Representer: Abbas

Group member: Syeda Laiba Bukhari, Asim Gul and Junaid Aftab

Presentation is: -

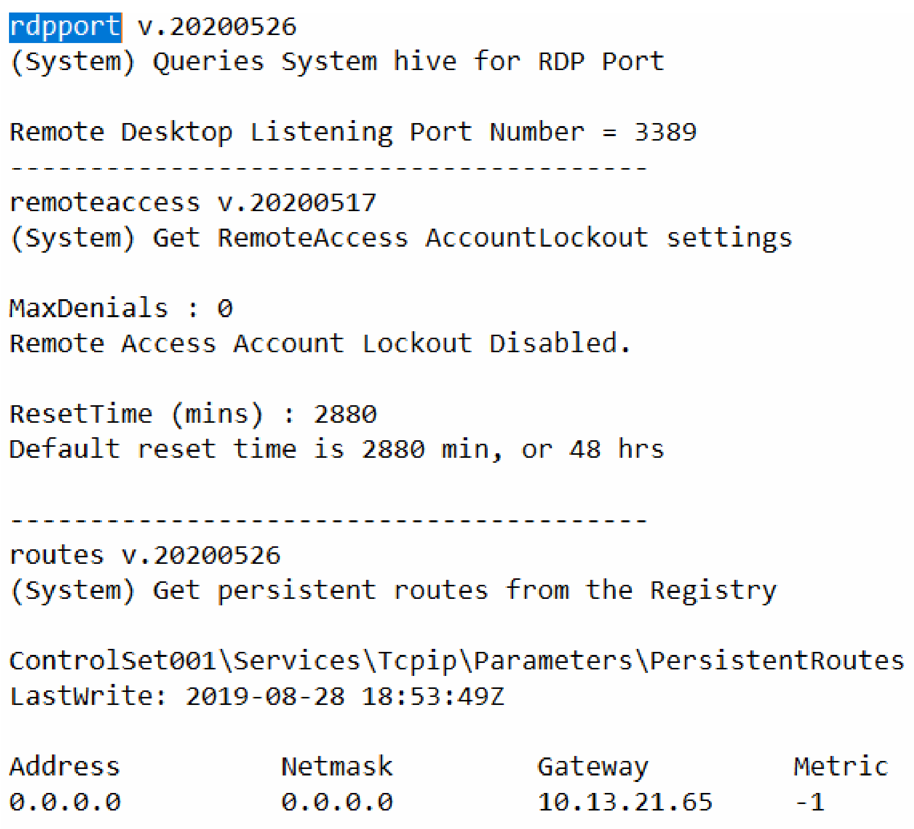
Active Directory Forensics-Case Study for Class Discussion

Key Found in Scenario:

1. **Initial Compromise:**
   - **05:56:13:** The "OMAction" user folder was created on the server.
   - **05:56:17:** An RDP connection was made to the server by "OMAction" from the IP address **10.1.53.78** (belonging to the ERP Terminal Server).
   - **05:56:18:** OMAction registered to use the **Local System Account**, gaining full administrative privileges.
2. **Disabling Security Measures:**
   - **05:56:55 - 05:58:03:** OMAction uninstalled multiple security tools, including Microsoft Endpoint Protection, Forefront Endpoint Protection, and Microsoft Security Client, likely to bypass detection and prevention mechanisms.
3. **File Copying and Execution:**
   - **07:22:** windows_encrypt.exe was copied to the C:\Users\ directory.
   - **07:26:** windows32_encrypt.exe was copied to the same directory.
   - **07:37:** bat.bat was copied but did not function due to cmd.exe incompatibility.
   - **08:38:** bat2.bat was created to execute windows_encrypt.exe using administrative parameters.
4. **Encryption Process:**
   - **09:11:28 AM:** The encryption process began, starting from the directory SysVol DFSSR/domain/scripts/.
   - It was noted that files were encrypted across the system, and a ransom note was generated.
5. **Erasure of Logs:**
   - All system and security logs were erased up until **January 24, 2023**, to cover traces of the attack.

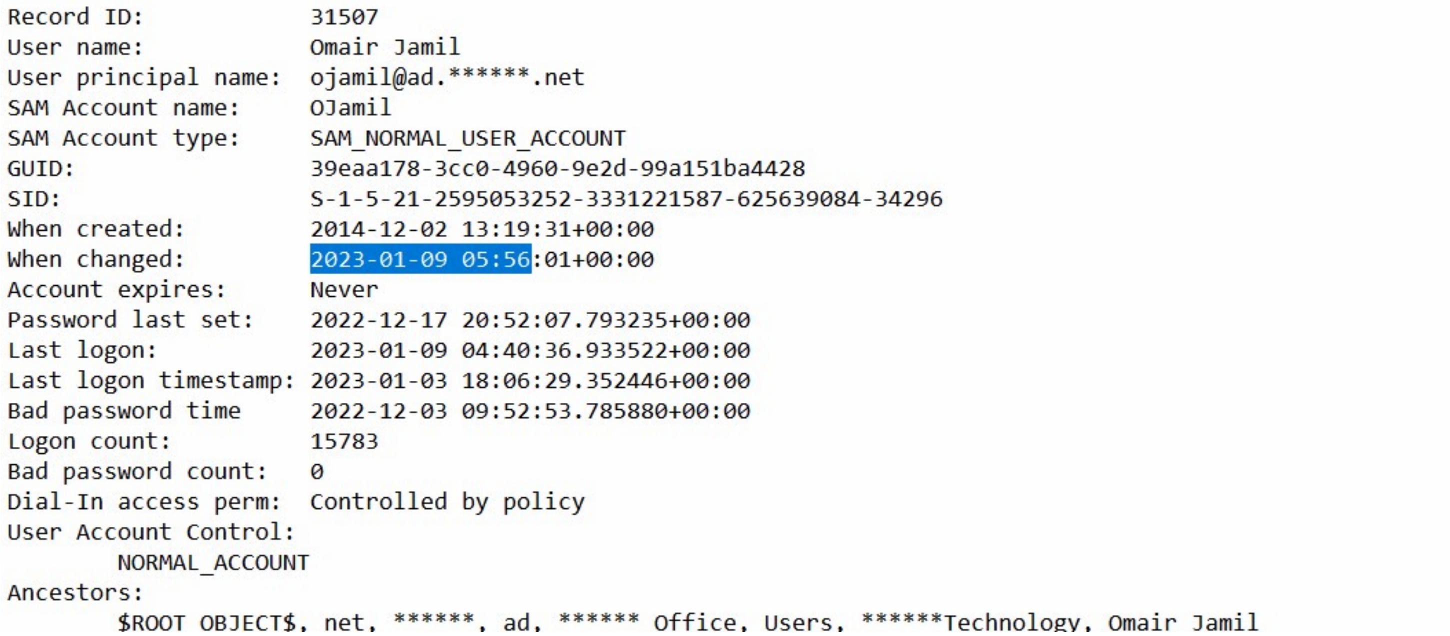
Key Events Leading to the Ransomware Attempt:

1. **05:56:13 to 05:59:54**:
    - User OMAction logged into the system via RDP from the IP address **10.1.53.78** (Terminal Server for ERP).

