

PWF - Investigation #001

System Information

Computername:

Registry: HKLM\System\CurrentControlSet\Control\Computename\

MSEdgeWin10

Windows Version:

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

ProductName	Windows 10 Enterprise Evaluation
ReleaseID	1809
BuildLab	17763.rs5_release.180914-1434
BuildLabEx	17763.1.amd64fre.rs5_release.180914-1434
CompositionEditionID	EnterpriseEval
RegisteredOrganization	Microsoft
RegisteredOwner	
InstallDate	2019-03-19 12:59:35Z
InstallTime	2019-03-19 12:59:35Z

Timezone:

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

SE Asia Standard Time

Network Information:

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

DhcpIPAddress	192.168.128.142
----------------------	------------------------

DhcpSubnetMask	255.255.255.0
DhcpServer	192.168.128.254
DhcpNameServer	192.168.128.2
DhcpDefaultGateway	192.168.128.2
DhcpSubnetMaskOpt	255.255.255.0

Shutdown time:

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

ShutdownTime	: 2022-07-24 16:45:17Z
---------------------	-------------------------------

Defender settings:

Registry: HKLM\Software\Microsoft\Windows Defender\

Key path:	Microsoft\Windows Defender\Real-Time Protection
LastWrite Time:	2022-07-24 15:27:02Z
DisableRealtimeMonitoring value	= 0

Users, Groups and User Profiles

Active accounts during the attack timeframe?

Username	: IEUser [1000]
Full Name	: IEUser
User Comment	: IEUser
Account Type	:
Account Created	: 2019-03-19 20:57:23Z
Name	:
Last Login Date	: 2022-07-24 15:15:57Z
Pwd Reset Date	: 2019-03-19 20:57:23Z
Pwd Fail Date	: Never

```
Login Count      : 15
Embedded RID     : 1000
--> Password does not expire
--> Normal user account
```

Which account(s) were created?

```
Username         : art-test [1003]
Account Created  : 2022-07-24 15:22:25Z
```

Which accounts are Administrator group members?

```
IEUser [1000]
art-test [1003]
```

Which users have profiles?

```
Path            : C:\Users\IEUser
SID             : S-1-5-21-321011808-3761883066-353627080-1000
LastWrite       : 2022-07-24 16:45:11Z
```

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.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

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

2022-07-24 15:17:20Z

Microsoft.Windows.Explorer (8)

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

{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\oobe\FirstLogonAnim.exe

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

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

{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F} – Lists the shortcut links used to start programs

2022-07-24 15:10:52Z

{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\System Tools\Control Panel.lnk (2)

2019-03-19 12:58:30Z

{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk (9)

{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk (7)

{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Notepad.lnk (6)

RecentDocs:

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

Shellbags:

NTUSER.DAT

Software\Microsoft\Windows\Shell\BagMRU

Software\Microsoft\Windows\Shell\Bags

USRCLASS.DAT

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

MRU Time	Resource
2022-07-24 15:17:13	My Computer\CLSID_Desktop [Desktop\1\0\]

```
PWF-main.zip [361431] [Desktop\2\]  
2022-07-24 15:17:59 PWF-main [Desktop\3\]
```

NTFS - File System Analysis

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

```
ART-attack-cleanup.ps1  
ART-attack.ps1  
PWF_Analysis-MITRE.png  
PWF_Analysis-MITRE.svg
```

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

```
124544
```

**** STANDARD INFO ****

```
Created On:          2022-07-11 07:45:32.0000000  
Modified On:         2022-07-11 07:45:32.0000000  
Record Modified On: 2022-07-24 15:17:09.6067768  
Last Accessed On:   2022-07-24 15:20:46.7647322
```

**** FILE NAME ****

```
File name: ART-attack.ps1  
Created On:          2022-07-24 15:17:09.5943660  
Modified On:         2022-07-24 15:17:09.5943660  
Record Modified On: 2022-07-24 15:17:09.5943660
```

Last Accessed On: 2022-07-24 15:17:09.5943660

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

⇒ Using **** STANDARD INFO ****

Modified	m...	2022-07-11 07:45:32.0000000	
Accessed	.a...	2022-07-24 15:20:46.7647322	
Changed (\$MFT)	..c.	2022-07-24 15:17:09.6067768	(Record Modified On)
Birth (Creation)	...b	2022-07-11 07:45:32.0000000	

Was "ART-attack.ps1" timestomped?

