2024

Perform Threat Hunting Against 2 Machines

MOSSÉ CYBERSECURITY INSTITUTE

AARON AMRAN BIN AMIRUDDIN

Student ID: nxCLnZGLgyOUMpnDw16rtDvYuTF2

Table of Contents

Executive Summary

During the threat-hunting investigation, we analyzed system data from two machines with hostnames of **0000DQQEE** and **0001LXQEN** to identify malicious activities indicative of compromise. By scrutinizing extracted datasets, we filtered for common suspicious processes such as unsigned or unverified binaries, processes executing from atypical paths (e.g., Temp, AppData), and commands linked to administrative or sensitive operations (cmd.exe, powershell.exe, reg.exe, etc.). Key findings revealed the presence of credential harvesting and privilege escalation attempts on machine **0000DQQEE**. The indicators discovered suggest that this machine has been compromised, while the other machine exhibits no obvious signs of malicious activity. To mitigate potential threats from threat actors, it is important to have ongoing effective monitoring and forensic analysis.

Investigation Approach

Before investigating both machines, Redline which is a memory analysis tool from FireEye, is used to extract data from the machines, which consists of **Domain Users**, **Logged On Users**, **User Accounts**, **Windows Drivers**, **Windows Persistence File Items**, **Windows Persistence Registry Items**, **Windows Persistence Services Items**, **Windows Processes**, **Windows Processes Memory Sections**, **Windows Services** and **Windows Tasks**. The data is then converted to Pandas for detailed analysis in Jupyter Notebooks.

An investigation plan is also strategised to ensure the machine datasets are thoroughly checked for indicators of compromise (IOCs). The perspective of the attacker is used to lay out what attacks are most likely executed. This means that possible attacks such as malicious commands executed with privileges or credential harvesting are used as IOCs which are then checked for correlation with known available user accounts.

Table 1: Categories of data and common IOCs

Categories	Common Indicators of Compromise (IOCs)
Domain Users	• Unusual domain user accounts (new or unknown accounts) • Suspicious login activity (e.g., unusual times or locations) • Elevated privileges granted to domain accounts (admin or system-level access) • Accounts with weak or reused passwords
Logged On Users	• Users logged in from multiple locations (indicating potential lateral movement) • Accounts used at unusual hours or in unexpected contexts • Concurrent sessions of the same user on multiple machines
User Accounts	• Creation of hidden, non-descriptive accounts (e.g., "user123" or "testadmin") • Presence of accounts that should not be there (e.g., accounts with names similar to system services or processes) • Disabled or locked accounts being re-enabled without authorized access or approval
Windows Drivers	• Loading of unsigned or suspicious drivers (e.g., malware-loaded drivers) • Drivers with unusual file paths (e.g., non-standard directories like C:\Windows\Temp) • Newly installed drivers or drivers modified unexpectedly • Legitimate drivers being overwritten with malicious drivers
Windows Persistence File Items	• Presence of unusual files in directories associated with persistence (e.g., C:\Windows\System32 or C:\Users) • Suspicious files being created on startup (e.g., files in startup folders or AppData) • Files with unusual names (random names, files that are not typically seen in the environment)

Windows Persistence Registry Items	• Modification or addition of registry keys related to persistence (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) • Registry entries that execute non-legitimate applications on system boot • Changes to RunOnce, Run, Services keys or the creation of new, unexpected keys
Windows Persistence Services Items	• Creation of new services (especially those with unusual names) • Services configured to start automatically but with suspicious or unsigned executables • Legitimate services being modified to execute malicious code
Windows Processes	• Malicious or suspicious processes running (e.g., unfamiliar process names like cmd.exe, powershell.exe) • Processes running from non-standard locations (e.g., C:\Windows\Temp\malicious.exe) • High CPU or memory usage by processes that are not typical for the system • Processes injecting into other processes (e.g., svchost.exe injecting into explorer.exe)
Windows Processes Memory Sections	• Suspicious memory sections (e.g., memory regions mapped by malicious code) • Unusual DLLs or shellcode loaded into memory regions by running processes • Memory alterations (process injection)
Windows Services	• Unusual service names or those running from suspicious paths • New services created or altered (especially those with a malicious nature) • Services with weak or unnecessary permissions (e.g., SYSTEM-level privileges for an unexpected service)
Windows Tasks	• New scheduled tasks created (especially those with hidden or random names) • Scheduled tasks set to run at unusual intervals or times • Tasks running non-standard or malicious executables, or commands with malicious intent

