IRWPX Challenge - Noarlunga

Narrative: We think a cyber criminal gang used a malicious document to exfiltrate some data from our system. Bonus points if you can figure out which CVE this traffic is linked to!

OFPOR TTPs

|  |
| --- |
|  |

BLUFOR TTPs

|  |
| --- |
|  |

Word Picture

|  |
| --- |
|  |

RFIs

|  |
| --- |
|  |

IRWPX Solution

Artefact: Malware Traffic Analysis 2025-01-09 (THURSDAY): **CVE-2017-0199** XLS --> HTA --> VBS --> STEGANOGRAPHY --> DBATLOADER/GULOADER STYLE MALWARE

OFPOR TTPs

|  |
| --- |
| T1189, T1190, T1105, T1204, T1027, T1071.001, T1048, T1041, T1555.003, T1005 (T1005 is hard to get, but can be implied from the stealer activity) |

BLUFOR TTPs

|  |
| --- |
| D3-NTSA, D3-WSAA |

Word Picture

|  |
| --- |
| The Suricata logs show host 10.1.9.101 engaging in clear signs of malware infection and data exfiltration. The system downloaded HTA and VBS scripts from external IPs, likely as part of a drive-by or phishing-based infection chain. It received Base64-encoded payloads consistent with ReverseLoader exploit kit activity and performed external IP lookups, typical of stealer malware verifying connectivity. Subsequent alerts confirm AgentTesla activity, including C2 communication and data exfiltration via FTP and TCP to remote servers. Overall, the traffic indicates an AgentTesla stealer compromise, involving payload delivery, execution, and credential theft followed by network exfiltration. |