]HackingTeam[

REMOTE CONTROL SYSTEM **V5.1**

A Stealth, Spyware-Based System for Attacking, Infecting and Monitoring Computers and Smartphones. Full intelligence on target users even for encrypted communications (Skype, PGP, secure web mail, etc.)

D. Vincenzetti, V. Bedeschi

Virtual invasions prompt real fears

NEWS ANALYSIS

China's success in accessing Pentagon networks highlights the need to counter cyber-attacks, says **Demetri Sevastopulo**

Lieutenant General Robert Elder, senior US Air Force officer for cyberspace issues, recently joked that North Korea "must only have one laptop" to make the more serious point that every potential adversary – except Pyongyang – routinely scans US computer networks.

North Korea might be impotent in cyberspace but its neighbour is not. The Chinese military sent a shiver down the Pentagon's spine in June by hacking into an unclassified network used by policy advisers to Robert Gates, defence secretary. While the People's Liberation Army has been probing Pentagon networks hundreds of times a day for the past few years, the US is ever more alarmed at the growing frequency and sophistication of the attacks.

The Pentagon spent several months deflecting the onslaught before the PLA penetrated its system, which was shut down for more than a week for diagnosis.

While officials are concerned that China might have downloaded information, they are more concerned about the strategic ramifications.

One senior US official said there was "no doubt" that China was monitoring e-mail traffic on unclassified government networks.

Intelligence professionals say China has found a simple way to compensate for its lack of expertise in recruiting non-Chinese spies in the US.

China has also come under scrutiny outside Washington. At a recent press conference with Angela Merkel, the German chancellor, Wen Jiabao, the Chinese premier, expressed "grave concern" over reports that the PLA had used "Trojan Horse" programmes to insert spyware into German government networks.

While Chinese military doctrine stresses the importance of cyberspace, many other countries, including the US, engage in electromagnetic trespassing.

Estonia accused Russia of orchestrating a massive attack that temporarily crippled government networks.

The Defence Science Board, an independent Pentagon advisory group, will soon publish a study on non-conventional military challenges that will examine cyber threats.

A former senior US official said the US had made headway in the area but that more needed to be done.

The US Air Force will soon create a cyber war-fighting command aimed at improving defensive and offensive capabilities to counter such asymmetric threats. "We want to ensure that we can operate freely in the domain," says Major General Charles Ickes, another senior Air Force official involved with cyberspace issues. "On the other hand . . . it is seen by everybody in the defence department as a war-fighting domain and you must have offensive capability."

Gen Ickes says the military must ensure that its actions do not inadvertently affect US civilian computer systems. Michael Green, former senior Asia adviser to President George W. Bush, points to an example where the Pentagon had to consider the legal ramifications of blasting a virus back at a hacker.

In an increasingly networked world, governments range of cyber threats, including terrorist attacks on critical infrastructure, commercial espionage and old-fashioned spying.

France and Germany have imposed restrictions on senior officials using BlackBerries out of concerns that US intelligence agencies could intercept sensitive e-mails.

Voicing similar concerns, the White House has imposed a ban on officials using the devices in some countries, including China. It is also examining whether to restrict domestic use, in a move to panic large swaths of Washington's BlackBerry-addicted officialdom.

Sami Saydjari, chief executive of Cyber Defense Agency and a former Pentagon cyber expert, warns of the potential for terrorist groups, such as al-Qaeda, to attack the financial, telecommunications and power sectors. To underscore the threat, he says that no cyber red team – hackers enlisted to attack systems to help identify weaknesses – has ever failed in its objective.

Gregory Garcia, assistant secretary for cyber security at the department of Homeland Security, says the number of cyber incidents reported to the department's computer readiness team so far this year is 35,000. That compares to 4,100 for the whole of 2005.

FINANCIAL TIMES

Number One Southwark Bridge, London SE1 9HL Tel: +44 20 7873 3000

SUBSCRIPTIONS:
Tel: +44 20 7775 6000
Fax: +44 20 7873 3428
fte.subs@ft.com
www.ft.com/subscribetoday
ADVERTISING:
Tel: +44 20 7873 3794 emeaads@ft.com
www.ft.com/advertising
CUSTOMER SERVICE:
Tel: +44 20 7775 6000
reader.enquiries@ft.com
LETTERS TO THE EDITOR:
Fax: +44 20 7873 5938
letters.editor@ft.com

Published by: The Financial Times Limited, Number One Southwark Bridge, London SE1 9HL, United Kingdom; Telephone: +44(0) 20 7873 3000; Fax: +44(0) 20 7407 5700; Editor: Lionel Barber.

