Application Layer Protocol, Technique T1437 - Mobile

Archived: 2026-04-05 12:58:44 UTC

Sub-techniques (1)

Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the mobile device, and often the results of those commands, will be embedded within the protocol traffic between the mobile device and server.

Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS.

Tactic Type: Post-Adversary Device Access

ⓘ

Platforms: Android, iOS

Last Modified: 24 October 2025

Procedure Examples

Mitigations

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Detection Strategy

ID	Name	Analytic ID	Analytic Description
DET0685	Detection of Application Layer Protocol	AN1793	Abuse of standard application protocols can be difficult to detect as many legitimate mobile applications leverage such protocols for language-specific APIs. Enterprises may be better served focusing on detection at other stages of adversarial behavior.
		AN1794	Abuse of standard application protocols can be difficult to detect as many legitimate mobile applications leverage such protocols for language-specific APIs. Enterprises may be

ID	Name	Analytic ID	Analytic Description
			better served focusing on detection at other stages of adversarial behavior.

References

1. ThreatFabric. (2023, December 21). Android Banking Trojan Chameleon can now bypass any Biometric Authentication. Retrieved July 7, 2025.
2. Albrecht, J., Islamoglu, A. (2025, July 21). Lookout Discovers Iranian APT MuddyWater Leveraging DCHSpy During Israel-Iran Conflict . Retrieved September 19, 2025.
3. A. Kumar, K. Del Rosso, J. Albrecht, C. Hebeisen. (2020, June 1). Mobile APT Surveillance Campaigns Targeting Uyghurs - A collection of long-running Android tooling connected to a Chinese mAPT actor. Retrieved November 10, 2020.
4. Cyble. (2022, October 27). Drinik Malware Returns With Advanced Capabilities Targeting Indian Taxpayers. Retrieved November 17, 2024.
5. Kucherin, G., et al. (2023, June 21). Dissecting TriangleDB, a Triangulation spyware implant. Retrieved April 18, 2024.