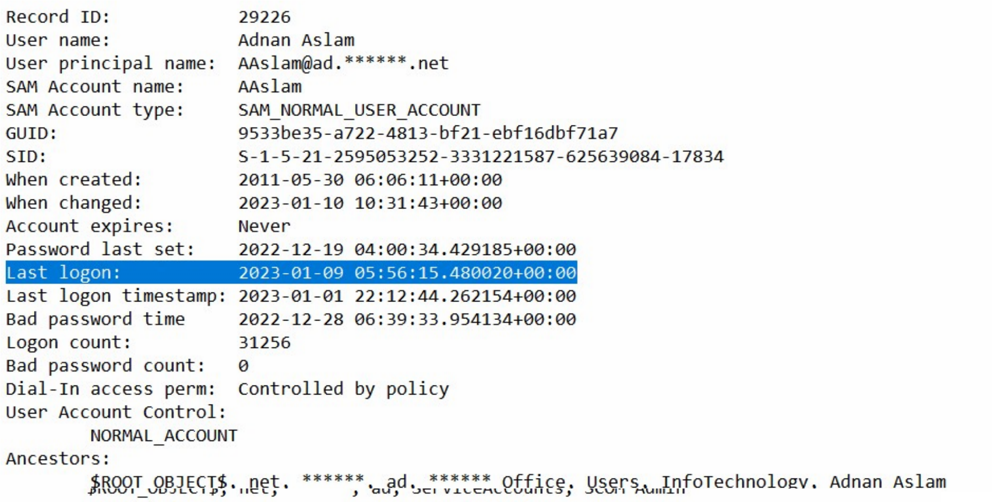


```
rdpport v.20200526
(System) Queries System hive for RDP Port

Remote Desktop Listening Port Number = 3389
----------------------------------------
remoteaccess v.20200517
(System) Get RemoteAccess AccountLockout settings

MaxDenials : 0
Remote Access Account Lockout Disabled.

ResetTime (mins) : 2880
Default reset time is 2880 min, or 48 hrs


----------------------------------------
routes v.20200526
(System) Get persistent routes from the Registry

ControlSet001\Services\Tcpip\Parameters\PersistentRoutes
LastWrite: 2019-08-28 18:53:49Z

Address          Netmask         Gateway         Metric
0.0.0.0          0.0.0.0         10.13.21.65     -1
```

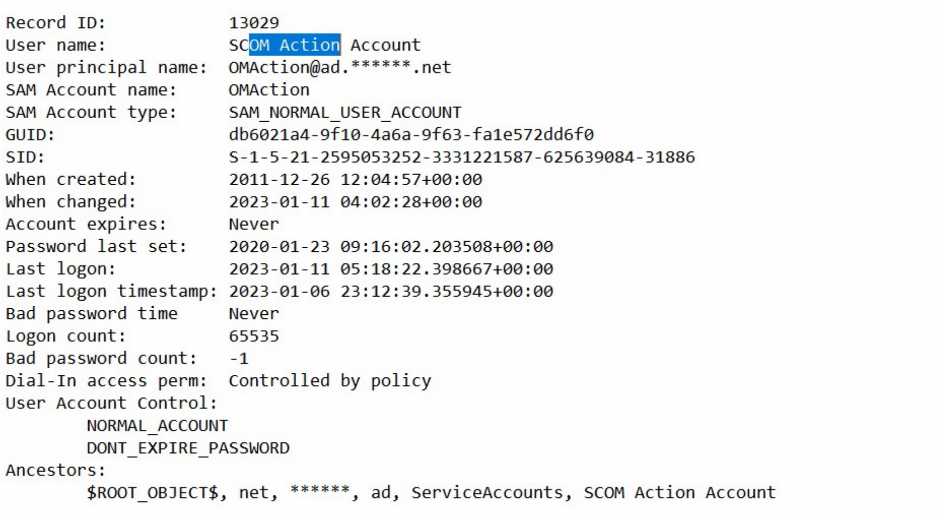
    - System security was compromised:
        - Antivirus (Microsoft Endpoint Protection and MS Forefront Endpoint Protection) was uninstalled by the user OMAction.
        - The system was left vulnerable for further malicious activity.



```
Record ID:             31507
User name:             Omair Jamil
User principal name:   ojamil@ad.******.net
SAM Account name:      OJamil
SAM Account type:      SAM_NORMAL_USER_ACCOUNT
GUID:                  39eaa178-3cc0-4960-9e2d-99a151ba4428
SID:                   S-1-5-21-2595053252-3331221587-625639084-34296
When created:          2014-12-02 13:19:31+00:00
When changed:          2023-01-09 05:56:01+00:00
Account expires:       Never
Password last set:     2022-12-17 20:52:07.793235+00:00
Last logon:            2023-01-09 04:40:36.933522+00:00
Last logon timestamp:  2023-01-03 18:06:29.352446+00:00
Bad password time      2022-12-03 09:52:53.785880+00:00
Logon count:           15783
Bad password count:    0
Dial-In access perm:   Controlled by policy
User Account Control:
        NORMAL_ACCOUNT
Ancestors:
        $ROOT OBJECT$, net, ******, ad, ****** Office, Users, ******Technology, Omair Jamil
```



```
Record ID:             29226
User name:             Adnan Aslam
User principal name:   AAslam@ad.******.net
SAM Account name:      AAslam
SAM Account type:      SAM_NORMAL_USER_ACCOUNT
GUID:                  9533be35-a722-4813-bf21-ebf16dbf71a7
SID:                   S-1-5-21-2595053252-3331221587-625639084-17834
When created:          2011-05-30 06:06:11+00:00
When changed:          2023-01-10 10:31:43+00:00
Account expires:       Never
Password last set:     2022-12-19 04:00:34.429185+00:00
Last logon:            2023-01-09 05:56:15.480020+00:00
Last logon timestamp:  2023-01-01 22:12:44.262154+00:00
Bad password time      2022-12-28 06:39:33.954134+00:00
Logon count:           31256
Bad password count:    0
Dial-In access perm:   Controlled by policy
User Account Control:
        NORMAL_ACCOUNT
Ancestors:
        $ROOT_OBJECT$, net, ******, ad, ****** Office, Users, InfoTechnology, Adnan Aslam
```



```
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
```

2. **07:22:11 to 07:37:00**:
   - Three suspicious files were copied into the C:\Users\ directory:
     - windows_encrypt.exe
     - windows32_encrypt.exe
     - bat.bat
   - These files were likely prepared as part of the ransomware attack.
3. **08:38:00**:
   - bat2.bat was created and modified using **WMIC process calls**.
   - This batch file was used to activate windows_encrypt.exe in administrative mode with the required credentials.

4. **09:11:28 AM**:
    - The ransomware (windows_encrypt.exe) began encrypting files on the server.
    - The encryption process started from the directory SysVol DFSSR/domain/scripts/.

