GOING AROUND WITH BLUETOOTH IN FULL SAFETY

F-Secure, in collaboration with Secure Network,
has created the first *on the road* test conducted in Italy to verify the level of vulnerability of Bluetooth technology now available on numerous devices, including latest generation "smart" phones

May 2006

The Reasons Behind this Experiment

Bluetooth is a word that is now commonly used. The literal meaning supposedly refers to the Viking Emperor Harald (Blåtand in Scandinavian), who lived at the beginning of the 10th century and united the kingdoms of Denmark, Norway and Sweden. **The objective of the Bluetooth protocol is in fact to unify different wireless data transmission technology among mobile and static electronic devices** such as PCs, cellular phones, notebooks, palm pilots, DVDs, MP3 devices, TV, Hi-Fi, cash registers, POS terminals and even household appliances such as refrigerators and washing machines. It is basically the **new alternative to infrareds** and is based on a short-wave radio technology able to transmit data across physical obstacles such as walls or other objects.

Bluetooth will become the prevasive technology to support wireless communication in various contexs of everyday life. At present, the greatest level of diffusion is witnessed in so-called smart phones, the latest generation of cellular phones, devices that, on top of offering all the functions of cutting-edge telephone technology enclose functions and applications typical of palm pilots, managed by an operative system, such as Symbian or Microsoft Windows Mobile. Smart phones allow sending and receiving SMSs, MMSs and e-mail, listening to mp3 files, watching videos, surfing the Internet, playing games, managing an agenda, synchronizing phone data with PC data and much more. In some cases, they can also become GPS navigators through a satellite decoder and specific software.

The smart phone market is still a **niche, which however has had a growth rate of 100% per year for the past 5 years**, limited at the moment by elements such as the high price or in some cases, the size and weight. **But 2006 could just be the year of the turnaround:** according to ABI Research, a market research company, **this year smartphones will reach 15% of the global cellular phone market,** equivalent to 123 million units sold, thanks to the growing request for applications such as mobile e-mail (according to Gartner, in 2006 this application will be used by 20 million people), to decreasing prices (thanks to volume growth), and to the broader choice of models. According to Gartner estimates, in Europe only, the growth rate in sales of intelligent cell phones will be of 49% per year between 2005 and 2009 and **in 5 years, 1 cellular sold on 3 will be "smart".**

This is why **F-Secure** – a Finnish company and the first to offer anti-virus protection technology for cellular phones – has decided to commission the first Italian *on the road* experiment aimed at verifying the potential weaknesses of Bluetooth devices and creating a mini-guide for a better understanding of Bluetooth technology, containing also indications on minimum precautions for safe use. **Knowing the vulnerabilities of Bluetooth enabled devices is just as important as understanding the technology potential**: on our part, with this work, we intend to take the first important step in this direction.

For this first check on the field, it's been decided to focus on Milan and its surroundings. In parallel, a similar experiment has been carried out directly by F-Secure during the last CeBIT, the information technology and telecom fair in Hannover between the past March 9th and 15th. During the course of the event, F-Secure technicians activated in their stand a surveying system similar to that created by Secure Network experts for the surveying carried out in Milan and surroundings, able to identify active Bluetooth devices present in a 100 mt range. The results have been impressive: during the course of the week, 12.500 devices with activated Bluetooth in visible mode have been identified. Find out the results of the test in Milan and surroundings in the next pages!

Miska Repo
F-Secure Italy Country Manager

Introduction

Mobile computing is quickly gaining ground in our daily experience; for this reason it is very important to understand the potential risks linked with all types of wireless devices.

If only three years ago, virology experts shyly started talking about cellular phone viruses, today the vulnerability of Bluetooth technology devices, such as BlueBug, BlueBump, is bringing to light new issues that cannot be undermined.

Smart phones, thanks to the advanced functions that define them, **are now very similar to personal computers: because of this, they are at the same time more vulnerable, more useful and more attractive for a potential attack.** This increased vulnerability is due to the presence of a system of evolved connectivity applications that expose the telephone and the data it contains to a series of risks deriving from activities such as sending e-mail, the transfer of data through the Internet, the exchange of MMS and WAP messages and the use of accessories and tool such as memory cards. Specifically, communications that take place through Bluetooth connections become potential vehicles for viruses and the target of attacks that can extract information from the smart phone.

