

# THE MOBILE VIRUSES – AN INCOMING THREAT

Eugene NICKOLOV

BULGARIAN ACADEMY OF SCIENCES  
National Laboratory of Computer Virology  
1113 Sofia, acad. G. Bonchev Str., Building 8  
[eugene@nlcv.bas.bg](mailto:eugene@nlcv.bas.bg), +359-2-97-333-98

## ABSTRACT

*The qualitative changes in the mobile phones operation systems used in the last years, as well as their negative effects on mobile security are discussed. The conditions determinant of the large-scale creation and spread of mobile malware are examined. Special attention is paid to the existing lapses in the Wireless Application Protocol (WAP) technology with respect to the relationship between the Wireless Transport Layer Security (WTLS) and Secure Sockets Layer (SSL) protocols. The protection possibilities are also discussed. Some recommendations are made which could be useful for the owners of mobile phones and personal digital assistants (PDA) in corporate and non-corporate environment.*

The possibility to infect the software of pocket PCs and PDAs with harmful programs has been known for a few years. Until recently mobile phones were too basic to spread even the simplest virus. The advent of smartphones functioning under a real, constantly evolving and improving operating system and the development of communication technology gave virus-writers a new niche for the creation of harmful software with destructive capabilities similar to those of computer viruses: theft, data destruction and modification, espionage, financial abuse. The closer mobile phones and PDAs get to the “real” computer, the greater the possibility of unauthorized access to confidential information and the danger of WAP-hackers.

What are the conditions that nurture the mass creation and distribution of mobile malicious software?

First of all, this is the increasing use of mobile devices. According to a recent survey done by the British Canalys today there are about 18 million devices in the world that use the operating system Windows Pocket PC. Cell phone sales for the last quarter of 2004 have increased more than twice compared to the same period in 2003. Only Nokia sold 5 million smartphones with more and more functional capabilities, and currently the ideas of functionality and safety do not go together. Even some types of text messages can turn any mobile phone “non-functional”.

The WAP-technology is getting more and more use in mobile communications: new WAP-sites appear, there is a quick increase in the number of subscribers that own WAP-supporting phones which on their own decrease in price and become fit for the mass consumer. The service providers constantly decrease prices for data transmissions and start new info-financial WAP-services including systems for mobile trade (m-commerce). Recently some financial institutions in the US and Japan started 24/7 banking through a mobile phone.

On the other hand, the technology and the protocols used by mobile devices have security breaches that benefit the creation and distribution of malicious software.

The mobile Internet access system has two components for information transmission – radio frequency and the infrastructure of the Internet itself. In GSM networks there are ways to protect the WAP protocol and on-line there are ways to protect the TCP/IP. The Wireless Transport Layer Security (WTLS), protocol which is part of the WAP specification, ensures safe data transmission from the subscriber's WAP-terminal to the WAP-gateway. During the online data transmission they are secured by the Secure Sockets Layer (SSL) protocol with a special 128-bit encoding key. Unfortunately in this well secured at first glance system, there is a weak link – the point where the mobile infrastructure connects to the Internet. During the recoding, the data remain completely unprotected for a certain period of time. The switch WTLS - SSL – WTLS, which takes place in the WAP-gateway, creates the opportunity for outside intervention in the incoming and outgoing information (e-mail, passwords or regular wml-sites).

WAP's security is supposed to significantly increase after the introduction of the so-called WIMs (Wireless Identity Module) that protect Internet-transactions through special encoding and a system of “digital signatures” for authorization of online operations from a given mobile user, but that security has yet to turn into reality.

Another innate weakness of a large number of mobile devices is the creation of the wireless connection (Bluetooth, Wi-Fi Internet access, etc.), which makes it impossible to scan traffic before it reaches its final destination.