When Was the Ransomware Attempted?

The **actual ransomware attempt** began when the windows_encrypt.exe file was executed, triggered by the bat2.bat file. This happened at **08:38 AM**, when bat2.bat was created, and the encryption process started shortly afterward at **09:11:28 AM**.

How the Ransomware Was Executed:

- The attacker (OMAction) had administrative privileges and created bat2.bat to pass the necessary commands to windows_encrypt.exe.
- The ransomware file started encrypting data at 09:11:28 AM, marking the onset of the ransomware attack.

Conclusion:

The **ransomware attempt** can be considered to have started between **08:38 AM (bat2.bat creation)** and **09:11:28 AM (encryption began)** on **January 9, 2023**.

If **two accounts ("Omair Jamil" and "Adnan Aslam") were created in the DUSERS** during the timeframe **05:56:13 to 05:59:54**, this suggests additional malicious actions alongside the ransomware attack preparations. Here's the potential significance of this activity:

Analysis of the Account Creation in DUSERS

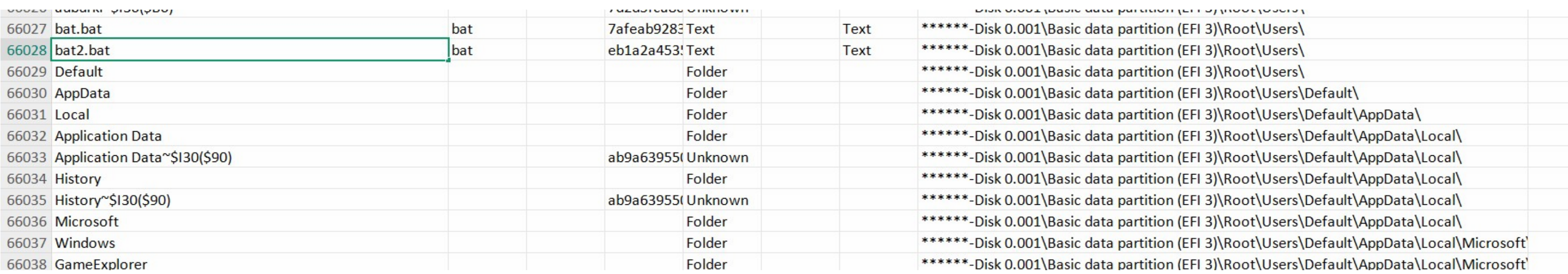
1. **Purpose of Accounts:**
   - These accounts could have been created as **backdoors** to maintain persistent access to the system in case the primary attack (via OMAction) was disrupted.
   - Such accounts are often given administrative privileges to bypass security measures or restore access if one method fails.
2. **Timeline Correlation:**
   - These accounts were login and after modified during the same session when OMAction accessed the server (05:56:13) and started uninstalling security software.
   - This aligns with the attacker's intent to prepare the system for the ransomware deployment.
3. **Role in the Attack:**
   - If these accounts had administrative privileges, they might have been used for:
     - Running additional malicious scripts.
     - Ensuring the encryption process could continue without interruption.
     - Hiding traces of the primary attack by creating confusion or redundancy.
4. **Connection to Ransomware Attempt:**
   - Although the ransomware encryption started later (08:38 to 09:11 AM), the activities on these accounts at this early stage indicates the attack was well-planned and systematic.

Potential Implications of the Created Accounts:

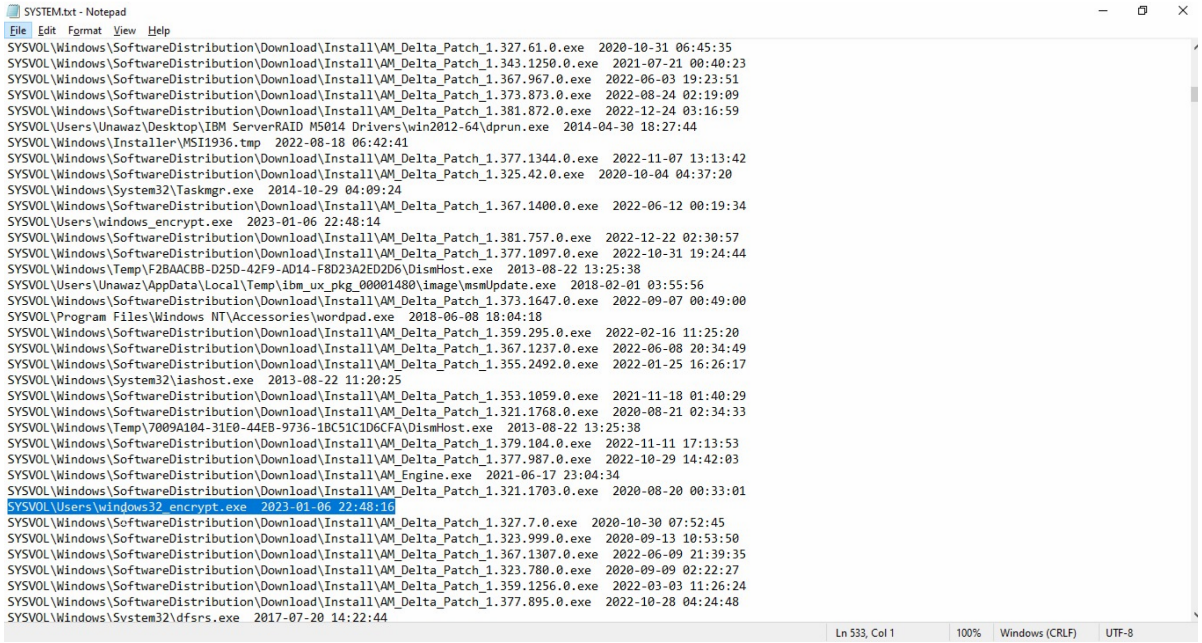
- These accounts suggest that **OMAction** might not have been the only user involved in the attack.
- Alternatively, the attacker might have used these newly created accounts for redundancy or to disguise their primary account's involvement.

