

INTERNET NEWS

Viruses Gearing up For The Smart Set

By [Jim Wagner](#)

March 4, 2005

As the boundaries between cell phones and desktop functionality blur, the danger of a worldwide wireless virus increases.

Do those sound like the words a doomsayer would revel in pronouncing? After all, [Paris Hilton](#) and her T-Mobile address book aside, there hasn't been anything approaching a worldwide cell phone security problem since carriers first started adding data capabilities to their handsets.

Take the first reports of [Cabir](#), a cell phone virus that got its start last year as a proof-of-concept vulnerability on Symbian OS-enabled phones. This was before people started discovering the virus in cell phones throughout Europe, Asia and finally the [United States](#).

To call Cabir a cell phone virus is somewhat of a misnomer. The bug doesn't travel over a mobile phone carrier's network, but rather through the Bluetooth connections found in certain types of mobile phones, which limits how far and how fast it can travel. When a user accepts a caribe.sis file and elects to install the program, Cabir searches for other Bluetooth-enabled devices in its range.

For the time being, there's no payload attached to the virus, although security firm Symantec ([Quote](#), [Chart](#)) warns the virus will shorten battery life because of the repeated scans for other Bluetooth devices.

Not as prevalent, but more destructive, is the [Skulls Trojan](#), which, when installed, overwrites Symbian OS application info and icons and replaces them with a skull icon.

The Trojan, which started appearing on Symbian OS shareware sites last year, only targets the data applications; regular phone service is still available after infection.

Smartphones and feature phones -- voice phones with data applications -- are the wave of a future that's fast approaching. According to a recent report by U.K.-based research firm Canalys, sales of the phones are up 101 percent in the fourth quarter of 2004 from the same quarter in 2003; Nokia alone sold nearly five million smartphones in the quarter.

Exposing The Mobile Virus

There's not much that separates the functionality of these phones from a desktop's or even a PDA's: PalmOne's [Treo 650](#) supports Microsoft Exchange Server 2003 out of the box, letting users synch their calendars and e-mail, while smartphone manufacturers are gearing up with [3-D graphics accelerators](#).

"Probably about a third of all the cell phones in the U.S. are used by people in the business sense," said Adam Zawel, director of wireless/mobile enterprise and commerce at the Yankee Group. "That doesn't mean that these devices are integrated into IT systems, but that will change when you get more smartphones, and you see the merger between smartphone and PDA functionality."

Experts say that a smartphone virus, one that will spread throughout the globe, is in the offering. It won't happen today. It probably won't even happen next year, they say, but it's inevitable.

"As the phone becomes more of a handheld computer, you're going to encounter the same sets of issues that you would encounter with your computer," said Evan Scott, president and founder of consulting firm Evan Scott Group. "Today it's not an issue because I think people still just use their phone as a phone; over the next four, five years, as people start to incorporate more computer activities in their handheld devices, then I think the viruses will become a bigger issue."

Part of the problem with smartphones, according to Vincent Weafer, Symantec security response senior director, is that while carriers can put gateways in place to scan the traffic coming through the networks, other wireless technologies circumvent that protection.

"If you look at many of these smartphones, you see that they don't just connect to the carrier," he said. "You have the ability to connect to other devices. You have Bluetooth. Some even come with the ability to use Wi-Fi access directly to the Internet, so that the problem is you will always need end-point security."

Weafer said that it is the same problem that exists with today's desktop systems, where you need security at the desktop as well as at the Internet provider.

A Lesson in History

While viruses today seem innocuous enough, and hardly worth the headache to diligent cell phone users, history has shown the desktop viruses of yesterday were merely a preamble to the danger they pose today.

Consider the Melissa virus, which was one of the first desktop viruses to gain worldwide notoriety. [Launched in 1999](#) through the alt.sex Internet discussion group, it tore through the Internet community, and though its author, David Smith, was eventually [jailed](#) for his actions, Melissa ended up causing more than \$80 million in damages worldwide.

Melissa was one of several big-name viruses -- remember the ["I Love You"](#) virus and Concept? -- that brought attention to desktop security; today's viruses, like [Bagle](#), can be even more costly, setting up e-mail proxies on the user's desktop to launch massive spam campaigns worldwide.

It's only a matter of time before smartphone viruses like Cabir start delivering a Trojan horse that causes monetary damage or results in the theft of private information, experts worry. Unlike the damage caused on the desktop by the first viruses, end users and companies alike are more aware of the potential dangers of cell phone viruses. But the mechanism for unified virus protection and security patches for mobile operating systems hasn't materialized, said one security analyst.

In The Event of an Attack?

Mikko Hypponen, research director at security firm F-Secure, said there's no easy method for an end user to update their smartphone's operating system. There are no Windows Updates in the event vulnerabilities in the platform are discovered.

Mobile operating system market leader Symbian, which licenses its technology to smartphone manufacturers like Nokia, Motorola, Sony Ericsson and Fujitsu, doesn't have an OS security update center on its Web site. The company says it works closely with anti-virus vendors, network operators and manufacturers to make its product secure.

PalmSource, another mobile OS, directs its users to the support site of the applicable handset manufacturer. And according to Hyponnen, handset manufacturers do not provide updates to the OS itself.

"The infrastructure doesn't exist; the only way to do it right now is to take your phone to the repair shop and leave it there for a day or two or sell it, which doesn't scale," Hyponnen said.

The reason there is no service, according to Symbian's security site, is because no one has discovered any vulnerabilities in its OS. None of the malware found in existing viruses, the site notes, can be attributable to vulnerabilities in the operating system. Instead, the viruses "mislead Symbian OS phone users into accepting and/or installing the malware."

Officials also point out that incidences of the viruses in the wild have been isolated and that only in rare cases do users need to take a phone into a service center to have applications re-installed.

Laurie Spindler, a spokeswoman for PalmSource, said that while the company does not have a platform like the Windows update site, there are third-party vendors that deliver software security features, such as Credant Technologies and JP Mobile.

Securing a Team Effort

In the end, it comes down to a question of responsibility. Who ultimately needs to make sure their smartphones are secure? Is it the mobile phone carrier, the end user, the phone's manufacturer or the OS provider?

Tom Pica, a spokesperson at Verizon Wireless, said providers and end users alike share responsibility.

"We have a role to play, and the user has a role to play," he said. "We're entering a new world of data, so just at home you have certain responsibilities in terms of you should have a firewall, you should have anti-virus protection and you should take care of things like passwords and what you store on your device."

The market is also lending a hand. Upal Basu is co-founder and vice president of marketing at mFormation, a mobile phone device management vendor for carriers and enterprises. Companies like mFormation that provide over-the-air diagnosis and patch updates regardless of the device, he said, will be a boon to carriers looking to provide mobile phone protection.

He said the question of responsibility is complex, and will only get more complex with time as the mobile population grows.

"Who gets affected the most if a virus does take off and who gets compromised the most? If it's an employee of an enterprise, the thing that gets affected is the business of that

company," he said. "So for the corporate users, I think it will be the IT department that takes responsibility for the virus.

"For the consumer world, it has to be the mobile operator in partnership with a file creation company to provide some sort of guarantee to all their customers that says, 'look when you use data services from Verizon, you are ensured that there is a virus check that happens automatically,'" he continued.

Fortunately, there's time for the industry and customers to figure this out, though Scott is convinced it will take a major virus on the scale of Melissa before users in the United States take cell phone viruses seriously. "We're a reactive society," he said.

You can bet Ms. Hilton, and all her contacts, are taking a pretty good look at security options right now.