Table 2: Attack type with corresponding categories and IOCs

Attack Type	Category	IOCs
Malicious Windows Commands	Windows Processes, Windows Services	tasklist, ipconfig, systeminfo, net, query, wmic, sc, rundll32, Powershell, mshta, netstat
Using Accessibility Features for Persistence	Windows Services, Windows Drivers, Windows Persistence File Items	narrator.exe, sethc.exe, utilman.exe, osk.exe, searchui.exe, magnify.exe, calculator.exe
Modifying a Windows Service	Windows Services, Windows Persistence Registry Items	sc, binPath, HKLM, ImagePath, FailureCommand, HKEY, svchost.exe, winlogon.exe, regedit.exe
Searching for Credentials in the Registry	Windows Persistence Registry Items, User Accounts, Windows Processes	reg.exe, ServiceName, Reg query, HKCU, HKLM, Lsass.exe, HKEY, PuTTY, SAM, kerberos
Path Interception	Windows Persistence Registry Items, Windows Services	%SystemRoot%, unquoted service paths
Process Injection	Windows Processes, Windows Processes Memory Sections, Windows Persistence Registry Items	.dll, Appinit_Dlls, AppCertDlls, Image File Executable Options, HKLM\Software\Microsoft\Windows, HKLM\Software\Wow6432Node\Microsoft\Windows, AppInit_DLLs

Compromised Machines

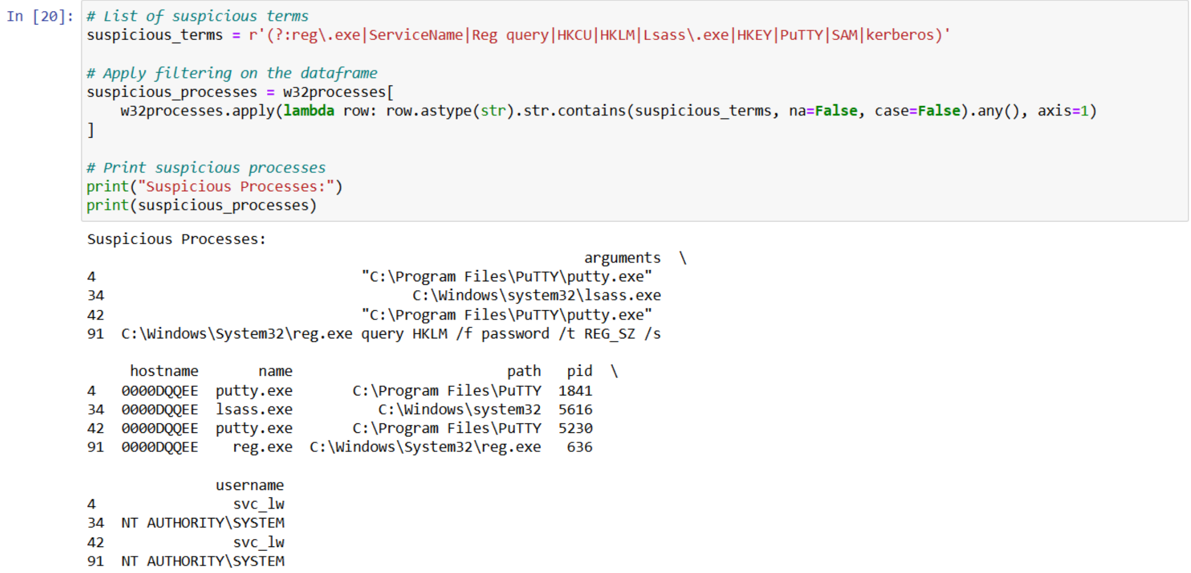
In this section, the reasons why machine **0000DQQEE** are considered compromised will be explained. Firstly, the domain users with the respective usernames of **timotlopez**, **Administrator** and **svc_lw** are identified from the **Domain Users** dataset of both machines.

