



Name: Arsalan, Mihad, Atique, Faheem Azam, Ahmad

Class: BS-DFCS

Section: A

Roll no: 002, 004, 018, 021, 027

Assignment submitted to

MS. Fatima

Forensic Artifacts of Active Directory Scenerio

```
DSUSERS_out.txt - Notepad
File Edit Format View Help
Bad password time 2022-02-09 08:11:01.275937+00:00
Logon count: 65535
Bad password count: 0
Dial-In access perm: Controlled by policy
User Account Control:
    NORMAL_ACCOUNT
    DONT_EXPIRE_PASSWORD
    TRUSTED_FOR_DELEGATION
Ancestors:
    $ROOT_OBJECT$, net, *****, ad, ServiceAccounts, SCOM Admin

Record ID: 13029
User name: SCOM Action Account
User principal name: OMAction@ad.*****.net
SAM Account name: OMAction
SAM Account type: SAM_NORMAL_USER_ACCOUNT
GUID: db6021a4-9f10-4a6a-9f63-fa1e572dd6f0
SID: S-1-5-21-2595053252-3331221587-625639084-31886
When created: 2011-12-26 12:04:57+00:00
When changed: 2023-01-11 04:02:28+00:00
Account expires: Never
Password last set: 2020-01-23 09:16:02.203508+00:00
Last logon: 2023-01-11 05:18:22.398667+00:00
Last logon timestamp: 2023-01-06 23:12:39.355945+00:00
Bad password time: Never
Logon count: 65535
Bad password count: -1
Dial-In access perm: Controlled by policy
User Account Control:
    NORMAL_ACCOUNT
    DONT_EXPIRE_PASSWORD
Ancestors:
    $ROOT_OBJECT$, net, *****, ad, ServiceAccounts, SCOM Action Account

Record ID: 13031
User name: Hassan Waheed
User principal name: HWaheed@*****.com
```

We can see **OMAction** user found in **NTDS.dit** file which is a action user that means it can be mapped to the local system or a domain user account

```
SOFTWARE.txt - Notepad
File Edit Format View Help

Classes\exefile\shell\open\command (Default) value: "%1" %*
LastWrite Time: 2013-08-22 15:40:42Z
Classes\Folder\shell\open\command (Default) value: %SystemRoot%\Explorer.exe
LastWrite Time: 2013-08-22 15:40:42Z
Classes\mscfile\shell\open\command (Default) value: %SystemRoot%\system32\mmc.exe "%1" %*
LastWrite Time: 2013-08-22 15:40:43Z
Classes\exefile\shell\runas\command (Default) value: "%1" %*
Classes\exefile\shell\runas\command IsolatedCommand value: "%1" %*
-----
uninstall v.20200525
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT hives

Uninstall
Microsoft\Windows\CurrentVersion\Uninstall

2023-01-09 02:07:37Z
System Center Endpoint Protection v.4.10.209.0

2023-01-09 02:07:36Z
Microsoft Forefront Endpoint Protection 2010 Server Management v.4.10.0209.0

2023-01-09 02:07:35Z
Microsoft Endpoint Protection Management Components v.4.10.0209.0

2023-01-09 02:06:58Z
Microsoft Security Client v.4.10.0209.0

2022-08-18 06:43:40Z
Microsoft Silverlight v.5.1.50918.0

2022-06-17 06:36:41Z
Active Directory Management Pack Helper Object v.1.1.0

2022-06-17 06:36:39Z
Microsoft Monitoring Agent v.10.19.10014.0

Ln 31973, Col 1 100% Windows (CRLF) UTF-8
```