Cellular phone viruses spread at present have fortunately not caused significant damage to other users, except for the obvious inconveniences due to telephone malfunctioning. Nonetheless, the situation must not be undermined because all the elements are in place for the danger of this threat to increase.

In the future, an increase of attacks aiming to make the mobile device unusable is to be expected, but also connections to payable numbers, able to generate illegal gains for the authors, and SMS and MMS spamming are set to increase as well. The greatest cause for concern however probably remains the user's privacy: the cellular phone represents in fact a precious source of personal data with its phone book, messages agenda and much more. This information can be deleted, modified or stolen also not involving a viral epidemic, using well-known attacks that are constantly evolving.

Few people today are aware of the risks that can be incurred by using apparently innocuous devices: this is shown by the fact that **in just a few hours of "ambushing", we have detected thousands of Bluetooth devices in *visible* mode and that therefore were potential targets for attacks.**

But we did not limit ourselves to detecting potentially vulnerable devices: together with F-Secure, in fact, we have created an updated guide on potential security threats and a series of technical and behavioral tips that users can apply so this widespread technology does not become another cause for stress.

Stefano Zanero,
Secure Network S.r.l., CTO

Luca Carettoni,
Secure Network S.r.l., Senior Consultant

Claudio Merloni,
Secure Network S.r.l., Senior Consultant

How Bluetooth Technology Works

Bluetooth technology allows to make wireless connections among electronic devices (desktop computers and notebooks, cellular phones, palm pilots, camcorders, etc) using radio waves at **2,4 GHz frequency** (the same used by Wi-fi 802.11 technology), letting devices covered by the signal communicate among each other. The frequency used varies from country to country with regards to National regulation.

When an individual connects different Bluetooth devices together, he creates around himself a so-called **PAN** (Personal Area Network), that is a small network with the possibility to exchange data and information as it usually occurs with a regular company LAN (Local Area Network).

Bluetooth technology is characterized by a **low power** (from 1 to 100 mW, a thousand times less than the transfer power of a GSM cellular phone) and a **communication speed** of around **1 Mbps**.

With regards to power, Bluetooth devices can be grouped in grades, each corresponding to a different reach:

- *Grade 1* – able to comunicate with Bluetooth devices in a 100 m range
- *Grade 2* – able to communicate with Bluetooth devices up to a 10 m range
- *Grade 3* – able to communicate with Bluetooth devices within a 10 m range

Currently, most devices used belong to Grades 2 and 3: for instance notebooks and cellular phones normally use Grade 2 Bluetooth communication technology.

Towards the end of 2004 an implementation of Bluetooth technology has been made that in the new versions allows a transfer speed of up to 2 and 3 Mbps and lower energy consumption. The important thing however is that cellular phones can dialogue among each other even if they use different versions of the Bluetooth protocol.

Bluetooth Technology Security: the Risks

The first security cracks with regards to this technology came about in November 2003: some of the Bluetooth protocol implementations seemed to allow access to data and information to unauthorized individuals.

In April 2004, the news of a relative possibility to force some of the Bluetooth implementations in order to access personal data, started to circulate: this was done by analyzing Bluetooth devices and retrieving the code used to encode data transmission.

Few months later, in Summer 2004, the possibility to intercept the Bluetooth signal from the 11th floor of a Las Vegas hotel was demonstrated by capturing 300 phone books from the cellular phones of unaware passerby's with the help of a directional antenna connected to a lap top computer: a discovery that has extended significantly the action range of potential aggressors.

A series of weaknesses, therefore, have brought about the need to reflect on the existence of a problem that, also in consideration of the rapid diffusion of Bluetooth technology, cannot be undermined.

When considering latest generation cellular phones, **4 types of threats can be identified for these types of devices**:

1. Damaging content such as viruses, worms or Trojan horses, which can be transmitted on user terminals through Bluetooth, SMS or MMS or through WAP pages. Taking advantage of their vulnerability (for instance through attacks to the Bluetooth protocol or through specially "deformed" SMS or MMS messages) such applications can also be installed on the device;

2. episodes of *denial of service* or system interruption, caused by the propagation of malware or other types of attacks;

3. unauthorized access to information using Trojan horse, spyware and eavesdropping attacks…

4. deletion, corruption or modification of data kept on the device

This means that, on top of the propagation of malware and viruses, a totally unaware user could be the victim of **phone book and agenda theft** with all the relative contact numbers and appointments. This as long as the thief does not take any further steps such as taking control of the device and making phone calls or sending messages charged to the victim.