Artifacts and Malware Indicators:

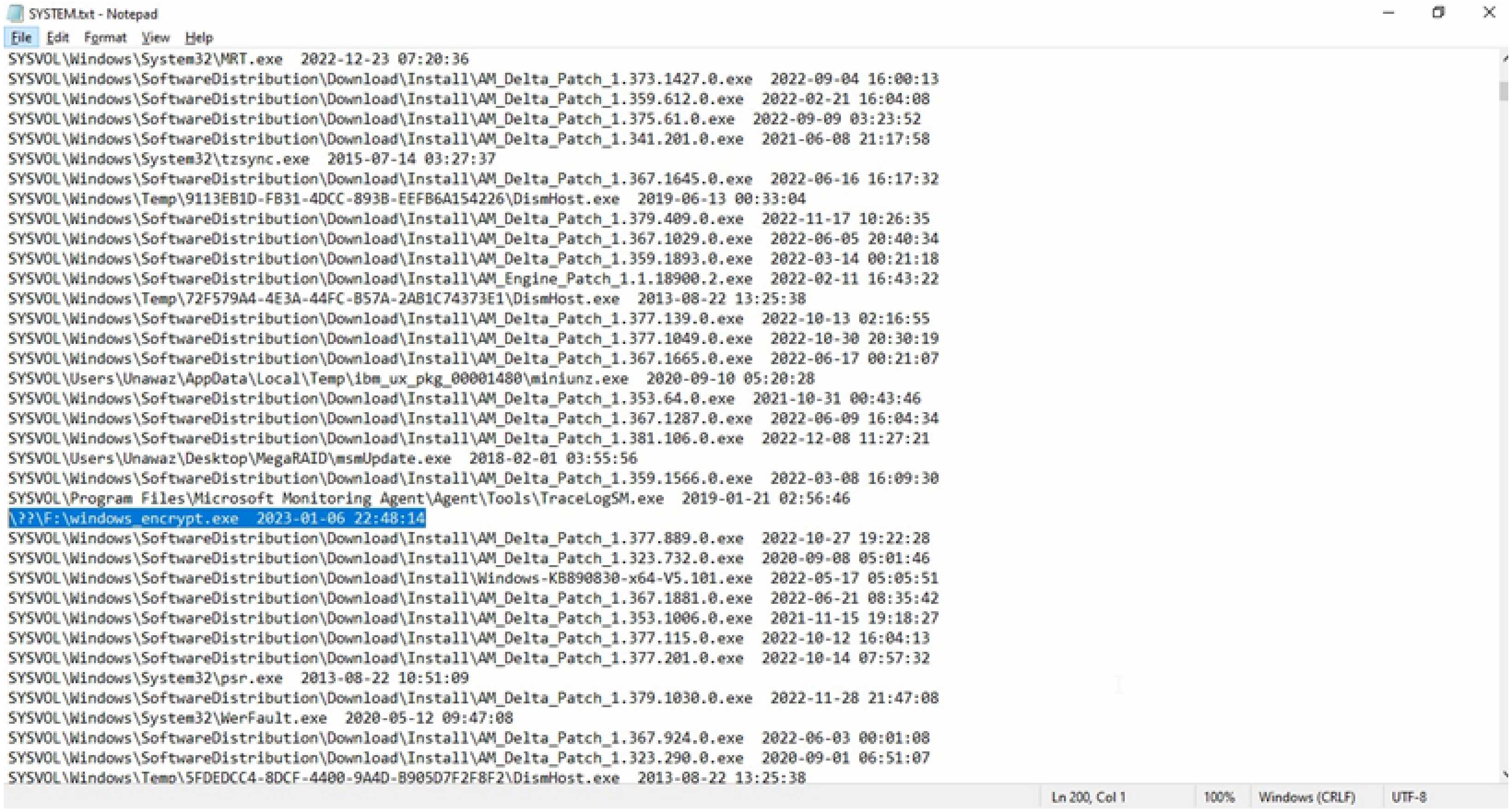
- **Primary Malware:**
  - **windows_encrypt.exe:**
    - This file encrypted the system and generated the ransomware note.
    - It was compiled on **January 6, 2023**, and executed on **January 9, 2023**.
- **Supporting Artifacts:**
  - **windows32_encrypt.exe:** Another file copied but likely not used for encryption.
  - **bat.bat:** An initial attempt to execute the malware but failed due to compatibility issues.
  - **bat2.bat:** Successfully used to execute windows_encrypt.exe in administrative mode.



66027	bat.bat	bat		7afeab9283	Text		Text	******-Disk 0.001\Basic data partition (EFI 3)\Root\Users\
66028	bat2.bat	bat		eb1a2a453	Text		Text	******-Disk 0.001\Basic data partition (EFI 3)\Root\Users\
66029	Default				Folder			******-Disk 0.001\Basic data partition (EFI 3)\Root\Users\
66030	AppData				Folder			******-Disk 0.001\Basic data partition (EFI 3)\Root\Users\Default\
66031	Local				Folder			******-Disk 0.001\Basic data partition (EFI 3)\Root\Users\Default\AppData\
66032	Application Data				Folder			******-Disk 0.001\Basic data partition (EFI 3)\Root\Users\Default\AppData\Local\
66033	Application Data~$I30($90)			ab9a63955(	Unknown			******-Disk 0.001\Basic data partition (EFI 3)\Root\Users\Default\AppData\Local\
66034	History				Folder			******-Disk 0.001\Basic data partition (EFI 3)\Root\Users\Default\AppData\Local\
66035	History~$I30($90)			ab9a63955(	Unknown			******-Disk 0.001\Basic data partition (EFI 3)\Root\Users\Default\AppData\Local\
66036	Microsoft				Folder			******-Disk 0.001\Basic data partition (EFI 3)\Root\Users\Default\AppData\Local\
66037	Windows				Folder			******-Disk 0.001\Basic data partition (EFI 3)\Root\Users\Default\AppData\Local\Microsoft'
66038	GameExplorer				Folder			******-Disk 0.001\Basic data partition (EFI 3)\Root\Users\Default\AppData\Local\Microsoft'



```
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\dprun.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\F2BAACBB-D25D-42F9-AD14-F8D23A2ED2D6\DismHost.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\iashost.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-9736-1BC51C1D6CFA\DismHost.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
```



```
SYSVOL\Windows\System32\MRT.exe  2022-12-23 07:20:36
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.373.1427.0.exe  2022-09-04 16:00:13
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.359.612.0.exe  2022-02-21 16:04:08
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.375.61.0.exe  2022-09-09 03:23:52
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.341.201.0.exe  2021-06-08 21:17:58
SYSVOL\Windows\System32\tzsync.exe  2015-07-14 03:27:37
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.1645.0.exe  2022-06-16 16:17:32
SYSVOL\Windows\Temp\9113EB1D-FB31-4DCC-893B-EEFB6A154226\DismHost.exe  2019-06-13 00:33:04
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.379.409.0.exe  2022-11-17 10:26:35
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.1029.0.exe  2022-06-05 20:40:34
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.359.1893.0.exe  2022-03-14 00:21:18
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Engine_Patch_1.1.18900.2.exe  2022-02-11 16:43:22
SYSVOL\Windows\Temp\72F579A4-4E3A-44FC-B57A-2AB1C74373E1\DismHost.exe  2013-08-22 13:25:38
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.139.0.exe  2022-10-13 02:16:55
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.1049.0.exe  2022-10-30 20:30:19
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.1665.0.exe  2022-06-17 00:21:07
SYSVOL\Users\Unawaz\AppData\Local\Temp\ibm_ux_pkg_00001480\miniunz.exe  2020-09-10 05:20:28
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.353.64.0.exe  2021-10-31 00:43:46
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.1287.0.exe  2022-06-09 16:04:34
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.381.106.0.exe  2022-12-08 11:27:21
SYSVOL\Users\Unawaz\Desktop\MegaRAID\msmUpdate.exe  2018-02-01 03:55:56
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.359.1566.0.exe  2022-03-08 16:09:30
SYSVOL\Program Files\Microsoft Monitoring Agent\Agent\Tools\TraceLogSM.exe  2019-01-21 02:56:46
\??\F:\windows_encrypt.exe  2023-01-06 22:48:14
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.889.0.exe  2022-10-27 19:22:28
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.323.732.0.exe  2020-09-08 05:01:46
SYSVOL\Windows\SoftwareDistribution\Download\Install\Windows-KB890830-x64-V5.101.exe  2022-05-17 05:05:51
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.1881.0.exe  2022-06-21 08:35:42
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.353.1006.0.exe  2021-11-15 19:18:27
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.115.0.exe  2022-10-12 16:04:13
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.377.201.0.exe  2022-10-14 07:57:32
SYSVOL\Windows\System32\psr.exe  2013-08-22 10:51:09
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.379.1030.0.exe  2022-11-28 21:47:08
SYSVOL\Windows\System32\WerFault.exe  2020-05-12 09:47:08
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.367.924.0.exe  2022-06-03 00:01:08
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.323.290.0.exe  2020-09-01 06:51:07
SYSVOL\Windows\Temp\5FDEDCC4-8DCF-4400-9A4D-B905D7F2F8F2\DismHost.exe  2013-08-22 13:25:38
```