The suspicious activities from the **Logged On Users** dataset from both machines are summarised in the following table:

Machine	Activity	Reason
0001LXQEN	cmd.exe	Interactive session or script execution could indicate malicious activity
	ruby.exe	Unusual process unless explicitly required
	CyberGhost.Service.exe	VPN application might indicate concealed network activity if unauthorized
0000DQQEE	cmd.exe	Could indicate IOC if unexpected
	kitty-0.70.0.6.exe and putty.exe	SSH clients may indicate lateral movement or unauthorized remote access
	svc_lw account logged in	Use of an **Enterprise Admin** account on a workstation is highly unusual
	net.exe and reg.exe	May indicate system configuration or reconnaissance activity

In the **User Accounts** dataset, machine **0001LXQEN** indicates that **timotlopez** account has both domain and local admin privileges, while **Administrator** account lacks local admin privileges, which aligns with best practices for minimizing its exposure. Machine **0000DQQEE** has the **svc_lw** account used on the machine, but its privileges as an **Enterprise Admin** reflects that it is potentially suspicious. The **timotlopez** account is once again both a domain and local admin, making it a critical target for monitoring.

Indicators of Compromise (IOCs)



```
In [20]: # List of suspicious terms
         suspicious_terms = r'(?:reg\.exe|ServiceName|Reg query|HKCU|HKLM|Lsass\.exe|HKEY|PuTTY|SAM|kerberos)'

         # Apply filtering on the dataframe
         suspicious_processes = w32processes[
             w32processes.apply(lambda row: row.astype(str).str.contains(suspicious_terms, na=False, case=False).any(), axis=1)
         ]

         # Print suspicious processes
         print("Suspicious Processes:")
         print(suspicious_processes)
```

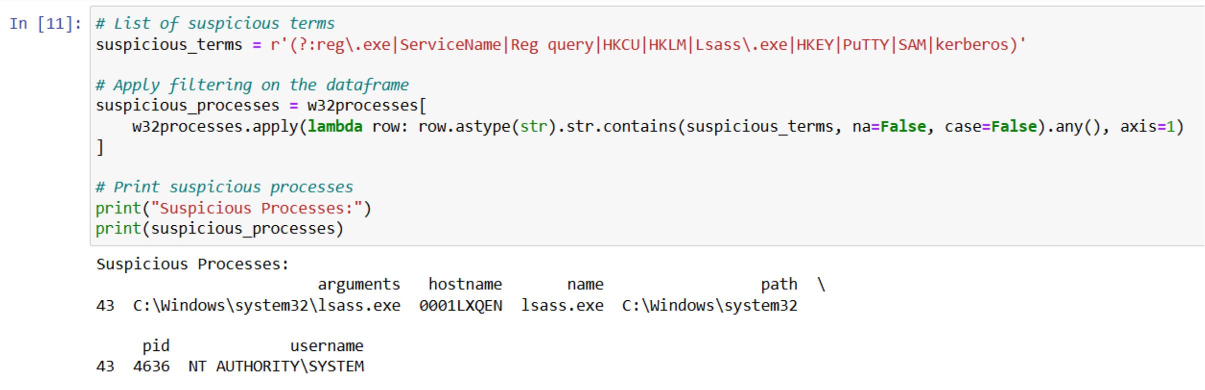
```
Suspicious Processes:
                                                          arguments  \
4                                "C:\Program Files\PuTTY\putty.exe"
34                                    C:\Windows\system32\lsass.exe
42                               "C:\Program Files\PuTTY\putty.exe"
91  C:\Windows\System32\reg.exe query HKLM /f password /t REG_SZ /s

     hostname       name                         path   pid  \
4   0000DQQEE  putty.exe       C:\Program Files\PuTTY  1841
34  0000DQQEE  lsass.exe          C:\Windows\system32  5616
42  0000DQQEE  putty.exe       C:\Program Files\PuTTY  5230
91  0000DQQEE    reg.exe  C:\Windows\System32\reg.exe   636

               username
4                svc_lw
34  NT AUTHORITY\SYSTEM
42               svc_lw
91  NT AUTHORITY\SYSTEM
```

Figure 1: Screenshot of filtered suspicious processes

When Windows Processes in machine **0000DQQEE** are searched for suspicious terms that involves accessing the registry, we can see multiple instances of suspicious activities being executed. Firstly, PuTTY which is a legitimate SSH client may indicate unauthorized remote access or communication with a command-and-control (C2) server. However, the arguments used are not shown, which could also mean concealing of malicious intent such as tunneling or data exfiltration.

