GARR Security Incident Management Procedure

Foreword

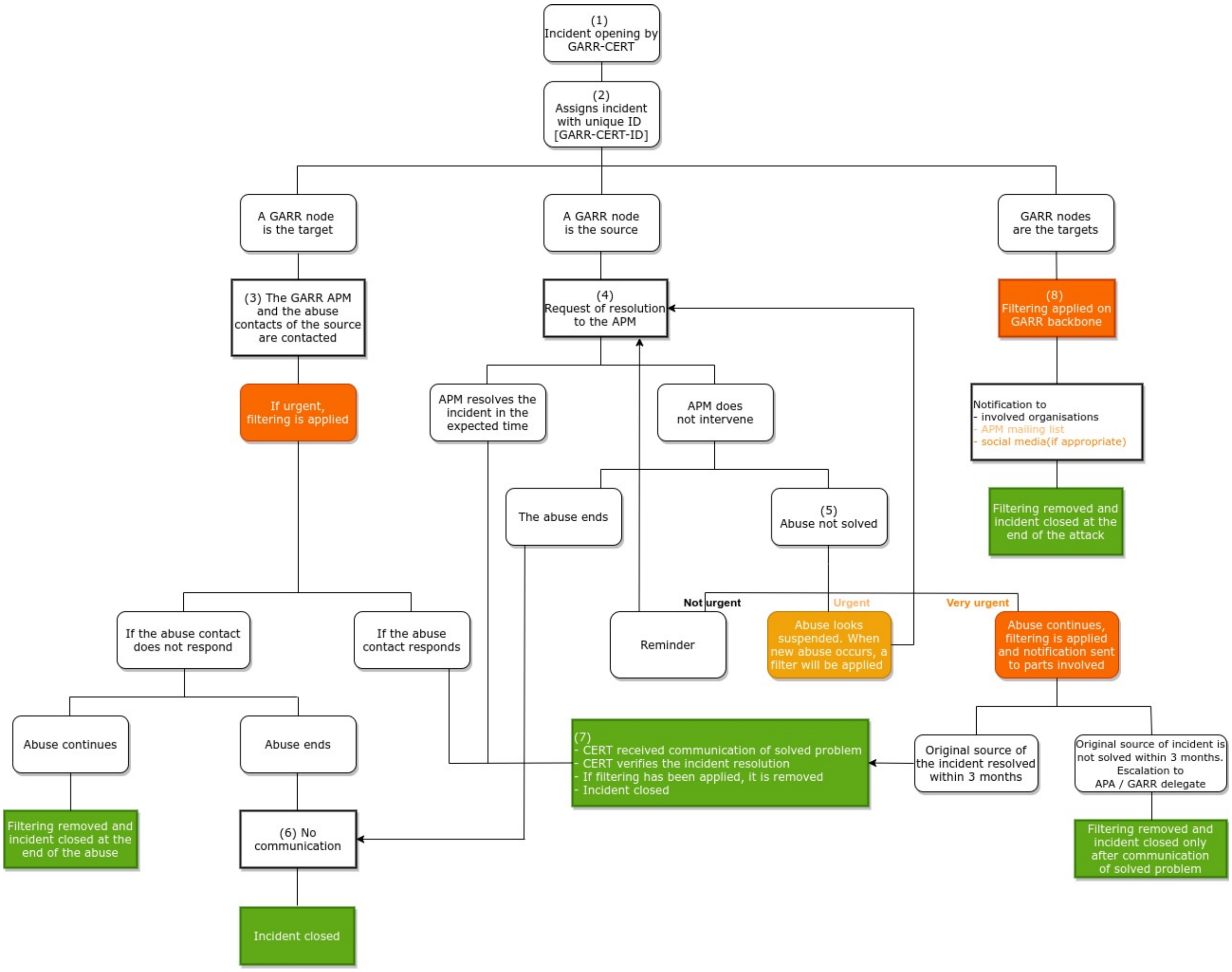
Contacts for security incidents
Each organisation connected to GARR network must appoint a local technical contact point, the APM (Access Port Manager). The APM manages the connection with GARR network and is technical liaison between the organisation and GARR also for the management of security incidents. The APM definition is available on the GARR institutional website.

Communications
Communication between GARR-CERT and involved organisations are usually performed via digitally signed e-mails

Protection from distributed external attacks
Since October 2019, GARR network is equipped with an automatic system for the mitigation of some types of external attacks, which are distributed and aimed at creating disservices (DDoS - Distributed Denial of Service). This system is based on Corero|Juniper technology. When some indicators exceed the threshold values, the network devices react and selectively eliminate the traffic corresponding to this type of attack by applying temporary filters, thus allowing the individual nodes to maintain normal network functionality. The procedure is automatic, without any user intervention. The indicators to be used and the respective threshold values are configured by GARR-NOC.

