|  |  |  |
| --- | --- | --- |
| **Student Name** | **:** |  |
| **Student ID** | **:** |  |
| **Class** | **:** |  |

**Objectives of the exercise:**

* To understand how to analyze APK files for potential security risks using VirusTotal.

**Requirement:**

* **APK file provided by instructor: InsecureBankv2.apk**
* **Internet access for using VirusTotal**
* **A web browser (Google Chrome, Firefox, etc.)**

**Introduction:**

**Understanding APK File**

* APK stands for Android Package Kit, and it’s the format in which Android applications are packaged and distributed. When you download an app from the Google Play Store or another app store, you’re downloading an APK file.
* APK files can contain malware, making it essential to verify their safety before installation.

**Understanding VirusTotal**

* VirusTotal is a free online service that allows users to analyze files, URLs, and IP addresses for potential malware, viruses, and security threats. It aggregates results from multiple antivirus engines and security tools to provide a comprehensive security analysis.
* Key Features of VirusTotal:
  + **Multi-Engine Scanning:** Uses over 70 antivirus scanners to detect threats in files and URLs.
  + **Static Analysis:** Extracts metadata, permissions, and structure of a file.
  + **Dynamic Analysis:** Observes file behavior when executed in a sandbox environment.
  + **Community Insights & Reports:** Users can leave comments and vote on whether a file or URL is suspicious. It provides historical data on previously scanned files and domains.
  + **API Integration:** Allows developers and cybersecurity professionals to integrate VirusTotal’s scanning capabilities into their own security tools.

**Questions:**

**Step 1: Register Account**

1. Open your web browser and search the link: <https://www.virustotal.com/gui/home/upload>.
2. Register using official student email
3. After successful registration, login using your account.

**Step 2: Uploading the APK File**

1. Click on the **"Choose File"** button.
2. Select the APK file you want to analyze; in this lab, upload **InsecureBankv2.apk**.
3. Click **"Open"**, then "Confirm Upload" to start the scan.

**Step 3: Analyzing the Scan Results**

After the scan completes, review the following:

1. **Detection Ratio**
   1. Shows how many antivirus engines detected the APK as malicious. Example: 5/70 means 5 antivirus engines flagged the file.