Another obvious IOC is the use of reg.exe with suspicious arguments. The arguments ‘query HKLM /f password /t REG_SZ /s’ are used to query the Windows Registry for entries containing the term “password” under the HKEY_LOCAL_MACHINE (HKLM) hive. This demonstrates an attempt to harvest sensitive data from machine **0000DQQEE**.

The IOCs mentioned above are strongly supported by the fact that **svc_lw** which is an Enterprise Admin account is the account responsible for compromising the system. To compare the findings with machine **0001LXQEN**, the same Python code is ran as input in Jupyter Notebook as seen in Figure 2.

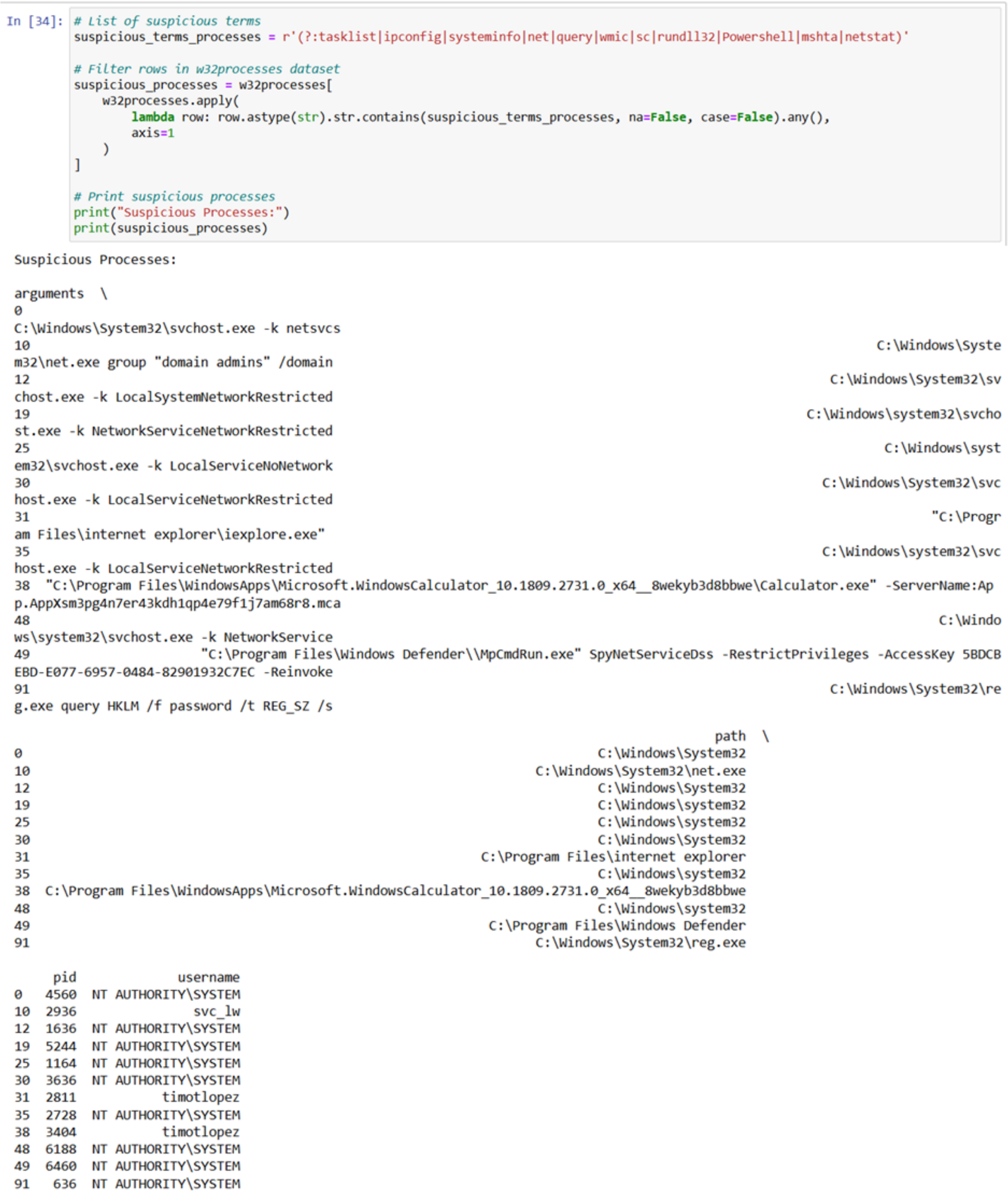


```
In [11]: # List of suspicious terms
         suspicious_terms = r'(?:reg\.exe|ServiceName|Reg query|HKCU|HKLM|Lsass\.exe|HKEY|PuTTY|SAM|kerberos)'

         # Apply filtering on the dataframe
         suspicious_processes = w32processes[
             w32processes.apply(lambda row: row.astype(str).str.contains(suspicious_terms, na=False, case=False).any(), axis=1)
         ]

         # Print suspicious processes
         print("Suspicious Processes:")
         print(suspicious_processes)
```

```
Suspicious Processes:
                        arguments   hostname       name                 path  \
43  C:\Windows\system32\lsass.exe  0001LXQEN  lsass.exe  C:\Windows\system32

     pid             username
43  4636  NT AUTHORITY\SYSTEM
```