Conclusion:

The ransomware attack was executed using the windows_encrypt.exe file, facilitated by the bat2.bat script. The OMAction account was the primary actor, which:

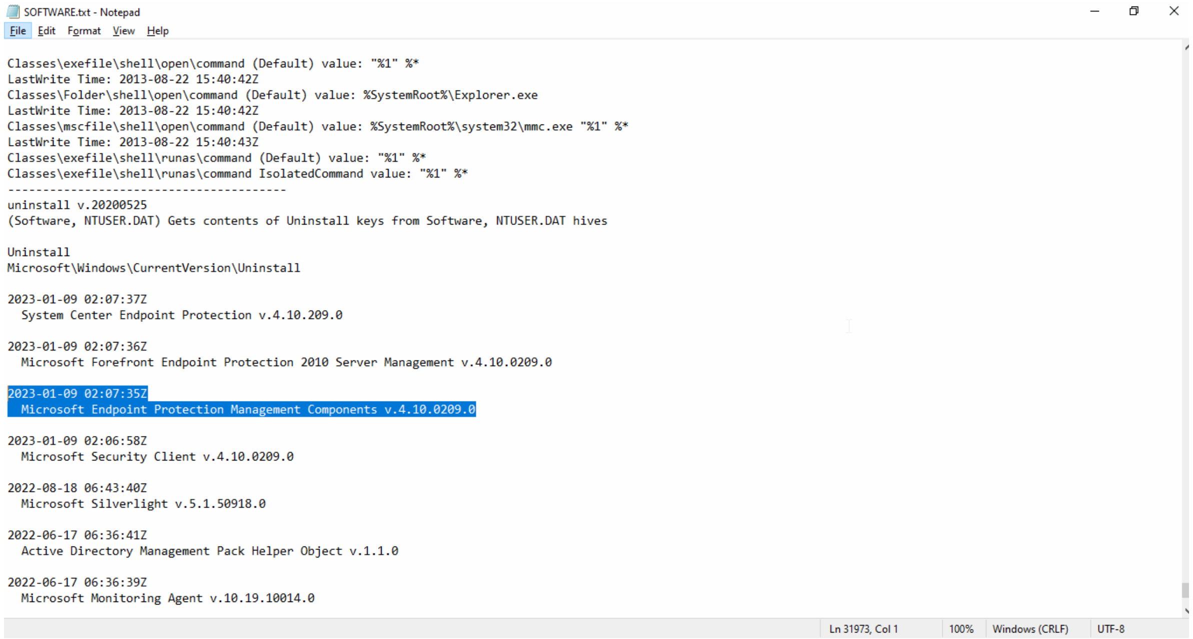
1. Gained RDP access to the server with administrative privileges.
2. Disabled security measures to allow malware execution.
3. Deployed and executed the ransomware (windows_encrypt.exe) that encrypted system files.

Malicious Files:

1. windows_encrypt.exe – Primary ransomware file.
2. bat2.bat – Script to execute the ransomware.
3. windows32_encrypt.exe – Copied but unused.

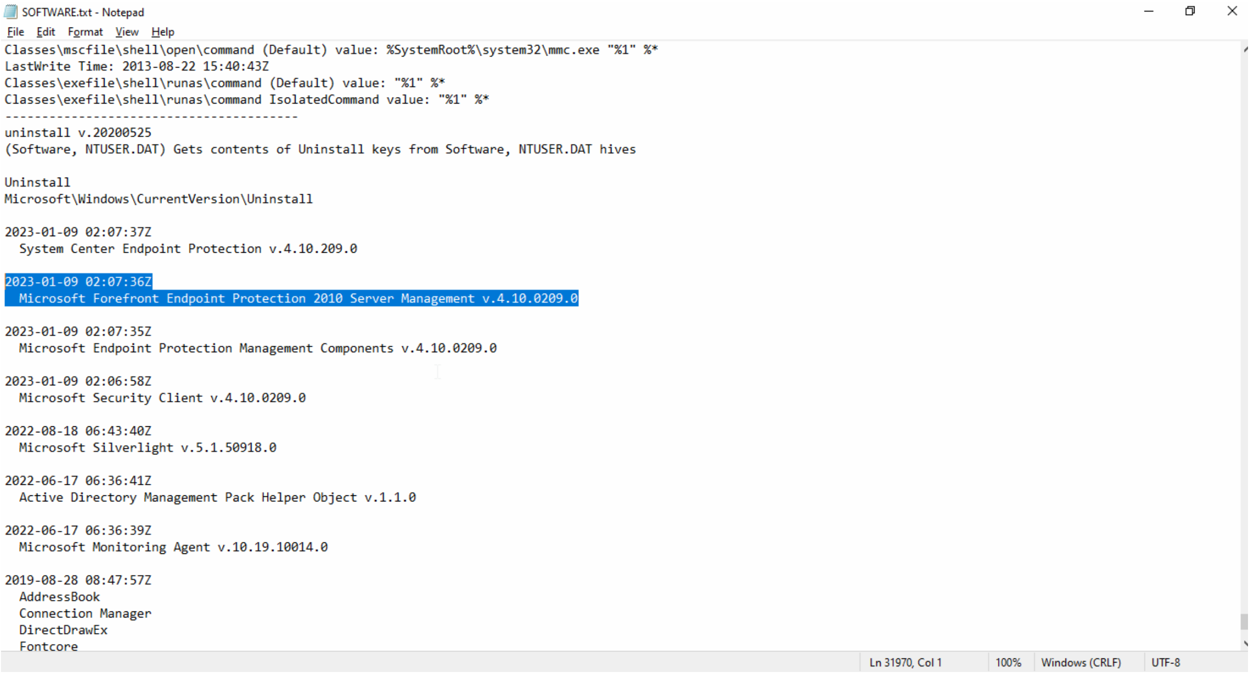
Uninstalled and Installed MS endpoint protection