|  |
| --- |
| **Answer:** |
| 14/66 |

1. **Static Analysis**

|  |  |
| --- | --- |
| **DETAILS** | **ANSWER** |
| **DETECTION TAB** | |
| **Security Vendor’s Analysis Detected as “MALICIOUS”** | 1. AhnLab-V3 - PUP/Android.FLPrev.1019545 2. Avast-Mobile - Android:Evo-gen [Trj] 3. Ikarus - Trojan-Spy.AndroidOS.Agent 4. QuickHeal - Android.Obfus.GEN41318 5. Sophos - Andr/Xgen-AOZ 6. Tencent - A.expense.smsvideo.a 7. Trustlook - Android.Malware.Spyware 8. AliCloud - Suspicious 9. Google - Detected 10. K7GW - Trojan ( 0001140e1 ) 11. Skyhigh (SWG) - Artemis!Trojan 12. Symantec Mobile Insight - AppRisk:Generisk 13. Trellix (ENS) - Artemis!5EE482906564 14. ZoneAlarm by Check Point - Andr/Xgen-AOZ |
| **CROWDSOURCED IDS RULES** | |
| **List High/Medium/Low/Info for Crowdsourced IDS Rules** | 1. Matches rule ET INFO Android Device Connectivity Check at Proofpoint Emerging Threats Open (LOW) – *Misc activity* 2. Matches rule ET INFO Android Device Connectivity Check – (LOW) – *Misc activity* |
| **DETAILS TAB** | |
| **BASIC PROPERTIES** | |
| **File Type** | Android, executable, mobile, apk |
| **File Size** | 3.30 MB (3462429 bytes) |
| **NAMES** | |
| **APK Name(s)** | 1. InsecureBankv2.apk 2. InsecureBankv2.apk.jar 3. app-debug.apk 4. InsecureBankv2 1.apk 5. InsecureBankv2 2.apk 6. 1743622654081-InsecureBankv2.apk 7. 1743585534805-InsecureBankv2.apk 8. 1743583628386-InsecureBankv2.apk 9. 1743582357056-InsecureBankv2.apk 10. 1743579471530-InsecureBankv2.apk |
| **CERTIFICATE ATTRIBUTES** | |
| **Certificate Attributes Valid From** | 2015-07-24 20:37:08 |
| **Certificate Attributes Valid To** | 2040-07-17 20:37:08 |
| **PERMISSIONS** | |
| **Permissions that has/have warning sign (!)** | 1. android.permission.SEND\_SMS 2. android.permission.READ\_PHONE\_STATE 3. android.permission.USE\_CREDENTIALS 4. android.permission.ACCESS\_COARSE\_LOCATION 5. android.permission.READ\_CALL\_LOG 6. android.permission.INTERNET 7. android.permission.READ\_PROFILE 8. android.permission.WRITE\_EXTERNAL\_STORAGE 9. android.permission.READ\_CONTACTS |
| **BEHAVIOUR TAB** | |
| **Detection for Activity Summary** | 1. Detection – NOT FOUND 2. Mitre Signatures – 20 INFO 3. IDS Rules – 1 LOW 4. Sigma Rules – NOT FOUND 5. Dropped Files – NOT FOUND 6. Network Comms – 2 HTTP, 17 DNS, 57 IP, 6 JA3 |
| **MITRE ATT&CK TACTICS AND TECHNIQUES** | |
| **Discovery** | 1. System Network Connection Discovery (INFO) – Checks an internet connection is available 2. Process Discovery (INFO) – Queries list of running processes/tasks 3. System Information Discovery (INFO) – Queries the unique device ID (IMEI, MEID or ESN) 4. Location Tracking (INFO) – Has permission to query the current location 5. Location Tracking (INFO) – Queries the phones location (GPS) |
| **Command and Control** | 1. Application Layer Protocol (INFO) – Uses HTTPS 2. Application Layer Protocol (INFO) – Performs DNS lookups 3. Non-Application Layer Protocol (INFO) – Performs DNS lookups 4. Encrypted Channel (INFO) – Uses HTTPS |
| **Defense Evasion** | 1. Obfuscated Files of Information (INFO) – Obfuscates method names 2. Delete Device Data (INFO) – Lists and deletes files in the same context |
| **Impact** | 1. Delete device data (INFO) – Lists and deletes files in the same context 2. Carrier Billing Fraud (INFO) – Has permission to send SMS in the background 3. Generate Fraudulent Advertising Revenue (INFO) – Loads advertisement |
| **Network Effects** | 1. Eavesdrop on Insecure Network Communication (INFO) – Monitors network connection state 2. Exploit SS7 to Redirect Phone Calls/SMS (INFO) – Has permission to send SMS in the background |
| **NETWORK COMMUNICATIONS** | |
| **HTTP Requests** | GET http://connectivitycheck.gstatic.com/generate\_204 204 |
| **DNS Resolutions** | 1. android.googleapis.com 2. beacons.gvt2.com 3. c.tenor.com 4. clientservices.googleapis.com 5. connectivitycheck.gstatic.com 6. firebaseinstallations.googleapis.com 7. gmscompliance-pa.googleapis.com 8. googlehosted.l.googleusercontent.com 9. i3.ytimg.com 10. instantmessaging-pa.googleapis.com 11. lh3-dz.googleusercontent.com 12. lh3.googleusercontent.com 13. media.tenor.com 14. play-lh.googleusercontent.com 15. www.googleapis.com 16. [www.gstatic.com](http://www.gstatic.com) 17. encrypted-tbn0.gstatic.com |
| **RELATIONS TAB** | |
| **Contacted Domains that has/have detections** | |  |  |  |  | | --- | --- | --- | --- | | **Domain** | **Detections** | **Created** | **Registrar** | | [android.googleapis.com](https://www.virustotal.com/gui/domain/android.googleapis.com) | 0/94 | 2005-01-25 | MarkMonitor Inc. | | [beacons.gvt2.com](https://www.virustotal.com/gui/domain/beacons.gvt2.com) | 0/94 | 2008-03-03 | MarkMonitor Inc. | | [c.tenor.com](https://www.virustotal.com/gui/domain/c.tenor.com) | 0/94 | 1995-07-30 | MarkMonitor Inc. | | [clientservices.googleapis.com](https://www.virustotal.com/gui/domain/clientservices.googleapis.com) | 0/94 | 2005-01-25 | MarkMonitor Inc. | | [connectivitycheck.gstatic.com](https://www.virustotal.com/gui/domain/connectivitycheck.gstatic.com) | 0/94 | 2008-02-11 | MarkMonitor Inc. | | [encrypted-tbn0.gstatic.com](https://www.virustotal.com/gui/domain/encrypted-tbn0.gstatic.com) | 0/94 | 2008-02-11 | MarkMonitor Inc. | | [firebaseinstallations.googleapis.com](https://www.virustotal.com/gui/domain/firebaseinstallations.googleapis.com) | 0/94 | 2005-01-25 | MarkMonitor Inc. | | [gmscompliance-pa.googleapis.com](https://www.virustotal.com/gui/domain/gmscompliance-pa.googleapis.com) | 0/94 | 2005-01-25 | MarkMonitor Inc. | | [googlehosted.l.googleusercontent.com](https://www.virustotal.com/gui/domain/googlehosted.l.googleusercontent.com) | 0/94 | 2008-11-17 | MarkMonitor Inc. | | [gstatic.com](https://www.virustotal.com/gui/domain/gstatic.com) | 0/94 | 2008-02-11 | MarkMonitor Inc. | |
| **Contacted IP addresses**  **that has/have detections** | |  |  |  |  | | --- | --- | --- | --- | | **IP** | **Detections** | **Autonomous System** | **Country** | | 108.177.119.95 | 1/94 | 15169 | US | | 108.177.127.94 | 1/94 | 15169 | US | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |  |  |  |  | |