Printed by: (Belgium) BEA Printing sprl, 16 Rue de Bosquet, Nivelles 1400; (Germany) Dogan Media Group, Hurriyet AS Branch Germany, An der Brucke 20-22, 64546 Morfelden - Walldorf; (Italy) Poligrafica Europa, S.r.l, Paderno Dugnano (M1), via Luigi Einaudi n. 21/23 Milan; (South Africa) Caxton Printers a division of CTP Limited, 16 Wright Street, Industria, Johannesburg; (Spain) Recoprint Impresion, S.L. Polig. Ind. Las Arenas, c/Ronda S/N, Ctra. de Andalucia km 17,500, 28320 Pinto, Madrid. (Sweden) Bold Printing Group/Boras Tidning Tryckeri AB, Odegardsgatan 2, S-504 94, Boras; (UAE) Al Nisr Publishing LLC, PO Box 6519, Dubai.

France: Publishing Director, Adrian Clarke, 40 Rue La Boetie, 75008 Paris. Tel. +33 (01) 5376 8250; Fax. +33 (01) 5376 8253; Commission Paritaire N° 0909 C 85347; ISSN 1148-2753; **Germany:** Responsible Editor, Lionel Barber; Responsible for Advertising content, Adrian Clarke; **Italy:** Owner, The Financial Times Limited; Direttore Responsabile: Anthony Barber; ISSN 1126-3466. **Spain:** Legal Deposit Number (Deposito Legal), M-32596-1995; Publishing Director, Lionel Barber; Publishing Company, The Financial Times Limited, registered office as above; Local Representative office, Castellana, 66, 28046, Madrid; ISSN 1135-8262. **Sweden:** Responsible Publisher, David Ibison; Telephone +46 (08) 215160.

The US Air Force will soon create a cyber war-fighting command aimed at improving defensive and offensive capabilities to counter such asymmetric threats. "We want to ensure that we can operate freely in the domain," says Major General Charles Ickes, another senior Air Force official involved with cyberspace issues. "On the other hand . . . it is seen by everybody in the defence department as a war-fighting domain and you must have offensive capability."

The Economist September 8th 2007

The Economist

Foiled, this time

A timely reminder of the risk of terrorism in Europe

THE targets are said to have included Frankfurt airport, Germany's busiest, and an American air base. The collective power of the bombs would have exceeded those used in Madrid and London in 2004 and 2005 respectively. But on September 4th the plot to commit Germany's bloodiest act of terrorism was foiled with the arrest of three men in a village in central Germany. The arrests came a day after Danish police averted another "major act of terrorism" by arresting eight young Muslims in the suburbs of Copenhagen. Six were later released but two were charged.

That terrorist conspiracies could be hatched in Denmark and Germany is not a complete surprise. The Danes have staged three terrorism swoops in three years. Last year two men of Lebanese origin planted suitcase bombs on two trains in Germany; they failed to explode. There have been many reports of young Germans going to Pakistan for training sessions. The interior minister, Wolfgang Schäuble, has given warning of high risks.

Yet most Germans assumed their country was relatively safe, mainly because (unlike Britain, Denmark and Spain) it did not send troops to Iraq. "Germans don't take the threat as seriously as they should," said Guido Steinberg, a former adviser to the chancellery on terrorism, days before the arrests.

That will change now. Two of the arrested men are German converts to Islam. The other is one of Germany's 3m Turks, who have provided few terrorist recruits. Two of the three had trained in Pakistan and all seem to have links with the Islamic Jihad Union, which staged several terrorist attacks in Uzbekistan in 2004. They may have been planning to strike on the anniversary of the September 11th attacks in New York. And they may have hoped to affect the debate on Germany's 3,000 troops in Afghanistan. Germany is to decide shortly whether to renew its commitments there, which are unpopular and opposed by many Social Democrats.

Germany's law-enforcement coup may also boost Mr Schäuble's campaign for a law that would allow the authorities to spy on suspected terrorists by secretly inserting "remote forensic software" into their computers. That proposal has sparked an outcry in a country that is especially sensitive to the possibility of abuse by secret police. Since the law has not yet been passed, the authorities could not use such spyware to catch the would-be bombers, Mr Schäuble said. But he added that, since terrorists use "modern communications", so should the government.

