Preparation 1

Objective: Establish contacts, define procedures, and gather information to save time during an attack.

- Mobile helpdesk must have a defined process in case of a suspected malware infection: replace the smartphone of the user with a new one and isolate the suspicious device for analysis by the forensic investigator.
- A good knowledge of the usual activity of the smartphone is appreciated (default and extra tools running on it). A smartphone support expert can be helpful to assist the forensic investigator.
- A monitoring should be done to check unusual user bill or network activity.

Identification 2

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

Main points of notification for suspicious smartphone:

- Antivirus raises alerts;
- Unusual system activity, unusually slow system;
- Unusual network activity, very slow Internet connection;
- The system reboots or shutdowns without reason;
- Some applications crash unexpectedly;
- User receive one or multiple messages, some could have unusual characters (SMS, MMS, Bluetooth messages, etc.);
- Huge increase in phone bill or web activity.
- Unusual calls to unusual phone numbers or at unusual hours/days.

Evidence such as website URLs need to be gathered.

Ask the user about his/her usual activity on the smartphone: which websites are browsed, which external applications are installed. This information can optionally be cross-checked with the company's policy.

Containment 3

Objective: Mitigate the attack's effects on the targeted environment.

- Ensure user is given a temporary or new permanent device to avoid any time constraint on the investigation.
- Back up the smartphone data.
- Remove battery to block all activity (wifi, Bluetooth, etc).
- Launch an antivirus check on the computers that are/have been synchronized or linked with the smartphone.
- Send the suspicious smartphone and appropriate components (SIM, battery, power cable, memory cards) to your security incident response team. This team will help to isolate the malicious content and send it to antivirus companies.

Remediation 4

Objective: Take actions to remove the threat and avoid future incidents.

If some encryption or password accesses are set, find out a way to get access to the stored data. If this is not possible, the investigation will suffer high limitations.

Specific tools should be used by your incident response team to lead forensic investigation on the smartphone.

Just for information, here is a short list of tools which can be useful:

Free tools: XDA Utils (Windows Mobile), MIAT (Mobile Internal Acquisition Tool – Symbian, Windows Mobile), TULP2G, Blackberry Desktop Manager

Commercial tools: XRY, Cellebrite, Paraben …

Actions:

- Remove SIM from the smartphone if not already done;
- Recover phone history, web history and all available logs;
- Recover server connections log if available;
- Identify and remove the threat on the smartphone.
- If the threat is related to an installed application, identify its location on Internet and remove it.

Recovery 5

Objective: Restore the system to normal operations.

If user needs to recover from the infected support, define a quarantine period and appropriate anti-virus check, if possible, to ensure nothing could harm user or the company's systems.

Restore the data saved previously from a trusted source on the destination device.

Once the investigations are over, wipe the infected smartphone (if possible) and reset it to factory settings with a pristine firmware and file system, in order to be used again.

Aftermath 6

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Report

An incident report should be written and made available to all of the actors.

The following themes should be described:

- Initial detection
- Actions and timelines
- What went right
- What went wrong
- Incident cost

Capitalize

Actions to improve the smartphone policy should be defined to capitalize on this experience.
Debrief the incident with user to improve his awareness of security problems.

SOCIETE GENERALE | CERT SOCIETE GENERALE

Incident Response Methodology

IRM #9

Malware on smartphone

How to handle a suspicious smartphone

IRM Author: CERT SG / Julien Touche
IRM version: 1.2

E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

Abstract

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.
Who should use IRM sheets?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes and do not panic. Contact your CERT immediately if needed.

Incident handling steps

6 steps are defined to handle security Incidents

- **Preparation: get ready to handle the incident**
- **Identification: detect the incident**
- **Containment: limit the impact of the incident**
- **Remediation: remove the threat**
- **Recovery: recover to a normal stage**
- **Aftermath: draw up and improve the process**

IRM provides detailed information for each step.