MALWARE GOES MOBILE

BY MIKKO HYPPONEN

Computer viruses are now airborne, infecting mobile phones in every part of the globe. Security companies, cellular operators and phone makers are moving to quash these threats before they spiral out of control

The day the computer security community had anticipated for years finally arrived in June 2004. I and other researchers who study malicious forms of software knew that it was only a matter of time until such malware appeared on mobile phones as well. As cell phones have evolved into smartphones—able to download programs from the Internet and share software with one another through short-range Bluetooth connections, worldwide multimedia messaging service (MMS) communications and memory cards—the devices' novel capabilities have created new vulnerabilities. Scoundrels were bound to find the weaknesses and exploit them for mischief or, worse, for criminal gain.

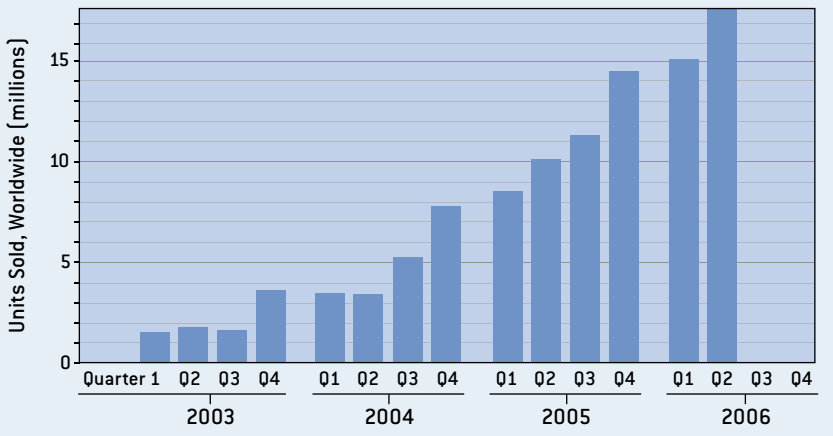
Sure enough, three summers ago security experts found the first rogue program written specifically for smartphones. Dubbed Cabir, it was a classic proof-of-concept virus, clearly created to

INFECTION of one smartphone by malicious software—malware—could bring down others in a domino effect.

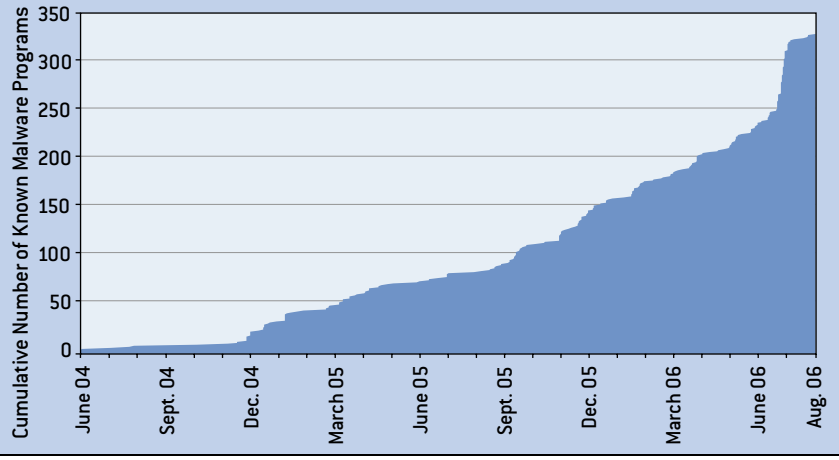
MORE PHONES, MORE TARGETS

The number of smart mobile devices in the world has expanded dramatically in recent years, and so has the amount of malware set loose to attack them. That mix is a recipe for disaster: as the size of a target audience increases, so, too, does the likelihood that miscreant programmers will attack it. And audience size is expected to soar in the years ahead. Industry analysts predict that more than 200 million smartphones will be sold in 2009.

