**Log Analysis Report**

**Name:- Kundan Keshav Gawande**

**ID:-28806  
   
 Batch Id:- 25VID1318\_Infrasecurity**

**Task 1**

**Log Entry Summary (Sysmon Event ID 10 - Process Access)**

**📌 What This Log Means:**

* **Event ID 10** in Sysmon indicates that **one process has accessed the memory of another process**, which can be used for malicious purposes like credential stealing or process injection.

**🔍 Detailed Breakdown**

|  |  |
| --- | --- |
| Field | Value |
| Rule Triggered | Credential Access - TeamViewer MemAccess |
| Time of Event | 2020-07-24 17:20:29 UTC |
| Computer | LAPTOP-JU4M3I0E |
| Source Process | frida-winjector-helper-32.exe |
| Source Location | C:\Users\bouss\AppData\Local\Temp\... |
| Target Process | TeamViewer.exe |
| Target Location | C:\Program Files (x86)\TeamViewer\TeamViewer.exe |
| Granted Access Rights | 0x147a (Includes memory reading, writing, and process query) |
| Call Trace | Shows DLLs used during access; heavily uses ntdll.dll, wow64.dll, and the injector binary |

**⚠️ Why This Is Suspicious**

* **Frida Injector**: frida-winjector-helper-32.exe is a known tool used for dynamic instrumentation — often leveraged in malware analysis, reverse engineering, and process injection.
* **Targeting TeamViewer**: Accessing the memory of a remote access application like TeamViewer is a red flag. Attackers may try to steal credentials, session tokens, or inject code to hijack sessions.
* **Temporary File Path**: Located in AppData\Temp, which is typical for malware loaders or scripts running unsigned binaries.

**🚨 Security Implications**

| **Threat Type** | **Details** |
| --- | --- |
| **Credential Access** | Could be stealing stored credentials or session tokens from TeamViewer memory |
| **Process Injection** | May attempt to inject code into TeamViewer to gain persistence or control |
| **Lateral Movement / Remote Control** | If successful, attacker may use TeamViewer’s capabilities against the victim |

**🛡️ Recommended Actions**

1. **Immediately investigate the frida injector process:**
   * Is it expected in your environment?
   * If not, this is likely malware or unauthorized research activity.
2. **Check if TeamViewer was accessed or misused** during that time.
3. **Review all other Sysmon logs**:
   * Especially Event IDs **1 (Process Create)**, **3 (Network Connection)**, and **11 (File Create)** around that timestamp.
4. **Isolate the device**, scan it with antivirus and forensic tools.
5. **Review user activity** and accounts for misuse.

**✅ Summary for Your Report**

On **24th July 2020 at 17:20 UTC**, the system detected a suspicious memory access event. A temporary executable (frida-winjector-helper-32.exe) attempted to access memory in the TeamViewer.exe process, indicating a potential credential-stealing or process injection attempt. The process originated from the AppData\Temp directory and used DLL calls commonly associated with injection techniques. This behavior matches the detection rule: **Credential Access - TeamViewer MemAccess**. Immediate investigation and containment actions are recommended.

### ****Task 2****

### ****Log Entry Summary (Security Event ID 4794 – DSRM Password Set)****

#### 📌****What Event ID 4794 Means:****

This event is logged when the **Directory Services Restore Mode (DSRM) password is set or changed**. This is a sensitive operation typically done by administrators and can indicate either:

* Legitimate domain controller maintenance, or
* **Potential unauthorized privilege escalation or backdoor creation** by an attacker.

### 🔍****Detailed Breakdown****

|  |  |
| --- | --- |
| Field | Value |
| ****Event ID**** | **4794** |
| ****Event Description**** | **DSRM account password was changed** |
| ****Time**** | **2017-06-09 19:21:26 UTC** |
| ****Computer**** | **2016DC.HQCORP.LOCAL (likely a Domain Controller)** |
| ****Performed By**** | **User: administrator@HQCORP** |
| ****SID (Security Identifier)**** | **S-1-5-21-...-500 → Indicates built-in Administrator account** |
| ****Logon ID**** | **0x2f336f** |
| ****Workstation**** | **2016DC** |
| ****Status**** | **0x0 (Success)** |

### ⚠️****Security Risk Evaluation****

|  |  |
| --- | --- |
| Risk Factor | Details |
| 🔑****DSRM Account**** | **DSRM is a local admin account on domain controllers, used when booting into restore mode.** |
| ❗****Potential Abuse**** | **An attacker with admin rights could set the DSRM password, then use it to log in offline, dump hashes, or create backdoors.** |
| 🕵️ ****Logged by Audit**** | **Presence of this log proves password was changed, which is rare in normal operations.** |
| 👤****Admin User**** | **Performed by the Administrator account, which should raise concern if unexpected.** |

### 🛡️ ****Recommendations****

1. 🔍**Verify Change Intent:**
   * Was this change expected (e.g., part of regular admin procedure)?
   * If **not planned**, it could be an **indicator of compromise**.
2. 🧑‍💻**Check Logon Sessions:**
   * Review logon sessions (Event IDs **4624**, **4672**) around the same timestamp.
3. 📅**Correlate With Other Events:**
   * Was this preceded by privilege escalation? (Event ID **4670**, **4674**)
   * Any unusual account creation or group membership change? (**4720**, **4728**, etc.)
4. 🧰 **Restrict DSRM Use:**
   * Log and monitor DSRM access.
   * Rotate DSRM password securely if unsure.
5. 📡**Monitor Domain Controller Activity:**
   * Look for new scheduled tasks, services, or process creation (Sysmon Event ID **1**).

### ✅ ****Summary for Your Report****

On **9th June 2017 at 19:21 UTC**, Event ID **4794** was logged, indicating that the **Directory Services Restore Mode (DSRM) password** on domain controller 2016DC.hqcorp.local was successfully changed by the **Administrator** account (S-1-5-21-...-500).  
Since this action grants local admin access to the DC in restore mode, it can be a critical security risk if performed without authorization. This should be reviewed for legitimacy, and all related activity should be audited to rule out compromise or misuse.