Using TimelineExplorer and check in colume: SI<SN

Hoặc cách khác là kiểm tra timestamp ở 2 phần **Standard info** và **File name** có sự chênh lệch

Yes

When was the file "deleteme_T1551.004" created and deleted?

2022-07-24 15:25:24 - FileCreate
2022-07-24 15:25:29 - FileDelete

What was the Entry number for "deleteme_T1551.004" and does it still exist in the MFT?

1976 (Entry number)
Yes (Overwritten)

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?

S-1-5-21-321011808-3761883066-353627080-1000

```
2022-07-24 16:45:10Z - Microsoft.Windows.ShellExperienceHost_cw5nlh2txyewy
2022-07-24 16:45:10Z - Microsoft.Windows.Cortana_cw5nlh2txyewy
2022-07-24 16:45:10Z - Microsoft.MicrosoftEdge_8wekyb3d8bbwe
2022-07-24 16:45:10Z - Microsoft.WindowsStore_8wekyb3d8bbwe
2022-07-24 15:14:07Z - windows.immersivecontrolpanel_cw5nlh2txyewy
2022-07-24 16:45:10Z - 
\Device\HarddiskVolume1\Windows\System32\ApplicationFrameHost.exe
2022-07-24 16:45:10Z - \Device\HarddiskVolume1\Windows\explorer.exe
2022-07-24 16:45:08Z - \Device\HarddiskVolume1\Program Files\VMware\VMware
Tools\vmtoolsd.exe
2022-07-24 16:45:06Z - \Device\HarddiskVolume1\Windows\System32\rundll32.exe
2022-07-24 15:22:43Z - \Device\HarddiskVolume1\Windows\System32\cmd.exe
2022-07-24 15:20:38Z - Microsoft.Windows.SecHealthUI_cw5nlh2txyewy
2022-07-24 16:45:09Z - InputApp_cw5nlh2txyewy
2022-07-24 16:45:06Z - 
\Device\HarddiskVolume1\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
2022-07-24 16:45:06Z - \Device\HarddiskVolume1\Windows\System32\notepad.exe
```

Application Compatibility Cache ("AppCompatCache") / Shimcache

Registry: *SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache*

Determine the cache entry position for:

- AtomicService.exe: 46
- mavinject.exe: 45

Line	Tag	Control_	Duplicate	Cache Entry Position	Executed	Last Modified Time	Path	Source File
46		1		45 NA	2018-09-15 09:09:53	C:\Windows\system32\mavinject.exe	D:\Cases\Analysis\Registry\SYSTEM	
47		1		46 NA	2022-04-27 11:14:48	C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe	D:\Cases\Analysis\Registry\SYSTEM	

AmCache

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

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

c51217ce3d1959e99886a567d21d0b97022bd6e3

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

Line	T...	Run Time	Executable Name
=	✓	=	🔍
58	✓	2022-07-24 15:11:07	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\CMD.EXE
59	✓	2022-07-24 15:11:07	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\CMD.EXE
60	✓	2022-07-24 15:11:07	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\CMD.EXE
57	✓	2022-07-24 15:11:08	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\CMD.EXE
56	✓	2022-07-24 15:16:17	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\CMD.EXE
316	✓	2022-07-24 15:18:39	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\1.0\POWERSHELL.EXE
415	✓	2022-07-24 15:19:06	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\SC.EXE
315	✓	2022-07-24 15:22:18	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\1.0\POWERSHELL.EXE
55	✓	2022-07-24 15:22:25	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\CMD.EXE
266	✓	2022-07-24 15:22:25	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\NET.EXE
267	✓	2022-07-24 15:22:25	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\NET.EXE
268	✓	2022-07-24 15:22:25	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\NET.EXE
314	✓	2022-07-24 15:22:28	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\1.0\POWERSHELL.EXE
326	✓	2022-07-24 15:22:30	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\REG.EXE
416	✓	2022-07-24 15:22:40	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\SCHTASKS.EXE
417	✓	2022-07-24 15:22:40	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\SCHTASKS.EXE
18	✓	2022-07-24 15:22:43	\VOLUME{01d4de9e09d44c1a-b009e7a9}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50CDD341815D5D2F34CBF90168017404\ATOMICS\T1543.003\BIN\ATOMICSERVICE.EXE
413	✓	2022-07-24 15:22:43	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\SC.EXE
414	✓	2022-07-24 15:22:43	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\SC.EXE
199	✓	2022-07-24 15:22:47	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\MAVINJECT.EXE
296	✓	2022-07-24 15:22:47	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\NOTEPAD.EXE
313	✓	2022-07-24 15:25:20	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\1.0\POWERSHELL.EXE
54	✓	2022-07-24 15:35:55	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\CMD.EXE
53	✓	2022-07-24 16:45:00	\VOLUME{01d4de9e09d44c1a-b009e7a9}\WINDOWS\SYSTEM32\CMD.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?

