Technical Report: Memory Forensic Analysis of the Prolaco Case

Luca Volonterio

January 20, 2026

1 Introduction

This report summarizes the forensic investigation of the memory image `prolaco.vmem`. The analysis focuses on a hidden process utilizing Direct Kernel Object Manipulation (DKOM) to evade standard system monitoring tools.

2 System Identification

The analysis was performed using the following profile:

- **Operating System:** Windows XP Service Pack 2 (x86)
- **Kernel Base Address:** `0x804d7000`
- **Memory Image:** `prolaco.vmem`

3 Process Discovery and DKOM Detection

A cross-view analysis using `pslist`, `psscan`, and `psxview` revealed a high-priority anomaly.

3.1 Unlinked Process Analysis

The process identified as **1_doc_RCData_61** (PID 1336) was found to be hidden from the standard process list:

- **pslist:** False (Hidden from the `ActiveProcessLinks` list).
- **psscan:** True (The `_EPROCESS` structure remains at physical offset `0x0113f648`).

This discrepancy is a definitive indicator of **DKOM**, where the malware manually unlinks itself from the kernel's doubly-linked list of active processes.

4 Module and Handle Analysis

Further investigation into the unlinked process (PID 1336) provided insights into its origin and capabilities.

4.1 Module Unlinking (LDR Manipulation)

Using the `ldrmodules` plugin, the executable was traced to the following path:
`Documents and Settings`
`Administrator`
`Desktop`
`1_doc_RCData_612.exe`. Notably, the `InInit` column returned **False** for this module, indicating that the malware manipulated the `LDR_DATA_TABLE_ENTRY` lists to hide its presence from module-scanning tools.

4.2 Mutex Identification

Analysis of process handles identified a suspicious Mutex (Mutant object):

- **Mutex Name:** `GoogleUpte.exeDm28sf0V@XK$NX8h0u`

The use of a typo-squatted name (GoogleUpte) combined with a unique alphanumeric suffix is a common trait of Trojan-type malware used to ensure only one instance of the infection is running.

5 Network Communication

The `connscan` plugin revealed that the launcher process, **ImmunityDebugger.exe** (PID 1136), established active outbound connections:

- **Local IP:** `172.16.176.143`
- **Remote IP:** `67.208.216.86` (Port 80)

The timing of these connections correlates with the creation of the hidden process, suggesting a C2 (Command and Control) interaction or a multi-stage payload download.

6 Conclusion

The investigation of the `prolaco.vmem` image confirms the presence of a stealthy backdoor. The malware achieved persistence by unlinking itself from the process and module lists in the kernel. The forensic artifacts (specifically the Mutex and the remote C2 IP) provide high-confidence indicators of compromise.