

]HackingTeam[

RCS Tactical Device

[Datasheet](#)

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l. The systems described in this document are furnished under a license agreement or non-disclosure agreement.

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of HT s.r.l. and protected by international copyright laws. Permission is granted to view and photocopy (or print) materials from this document for personal, non-commercial use only. Any other copying, distribution, retransmission or modification of the information in this document, whether in electronic or hard copy form, without the express prior written permission of HT s.r.l., is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

All contents of this document are: Copyright © 2012 HT s.r.l. All rights reserved.

Document Approval

Revision	Author(s)	Release Date
1.0	Valeriano Bedeschi	16 th April 2012

Table Of Contents

1	Overview.....	4
1.1	Deployment scenarios.....	4
1.1.1	Wireless cracking.....	4
1.1.2	Target identification.....	4

1

Overview

HackingTeam's *Tactical Device* is a laptop computer that can be used to perform different tasks in a tactical scenario when the operator has the ability to physically be close to the target. The disk is entirely encrypted in order to guarantee security.

The Tactical Device contains software that allows the operator to infect the target with RCS Agent using the Tactical Network Injector capabilities. It also support the cracking process of the Wi-Fi encryption key and the identification of the target while the operation is in progress.

Deployment of the Tactical Device can be done inside any network: from small home Wi-Fi networks to public hotspots (airports, pubs, hotels).

The Tactical Device comes with all the equipment needed: Wi-Fi network cards, Ethernet adapters and a 3G modem to guarantee connectivity in any scenario.

Wi-Fi cards support all the standard networks (802.11a, 802.11b, 802.11g, 802.11n), and optionally provide removable antennas with RP-SMA connectors that allow the operator to use any kind of external equipment.

Additional batteries are provided for long tactical operations, besides power adapters and a hard case for carrying everything safely.

1.1 Deployment scenarios

The target infection using the Tactical Device consists in two different steps: intrusion and infection.

In the first optional step the operator has to gain access to the same network used by the target, while the second step is the identification of the target device and the injection of the RCS Agent into the network traffic using the Tactical Network Injector.

1.1.1 Wireless cracking

If the target is connected to a protected Wi-Fi network, the operator needs to know the passphrase to authenticate the Tactical Device.

If this information isn't available via different channels, the Wireless Network Intruder can be used to break the security.

Supported encryptions are Wired Equivalent Privacy (WEP-40 and WEP-104), Wi-Fi Protected Access (WPA-Personal, WPA2-Personal) and Wi-Fi Protected Setup (WPS).

1.1.2 Target identification

The identification of the target can be done in realtime during the operation.

The Tactical Network Injector monitors all the clients connected to the network and gathers

information about hostnames and visited webpages: in that way the operator can select the real target without reconfiguring the injection rules serverside.

1.1.3 Target infection

The deploy of the RCS Agent is performed using the Network Injector. The Tactical Device needs to be connected to the Internet using any kind of connection available (wired, wireless or 3G)