C:\Path\AtomicRedTeam.exe

(NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run)

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?

batstartup.bat

Windows Services

Registry: *HKLM\SYSTEM\CurrentControlSet\Services*

When was the suspicious atomic service installed?

2022-07-24 15:22:43Z

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?

T1053_005_OnLogon

LastWrite: 2022-07-24 15:22:40Z

Id: {8B42D2C0-80F7-476B-BF26-AAD439F3FDEC}

Task Reg Time: 2022-07-24 15:22:40Z

T1053_005_OnStartup

LastWrite: 2022-07-24 15:22:40Z

Id: {A5BF28A7-FC21-47B9-BE18-86C6B7E7E139}

Task Reg Time: 2022-07-24 15:22:40Z





How many times did they execute?

Never (Last start: N/A, Last stop: N/A)

Windows Event Log Analysis





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

Source	Event IDs	Description
Microsoft-Windows-Windows Defender	5000	Defender enabled
	5001	Defender disabled

Type	Date	Time	Event	Source	Category	User	Computer
 Information	24/7/2022	10:27:08 PM	5000	Microsoft-Windows-Windows Defender	None	\SYSTEM	MSEDGEWIN10
 Information	24/7/2022	10:16:44 PM	5001	Microsoft-Windows-Windows Defender	None	\SYSTEM	MSEDGEWIN10
 Information	24/7/2022	10:16:28 PM	5000	Microsoft-Windows-Windows Defender	None	\SYSTEM	MSEDGEWIN10
 Information	24/7/2022	10:14:48 PM	5001	Microsoft-Windows-Windows Defender	None	\SYSTEM	MSEDGEWIN10

Description

Windows Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was enabled.

Type	Date	Time	Event	Source	Category	User	Computer
 Information	24/7/2022	10:27:08 PM	5000	Microsoft-Windows-Windows Defender	None	\SYSTEM	MSEDGEWIN10
 Information	24/7/2022	10:16:44 PM	5001	Microsoft-Windows-Windows Defender	None	\SYSTEM	MSEDGEWIN10
 Information	24/7/2022	10:16:28 PM	5000	Microsoft-Windows-Windows Defender	None	\SYSTEM	MSEDGEWIN10
 Information	24/7/2022	10:14:48 PM	5001	Microsoft-Windows-Windows Defender	None	\SYSTEM	MSEDGEWIN10

Description

Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.

System	7045	A new service was installed
--------	------	-----------------------------

Type	Date	Time	Event	Source	Category	User	Computer
Information	24/7/2022	10:22:43 PM	7045	Service Control Manager	None	\S-1-5-21-321011808-3761883066-353627080-1000	MSEDGEWIN10
Information	24/7/2022	10:19:05 PM	7045	Service Control Manager	None	\S-1-5-21-321011808-3761883066-353627080-1000	MSEDGEWIN10
Information	24/7/2022	10:19:05 PM	7045	Service Control Manager	None	\S-1-5-21-321011808-3761883066-353627080-1000	MSEDGEWIN10
Information	25/7/2022	12:09:18 PM	7045	Service Control Manager	None	\SYSTEM	MSEDGEWIN10

Description

A service was installed in the system.

Service Name: AtomicTestService_CMD
Service File Name: C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Type	Date	Time	Event	Source	Category	User	Computer
Information	24/7/2022	10:22:43 PM	7045	Service Control Manager	None	\S-1-5-21-321011808-3761883066-353627080-1000	MSEDGEWIN10
Information	24/7/2022	10:19:05 PM	7045	Service Control Manager	None	\S-1-5-21-321011808-3761883066-353627080-1000	MSEDGEWIN10
Information	24/7/2022	10:19:05 PM	7045	Service Control Manager	None	\S-1-5-21-321011808-3761883066-353627080-1000	MSEDGEWIN10
Information	25/7/2022	12:09:18 PM	7045	Service Control Manager	None	\SYSTEM	MSEDGEWIN10

Description

A service was installed in the system.

