zLABS™

2026 zLabs Year in Review

The Evolution of Mobile Attacks: AI-Assisted Malware, Device Takeover and Enterprise Threats



Key investigations and mobile security priorities for 2027

Research period: January 1 through November 1, 2026
Published: November 17, 2026

ZIMPERIUM®

Executive Summary

Cybercriminals are leveraging sophisticated and easily accessible AI to supercharge their attacks and their primary target is also the most vulnerable: Mobile. Mobile apps and devices are the least protected attack surface, while also being the gateway to most users' corporate and personal identities, enterprise network access and even banking transactions.

Zimperium's 2026 Global Mobile Threat Report documented a 380% increase in phishing attacks detected specifically on employee mobile devices. Throughout 2026, Zimperium's zLabs threat research team exposed the techniques behind attackers' attempts to compromise mobile devices and applications, including AI-assisted malware execution, browser-based iOS exploitation and real-time payment manipulation.

The research identifies five priorities for enterprise security:



AI-assisted malware
Generative AI helps malware interpret device interfaces, avoid traditional detection methods and automate interactions.



Browser-based iOS exploitation
Exploit chains target vulnerable devices through webpages without requiring application installation.



Financial fraud and corporate access
Attackers manipulate transactions and target enterprise credentials.



Persistent surveillance and extortion
Malware combines data theft, remote control and ransomware capabilities.



Shadow AI and application risk
New AI capabilities and AI-generated code require organizations to reassess application security and data exposure.

In 2027, organizations must move beyond traditional enterprise defenses to address a mobile-first attack strategy increasingly powered by AI. That requires dedicated, AI-empowered mobile security to detect threats on devices, identify application vulnerabilities and protect apps during use. By stopping threats where they occur, organizations can prevent mobile compromise from becoming a gateway to corporate accounts, sensitive data and financial fraud.

2026 zLABS YEAR IN REVIEW

2026 Mobile Threat Landscape

Growth by the Numbers

Zimperium's 2026 Global Mobile Threat Report reveals significant growth in mobile phishing, malicious link engagement and spyware.



Mobile Phishing

380%

Increase in detected phishing events on employee mobile devices since January 2025.



Malicious-Link Clicks

110%

Increase in devices where employees clicked malicious links in 2025 vs. 2024.



Mobile Spyware

4x+

Year-over-year increase in spyware presence on mobile devices.



What the Findings Reveal

Mobile threats are expanding across multiple attack vectors, increasing the importance of detecting malicious activity and protecting the devices employees rely on for business access.

Source: Zimperium, 2026 Global Mobile Threat Report, July 2, 2026. Metrics reflect different measurement periods and populations.

2026 zLabs Research Highlights

Four investigations reveal how mobile threats are advancing through AI-assisted automation, extensive device control and persistent malicious infrastructure.



AI-ASSISTED MALWARE

RatHat

AI-Powered Navigation

Uses generative AI to interpret Android device interfaces and assist navigation during malware execution.



BANKING MALWARE

ToxicPanda 2.0

167
Remote Commands

Credential overlays target 349 financial institutions.



DEVICE TAKEOVER

Rokarolla

217
Financial Apps Targeted

Targets banking and cryptocurrency apps and supports 137 commands.



REMOTE ACCESS TROJAN

Arsink RAT

1,216
Distinct APK Hashes

317 Firebase Realtime Database endpoints identified during the investigation.



What the Research Reveals
Attackers are expanding their ability to interact with, control and exploit mobile devices creating new challenges for detecting threats and protecting sensitive information.

Source: Zimperium zLabs, selected 2026 investigations. Figures represent separate research measures.

1 AI is Becoming Part of Mobile Malware Execution

AI's role in cyberattacks extends beyond creating convincing messages or assisting with code development. The RatHat investigation provides a concrete example of generative AI being used within mobile malware operations.

RatHat captures information about the device's interface and uses generative AI to help locate elements and guide navigation. This allows interface interactions to rely on interpretation of the current screen rather than fixed coordinates alone.

