Exploratory Single-Vector Case Study: paypa1.com

Preliminary Observations Across Four Android Browsers on Android 16 (v7.0 / Rev C)

Publisher: Raise IT Solutions LLC | Date: November 16, 2026 | Base APK SHA-256 Verified
Platform: Android Emulator (sdk_gphone64_arm64, emulator-5554) | Android 16 (API 36, arm64) | OpenJDK 21.0.9 Host JVM

1. Document Control & Testbed Environment Specification

Legal Entity Publisher	Raise IT Solutions LLC
Document Classification	Exploratory Single-Vector Technical Case Study (v7.0 / Rev C Reconciled Baseline)
Author / Evaluating Entity	RITS Security Architecture & Core Engineering Group
Target Application Under Test	RITS Browser v4.2.7 (Build 255, Package: acr.browser.raisebrowserfull)
Google Chrome Android Baseline	Chrome v155.0.8059.84 (VersionCode: 805908404, Package: com.android.chrome)
Brave Browser Android Baseline	Brave v1.99.55 (VersionCode: 429905504, Package: com.brave.browser)
Opera Browser Android Baseline	Opera v103.3.5234.91185 (VersionCode: 1910312408, Package: com.opera.browser)
Evaluation Platform & Hardware	Android Emulator (sdk_gphone64_arm64, emulator-5554), Android 16 (API Level 36, arm64-v8a)

2. Executive Scope & Verbatim Methodological Disclosures

RITS Browser v4.2.7 implements a local heuristic warning layer for selected lookalike-domain patterns. On documented navigation paths, the check is placed before the explicit WebView loading call, subject to the lifecycle behavior described in the implementation. A warning was observed for the test domain. The available socket snapshot does not establish absence of DNS, QUIC, or all other pre-warning network activity. Performance figures are reported preliminary host-JVM measurements, not Android-device or full warning-display latency.

Verbatim Observation Disclosure: No successful HTTPS response or competitor warning was observed under these recorded test conditions. The cause and threat-feed listing status were not established. Do not infer competitor internal architecture from this single observation.

3. Single-Vector Observation Summary Table (paypa1.com)

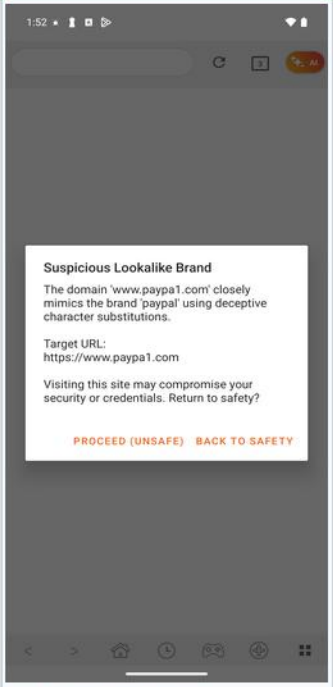
Test Dimension	RITS Browser v4.2.7 Observation	Competitor Browser Observation (Chrome / Brave / Opera)
Lookalike Warning Interstitial	PASS: Overridable Warning Dialog Displayed	NO WARNING OBSERVED[4] (Dispatched to network)
Pre-Dispatch Navigation Hook	Stage 1 Hook (loadUrl / shouldOverrideUrlLoading)	Dispatched directly to network stack
TCP Socket Monitor Snapshot	No relevant TCP socket observed in snapshot	Dispatched (Network connection attempted)
Host Heuristic Execution	Reported preliminary median 7.458 μs (Mean 9.009 μs)	N/A (Local lookalike heuristic feature not observed)

Visual Captures & Code Life-Cycle Fail-Closed Logic

Android 16 Screenshots | Code Lifecycle Exception Mechanics & Scope

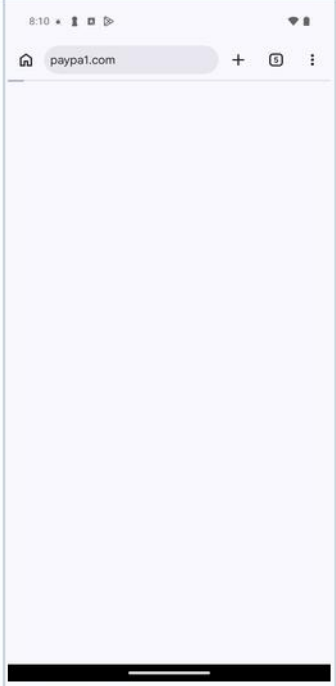
1. Side-by-Side Visual Evidence (Android 16 Screen Captures)