MS Endpoint MS / forefront Protection and was uninstalled for copies or copy the malware files (window_encrypt.exe) and cmd file to run the malware bat2.bat file.



```
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
```

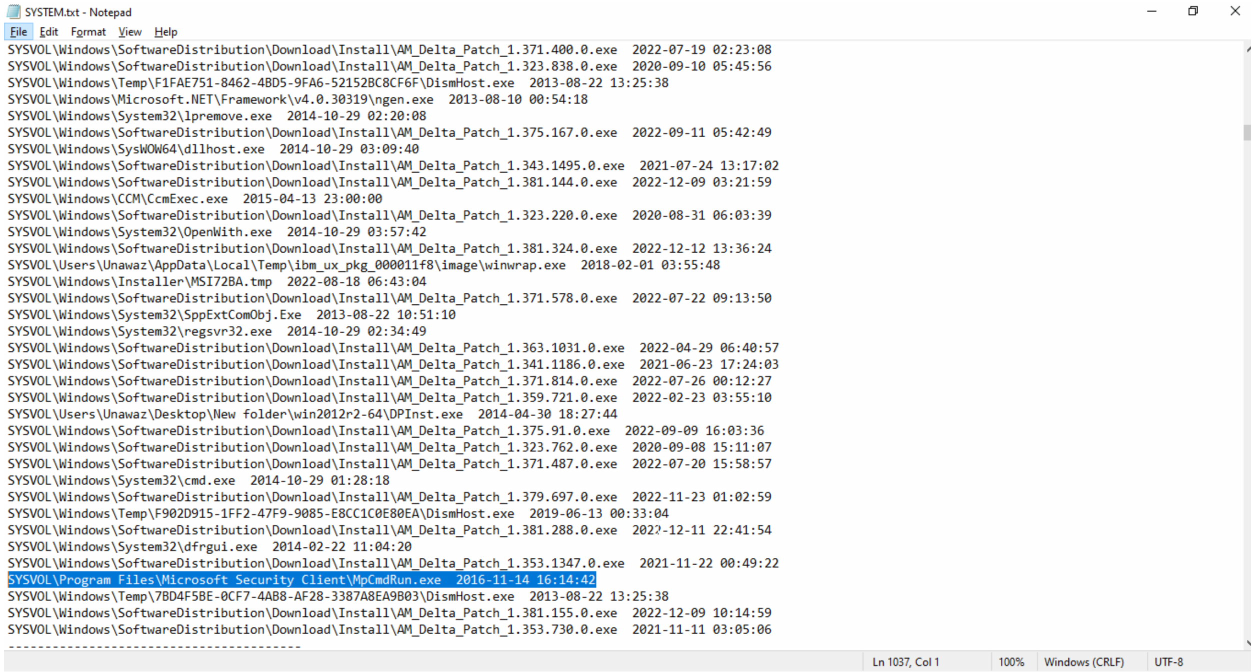
MS forefront Endpoint Protection was uninstall showing an indicator to suspicious activity.



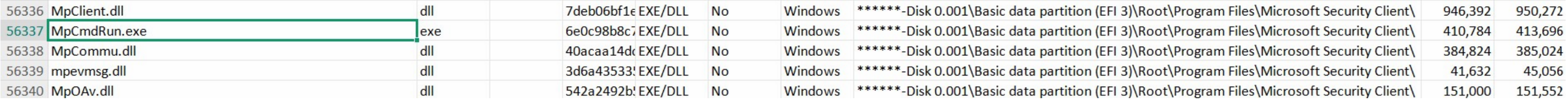
```
Classes\mscfile\shell\open\command (Default) value: %SystemRoot%\system32\mmc.exe "%1" %*
LastWrite Time: 2013-08-22 15:40:43Z
Classes\exefile\shell\runas\command (Default) value: "%1" %*
Classes\exefile\shell\runas\command IsolatedCommand value: "%1" %*
----------------------------------------
uninstall 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
```

MPCMDRun.exe

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.

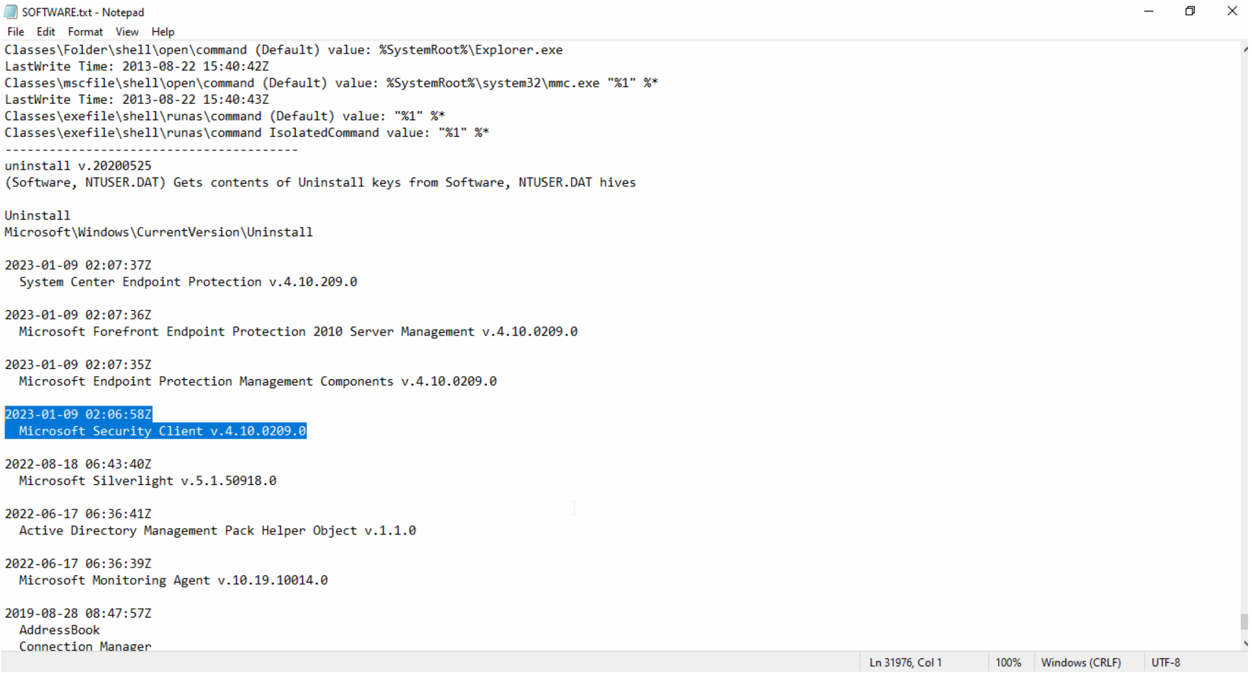


```
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.371.400.0.exe  2022-07-19 02:23:08
SYSVOL\Windows\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.323.838.0.exe  2020-09-10 05:45:56
SYSVOL\Windows\Temp\F1FAE751-8462-4BD5-9FA6-52152BC8CF6F\DismHost.exe  2013-08-22 13:25:38
SYSVOL\Windows\Microsoft.NET\Framework\v4.0.30319\ngen.exe  2013-08-10 00:54:18
SYSVOL\Windows\System32\lpremove.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\SysWOW64\dllhost.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  202?-12-11 22:41:54
SYSVOL\Windows\System32\dfrgui.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
----------------------------------------
```