Figure 2: Screenshot of lsass.exe listed as suspicious process

Note that there are no presence of IOCs in machine **0001LXQEN**, despite lsass.exe running as a process.



```
In [34]: # List of suspicious terms
         suspicious_terms_processes = r'(?:tasklist|ipconfig|systeminfo|net|query|wmic|sc|rundll32|Powershell|mshta|netstat)'

         # Filter rows in w32processes dataset
         suspicious_processes = w32processes[
             w32processes.apply(
                 lambda row: row.astype(str).str.contains(suspicious_terms_processes, na=False, case=False).any(),
                 axis=1
             )
         ]

         # Print suspicious processes
         print("Suspicious Processes:")
         print(suspicious_processes)
```

```
Suspicious Processes:

arguments  \
0   
C:\Windows\System32\svchost.exe -k netsvcs
10                                                                                                            C:\Windows\Syste
m32\net.exe group "domain admins" /domain
12                                                                                                      C:\Windows\System32\sv
chost.exe -k LocalSystemNetworkRestricted
19                                                                                                   C:\Windows\system32\svcho
st.exe -k NetworkServiceNetworkRestricted
25                                                                                                             C:\Windows\syst
em32\svchost.exe -k LocalServiceNoNetwork
30                                                                                                     C:\Windows\System32\svc
host.exe -k LocalServiceNetworkRestricted
31                                                                                                                   "C:\Progr
am Files\internet explorer\iexplore.exe"
35                                                                                                     C:\Windows\system32\svc
host.exe -k LocalServiceNetworkRestricted
38  "C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1809.2731.0_x64__8wekyb3d8bbwe\Calculator.exe" -ServerName:Ap
p.AppXsm3pg4n7er43kdh1qp4e79f1j7am68r8.mca
48                                                                                                                    C:\Windo
ws\system32\svchost.exe -k NetworkService
49                     "C:\Program Files\Windows Defender\\MpCmdRun.exe" SpyNetServiceDss -RestrictPrivileges -AccessKey 5BDCB
EBD-E077-6957-0484-82901932C7EC -Reinvoke
91                                                                                                      C:\Windows\System32\re
g.exe query HKLM /f password /t REG_SZ /s

                                                                                          path  \
0                                                                          C:\Windows\System32
10                                                                 C:\Windows\System32\net.exe
12                                                                         C:\Windows\System32
19                                                                         C:\Windows\system32
25                                                                         C:\Windows\system32
30                                                                         C:\Windows\System32
31                                                          C:\Program Files\internet explorer
35                                                                         C:\Windows\system32
38  C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1809.2731.0_x64__8wekyb3d8bbwe
48                                                                         C:\Windows\system32
49                                                           C:\Program Files\Windows Defender
91                                                                 C:\Windows\System32\reg.exe

     pid             username
0   4560  NT AUTHORITY\SYSTEM
10  2936               svc_lw
12  1636  NT AUTHORITY\SYSTEM
19  5244  NT AUTHORITY\SYSTEM
25  1164  NT AUTHORITY\SYSTEM
30  3636  NT AUTHORITY\SYSTEM
31  2811           timotlopez
35  2728  NT AUTHORITY\SYSTEM
38  3404           timotlopez
48  6188  NT AUTHORITY\SYSTEM
49  6460  NT AUTHORITY\SYSTEM
91   636  NT AUTHORITY\SYSTEM
```