Germany's law-enforcement coup may also boost Mr Schäuble's campaign for a law that would allow the authorities to spy on suspected terrorists by secretly inserting "remote forensic software" into their computers. That proposal has sparked an outcry in a country that is especially sensitive to the possibility of abuse by secret police. Since the law has not yet been passed, the authorities could not use such spyware to catch the would-be bombers, Mr Schäuble said. But he added that, since terrorists use "modern communications", so should the government.

SECURITY

Trojan Horse

German government wants to use software to catch terrorists.

Under the government's plan, so-called FedTrojan software would be installed surreptiously in the computers of terrorist suspects. The software could retrieve information such as keys pressed, web sites visited, emails and instant messages sent and received, the contents of files created on the computers, and programs used.

Introduction

Hacking Team

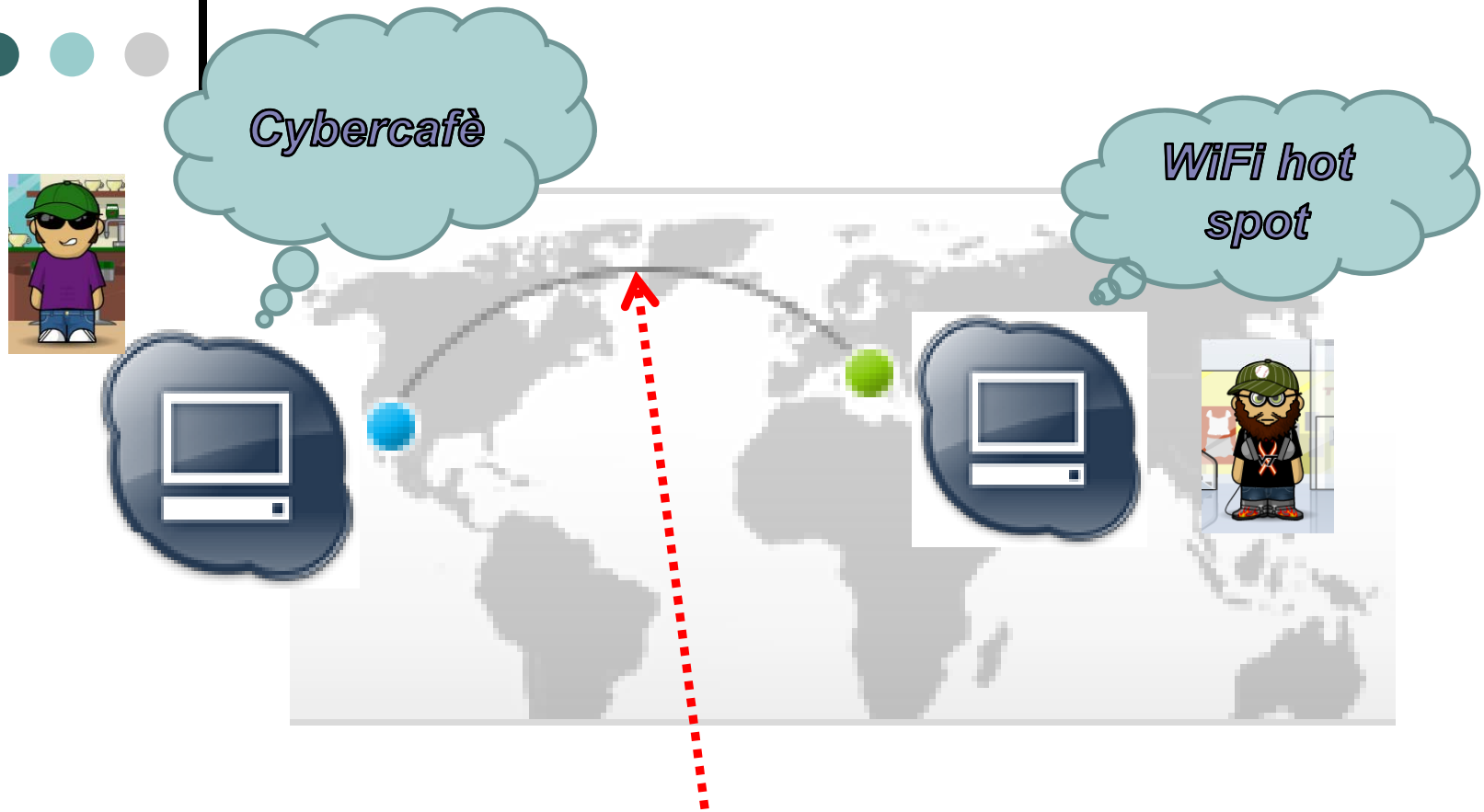
- HT Srl is a 100% Italian company founded in 2003 by Valeriano Bedeschi and David Vincenzetti. Venture-backed in 2007 by two Italian VC funds
- The company is an active player in the IT security market and it offers Ethical Hacking (pentest) services, security tools and intelligence instruments for governmental institutions
- HT has developed a highly innovative offensive IT security system which, in specific circumstances, allows Law Enforcement Agencies to attack and control target PCs **from a remote location**