SMARTPHONES ON THE RISE



GROWTH IN MOBILE MALWARE



capture bragging rights. It caused no damage to an infected device, other than running down the phone's battery as the virus tried to copy itself to another smartphone by opening a Bluetooth connection. The anonymous author, most likely somewhere in Spain, chose to post Cabir on a Web site rather than releasing it into the wild. But within two months other scofflaws had turned it loose in Southeast Asia. It soon spread worldwide.

Even though we had been on the lookout for viruses such as Cabir, security experts were not fully prepared to deal with it. As soon as the alert was sounded, my co-workers and I at F-Secure, a computer security firm, started inspecting the new virus, which was a type known as a worm [*see box on opposite page for definitions of terms*]. But we had no safe place to study it; unlike a computer virus that can be observed and dissected on a machine that is disconnected from any network, wireless malware can spread—in some cases, even make transoceanic leaps—the moment the infected phone is powered up.

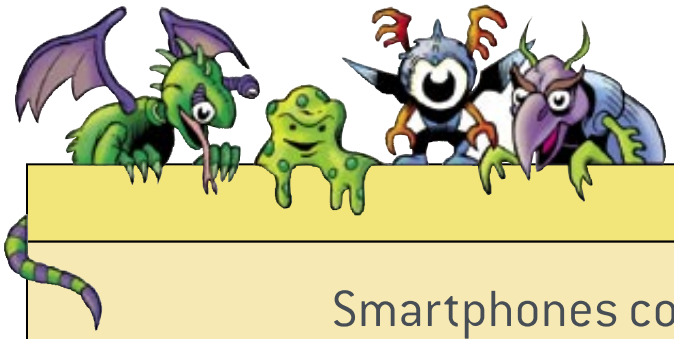
So we took four cell phones hit by Cabir to the basement bomb shelter in our office building and posted a guard at the door before turning them on, lest an unsuspecting employee walk in and catch the bug. Later that year F-Secure built two aluminum-and-copper-encased laboratories, impenetrable to radio waves, to study this contagious new form of malware.

Although the initial version of Cabir was relatively innocuous, some unscrupulous malware writers rushed to modify it into forms that are more virulent and damaging, while others began crafting novel kinds of attacks. Mobile viruses on the loose now can completely disable a phone, delete the data on it or force the device to send costly messages to premium-priced numbers. Within two years the number of viruses targeting smartphones soared from one to

Overview/*Imperiled Phones*

- The first malicious software aimed at smartphones hit in 2004. Smartphones are mobile phones that permit users to install software applications from sources other than the cellular network operator.
- Today more than 300 kinds of malware—among them worms, Trojan horses, other viruses and spyware—have been unleashed against the devices.
- As sales of such sophisticated phones soar worldwide, the stage is being set for the massive spread of malware. Steps are being taken to prevent that scenario, but the opportunity to block the onslaught is unlikely to last long.

MIRACLE STUDIOS (*preceding pages* and *opposite page*); LUCY READING-IKKANDA (*this page*); SOURCES: CANALYS (*top graph*) AND F-SECURE SECURITY RESEARCH (*bottom graph*)



more than 200, a rate of growth that roughly paralleled that of computer viruses in the first two years after the first PC virus, called Brain, was released in 1986.

Despite Herculean efforts to rein it in, PC malware continues at a gallop: more than 200,000 forms have been identified so far, and today an unprotected PC is often infected within minutes of connecting to the Internet. The economic costs of the 20-year onslaught have been steep, and they are spiraling higher as old-school malware written for glory has given way to a new era of "crimeware" designed for spamming, data theft or extortion.

Mobile malware, though little more than a nuisance today, could quickly escalate into an even more formidable problem than PC malware in the years ahead unless the security community, cellular network operators, smartphone designers and phone users all work together to hold it in check. The history of PC malware is humbling, but it offers lessons that will help us to anticipate some of the ways in which mobile virus writers will strike next and to take steps to thwart them.

A Rising Tide

IN 1988 many computer experts dismissed viruses as inconsequential novelties. That assessment proved regrettably naive. For mobile malware, the time is now 1988, and we have a brief window in which to act to avoid repeating the mistakes of the past.

