



HACKING ANDROID

Exploiting and Defending Against Remote Access Backdoors

THE TEAM



Emmanuel Adewa
Ethical Hacker



Sireen Rahhal
Ethical Hacker




WHY THIS TOPIC?

Global Nature of The Threat

The proliferation of backdoor-infected Android applications (APKs) represents a significant global cybersecurity concern, affecting millions of devices and users worldwide.

Scale of Impact

Android's openness and popularity make it a prime target for malicious APKs that enable unauthorized access, leading to data breaches, fraud, and large-scale botnets.



Security Education

Foster understanding of defense against threat.



Human Vulnerability

Elevate Social engineering as a key weakness in security chain.



App Download Danger

Show how apps can be weaponized into undetected backdoors

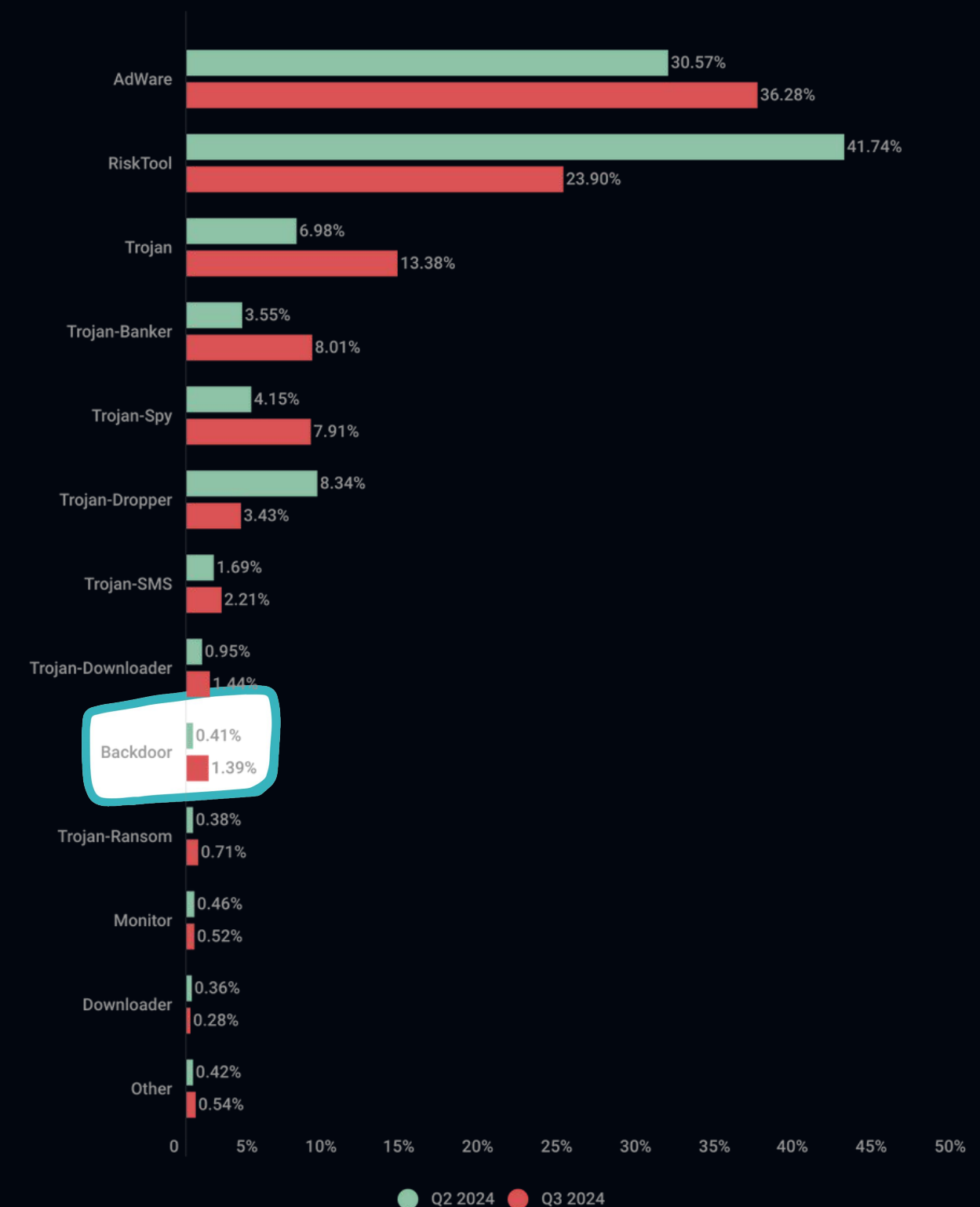
THREAT LANDSCAPE

A snapshot of emerging malware trends and cybersecurity challenges for Android:



