

EZURiO

Wireless out of the box

Mobile phone viruses – just what the network operators want?

Instead of educating customers and shipping phones in a safe default mode, it's becoming fashionable to blame Bluetooth for spreading phone viruses. Is that fair, or does it raise the spectre of mobile operators deciding that they can do without Bluetooth, turning the phone back into something where they retain complete ownership?

"When handset vendors promote their phones with the slogan "Infect your friends", what hope is there for a balanced debate on mobile phone security?"

Nick Hunn
CTO - Ezurio Ltd

February 2005

Ezurio Ltd
126 Colindale Avenue
London NW9 5HD
United Kingdom

Tel: +44 208 938 1000
Email : info@ezurio.com
Web: www.ezurio.com

©2005 Copyright Ezurio Ltd
All rights reserved

Mobile phone viruses – just what the network operators want?

Security experts have found a new streak of paranoia to mine – the appearance of viruses on mobile phones. It's an issue that is real, but one that both manufacturers and network operators are keeping remarkably quiet about. Instead of educating customers and shipping phones in a safe default mode, it's becoming fashionable to blame Bluetooth. Given the current distaste for Bluetooth that operators like Verizon are exhibiting, there is a real danger that some may even see mobile viruses as an opportunity to turn back the clock, disabling Bluetooth and returning to their preferred but discredited model of the phone and network as a walled garden.

The end of January saw a flurry of reports from security analysts about the latest mobile phone viruses. Since the Cabir virus was discovered nine months ago there has been a slow and inevitable release of increasingly malignant programs that spread on Symbian smartphones and which use Bluetooth as the method of propagating themselves. Last autumn saw the stakes raised with the arrival of Skulls, which could change icons on the phone, making it difficult to use. Now we have Gavno, which can potentially disable the handset by overwriting system files with corrupted data.

That's more than enough to grab the attention of the security analysts, who have jumped to christen these programs "Bluetooth viruses". The name may be racy, but it conceals the reality that these malicious programs should not be blamed on Bluetooth, but on the way manufacturers and networks configure their handsets. And although they've all been written on the Symbian platform, that's only a confirmation of Symbian's market leading position. Other phone operating systems are equally vulnerable and will inevitably be targeted.

The security industry obviously wants to take the opportunity of highlighting the dangers, as if they can hook into the paranoia surrounding PC viruses it opens up the mouth-watering prospect of them selling anti-virus software for every handset. In reality the viruses on Symbian handsets are far more akin to the phishing scams in the email world that rely on user gullibility and ignorance rather than flaws in the handset.

If you received an unsolicited CD through the post labelled "Unknown software" would you install it on your PC? You should have learnt enough by now to answer no. If you receive an unsolicited program on your smartphone and are asked the same question, what do you do? That's how the current mobile viruses spread – not by cleverly worming their way into your handset, but by asking the question to which the user answers "Yes – come on in." You're even asked if you're sure two more times. But still users fall for it.

Bluetooth gets blamed despite the fact that it's only the innocent messenger that carries the program. Once you have a malicious program like this on your handset it will use the Bluetooth connection on the phone to search for other phones within range that have both Bluetooth turned on and which are also set up to promiscuously receive unsolicited messages from all and sundry. (Incidentally this is not a clever way to configure your phone, but it's the one in which most manufacturers decide to sell it to you.) The malicious application claps its hands, or jiggles its bits, or whatever these things do and promptly sends a copy of itself to the next phone. The newly infected phone pops up a message on its screen asking a question along the lines of "New application received – do you want to install it?" If you say yes, you'll be asked a second time whether you really want to. If you still say yes, you'll be asked a third and final time. At which point a positive answer will get you the virus, along with the dubious honour of propagating it to those around you. And the security companies get the chance to blame Bluetooth and sell us all anti-virus software.

There's a cheaper and easier way to stop these viruses. It's to set up Bluetooth safely on your phone in the first place and to learn to say "NO" to any unsolicited messages. Essentially it's three steps:

- Make Bluetooth on your phone invisible by going to the Bluetooth menu and setting it to be "non-discoverable" or "hidden". It will still work with your headset, PC, PDA and other Bluetooth devices – you just need to temporarily make Bluetooth visible when you set them up (or "pair" them, in the Bluetooth lingo). But it means your phone ignores Bluetooth spam.
- Always remember to delete any unsolicited messages without opening them.
- If your phone asks you if you want to install a program that you haven't just sent to it, say "NO".

That's it.

Remember the examples of St Peter and Julius Caesar. You'll be asked three times – just keep on saying no.

It's easy, it's been defined within the Bluetooth standard since day one and it works. So why aren't the phone manufacturers and network operators telling their users? This should be in big print on the Quick Start Guide of every phone. Instead of which you'll be lucky to find it on page 172 of the manual. And while you're searching for it you'll start to hear the rumours that Bluetooth is unsafe.