Furthermore security with Bluetooth and Wi-Fi wireless connections is lower since they transmit signals on radio frequencies which are often not encrypted and can be intercepted by all users within a certain distance from the emitting mobile device. Wi-Fi security can be increased to a certain extent by using Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA), which encrypt the radio frequency between the access point and the mobile device, but WEP is not enabled by default and its use requires user intervention. Bluetooth has even lower security than Wi-Fi, since most software packages do not include encoding. Infrared ports have the highest security since they require physical proximity between the devices (distance under 1.20 m), and the incoming side needs to explicitly agree to the connection.

One of the most dangerous mobile device operations from a security standpoint is the synchronization with a personal computer. Usually the inbox, contacts list, calendar, notes and agenda are synchronized. This allows the entry of worms, viruses and Trojans from the mobile device to the computer or vice versa, since in order to synchronize, some TCP and UDP ports are open. A firewall limits the systems and the applications that have access to these ports.

Another mobile device weakness is that the creators of operating systems do not offer an easy way to update their products. There is no appropriate infrastructure and if there are bugs in the platform, it is not possible to download patches of the Internet. Indeed, none of the mobile viruses known today use a weakness of the operating system but these systems have not undergone thorough tests and may have security defects.

It is interesting that the massive creation of mobile viruses in 2004 came at the same time with the new security measures taken by Microsoft in order to protect MS Windows XP. It is possible that some of the virus writers switched their efforts to mobile devices. This is one of the reasons why the history of mobile viruses will probably repeat that of computer ones.

Here is a short chronology of events:

The first virus striking mobile phones, TIMOFONICA, appeared in Spain in 2000. Actually this is a regular computer worm written in VB SCRIPT, which sends online through an SMS-gateway unwanted text messages to generated numbers of the subscribers of the cell phone service provider MOVISTAR. TIMOFONICA did not do any other harm and was not widely spread. However, only 4 years later the first malicious mobile phone viruses appeared.

The first one, Cabir, was discovered on June 15<sup>th</sup> 2004. It spreads through mobile networks and infects phones working under Symbian OS. (i.e. all of Nokia's phones that use Series 60). The worm is created by an anonymous author, probably Philipino, nicknamed "Vallez", who belongs to an international virus-writing group "29A", that specializes in the creation of conceptually malicious software. This group includes the authors of viruses like Cap (the first macrovirus that caused global epidemics), Stream (the first virus for additional streams in NTFS), Donut (the first virus for .NET platforms), Rugrat (the first virus for Win64 platforms). Cabir is also a conceptual virus which spreads through a file with the extension SIS (distributive of OS Symbian), masked as a security program called Caribe Security Manager. It does not have destructive functions but empties fully charged batteries for 5-6 hours.

Taking over the infected phone, the virus scans the access devices using Bluetooth, picks the first one and sends it a copy of itself. It is important to note that the mobile phone can not be infected unless the user explicitly agrees to install the malicious program. Today there are 15 known versions of Cabir.

On July 17<sup>th</sup>, 2004 Duts came into the world – the first virus for PocketPCs, operating under MS Windows Pocket PC. It is interesting that it has been created by the same people as Cabir, probably as the realization of a new virus conception. Two weeks later came Backdoor.WinCE.Brador.a – the first backdoor for PocketPCs under MS Windows CE (only 5632 bites in size). It determines the IP-address of the infected system and emails it to its author (probably a Russian), to inform him that the infected computer is connected to the Internet, then it opens a certain port to accept a variety of commands – save, copy/paste, delete files.

On August 11<sup>th</sup> in the hacked illegal version of the game "Mosquitos 2.0" was found another virus - QDial26, which also infects smart phones with operating system Symbian Series 6.0 (Nokia 3650, 7650, 6630, Motorola A925, Siemens SX1, SonyEricsson P900 and Samsung D710). It sends a high-priced text message to a certain phone number registered in the UK, but did not get widespread either. Later it turned out that the virus was incorporated in the game by its creators as a safeguard against software pirates and gets activated only when the hacked version is installed.

