Abuse Report Investigation Process

Abuse reports are received by our request tracking system, RT - Request Tracker, so that each case/thread will be threated by our Abuse Team.

Tickets can be generated:

- by other ISPs
- by BL (BlackList) maintainers - RBL, DNSBL and URI DNSBL -
- by Abuse form available on the page: www.register.it/abuse
- by internal monitoring system, 24/7

Abuse classification:

- internal suspension notification to track each abuse activity;
- clients requests for email/dns/hosting reactivation after service suspension;
- ISP or BL warning notifications about SPAM or other service violations or attempts of;
- Copyright infringement violations;
- ISP or BL notifications of fraudolent activities like Phishing emails or Phishing web-site hosting.

Based on the case type and on the requestor type, each case can be threated differently, basic steps upfront a malware/fraudolent notification are:

- abuse h24 activity is triggered after a monitoring alert, or external notification (usually a suspension activity);

- service is suspended for website or domain or mailbox, and the client is notified about it (abuse@register.it is in cc), eventually the requestors of this suspension will receive a reply from Abuse team stating that the particular fraudolent service notified was suspended (or IP Address put in black-hole).

The notification sent to clients after hosting suspension, will include a complete virus/malware scan of the hosting web space, along with the possible causes of illegal uploaded files causing the fraudolent activity. This will lead the client to remove the infected files and eventual exploits or vulnerabilities before asking for service re-activation. The same hosting web space scan will be done prior eventual hosting service reactivation request.

If the suspension is about a mailbox user or a dedicated server, clients will be warning about basic security improvement steps to secure up the service.

Copyright infringement notification will be forwarded to clients.

To better track and summarize cases by domain or client we do set tag/label for each case (both manually and automatically) and to ease up the job when we need to search for some cases, creating an "abuse cases search tool" on top of our request tracking system.

The Abuse reports are stored on our db for at least 2 years