Mobile Threat of the Month

January 2025

DNS Injection Attacks Increasing on Mobile

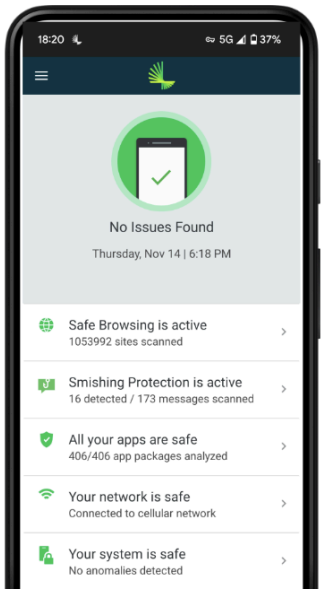
How it works

DNS injection attacks use fingerprinting techniques to gather information about devices on a network by analyzing DNS queries. With most Internet traffic now encrypted and most websites implementing secure headers, attackers are turning their attention to DNS, where most queries are still unencrypted and easy to manipulate.

Potential Impact

Using rudimentary tools, attackers can exploit unencrypted DNS queries generated by mobile devices to perform fingerprinting. This process enables them to identify and map the applications, services, and systems used within your organization. Through DNS injection, malicious actors can intercept DNS traffic, exfiltrate sensitive data, or redirect mobile devices to fraudulent websites or backend systems by injecting manipulated responses into DNS queries. Such attacks can facilitate credential theft, session hijacking, or other malicious activities, ultimately elevating the risk of a data breach.

How to protect your mobile device



You can mitigate the risks of DNS fingerprinting and DNS poisoning by utilizing a secure DNS provider. Encrypted DNS requests ensure that your device's queries remain private and protected from interception. This encryption prevents unauthorized access to query data and eliminates the risk of tampering with DNS responses provided by the local DNS configuration.

Lookout Mobile Security (MES) provides unrivalled visibility and protection against mobile threats targeting iOS, Android and ChromeOS devices with the world's largest AI-driven mobile security dataset. This includes robust detection and prevention capabilities against mobile network attacks, including DNS injection.

Source: Lookout Mobile Threat Spotlight Article