On the same date the users of the Japanese service provider NTT DoCoMo, whose phones support i-mode, were asked to fill out an online survey with a hidden trojan. The answer "yes" on some of the questions was followed by a phone call to the police without any user participation.

A month later a hacker sent a malicious link to all smart phone users in Japan. Every time the link gets activated, there is an automated dial to a certain phone number. The increased traffic caused a temporary paralysis of the mobile service provider in question.

In November 2004 a new virus appeared – the trojan Skulls, infecting smart phones and mobile phones under OS Symbian Series 60, Nokia 7610 in particular. It is spread together with the user interface managing program Extended Theme Manager, offered by a few free software Internet sites. Starting the program changes the icons and blocks all applications (email, calendar, Web-browser, SMS and MMS sending, camera, etc.), except the voice interface. However the first version of Skulls cannot be considered as dangerous, since it does not have a self-disseminating function and the infection occurs only after the virus file has been consciously installed. Soon thereafter though, a second improved version Skulls.B came out which infects Nokia, Siemens, Panasonic and Sendo smartphones. It can be referred to as a hybrid because it installs also the worm Cabir.B, which can spread to other Bluetooth-devices. The next few versions Skulls.C, Skulls.D, Skulls.E, Skulls.F, Skulls.G, Skulls.H block not only the basic software but also the applications necessary to remove the virus from the infected phone and include some versions of the worms Cabir and Locknut.B.

In 2004 CE Europe conducted an advertising campaign for its computer game Resident Evil: Outbreak, that used a mechanism similar to the spread of mobile phone viruses: mass

sending of text messages warning about the infection with a "T-virus" and sending the user for more information to a certain website. In fact this is a virus hoax – it warns about a non-existent virus and does not cause any harm other than changing the ring tone but the epidemics it caused was out of the control of the company creator and caused panic among users in all of Western Europe.

Actually the idea to use virus mechanisms for advertising is not a new one. As long ago as September 1996 Penguin Books used the computer virus Irina to advertise its new interactive book Irina.

In December 2004 r. SEXXXY (Cabir.U) came out – it is the first Trojan for Symbian, especially aimed at deactivating antivirus software. It is masked as an installation file for the popular game Metal Gear Solid and has been noticed on a few websites that distribute communicator software. After its start the Trojan turns off the antivirus programs, blocks the file managers and all programs that can be used to disinfect the communicator. After that it installs the virus Cabir.C, which searches for Bluetooth access devices and loads SEXXXY.sis on them. Starting that file blocks the application access key.

In the end of 2004 Russia saw the trojan Troj/Delf-HA which makes infected computers send text messages to random numbers.

January 2005 marked the appearance of Gavno.a – the smallest (only 2KB) and most destructive Trojan for Series 60 mobile phones, operating under Symbian OS v7 (namely Nokia 6600 and 7610). The virus file masked as a patch for the operating system leads to constant random rebooting of the phone and blocks all applications, including the capability to make phone calls and disturbs Symbian's internal processes. The same approach is used by SEXXXY, but it blocks only one key. Gavno.b's improved version includes the trojans Cabir and Camtimer, with Cabir disseminating copies of Gavno.b and Camtimer through Bluetooth to other closely located Symbian phones.

Lasco.A also appeared in January 2005 and is the first virus specifically aiming to spread through Bluetooth. It infects smart phones and PocketPCs and for the first time unites both mechanisms for self propagation of mobile phone malicious software: on its own through Bluetooth, and through infecting widely used executive files. This combined with the automatic start of the virus after the infection lead to the rapid spread of the virus although it can not be installed without the explicit consent of the user.

Clearly mobile viruses are not a real threat yet although the six basic viruses found in 2004 increased extremely quickly to 30 versions after their source code was published on the Internet. Most of them were created as the proof for a certain virus conception rather than to cause harm: they need the users consent when being installed, they don't try to hide their presence, they can be removed fairly easily and can not alter or destroy the information saved on the sim-cards. It is noteworthy though that the first malicious mobile viruses attack devices that work under Symbian, which dominates the smart phone market.

