Lookout

Mobile Threat of the Month

November 2025

Herodotus Android Trojan

Herodotus is a potent Android banking trojan that steals credentials, intercepts one-time passcodes, and grants attackers full remote control over an infected device. It features a sophisticated evasion technique designed to bypass behavioural anti-fraud solutions. Consciously delaying credential input at random intervals, it mimics human typing and avoids being flagged for machine-like speed. This malware is sold as a Malware-as-a-Service (MaaS) on underground forums, making it accessible for widespread global campaigns.

How it Works

The attack follows a clear, multi-stage process:

1. Lure: The victim receives a text message (SMS) creating a sense of urgency (e.g., a fake bank alert, a delivery notification). This initial message typically contains a link.

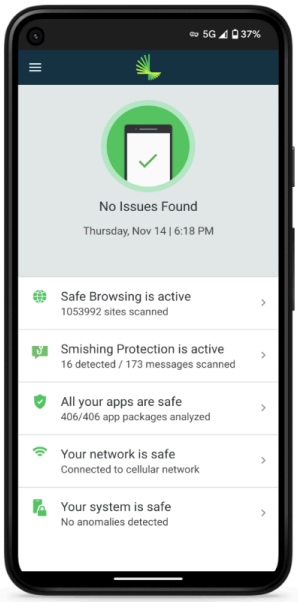
2. Download: The link directs the user to a web page prompting them to download and install a malicious Android application (APK) from outside the official Google Play Store. The app is often disguised as a "security update" or a required banking application.

3. Infection & Takeover: Once installed, the app seizes full control of the device. It can now operate in the background, read the screen, intercept SMS (including 2FA codes), and display fake overlay screens on top of legitimate apps to steal login credentials.

Lookout Mobile Security

Lookout is designed to protect businesses from complex threats like the Herodotus Trojan by providing a layered defence for iOS and Android devices that addresses each stage of the malware's attack chain.

Phishing and Content Protection: This feature automatically scans links from any source, including SMS messages, email, and messaging apps. When an employee clicks a link, Lookout checks the URL in real-time against its global threat intelligence network, identifies the link as malicious and blocks the user from accessing fake websites where malware is hosted.



AI-Based Smishing Detection: For more advanced attacks that may not use a previously known bad link, Lookout uses AI to analyse the content and intent of the message itself. It can detect suspicious language, a "sense of urgency" (e.g., "Your bank account is locked, click here"), and other social engineering red flags to proactively warn the user and IT.

App Threat Protection: If somehow phishing protection was bypassed, Lookout's platform continuously scans all apps on the device, including those "sideloaded" from outside the official Google Play Store. The Herodotus app would be flagged as a Trojan or malware based on its code, signatures, and known malicious behaviours.

Containment: Most importantly, Lookout can trigger a Conditional Access policy. The infected device is immediately assessed as "non-compliant" or "high-risk," which automatically blocks its access to all company resources—such as email, company files, and internal apps—until the Herodotus Trojan is fully removed.