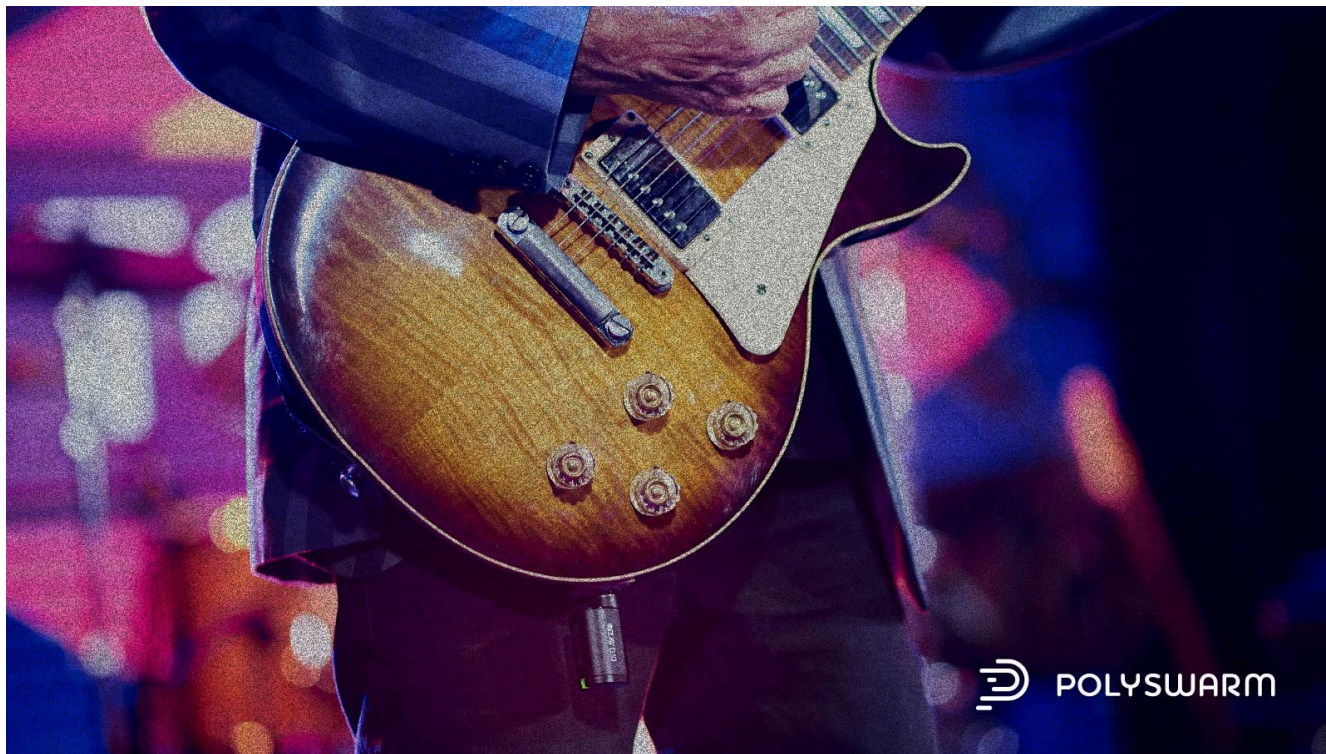


Rokarolla Expands the Android Fraud Playbook

 blog.polyswarm.io/beyond-banking-trojans-rokarolla-expands-the-android-fraud-playbook

The Hivemind



Verticals Targeted: Financial, Cryptocurrency

Regions Targeted: Global

Related Families: Rokarolla

Executive Summary

Researchers have identified Rokarolla, a newly discovered Android banking trojan distributed through malicious websites impersonating trusted applications such as TikTok, Google Chrome, and Google Play Protect. The malware targets at least 217 banking and cryptocurrency applications and leverages Android Accessibility Services, phishing overlays, SMS interception, keylogging, screen monitoring, and call blocking to facilitate financial fraud. Rokarolla exposes at least 137 operator commands and employs multiple persistence and evasion mechanisms, allowing attackers to maintain

extensive control over infected devices while minimizing user awareness and intervention.

Key Takeaways

- Rokarolla targets at least 217 banking and cryptocurrency applications through credential theft and phishing overlays.
- The malware relies heavily on Android Accessibility Services to automate actions, harvest data, and facilitate fraud.
- Operators can steal SMS messages, intercept authentication codes, capture keystrokes, manipulate clipboard contents, and monitor device activity.
- The malware supports multiple fallback C2 domains, increasing operational resilience.
- Rokarolla can disable security controls, conceal its presence, and interfere with communications that could alert victims to fraudulent activity.