These 30 threats to mobile security seem harmless when compared with the more than 180 000 known computer viruses but the first attempts at real virus attacks in mobile networks give as a glimpse at what to expect from mobile viruses in the future: overexploitation of mobile networks and putting communicators out of order, sending pictures and/or confidential information, constant dialing of phone numbers stored in the address book and sending high-priced text messages. Furthermore the availability of free or cheap text message sending can soon turn phone-spam into a larger problem similar to Internet-spam. Unlike computer viruses though the mobile malicious software threatens to cause functional, informational and financial loss to every single user, especially since in a few years mobile devices will probably become the most common way to access the Internet.

Nonetheless, malicious software is not the only danger to smartphones. Cell phones and other mobile devices, such as Research In Motion's BlackBerry have risks for their

users on a very basic level since they usually have a large volume of confidential information that is not password protected. That makes them vulnerable to the so-called blue snarfing – no-trace information theft from Bluetooth devices by using the weaknesses of the wireless technology. This how Paris Hilton’s T-Mobile Sidekick was hacked in early February and all the information it contained – pictures, text messages, email addresses and address book, was published on a few websites.

## **PROTECTION POSSIBILITIES**

The creation of a decent protection for mobile devices has to become a joint task. The responsibility should be born by the service provider who should install antivirus products on his servers, the device producer, the operating system producer and the end-user.

Some of the measures that can be taken are:

- ◆ Development of phone firewalls to provide antivirus and antispam protection. McAfee, Symantec, Check Point, Trend Micro and other offer products with similar capabilities.
- ◆ Turning unauthorized access preventive technologies into part of mobile device users’ protection.
- ◆ Incorporation of a variety of options for automatic locking of mobile devices as well as a variety of passwords, secret questions, encoding and hiding the information saved.
- ◆ Creation of mechanisms for quarantining of infected or unprotected mobile devices.
- ◆ Introduction of the possibility to delete all data after several wrong password inputs or lack of synchronization with a computer after a certain period of time.

## **RECOMMENDATIONS FOR MOBILE PHONE USERS**

All mobile phone and mobile software producers treat security earnestly and constantly develop and improve protection and anti-virus programs for their products. Users can protect their cell phones on their own by denying access to infected application using the following simple measures:

- ◆ Accept and load system files only from trusted sources. This includes the provider’s portals and other well-known producer resources which implement the appropriate security measures against viruses and other dangerous applications.
- ◆ If a warning appears on your phone while loading an application, that means that the file you are loading has not been officially registered. In this case, you should be extremely careful and check whether the file is safe.

## **RECOMMENDATIONS FOR PDA USERS**

Although PDAs are used as a bearer of malicious software rather than the end target of the attack, a hacker can identify a certain device by automatically scanning the ports and attack it directly. The popularity of Wi-Fi and CDMA wireless access increases the probability of such attacks. Here are the basics of what users can do:

- ◆ Protect your PDA with a good password.
- ◆ Scan the device frequently with a good and updated antivirus program.
- ◆ Encrypt the confidential information which is stored on the device.
- ◆ Install all security patches for the operating system in question (Windows Mobile, Palm OS, Java VM, Research In Motion (RIM) BlackBerry, Symbian OS or Linux)
- ◆ If possible use VPN for a wireless connection.

- ◆ Create different profiles with various passwords and limit the applications available when sharing a digital organizer among several users.
- ◆ Limit the number of wrong passwords that can be entered to avoid brute force attacks.
- ◆ If you store confidential information on the device install a bit information deleting software.
- ◆ Do not forget that PDAs are always on and if the Wi-Fi connection is allowed the device can constantly be sending data to wireless access points.

