# Status of cell phone malware in 2007

***Mikko Hypponen***
***Chief Research Officer***
***F-Secure Corporation***
***http://www.f-secure.com***
***http://mikko.hypponen.com***

Smartphones rock. However, smartphones can get infected as well. Mobile phone viruses are not science fiction.

As cell phones have evolved into smartphones capable of downloading programs from the internet and sharing software with one another through short-range Bluetooth connections, worldwide multimedia messaging service (MMS) communications and memory card slots, these new capabilities have created a platform for new kinds of viruses as well.

In June 2004 the first rogue program written specifically for smartphones was found. Known as **Cabir**, it was a classic proof-of-concept worm, written by a (now-defunct) hobbyist virus-writing group known as **29A** to capture bragging rights. It caused no direct damage to an infected device, but simply tried to copy itself to another smartphone by opening a Bluetooth connection. The author of the virus chose to post it on a web site rather than releasing it into the wild. But within weeks, someone had downloaded it and turned it loose in Southeast Asia. It soon spread worldwide – and is still seen in the wild today, three years later.

When we started inspecting the new virus at F-Secure labs in 2004, 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 try to 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 one of us to guard the door before turning the phones on in order to inspect the operation of the virus. Nowadays we operate several purpose-built 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, other malware writers rushed to modify it into forms that are more virulent and damaging. Others started developing totally new 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 numbers. Within three years, the number of viruses targeting smartphones soared from 1 to more than 350, a rate of growth that roughly parallels that of computer viruses in the first years after the first PC virus, called Brain, was released in 1986.

Mobile malware, although little more than a nuisance today, could escalate into as bad a problem as 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.

The target population for malicious mobile software is enormous and growing by leaps. There are now way over two *billion* mobile phones in the world.

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 commodity operating systems, web browsers, email 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.

Bluetooth, for example, allows mobile worms to attempt spreading by mere proximity, almost like the influenza virus. A Bluetooth-equipped phone 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 – although with current viruses, the recipients have to actively acknowledge the virus transmission before they can get infected. And any event that gathers a large crowd presents perfect breeding grounds for Bluetooth viruses.

And this host population is growing rapidly. Smartphones got started as expensive business models, but their popularity with consumers has now taken off. With each generation the devices accrete more PC-like functionality. At the same time that smartphones have begun sporting features such as hi-res videocameras, 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 are selling tens of millions of smartphones a 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 ownership is still relatively low. Research by Canalys, a consultancy, 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 chose to forego 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.

If these forecasts prove accurate, smartphones could in the very near future make up the majority 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 soft 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 Trojans and worms released so far infect the Symbian operating system, which runs on majority of smartphones worldwide —including phones made by Nokia, Samsung, Sony Ericsson and Motorola. By contrast, only a few varieties of malware infect devices based on Microsoft's Windows Mobile or PocketPC platforms as they simply don't have the market share.

The Symbian bias partly explains why mobile malware is currently most prevalent in Europe and South-East Asia, where Symbian is commonplace, but is rarer in North America as well as in Japan or South Korea. Cellular operators in North America have spread their markets more equally across the various platforms (including nice platforms like Palm and Blackberry). The Japanese and Korean markets used to be dominated by Linux-based phones, and carriers there heavily restrict the types of applications 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 more widespread. Phone makers and carriers should install antivirus software by default, just as PC manufacturers and ISPs now do.

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. In some countries, cyber criminals are virtually untouchable because authorities lack the technical expertise, resources or will to enforce 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 have figured this out. As an example, in May 2007 F-Secure Security labs found three new for-profit SMS trojans – known as **Viver**. The Viver family of trojans claims to be utility programs for Symbian-based smartphones. They were uploaded to popular file sharing sites in the hopes that people will download and install them.

When run, the Viver trojans immediately start sending text messages to premium-rate numbers. The messages are sent with international area codes, so they are able to reach the correct destination worldwide. These messages are sent as frequently as every five minutes, and they could cost the user up to $7 per message. The money of course goes to the author of the virus.

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 is preparing a similar service that will allow users to buy items using their phone. Such services will 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 smartly in the next couple of years. There is a window of opportunity now to thwart mobile malware while it is in its infancy and while smart phone services are still fairly flexible in their design. But it won't stay open for long.

Consider all the ways that hackers could wreak havoc with smartphones, but haven't yet. On personal computers, many of the worst culprits spread via email 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 email. It is only a matter of time until malware appears that can propagate as email 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. So far, only a handful of mobile spyware has been seen. One of them, 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. Similar spy programs have been made for Windows Mobile devices and even for Symbian Series 60 3rd edition devices – complete with a "*Symbian Signed*" signature on them!

None of the known 360 forms of mobile malware released so far exploit security vulnerabilities in order to insert themselves into a vulnerable machine. Instead, mobile malware relies exclusively on 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 those like **Cabir** and **CommWarrior** that spread via Bluetooth, do not. Yet 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 people victimized by such viruses: why did they click "*Yes*"? A common answer is that they didn't, at first—they chose "*No*." But then the question immediately reappeared on the screen. A worm, you see, doesn't take no for an answer, and it gives the user no time to hit the menu option to disable Bluetooth. Unfortunately even the most recent versions of most Symbian phones permit this kind of Bluetooth harassment that effectively denies a person use of her phone until she acquiesces to the file transfer. (Or until she walks out of range from whatever infected device is sending the request; but few people realize they have this option.)

Some mobile operators already filter their stream of MMS messages to stop malicious MMS messages; 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 the phone that

will make it harder for malware to get at sensitive data in the device's memory or to hijack its payment mechanisms.

Governments could also play a more constructive role than they have so far. Although 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, don't always collect reliable and timely statistics that could be used to track software crimes.

The security research community has been proactively studying mobile platforms, looking for vulnerabilities in the code and in the system designs that might offer entry for malware. We hope to find these holes so that they can be patched before bad actors exploit them in the inevitable next round of this constant battle.