Evidence per
Ian Whiffin
Andrew Hoog
Mari DeGrazia
Alexis Brignoni
Sarah Edwards

Upload suspicious .apk files to the Sandboxes
Online Mobile Malware proper Content Provider.
call the ContentResolver (the global instance that provides many native and third-party applications. The code would then be delivered to the broadcast receivers using Intents.
components or between entirely different applications.
Services:
through the User Interface (UI).
Users can navigate to/from and interact with activities directly in the AndroidManifest.xml file.
Granted to an application by the user
a transaction change so the database can be restored to a known state if an error
store original data before a transaction change so
and
contain ." SQLite files correspond to a database that
the magic number "

••

Devic
e performance problems
•

Unexplained device behaviors
- Unexplained settings changes
- Risky downloads, browsing or link-clicking
- Tools installed on the local machine for - Local Static Malware Analysis

FOR585:
Smartphone Forensic Analysis In-Depth
for585.com/course

Mobile Malware and Spyware
Key Artifacts: Static Analysis
Response Process: Response to an application by the user (1) during installation or (2) upon execution/behavior Found in the AndroidManifest.xml file
Activities: One or more activities comprise each application.
Users can switch to/from and interact with activities directly through the User Interface (UI) of the application
Services: Tasks often running in the background and integrated into the application, e.g., your Research Information System Services. Examples: music playing during a game application, or a location-based service that continually gets your location
Broadcast Receivers: Facilitates the exchange of information between applications. Receivers receive messages from components or between entirely different applications. Applications that are not allowed to receive messages are not delivered to the broadcast receivers using intents.
Content Providers: Refers to how information is stored in a database and shared between multiple applications within the same application or across multiple applications. The code would not be executed if they did not have access to the content (which passes on the request to the proper Content Provider)

Common Signs and Symptoms
- Android devices are most at-risk for the mobile malware infection
- Poor battery life
- Downloaded codes and fake applications
- Unusually large files
- Data plan usage
- Device performance problems
- Unexplained application errors

Online Mobile Malware Sandboxes
Uploaded suspicious .apk files to the internet for online sandbox analysis:
- https://www.sandbox4n6.com/
- https://malware.com/

Mobile Malware Detection

FOR585:
Smartphone Forensic Analysis In-Depth
for585.com/course

SQLite
Timestamp Conversion
Timestamps are stored in place databases as one of several numerical representations. (Timestamps are assumed to be stored in UTC, you may need to verify this.)

UNIX Epoch (10 digit number - number of seconds since 01/01/1970 00:00:00 UTC)

- SELECT contentions(10 COLUMNS, unsecond, -locations-);

Local time is correct by the device settings (this can be done for all the Timestamps)

- SELECT contentions(10 COLUMNS, unsecond, -locations-);

For Absolute time, number of seconds since 01/01/2001 00:00:00 UTC.

- SELECT contentions(10 COLUMNS, unsecond, -locations-);

Chrome time accounts for accurate to the MICROSECOND, which requires dividing the number by 1000000.

- SELECT contentions(10 COLUMNS, unsecond, -locations-);

Basic Analysis Query Structure
Get everything from a single table:

- SELECT contentions, columns, FROM & A TRACK;

Get two columns from a single table:

- SELECT contentions, columns, FROM & A TRACK;

Table Joins
Selecting data from two or more tables that have a column in common and joining them into one table. Identify tables of interest that contain unique values.

LEFT JOIN: result is returned from the LEFT table even if there are no matches in the RIGHT. Using the LEFT JOIN returns all the text messages, including those with and without attachments.


INNER JOIN: returning rows that are returned with both match in a way. Using the INNER JOIN (also achieved by typing "JOIN" in the query) returned just the messages that contained attachments.