The malware combines this capability with Android Accessibility abuse and Wireless Debugging self-pairing to obtain shell-level access. It also deploys a background component that operates outside the malicious application's lifecycle and can reinstall the application after removal.

Featured Investigation: RatHat
Published: September 16, 2026

What zLabs documented

- Generative AI used to interpret interface elements and support navigation.
- Accessibility abuse to automate changes to device settings.
- Wireless Debugging abuse to obtain shell-level access.
- Credential theft through overlays, input monitoring and authentication-code interception.
- A persistence mechanism capable of restoring the malicious application after removal.

Why it Matters

RatHat illustrates how AI-assisted interface navigation can operate alongside credential theft and persistence mechanisms. Under the conditions described in the investigation, removing the visible malicious application may not eliminate every component of a compromise.

For security teams, the investigation reinforces the need to assess device behavior and integrity throughout an incident, including after an apparent removal.

RatHat also highlights the importance of operating-system-level visibility in investigating advanced mobile threats. By abusing Wireless Debugging to establish shell-level access and deploy components outside the application's lifecycle, the malware demonstrates why security teams need visibility beyond the application sandbox. Correlating device behavior with security and network telemetry can help investigators reconstruct attack activity, identify persistence mechanisms, and assess the full scope of a compromise.

2 Device Control Expands Financial Fraud Capabilities

The financial investigations reviewed here demonstrate several routes to fraud. Some threats use overlays to capture credentials. Others provide extensive remote control or intervene directly during a payment.

These capabilities require financial institutions to consider the security of the device where a customer initiates and authorizes a transaction, alongside the security of the account and application.

Featured Investigation: PixRevolution
Published: March 11, 2026

PixRevolution targets Brazil's PIX payment system. The malware monitors the victim's screen and enables a remote operator to intervene during a transfer, redirecting funds while the victim proceeds through what appears to be a familiar payment interaction.

Why it Matters

The legitimate user can initiate a transaction while an attacker manipulates its outcome. This creates a security challenge that extends beyond identifying a stolen password or an unfamiliar login.

Featured Investigation: ToxicPanda 2.0
Published: August 19, 2026

zLabs identified an updated ToxicPanda variant with 167 remote commands and credential-stealing overlays associated with 349 targeted financial institutions. Separately, the research describes PIN theft targeting more than 140 banking and cryptocurrency applications. The variant also includes Accessibility abuse and a mechanism for enabling Wireless Debugging.

Why it Matters

The investigation shows an established malware family expanding both its targeting and its operational capabilities. Organizations must account for updates to known threats as well as newly identified malware.

Supporting Investigation: Rokarolla
Published: June 16, 2026

Rokarolla targets 217 banking and cryptocurrency applications and includes 137 commands. Its capabilities include lock-screen credential theft, keylogging, SMS collection and fraudulent overlays, alongside mechanisms designed to interfere with user intervention.

Why it Matters

Extensive device control gives attackers multiple ways to collect sensitive information and facilitate fraud. A single compromised phone can expose more than one financial application.

3 Mobile Phishing Targets Enterprise Identity

Mobile threats also affect enterprise identity. Employees routinely open messages, follow links and sign into business services from their phones, creating opportunities for attackers to present fraudulent authentication requests.

RecruitTrap illustrates how a phishing campaign can tailor its experience to mobile users while deliberately seeking corporate credentials.



Featured Investigation: RecruitTrap
Published: August 24, 2026

Building on earlier third-party reporting of recruitment-themed phishing, zLabs conducted extended analysis of the campaign and documented fake login flows that adapt to the victim's device. On mobile, the attack presents a full-screen counterfeit login page in place of the simulated browser window shown to desktop users.

The phishing kit also screens submitted email addresses and rejects personal email domains, directing the campaign toward corporate accounts.

Why it Matters

A recruitment interaction on an employee's phone can become a route to enterprise account compromise. The campaign's screening logic demonstrates deliberate interest in business access.