Among existing attacks that damage devices using Bluetooth technology - classified by security experts worldwide – some are particularly known and widespread:

- **BlueSnarf** – This type of attack bases itself on the OBEX Push service, which is the type of service that is commonly used to exchange electronic business cards. Easy to set in place when a cellular has Bluetooth set on visible mode, BlueSnarf allows connecting to a cellular phone and accessing the phone book and agenda without authorization.

- **Bluejacking** – Taking advantage of the IDs that devices exchange at the beginning of a connection – just think of when you associate your cell phone to a computer - short deceitful text messages can be transmitted. A user could, for instance, be invited to dial a code to solve network problems and, unconsciously, authorize an aggressor to acquire all the necessary privileges to access a phone book, agenda or file and potentially compromise information and data residing on the device.

- **BlueBug** – This vulnerability allows to access the *AT Commands* of the cellular phone – a set of commands that give instructions to the cellular phone – allowing the aggressor to use the phone services without the user's knowledge: this includes incoming and outgoing phone calls, sent, received or deleted SMS messages and many more intrusive operations as well as the possibility to modify the device's configuration parameters.

- **BlueBump** – A type of attack that takes advantage of the vulnerability linked with the Bluetooth connection type that is always active giving the possibility to unauthorized cellular phones to continue accessing as if they were still part of the list of authorized cell phones. This type of attack, on top of leading to the theft of data present on the cellular phone, can bring aggressors to use WAP and Gprs services without the owner's knowledge.

Bluetooth and Worm: How Do Viruses Spread Concretely Among Cellular Phones?

The propagation of viruses can take multiple forms that are destined to change and become constantly more automatic **often taking advantage of *social engineering* techniques**: the unfortunate individual, finding an “attractive” message on the cellular phone with the invitation to download and attachment or install a program, does not hesitate to proceed with the operation, infecting his or her device and giving way to the propagation of the worm.

Striking examples of this technique were witnessed with **Cabir**, one of the first cellular phone viruses to have ended up on the pages of newspapers in Summer 2004 and the first case of virus able to replicate itself only through the presence of nearby active Bluetooth phones.

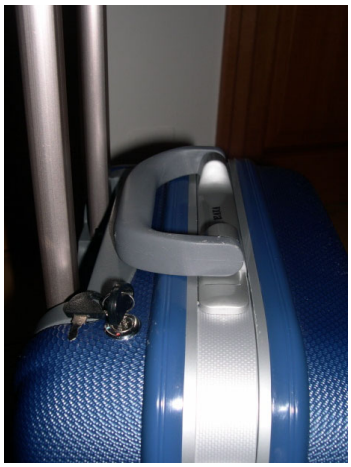
Another clamorous case was the identification or **Commwarrior**, a virus with a strange behavioral scheme that would spread from 8 A.M. to midnight using Bluetooth connections and from midnight to 7 A.M. would focus on MMS messages. If MMS messages have a certain cost, it is easy to understand the financial impact of this type of virus for its victim!!

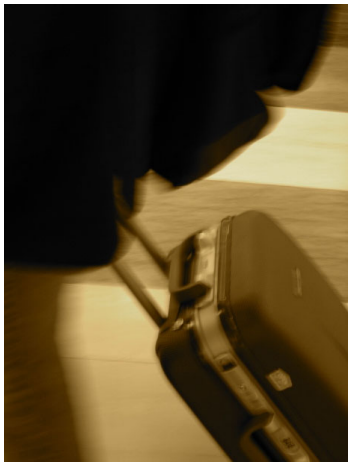
Another method of propagation can take place through the sending of infected messages, opening TCP/IP connections directly from the applications and offering thus malware a further chance to spread.