Service Name: Sysmon
Service File Name: C:\Windows\Sysmon.exe
Service Type: user mode service
Service Start Type: auto start
Service Account: LocalSystem

Security

4624

An account was successfully
logged on

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	24/7/2022	10:15:57 PM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:15:57 PM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:15:45 PM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	MSEDGEWIN10

Description

An account was successfully logged on.

Subject:

Security ID: S-1-5-18
Account Name: MSEDGEWIN10\$
Account Domain: WORKGROUP
Logon ID: 0x3e7

Logon Information:

Logon Type: 2
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: No

Impersonation Level:

Impersonation

New Logon:

Security ID: S-1-5-21-321011808-3761883066-353627080-1000
Account Name: IEUser
Account Domain: MSEDGEWIN10
Logon ID: 0x548ae
Linked Logon ID: 0x5488b
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	24/7/2022	10:22:25 PM	4732	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4724	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4738	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4798	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4732	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4738	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4722	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4720	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4728	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:15:45 PM	4672	Microsoft-Windows-Security-Auditing	Special Logon	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:15:45 PM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:15:45 PM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	MSEDGEWIN10

Description

Special privileges assigned to new logon.

Subject:

Security ID: S-1-5-21-321011808-3761883066-353627080-1000
Account Name: IEUser
Account Domain: MSEDGEWIN10
Logon ID: 0x25f78

Privileges:

SeSecurityPrivilege
SeTakeOwnershipPrivilege
SeLoadDriverPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeDebugPrivilege
SeSystemEnvironmentPrivilege
SeImpersonatePrivilege
SeDelegateSessionUserImpersonatePrivilege

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	24/7/2022	10:22:25 PM	4732	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4724	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4738	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4798	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4732	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4738	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4722	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4720	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4728	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:15:45 PM	4672	Microsoft-Windows-Security-Auditing	Special Logon	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:15:45 PM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:15:45 PM	4624	Microsoft-Windows-Security-Auditing	Logon	N/A	MSEDGEWIN10

Description

A member was added to a security-enabled global group.

Subject:

Security ID: S-1-5-21-321011808-3761883066-353627080-1000
Account Name: IEUser
Account Domain: MSEDGEWIN10
Logon ID: 0x25f78

Member:

Security ID: S-1-5-21-321011808-3761883066-353627080-1003
Account Name: -

Group:

Security ID: S-1-5-21-321011808-3761883066-353627080-513
Group Name: None
Group Domain: MSEDGEWIN10

Additional Information:

Privileges: -

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	24/7/2022	10:22:25 PM	4732	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4724	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4738	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4798	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4732	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4738	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4722	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4720	Microsoft-Windows-Security-Auditing	User Account Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:22:25 PM	4728	Microsoft-Windows-Security-Auditing	Security Group Management	N/A	MSEDGEWIN10
Audit Success	24/7/2022	10:15:45 PM	4672	Microsoft-Windows-Security-Auditing	Special Logon	N/A	MSEDGEWIN10

Description

A user account was created.

Subject:

Security ID: S-1-5-21-321011808-3761883066-353627080-1000
Account Name: IEUser
Account Domain: MSEDGEWIN10
Logon ID: 0x25f78

New Account:

Security ID: S-1-5-21-321011808-3761883066-353627080-1003
Account Name: art-test
Account Domain: MSEDGEWIN10

Attributes:

SAM Account Name: art-test
Display Name: <value not set>
User Principal Name: -
Home Directory: <value not set>
Home Drive: <value not set>
Script Path: <value not set>
Profile Path: <value not set>
User Workstations: <value not set>
Password Last Set: <never>
Account Expires: <never>
Primary Group ID: 513
Allowed To Delegate To: -
Old UAC Value: 0x0
New UAC Value: 0x15
User Account Control:
Account Disabled
'Password Not Required' - Enabled
'Normal Account' - Enabled
User Parameters: <value not set>
SID History: -
Logon Hours: All

Windows PowerShell

400

Engine state is changed from
None to Available

Type	Date	Time	Event	Source	Category	User	Computer
Information	24/7/2022	10:22:37 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEWIN10
Information	24/7/2022	10:22:29 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEWIN10
Information	24/7/2022	10:22:19 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEWIN10
Information	24/7/2022	10:21:38 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEWIN10
Information	24/7/2022	10:21:17 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEWIN10

Description

Engine state is changed from None to Available.