Backdoor APK Incidents

- Major campaigns like Badbox 2.0, Xamalicious, and Necro have infected over 12 million Android devices globally.
- As many as 6.7 million attacks involving malware, adware or potentially unwanted mobile apps were prevented.



CYBERSECURITY CONCEPT

This topic touches upon all three core cybersecurity concepts: confidentiality, integrity, and availability (CIA triad), but primarily focuses on integrity and availability, with a secondary concern for confidentiality.



Confidentiality



Integrity



Availability



RESEARCH PROCESS

1

Android Security Fundamentals

Explore common OS vulnerabilities (intent flaws, permission bypasses) and built-in defenses.

2

Exploitation Frameworks

Master Metasploit (msfvenom/console, listeners, Meterpreter) and TheFatRat (code injection, APK signing/verification).

3

Network Tunneling & Hosting

Explore Ngrok for secure remote access and Python's HTTP server for file hosting.

4

Test Environments

Leverage VMware and Genymotion emulators, and understand differences from physical devices

5

Human & Legal Factors

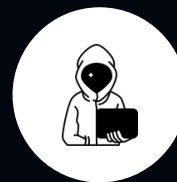
Study social engineering tactics and prevention, alongside ethical hacking principles and legal frameworks.

THE APPROACH



Environment Setup

Configure Kali Linux (VMware) with TheFatRat and Ngrok. Set up an Android emulator (Genymotion) as the target device.



Payload Creation and Delivery

Generate a malicious APK with a Meterpreter reverse TCP payload using TheFatRat; host the APK on a local Python HTTP server; Simulate the download and installation of the APK on the Android emulator.

Loading....

90%





Reverse Connection and Session Establishment

Configure Metasploit to listen for the incoming connection, utilizing Ngrok for remote access simulation. Establish a Meterpreter session upon APK execution.



Post-Exploitation and Data Exfiltration

Demonstrate various post-exploitation techniques: Privilege escalation, data exfiltration (call logs, contacts, SMS), device control (webcam, geolocation, app hiding).

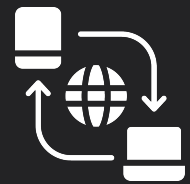


BootCon Demonstration

</> HACKING ANDROID </>



DEMONSTRATION SUMMARY



Established Remote Access

Ngrok tunneling and a reverse shell bypassed network restrictions to simulate a real-world remote attack.



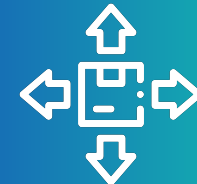
Delivered a Malicious Payload

Hosted and installed a TheFatRat generated malicious APK via HTTP, underscoring danger of untrusted apps.



Gained Full Device Control

Payload execution spawned a Meterpreter session, granting full device control and access to data.




Post-Exploitation Capabilities

Showed how post-exploitation tools can escalate privileges and enable malicious actions on compromised devices.



Emphasized Security Risks

The demo stressed avoiding unknown-source apps and keeping security measures up to date.





MITIGATION STRATEGIES



APP SOURCES

Disable “Install from unknown sources” in your settings to prevent installing apps outside the Play Store and reduce the risk of malicious APKs.



APP PERMISSIONS

Grant apps only necessary permissions, avoiding unnecessary access to sensitive data or device functions.



OS & APP UPDATE

Regularly update your Android OS and apps to patch vulnerabilities and reduce security risks.



PLAY PROTECT

Enable Google Play Protect for real-time app scanning and malware defense.



SOCIAL ENGINEERING

Stay alert to social engineering tactics like phishing and deceptive links to avoid installing malware.



MOBILE SECURITY SOFTWARE

Use reputable mobile security software for real-time scanning, malware detection, and network monitoring.

THANKS FOR WATCHING

We hope you learned something new. Do you have
any questions?