One such mistake was to underestimate how quickly malware would grow in prevalence, diversity and sophistication. Prevalence is a function of both the population of potential hosts for virtual pathogens and of their rate of infection. The target population for malicious mobile software is enormous and growing by leaps. There are now more than two *billion* mobile phones in the world.

It is true that the great majority of these are older cell phones running closed, proprietary operating systems that are largely immune from viral infection. But customers are quickly abandoning these devices for newer generations of smartphones that run more open operating systems, Web browsers, e-mail and other messaging clients and that contain Flash memory card readers and short-range Bluetooth radios. Each of these features offers a conduit through which malware can propagate.

Smartphones could in the very near future make up most of the world's computers.

Bluetooth, for example, allows certain mobile worms to spread among vulnerable phones by mere proximity, almost like the influenza virus. A Bluetooth-equipped smartphone can identify and exchange files with other Bluetooth devices from a distance of 10 meters or more. As victims travel, their phones can leave a trail of infected bystanders in their wake. And any event that attracts a large crowd presents a perfect breeding ground for Bluetooth viruses.

A particularly nasty form of Cabir, for example, spread so rapidly through the audience at the 2005 world track and field championships in Helsinki that stadium operators flashed warnings on the big screen. Most smartphones can put Bluetooth into a "nondiscoverable" mode that protects them from invasion by worms. But few users avail themselves of this feature. While giving a talk at a computer security conference this spring, I conducted a quick scan of the room and found that almost half the professionals in the audience had left the Bluetooth radios in their phones wide open. The proportion is even higher among the general population, so these devices offer a disturbingly effective vector for invisible parasites.

And this host population is growing rapidly. Smartphones got started as expensive business models, but their popularity with consumers has recently taken off. With each generation the devices accrete more PC-like functionality. At the same time that smartphones have begun sporting features such as video cameras, GPS navigation and MP3 players, their prices have dropped—subsidized in part by network operators, who hope the new capabilities will encourage customers to spend more on cellular services. Manufacturers sold more than 40 million smartphones last year, and industry analysts expect to see 350 million units in service by 2009.

In the medium term, these devices may be adopted most quickly in emerging economies, where computer owner-

A Malware Primer

PHISHING SCAM
Fraudulent Web page, e-mail or text message that entices the unwary to reveal passwords, financial details or other private data.

SPYWARE
Software that reveals private information about the user or computer system to eavesdroppers.

TROJAN HORSE
A program that purports to be useful but actually harbors hidden malicious code.

VIRUS
Originally, computer code that inserts itself into another program and replicates when the host software runs. Now often used as a generic term that also includes Trojan horses and worms.

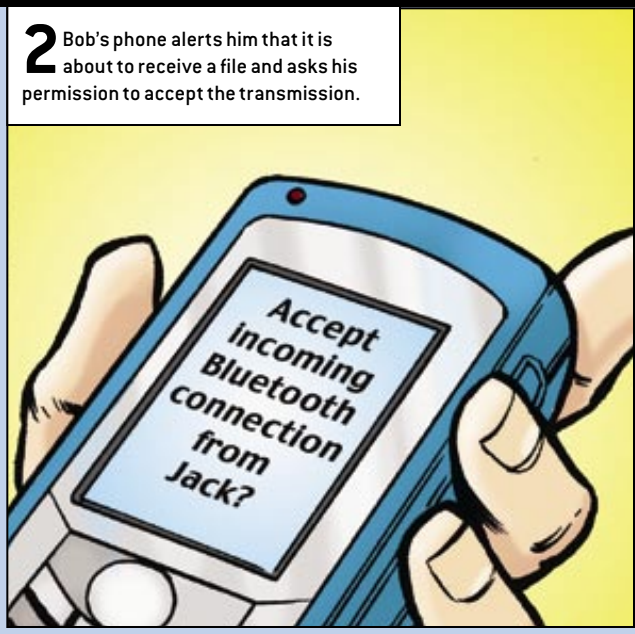
WORM
Self-replicating code that automatically spreads across a network.