Details:

NewEngineState=Available
PreviousEngineState=None

SequenceNumber=13

HostName=ConsoleHost
HostVersion=5.1.17763.316
HostId=cbe24744-9e1f-4e30-b622-a5b81bc798ee

HostApplication=powershell.exe & { \$url = 'https://github.com/redcanaryco/atomic-red-team/raw/master/atomics/T1566.001/bin/PhishingAttachment.xlsm'
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
Invoke-WebRequest -Uri \$url -OutFile \$env:TEMP\PhishingAttachment.xlsm'
EngineVersion=5.1.17763.316
RunspaceId=8b6af2ed-0721-49cb-a19b-6aca54588ece
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=

Type	Date	Time	Event	Source	Category	User	Computer
Information	24/7/2022	10:22:37 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEWIN10
Information	24/7/2022	10:22:29 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEWIN10
Information	24/7/2022	10:22:19 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEWIN10
Information	24/7/2022	10:21:38 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEWIN10
Information	24/7/2022	10:21:17 PM	400	PowerShell	Engine Lifecycle	N/A	MSEDGEWIN10

Description

Engine state is changed from None to Available.

Details:

```
NewEngineState=Available  
PreviousEngineState=None  
  
SequenceNumber=13  
  
HostName=ConsoleHost  
HostVersion=5.1.17763.316  
HostId=cfcc0e8c-8e2d-4d20-925d-5080b8173773d  
HostApplication=powershell.exe & (# Encoded payload in next command is the following "Set-Content -path $env:SystemRoot\Temp\art-marker.txt -value "Hello from the Atomic Red Team""  
reg.exe add "HKLM\CURRENT_USER\Software\Classes\AtomicRedTeam" /v Art /t REG_SZ /d "http://www.atomicredteam.com/Tools/GcgVgUmqwvc9Uzr1Wl2Fydc1YXZr2udHh0IiAtdmfDsdWUqIkhbGxvIGZyb2QgdGhlIEF0b2lpYyBSZWQvGVhbS1="  
ie.exe ([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String((go HKCU\Software\Classes\AtomicRedTeam\Art))))  
  
EngineSpaceId=5.1.17763.316  
RunspaceId=a2a3e8006-7f5e-4bae-9f8d-b6cae7fe2ed1  
PipelineId=  
CommandName=  
CommandType=  
ScriptName=  
CommandPath=  
CommandLine=  
  
Administrator: Windows Power x [ ] - x + v  
PS C:\> echo "U2V0LUNvbmlRbnQgLXBhdGggIiRlbnY6U3lzdGVtUm9mdC9UZw1wL2FydC1tYXJrZXIudHh0IiAtdmfDsdWUqIkhbGxvIGZyb2QgdGhlIEF0b2lpYyBSZWQvGVhbS1=" | base64 -d  
Set-Content -path "$env:SystemRoot\Temp\art-marker.txt" -value "Hello from the Atomic Red Team"
```

Type	Date	Time	Event	Source	Category	User	Computer
Information	24/7/2022	10:25:20 PM	400	PowerShell	Engine Lifecycle	N/A	MSEdgeWIN10
Information	24/7/2022	10:22:46 PM	400	PowerShell	Engine Lifecycle	N/A	MSEdgeWIN10
Information	24/7/2022	10:22:37 PM	400	PowerShell	Engine Lifecycle	N/A	MSEdgeWIN10
Information	24/7/2022	10:22:29 PM	400	PowerShell	Engine Lifecycle	N/A	MSEdgeWIN10
Information	24/7/2022	10:22:19 PM	400	PowerShell	Engine Lifecycle	N/A	MSEdgeWIN10

Description

Engine state is changed from None to Available.

