Braylock Global — DNS Threat Defense Briefing

Overview:
Recent exploits involving DNS TXT records have demonstrated how attackers can embed malware payloads within DNS queries. These include executable headers, stagers, and disguised binary fragments that bypass standard perimeter defenses and may infiltrate endpoint or API-based systems silently.

Threat Vector Details:
- Malicious DNS TXT records can contain Base64-encoded executables, 'magic byte' headers, or scripts.
- Common targets include auto-resolving systems, unsecured API calls, or agents parsing TXT data.
- Attackers exploit DNS’s trusted status and lack of deep inspection in most environments.

Braylock Defense Protocol:
- Strict DNS TXT sanitization filters across Cortex-PrimeQ OS, WhisperLink, SentientX, and CFOCore.com.
- Signature-based 'magic byte' scanning integrated into DNS resolution logic.
- All DNS interactions routed through secure resolver layers with TXT record parsing disabled by default.
- AuditMode.AI integration logs, hashes, and monitors all DNS interactions for forensic trails.
- Network segmentation enforced to block outbound recursive DNS calls from AI agents.

Security Outcome:
→ Braylock products are now hardened against DNS TXT payload delivery vectors.
→ No raw external TXT records can trigger AI execution, memory parsing, or downstream API chain events.
→ DNS forensics is now embedded into AuditMode.AI certification for all Braylock IP assets.

This protocol ensures Braylock Global’s platforms are protected against one of the stealthiest emerging malware vectors, reinforcing investor confidence and sovereign trust alignment.

Contact: gpmiddleton71@gmail.com
Visit: https://braylockglobalai.com