INCIDENT RESPONSE METHODOLOGY

# IRM #9 MALWARE ON SMARTPHONE

How to handle a suspicious smartphone

IRM Author: CERT SG
Contributor: CERT aDvens
IRM version: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

C'EST VOUS L'AVENIR
SOCIETE GENERALE

# 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. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.**

**→ IRM CERT SG: https://github.com/certsocietegenerale/IRM**

**→ IRM CERT aDvens (French version): https://github.com/cert-advens/IRM**

# INCIDENT HANDLING STEPS

## 6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

1. Preparation: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process

**IRM provides detailed information for each step of the incident response process. The steps come from NIST Computer Security Incident Handling Guide.**

# PREPARATION

## OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

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.

It is recommended to:

- Enable logging (MDM, applications list or else)
- Install Antivirus/Security apps over smartphone
- Configure a VPN to analyze network activity

For Forensic:

- For Android:
    - Activate Developer options with USB Debugging (be careful it could be a risk, public USB charging facilities for example) or have a process to activate it
    - Unlock OEM options if possible
- Test your extraction routines in advance to make sure they are compatible with your evidence

# IDENTIFICATION

**OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.**

**Main points of notification for suspicious smartphone:**

- Antivirus/Security apps raise alerts
- Check for anomalous rights granted to applications
- Anomalous system activity, unusually slow functioning
- Anomalous network activity, slow Internet connection
- The system reboots or shutdowns without reason
- Applications crash unexpectedly
- User receives one or multiple messages, containing unusual characters (SMS, MMS, Bluetooth messages, etc.)
- Increase in phone bill or web activity
- Calls to unknown phone numbers or at unusual hours/days
- A monitoring should be done to check unusual user bill or network activity

**Ask the user about his/her usual activity on the smartphone: which websites usually visited, which external applications are installed.**

# CONTAINMENT

## OBJECTIVE: MITIGATE THE ATTACK'S IMPACTS ON THE TARGETED ENVIRONMENT.

**Ask the user to provide his/her credentials to access the smartphone including:**

- SIM card PIN code
- Smartphone password
- iCloud login/password
- Google Play credentials,
- backup password…

- Ensure the user is provided with a replacement device to use during the investigation.
- Back up the smartphone data by creating a physical filesystem, logical backup or manual acquisition.
- Put the phone in a faraday bag if available.

**After acquisition, remove the battery (if feasible) or put the phone in the airplane mode to block all activity (WiFi, Bluetooth, etc).**

**Additional actions:**

- Remove the SIM to perform additional analysis outside the smartphone.
- Perform an antivirus or security scan of the backup or acquired files on a dedicated forensic station.
- Perform applicable forensic routine base on your use case.

Specific tools should be used by your incident response team to lead forensic investigation on the smartphone.
**Use a dedicated forensic solution to analyze the captured data or the smartphone (Cellebrite, XRY, Oxygen, Axiom, Andriller, etc.)**

# REMEDIATION

## OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

- Remove the identified threat from the smartphone.

**Or**

- Wipe the infected smartphone and Hard/Soft reset it to factory settings with a pristine firmware.

- Reinsert the SIM card back into the smartphone.

**Signal all identified malicious applications still available through marketplaces for removal.**

# RECOVERY

## OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

- Selectively reinstall saved data and apps from the backup.

**You may consider retaining the device for an additional quarantine period to perform appropriate security checks.**

*For more details on authentication and infrastructure recovery, check the Large-scale malware compromise IRMXXX*

# LESSONS LEARNED

## OBJECTIVE: DOCUMENT THE INCIDENT’S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES.

**Report**

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

Following themes should be described:

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

**Capitalize**

Actions to improve the smartphone policy should be defined to capitalize on this experience.

Debrief the incident with user to improve his/her awareness.