b. Advanced training (10 days)

The advanced training course will be performed in Italy at HT premises and it will be focused on specific hacking and security subjects.

Content of the course will be customized depending on skill levels (which need to be at least medium) and includes Hacking Techniques and Remote Infection Vectors for installing Client Modules.

Skill level required for attending this training session is medium/high.

Attendees should have good knowledge of IP Networking, Windows and Linux operating systems.

Application level protocols, basic programming skills (scripts, C, HTML as minimum).

The training will be designed for both PC and Mobile platforms and includes:

- Introduction to hacking and exploitation techniques
- Social Engineering techniques
- Attack simulation made from Internet
- Attack performed inside the LAN
- Application security
- Advanced technologies for probing and fingerprinting
- Remote Infection: Injection Proxy
- Remote Infection: Client side exploits
- Remote Infection: Website malicious content
- Remote Infection: Exploit Portal
- Remote Infection: Remote Mobile Infection
- Remote Infection: Mail attachment

THIRD DAY – Training for Viewer
Learn best practices for information collected by RCS.
Skill level: basic, internet applications knowledge required.

Activities
Viewing information
Viewing of information collected by each individual agent
- Key logger
- URL monitoring
- User/password monitoring
- Screen Snapshot
- Printing monitoring
- Clipboard monitoring
- File Capture
- Crisis
- VoIP
- Microphone
- Webcam
- Instant Messaging
- Mail Messaging
- SMS/MMS
- Call
- Location Tracking
Analysis of information
Perform query within information
- Clarify what do the different query parameters mean
Perform query within information collected across different agents on one target
Perform query across targets
Export options for collected information
Export options for query results

FOURTH DAY – Training for technical operator
Learn best practices for operational configuration of RCS.
Skill level: medium. Knowledge of IP networking, Windows/Linux/Mobile operating systems.

Activities
Method of infection
Explanation of exe melting procedure.
- Practice melting with common executables
- Practice using USB and CD boot infection method
- Explanation and practice of injection proxy method Using PC/laptop
Creation of Backdoor for PC and Mobile
Explanation of each trigger event
- Executed Processes
- Network Connection
- Screensaver start/stop
- Date/Time
- Windows Event
- Quota
- On Call

Headquarters: Via della Moscova, 13 20121 Milano
Tel. +39 02 29060603 – Fax +39 02 63118946
e-mail info@hackingteam.it – web http://www.hackingteam.it
P.IVA. 03924730967 – Capitale Sociale € 223.572,00 i.v.
N° Reg Imprese / CF 03924730967 – N° REA 1712545
- 17 -
HT S.r.l.
Offer n. 201002014-3 MB

- On battery
- On SIM changes
- On connection
Explanation of each agent type (including limitations)
- Key logger
- URL monitoring
- User/password monitoring
- Screen Snapshot
- Printing monitoring
- Clipboard monitoring
- File Capture
- Crisis
- VoIP (i.e. Skype)
- Microphone
- Webcam
- Instant Messaging
- Call Logging
- GPS Logging
- Cell Logging
- SMS/MMS capture
- Contact list capture
- Calendar/Task capture
- Mail Messages
Explanation of actions sent to backdoor
- Synchronize
- Start / Stop agent
- Uninstallation
- Command Execution
- Send SMS
Controlling Client Module
Explanation of available actions to control backdoor.

Headquarters: Via della Moscova, 13 20121 Milano
Tel. +39 02 29060603 – Fax +39 02 63118946
e-mail info@hackingteam.it – web http://www.hackingteam.it
P.IVA. 03924730967 – Capitale Sociale € 223.572,00 i.v.
N° Reg Imprese / CF 03924730967 – N° REA 1712545
- 18 -
HT S.r.l.
Offer n. 201002014-3 MB