The investigation also highlights how mobile presentation can make fraudulent authentication flows difficult to assess. Organizations need protection at the point where employees encounter these requests, supported by clear verification and reporting procedures.

4 Mobile Threats Combine Surveillance, Extortion and Remote Access

Several investigations show malware combining capabilities that expose victims to multiple forms of harm. Surveillance can reveal private communications and sensitive files. Remote access can enable continued collection or manipulation. Ransomware adds another means of coercion.

Featured Investigation: Mantax Otax
Published: September 9, 2026

Mantax Otax combines spyware capabilities with ransomware functionality targeting older Android versions. Its surveillance features include screen recording, browser-history collection, lock-screen PIN theft, contact and message harvesting, file exfiltration and unauthorized photography.

The malware also includes an on-screen communication mechanism for ransom demands.

Why it Matters

Data theft and encryption create different consequences for victims. Incident response must establish what information was exposed as well as whether data was encrypted or device access was disrupted.

Featured Investigation: Arsink RAT
Published: January 29, 2026

Arsink RAT uses services including Google Apps Script, Google Drive, Firebase and Telegram for command-and-control or data exfiltration.

During the investigation, zLabs identified:

Research Measure	Finding
Distinct APK hashes	**1,216**
Firebase Realtime Database endpoints	**317**
Unique victim IP addresses extracted through infrastructure enumeration	**45,000**

Why it Matters

Arsink illustrates the infrastructure behind a mobile surveillance operation and the use of widely available services to support malicious activity.

The IP-address count is an infrastructure observation. It should not be interpreted as a count of confirmed individuals, devices or enterprise compromises.

5 Browser-Based Exploits Extend Mobile Threats Beyond Malicious Apps

Mobile compromise does not always begin with a malicious application. The Coruna and DarkSword investigation demonstrates how attackers can use browser-based exploit chains to target iOS devices through websites that may appear legitimate, without requiring users to install an application or approve additional permissions.

Featured Investigation: Coruna and DarkSword
Published: October 29, 2026

zLabs identified 608 websites loading Coruna-family code through October 2026. The investigation uncovered shared infrastructure delivering Coruna and DarkSword-derived exploit chains based on the targeted iOS version. Attackers used hidden webpage elements to load malicious code, including through legitimate websites and compromised software dependencies.

The research also documented advanced post-exploitation capabilities, including access to sensitive device information, manipulation of system security controls and mechanisms designed to conceal malicious activity. During analysis of the iOS 18 chain, zLabs confirmed the exfiltration of an Apple Notes database and an inventory of 214 installed applications from a test device.

Why it Matters

Browser-based exploitation can expose mobile devices without the warning signs typically associated with malicious application installation. The investigation reinforces the importance of timely operating-system updates, device-integrity monitoring and mobile threat detection that extends beyond application-based threats.

AI Adoption is Changing Mobile Application Risk

While zLabs investigations document attackers incorporating AI into malware operations, the 2026 Global Mobile Threat Report examines another dimension of risk: AI within the applications organizations build and use.

The report documents 14x growth in AI embedded within Android apps and 7x growth on iOS compared with the 2025 baseline. Adoption within business apps increased 136%. As applications introduce AI capabilities, organizations need to reassess their data access, integrations and security controls.

AI-assisted development also requires security oversight. The GMTR also reports that, by 2027, 25% of software defects will trace to AI-generated code, up from less than 1% in 2023.

Together, these findings reinforce the need to assess mobile applications as they change and protect them against exploitation after deployment. AI adoption alone does not establish that an application is insecure, but it introduces changes that security teams must evaluate.

What These Investigations Mean for Organizations

Across the selected research, attackers exploit the relationships between mobile devices, identities and applications. A phone can hold authentication codes, display sensitive information and provide access to business or financial services. Device compromise can expose several of those functions at once.