ANATOMY OF AN ATTACK

Even an astute person can fall victim to a well-designed mobile worm, such as CommWarrior. Some 15 variants of this worm have been seen since the malware was first spotted in March 2005. CommWarrior exploits the Bluetooth user interface to persuade victims to install the malware on their phones. Once active, it can spread rapidly via Bluetooth connections, multimedia (MMS) messages and memory cards.

1 As Bob boards a bus, his smartphone beeps. Another phone in the vehicle is carrying CommWarrior.Q, which is attempting to copy itself onto Bob's phone via Bluetooth.

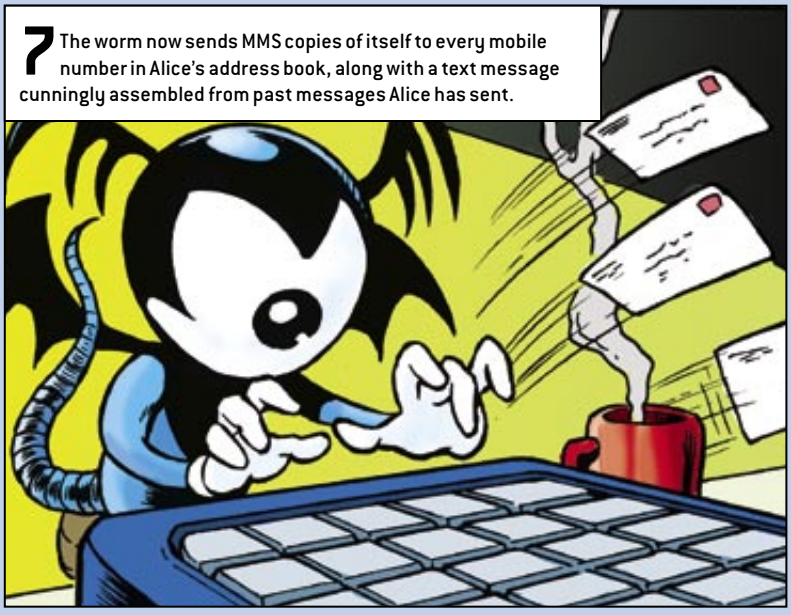
2 Bob's phone alerts him that it is about to receive a file and asks his permission to accept the transmission.