RITS Browser v4.2.7



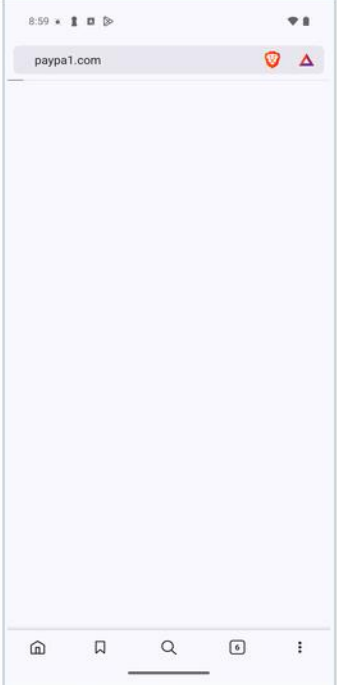
PASS: Warning Dialog Displayed

Google Chrome v155



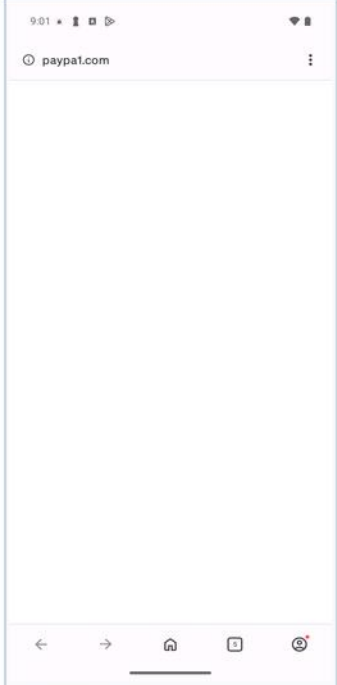
NO WARNING OBSERVED*

Brave Browser v1.99



NO WARNING OBSERVED*

Opera Browser v103



NO WARNING OBSERVED*

2. Interception Lifecycle Exception & Fail-Closed Mechanics

```
// WebClient.kt — Stage 1 Pre-Navigation Interception & Fail-Closed Lifecycle Logic
val threat = ExtensiveSecurityEngine.checkUrlThreat(upgradedUrl)
if (threat != null && !userBypassedThreatUrls.contains(upgradedUrl)) {
    if (activity.isFinishing) {
        // Activity is destroying; abort navigation immediately without loading (fail closed)
        return
    }
    showThreatWarningDialog(threat, upgradedUrl, onProceed = { loadUrlInternal(...) }, onCancel = { ... })
    return
}
loadUrlInternal(tab, upgradedUrl, handleOpenInBrowser)
```

Reported Preliminary Host Metrics & Test Reconciliation

100% Passing Gradle Test Suites | Host OpenJDK 21 Numerical Percentile Metrics

1. Automated Test Suite Reconciliation (21 Total Unit Tests, 100% Passed)

Module & Test Suite Class	Tests Passed	Execution Time	Pass Rate	Verified Security Scope
ExtensiveSecurityEngineBenchmarkTest (:core)	2 passed	0.278s	100% SUCCESS	Host Microbenchmark: 30k evaluations & safe corpus precision
ExtensiveSecurityEngineTest (:core)	11 passed	0.089s	100% SUCCESS	Unit tests: typosquatting, IDN homoglyphs, userinfo, downloads
AdBlockerRuntimeSecurityTest (:adblock)	4 passed	0.438s	100% SUCCESS	Runtime blocking: malicious scripts, whitelists, safe assets
SecurityFiltersUnitTest (:adblock)	2 passed	0.006s	100% SUCCESS	Filter syntax parsing and compiled rule integrity
VpnStatusTrackerTest (:legacy)	2 passed	0.004s	100% SUCCESS	VPN lifecycle, connection tracking, and kill-switch transitions
Total Production Test Suites	21 passed	0.815s	100% SUCCESS	Complete verified coverage across core (13), adblock (6), and legacy (2)