Filtering
In some special cases, incident management involves filtering one or more network addresses on routers managed by GARR. We would like to emphasize that the application of these filters is always intended to protect and safeguard the functionality of the network and the connectivity services available to users of the GARR network. In the most evident case in which GARR IPs are the direct or indirect targets of an external attacke, the request for intervation of filtering by CERT/NOC often comes from users (APMs) themselves, asking to recover access to their devices and possibly intervene on their configurations in order to mitigate the problem also at the local level. In the event that GARR IPs are clearly the source of illicit traffic and there is no response from the APM in the expected times, the IPs involved are filtered by GARR (with the criteria described in the security incident management procedure), in order to protect its users and prevent any possible legal consequences. Three months after the filtering, in the absence of a response from the APM, GARR will proceed to inform the APA and the GARR Delegate of the competent Authority (escalation).

Workflow


(1) Incident opening by GARR-CERT
(2) Assigns incident with unique ID [GARR-CERT-ID]
A GARR node is the target
A GARR node is the source
GARR nodes are the targets
(3) The GARR APM and the abuse contacts of the source are contacted
(4) Request of resolution to the APM
(8) Filtering applied on GARR backbone
If urgent, filtering is applied
APM resolves the incident in the expected time
APM does not intervene
Notification to
- involved organisations
- APM mailing list
- social media(if appropriate)
The abuse ends
(5) Abuse not solved
Filtering removed and incident closed at the end of the attack
Not urgent
Urgent
Very urgent
If the abuse contact does not respond
If the abuse contact responds
Reminder
Abuse looks suspended. When new abuse occurs, a filter will be applied
Abuse continues, filtering is applied and notification sent to parts involved
Abuse continues
Abuse ends
(7)
- CERT received communication of solved problem
- CERT verifies the incident resolution
- If filtering has been applied, it is removed
- Incident closed
Original source of the incident resolved within 3 months
Original source of incident is not solved within 3 months. Escalation to APA / GARR delegate
Filtering removed and incident closed at the end of the abuse
(6) No communication
Filtering removed and incident closed only after communication of solved problem
Incident closed

Security Incident Management Procedure in use at GARR-Cert

1. When a security issue occurs to an organisation connected to GARR network, GARR-CERT evaluates the opening of a security incident and decides: its priority, the resolution procedures and the communications with the subjects involved.

2. GARR-CERT assigns an unique ID number to the incident (Ticket ID).
   - In the event that a GARR entity or user is the victim of the illegal event, go to point 3.
   - In the event that the the illegal event originates from GARR entity or user, go to point 4.
   - In the event that the illegal event originates from one or more sources and is intended against multiple GARR users, go to point 8.

3. GARR-CERT informs the APM and the appropriate contacts for the system originating the abuse origin. In cases of particular gravity and urgency, GARR-CERT assesses whether it to apply a temporary filter (through GARR-NOC) in order

to mitigate the attack, when not already applied by the automatic DoS mitigation system.

- If the abuse ends and the reference contact for the system originating it does not respond, go to point 6.
- If the contact for the system that originated the abuse responds, go to point 7.
- The incident is closed on its own after the abuse ends.

4. GARR-CERT asks the APM to resolve the incident within a time commensurate with the seriousness of the case (below, some examples of issue resolution times). Whenever possible, GARR-CERT also provides useful tips, if necessary. If deemed appropriate, GARR-CERT also responds to those who reported the accident.
    - In the event that the APM intervenes within the required time, go to point 7.
    - In the event that the APM does not intervene within the required time and the abuse ceases, go to point 6.
    - In the event that the APM does not intervene within the required time and the abuse continues, it follows in point 5.

5. GARR-CERT proceeds in one of the following ways, depending on the seriousness of the case:
    - Sends a reminder (2nd communication, etc.) to the APM, inviting them again to intervene . Go back to step 4.
    - Sends a filtering notice to the APM (and a copy to GARR-NOC and to GARR management) stating that if the illicit event continues or reoccurs, GARR-NOC will apply the appropriate temporary filtering, without further notice. Go back to step 4.
    - Requests the application of a suitable filter to GARR-NOC and, after confirmation of filtering, GARR-CERT notifies the APM and the other parties involved.
    - f within three months from the application of the filtering, the APM intervenes to resolve the problem, go to point 7, otherwise GARR-CERT will proceed to inform the APA and the GARR Delegate of the competent Authority; the incident will therefore be closed and the relative filter removed only following the communication of resolution.

6. GARR-CERT does not receive any communication: the incident is automatically closed.

7. GARR-CERT receives the communication of the issue resolution and, when technically possible, verifies the actions taken before closing the incident and alerting all parties involved. If a filter has been applied by GARR-NOC, GARR-CERT requests its removal and waits for confirmation before closing the incident.

