DFIR REPORT – DNA ANALYSIS PORTAL INCIDENT

1. Case Background

A digital forensics investigation was initiated following the suspected compromise of a Windows workstation belonging to a user involved in sensitive investigative work. The user reported receiving a file that claimed to provide access to a DNA analysis portal relevant to an ongoing case. Upon opening the file, no visible browser window or application was launched, leading the user to believe the file was non-functional. Subsequently, a critical investigative file was found to be missing from the system, prompting concerns of a silent cyber compromise. The incident was escalated to the forensic analysis team for in-depth examination.

2. Investigation Objectives

The primary objectives of this investigation were to identify the malicious artifact responsible for the compromise, determine the attacker-controlled infrastructure involved, and accurately attribute the vulnerability exploited during the attack. Additionally, the investigation aimed to reconstruct the execution flow in order to explain the disappearance of sensitive files without obvious user interaction.

3. Evidence Acquisition

The sole forensic artifact provided for analysis was a volatile memory image acquired from the affected system. The memory image, named **ophelia.raw**, was analyzed in a controlled environment using the Volatility 3 Framework. Memory forensics was selected as the primary analysis method due to its ability to reveal in-memory artifacts, execution traces, and transient files that may not be present on disk.

4. System Profiling and Process Analysis

Initial analysis of the memory image revealed that the system was running a 64-bit instance of Microsoft Windows 10 (build 19041). Process enumeration showed a largely normal execution environment, including standard system processes, user applications, and security services. No overt signs of malware injection or process hollowing were observed. This suggested that the attack relied on trusted system components rather than custom malicious executables.

5. File System Artifact Discovery

Given the social engineering aspect described in the incident, analysis focused on Windows shortcut and Internet Shortcut (.url) files, which are commonly abused to disguise malicious execution as benign links. A memory-based file scan identified a suspicious file located at **C:\Users\Igor\Documents\Important Links\dna_analysis_portal.url**. The filename and location closely matched the description of the file received by the user.

6. File Extraction and Content Analysis

The identified Internet Shortcut file was extracted directly from memory using its virtual address. Examination of the recovered file contents revealed that the shortcut did not reference a web URL. Instead, it pointed to a legitimate Windows diagnostic binary, **iediagcmd.exe**, while redirecting the working directory to a remote UNC path hosted on an external WebDAV server. The shortcut was also configured to display a Microsoft Edge icon, increasing the likelihood of user trust.

7. Execution Flow and Malicious Behavior

When the user opened the Internet Shortcut file, Windows executed the referenced trusted binary. Due to the manipulated working directory, subsequent execution attempts caused Windows to retrieve additional resources from the attacker-controlled WebDAV share at **\\10.72.5.205\webdav\**. This technique allowed the attacker to introduce malicious behavior without dropping obvious malware to disk. The lack of visible indicators explains why the user did not immediately suspect compromise.

8. Exploited Vulnerability

The observed attack behavior precisely matches **CVE-2025-33053**, a Microsoft Windows vulnerability that enables execution hijacking through crafted Internet Shortcut (.url) files. This vulnerability allows attackers to bypass security prompts and redirect execution flow to attacker-controlled remote directories, such as WebDAV shares, by abusing trusted system binaries. The exploitation of this CVE fully accounts for the silent nature of the compromise.

9. Indicators of Compromise (IOCs)

Indicator Type	Value
Malicious File	dna_analysis_portal.url
Remote IP Address	10.72.5.205
Protocol	WebDAV
Abused Binary	iediagcmd.exe
CVE	CVE-2025-33053

10. Conclusion

This investigation confirms that the affected system was compromised through a malicious Internet Shortcut file masquerading as a legitimate DNA analysis portal link. By exploiting CVE-2025-33053, the attacker successfully leveraged trusted Windows components and a remote WebDAV server to achieve execution without raising immediate suspicion. This technique explains both the absence of visible malicious activity and the subsequent disappearance of sensitive files.

11. Final Flag

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