## **RECOMMENDATIONS FOR PDA CORPORATE USAGE**

The minimum that the corporate PDA security policy should include is:

- ◆ Protection of personal databases such as address books, calendars and data books.
- ◆ Protection of database applications such as SQL Server CE.
- ◆ Encoding of confidential files, folders and databases with at least 8 bit keys.
- ◆ Increasing password protection by locking the device.
- ◆ Putting expiration dates on the passwords used.
- ◆ Installing a firewall that allows connection only to authorized IP addresses.
- ◆ Banning all synchronization capabilities that are not being used.
- ◆ Ban on PDA password storage on desktops and vice versa.
- ◆ Installation and updating of good antivirus software.
- ◆ Installation of a special authentication software in order to avoid brute force attacks and password eavesdropping.
- ◆ Installation of the latest operating system security patches.
- ◆ Ban on the use of unauthorized Wi-Fi access points.
- ◆ Informing employees about social engineering methods for obtaining passwords and access to confidential information.

Viruses that are a real threat to the majority of mobile device users are yet to be created. One of the reasons is the large variety of models for mobile phones, organizers and PocketPCs and all of them use different software. For now this makes it practically impossible to create a universal mobile virus. Sooner or later though the mobile device operating systems will be standardized and virus writers will find ways to access them without user consent. With the growing integration between mobile phones and PDAs the threat of virus and spam epidemics will also increase.

## **MOBILE DEVICE WEAKNESSES**

The dangers to the security of PDAs, PocketPCs and smartphones are the same as those to personal computers:

- ◆ Viruses, trojans and worms.
- ◆ Data theft.
- ◆ Mobile exploits.
- ◆ Authentication theft.
- ◆ Wireless exploits.
- ◆ Service denied type attacks.
- ◆ TCP hijacking.

## MOBILE DEVICE SECURITY ENHANCING PRODUCTS AVAILABLE:

- ◆ Antivirus products.
- ◆ Authentication products.
- ◆ Bit-wiping software.
- ◆ Database security increasing products.
- ◆ Coding products.
- ◆ Firewalls.
- ◆ VPN.
- ◆ Wireless security enhancing products.