8. Having analysed the attack through the available monitoring tools, GARR-CERT and NOC coordinate to apply a filter on the GARR backbone. A notification is sent to the appropriate contacts for the network or networks originating the abuse, to the users involved (individually or though the APM mailing list) and eventually the news is published following the communication channels of GARR [web, social]. The closure of the incident and the removal of the filters on the backbone are subject to verification of the end of the attack.

Types of incidents currently treated (with indication of the incident response time)

Depending on the type, below are listed the expected time required for the APM to resolve the incident starting from the notification. In case the APM needs more time to resolve the incident, it is necessary to make an explicit request to GARR-CERT.

- Phishing (4 hours)
- DoS (5 hours)
- Connection Attempts (1 day)
- Compromised Node/Account (1 day)
- Probe (1 day)
- Malware/Virus (1 day)
- Vulnerable Node/Account (3 days)
- Spam (3 days)
- Piracy (3 days)

In case of emergency

Even outside the NOC and CERT operating hours, In the event of an incident which significantly impacts user connectivity, such as a distributed SYNFlood, the managers of GARR-NOC and CERT decide how to:

- a) apply any filters at the GARR router level also within times shorter than those foreseen in the Incident Management Procedure,
- b) send a communication to the users involved and, after hearing the Director of the Network Department [and/or GARR Director], if and how to disseminate the event and details to other subjects or publicly.

Other cases that expose users to serious security problems, for example in the case of ongoing data breaches involving particular data, can also be treated as a precaution as in the previous point (a).

Regulatory references

The updating of GARR Security Incident Management Procedure is due, in addition to the evolution of the types of threats to the network and user systems, also to the evolution of the regulations in force in Italy related to cybercrime.

Before the recent directives contained in the Minimum Security Measures for the Public Administration (AgID, 26/4/2016 - https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict) and transposition in Italy of the European Regulation for the Protection of Personal Data (Legislative Decree 101/2018 - https://www.garanteprivacy.it/web/guest/provvedimenti/provvedimenti-a-carattere-generale), cybercrime appears for the first time in Italy with Law 547 of 1993, which introduces changes and additions to the Criminal Code and the Criminal Procedure Code regarding cybercrime.

These are, to date, the cybercrimes punished by the Italian Penal Code (courtesy translation):

- **Computer fraud** - Article 640 ter of the Penal Code, it consists in altering an IT system to obtain an unfair profit. Penalty envisaged: imprisonment from six months to three years and a fine of 51 to 1.032 euros. Examples: phishing.
- **Abusive access to an IT or telecommunication system** - Article 615 ter of the Penal Code, It is an access by a person entering an IT or telecommunications system protected by security measures, or remains there against the express or tacit will of those who have the right to exclude it. Planned penalty: imprisonment of up to three years. According to the jurisprudence of the Supreme Court of Cassation, the offence under examination is committed by the person who, despite being authorised, accesses or maintains himself in a protected computer or telecommunication system, violating the conditions and limits resulting from the complex of prescriptions given by the system owner to delimit objectively access.
- **Unauthorised possession and dissemination of access codes to computer and telecommunication systems** - Article 615 quater of the Italian Penal Code punishes with imprisonment of up to one year and a fine of up to 5 164 euros. Crimes committed by those who - in order to obtain a profit for themselves or to harm others - illegally procure, reproduce, disseminate, communicate or deliver codes, keywords or other means suitable for accessing a computer or telecommunication system, protected by security measures, or in any case provides indications or instructions suitable for the aforementioned purpose.
- **Dissemination of equipment, devices or computer programs aimed at damaging or interrupting an IT or telecommunication system**- Article 615 quinquies of the Italian Criminal Code Imprisonment of up to two years and a fine of up to € 10 329 for the dissemination of equipment, devices or IT programs aimed at damaging or interrupting an IT or telecommunication system. The offence is committed by those who procure, produce, reproduce, import, disseminate, communicate, deliver or, in any case, make available to other equipment, devices or computer programs for the purpose of unlawfully damaging an IT or telecommunication system, information, data or programs contained therein or relevant to it or to favor the interruption, total or partial, or the alteration of its functioning.
- **Illegal interception, impediment or interruption of communications** - Articles 617 quater and 617 quinquies of the Italian Penal Code Those who, without being authorised, intercept, prevent, interrupt or reveal IT communications and who install equipment aimed at intercepting, interrupting or preventing IT communications are respectively sanctioned.
- **Falsification, alteration, suppression of communications and damage to systems** - Those who falsify, alter or suppress the computer communication acquired through interception (article 617 sexies of the criminal code) and who destroy, deteriorate, or delete, data, information are also sanctioned by the penal code o computer programs (article 635 bis of the criminal code). And, with regard to the crime of violation and theft of correspondence, law no. 547/1993, updating article 616 of the Italian Penal Code, specifies that "correspondence" means correspondence by letter, telegraph, telephone, IT or carried out with any other form of distance communication.