



Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2015-03-02 17:09:59	2015-03-02 17:12:29	150 seconds	1.2-dev

## File Details

File name	1F68ADDF38F63FE821B237BC7BAABB3D_IBanking_Chase.apk
File size	808241 bytes
File type	Java archive data (JAR)
CRC32	22C1A158
MD5	1f68addf38f63fe821b237bc7baabb3d
SHA1	570617b47dc93bba5c9171fd005928107edcee57
SHA256	8458a9bc5ee516164ff96d5ec7a4fc154bf07229b8d74b39285c9c8d38fbc42e
SHA512	b9fafde7c8487c6deb886f420aad09a984dc45323bd2a6eff5f4475abdf604b94e69f8e8965758a185459a04ece9198a150e2708c6216488f6c4bc01bfe49a7
Ssdeep	24576:PDO+fiAppRUy/Z+QiY41jY+gBq+ZidWr1Y:7/BPsyR+Qf4FIZid6m
PEiD	None matched
Yara	None matched
VirusTotal	<a href="#">Permalink</a> VirusTotal Scan Date: 2015-03-02 13:19:00 Detection Rate: 36/57 ( <a href="#">Expand</a> )

## Android Application Info

Package	com.BioTechnology.iClientsService7
Main Activity	com.soft360.iService.MainActivity

## Activities

## Services

## Receivers

## Permissions

## Signatures

Application Queried Phone Number (Dynamic)

Performs some HTTP requests (Traffic)

File has been identified by at least one AntiVirus on VirusTotal as malicious (Osint)

Application Registered Receiver In Runtime (Dynamic)







Application Asks For Dangerous Permissions (Static)

Application Uses Reflection Methods (Static)

Application Sending SMS messages (Dynamic)

File has been identified by more the 10 AntiVirus on VirusTotal as malicious (Osint)

## Android Dynamic Analysis

 <b>SMS Messages</b>
 <b>Registered Broadcast Receivers</b>
 <b>Reflection Calls</b>
 <b>Fingerprints</b>
 <b>Content Values</b>
 <b>System Properties</b>

## Android Static Analysis

[Static Reflection Method Calls](#)

[Static ACCESS\\_NETWORK\\_STATE Method Calls](#)

[Static RECORD\\_AUDIO Method Calls](#)

[Static SEND\\_SMS Method Calls](#)

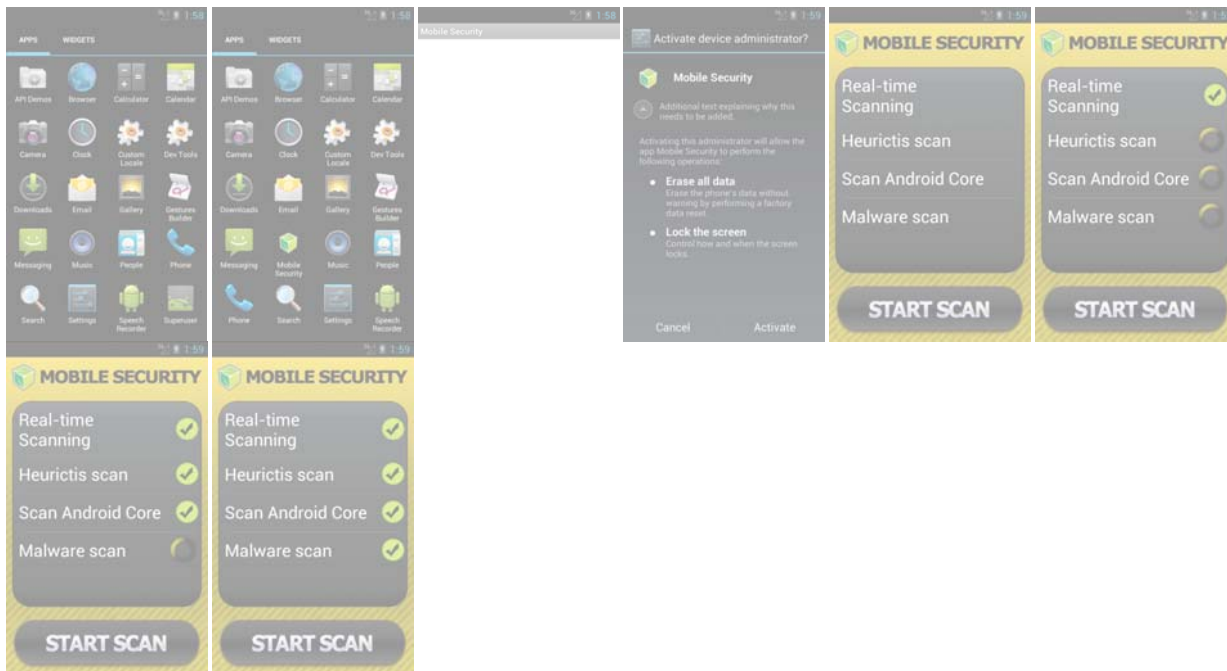
[Static VIBRATE Method Calls](#)

[Static INTERNET Method Calls](#)

[Static READ\\_CONTACTS Method Calls](#)

[Static READ\\_PHONE\\_STATE Method Calls](#)

## Screenshots



## Network Analysis

[Hosts Involved](#)

[DNS Requests](#)

[HTTP Requests](#)

[Dynamic HTTP/HTTPS Requests](#)

## Volatility

---

Nothing to display.

---