]HackingTeam[

EXHIBIT A (TRAINING)

a. RCS Training (5 days)

The advanced training course will be performed at Customer premises and it will be focused on Remote Control System Installation and Operation.
Training session is designed for up to six attendees **for 5 full days.**

| **FIRST DAY - Installation of RCS** |
| Documentation of the installation process to ensure subsequent installations can be performed without assistance of HT |
| Skill level basic to medium. Linux/Windows operating system administration required and IP Networking. |
| **Activities** |
| Installation of RCSDB |
| - Installation procedure |
| - Required configuration for host OS including ports to be opened |
| Installation of ASP server |
| - Installation procedure |
| - Required configuration for host OS including ports to be opened |
| - Configuration of dummy web server and document options available |
| Installation of Console (Administrator, Configurator, Viewer) |
| - Installation procedure |
| - Required configuration |
| Installation of Mediation Node |
| - Installation procedure |
| - Required configuration |
| Installation of Anonymizer Network |
| - Installation procedure |
| - Required configuration |

| **SECOND DAY - Training for system administrator** |
| Learn best practices for administrative configuration of RCS. |
| Skill level basic. Internet applications knowledge required. |
| **Activities** |
| Configuration of roles and permissions |
| Setup initial user accounts, user groups including appropriate permissions for each user group |
| - Administrator |
| - Technical |
| - Viewer |
| Basic verification that RCS system works using simple client module |
| - Creation |
| - Infection |
| - Trigger and reporting to ASP/RCSDB of captured information |
| - Viewing of captured data |
| - Shutdown of client module |

Management of Activities and Targets
- Creation of activities and targets
- Closure of activities and targets

Perform auditing

Establish procedure for regular audit of access and actions performed by users accordingly to roles
- Admin
- Tech
- User

Monitor system health

Establish procedure to monitor health of critical system components and interventions to be performed when situations arise for
- RCSDB
- ASP
    - o RSS
    - o RSSM
    - o RLD
    - o RNC

Procedure for applying patches/upgrades

Performing backup/disaster recovery

Establish critical files required for disaster recovery in
- RCSDB
- ASP
    - o RSS
    - o RSSM
    - o RLD
    - o RNC

Establish procedure for disaster recovery using backup files

THIRD 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
- On battery
- On SIM changes
- On connection

Explanation of each agent type (including limitations)
- Key logger
- URL monitoring

- 2 -
HT S.r.l.
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° R.E.A. 1712545

- Userid/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.

FOURTH 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
- Userid/password monitoring
- Screen Snapshot
- Printing monitoring
- Clipboard monitoring
- File Capture
- Crisis
- VoIP
- Microphone
- Webcam
- Instant Messaging
- Mail Messaging
- SMS/MMS
- Call
- Location Tracking

- 3 -
HT S.r.l.
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° R.E.A. 1712545

Analysis of information
Perform query within information collect by a single agent
-    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

FIFTH DAY – Ticket Support System Learn best practices for using the Support System. Skill level basic. Internet applications knowledge required.
Activities
<u>Viewing information</u> -   Ticket Management -   Secure File Transfer -   Secure Portal Access
Anonymizer Network Learn best practices for using the Anonymizer chain. Skill level basic. Linux and Internet applications knowledge required.
Activities
<u>Viewing information</u> -   Anonymizer Management

]HackingTeam[

b. Advanced training (5 days) - Hacking Techniques and Security

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.

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

- Introduction to hacking and exploitation techniques
- Attack simulation made from Internet
- Attack performed inside the LAN
- Remote Infection: Injection Proxy
- Remote Infection: Remote Mobile Infection (WAP Push)
- Remote Infection: Client side exploits
- Remote Infection: Website malicious content
- Remote Infection: Mail attachment

Training session is designed for six attendees **for 5 full days.**

Attendees should have good knowledge of IP Networking, Windows and Linux operating systems, Application level protocols, basic programming skills (scripts, C, HTML as minimum).