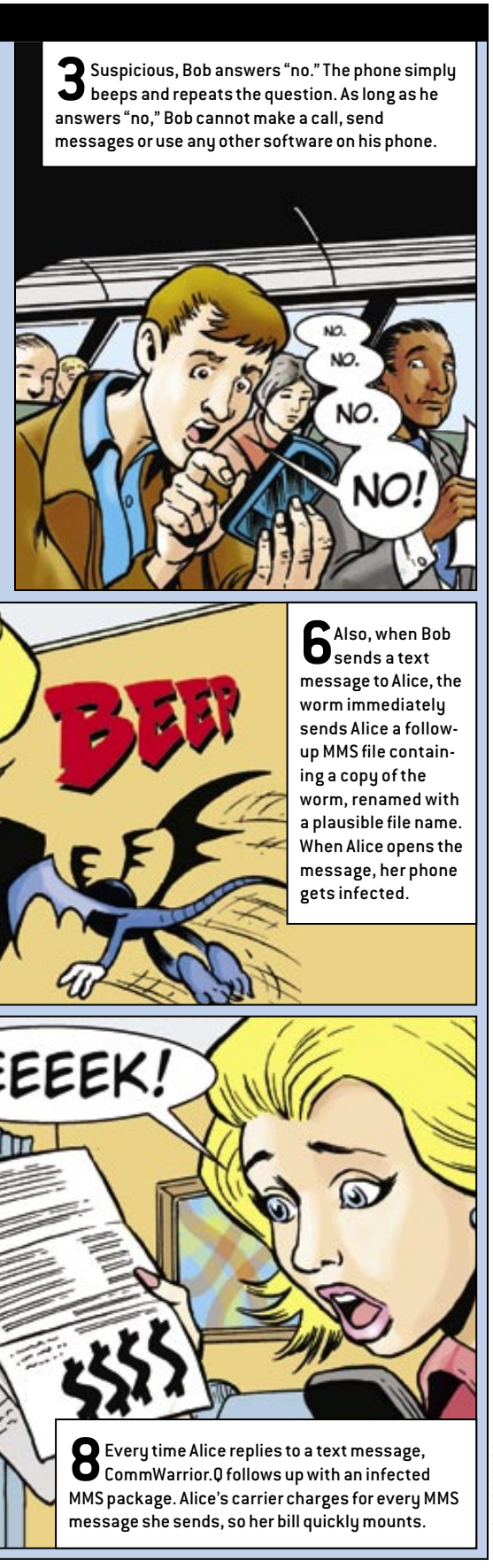


4 Bob needs to make an urgent call so he finally answers "yes" to the transmission query and to the installation and security queries after it. His phone now becomes infected. If Bob should place his phone's memory card into another phone to transfer an application, the second device would become infected.

5 CommWarrior.Q begins scanning for other Bluetooth devices nearby and attempts to copy itself onto any it finds, sometimes onto several at once.

7 The worm now sends MMS copies of itself to every mobile number in Alice's address book, along with a text message cunningly assembled from past messages Alice has sent.





MIRACLE STUDIOS

ship is still relatively low. Research by Canalys, a high-tech consultancy near Reading, England, found that smartphone sales in the first quarter of this year grew twice as fast in eastern Europe, Africa and the Middle East as they did in western Europe. Industry analysts predict that some developing nations will choose to forgo construction of a wired Internet infrastructure and will instead upgrade their digital wireless networks and promote smartphones as affordable computers. The wireless route can be much less expensive to construct and maintain (and, from a censor's perspective, much easier to monitor and control).

If these forecasts prove accurate, smartphones could in the very near future make up most of the world's computers. And huge populations of users who have little or no experience with computers could soon be surfing the Web and sharing files with their phones. They would present mobile malware creators with an irresistibly large and unwary target.

One lesson from PC viruses is that the bigger the target, the bigger the attraction for nefarious programmers. The vast majority of desktop malware works only on the ubiquitous Microsoft Windows operating system. For the same reason, nearly all the mobile worms and Trojan horses released so far infect the Symbian operating system, which runs some 70 percent of smartphones worldwide—including phones made by Nokia, Samsung, Sony Ericsson and Motorola. In contrast, only a few varieties of malware infect Microsoft's PocketPC or Windows Mobile, Palm's Treo, or Research in Motion's BlackBerry devices. The Symbian bias partly explains why mobile malware is currently most prevalent in Europe and Southeast Asia, where Symbian is commonplace, but is rarer in North America, Japan and South Korea. Cellular operators in North America have spread their markets more equally across the various platforms. The Japanese and Korean markets were dominated for a long time by Linux-based phones, and carriers there heavily restrict the types of applications that users can install on their phones.

Carriers would be wise to begin educating cellular customers now about how to identify and avoid mobile viruses, rather than waiting until these infections become epidemic. Phone makers should install antivirus software by default, just as PC manufacturers now do. And regulators and phone companies can also help avoid the monoculture problem that plagues PCs by encouraging a diverse ecosystem for smartphones in which no single variety of software dominates the market.

From Kicks to Crime

DIVERSITY CUTS both ways, of course. Over time malware, too, inevitably mutates into new species that attack and subvert useful software in an ever widening variety of ways. On the PC, the early viruses were eventually joined by Trojans, worms, spyware and most recently phishing attacks. Since 2003 much of the new malware appearing on PCs has been written for profit rather than for mere mischief. Organized gangs of cyber-criminals now operate all over the world. Thieves use crimeware to make money by stealing financial data, business secrets or computer resources. Spammers assemble "botnets" of hacked machines to forward bulk e-mail and phishing scams. And blackmailers extort money with threats of digital destruction or of virtual blockades that shut down a company's Web or e-mail servers. In some countries, cyber-criminals are virtually untouchable because authorities lack the technical

THE AUTHOR

MIKKO HYPPONEN is chief research officer for F-Secure, a computer security company in Helsinki that consults for mobile phone makers and network operators. His team of virus fighters has been first to identify and combat dozens of viruses in the 15 years he has worked at F-Secure, including the infamous LoveLetter worm in 2000. A co-author of two books on computer security, Hypponen has assisted with investigations by Microsoft, the U.S. Federal Bureau of Investigation, the U.S. Secret Service and Scotland Yard in the U.K.