## BIBLIOGRAPHY (20050430)

- [01] <http://enterprisesecurity.symantec.com/article.cfm?articleid=5455&EID=0>
- [02] [http://www.mcafeesecurity.com/us/about/press/corporate/2005/20050425\\_185320.htm](http://www.mcafeesecurity.com/us/about/press/corporate/2005/20050425_185320.htm)
- [03] <http://www.mobilecommunitydesign.com/archives/000088.php>
- [04] <http://www.cybertelexcom.org/spam/fcc.htm>
- [05] <http://www.securitypark.co.uk/article.asp?articleid=23072&CategoryID=4>
- [06] <http://www.eweek.com/article2/0.1759.1779359.00.asp>
- [07] <http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=35480>
- [08] <http://www.cooltechzone.com/index.php?option=content&task=view&id=1069>
- [09] [http://www.communications-news.com/comms\\_news/comms\\_news\\_story.ehtml?o=968](http://www.communications-news.com/comms_news/comms_news_story.ehtml?o=968)
- [10] <http://www.net-security.org/news.php?id=7007>
- [11] [http://www.betanews.com/article/Mobile\\_Phone\\_Virus\\_Surfaces\\_in\\_US/1109005073](http://www.betanews.com/article/Mobile_Phone_Virus_Surfaces_in_US/1109005073)
- [12] [http://www.infoworld.com/article/05/04/25/HNhackersplot\\_1.html](http://www.infoworld.com/article/05/04/25/HNhackersplot_1.html)
- [13] <http://www.securityfocus.com/columnists/294>
- [14] [http://www.mobilecompetency.com/mv\\_newsletters/mv\\_Sept23\\_2004.html](http://www.mobilecompetency.com/mv_newsletters/mv_Sept23_2004.html)
- [15] <http://www.networkmagazineindia.com/200201/focus2.htm>
- [16] [http://techrepublic.com.com/5100-6314\\_11-5274902.html#](http://techrepublic.com.com/5100-6314_11-5274902.html#)
- [17] <http://news.bbc.co.uk/2/hi/technology/4445125.stm>
- [18] <http://www.esato.com/news/article.php?id=499>
- [19] [http://www.surgeryofsound.co.uk/mobile\\_phone\\_viruses.htm](http://www.surgeryofsound.co.uk/mobile_phone_viruses.htm)
- [20] <http://www.microsoft.com/athome/security/viruses/mobilevirus.msp>
- [21] <http://informationweek.com/story/showArticle.jhtml?articleID=57703724>
- [22] <http://billday.com/2005/02/20/thiry-mobile-viruses-and-counting/>
- [23] <http://www.techweb.com/wire/security/57703667>
- [24] <http://securitypronews.com/insiderreports/insider/spn-49-20050421MobileVirusesContinueToIncrease.html>
- [25] <http://in.rediff.com/money/2005/apr/25virus.htm>
- [26] <http://www.computing.co.uk/features/1140643>
- [27] <http://www.computershopper.co.uk/shopper/news/72162/mcafee-sounds-alarm-for-mobile-viruses.html>
- [28] <http://www.techworld.com/security/features/index.cfm?fuseaction=displayfeatures&featureid=1259&page=1&pagepos=2>
- [29] [http://mobile.f-secure.com/support/faq\\_threat.shtml](http://mobile.f-secure.com/support/faq_threat.shtml)
- [30] <http://www.mobilepipeline.com/159401274>
- [31] <http://informationweek.com/story/showArticle.jhtml?articleID=57703710>
- [32] <http://www.orah.com/index.php?option=news&task=viewarticle&sid=86>
- [33] <http://weblog.physorg.com/news1500.html>
- [34] [http://www.theregister.co.uk/2005/04/13/mobile\\_botnet/](http://www.theregister.co.uk/2005/04/13/mobile_botnet/)
- [35] [http://www.notestomysel.net/notes/2004/08/mobile\\_viruses.html](http://www.notestomysel.net/notes/2004/08/mobile_viruses.html)
- [36] <http://www.emediawire.com/releases/2005/2/prweb208033.htm>
- [37] <http://news.techwhack.com/508/mcafee-ntt-docomo/>
- [38] [http://www.holz-elektronik.de/holz/de/aktuelles/unternehmensnews/20050317\\_3.html](http://www.holz-elektronik.de/holz/de/aktuelles/unternehmensnews/20050317_3.html)
- [39] <http://www.webpronews.com/news/itnews/wpn-41-20050420MobileVirusesDouble.html>
- [40] <http://crossword.uniontrib.com/news/computing/20050420-0723-tech-mobile-viruses.html>
- [41] <http://www.telecomasia.net/telecomasia/article/articleDetail.jsp?id=148130>
- [42] [http://www.tekrati.com/T2/Analyst\\_Research/ResearchAnnouncementsDetails.asp?Newsid=4374](http://www.tekrati.com/T2/Analyst_Research/ResearchAnnouncementsDetails.asp?Newsid=4374)
- [43] [http://www.findarticles.com/p/articles/mi\\_m0GTV/is\\_8\\_21/ai\\_n6354802](http://www.findarticles.com/p/articles/mi_m0GTV/is_8_21/ai_n6354802)
- [44] [http://www.ericsson.com/mobilityworld/sub/articles/other\\_articles/05mar12](http://www.ericsson.com/mobilityworld/sub/articles/other_articles/05mar12)
- [45] <http://www.thefeature.com/article?articleid=100969>

---

### AUTHOR INFORMATION:

*Eugene NICKOLOV is a Professor of Informatics, Doctor on Mathematical Sciences (DSc), Doctor of Computer Sciences (PhD), Engineer of Radioelectronics, Master of Microelectronics and Director of National Laboratory of Computer Virology at Bulgarian Academy of Sciences.*