MS Endpoint Protection was uninstall showing an indicator to suspicious activity

```
SOFTWARE.txt - Notepad
File Edit Format View Help

Classes\mscfile\shell\open\command (Default) value: %SystemRoot%\system32\mmc.exe "%1" %*
LastWrite Time: 2013-08-22 15:40:43Z
Classes\exefile\shell\runas\command (Default) value: "%1" %*
Classes\exefile\shell\runas\command IsolatedCommand value: "%1" %*
-----
uninstall v.20200525
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT hives

Uninstall
Microsoft\Windows\CurrentVersion\Uninstall

2023-01-09 02:07:37Z
System Center Endpoint Protection v.4.10.209.0

2023-01-09 02:07:36Z
Microsoft Forefront Endpoint Protection 2010 Server Management v.4.10.0209.0

2023-01-09 02:07:35Z
Microsoft Endpoint Protection Management Components v.4.10.0209.0

2023-01-09 02:06:58Z
Microsoft Security Client v.4.10.0209.0

2022-08-18 06:43:40Z
Microsoft Silverlight v.5.1.50918.0

2022-06-17 06:36:41Z
Active Directory Management Pack Helper Object v.1.1.0

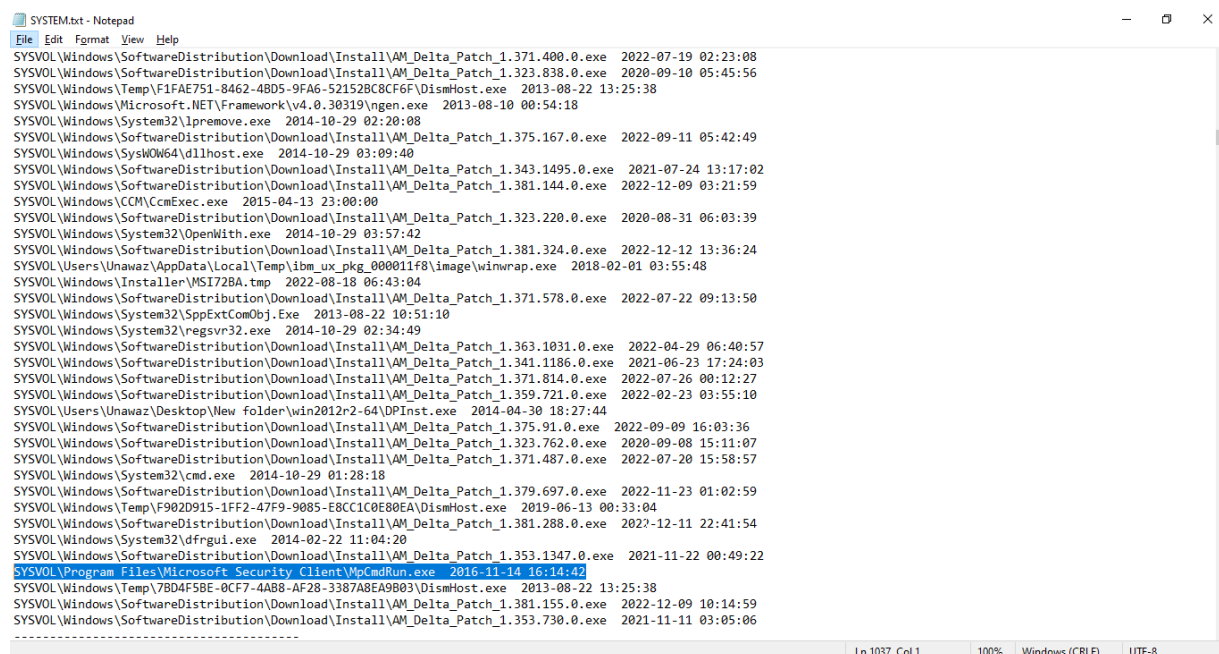
2022-06-17 06:36:39Z
Microsoft Monitoring Agent v.10.19.10014.0

2019-08-28 08:47:57Z
AddressBook
Connection Manager
DirectDrawEx
Fontcore

Ln 31970, Col 1 100% Windows (CRLF) UTF-8
```

At the same time MS forefront Endpoint was also uninstalled showing an indicated to potentially creating a window of