What actually happens

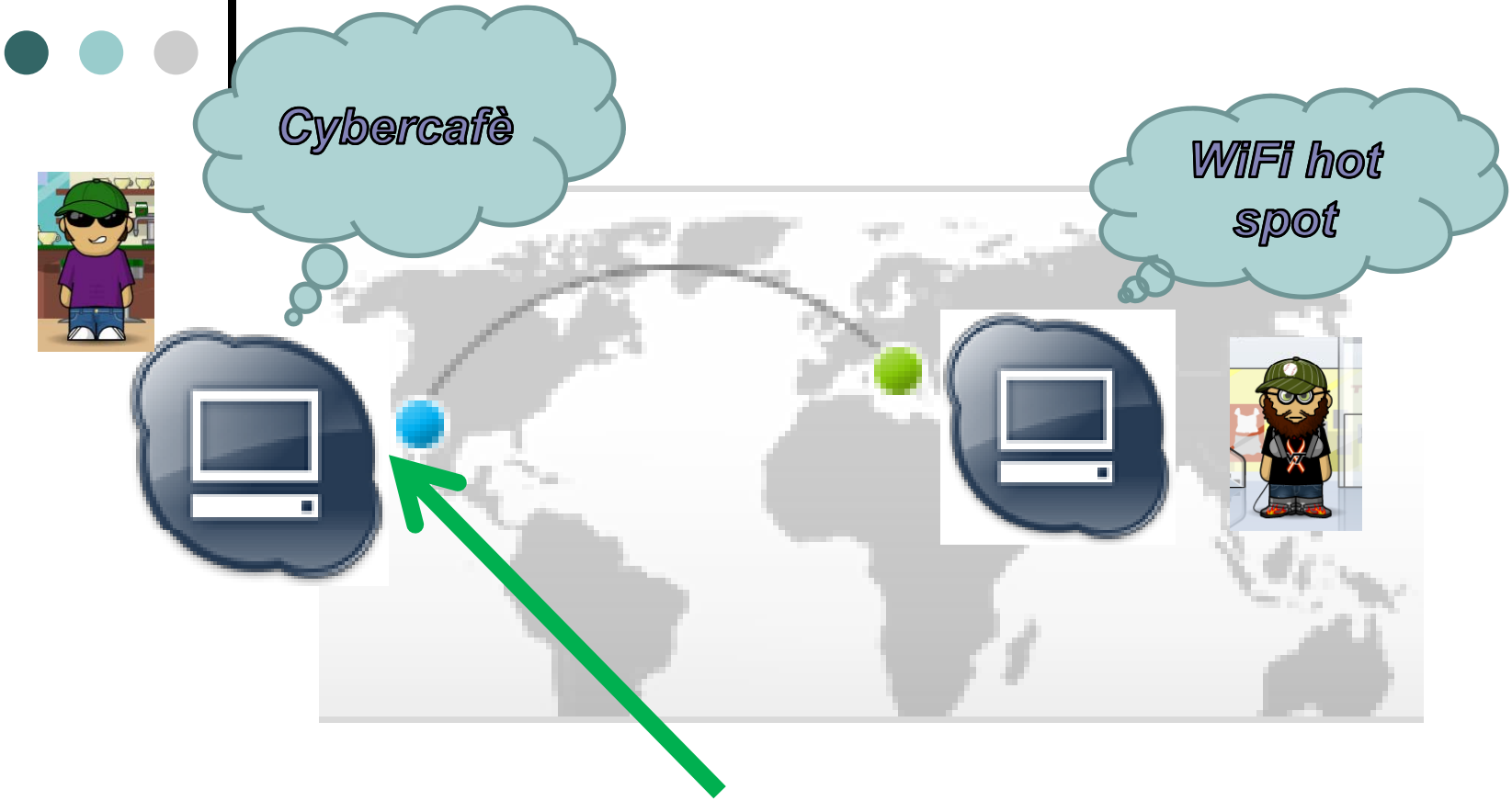
- IT offensive security represents a new and highly innovative technology
- It's growing very fast because of phenomena such as terrorism, industrial espionage and insider trading
- Advanced use of the Internet by terrorists makes LEAs increasingly nervous
- Example: the exponential growth of encrypted VoIP communications (***Skype*** claims 300+ millions of users) by residential and business users, ***is a nightmare for LEAs***