Useful Stuff
Columns Reusing: _Tabelle.ANNAME.ATABLENAME" AS "Chat Messages"
Counting:

- SELECT contentions, columns, FROM & A TRACK;

Aggregating with GROUP BY and COUNT (count messages per contact):

- SELECT contentions, columns, FROM & A TRACK;

Sorting with ORDER BY:

- SELECT contentions, columns, FROM & A TRACK;

Searching with WHERE and LIKE:

- SELECT contentions, columns, FROM & A TRACK;

Free Scripts and Helpful Utilities

- SQL scripts for processing of sqlite database files
- iOS sysdiagnose documents
- Records-Parser
- Android-USESTATS-XML-Protobuf
- Installation-Logs-Parser
- Protobuf Parser
- ALEAPP
- iPhone sysdiagnose documents
- iOS Triage
- Graffiti
- iOS device
- Cold Hot
- Brute force is needed
- Encryption Type?
- END = Ending
- DESC = Descending
- APPLY ENSURE
- No decryption keys are available
- FileParser
- SQLite miner
- Records-Parser
- Query-Repo
- FAPK
- Protobuf Parser
- ALEAPP
- iPhone sysdiagnose documents
- iOS Triage
- Graffiti
- iOS device
- Cold Hot
- Brute force is needed
- Encryption Type?
- END = Ending
- DESC = Descending
- APPLY ENSURE
- No decryption keys are available
- FileParser
- SQLite miner
- Records-Parser
- Query-Repo
- FAPK
- Protobuf Parser
- ALEAPP
- iPhone sysdiagnose documents
- iOS Triage
- Graffiti
- iOS device
- Cold Hot
- Brute force is needed
- Encryption Type?
- END = Ending
- DESC = Descending
- APPLY ENSURE
- No decryption keys are available
- FileParser
- SQLite miner
- Records-Parser
- Query-Repo
- FAPK
- Protobuf Parser
- ALEAPP
- iPhone sysdiagnose documents
- iOS Triage
- Graffiti
- Android Extraction
- Malware: Malware Analysis
- Encryption Type?
- END = Ending
- DESC = Descending
- APPLY ENSURE
- No decryption keys are available
- FileParser
- SQLite miner
- Records-Parser
- Query-Repo
- FAPK
- Protobuf Parser
- ALEAPP
- iPhone sysdiagnose documents
- iOS Triage
- Graffiti
- iOS device
- Cold Hot
- Brute force is needed
- Encryption Type?
- END = Ending
- DESC = Descending
- APPLY ENSURE
- No decryption keys are available
- FileParser
- SQLite miner
- Records-Parser
- Query-Repo
- FAPK
- Protobuf Parser
- ALEAPP
- iPhone sysdiagnose documents
- iOS Triage
- Graffiti
- iOS device
- Cold Hot
- Brute force is needed
- Encryption Type?
- END = Ending
- DESC = Descending
- APPLY ENSURE
- No decryption keys are available
- FileParser
- SQLite miner
- Records-Parser
- Query-Repo
- FAPK
- Protobuf Parser
- ALEAPP
- iPhone sysdiagnose documents
- iOS Triage
- Graffiti
- iOS device
- Cold Hot
- Brute force is needed
- Encryption Type?
## iOS Cheatsheet

<table>
<thead>
<tr>
<th>Device Information</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>含义深刻</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Passwords and Account Information</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>账户密码</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings – System Controlled – Keyboards, Dictionary, Log, BT Address, etc.</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>键盘和字典</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings – User Controlled – Sync Settings, Springboard, etc.</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>用户自定</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Communications – SMS, Calls, Email</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>短信和通话</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Browser Activity</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>浏览器活动</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Multimedia</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>媒体</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Connections</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>网络</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syncing Artifacts</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>同步</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location Artifacts</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>位置</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traces of Destruction – Wiping, etc.</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>抹杀痕迹</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

## Android Cheatsheet

<table>
<thead>
<tr>
<th>Device Information</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>设备信息</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Passwords and Account Information</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>账户密码</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Settings</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>系统设置</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Settings</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>用户设置</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Communications – SMS, Calls, Emails</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>短信和通话</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Browser Activity</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>浏览器活动</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Multimedia</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>媒体</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Connections</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>网络</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syncing Artifacts</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>同步</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location Artifacts</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>位置</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Native Applications</th>
<th>Timestamp</th>
<th>MD</th>
<th>Beta</th>
<th>Synopsis</th>
</tr>
</thead>
<tbody>
<tr>
<td>原生应用</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>