IRWPX Challenge - Nectarine

Narrative: We think that some script in pages from legitimate but compromised websites leads to fake CAPTCHA style pages and Clipboard Hijacking. These pages ask users to paste malicious script into a Run window.

OFPOR TTPs

|  |
| --- |
|  |

BLUFOR TTPs

|  |
| --- |
|  |

Word Picture

|  |
| --- |
|  |

RFIs

|  |
| --- |
|  |

IRWPX Solution

Artefact: Malware Traffic Analysis 2025-04-04 (FRIDAY): KONGTUKE ACTIVITY

OFPOR TTPs

|  |
| --- |
| T1189, T1190, T1059.001, T1071.004, T1071.001, T1573, T1590.005 |

BLUFOR TTPs

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

Word Picture

|  |
| --- |
| The Suricata logs show host 10.4.4.101 engaging in multiple suspicious activities between 03:14 and 03:18. It queried malicious domains (including \*.top and exploit-kit sites), executed PowerShell with outbound HTTP requests, and communicated with known C2 servers linked to TA582 and AsyncRAT/zgRAT malware. The host also performed repeated external IP lookups using ipify, dyndns, and ipinfo—typical of infected systems establishing outbound control. Indicators suggest initial exploitation, PowerShell-based execution, and active command-and-control over HTTP/S and DNS channels. Overall, the logs strongly indicate a compromised Windows system performing malware beaconing and potential exfiltration. |