What actually happens

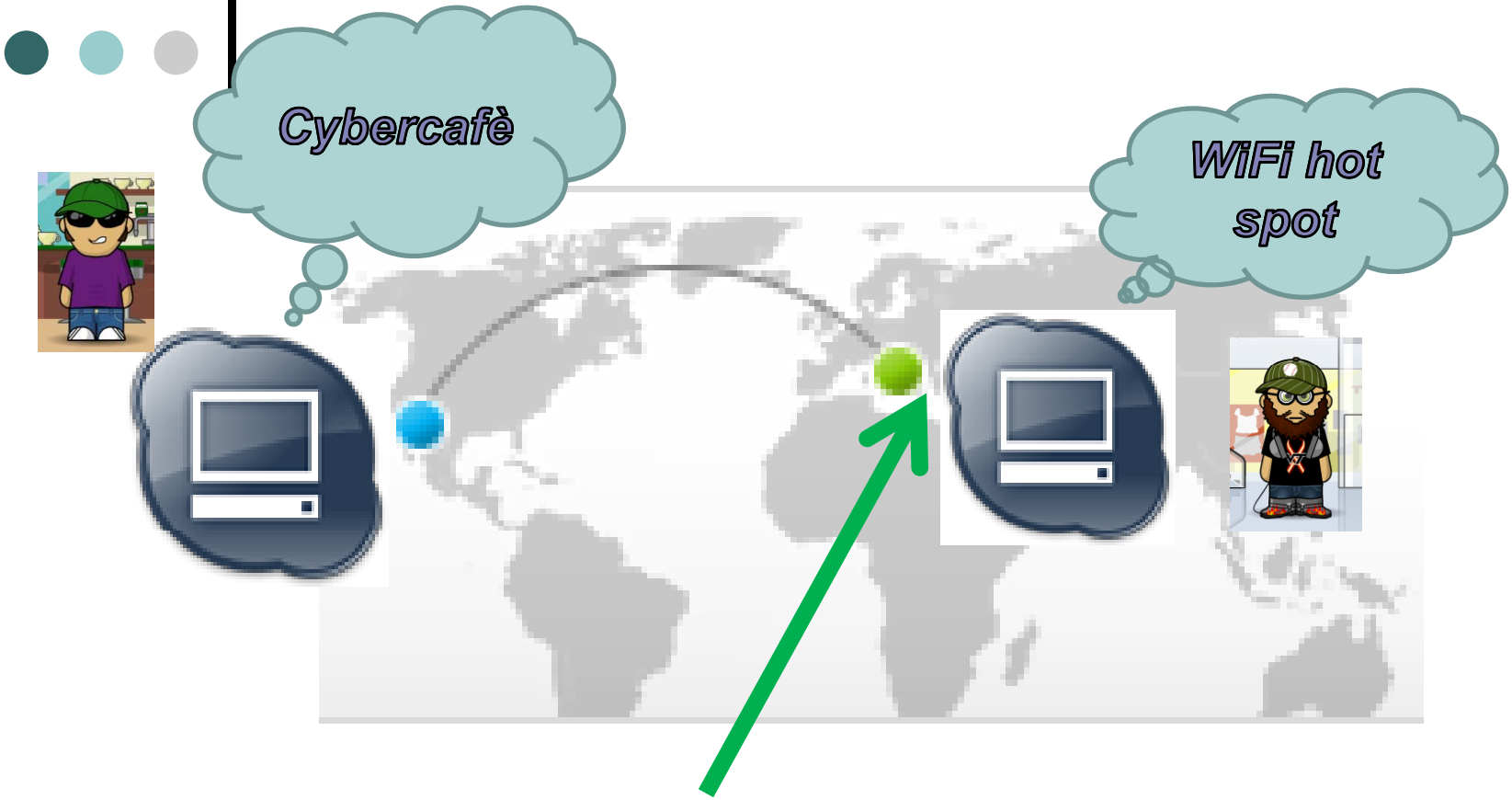
- If…
  - Skype encrypts online conversations by default
  - Skype is *ubiquitous* (same phone number, location independent)
  - Skype is likely to be one of the favourite ways of communication by tech-savvy criminals
- Then...
  - ***Governments should use spyware-based wiretapping technologies (that is, offensive technologies) to foil tech-savvy criminals' communications***
  - (Some countries still lack a law that would allow the authorities to spy on suspected criminals by secretly inserting "***remote forensic software***" into their computers)



