



THE BUSINESS TECHNOLOGY NEWS MAGAZINE FOR THE EMPOWERED ENTERPRISE

Search

GO

[Home](#)

[Previous Issues](#)

[Subscribe](#)

[Contact](#)

[About Us](#)

[Buyers Guide](#)

User name

Password

[Lost your password?](#)

LOGIN

## On The Cover

### The industry that cried wolf

Author: Brian Bakker

Issued: Thursday, May 18, 2006

*Is ransomware a reality? The IT industry has a history of spreading fear, uncertainty and doubt in order to sell more products. The anti-virus sector is particularly adept at using this technique. So when it warns of a chilling new threat in malware that infiltrates our data and holds it hostage, do we believe it?*

ANTI-VIRUS (AV) software is big business. According to Mark Walker, business development director (MEA) at IDC, the worldwide AV market sold wares worth more than \$3.6 billion in 2004, running at a compound annual growth rate over 30%. Interestingly, this sector still hosts a plethora of players, at least ten of which are represented in South Africa.

But apart from highlighting and helping to fix well-documented vulnerabilities in client operating platforms, why does it attract so much money? The suspicion has been that this is partly due to its usual tactic of spreading doom and gloom.

Jay Heiser, research VP at Gartner, says while he doesn't quite believe AV companies are pulling the wool over customers' eyes, they do always seem to be making things out to be worse than they are.

#### SHOCK AND HORROR

The latest warning to emanate from this industry has all the hallmarks of shock and horror. In a white paper published recently on its blog, AV firm Kaspersky Labs asserts that an evolution is under way in the field of malware. It says remote malicious users have moved away from the stealth use of infected computers (stealing data from them, using them as part of zombie networks etc) to direct blackmail, demanding payment from victims.

"Users quickly understand that something has happened to their data. They are then told that they should send [money] to an e-payment account. The ransom demanded varies significantly, depending on the amount of money available to the victim."

According to Jeremy Matthews, country manager of Panda Software in SA, this is consistent with its own findings in its Q106 report: "Crimeware is an undeniable reality. Malware authors are no longer looking for either personal or media fame. Their [focus] is ... on trying to obtain the maximum economic benefit," he says.

Kaspersky offers some evidence, saying that cyber crime last year used two Trojans: GpCode and Krotten. "The first encrypts user data; the second makes modifications to the victim machine's system registry, causing it to cease functioning."

According to Clifford Katz, CEO of Information Security Architects, it's important to put such information into context. "You have to understand what a security practitioner does. His job is to conceptualise a possible threat and bounce it off his peers as a concept. If the idea survives the peer-review process they may try to simulate it, and only if they can prove the concept do they classify it as practical."

Of course, the weakness in this system is that the practitioners' academic fiddling is monitored closely by malware writers. They voraciously consume any white papers that result from such research. Even so, many of these concepts are so complex they never make it out of the lab and "into the wild", as they say in the industry.

Marius van Oers, a research scientist in McAfee's laboratories, confirms this but says some instances of extortionate malware have been noted. "Today we have about 190 000 entries for



Clifford Katz, MD, Information Security Architects

malware and this is increasing on average by 200 new entries a day. Of those, less than five can be described as extortionate."

On the likelihood of this number increasing in the future, van Oers says: "I'm not a fortune teller. It may go higher, it may not, but for the moment [I can say] it's not a commonly used technique."

However, as theoretically possible as a proliferation of such malware is, Heiser identifies a practical problem with the concept. "My understanding is that the money is easier to track than an attacker is. Getting away with a scheme like this would require circumvention of the controls of the global financial system."

### **LINUX COMES UNDER FIRE**

Another trend identified by Kaspersky, citing "an almost 100% increase" on last year's figures, shows that virus writers are almost falling over themselves in targeting systems running Linux. The figures supplied are 422 (2004) and 863 (2005).

McAfee's van Oers puts this into context: "Linux viruses first emerged in any numbers around 1999, and then people said we should see a big increase, but we're now in 2006 and the total is only 800-900. Sure there is a steady increase, but compared to absolute numbers in the Windows environment ... it's insignificant."

Gartner's Heiser believes this is purely a function of PC populations (and, by logical extension, a matter of time). "It's a function of the connected population and of recognition by the attacker community. And there's a certain level of copycat[ting]. Once one sees that something is feasible, everybody starts. You often see that with whole new classes of Windows vulnerabilities."

Katz agrees. He foresees a time when the number of Linux and Mac viruses could be comparable to those found in Windows. Riaan van Niekerk, systems architect at Obsidian, scoffs at the assertion. "Linux is much more resistant architecturally to malware. This is because of the security model, the separation of privileges. You have a root user (equivalent to the administrator on Windows) and everybody else has only limited access to the system," he says.

The result, he adds, is that even if a user does encounter a Linux virus, the malware will only be able to infect the parts of the system that the user actually has access to; his home directory. Van Niekerk notes that this also holds for the Apple Mac, because it, too, has its origins in Unix.

However, there is another dark cloud looming on the horizon of Linux security. "Standardisation might simplify things for application developers, but will also do so for malware writers. But Linux does have a defence unavailable to Windows: the fact that it is open source. If somebody compromises a system library somewhere it will be picked up very quickly by any one of the hundreds of thousands of guys looking through the source code for possible errors," explains van Niekerk.

So it seems that regardless of platform, the threat is real, although some threats are perhaps more real than others. According to Heiser, "these problems are not going to go away; if anything, they're going to intensify".

[⏪ ⏪](#) Back