From Summer 2004 to today, identified cases of virus epidemics affecting mobile devices have increased worldwide, using different techniques: **just think that by the end of May 2006, F-Secure research laboratories have classified over 200 existing viruses!!** An updated list, that gets longer by the day, can be seen at *http://www.f-secure.com/wireless/threats/*

Walking Around Milan and Surroundings with *Blue*Bag

During the course of our experiment, we focused on the identification of the number of **active Bluetooth devices in visible mode**. This is in fact the condition of greatest potential risk for users. Theoretically attacks are possible also to Bluetooth devices in hidden mode, but they are much more complicated to set up[1] For this reason, our test was focused exclusively on the detection of devices in visible mode, that is those that are easier to attack. Our intent was not to establish a percentage of "distracted" users with regards to the total number of cellular phone owners, but rather to simply evacuate the potential damage a potential aggressor – or an unaware infected user - could perpetrate.
To carry out our surveying process without being noticeable, the Secure Network team of researchers has developed what they came to call "***Blue*Bag"**, that is a real **traveling research laboratory *disguised* as a trolley!**





Apparently a simple trolley, the BlueBag contained a surveying system able to identify Bluetooth devices present in a 150 mt range.

[1] *A brute-force attack to find potential cellular phones with active Bluetooth technology in "hidden" mode is NOT feasible in generic context given the enormous expenditure in terms of time that it would entail. An attack with this method is possible only if a specific device is to be targeted and also in this case it is first necessary to identify the brand and model of the device to be able to carry out the attack for a rather long period of time (ex. The model and brand can be identified through visual contact and during office hours, when the subject leaves the device on his or her desk, the attack is carried out). Considering what's been said, it is apparent therefore how the "hidden" mode is a preventive solution that ensures a certain degree of security since it extends considerably the time necessary for an aggression. This mode keeps the phone safe also from worm infections that use Bluetooth technology to replicate since the research of victim devices occurs through a simple scanning of devices in the area.*

The Places Where Surveying Was Made

It was decided to conduct surveying in different moments and place – all high-transit – in several areas of Milan and surroundings:

- ***Fiera MilanoCity*** during ***Infosecurity 2006***
- ***Orio Center*** Shopping Mall
- ***MM2 Cadorna*** Metro Station
- ***Assago MilanoFiori*** Office District
- Milan ***Central Station***
- ***Milano Malpensa*** Airport
- ***Politecnico di Milano***, Leonardo Branch

The choice was made with the objective to verify if and how the presence of potentially vulnerable devices varied in different contexts populated by different people: at the *Central Station,* for instance, the presence of a heterogeneous user base is highest; at the *Orio Center* on a Saturday there are many young people and families, subjects that could potentially be the easiest prey for cyber criminals because of their unawareness of dangers linked with new technologies, as opposed to visitors and exhibitors at *Infosecurity* the IT security fair.

In further detail. At the Orio Center Shopping Mall, it was decided to hold a first session on a weekday and then hold two more session during Saturday afternoons. Also for Infosecurity 2006, held in Milan from February 8th to the 10th, it was decided to have two sessions on two separate days: on the opening and closing days.

It must further by underlined that, in cases where surveying was carried out over several days, "stable" Bluetooth devices (such as PCs or printers) were included in the final count only once, so the **final test data refers to unique devices.**

On the road surveying results

Unique devices with active Bluetooth in visible mode detected in the 7 days of the experiment amounted to a total of 1405 including cellular and smart phones (1312), PCs / notebooks (39), palm pilots (21), GPS navigators (15), printers (5) and other various devices (13).

Type	*Quantity*
Cellular phones/Smartphones	***1312***
PCs/Notebooks	***39***
Palm pilots *(w/o phone functions)*	***21***
GPS Navigators	***15***
Printers	***5***
Other	***13***

This data not only **underlines the capillary diffusion of Bluetooth technology in everyday life** – from offices to stores to our bags where we hold latest generation cellular phones – but it also highlights the fact that, if we were cyber criminals, even with these brief ambushes carried out with "home made" equipment, we would've had access to **over 1300 Bluetooth cellular and smart**