vulnerability.



```
SYSTEM.txt - Notepad
File Edit Format View Help
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.371.400.0.exe 2022-07-19 02:23:08
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.323.838.0.exe 2020-09-10 05:45:56
SYSVOL\Windows\Temp\F1FAE751-8462-4B05-9FA6-52152BC8CF6F\DisMHost.exe 2013-08-22 13:25:38
SYSVOL\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe 2013-08-10 00:54:18
SYSVOL\Windows\System32\ipremove.exe 2014-10-29 02:20:08
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.375.167.0.exe 2022-09-11 05:42:49
SYSVOL\Windows\System32\iprermove.exe 2014-10-29 03:09:40
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.343.1495.0.exe 2021-07-24 13:17:02
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.381.144.0.exe 2022-12-09 03:21:59
SYSVOL\Windows\CCM\CcmExec.exe 2015-04-13 23:00:00
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.323.220.0.exe 2020-08-31 06:03:39
SYSVOL\Windows\System32\OpenWith.exe 2014-10-29 03:57:42
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.381.324.0.exe 2022-12-12 13:36:24
SYSVOL\Users\Unawaz\AppData\Local\Temp\ibm_ux_pkg_000011f8\image\winwrap.exe 2018-02-01 03:55:48
SYSVOL\Windows\Installer\MSI72BA.tmp 2022-08-18 06:43:04
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.371.578.0.exe 2022-07-22 09:13:50
SYSVOL\Windows\System32\SppExtComObj.Exe 2013-08-22 10:51:10
SYSVOL\Windows\System32\regsvr32.exe 2014-10-29 02:34:49
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.363.1031.0.exe 2022-04-29 06:40:57
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.341.1186.0.exe 2021-06-23 17:24:03
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.371.814.0.exe 2022-07-26 00:12:27
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.359.721.0.exe 2022-02-23 03:55:10
SYSVOL\Users\Unawaz\Desktop\New folder\win2012r2-64\DPInst.exe 2014-04-30 18:27:44
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.375.91.0.exe 2022-09-09 16:03:36
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.323.762.0.exe 2020-09-08 15:11:07
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.371.487.0.exe 2022-07-20 15:58:57
SYSVOL\Windows\System32\cmd.exe 2014-10-29 01:28:18
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.379.697.0.exe 2022-11-23 01:02:59
SYSVOL\Windows\Temp\F902D915-1FF2-47F9-9085-E8CC1C0E80EA\DisMHost.exe 2019-06-13 00:33:04
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.381.288.0.exe 2022-12-11 22:41:54
SYSVOL\Windows\System32\dfmgrui.exe 2014-02-22 11:04:20
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.353.1347.0.exe 2021-11-22 00:49:22
SYSVOL\Program Files\Microsoft Security Client\MpCmdRun.exe 2016-11-14 16:14:42
SYSVOL\Windows\Temp\7BD4F5BE-0CF7-4AB8-AF28-3387A8EA9B03\DisMHost.exe 2013-08-22 13:25:38
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.381.155.0.exe 2022-12-09 10:14:59
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.353.730.0.exe 2021-11-11 03:05:06
Ln 1037, Col 1 100% Windows (CRLF) UTF-8
```

The file **MPCMDRun.exe** was found on the system. This executable is associated with Windows Defender and typically used for malware scanning. When a security application like Microsoft Defender is unregistered in the Windows Security Center (WSC), it means that Windows does not officially recognize it as the active antivirus program. This status could occur due to improper installation, corruption of the program, or intentional tampering by a malicious actor.

```
SOFTWARE.txt - Notepad
File Edit Format View Help
Classes\Folder\shell\open\command (Default) value: %SystemRoot%\Explorer.exe
LastWrite Time: 2013-08-22 15:40:42Z
Classes\mscfile\shell\open\command (Default) value: %SystemRoot%\system32\mmc.exe "%1" %*
LastWrite Time: 2013-08-22 15:40:43Z
Classes\exefile\shell\runas\command (Default) value: "%1" %*
Classes\exefile\shell\runas\command IsolatedCommand value: "%1" %*
-----
uninstall v.20200525
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT hives

Uninstall
Microsoft\Windows\CurrentVersion\Uninstall

2023-01-09 02:07:37Z
System Center Endpoint Protection v.4.10.209.0

2023-01-09 02:07:36Z
Microsoft Forefront Endpoint Protection 2010 Server Management v.4.10.0209.0

2023-01-09 02:07:35Z
Microsoft Endpoint Protection Management Components v.4.10.0209.0

2023-01-09 02:06:58Z
Microsoft Security Client v.4.10.0209.0

2022-08-18 06:43:40Z
Microsoft Silverlight v.5.1.50918.0

2022-06-17 06:36:41Z
Active Directory Management Pack Helper Object v.1.1.0

2022-06-17 06:36:39Z
Microsoft Monitoring Agent v.10.19.10014.0

2019-08-28 08:47:57Z
AddressBook
Connection Manager

Ln 31976, Col 1 100% Windows (CRLF) UTF-8
```

