INCIDENT RESPONSE METHODOLOGY

# IRM #8
# BLACKMAIL

Guidelines to handle blackmail attempt

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/certadvens/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.**

**Contacts**

- Identify internal contacts (security team, incident response team, legal department etc.).
- Identify external contacts who might be needed, mainly for investigation purposes like Law Enforcement.
- Make sure that security incident escalation process is defined, and the actors are clearly defined.
- Be sure to have intelligence gathering capabilities (communities, contact, etc.) that might be involved in such incidents.

**Awareness**

- Make sure that all the relevant employees are aware of blackmail issues. This can be part of the security awareness program.

**Verify backup and incident response process is in place and up to date.**

# IDENTIFICATION

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

- Alert relevant people.
- Keep traces of any communications related to the incident (don't send emails to trash; write down any phone contact with phone number and timestamp if available, fax, etc.) Try to get as much details as you can about the author (name, fax, postal address, etc.).
- Examine possible courses of actions with your incident response team and legal team.
- Investigate email to get all the information about the incident (username, MX servers, etc.).
- If internal data is concerned, check you have a safe backup of it and try to find out how it was gathered.
- Include top management to inform them that blackmail is happening and is being handled according to a defined process.

# CONTAINMENT

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

Determine how you can answer to the blackmail and the consequences and costs of ignoring, answering yes or no.

**Most common threats tied with blackmail are:**

- Denial of service
- Reveal sensitive data on Internet (credit card or other personal data from customers or internal worker/director, confidential company data, etc.)
- Reveal sensitive private information about employees/VIPs
- Block your data access (wiped or encrypted through ransomware for example [1])
- Mass-mailing using the brand (spam, sextortion, child pornography [2], bad rumors, etc.)

**Check the background**

- Check if similar blackmailing attempts have taken place in the past. Check if other companies have been threatened as well
- All related technical data should be checked carefully and collected for investigation purposes
- Search if anyone would have any interest into threatening your company:
  - Competitors
  - Ideologically-motivated groups
  - Former or current employees
- Try to identify the attacker with the available pieces of information
- More generally, try to **find how the attacker got into the system or got the object of the blackmail**

**Contact local law enforcement to inform them.**

Try to gain time and details from fraudster. Ask:

- Proof of what he said: example data, intrusion proof, etc.
- Time to get what fraudster wants (money, etc.)

*[1] https://en.wikipedia.org/wiki/Ransomware_(malware)*
*[2] https://en.wikipedia.org/wiki/Sextortion*

# REMEDIATION

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

If a flaw has been identified on a technical asset or a process allowing the attacker to get access to the object of the blackmail, ask for IMMEDIATE fix in order to prevent another case.

- After getting as much information as possible, ignore the blackmail and ensure appropriate watch is in place to detect and react accordingly on any new follow-ups.
- Don’t take any remediation decision alone if strategic assets or human people are targeted. Involve appropriate departments.

**Remember that a positive answer to the fraudster is an open door for further blackmails.**

# RECOVERY

## OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.

Notify the top management of the actions and the decision taken on the blackmail issue.

*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.**

If you don't want to file a complaint, at least notify Law Enforcement as other organizations could be affected. At the same time, inform hierarchy and subsidiaries to have a unique position in case the fraudster tries to blackmail another internal department.

**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 blackmail handling processes should be defined to capitalize on this experience.