Computers do not have a built-in billing system; mobile phones do. The bad guys will exploit this feature before long.

MIRACLE STUDIOS

expertise, resources or will to enforce laws against computer crimes.

As for-profit virus writing increases, the likelihood of severe mobile malware attacks escalates as well. After all, every phone call placed and every text or multimedia message sent is also a financial transaction. That opens up a flood of potential earning opportunities for profiteer hackers and virus authors. Computers do not have a built-in billing system; mobile phones do. The bad guys will exploit this feature before long.

Indeed, at least one already has. A Trojan called RedBrowser sends a continuous stream of text messages from any phone it infects to a number in Russia until the user disables the phone. Each message is charged at a premium rate of about five dollars, resulting in huge bills for the unfortunate victims. Some cellular carriers hold their customers liable for such unauthorized transactions, and when they do, the criminals, who own the premium number, collect the premium fees. Luckily, RedBrowser has so far only been spotted inside Russia.

Meanwhile service providers in North American markets are beginning to introduce "mobile wallets." Customers will be able to use their phones to transfer funds from their accounts to others by sending specially formatted text messages. PayPal, a digital payments firm, offers a similar service that allows users to buy items using their phones. Such services could be of intense interest to malware authors.

With both the sophistication of mobile malware and the technological and financial capabilities of mobile phones on the rise, we will have to move rapidly in the next couple of years. Actions now could thwart mobile malware while it is in its infancy and while smartphone services are still fairly flexible in their design. But that window of opportunity will not stay open for long.

More Dangers Ahead

THE REASON FOR HASTE is clear when one considers all the ways that hackers could—but have yet to—wreak havoc with smartphones. On personal computers, many of the worst culprits spread via e-mail or force infected machines to spew spam onto the Internet. None of the miscreant programs released so far for smartphones capitalize on the devices' ability to send e-mail. It is only a matter of time until malware appears that can propagate as e-mail attachments or can turn phones into spam-sending robots.

Spyware is another mushrooming problem in the PC arena, and the potential for surreptitious software on phones to destroy privacy is obvious. Only a handful of such programs have been seen as yet. One, called FlexiSpy, periodically and invisibly sends a log of phone calls and multimedia messages, both sent and received, to a third party. The eavesdropper needs to gain physical access to the phone to download and install the spying program.

It may not be long, however, before hackers incorporate this kind of eavesdropping behavior into viruses that replicate on their own. With new phones featuring voice recorder capability, manufacturers should take extra care to ensure that these features cannot easily be exploited by malware to record conversations and then beam the recordings to a snoop.

Then there is the surprising fact that not one of the more than 300 forms of mobile malware released as yet exploits programming bugs or security design flaws to insert itself into a vulnerable machine. This has long been a standard modus operandi for many PC viruses and Trojans.

So far mobile malware writers have instead relied exclusively on "social engineering"—in other words, tricking users into actively allowing installation of the malicious program on their phones. Some camouflage themselves as useful utilities or desirable games. But some, especially ones like Cabir and CommWarrior that spread via Bluetooth, do not. Many people accept the files even when the device warns of the security risk and gives them a chance to refuse the foreign software.

I and other researchers have asked

Some Protective Software for Smartphones

COMPANY	PROGRAM NAME	SUPPORTED OPERATING SYSTEMS
F-Secure	Mobile Anti-Virus Mobile Security	PocketPC, Symbian, Windows Mobile Nokia Communicators
McAfee	VirusScan Mobile	PocketPC, Symbian, Windows Mobile
Symantec	AntiVirus for Handhelds Mobile Security	Palm, PocketPC, Windows Mobile Symbian
Trend Micro	Mobile Security	PocketPC, Symbian, Windows Mobile