Again MS Security Client was uninstalled to create a vulnerable system so that system can be exploited easily

```
SOFTWARE.txt - Notepad
File Edit Format View Help
LastLoggedOnUser = AD\administrator
LastLoggedOnSAMUser = AD\administrator
LastLoggedOnUserSID = S-1-5-21-2595053252-3331221587-625639084-500
-----
licenses v.20200526
(Software) Get contents of HKLM\Software\Licenses key

Licenses not found.
-----
macaddr v.20200515
(System, Software) --

Microsoft\Windows Genuine Advantage not found.
-----
msis v.20200517
(Software) Determine MSI packages installed on the system

Classes\Installer\Products
LastWrite Time 2023-01-09 02:07:35Z

2023-01-09 02:07:36Z
Microsoft Forefront Endpoint Protection 2010 Server Management;d:\02bfa10a62ed60b7258d3e\amd64\FEPClient.msi
2023-01-09 02:07:35Z
Microsoft Endpoint Protection Management Components;d:\02bfa10a62ed60b7258d3e\amd64\EppManagement.msi
2023-01-09 02:06:58Z
Microsoft Security Client;d:\02bfa10a62ed60b7258d3e\amd64\lepp.msi
2022-08-18 06:43:41Z
Microsoft Silverlight;d:\df6137d3f98fad84a43608cbdc80e406\silverlight.msi
2022-06-17 06:36:39Z
Microsoft Monitoring Agent;C:\Windows\422C3AB1-32E0-4411-BF66-A84FEFCC8E2\WOMAgent.msi
2020-09-10 05:32:18Z
MegaRAID Storage Manager;C:\Users\Unawaz\Desktop\MegaRAID\MSM.msi
2020-09-10 05:21:11Z
Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.51106;C:\ProgramData\Package Cache\{6C772996-BFF3-3C8C-8608-B3D48FF05D65}\v11.0.51106\packages\vcRuntimeAdditional_x86\vc_runtimeAdditional_x86.msi
Microsoft Visual C++ 2012 x86 Minimum Runtime - 11.0.51106;C:\ProgramData\Package Cache\{E824E81C-80A4-3DFF-B5F9-4842A9FF5F7F}\v11.0.51106\packages

Ln 31169, Col 1 100% Windows (CRLF) UTF-8
```

```
SOFTWARE.txt - Notepad
File Edit Format View Help
LastWrite: 2023-02-06 09:56:31Z

LastLoggedOnUser = AD\Administrator
LastLoggedOnSAMUser = AD\Administrator
LastLoggedOnUserSID = S-1-5-21-2595053252-3331221587-625639084-500
-----
Licenses v.20200526
(Software) Get contents of HKLM/Software/Licenses key

Licenses not found.
-----
macaddr v.20200515
(System,Software) --

Microsoft\Windows Genuine Advantage not found.
-----
msis v.20200517
(Software) Determine MSI packages installed on the system

Classes\Installer\Products
LastWrite Time 2023-01-09 02:07:35Z

2023-01-09 02:07:36Z
Microsoft Forefront Endpoint Protection 2010 Server Management;d:\02bfa10a62ed60b7258d3e\amd64\FEPCClient.msi
2023-01-09 02:07:35Z
Microsoft Endpoint Protection Management Components;d:\02bfa10a62ed60b7258d3e\amd64\EppManagement.msi
2023-01-09 02:06:58Z
Microsoft Security Client;d:\02bfa10a62ed60b7258d3e\amd64\sepp.msi
2022-08-18 06:43:41Z
Microsoft Silverlight;d:\df6137d3f98fad84a43608cbdc80e406\silverlight.msi
2022-06-17 06:36:39Z
Microsoft Monitoring Agent;C:\Windows\422C3AB1-32E0-4411-BF66-A84FEFCC8E2\MOMAgent.msi
2020-09-10 05:32:18Z
MegaRAID Storage Manager;C:\Users\Unawaz\Desktop\MegaRAID\MSM.msi
2020-09-10 05:21:11Z
Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.51106;C:\ProgramData\Package Cache\{6C772996-BFF3-3C8C-860B-B3D48FF05D65}\v11.0.51106\packages
Ln 31167, Col 2 100% Windows (CRLF) UTF-8
```

```
SOFTWARE.txt - Notepad
File Edit Format View Help
LastWrite: 2023-02-06 09:56:31Z

LastLoggedOnUser = AD\Administrator
LastLoggedOnSAMUser = AD\Administrator
LastLoggedOnUserSID = S-1-5-21-2595053252-3331221587-625639084-500
-----
Licenses v.20200526
(Software) Get contents of HKLM/Software/Licenses key

Licenses not found.
-----
macaddr v.20200515
(System,Software) --

Microsoft\Windows Genuine Advantage not found.
-----
msis v.20200517
(Software) Determine MSI packages installed on the system

Classes\Installer\Products
LastWrite Time 2023-01-09 02:07:35Z

2023-01-09 02:07:36Z
Microsoft Forefront Endpoint Protection 2010 Server Management;d:\02bfa10a62ed60b7258d3e\amd64\FEPCClient.msi
2023-01-09 02:07:35Z
Microsoft Endpoint Protection Management Components;d:\02bfa10a62ed60b7258d3e\amd64\EppManagement.msi
2023-01-09 02:06:58Z
Microsoft Security Client;d:\02bfa10a62ed60b7258d3e\amd64\sepp.msi
2022-08-18 06:43:41Z
Microsoft Silverlight;d:\df6137d3f98fad84a43608cbdc80e406\silverlight.msi
2022-06-17 06:36:39Z
Microsoft Monitoring Agent;C:\Windows\422C3AB1-32E0-4411-BF66-A84FEFCC8E2\MOMAgent.msi
2020-09-10 05:32:18Z
MegaRAID Storage Manager;C:\Users\Unawaz\Desktop\MegaRAID\MSM.msi
2020-09-10 05:21:11Z
Microsoft Visual C++ 2012 x86 Additional Runtime - 11.0.51106;C:\ProgramData\Package Cache\{6C772996-BFF3-3C8C-860B-B3D48FF05D65}\v11.0.51106\packages
Ln 31165, Col 1 100% Windows (CRLF) UTF-8
```