The investigations point to four practical priorities:

Security priority	Implication
Detect device compromise	Identify malicious behavior, suspicious permissions and unauthorized device control.
Protect mobile authentication	Address phishing and credential theft where employees encounter login requests.
Protect sensitive application interactions	Account for overlays, screen monitoring and compromised environments during authentication and transactions.
Validate remediation	Determine whether persistent components or unauthorized access remain after apparent malware removal.

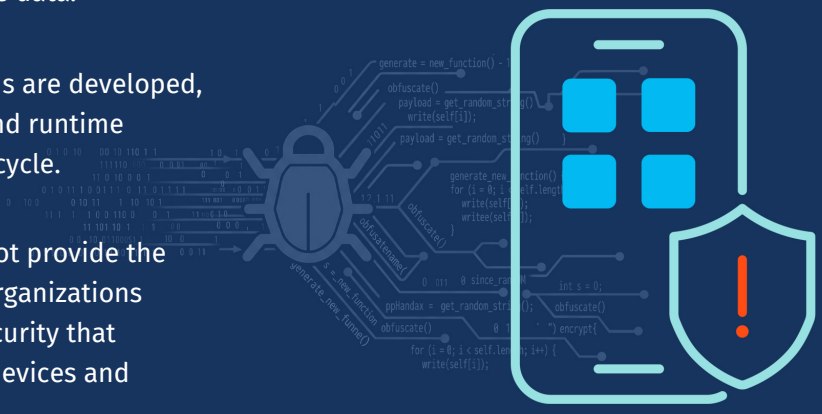
Organizations should connect mobile threat detection to their identity, SOC, fraud and incident response processes. A compromised device may require action beyond removing an application, including reviewing exposed credentials and affected sessions.

LOOKING AHEAD TO 2027

Dedicated Mobile Security is an Enterprise Imperative

Zimperium expects AI to further accelerate mobile attack capabilities in 2027, enabling malware to interpret device interfaces, automate interactions and adapt during execution. As cybercriminals advance their mobile-first attack strategy, they are targeting the devices employees use to authenticate, access corporate applications and handle sensitive business data.

AI is also changing how mobile applications are developed, reinforcing the need for security testing and runtime protection throughout the application lifecycle.



Traditional enterprise security alone cannot provide the protection this attack surface demands. Organizations need dedicated, AI-empowered mobile security that detects threats and responds directly on devices and within applications.

Detecting and stopping threats on mobile devices is critical to preventing attackers from using compromised devices or stolen credentials to gain access to corporate environments. Mobile security must be an integral part of enterprise defense, with visibility and response capabilities designed for the devices and applications where these attacks occur.

Research Scope and Methodology

This report synthesizes eight selected zLabs investigations published between January 1 and November 1, 2026. It includes original malware research and extended analysis of previously reported campaigns; RecruitTrap is identified as an extended analysis rather than solely an original discovery.

This review also incorporates selected findings from Zimperium's 2026 Global Mobile Threat Report. Those findings retain the GMTR's measurement periods and methodology, which may differ from the investigation periods covered here. Third-party forecasts cited in the GMTR are attributed to their original source.

The selected investigations illustrate attacker capabilities and security implications. They do not constitute a comprehensive measure of global mobile threat prevalence or establish year-over-year growth across the threat landscape.

Application targets, infrastructure endpoints, malware samples and IP addresses are distinct measures. Counts from separate investigations should not be combined without deduplication and methodological review. Publication dates may also differ from the periods in which samples or campaign activity were observed.

Research and Sources

RatHat
ToxicPanda 2.0
PixRevolution
Rokarolla
RecruitTrap
Mantax Otax
Arsink RAT
Coruna and DarkSword
2026 Global Mobile Threat Report

About Zimperium

Zimperium is the world leader in AI-empowered mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging the power of AI to deliver autonomous security that counters evolving threats including mishing, malware, and zero-day attacks.

www.zimperium.com



ZIMPERIUM®

Learn more at: **zimperium.com**
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244

© 2026 Zimperium, Inc. All rights reserved.