Ophelia – DFIR Write-up

Description

A detective at Moscow PD, Department 19, receives a message asking him to check the forensic analysis portal for a DNA report. Attached to the message is a file containing a link to the portal. He opens the attachment, but initially, nothing seems to happen, so he overlooks it. Later, he realizes that a crucial file from an ongoing case has gone missing.

He has provided the forensic artifacts from his computer to you, his colleague at the cyber forensics department, to figure out what went wrong. Find:

- The filename of the attachment
- The ip from where the malware was executed
- The CVE the attacker exploited

Flag format: nite{file_name.ext_XXX.XXX.XXX.XXX_CVE-XXXX-XXXXX}

Evidence Used

• Memory dump: ophelia.raw
• Analysis tool: Volatility 3
• Operating system: Windows 10 (Build 19041)

The memory capture timestamp showed the incident occurred on December 7th, 2025 at 14:00:47 UTC.

Locating the Attachment

Since there are talks about a DNA report, I started by looking for files that matched this theme and `url` files stood out immediately since they can be abused to execute local binaries instead of just opening websites.

Using Volatility's `filescan` plugin and filtering for anything related to DNA

```
python vol.py -f ophelia.raw windows.filescan | findstr /i dna
```

I found **`dna_analysis_portal.url`** inside the user's Documents directory under a folder named `Important Links`.

File Extraction and Inspection

I extracted the file from memory using its virtual address `0xc201a703b260`

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

Inspecting the shortcut showed multiple red flags. The URL field pointed to `URL=C:\Program Files\Internet Explorer\iediagcmd.exe`, a legitimate Windows diagnostic binary. The working directory was set to a remote WebDAV share, the icon was spoofed to look like `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`, and the shortcut was configured to launch minimized.

Attack Behavior

This attack relies on abusing `iediagcmd.exe` as a LOLBin. When the user opens the shortcut, Windows launches the signed binary while setting the working directory to an attacker-controlled WebDAV server. Due to Windows search order behavior, a malicious `route.exe` binary is loaded remotely and executed without ever being written to disk.

Exploited Vulnerability

The technique used here maps directly to CVE-2025-33053, a Windows shortcut vulnerability that allows arbitrary code execution by abusing the `WorkingDirectory` field in `.url` files.

Network Indicators

The WebDAV share hosting the malicious payload was located at IP address `10.72.5.205`. This system acted as the remote execution source for the attack.

Summary

- Initial infection vector: `dna_analysis_portal.url`
- Attacker IP: `10.72.5.205`
- CVE exploited: `CVE-2025-33053`
- LOLBin abuse: iediagcmd.exe
- Payload: route.exe

Final Flag

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