Figure 3: Screenshot of suspicious processes as evidence of IOCs

When the **Windows Processes** dataset is filtered for suspicious processes in machine **0000DQQEE**, the output are returned as shown in Figure 3. We can observe that net.exe with process ID of 2936 has been executed by **svc_lw**, and the reg.exe process attempting to harvest credentials under the username **NT AUTHORITY\SYSTEM** proves that privilege escalation was unfortunately already succesful.

A minor possible IOC would be the naming convention of the account **svc_lw** due to the 'svc_' prefix. The 'svc_' prefix is commonly used for service accounts, which are often created to run background processes or system services. Attackers frequently create malicious service accounts with legitimate-sounding names to blend in with legitimate system activity, granting themselves persistent access while avoiding detection. Another factor is that by using short, nondescriptive suffixes like ‘lw’, it avoids drawing attention, thus allowing the malicious account to persist on the machine.

Recommendations

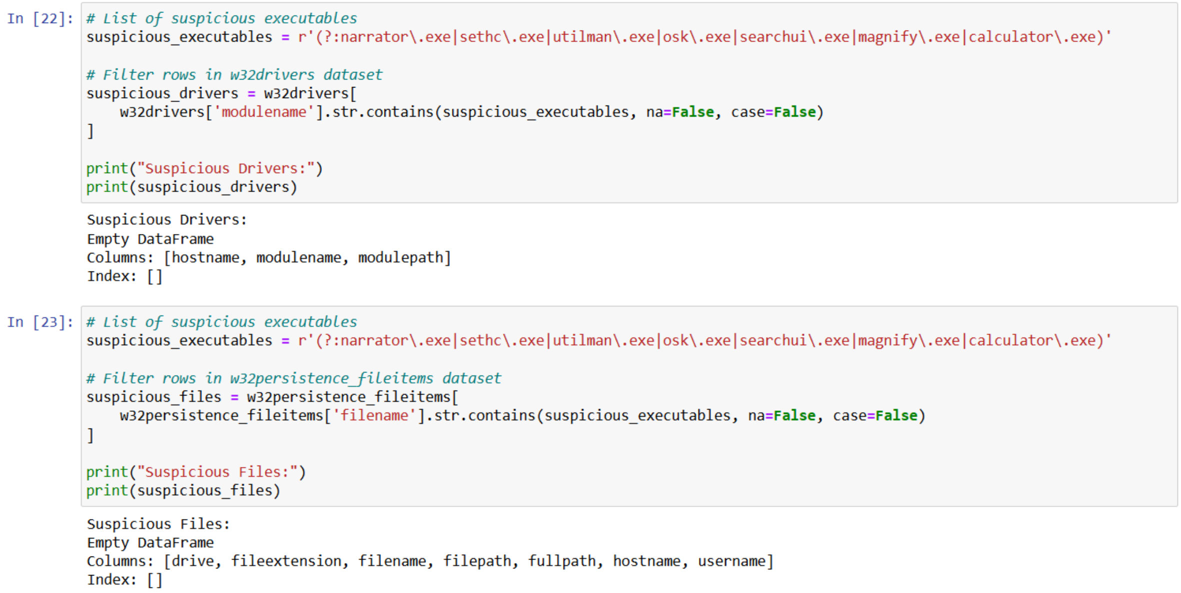
A priority recommendation is to isolate the compromised machine **0000DQQEE** by disconnecting it from the network to prevent further access or lateral movement. Malicious processes like **reg.exe** and **putty.exe** should be terminated after isolating the machine. It is also important to use forensic tools to gather evidence, such as memory dumps and process logs. Any persistence mechanisms, such as scheduled tasks and startup scripts, should be identified and removed.