Passive monitoring is useless against most encrypted communication systems (such as Skype)



Offensive security monitoring is highly effective on most communication systems



Offensive security monitoring is highly effective on most communication systems

Why IT offensive security

- Cyber space is a very attractive place for criminals: It's cheap, quick and easy to access
- IT offensive security systems can be complementary to more traditional passive IT monitoring solutions
- Governments need to have both ***defensive*** and ***offensive*** *(IT)* ***capabilities***

IT offensive security

- Operational scenarios:
  - “Standard” criminal investigation (evidence gathering) performed by Governmental Organizations such as Police and Tax Police.
  - Intelligence gathering activities performed by Security Agencies when cracking-down terrorism and serious organized crimes.
  - (Corporate scenario: when fighting white collar crimes, I.P. theft, insider trading)

Remote Control System

- ***Remote Control System is an IT stealth investigative tool for LEAs.*** *(It is offensive security technology. It is spyware. It is a trojan horse. It is a bug. It is a monitoring tool. It is an attack tool. It is a tool for taking control of the endpoints, that is, the PCs)*
- It permits passive monitoring and ***active*** control of all data and processes on selected target computers.
- Such computers might or might not be connected to the Internet.

Functionalities

Monitoring and Logging

Remote Control System can monitor and log any action performed by means of a **personal computer**

- Web browsing
- Opened/Closed/Deleted files
- Keystrokes (any UNICODE language)
- Printed documents
- Chat, email, instant messaging
- Remote Audio Spy
- Camera snapshots
- ***Skype*** (VoIP) conversations
- …

PC architectures

- Windows XP
- Windows 2003
- Windows Vista

- Q109: MAC OS
- Q409: Linux

Monitoring and Logging

Remote Control System can monitor and log any action performed by means of a **smartphone**

- Call history
- Address book
- Calendar
- Email messages
- Chat/IM messages
- SMS/MMS interception
- Localization (cell signal info, GPS info)
- Remote Audio Spy
- Camera snapshots
- Voice calls interception
- …

Smartphones architectures

- Windows Mobile 5
- Windows Mobile 6

- Q109: iPhone
- Q409: RIM/BlackBerry
- Q409: Symbian

Invisibility

- Allows monitoring (all) PC user's activities
- After the installation, Remote Control System cannot be detected by any bugged computer user
  - Existing files are not modified
  - No new files appear on the computer's hard disk
  - No new processes are executed
  - No new network connections are established
  - **Antivirus, antispyware, anti-key-loggers cannot detect our bug**
    - **E.g., Gartner Endpoint Security Magic Quadrant**

Flexibility

- Goes beyond logging and monitoring
- Allows performing actions on a bugged computer
  - Search and view data on the hard disk
  - Execute commands remotely
  - Possibly modify hard disk contents
  - ***Trigger actions in response to events***
    - Start sending data only when the screensaver is active, remove itself on a preconfigured date, etc.

Attack/Infection vectors

- Remote Control System is software, not a physical device
  - Which can be installed ***remotely***
    - Computer can be bugged by means of several infection vectors
    - Intelligence information about remote target mandatory
  - … but ***local*** installation remains a option
    - Usually very effective

Remote installation

- Remote infection vectors
  - Executable melting tool
  - HTTP Injection Proxy
  - HT Zero-day Exploits library (library is “indirectly” accessed by customer)
  - HT consultancy: anonymous attack scenario analysis, attack cookbook
    - E.g., Moving target using Skype

Local (physical) installation

- Local infection vectors
  - (Bootable) CD-ROM
  - (Bootable/Autorun) USB pen drive
  - Direct hard disk infection by means of tampering with computer case
  - Fireware Port/PCMCIA attacks
  - HT consultancy: anonymous attack scenario analysis, attack cookbook
    - E.g., Internet Café using DeepFreeze

Critical issues

Remote Control System could not work without the following features

1. **Invisibility**, at system and network level
2. **Flexibility** (**event-based logic**)
3. Infection capabilities (**attack vectors**)
4. Robustness & Scalability (being used by many clients in real security scenarios)
5. ***Centralized management of unlimited HETEROGENEUS targets***

www.hackingteam.it