**FTC Zapping Rachel Robocall Contest**

**DEF CON 22 Aug 7-10, 2014**

**PHASE 2: Attacker**

**SUBMISSION: “DROID RACHEL”**

**Summary:**

DROID RACHEL is an Android based “Smartdialer” featuring multi-layered honeypot detection and enabling highly targeted, distributed robocall campaigns. It recognizes and avoids numbers with less human characteristics while focusing on target numbers within the same area code. With 1 billion Android devices in use, DROID RACHEL demonstrates the potential role of mobile devices in distributed Vishing and Smishing campaigns.

**Description of DROID RACHEL’s honeypot circumvention technics:**

1. CARRIER Check: DROID RACHEL is optimized to reach individuals, which are likely customers of AT&T or Verizon. Other carrier + VoIP landlines are ignored.
2. CNAME Check: DROID RACHEL avoids numbers with placeholder “City State” CNAME records. High value targets have valid CNAME records.
3. TYPE Check; DROID RACHEL prefers wireless numbers for higher response rates as well to support remotely configurable SMS campaigns
4. AREA CODE Check; DROID RACHEL matches the area code of the dialer with the target area code for significant higher response rates

Attachment A shows how each of these rules validate **collectively** to **FALSE** for **all numbers provided** in the honeypot. Consequently DROID RACHEL did not attempt to call any of the numbers in the honeypot.

**Additional theoretical circumvention technics with DROID RACHEL:**

1. Active cell phone lines: A significant volume of telemarketing and fraud calls are sent from VoIP based systems today. DROID RACHEL uses higher trusted cellular phone lines.
2. Distributed attack: DROID RACHEL assumes the presence of traffic based detection, it may distribute an attack over millions of devices (across locations, actors, devices and time).
3. SMS is a proven, widely used, alternative platform for soliciting, impersonating and defrauding individuals. DROID RACHEL can be expanded to use SMS exclusively or in combination with robocalls.
4. Viral and low cost: DROID RACHEL can reach new devices (“actors”) as a for-profit application or as malware. DROID RACHEL executes in the device’s idle background, during business hours.

**DROID RACHEL learnings for building better honeypots:**

1. Distributed honeypots: Honeypots must be extended to include ‘live’ numbers connected by top 3 US carriers, and must cover landline and cell phones, across international boarders.
2. Story line detection: Attachment C shows DROID RACHEL force dialing itself. It utilizes a pre-recording which may be remotely fetched. Honeypots must be capable of detecting patterns in campaign story lines (cleartext, biometric voices).

**Submission attachements:**

* Attachment A: “A\_FTC\_Zapping Rachel-Phase2\_DroidRachel\_Algorithm\_08092014.xlsx”
* Attachment B: “B\_FTC\_Zapping Rachel-Phase2\_DroidRachel\_Presentation\_08092014.ppt”
* Attachment C: “C\_FTC\_Zapping Rachel-Phase2\_DroidRachel\_DemoVideo\_08092014.mov”
* Attachment D: “D\_DroidRachel\_08092014.apk” (compiled Android application)
* Attachment E: “E\_DroidRachel\_08092014.zip” (source code of Android application)

**System Requirements for running Droid Rachel:**

* Android 4.3+ devices with active SIM
* “Allow untrusted sources” in Settings > Security
* Email Attachment D “.apk" file to device’s gmail address
* Open email in default Gmail app, tap to install
* Alternatively run DROID RACHEL in Android SDK Emulator

Notes:

* DROID RACHEL campaigns during 8am-10pm local time
* DROID RACHEL campaigns only while device is idle
* DROID RACHEL will self-destruct after 10 campaign runs