



Crime fears as cheap PCs head for Africa

Initiatives such as the OLPC and Classmate could mean an explosion in botnets in the developing world, warn security experts

Pete Warren

What if the plans to spread low-cost One Laptop Per Child (OLPC) and Intel Classmate computers to the developing world work? What if in a few years there are hundreds of millions of them out there? Many might applaud. But among computer security experts, there's growing concern that those schemes could inadvertently lead to a huge increase in computer crime.

Initiatives such as the OLPC and the Classmate are intended to help bridge the digital divide. But security experts warn that there could be an unforeseen negative effect.

"There is the possibility of creating the largest botnet in the world," says Yuval Ben-Itzhak of Finjan, a computer security company. This view is borne out by a recent report by F-Secure identifying Africa as one of the emerging cybercrime threats (tinyurl.com/ytdcf5).

Phenomenal take-up

"Within the past few years, internet take-up in emerging markets has been phenomenal," says Mikko Hypponen, chief research officer at F-Secure. "The trend is expected to continue and spread into areas such as Africa, India and central America. People are developing sophisticated computer skills. But," he adds, "they have limited opportunities to profit from them legally. There will be a delay before legal systems catch up with developments in the IT sector. Computer criminals may also be able to escape the law more easily in countries which are undergoing serious political and security problems."

The case of Onel de Guzman, the student who wrote the 2000 Love Bug virus and who escaped prosecution because

the Philippines, his home, had no offence with which to prosecute him, is a case in point. But Ivan Krstic, OLPC's director of security hardware, points to the choice of Linux as the operating system for the computers. "You cannot have one program loading from the internet that can then go to your [email] address book and then send out a spam message to everyone," Krstic explains. "The program can only work in its own area and has no functionality beyond that."

"For anything to be able to achieve that overall control, the attack would have to be written to the system kernel, and those are the hardest attacks to launch. Those vulnerabilities do exist, but they are patched very quickly. It would be difficult to get them to run bots." However, there is an option to run Windows XP on the machine – which means, concedes Krstic, "they can be attacked. All of the connotations of Windows security apply."

The Windows-based Intel Classmate also includes a nod at security. Countries buying it can opt for antivirus software, included for a higher price, but must negotiate that with AV companies themselves; and a hardware setting disables the laptop if it is not connected to an antivirus monitoring network for a certain period of time. This is to safeguard the machine from becoming part of a botnet, which can disable antivirus checking.

The bigger problem in the long term may be the developing world's choice of operating system. "Most of the machines we are shipping have Windows on them. That's the operating system most countries want," says Intel. It adds that teachers will receive training from Intel to monitor the network and will be able to see if changes have been made to the machines: "Some schools using the computers will have a teacher who is responsible for security on their networks, others will have an IT person." As a last resort the Classmate, like the OLPC XO, can be wiped clean and restored to its factory settings.

But while Windows has its problems, Linux may not offer much better protection, says Guillaume Lovet, a botnet expert for Fortinet. "The first botnets

were Stacheldraht, Trinoo and TFN, and were built in Linux," says Lovet. He also dismisses claims that the low bandwidth and internet use in parts of the developing world – the World Economic Forum's 2007 Africa Competitiveness Report estimated that African internet use was just 3.4% of the world total – would act as a brake on the development of botnets.

"It doesn't take any bandwidth to control or make a botnet," Lovet says. "Aggregated bandwidth is what is important, and that would still be massive. You could still build a huge cyber-weapon with only a thousand of these machines."