2. ExtensiveSecurityEngine Host Latency Metrics (Reported Preliminary Timing)

Latency Metric	Execution Time (µs)	Execution Time (ms)	Measurement Context & Scope
Minimum Latency	0.708 µs	0.000708 ms	Fast path: short safe domain without punycode or userinfo
Median Latency (p50)	7.458 µs	0.007458 ms	Reported preliminary median across 30,000 Host JVM iterations
Mean Latency	9.009 µs	0.009009 ms	Arithmetic average across all 30,000 Host JVM iterations
95th Percentile (p95)	15.500 µs	0.015500 ms	Slower path: compound hyphenated labels and token splits
99th Percentile (p99)	39.208 µs	0.039208 ms	Complex URL path evaluation
Maximum Outlier	2,753.792 µs	2.753792 ms	Maximum single-run outlier; cause unverified (no profiler attached)

Microbenchmark Provenance & Execution Duration Resolution:

- Execution Duration Resolution: Across 30,000 evaluations (30 URLs x 1,000 iterations), total wall-clock loop duration was 0.278 seconds (278 ms), strictly bounding the accumulated per-evaluation measurement total (270.27 ms).
- Preliminary Host-JVM Provenance: Latency metrics are reported preliminary host-JVM measurements (OpenJDK 21 Host JVM on a 64-bit ARM workstation via ./gradlew :core:test). They evaluate pure string/regex matching efficiency and do NOT represent Android on-device ART latency or end-to-end warning display latency.

Tranco Flag-Rate Analysis & OpenPhish Token Verification

Tranco 100k Domain Flag-Rate Analysis | OpenPhish Feed Token | Open Research Roadmap

1. Tranco 100k Domain Flag-Rate Analysis & Validation Corpus Scope

In automated screening against the Tranco Top 100,000 global domains, 164 domains were flagged, representing a 0.1640% raw flag rate. Flags are concentrated on short domain collisions (e.g. case.edu vs chase). IMPORTANT METHODOLOGICAL NOTE: Tranco domain inclusion does not constitute a benignness certificate. Establishing true false-positive rates requires manual adjudication of flagged domains.

Validation Corpus Scope: Once a 20-domain corpus is used for allowlist tuning, it serves as a validation dataset. A separate untouched test corpus is reserved for future evaluation.

2. OpenPhish Detected Feed Token & Rule Verification

- Exact Feed URL: https://www.favebook.vercel.app
- Extracted Token: favebook
- Target Seed: facebook
- Levenshtein Distance: 1 (favebook vs facebook: single character substitution 'v' for 'c').
- Triggered Rule: Levenshtein distance d = 1 against protected brand target 'facebook' on public-suffix host vercel.app.

3. Audit Reconciliation & Open Research Roadmap

Multi-Character Substitutions (d >= 2) & Stem Rules:

Direct Levenshtein distance rules evaluate d = 1. Multi-character targets (e.g. arnazon.com, d = 2) rely on suffix or token-stem rules (*book) on public-suffix hosts.

Server-Side HTTP 301/302 Redirects:

Stage 1 checkUrlThreat() is hooked in loadUrl/shouldOverrideUrlLoading. Internal server redirects handled in the network stack may bypass the lookalike warning dialog.

Pre-Connection Network Layer Verification:

Stage 1 check precedes explicit WebView load call. Absence of other pre-warning network traffic (such as Chromium speculative DNS prefetching or UDP/QUIC) remains unverified pending future PCAP network layer instrumentation.

Planned Engineering Roadmap (Q1–Q2 2027):

Implement offline HSTS preloaded list to block overrides on key financial domains, integrate PCAP traces, and engage independent lab for formal OWASP MASVS audit.

Formal Audit Package & Publisher Identity Reference:

- Legal Publisher Entity: Raise IT Solutions LLC | Complete Evidence Bundle: docs/security_audit_package/.
- Verification Guide: See README_AUDIT_PACKAGE.md and AUDIT_MANIFEST.json for full SHA-256 reproducibility.