Technical Report: Memory Forensic Analysis of the Cridex Infection

Luca Volonterio

January 20, 2026

1 Introduction

This report outlines the methodology and evidence gathered during the forensic analysis of the memory dump `cridex.vmem`. The investigation aimed to identify malicious activity, compromised processes, and Indicators of Compromise (IoC) related to the Cridex banking trojan.

2 System Identification

The analysis began by determining the correct memory profile using the `imageinfo` and `kdbgscan` plugins. The target system was identified as:

- **Operating System:** Windows XP Service Pack 3 (x86)
- **Dump Timestamp:** 2012-07-22 02:45:08 UTC
- **Memory Architecture:** 32-bit with Physical Address Extension (PAE)

3 Process and Network Analysis

Initial triage using `pslist` and `connscan` revealed critical anomalies within the **explorer.exe** process (PID 1484).

3.1 Suspicious Network Connections

The `explorer.exe` process, which typically manages the user interface and local file system, was found to have established active connections to external IP addresses on non-standard port 8080:

- `172.16.112.128:1038` → `41.168.5.140:8080` (South Africa)
- `172.16.112.128:1037` → `125.19.103.198:8080` (India)

4 Code Injection Detection

The `malfind` plugin confirmed a "Process Injection" attack within `explorer.exe`.
A suspicious memory region was identified at address `0x1460000` with `PAGE_EXECUTE_READWRITE` (RWX) permissions.

4.1 The Significance of the MZ Header

At the start of this memory region, the hexadecimal signature **4D 5A** (ASCII: **MZ**) was discovered.

The **MZ header** (named after Mark Zbikowski) is the mandatory signature for Windows executable files. In a legitimate environment, an MZ header in memory is always associated with a module loaded from the disk and registered in the system's module list. Finding an orphaned MZ header in a private memory allocation is the "smoking gun" of an injection:

1. **Payload Identification:** It proves that an entire, self-contained executable program has been written into the process memory.
2. **Evasion Technique:** By residing inside `explorer.exe`, the malware inherits the trust of a system process, allowing it to bypass firewalls and stay hidden from standard task managers.

5 String Analysis and Malware Identification

Strings extracted from the injected region confirmed the presence of the Cridex trojan. Key artifacts included:

- **Browser Hooking:** References to `PR_Read`, `PR_Write`, and `SSL_ImportFD` (targeting Firefox/NSS).
- **Form Grabbing:** Presence of web tokens such as `__VIEWSTATE` and `__EVENTVALIDATION`.
- **Bot Communication:** An RSA public key used for encrypted communication with the Command & Control (C2) servers.
- **Mutex:** The unique identifier `ACCOUNTING12_1CF266058149A9A8`.

6 Conclusion

The analysis confirms a high-severity infection by the Cridex banking trojan. The malware utilized process injection into `explorer.exe` to maintain a stealthy presence and intercept sensitive user data. The discovery of the MZ header within an RWX memory segment provided the definitive evidence of this unauthorized code execution.