Training DNII – DIVTEC on site

From June 30th, 2014 to July 4th. 2014

Explanations and tests made

- User/Groups administration.
  - Explanations about mangagement and about different kind of privilegies.
- Monitor: System and license status.
  - A license update was perfomed to exten maintenance to July 10th
- Audit: history of users and system actions
- System: management of system architecture.
  - VPSs management and anonimyzers installation. One VPSs was substituted by a new one and instructions were given in case DNII wants to use their own VPSs for anonymizers.
  - Review of system status and check of Backups status (DNII needs to set an external drive).
  - Explanation about log viewing and understanding.
- Operations:
  - Structure: operations, target, factories and agents.
  - Creation and edition and management of every instance, including Closing and Deleting.
  - Factory creation and configuration. Including templetes, export/import and vectors generation.
  - Vectors deploying in Android, Blackberry and iPhone. All phones provided both by DNII and Hackingteam.
    - Local installation
    - Installation package
    - Melted application
    - SMS (WAP push was tested but not suppported by operator)
    - QR / Web link
- Analysis:
  - Dashboard management
  - Filtering and editing (relevance, notes and report marking)
  - Filter templates
  - Alerting system to be warned by new instances, evidences matching filters and synchronizations.
  - Evidence exportation:
    - Single evidences
    - Reports in HTML with content filtered by analyst.

Notes about activities and about DIVTEC team:

DNII DIVTEC has a working room with around 10 working stations and 10 people were attending the explanations and practising.

Working time was from 10AM to 5PM with 1 hour for lunch. Following client schedules.

Every day, was performed theory and practice about different parts of RCS and, all questions that were not possible to solve at the moment, were answered day after through HT support people answers.

As in real operations, we have experienced disconnections and different levels of success during infections. All of them reasonable.

Client has performed tests and practices on several phones and realized that every combination of software-harware is different, therefore, agents deployed can gather different levels of information.

Client realized that every phone kind have some infection ways, not commong always among all. I.e. some can be infected localy though cable and others through a downloaded application.

DIVTEC team has the knowledge and capabilities to, with practising, perform successfull operations in future. They have understood that an infection is not just technical work, but, in most times, also social engineering. They have the target of go even deeper on tests to realize, as much as possible, what are they able to do and under what conditions and environment.

Client has been told about other RCS users success operations and operative style. Target of these dialogs was to improve DIVTEC imagination regarding atacks and operations, and also regarding the cooperation with other teams working on the ground or like lawful interception team to gather information about targets to improve infection possibilites.

Team has been explained about the HT support and maintenance service. They can access it anytime they need in order to request support or report problems. This service includes also every update released by HT during maintenance period, so their feedback is always welcome by HT to improve RCS performance and capabilities.

July 4th, 2014

NICE

Hacking Team