1. Identify the Graph Representation under the **Relations Tab**, **Graph Summary** (Screenshot).

|  |
| --- |
|  |

1. From the reports above, identify the importance of **Security Tests and Risk Assessment.**

|  |
| --- |
| **Answer:** |
| **Any relevant answer can be accepted.**  **1. Find and Fix Problems Before Hackers Do**  Security tests help you check if your app has weak spots that hackers can use. It’s like locking your doors and windows before leaving your house.  **2. Protect Your Personal Information**  These tests make sure your app doesn’t leak private things like passwords, bank details, or contacts. It keeps your data safe from being stolen.  **3. Avoid Trouble and Keep Users Happy**  If your app is safe, people trust it more. It also helps you avoid legal issues or bad reviews because of security problems. |

Step 4: Analyzing VirusTotal Scan Results

1. You uploaded an APK file to VirusTotal, and the scan results show that 13 out of 67 antivirus engines detected it as malicious. Based on these results, explain the steps you should take before deciding whether to install the APK.

|  |
| --- |
| **Answer:** |
| **Any relevant answer can be accepted.**  **1. Review Detailed VirusTotal Findings**  Look at the names of the detected threats and what kind of malware they suggest (e.g., spyware, trojan, riskware). If multiple engines agree on the threat type, it’s likely dangerous.  **2. Research the APK Source**  Ask: Where did you get this APK?  If it’s not from a trusted developer or official source (like Google Play Store), it’s risky. Even if it’s for testing, you should be cautious.  **3. Test in a Safe Environment (Sandbox or Emulator)**  Never install a suspicious APK on your personal phone. Use an Android emulator or isolated test device to see how it behaves without risking your data.  **Final Decision: Avoid Installation Unless Absolutely Necessary**  With 13 detections, it's best to avoid installing the APK unless you're conducting a security test for learning purposes and doing it in a controlled lab setting. |

1. During the static analysis of an APK file in VirusTotal, you find that the app requests the following permissions:
   1. android.permission.USE\_CREDENTIALS
   2. android.permission.READ\_PHONE\_STATE
   3. android.permission.SEND\_SMS
   4. android.permission.READ\_CONTACTS

Analyze the potential security risks associated with these permissions.

|  |
| --- |
| **Answer:** |
| **Any relevant answer can be accepted.**  a. android.permission.USE\_CREDENTIALS  Risk: This allows the app to access stored accounts (like email or social media) on your phone.  Why it’s risky: If abused, the app could access your personal accounts or even try to steal your login info.  b. android.permission.READ\_PHONE\_STATE  Risk: Lets the app read phone details like your number, IMEI, and whether you’re in a call.  Why it’s risky: Can be used to track your device, spy on your activity, or fingerprint your phone for targeted attacks.  c. android.permission.SEND\_SMS  Risk: Allows the app to send text messages without asking you.  Why it’s risky: Can be used to send SMS to premium numbers, leading to unexpected charges, or spread malware via SMS.  d. android.permission.READ\_CONTACTS  Risk: Lets the app see your entire contact list.  Why it’s risky: Can be used to steal personal data or spread scams/malware by sending messages to your contacts pretending to be you. |