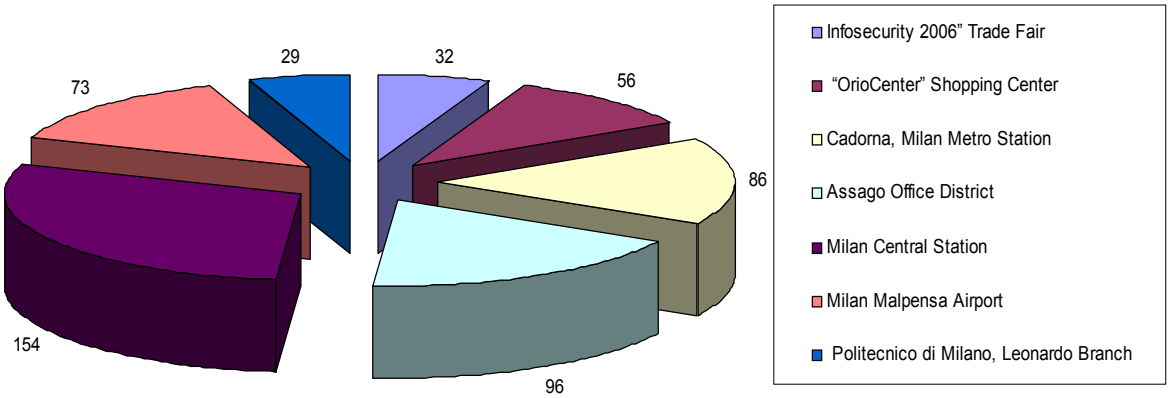
phones that could be attacked in less than 24 hours[2]; some of these could be also infected and afterwards spread the infection to other unprotected cellular phones …

The chart below lists the **scanning sessions** made, indicating the date and time interval during which the surveying was made.

Place	*Surveying Sessions*	*Scanning Times*	*Scanning Duration*	*Number of devices detected*	*Average unique devices detected per hour*	*Number of devices detected **
"Infosecurity 2006" Trade Fair	08/02	15:07-18:04	2:57	***94***	***32***	***94***
	10/02	15:01-16:46	1:45	***55***	***31***	***55***
"OrioCenter" Shopping Center	01/03	15:49-18:50	3:01	***23***	***8***	***23***
Cadorna, Milan Metro Station	09/03	08:43-09:22	0:39	***56***	***86***	***56***
Assago Office District	09/03	12:53-15:20	2:27	***236***	***96***	***236***
Milan Central Station	09/03	15:40-16:52	1:12	***185***	***154***	***185***
"OrioCenter" Shopping Mall, Saturday afternoon	11/03	16:00-17:56	1:56	***212***	***110***	***216***
	11/03	18:20-20:08	1:48	***142***	***79***	***166***
Milan Malpensa Airport	13/03	09:15-10:41	1:26	***123***	***86***	***123***
	13/03	11:01-14:00	2:59	***198***	***66***	***219***
Politecnico di Milano, Leonardo Branch	14/03	10:56-13:44	2:48	***81***	***29***	***82***
TOTAL	**11**		**22:58**	***1405***		***1455***

** This number does NOT refer to unique devices but to the total number of devices detected at the end of each session.*

On the basis of data collected, it was possible to calculate **the average number of unique devices detected per hour in each examined place:**



It can immediately be noted that there are no significant differences in terms of risk awareness with respect to the different environments tested: so much at the Central Station

[2] *Surveying, lasted overall 22 hours and 58 minutes, as can be seen in the chart on the following page*

as at the Malpensa Milan Airport – mostly populated by a heterogeneous public – as at the Assago Office District, where most users are believed to use these devices for work purposes, the average detected number of potentially vulnerable Bluetooth devices per hour was high. The situation was significantly better – indicating a greater awareness of users with regards to security risks – at Infosecurity and the University.

On 1405 unique devices detected, a **further analysis was made to determine the number of devices that had activated some of the most broadly diffused services,** which are those especially targeted as transmission vehicles for worms (refer to chart below)

Type	***Number***
OBEX Object Push / OBEX File Transfer *Service enabling file transfer*	***313***
Headset/Handfree Audio Gateway *Service enabling the connection to Bluetooth headsets*	***303***
Dial-up Networking *Service enabling Internet connection and surfing through cell phone*	***292***

As shown in the chart, on **313 devices the OBEX Push service is active;** the latter is normally used for the transfer of information (business cards for instance) or files and application. Actually, **all** cellular / smart phones (that is **1312 devices**) have the OBEX Push service; **313** are those found in the BlueBag's "range of action" for a period of time long enough to allow their recognition. This data is worrisome nonetheless considering that this very service, because of its features, **can become a dangerous propagation channel for virus attacks.**

This obviously doesn't mean that the service must not be activated: the goal of our experiment, in fact, was rather to raise awareness of the risks tied to sometime superficial behavior. **It would in fact be enough to set the phone's Bluetooth connection mode to not visible to make the life of potential aggressors much more complicated!** This minimal precaution, while not being enough to fully eliminate risks, allows to reduce attacks or at least to make them more difficult.