A new installation of Microsoft Endpoint Protection Management, Microsoft Security Client version, MS Endpoint Protection Management is displayed in this step, presumably to restore the earlier uninstalled security measures to cover tracks so that system administrator may not note the suspicious activity by the

malicious actor

```
SYSTEM.txt - Notepad
File Edit Format View Help
SYSVOL\Windows\Temp\4D0A1C52-8350-43D2-A5F6-41463583AA5B\DisHost.exe 2013-08-22 13:25:38
SYSVOL\Windows\System32\vsqmcns.exe 2014-10-29 01:39:52
SYSVOL\Program Files\Microsoft Security Client\MsMpEng.exe 2016-11-14 16:14:42
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.373.1312.0.exe 2022-09-01 01:03:59
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.355.2631.0.exe 2022-01-28 16:14:13
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.371.514.0.exe 2022-07-21 08:28:35
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.355.143.0.exe 2021-12-13 08:29:17
SYSVOL\Windows\System32\PING.EXE 2013-08-22 10:02:58
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.1327.0.exe 2022-06-10 07:55:49
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.221.0.exe 2022-10-14 15:52:03
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.329.3049.0.exe 2021-01-30 20:48:38
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.361.222.0.exe 2022-12-10 14:44:17
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.375.1347.0.exe 2022-10-03 13:54:00
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.359.1729.0.exe 2022-03-11 08:15:09
SYSVOL\Windows\Microsoft.NET\Framework64\v4.0.30319\ngentask.exe 2013-08-10 00:41:20
SYSVOL\Windows\Temp\0A6100CC-0A87-4C91-BEC2-6A5897D0753A\DisHost.exe 2013-08-22 13:25:38
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.51.0.exe 2022-10-11 17:27:52
SYSVOL\Windows\CM\SMSCFGRC.cpl 2015-04-13 23:00:00
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.335.1094.0.exe 2021-04-20 00:21:51
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.321.2064.0.exe 2020-08-24 05:39:44
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.991.0.exe 2022-10-29 16:04:57
SYSVOL\Program Files\Microsoft Monitoring Agent\Agent\HealthService.exe 2020-01-06 18:44:26
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.353.1811.0.exe 2021-12-02 00:54:51
SYSVOL\Windows\SoftwareDistribution\Download\Install\WpSigStub.exe 2021-08-30 20:45:37
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.327.61.0.exe 2020-10-31 06:45:35
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.343.1250.0.exe 2021-07-21 00:40:23
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.967.0.exe 2022-06-03 19:23:51
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.373.873.0.exe 2022-08-24 02:19:09
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.381.872.0.exe 2022-12-24 03:16:59
SYSVOL\Users\Unawaz\Desktop\IBM ServerRAID M5014 Drivers\win2012-64\dpnrun.exe 2014-04-30 18:27:44
SYSVOL\Windows\Installer\MSI1936.tmp 2022-08-18 06:42:41
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.1344.0.exe 2022-11-07 13:13:42
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.325.42.0.exe 2020-10-04 04:37:20
SYSVOL\Windows\System32\Taskmgr.exe 2014-10-29 04:09:24
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.1400.0.exe 2022-06-12 00:19:34
SYSVOL\Users\windows_encrypt.exe 2023-01-06 22:48:14
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.381.757.0.exe 2022-12-22 02:30:57
```

```
SYSTEM.txt - Notepad
File Edit Format View Help
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.327.61.0.exe 2020-10-31 06:45:35
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.343.1250.0.exe 2021-07-21 00:40:23
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.967.0.exe 2022-06-03 19:23:51
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.373.873.0.exe 2022-08-24 02:19:09
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.381.872.0.exe 2022-12-24 03:16:59
SYSVOL\Users\Unawaz\Desktop\IBM ServerRAID M5014 Drivers\win2012-64\dpnrun.exe 2014-04-30 18:27:44
SYSVOL\Windows\Installer\MSI1936.tmp 2022-08-18 06:42:41
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.1344.0.exe 2022-11-07 13:13:42
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.325.42.0.exe 2020-10-04 04:37:20
SYSVOL\Windows\System32\Taskmgr.exe 2014-10-29 04:09:24
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.1400.0.exe 2022-06-12 00:19:34
SYSVOL\Users\windows_encrypt.exe 2023-01-06 22:48:14
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.381.757.0.exe 2022-12-22 02:30:57
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.1097.0.exe 2022-10-31 19:24:44
SYSVOL\Windows\Temp\F28AACB8-D25D-42F9-AD14-F8D23A2ED2D6\DisHost.exe 2013-08-22 13:25:38
SYSVOL\Users\Unawaz\AppData\Local\Temp\ibm_ux_pkg_00001480\image\msmUpdate.exe 2018-02-01 03:55:56
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.373.1647.0.exe 2022-09-07 00:49:00
SYSVOL\Program Files\Windows NT\Accessories\wordpad.exe 2018-06-08 18:04:18
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.359.295.0.exe 2022-02-16 11:25:20
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.1237.0.exe 2022-06-08 20:34:49
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.355.2492.0.exe 2022-01-25 16:26:17
SYSVOL\Windows\System32\lsasshost.exe 2013-08-22 11:20:25
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.353.1059.0.exe 2021-11-18 01:40:29
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.321.1768.0.exe 2020-08-21 02:34:33
SYSVOL\Windows\Temp\7009A104-31E0-44EB-9736-1BC51C106CFA\DisHost.exe 2013-08-22 13:25:38
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.379.104.0.exe 2022-11-11 17:13:53
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.987.0.exe 2022-10-29 14:42:03
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Engine.exe 2021-06-17 23:04:34
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.321.1703.0.exe 2020-08-20 00:33:01
SYSVOL\Users\windows32_encrypt.exe 2023-01-06 22:48:16
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.327.7.0.exe 2020-10-30 07:52:45
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.323.999.0.exe 2020-09-13 10:53:50
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.1307.0.exe 2022-06-09 21:39:35
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.323.780.0.exe 2020-09-09 02:22:27
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.359.1256.0.exe 2022-03-03 11:26:24
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.895.0.exe 2022-10-28 04:24:48
SYSVOL\Windows\System32\dfsrs.exe 2017-07-20 14:22:44
```

