

**LastWrite Time: 2023-10-23 23:11:04Z**

**DisableRealtimeMonitoring value = 1**

**Users, Groups and User Profiles**

Active accounts during the attack timeframe?

**Username : IEUser [1001]**

SID : S-1-5-21-781923729-2736753865-2647957202-1001

Account Type :

Account Created : Mon Oct 23 22:14:30 2023

Name :

Last Login Date : Mon Oct 23 23:07:47 2023 Z

Pwd Reset Date : Mon Oct 23 22:14:31 2023 Z

Pwd Fail Date : Never

Login Count : 5

--> Password does not expire

--> Normal user account

Which account(s) were created?

**Username : art-test [1002]**

Account Created : Mon Oct 23 23:27:06 2023 Z

Which accounts are Administrator group members?

**Username : IEUser [1001]**

**Username : art-test [1002]**

Which users have profiles?

**Path : C:\Users\IEUser**

**SID : S-1-5-21-781923729-2736753865-2647957202-1001**

**LastWrite : 2023-10-24 02:21:35Z**

**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

**UserAssist:**

NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA} - A list of applications, files, links, and other objects that have been accessed.

{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F} – List the shortcut links used to start programs 2023-10-23 23:13:53Z.

**Microsoft.Windows.Explorer (6)**

**{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WindowsPowerShell\v1.0\powershell.exe**

**{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe**

**{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe**

**RecentDocs:**

**NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**

**N/A**

**ShellBags:**

**NTUSER.DAT:**

**HKCU\ Software\Microsoft\Windows\Shell\BagMRU**

**HKCU\ Software\Microsoft\Windows\Shell\Bags**

**USRCLASS.DAT:**

**Local Settings\Software\Microsoft\Windows\Shell\BagMRU**

**\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags**

**MRU Resource**

**2023-10-23 23:16:55 PWF-main\PWF-main [Desktop\3\0\]**

**2023-10-23 23:19:50 PWF-main [Desktop\3\]**

**2023-10-23 23:19:50 PWF-main\PWF-main\Install-Sysmon [Desktop\3\0\0\]**

**2023-10-23 23:19:50 PWF-main\PWF-main\AtomicRedTeam [Desktop\3\0\1\]**

**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?