Final Remarks

From an initial analysis of the results brought out during the course of the experiments, a broad diffusion of devices based on Bluetooth technology can be noted: this technology, at first sight, seems to be constantly more within everyone's reach and an integrating part of everyone's life, not only for professional activities but also for personal use. This makes user awareness of both the advantages and the risks of this technology of the future all that more important.

Moreover, it must not be forgotten that latest generation devices often represent a daily work tool that many people with a medium/high level of responsibility use within their companies. This implies that often trendy or innovative cellular phones or palm pilots hold particularly tempting information for potential aggressors interested in industrial espionage or looking for sensitive data.

Without creating useless alarmism, it is important to understand how some simple tricks – such as keeping the Bluetooth connection on hidden mode as opposed to visible – can contribute in increasing the security level of the device, discouraging possible attacks on part of potential aggressors.

It is important to point out that come cellular phone are launched on the market with a configuration that entails that, it the Bluetooth connection is activated, the visible mode is set as default: the user must the manually modify the setting, enabling the "hidden" mode. In other cases, the visible mode must be requested explicitly by the user and is each time re-set automatically as invisible after a short period of time. This was shown to be effective: many users wouldn't otherwise perform this short and easy operation, leaving their device visible to everyone.

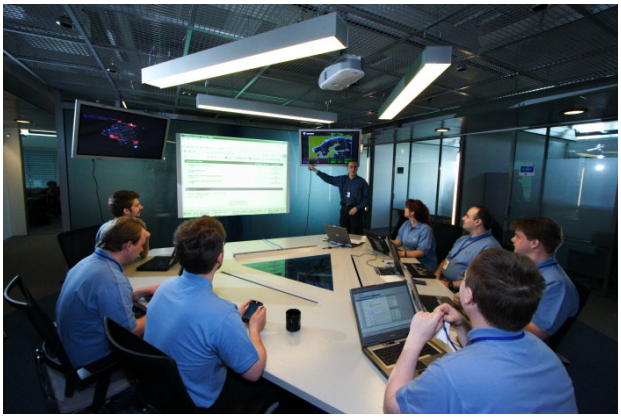
Another important thing to know with regards to default settings on cellular phones, deals with the ID name of the device: our survey has shown that, in most cases, the users does not bother to change the configuration parameters set by the producer, allowing therefore immediate identification of the telephone model. This apparently trivial information allows to associate potential weaknesses known to the different device models giving potential aggressors the chance to make a targeted attack with high success probabilities.

To conclude, an interesting fact: on top of the data collected, the system set up for this research could be successfully used also to "capture" potential Bluetooth worms present in the environment. The *BlueBag,* used in *honeypot* mode, remains invisible in the environment listening and ready to receive all types of connection requests from infected devices. In some moments of the research, tests of this type have been made but have not registered worms. Future research could further analyze the real threat of this type of attack through sessions specially-planned for this purpose.

F-Secure's commitment

Although databases listing weaknesses for each device model do not yet exist, security experts and enthusiasts of the field are uniting to make available – through a forum and specially-developed websites – a list of weaknesses noted and the possible solutions to face deriving problems. This attitude contributes to creating awareness with regards to an issue that is becoming increasingly serious each day.

Research in the field of cellular phone security requires specific resources and tools.



This is a field that F-Secure has been committed to and that has further been confirmed with the renewal of the research laboratories at the Head offices in Helsinki. A flagship of the Finnish company, the new research center is at the cutting-edge of technology in terms of modern infrastructure to allow the *task force* of researchers to face new emergencies 24 hours a day.