These two files “windows_encrypt.exe” and “windows32_encrypt.exe” were the ransomware files that was run to encrypt the system and display the ransom note.

```
SYSTEM.txt - Notepad
File Edit Format View Help
Start = Manual
Group =

Mon Jan 9 03:09:03 2023 Z
Name = BITS
Display = @%SystemRoot%\system32\qmgr.dll,-1000
ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs
Type = Share_Process
Start = Manual
Group =

Mon Jan 9 02:17:00 2023 Z
Name = MsMpSvc
Display = Microsoft Antimalware Service
ImagePath = "C:\Program Files\Microsoft Security Client\MsMpEng.exe"
Type = Own_Process
Start = Auto Start
Group = COM Infrastructure

Mon Jan 9 02:06:55 2023 Z
Name = MpBoot
Display = Microsoft Malware Protection Boot Driver
ImagePath = system32\DRIVERS\MpBoot.sys
Type = Kernel driver
Start = Boot Start
Group = Early-Launch

Mon Jan 9 02:06:46 2023 Z
Name = MpFilter
Display = Microsoft Malware Protection Driver
ImagePath = system32\DRIVERS\MpFilter.sys
Type = File system driver
Start = Boot Start
Group = FSFilter Anti-Virus

Name = NisDrv
Display = Microsoft Network Inspection System
```

A suspicious entry **mprun** was identified in the system's autostart configuration. Autostart entries often indicate persistence mechanisms used by malware or unauthorized programs to execute on system startup. The **mprun** entry could potentially be related to malicious software aiming to gain persistence.