Auntie Hecker Threat Network Report (Public Redacted Version)

This document summarizes public-facing findings from captured HAR sessions, packet data, and router interface artifacts reviewed as part of the Auntie Hecker investigation.

KEY OBSERVATIONS:

1. THREAT DOMAINS INVOLVED

- dotdaplug.com
- remotewd.com
- waconazure.com
- support-global-it-ss.com
- coolbreeze.eu.org
- hosting-global-it-ss.com

2. POTENTIAL LEGITIMATE SERVICES CO-OPTED

- shaw.ca (used to mask interface abuse)
- akamaiedge.net (CDN hiding)
- cloudflare IPs

3. ARTIFACTS OF INTERFACE SPOOFING

- Shaw-branded image files embedded in pages that also triggered connections to known C2 domains
- Use of images and JS requests in non-standard ways (e.g., tracking via .png requests)

4. NETWORK STRUCTURE

- A central device routed traffic to both legitimate and malicious services
- Visual network diagram confirms split between safe and suspicious connections

5. RISK SUMMARY

- Evidence suggests infection was present at a critical network junction
- DNS abuse and transparent redirect tactics may have been in use
- Activity appears stealthy, persistent, and coordinated

RECOMMENDED ACTIONS:

- Replace any networking hardware involved
- Audit all connected devices
- Block listed domains using DNS sinkholing or firewall rules
- Use a clean, isolated network for investigation going forward

NOTE:

This report is safe to publish publicly and contains no device identifiers, IPs, or usernames.

--- END PUBLIC REPORT ---