As of June 2005, F-Secure has chosen to implement in the new laboratories a new area specifically-designed for the study and analysis not only of traditional viruses but also of new threats to security such as cellular phone viruses. This type of analysis, in fact, requires first of all wide spaces that allow the accurate study of Bluetooth virus diffusion methods in total isolation from radio frequencies. For this purpose, F-Secure has set-up a room, inside its new laboratory, which allows to block out all types of radio signals, facilitating this way the analysis of all possible threats to the *mobile* environment.

What worries security experts is not so much the sporadic attack though out by teenagers, the most common virus creators, as the rather continuous surfacing of actual criminal organizations that are becoming increasingly widespread and incontrollable. The phenomenon, that for the moment has targeted mainly the realm of PCs, could also repeat itself in the mobile world.

There's no need for panic, but rather for greater attention and awareness: the birth of new technologies must not endanger our privacy. In order to protect oneself, it is essential to be familiar with the risks and, most importantly, the possible solutions in order not to fall into the trap of mobile aggressors! **The experiment F-Secure promoted in Italy with the support of Secure Network has this very objective.**

Some Tips In Order Not to Fall into a Trap

F-Secure and Secure Network, thanks to their broad experiment with computer security, have drafted a short list of tips in order not to end up being victims of potential attacks on part of mobile aggressors. Here it is below:

1. **Be careful when downloading new software or applications from the Internet:** before proceeding with the installation of new software or downloading new applications from the Internet, always verify the reliability of the source.

2. **Pay attention to possible anomalies in the functioning of the device:** considering that without an installed security application it is rather difficult to identify a virus, there are nonetheless situations that can alarm the user. Generally, in fact, viruses cause anomalies on the telephone like for instance a sudden increase in communication activity, an unusual consumption of the battery, the reception of undesired messages, the deletion of icons or the modification of the latter.

3. **Remember to deactivate Bluetooth after use and if this is not possible, at least set the device on "hidden" mode.** This precaution ensures at leas a minimal level of security since it elongates the time necessary for a potential aggression.

4. **Modify the cellular phone's ID name**: Many users tend to maintain the default ID name of their cell phones set by the producer which is usually associated with the specific model of the device. This simple information can allow and aggressor to associate to the device well-know weaknesses that can therefore be taken advantage of.

5. **Always update security and antivirus software:** to successfully contrast attacks, all security software must be updated. Software that is not updated is not useful since *computer insecurity* is in constant evolution and *old* software is not designed to face new issues. It is important to underline that "old" refers to software that can be only one month old since software updated are made weekly.

6. **Be careful when choosing PIN numbers to associate devices:** too often the codes given by the manufacturer are maintained or, even worse, easily traceable information is used (birthdates for instance).

How the F-Secure Cellular Phone Antivirus Works

After the software has been installed and the update service has been activated, the scanning and updating functions of the database become automatic and the user doesn't need to worry about a thing.

As a matter of fact, a good antivirus automatically analyses all the telephone's files each times they are used and – in order to prevent infections – thanks to *real time scanning* functions, intercepts and analyses all the files automatically as soon as they are saved, copied, downloaded or otherwise modified without requiring action on the user's part. All identified viruses are automatically quarantined.

Site opened by Commwarrior.C

mobile.f-secure.com

In critical cases, the antivirus update can be sent to users by SMS (F-Secure Mobile AntiVirus is the only solution available on the market that allows business users to obtain additional updates via SMS). In most cases however, protection is active long before the device could be infected.

The Authors of the Experiment

F-Secure (www.fsecure.com) is a world leader in the field of antivirus and intrusion prevention: according to independent research, in 2004 and 2005, F-Secure's response time to new threats was significantly faster than that of all of its competitors. F-Secure protects household PCs and company networks from computer viruses and other threats to security transiting through the internet and mobile networks. F-Secure solutions offered are available for workstations, gateways, servers and cellular phones and include antivirus and desktop firewalls with intrusion prevention, anti-spam and anti-spyware functions as well as solutions for IPS network control. Created in 1988, F-Secure is listed on the Helsinki Stock Market since 1999 and is one of the companies that have registered the most sustained growth in the field. The company is headquartered in Helsinki, in Finland, and has offices all over the world. The protection of F-Secure technology is available also through ISPs such as France Telecom, TeliaSonera, PCCW and Charter Communications. F-Secure is a world leader in the protection of cellular phones and has partnerships with entities such as T-Mobile, Swisscom and Nokia. The team of F-Secure researchers makes available a constantly updated outlook on the virus situation on a global level through the weblog http://www.f-secure.com/weblog/

