

# INCIDENT RESPONSE METHODOLOGY

# **IRM #1**

# **MALWARE**

# **INFECTION**

# **RESPONSE**

---

Guidelines to handle information  
system Worm infections

IRM Author: CERT SG

Contributor: CERT aDvens

IRM version: 2.0

E-Mail: [cert.sg@socgen.com](mailto: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. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.**

## References:

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

- Define actors, for each entity, who will be involved into the crisis cell. These actors should be documented in a contact list kept permanently up to date.
- Make sure that analysis tools are up, functional (EDR, Antivirus, IDS, logs analyzers), not compromised, and up-to-date.
- Make sure to have architecture map of your networks.
- Make sure that an up-to-date inventory of the assets is available.
- Perform a continuous security watch and inform the people in charge of security about the threat trends.

# IDENTIFICATION

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

## **Detect the infection**

Information coming from several sources should be gathered and analyzed:

- Antivirus logs
- IDS/IPS
- EDR
- Suspicious connection attempts on servers
- High number of locked accounts
- Suspicious network traffic
- Suspicious connection attempts in firewalls
- High increase of support calls
- High load or system freeze
- High volumes of e-mail sent

**If one or several of these symptoms have been spotted, the actors defined in the “preparation” step will get in touch and if necessary, create a crisis cell.**

## **Identify the infection**

Analyze symptoms to identify the malware, its propagation vectors and countermeasures.

Leads can be found from:

- CERT’s bulletins
- External support contacts (antivirus companies, etc.)
- Security websites
- Threat intelligence capabilities and providers

**Notify Chief Information Security Officer.**

**Contact your national CERT and regulators if required.**

## **Assess the perimeter of the infection**

Define the boundaries of the infection (i.e.: global infection, bounded to a subsidiary, etc.).

If possible, identify the business impact of the infection.

*For more details, check the Windows and Linux intrusion IRM-2 and IRM-3*

# CONTAINMENT

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

The following actions should be performed and monitored by the crisis management cell:

### Disconnect the infected area from the Internet.

1. Isolate the infected area. Disconnect it from any network.
2. If business-critical traffic cannot be disconnected, allow it after ensuring that it cannot be an infection vector or find validated circumventions techniques.
3. Neutralize the propagation vectors. A propagation vector can be anything from network traffic to software flaw. Relevant countermeasures have to be applied (patch, traffic blocking, disable devices, etc.).

For example, the following tools/techniques can be used:

- EDR
  - Patch deployment tools (WSUS)
  - Windows GPO
  - Firewall rules
  - Operational procedures
4. Repeat steps 2 to 4 on each sub-area of the infected area until the worm stops spreading. If possible, monitor the infection using analysis tools (antivirus console, server logs, support calls).

**The spreading of the malware must be monitored.**

### Mobile devices

- Make sure that no laptop, Smartphone or mobile storage can be used as a propagation vector by the malware. If possible, block all their connections.
- Ask end-users to follow directives precisely.

**At the end of this step, the infection should be contained.**

# REMEDIATION

---

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

## Identify

Identify tools and remediation methods.

The following resources should be considered:

- Antivirus signature database
- External support contacts
- Security websites
- Yara scan, Loki, DFIR-ORC, ThorLite
- EDR search

**Define a disinfection process. The process has to be validated by an external structure, i.e. CERT, SOC, Incident Response team.**

**The most straight-forward way to get rid of the worm is to remaster the machine.**

## Test

Test the disinfection process and make sure that it properly works without damaging any service.

## Deploy

Deploy the disinfection tools. Several options can be used:

- EDR
- Windows WSUS and GPO
- Antivirus signature deployment
- Manual disinfection
- Vulnerability patching

**Warning: some worm can block some of the remediation deployment methods. If so, a workaround must be found.**

**Remediation progress should be monitored by the crisis cell.**

# RECOVERY

---

## **OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS.**

Verify all previous steps have been done correctly and get a management approval before following next steps:

1. Reopen the network traffic that was used as a propagation method by the malware
2. Reconnect sub-areas together
3. Reconnect the mobile laptops to the area
4. Reconnect the area to your local network
5. Reconnect the area to the Internet

**All these steps shall be made in a step-by-step manner and a technical monitoring shall be enforced by the crisis team.**

*For more details on authentication and infrastructure recovery, check the Large-scale malware compromise IRM-18*



# LESSONS LEARNED

---

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

## **Report**

A crisis report should be written and made available to all of the actors of the crisis management cell.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

## **Capitalize**

Actions to improve the worm infection management processes should be defined to capitalize on this experience.