Details:

```

NewEngineState=Available
PreviousEngineState=None

SequenceNumber=13

HostName=ConsoleHost
HostVersion=5.1.17763.316
HostId=d0a9e876-9e79-4e0f-ac66-54f62417737a
HostApplication=powershell.exe & {$mypid = (Start-Process notepad -PassThru).Id
mavinject $mypid /INJECTRUNNING C:\AtomicRedTeam\atomics\T1055.001[src\x64\T1055.001.dll]
EngineVersion=5.1.17763.316
RunspaceId=37454b73-8341-4670-9642-12d06681e3f4
PipelineId=

```

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

Type	Date	Time	Event	Source	Category	User	Computer
Information	24/7/2022	10:22:47 PM	1	Microsoft-Windows-Sysmon	(1)	\SYSTEM	MSEDGEWIN10
Information	24/7/2022	10:22:47 PM	1	Microsoft-Windows-Sysmon	(1)	\SYSTEM	MSEDGEWIN10
Information	24/7/2022	10:22:45 PM	1	Microsoft-Windows-Sysmon	(1)	\SYSTEM	MSEDGEWIN10

Description

The description for Event ID (1) in Source (Microsoft-Windows-Sysmon) could not be found. Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event:

```
-
2022-07-24 15:22:47.751
{43199d79-63c7-62dd-4701-00000000e00}
5052
C:\Windows\System32\mavinject.exe
10.0.17763.1 (WinBuild.160101.0800)
Microsoft Application Virtualization Injector
Microsoft® Windows® Operating System
Microsoft Corporation
mavinject64.exe
"C:\Windows\system32\mavinject.exe" 6456 /INJECTRUNNING C:\AtomicRedTeam\atomic\T1055.001\src\x64\T1055.001.dll
C:\Users\IEUser\AppData\Local\Temp\
MSEDGEWIN10\IEUser
{43199d79-6221-62dd-785f-020000000000}
0x25f78
1
High
MD5=72D5E2A3FF5D88C891E0DF1AA28B6422,SHA256=ABB99F7CFD3E9EB294501AFA082A8D4841278CC39A4FB3DFF9942CA1F71A139,IMPHASH=96A5873241D90136570C05E55F085B2A
{43199d79-63c5-62dd-4401-00000000e00}
5936
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
"powershell.exe" & {$mypid = (Start-Process notepad -PassThru).id
mavinject $mypid /INJECTRUNNING C:\AtomicRedTeam\atomic\T1055.001\src\x64\T1055.001.dll}
MSEDGEWIN10\IEUser
```

Type	Date	Time	Event	Source	Category	User	Computer
Information	24/7/2022	10:20:56 PM	22	Microsoft-Windows-Sysmon	(22)	\SYSTEM	MSEDGEWIN10
Information	24/7/2022	10:20:56 PM	3	Microsoft-Windows-Sysmon	(3)	\SYSTEM	MSEDGEWIN10
Information	24/7/2022	10:20:49 PM	3	Microsoft-Windows-Sysmon	(3)	\SYSTEM	MSEDGEWIN10
Information	24/7/2022	10:20:49 PM	22	Microsoft-Windows-Sysmon	(22)	\SYSTEM	MSEDGEWIN10
Information	24/7/2022	10:20:49 PM	3	Microsoft-Windows-Sysmon	(3)	\SYSTEM	MSEDGEWIN10
Information	24/7/2022	10:20:48 PM	3	Microsoft-Windows-Sysmon	(3)	\SYSTEM	MSEDGEWIN10
Information	24/7/2022	10:20:48 PM	22	Microsoft-Windows-Sysmon	(22)	\SYSTEM	MSEDGEWIN10
Information	24/7/2022	10:20:48 PM	22	Microsoft-Windows-Sysmon	(22)	\SYSTEM	MSEDGEWIN10

Description

The description for Event ID (22) in Source (Microsoft-Windows-Sysmon) could not be found. Either the component that raises this event is not installed on the computer or the installation is corrupted.You can install or repair the component or try to change Description Server.

The following information was included with the event:

```
-
2022-07-24 15:20:46.889
{43199d79-62cf-62dd-c800-00000000e00}
3488
raw.githubusercontent.com
0
::ffff:185.199.108.133::ffff:185.199.109.133::ffff:185.199.110.133::ffff:185.199.111.133;
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
MSEDGEWIN10\IEUser
```

Memory Analysis

with Volatility3

Important memory related artifacts:

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

PID of suspicious processes?

<code>powershell.exe</code>	3488
<code>notepad.exe</code>	6456
<code>AtomicService.exe</code>	4932

Suspicious registry key in HKCU?