DRONA
CYBER SOLUTIONS

// GLOBAL THREAT INTELLIGENCE BRIEF

Glitch SPY: An Emerging Android RAT

> Detailed technical breakdown of an advanced mobile threat abusing Android Accessibility Services for automated financial fraud and crypto-clipping operations.

PREPARED BY

Drona Cyber Solutions Pvt Ltd

DATE OF ISSUE

July 1, 2026

CLASSIFICATION MATRIX

HIGH: RED MED: AMBER LOW: GREEN

THREAT AWARENESS ADVISORY

Emerging Android Malware Family: Glitch SPY

Issued By: Drona Cyber Solutions Pvt Ltd **Intelligence Source:** Drona Threat Intel

Target Sector: Mobile Users / Financial / Crypto **Severity Classification:** HIGH

Executive Summary

Drona Threat Intel identified an emerging Android malware family tracked as Glitch SPY, distributed through a fraudulent Polish apartment and house rental platform designed to lure users into downloading an Android APK [cite: 22]. Based on the Polish-language lure and rental-themed distribution website, the activity appears to be Poland-focused, targeting users in Poland or Polish expats [cite: 23]. The downloaded application functions as a dropper and installs the Glitch SPY payload after convincing the user to allow installation from unknown sources [cite: 24]. Glitch SPY prompts the victim to enable Android Accessibility Service, which it abuses to automate permission grants, interact with the device UI, extract visible screen content, perform gestures, support remote input, and enable further post-infection activity [cite: 25].

CRITICAL RISK WARNING (MEDIUM MATRIX METRIC)

Glitch SPY maintains a persistent WebSocket channel to its C&C server and supports over 70 commands spanning live screen streaming and remote control, screenshot and screen-reader capture, SMS, contact, call log, and location theft, camera and microphone surveillance, keylogging, file management, and shell execution [cite: 26]. Beyond standard surveillance, it includes a crypto-clipper that swaps copied wallet addresses across multiple blockchain formats, file encryption/decryption routines, device-unlock and credential-capture logic, and a hidden remote-browser capability that lets attackers conduct web-based account takeover from the victim's own device and IP [cite: 27].

Attack Chain & Distribution Mechanism

The infection vector utilizes high-quality social engineering techniques aligned with rental property searches [cite: 117]:

- **The Lure Website:** Attackers deploy a deceptive domain (tutaj-dompl[.]com) masquerading as a legitimate Polish apartment and house rental platform called "Tutaj Dom" [cite: 94, 95]. The site offers commission-free property viewings and requests users to download an application to finalize bookings [cite: 95, 96].
- **The Dropper Phase:** The downloaded application is the Brokewell Android Loader, which acts as a dropper and deploys the Glitch SPY payload after prompting the user to allow installation of applications from unknown sources [cite: 79, 80].

- **Payload Deployment:** Once permitted, the loader installs the primary Glitch SPY binary, immediately prompting the user to grant access to the Android Accessibility Service [cite: 163, 164].

Technical Analysis of Core Capabilities

Glitch SPY features an aggressive suite of post-compromise actions controlled remotely via a persistent WebSocket connection [cite: 26, 203]. Its primary operational capabilities include:

- **Accessibility Abuse:** Automatically clicks through system warnings, auto-grants intrusive device permissions, performs remote gestures, and extracts visible on-screen text dynamically [cite: 199, 200].
- **Surveillance & Data Theft:** Supports live near-real-time screen streaming, screenshot extraction, offline keylogging, call log harvesting, contact list theft, precise GPS tracking, and remote camera/microphone recording [cite: 82, 213].
- **Advanced Crypto Clipper:** Actively monitors the device clipboard [cite: 332]. If a cryptocurrency wallet address is copied, it seamlessly swaps the address for an attacker-controlled destination across multiple blockchain environments, including ETH/EVM, TRON/TRX, Bitcoin Legacy, and Bech32 formats [cite: 83, 333].
- **Off-Screen Remote Browser:** Spawns a hidden off-screen window WebView session directly on the infected device [cite: 389, 391]. Attackers can execute automated JavaScript injections, navigate financial portals, and perform unauthorized account takeovers using the victim's active session cookies and authorized device IP [cite: 418, 440].
- **Evasion & Persistence:** Suppresses standard biometric prompts to force password or PIN entry fallback, hides its application launcher icon, and systematically prevents manual uninstallation by interrupting device management settings [cite: 149, 223].

Strategic Recommendations for Corporate & Client Awareness

To reduce systemic risk against advanced mobile threats such as Glitch SPY, organizations and clients should immediately enforce the following operational guardrails [cite: 505, 506]:

Mitigation Pillar	Actionable Security Requirement (Low Sensitivity Baseline)
Strict Source Restraints	Enforce a strict policy mandating the download of mobile applications exclusively from trusted official platforms, such as the Google Play Store [cite: 507, 509]. Avoid third-party app stores or untrusted installation links [cite: 509].

Mitigation Pillar	Actionable Security Requirement (Low Sensitivity Baseline)
Accessibility Restrictions	Educate users to treat any application requesting Accessibility Service permissions or installations from unknown sources with extreme scrutiny [cite: 502]. Denying unknown installer rights stops payloads entirely [cite: 501].
Multi-Factor Enforcement	Implement robust Multi-Factor Authentication (MFA) parameters for banking and financial applications to add an extra layer of protection, even if credentials are compromised [cite: 512, 513].
Endpoint Security Layers	Ensure that Google Play Protect remains enabled on all endpoints at all times [cite: 503] and utilize mobile security solutions that include real-time system scanning [cite: 516, 517].
Incident Response Preparedness	If an infection is suspected, users must instantly isolate the device, report the incident to their bank and local authorities [cite: 514, 515], reset credentials from an uncompromised machine, and perform a factory reset [cite: 516].

Indicators of Compromise (IoCs)

Indicator Value	Type	Context / Description
`hxxps://tutaj-dompl[.]com/Tutajdom.apk`	URL	Malicious Lure Distribution Domain [cite: 533]
`sportypointsrewards[.]com`	Domain	Glitch SPY Command & Control (C2) Infrastructure [cite: 533]
`80af5e921cf8a3052fe4483bb2eb15953590e72ed003ac61c0b9135575c32075`	SHA-256	Glitch SPY Payload Executable Binary Hash [cite: 533]