The compromised credentials for accounts like **svc_lw** and **timotlopez** should be reset, and the **NT AUTHORITY\SYSTEM** account should be audited for misuse or signs of exploitation. Privileges of service accounts, in general, should be limited to only what is necessary for their specific functions. For example, the use of PowerShell and CMD should be restricted for non-administrators. Additionally, policies to restrict access to **lsass.exe** should be configured using Windows’ built-in **Credential Guard**. Created accounts should adhere to standardized naming conventions approved by company management.

To enhance threat detection and response, a **Security Information and Event Management (SIEM)** system should be implemented to centralize and analyze logs from all endpoints and servers. This will help identify unusual activities or patterns indicating a compromise. Furthermore, deploying an **Endpoint Detection and Response (EDR)** solution can provide real-time monitoring, investigation, and remediation of threats on endpoints, helping to detect malicious processes and lateral movement earlier.

Limitations and Constraints

The limitations of this threat hunting investigation is that there were not enough major evidences to prove that machine **0000DQQEE** is fully compromised. Other highly possible IOCs were searched for in their corresponding datasets, and in most cases, no matching results were returned as seen in Figure 4.



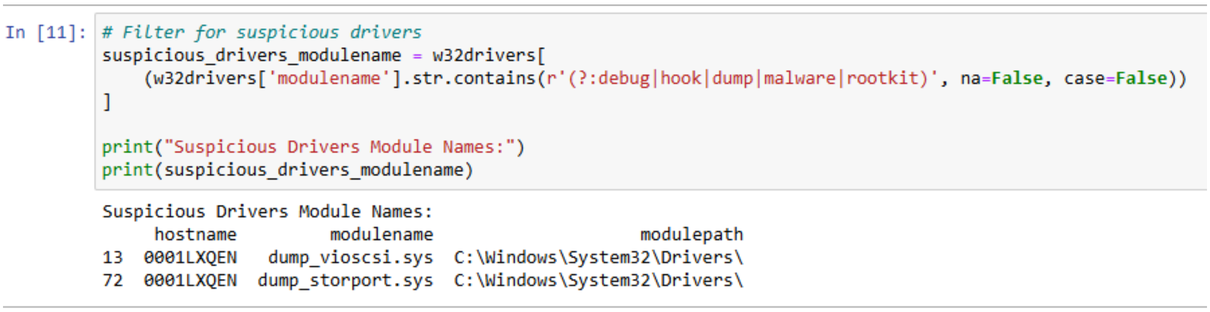
```
In [22]: # List of suspicious executables
         suspicious_executables = r'(?:narrator\.exe|sethc\.exe|utilman\.exe|osk\.exe|searchui\.exe|magnify\.exe|calculator\.exe)'

         # Filter rows in w32drivers dataset
         suspicious_drivers = w32drivers[
             w32drivers['modulename'].str.contains(suspicious_executables, na=False, case=False)
         ]

         print("Suspicious Drivers:")
         print(suspicious_drivers)

         Suspicious Drivers:
         Empty DataFrame
         Columns: [hostname, modulename, modulepath]
         Index: []

In [23]: # List of suspicious executables
         suspicious_executables = r'(?:narrator\.exe|sethc\.exe|utilman\.exe|osk\.exe|searchui\.exe|magnify\.exe|calculator\.exe)'

         # Filter rows in w32persistence_fileitems dataset
         suspicious_files = w32persistence_fileitems[
             w32persistence_fileitems['filename'].str.contains(suspicious_executables, na=False, case=False)
         ]

         print("Suspicious Files:")
         print(suspicious_files)

         Suspicious Files:
         Empty DataFrame
         Columns: [drive, fileextension, filename, filepath, fullpath, hostname, username]
         Index: []
```

Figure 4: Empty search results returned for suspicious executables

Furthermore, supporting evidences like process logs were not included together with the datasets, making certain assumptions probable as discussed in the next section.

Assumptions

An assumption made is using driver names which contains debug, hook, dump, malware or rootkit from the **Windows Drivers** dataset to indicate malicious behavior, as seen in Figure 5 below.