In the early days of the Cabir virus, little harm was done, but the more recent appearance of Skulls and Gavno have moved to a level that will modify data, or even stop your phone working.

It doesn't take a genius to realise that even more devious features will be added to these programs. It's fairly trivial to add a silent dialler that will constantly make calls to a premium rate number or short code, racking up your phone bill in the same way that auto-diallers have done for PC modems.

In fact one of the earliest Symbian "viruses" did include an autodialler. At the start of 2004 a cracked version of Mosquitos started to circulate that silently dialled premium numbers. The industry response was to issue a press release, effectively saying you only get what you deserve if you download pirate software (<http://www.symbian.com/press-office/2004/pr040810.html>). This was before the first application that used Bluetooth to spread itself, but nothing was mentioned about Bluetooth settings. Even after Cabir opened this particular Pandora's box, there's still a great ambivalence towards addressing it. In January 2005 Nokia launched its Snakes game for N-Gage, which it recommends should be spread using Bluetooth. Visit their website at <http://web.n-gage.com/snakes/main.jsp> and you'll find an "INFECT" button, with the messages "Infect your friends" and "Spreading the snakes is just as easy as getting it". When handset vendors promote their phones with the slogan "Infect your friends", what hope is there for a balanced debate on mobile phone security?

The increasing functionality of smartphones, where most of the call features are accessible to programs adds further levels of speculation as to where this malware will go. As well as silent diallers, programs can be written to send abusive messages to other names in your phonebook. They can forward your existing text messages to others in your address book – a feature that will have business users quaking, and with a little external help they can even send text messages that appear to come from another contact and not from you. If you don't think that's possible, there's a nice application (not a virus) called SMS Extender that you can purchase from <http://www.simeda.com/smsxtender.html> that will open you eyes to the potential of SMS. Try it out.

An even more devious programmer could devise a program that infects and spreads between Symbian handsets, but only sends a critically destructive

program to Microsoft handsets. Or a Nokia one that destroys Sony-Ericsson handsets. Both of which are perfectly feasible to implement. If I can think these up, you can be pretty sure there's someone out there thinking up a whole lot worse.

One would assume that the spectre of this malware would be anathema to the mobile industry. At the minimum level it renders a handset unusable – something the networks may consider a minor inconvenience for the user, but a more major one for themselves as it stops the revenue stream from your calls.

Moreover, this prospect of spurious billing is a potential nightmare for the operators as users will start to question their bills. Unless we posit the existence of more altruistic autodialing virus that only calls charity donation lines; after all, how many users would have disputed the donations that such a virus would have made on their behalf to tsunami relief if it had been in existence?

So why the silence? Neither the manufacturers or networks would appear to have anything to gain by letting the spread of these programs gain momentum. Or do they? Look at what is happening with Verizon - one of the U.S. operators. They've changed the software in the Motorola V710 phone that they sell to disable Bluetooth. Not to stop viruses, but to stop users transferring images, ring tones and music to their phone from their PC. Their worry is that their users will make these transfers for free, just like Bluetooth users do everywhere else in the world, rather than paying them money to do it over the network. Not surprisingly their users are enraged and have just taken Verizon to court.

I doubt Verizon have wised up to the fact that they could have used the spectre of Bluetooth viruses as a defence (and if they try remember they could have set the phones to be non-discoverable as a far safer alternative). But if the networks make no attempt to educate their users it will become increasingly tempting for some of them to disable Bluetooth and cast it as the bogeyman. In their eyes disabling Bluetooth puts them back in control of everything on your phone. That means if you want to change anything you have to pay them. It's back to the womb-like security of the walled garden that they set up for WAP. It didn't work then, but they'd love to try again.

We need to make sure it doesn't happen. Bluetooth is becoming increasingly important to handset users. Not just for headsets, but for transferring photos, video clips and music between PC and phone as well as for synchronising data. The networks have no capability to transfer high resolution images from multi-megapixel cameras – without Bluetooth the smartphone becomes a severely disabled product.

It is important for all parts of the industry to realise that education is the key. Shipping handsets configured sensibly and explaining how to use Bluetooth will increase phone usage – ignoring the problem will just diminish user confidence in both handsets and the mobile operators. We've seen what happened in the PC industry when they tried to deny the problem. It's time for the mobile industry to show their intelligence by learning from those mistakes.

Of course, it's not just Bluetooth that can spread these viruses. MMS allows all sorts of file attachments to be sent over GPRS, so there's a future job for the networks to install virus checking within the network. And they're even quieter about that. If they believe disabling Bluetooth will solve the problem, they may well find it enrages and encourages hackers to turn their attention from short range Bluetooth distribution to wide area network distribution. And that gets really scary.

Ezurio is a leader in Bluetooth technology, providing products and embedded wireless technology to market leading companies. Visit www.ezurio.com for more white papers and background articles about wireless technologies.

Ezurio is a management spin out of TDK Systems Europe, funded by 3i.