56336	MpClient.dll	dll		7deb06bf1e	EXE/DLL	No	Windows	******-Disk 0.001\Basic data partition (EFI 3)\Root\Program Files\Microsoft Security Client\	946,392	950,272
56337	MpCmdRun.exe	exe		6e0c98b8c7	EXE/DLL	No	Windows	******-Disk 0.001\Basic data partition (EFI 3)\Root\Program Files\Microsoft Security Client\	410,784	413,696
56338	MpCommu.dll	dll		40acaa14dc	EXE/DLL	No	Windows	******-Disk 0.001\Basic data partition (EFI 3)\Root\Program Files\Microsoft Security Client\	384,824	385,024
56339	mpevmsg.dll	dll		3d6a43533!	EXE/DLL	No	Windows	******-Disk 0.001\Basic data partition (EFI 3)\Root\Program Files\Microsoft Security Client\	41,632	45,056
56340	MpOAv.dll	dll		542a2492b!	EXE/DLL	No	Windows	******-Disk 0.001\Basic data partition (EFI 3)\Root\Program Files\Microsoft Security Client\	151,000	151,552

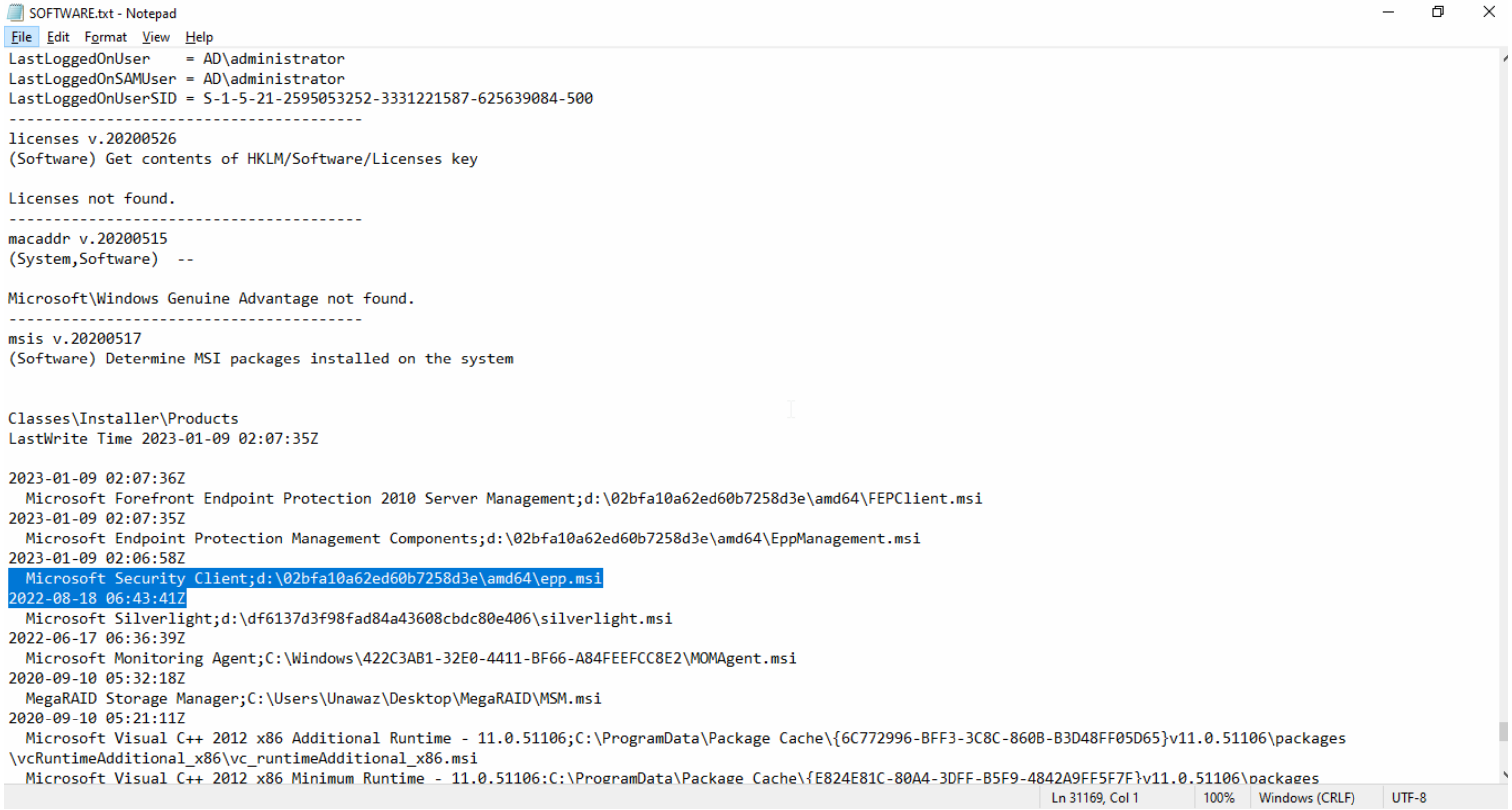
Again, **MS Security Client** was uninstalled to create a vulnerable system so that system can be exploited easily



```
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
```