A Bestiary of Mobile Malware

NAME	TYPE AND METHOD OF INFECTION	EFFECTS
Cabir (discovered June 2004)	Worm. Connects to other Bluetooth devices and copies itself	Constant Bluetooth scanning drains phone's battery
CommWarrior (discovered March 2005)	Worm. Replicates via Bluetooth; sends itself as an MMS file to numbers in phone's address book and in automatic replies to incoming SMS (text) and MMS messages; copies itself to the removable memory card and inserts itself into other program installation files on phone	Some users incur a charge for every MMS file the worm sends; variants of the worm disable phone entirely
Doomboot (discovered July 2005)	Trojan horse. Pretends to be a version of the Doom 2 video game, enticing users to download and install it	Prevents phone from booting and installs Cabir and CommWarrior on phone
RedBrowser (discovered February 2006)	Trojan horse. Deceptive description on a Web site offering many downloadable programs entices users to install this Java program, which runs on hundreds of phone models	Surreptitiously sends a stream of text messages, at a premium rate of $5 each, to a phone number in Russia
FlexiSpy (discovered March 2006)	Spyware. Internet download, typically installed by someone other than phone owner	Sends a log of phone calls and copies of text and MMS messages to a commercial Internet server for viewing by a third party

people victimized by such viruses: Why did you click "yes"? A common answer is that they did not at first—they chose "no." But then the question immediately reappeared on the screen. A worm, you see, does not take no for an answer, and it gives the user no time to hit the menu option to disable Bluetooth [*see box on pages 74 and 75*]. Unfortunately, even the newest versions of most smartphones permit the kind of Bluetooth harassment that effectively denies a person use of a phone until the individual accepts the file transfer (or until the user walks out of range of whatever infected device is sending the request—although few people realize they have this option).

Staying a Step Ahead

THE ONLY HOPE of stopping mobile malware before it seriously degrades the utility and value of smartphones is quick and concerted action on the part of all concerned. Antivirus software now available from many companies can immunize and disinfect smartphones. Yet few customers have installed such protection. That needs to change.

Phones should also incorporate firewall software that warns the user when a program on the phone seizes the initiative to open an Internet connection. This is an especially important form of protection for smartphones that can connect to Wi-Fi (also called 802.11) networks and thus directly to the public Internet. Many cellular companies aggressively filter traffic on the GPRS or UMTS data networks that their mobile devices use; open Wi-Fi networks have no such protection. And while some carriers already filter their MMS streams to remove messages bearing malicious attachments, all should do so.

Some of the biggest phone manufacturers have joined the Trusted Computing Group, which has been hammering out industry standards for microcircuitry inside phones that will make it harder for malware to get at sensitive data in the device's memory or to hijack its payment mechanisms. And Symbian recently released a new version of its operating system that does an improved job of protecting key files and that requires software authors to obtain digital certificates from the company. The new Symbian system refuses to install programs not accompanied by a certificate. Unless disabled by a user, the system effectively excludes all mobile malware discovered to date.

Governments could also play a more constructive role than they have so far. Even though most countries have passed laws against hacking both ordinary computers and the computers inside cell phones, enforcement is lax or nonexistent in most of the world. Many of the nations hit hardest so far by mobile malware outbreaks, such as Malaysia, Indonesia and the Philippines, do not always collect reliable and timely statistics that could be helpful for tracking software crimes.

For our part, my team and others in the security research community have been proactively studying Symbian and PocketPC, looking for vulnerabilities in the code and in the system designs that might afford entrée to malware. We hope to find these holes so that they can be patched before the bad guys exploit them in the inevitable next round of this constant battle. SA

MORE TO EXPLORE

Mobile Phones as Computing Devices: The Viruses Are Coming! David Dagon, Tom Martin and Thad Starner in *IEEE Pervasive Computing,* Vol. 3, No. 4, pages 11–15; October–December 2004.

Mobile Phones: The Next Frontier for Hackers? Neal Leavitt in *Computer,* Vol. 38, No. 4, pages 20–23; April 2005.

Mikko Hypponen and his teammates blog at **www.f-secure.com/weblog/**

Trusted Computing Group: **www.trustedcomputinggroup.org/groups/mobile**