Secure Network (www.securenetwork.it) is specialised in consulting, training and computer security services. The Secure Network research team is at the cutting-edge of innovation in Ethical Hacking techniques and Intrusion Surveying technology. Secure Network Penetration Tests combine our analysts' fine-tuned skills with the most cutting-edge analysis techniques, ensuring a service that is not only updated but also ahead of the market. In 2005, Secure Network has launched SecureGuard, the only IDS as at today with unsupervised learning tools. In 2006, Secure Network has introduced the first transparent coding tool to safeguard the security of CAD designs. CryptoCAD is the much-needed answer to the world of design, which for long has been in need of help to defend itself from industrial espionage. Secure Network offers complete services able to respond to the problems of the small business as well as big companies at all levels: strategic, tactical and operative.

Glossary

Antivirus – Program which, by scanning the memory and the mass memory of a computer, identifies, isolates and eliminates viruses possibly present.

Backdoor – Mechanism allowing access to a program using privileges usually known only to the system administrator.

Denial of Service – Attack aimed at blocking the use of a resource or taking possession of it.

Dropper – Program which installs a virus or a Trojan horse without the user's knowledge.

Eavesdropping – Attempt to intercept a message before it reaches the receiver (attack of the "*man-in-the-middle*" type)

Virus Signature – Contains information on known viruses in order to identify them on a computer during scanning. Constant updating of signatures is essential to recognizing also the newest viruses that are added on to the listing of signatures.

IMEI (International Mobile Equipment Identity) – Cellular phone series number that universally identifies the device, model and manufacturer.

Malware – Term indicating any type of software believed to be dangerous to a system (viruses, Trojan horses, etc). The name derives from *Malicious Software*.

Pairing – association of cellular phone devices

Patch antivirus – Programs able to identify and remove from the system a single and specific virus, usually made available for free by antivirus software manufacturers to face emergency situations while waiting fro an update of their products.

Piconet: small wireless networks made up of two or more peripherals that share a communication channel using Bluetooth, up to a maximum of 8 devices.

Quarantine – Security measure used by the antivirus when an infected or suspect file is identified. The file is isolated in a way to make in innocuous to the system. The isolation can come about for several reasons: the antivirus is not able to remove the virus from the file, the virus is unknown, the file is believed to contain a virus, etc. Generally, the user can see the quarantined file in order to decide whether or not to eliminate it permanently.

Shareware – Type of software distribution which allows the copying of a program or a limited version of the latter for a trial period.

Smart phone – Generic term used to indicate the union of cellular phone and palm pilot. It is in fact a cellular phone with the functions of a palm pilot using a complete operating system such as Symbian OS, Smart phone 2002, Palm OS, Crossfire or Linux.

Spamming – Massive indiscriminate mailing of large quantities of undesired advertising e-mails without the receiver's request.

Spyware – Software (generally a worm or a Trojan horse) able to detect and capture, without the user's knowledge, surfing habits, sequences of keys pressed on a keyboard and even passwords to access restricted company information.

Trojan Horse – Program containing codes used to perform functions without the user's knowledge. Generally, the goal of a *Trojan Horse* is to allow unauthorized access to the system on which it is run (a *backdoor*) to then perform specific functions. As opposed to viruses, Trojan Horses do not self-replicate, but are installed by users unaware of the true purpose of the program.

Virus – Software able to self-replicate and spread through computer systems in several ways (usually through the exchange of infected software), infecting other programs. Some viruses can cause serious damage to systems.

Vulnerability - A crack of the system that can allow other applications to connect with the system without prior authorization or without the user's knowledge.

WAP (Wireless Application Protocol) – Standard global communication protocol among cellular telephones and the Internet that allows GSM or GPRS cellular phone users to access Internet content specifically laid out in order to be viewed on small telephone screens.

Worm – Program able to self-replicate and transmit itself among systems, often through e-mail or, (in the case of cellular phones) using interconnection technology such as Bluetooth. As opposed to viruses, worms do not infect other programs and are autonomous. Some worms are able to seriously damage computer systems.