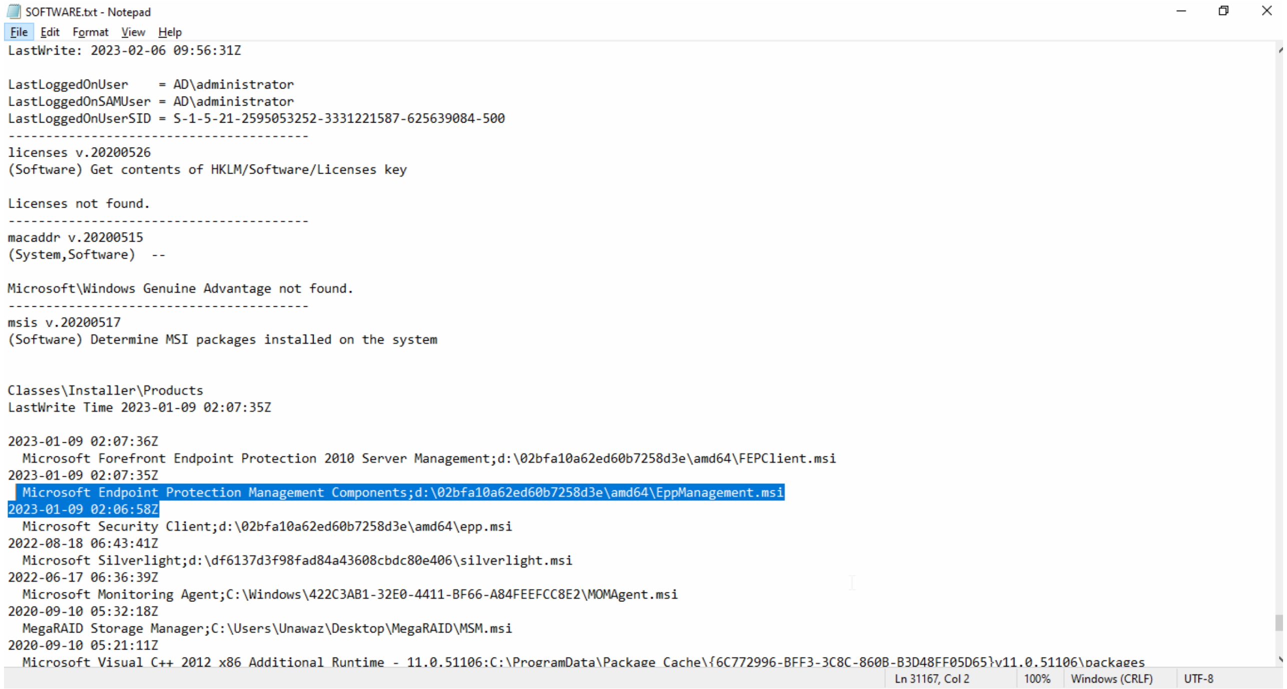
A new installation of **Microsoft Endpoint Protection Management**, **Microsoft Security Client version**, **MS Endpoint Protection Management** is displayed in this step, presumably to restore the earlier uninstalled security measures to cover tracks so that system administrator may not note the suspicious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

Install Microsoft security client



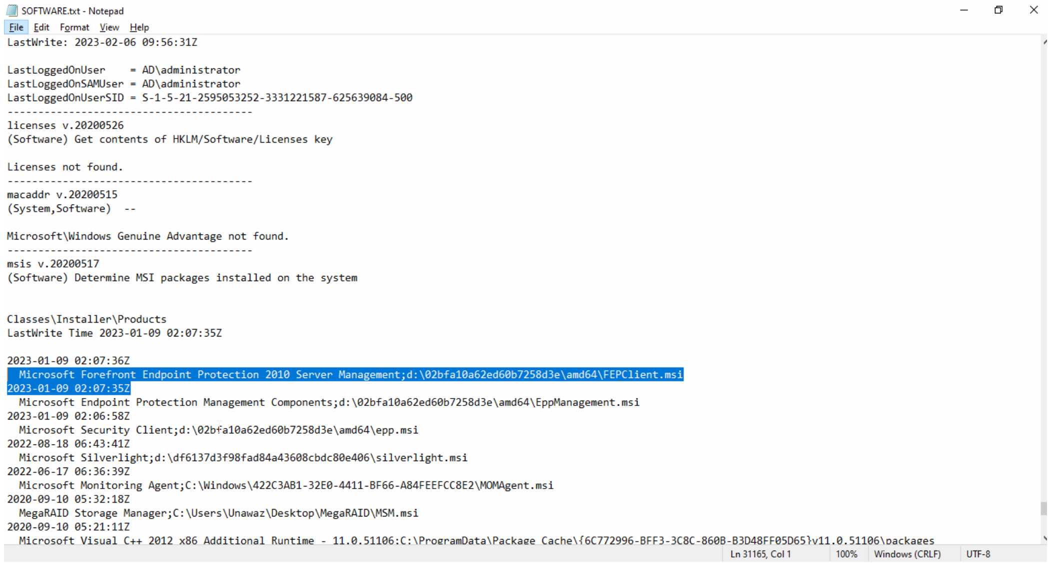
```
LastLoggedOnUser    = AD\administrator
LastLoggedOnSAMUser = AD\administrator
LastLoggedOnUserSID = S-1-5-21-2595053252-3331221587-625639084-500
----------------------------------------
licenses v.20200526
(Software) Get contents of HKLM/Software/Licenses key

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\epp.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-A84FEEFCC8E2\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
\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
```

Installed MS endpoint protection



```
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\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\epp.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-A84FEEFCC8E2\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
```

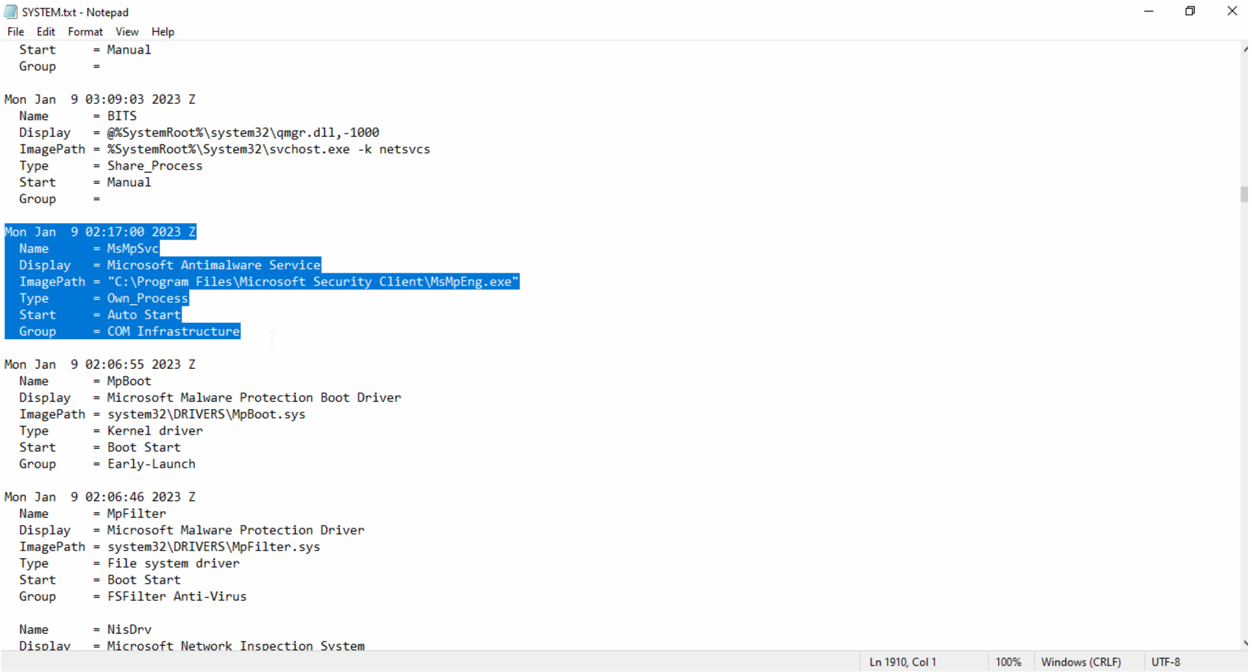
Installed MS forefront endpoint protection



```
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\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\epp.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-A84FEEFCC8E2\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
```

Mprun.exe

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.



```
  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
```