For the botnet herders – the people who

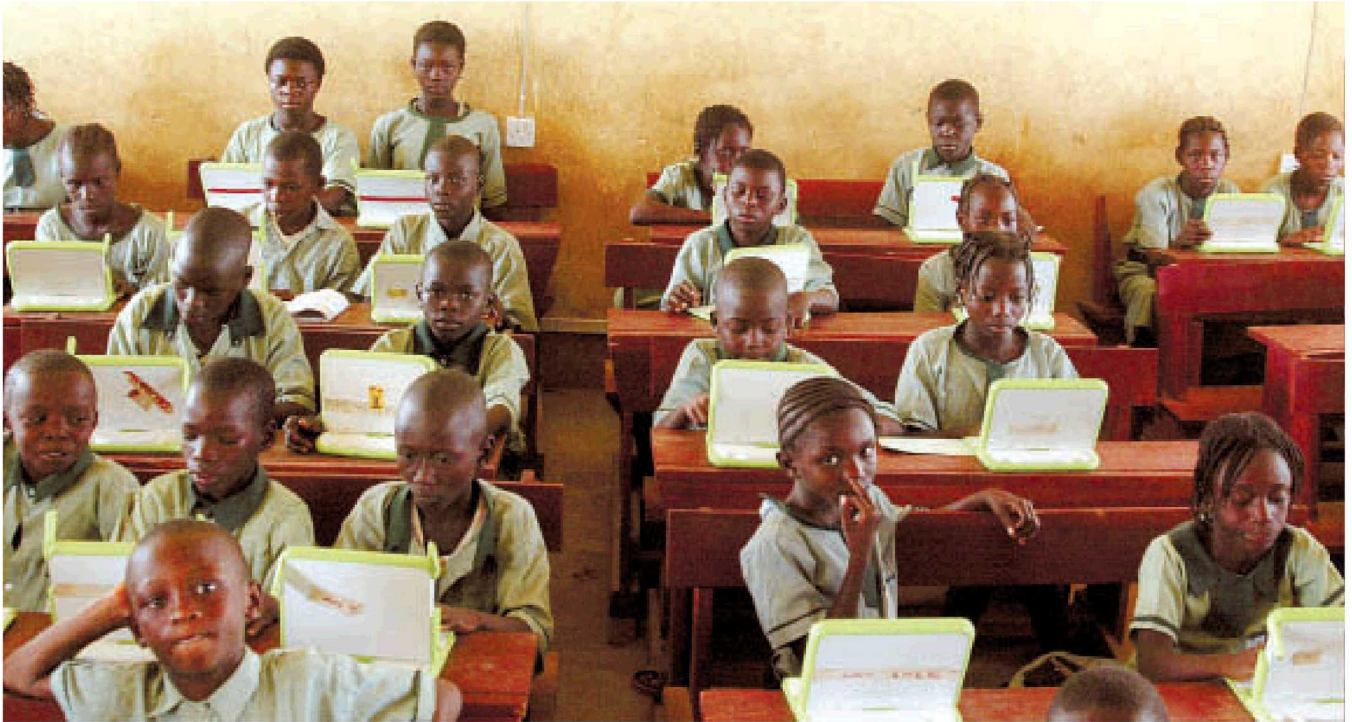
The rush for the developing market

The **OLPC XO** is a toughened, stripped-down laptop weighing 1.3kg that uses a 433Mhz AMD chip, 2GB flash drive and mesh Wi-Fi to create a local area network. The Linux-based OLPC, which is about to be tested by Microsoft for use with XP, can connect to the internet and has three USB ports.

Intel's Classmate is built with a 900Mhz Celeron M chip which can run Windows XP or Linux, uses Wi-Fi and has a 2GB Flash drive for the Windows variant and a 1GB Flash drive for the Linux version. The 1.4kg Classmate comes with two USB ports and costs between £115 and £150.

The **Asus Eee PC** range is less rugged. There are four 7in models weighing 920g and sporting an Intel Celeron processor. Their Flash drives range from 2GB to 8GB, with between 512MB and 1GB of Ram. They have three high-speed USB 2.0 ports and Wi-Fi. All run Linux and can run Windows XP, and cost around £200.

Acer, Gigabyte, Lenovo and Everex have all announced low-cost laptops that can compete in this area.



The OLPC could have the unwanted side effect of fuelling cybercrime in Africa, which experts highlight as an upcoming hotspot
 Photograph: Afolabi Sotunde/Reuters

create and control botnets – there would also be kudos in staking a claim in a new area. “We have seen botnets involved in landgrab exercises in the past,” says Greg Day, a security analyst for McAfee.

Just as alarming for Mark Sunner, chief technology officer of Messagelabs, which monitors email traffic on behalf of the government, is that the machines could be used as a recruiting ground for criminals.

Herd goats, or bots?

“You can imagine a whole swathe of internet boiler-rooms being created among people who can make more money from internet crime than herding goats,” says Sunner, who points to the fact that Africa already has the highly technologically literate Nigerian 419 group, one of the oldest cyber-crime organisations.

The latter are very dangerous, says a former head of the UK’s now disbanded West African Organised Crime Unit. “They are organised like a business. They are already building most of the bogus bank sites on the web. If you ship computers to Nigeria then a lot of them will inevitably make their way to 419. I mentioned this to someone who is still monitoring 419 and they said ‘you might as well shut down the internet and go back to pen and ink’.”

Sunner, meanwhile, notes the dangers that the machines represent to Africa’s own emerging internet infrastructure. “There are a lot of viruses already heading for Africa and China and the consequences of spam can be terrible if you do not have much bandwidth,” he says.

Both Intel and OLPC point out that the laptops will often only have intermittent

connectivity. That might lower the risk of getting infected – or the chances of getting security upgrades.

But the bleak picture may be avoidable, says Rolf Roessing, a security expert for KPMG. “If we are to bring IT to Africa then it will not work unless we bring security with it. Computer security in the west grew because of a loss of innocence and there are still weaknesses in the developed world because of a lack of awareness. If you bring IT to developing countries then you have to develop awareness, too.”