Background

Rokarolla demonstrates the continued sophistication of Android banking malware by combining credential theft, device surveillance, accessibility abuse, and fraud-enablement capabilities within a single malware family. Rather than relying on a single collection method, the malware employs multiple mechanisms to obtain sensitive information and maintain access to infected devices. The breadth of targeted banking and cryptocurrency applications suggests a financially motivated operation focused on maximizing opportunities for fraud and account compromise. Researchers also observed infrastructure redundancy and dynamic configuration capabilities that may help operators maintain access even if portions of their infrastructure are disrupted. Zimperium recently [reported](#) on Rokarolla.

Technical Analysis

Initial Infection and Deployment

Rokarolla is distributed through malicious websites that impersonate legitimate software distribution portals. Victims are presented with applications disguised as trusted software, including popular consumer applications and security-related tools. The initial dropper installs a second-stage payload while masquerading as Google Play Protect, helping to establish trust during the installation process.

Following installation, the malware requests Accessibility Service permissions along with access to SMS messages, notifications, and other sensitive device functions. These permissions enable many of the malware's core surveillance and fraud capabilities.

Accessibility Service Abuse

Accessibility Services play a central role in Rokarolla's operation. The malware abuses these services to monitor user activity, interact with applications, collect screen content, automate actions, and facilitate credential theft. Researchers observed the malware parsing user interface elements, identifying application content, and leveraging accessibility functions to support its overlay attacks and surveillance operations.

Command-and-Control Infrastructure

The malware communicates with its C2 infrastructure over HTTPS and initially transmits detailed device telemetry, including hardware information, Android version data, localization settings, battery status, memory utilization, and storage information. This data is used to generate a unique bot identifier and profile infected devices.

Researchers observed support for multiple fallback domains and remote configuration updates, allowing operators to dynamically modify active infrastructure and maintain communications if individual domains become unavailable. The malware exposes at least 137 distinct commands that provide operators with extensive control over infected devices, supporting surveillance, credential theft, fraud facilitation, and device management functions.

Financial Credential Theft

A primary capability of Rokarolla is the theft of banking and cryptocurrency credentials through overlay-based phishing attacks. The malware retrieves a remotely managed list of targeted applications and associated phishing resources from its C2 infrastructure. When a targeted application is launched, Rokarolla displays a fraudulent HTML-based overlay that mimics the legitimate application's login interface.

Victims may unknowingly enter usernames, passwords, payment card information, and other sensitive data into the fraudulent interface, which is subsequently transmitted to attacker-controlled infrastructure. Because the phishing content is displayed directly over legitimate applications, users may have difficulty distinguishing the malicious interface from the authentic application.

Device Unlock Credential Harvesting

Researchers observed functionality designed to collect Android device unlock credentials, including PINs, passwords, and unlock patterns. The malware accomplishes this by presenting lock screen overlays that closely resemble legitimate Android authentication prompts, enabling attackers to capture credentials entered by victims.

SMS Theft and Call Interception

Rokarolla includes extensive communications interception capabilities. The malware can exfiltrate SMS messages, send messages from the victim's device, and potentially obtain one-time passcodes delivered through SMS. These capabilities may facilitate account compromise against services that rely on SMS-based authentication.

Researchers also documented functionality that allows the malware to block, disable, or intercept phone calls. Such capabilities could interfere with fraud alerts, verification calls, or other communications intended to notify victims of suspicious account activity.

Surveillance and Data Collection

The malware incorporates numerous surveillance functions, including:

- Keylogging capabilities
- User interface logging
- On-screen text extraction
- WhatsApp contact harvesting
- Screenshot collection
- Clipboard manipulation

Researchers noted that clipboard modification functionality could be used to replace cryptocurrency wallet addresses or other sensitive values without the victim's knowledge, potentially facilitating financial theft.

Snapshot-Based Screen Monitoring

Instead of relying on continuous screen-streaming technologies, Rokarolla employs a screenshot-based monitoring mechanism. The malware periodically captures screenshots, compresses them into PNG format, and transmits them to C2 infrastructure along with associated timestamps. This approach enables operators to monitor victim activity while collecting visual information from the device.

Evasion and Persistence

Rokarolla incorporates multiple techniques intended to evade detection and maintain persistence. Researchers observed attempts to disable Google Play Protect, hide the application icon from the device launcher, suppress audio notifications and vibrations, and obstruct user interaction through deceptive overlays. The malware can also keep the device display active to prevent interruptions caused by screen locking or timeout events.

Analyst Commentary

Rokarolla highlights the continuing effectiveness of Accessibility Service abuse within the Android threat landscape. Rather than depending on a single credential theft technique, the malware combines phishing overlays, device unlock credential harvesting, SMS interception, call blocking, keylogging, clipboard manipulation, and screenshot collection to create multiple paths for fraud and account compromise. This layered approach increases operational flexibility and provides attackers with alternative methods for obtaining sensitive information when individual collection techniques are unsuccessful.

The malware's ability to dynamically retrieve targeted application lists, phishing content, and updated infrastructure configurations further demonstrates how Android banking trojans continue to adopt more modular operational models. Defenders should prioritize detection of unauthorized Accessibility Service usage, suspicious overlay activity, SMS handler modifications, unexpected call management permissions, and application sideloading behavior.