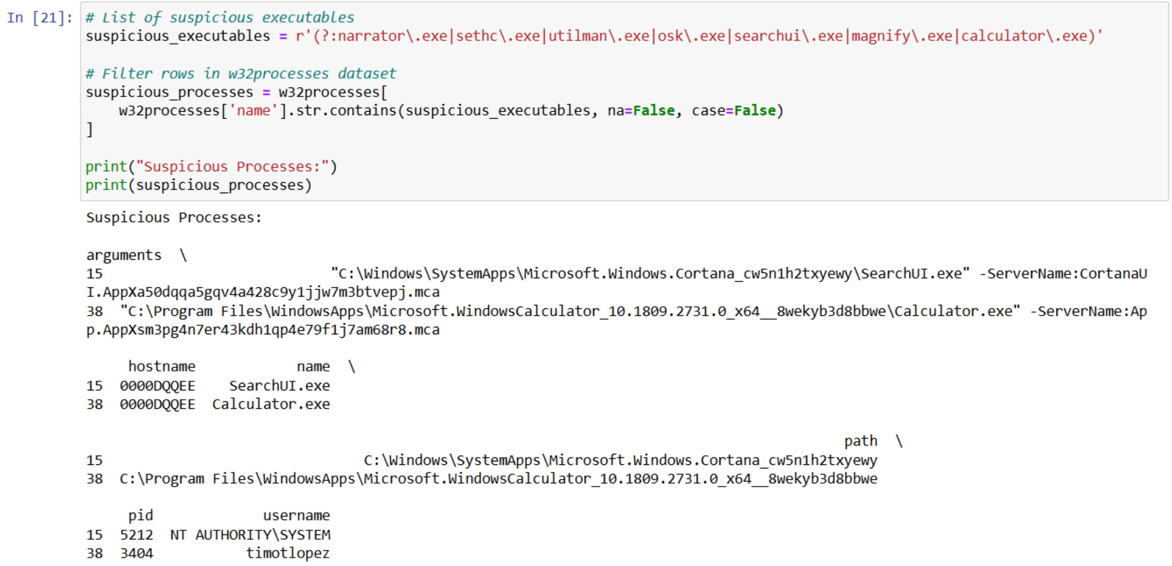


```
In [11]: # Filter for suspicious drivers
         suspicious_drivers_modulename = w32drivers[
             (w32drivers['modulename'].str.contains(r'(?:debug|hook|dump|malware|rootkit)', na=False, case=False))
         ]

         print("Suspicious Drivers Module Names:")
         print(suspicious_drivers_modulename)

         Suspicious Drivers Module Names:
              hostname         modulename                      modulepath
         13  0001LXQEN   dump_vioscsi.sys  C:\Windows\System32\Drivers\
         72  0001LXQEN  dump_storport.sys  C:\Windows\System32\Drivers\
```

Figure 5: Filtered module names of suspicious drivers

However, the same results are obtained from both machines, indicating that the system files are likely to be harmless.

The next assumption is that the **timotlopez** account could be a victim of lateral movement and privilege escalation from the **svc_lw** account as seen in Figure 6. This assumption requires further investigation for solid evidences, since Calculator.exe could just be a benign process.



```
In [21]: # List of suspicious executables
         suspicious_executables = r'(?:narrator\.exe|sethc\.exe|utilman\.exe|osk\.exe|searchui\.exe|magnify\.exe|calculator\.exe)'

         # Filter rows in w32processes dataset
         suspicious_processes = w32processes[
             w32processes['name'].str.contains(suspicious_executables, na=False, case=False)
         ]

         print("Suspicious Processes:")
         print(suspicious_processes)
```

```
Suspicious Processes:

arguments  \
15                           "C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe" -ServerName:CortanaU
I.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca
38  "C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1809.2731.0_x64__8wekyb3d8bbwe\Calculator.exe" -ServerName:Ap
p.AppXsm3pg4n7er43kdh1qp4e79f1j7am68r8.mca

     hostname            name  \
15  0000DQQEE    SearchUI.exe
38  0000DQQEE  Calculator.exe

                                                                                          path  \
15                                 C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy
38  C:\Program Files\WindowsApps\Microsoft.WindowsCalculator_10.1809.2731.0_x64__8wekyb3d8bbwe

     pid             username
15  5212  NT AUTHORITY\SYSTEM
38  3404           timotlopez
```

Figure 6: Suspicious executables related to timotlopez account