FILE | 2015-03-02 17:09:59 | 2015-03-02 17:12:29 | 150 seconds | 1.2-dev

File Details

File name | 1F68A0DF38F63FE821B237BC7BAAB930D_IBanking Chase.apk
File size | 808241 bytes
File type | Java archive data (JAR)
CRC32 | 22C1A158
MD5 | 1f68addf38f63fe821b237bc7baabb3d
SHA1 | 570612b47dc93bba5c9171fd005928107edcee57
SHA256 | 8458a9bc6e51616af96ed5ec7a4fc154bf07729b8d74b59285c9c8d38fbc42e
SHA512 | 9af9afde7c34d7c5deeb886f420aad89a984dc4532bc62a6eff54475abdf684b94e69f8e8965758a185459a04e3e9198a15e2780c6216488f6c4bc01bfe49a7
Sseep | 2d4576:PDO+[APpRUy/z+QiYfJy+gQZldWr1Y:7/BPsyr+Qf4FtIzid6n
PEID | None matched
Yara | None matched

VirusTotal
Permalink
VirusTotal Scan Date: 2015-03-02 13:19:00
Detection Rate: 36/57 (Expand)

Android Application Info

Package | com.biotechnology.icslientsService7
Main Activity | com.soft360.1service.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

SMS Messages
Registered Broadcast Receivers
Reflection Calls
Fingerprints
Content Values
System Properties

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
Nothing to display.