PolySwarm can provide additional visibility into emerging Android malware families, malicious infrastructure, suspicious APKs, and evolving indicators of compromise by leveraging threat intelligence generated by a global community of security vendors and independent researchers. As Android banking trojans continue to evolve beyond simple credential theft into comprehensive fraud-enablement platforms, access to diverse threat intelligence sources can help defenders accelerate investigations, improve detection coverage, and identify emerging threats earlier in the attack lifecycle.

IOCs

PolySwarm has multiple samples associated with Rokarolla.

890ecea4ebe4fea692ad36adf02abeb37c181cb7bdb6122cd52d9aaafe7d6cf3

1ba364113c4cec5542d1b2c76d7c163a66bdf90bc373256d5178f880f9742960

d7d960ef10b08c472ad397b6fd9e9481338b2077c7c2f44d3dc2c65b19345ae0

57307ee8a3cda10730eacecaf789fab6f8771f9d29397e07c31a6bd4551bba10

3fae7ede2ef9c809b54504c3d78e5111d7fad0b522c707b8f6ff21015af79251

fe41e6c1725f63582f022a17abe098e49338a78118a00ca87785b2fa0cf3dadf

be8573971b85fda81a2fac27adb7a3a9b2cf7e1d9bdf713361a725324d378d34
5139253b1f30b34ab3aa888aba175866fa1f82728ab07b999c24b49b191c3f68
43888be8debbbd74012484d4e4f9a1c70c2ff3970e0bf499c9aebba9776930a1
a5e6763b09553691c8b42deefb725fa3b8c133a03a34cea87740b1f13d08bac3
1d3270a9141f8f16047799f1132633d72fd421b6c8f1878b5ef04ced6add4db8
62aef76c2d1897203649844b45317d9e1723819479a2b88ca4b3290ca9f4c9f0
48a3db92fac1ba9c218253576e09f42faabeaf48cf80663cf32e06b0a66e983d
726095e56c693977b7796dc7cead2e2a49551d77d3f442aaa28997615ba07e99
c3cfe522d2da15b033f65eb5377bf9e99be598dc4c21729e6f168dbc8f19540b
3e25c28c5e93376683e841b7ad60f9383bb3bf831284a93a4aae798fc769d767
8d65e4df0ad369f491698437413afd1bd55fff309860f9cdecc778c9ac062282
c08cd3f78c0edcced6b1a694284b6ed4a9e0422f469e07c702c4a8d1f6c186f4
696ef29f77a91aa91279c83088a07ab137d5049dc096ef862a35f9d890a552b3
8ddbcebe1014a645855986e85b2c54ee167baf1e9a0d74179faf81a5ee6878f4
1e4ed7e40608750cd0bfe96f5ed493a022b58ec54da2345336c522f7c78197af
c505353a6c58a21cb7b0343202e8629bee2f121f01c21dd8e0b61b7c55b77495
aec2a36e8d68b23444348a7cec2d6ec287cb8810d1e190e04743645426ababb1
f49be77b95cabd28d2dfe91786863576f6bd3f43a9d6de67a5b5851afe3aff9a
e76cbdf420540a18e2ddea02938acf3c4b4139f3511d314dca9781afe1e439bb
c3e324106803df27f5b6e0d49d2daf02d4cde396af4401f1ad29d78198e370b6
ed036356fa2d3490d3ddb5ee7ae98bab80b505938f0199d9b10f12266f345896
d6403ec82659eb62424bb1033615a8df27635080d02e438a4ee7e2334b1155f7
c734a665f04eb9ab17047e65940fc35bad0221d59c2fc4fd0d170f2181514034

e134cffcbe1fa8a861fd1f9a506f10ca5ff56cd5082360ef13d204676792e8bc
f0c18f045e3bb0193ef1169f5fa1abff7aa47e9a23da35cf67bbb9548a5e32c0
f8cb375a4129358ad5881c29a6921fc1e5773028c0b31da83298f606118b185a
3c304a1ac73590aaf94b62711a5f2fd0cbb863dab13aef6ec1eb156f4a7bd5b9
2eb80e5519fc6defcec8cc30a5cf4f75ee5ec8d2435759bb77c19826f1e20efb
1f4c70cb317ffd25adc828fbac3bb8f07739e23111f7b7905926489fe35f8973

Click [here](#) to view all samples of Rokarolla in our PolySwarm portal.

Don't have a PolySwarm account? Go [here](#) to sign up for a free Community plan or subscribe.

Contact us at hivemind@polyswarm.io | Check out our [blog](#) | [Subscribe](#) to our reports.

Topics: [Threat Bulletin](#), [Android Malware](#), [Android banking trojan](#), [mobile banking fraud](#), [cryptocurrency malware](#), [Rokarolla](#), [banking malware](#), [Android phishing overlays](#)