



Kaspersky Lab provides protection against viruses, spam and hackers

Phone malware on the rise

Kaspersky Lab is an international software company that offers advanced Secure Content Management solutions, both to home users and to large network environments for protection against viruses, spyware, spam and hackers.

In 2006 some 500,000 new viruses were detected. That number is about the same as that of all viruses that were ever encountered over the past twenty years. In 2007 the total number of viruses once again almost doubled up to a million. 2008 was a real record breaker when it comes to virus infections. Some two million detections, and that only within the first six months of the year. Hotspot considered these frightening numbers to be a good reason to meet Eddy Willems Security Evangelist by Kaspersky Lab. Not only about these Internet threats themselves. But also about the opportunities they may bring the retail branch.

In August 2008 Kaspersky Lab developed two new anti-virus programs, Kaspersky Internet Security and Kaspersky Mobile Security. But before going into the details, we asked Eddy Willems how we should perceive his title as 'IT Security Evangelist'.

"I belong to a group of analysts who took up the role to explain - in comprehensive language - what is going on in the field of computer security. This information is meant both for the corporate world and for the media. It is important to provide clarity for instance about the protection of notebooks, pda's and business networks. The corporate information I provide is often more technical, because it is aimed at people with technical backgrounds."

Kaspersky Lab is a company that is still relatively unfamiliar to the general public, as a provider of anti-virus and security solutions. Will that change?

"Kaspersky is a company that is on the move. Globally, we are a 'top 5 player'. In many countries we are even third place on the consumer market. In the business market Kaspersky Lab is doing particularly well, with a global ranking between 4 and 5. Obviously there is a reason that fourteen of the twenty-seven ICT companies on the NASDAQ choose Kaspersky as the engine for their security."

What is Kaspersky's added value?

"Kaspersky has a clear focus on security. You often see our competitors come out with a whole range of products. These all-in-one products often have just that as a disadvantage. You can compare it to buying a new stereo system. A sound system with separate components sounds a lot better than an all-in-one piece of equipment."

The number of known viruses is growing rapidly. Does this affect the way your technology detects and eliminates them?

"In order to keep viruses outside computer systems, we make use of new technology in the Kaspersky Anti-Virus 2009-suite. Of course our regular virus scanner is still there as well, because that is the trusted technology. Currently we make use of four types of technology: 1 = signature, 2 = behaviour blocking two, 3 = Heuristics and 4 = desktop firewall."

Heuristics?

"Heuristics is special procedure to detect new and unknown viruses, without depending on virus signatures. Through analysis we look at potentially dangerous files. Heuristics also works in a similar way as a scanner, but it is much more versatile and more intelligent as well."

And what does behaviour blocking contain?

"The technology looks at the behaviour of programs. It compares that behaviour to the behaviour it is supposed to have. Behaviour blocking can for example prevent a hard drive from being formatted."

The fourth technology you mentioned; desktop firewall, isn't that often standard software that comes with any new computer?

"True, when you buy a new computer or a notebook, it comes with firewall protection, but that is very basic software, that does not respond to all attacks that are currently out there. In many cases it only looks at attacks from the outside and not at 'internal attacks' for example when your computer spontaneously starts sending e-mails."

Let's go back to viruses for a moment. You would think everyone has anti-virus software installed on his PC, both consumers and entrepreneurs.

"You would be surprised. Some 20 percent of households and entrepreneurs have no interest in any form of protection. Yes, when you buy a new computer it mostly comes with anti-virus software but that application runs out within 6 to 12 months. Many people fail to renew their subscription. When you look at all computers you can say that 25 percent of them are really secure. This means that 75 percent of all computers is not protected against malware or other threats."

So finally, can you give me an example of a risk you run when you don't protect your pc.

"Botnets are a mean danger. Your unprotected computer can become part of a botnet. In a botnet, the attacker uses someone else's computer, for example, to send out spam. The problem ➔

Kaspersky's 'IT-Security evangelist', Eddy Willems:

"New threats and new solutions as virus battle grounds broaden substantially"



of botnets can be excessive. There are botnets that use, or rather misuse a 100.000 to 500.000 computers for sending spam. That is why it's often useless to shut down websites from which spam was sent."

Couldn't you develop a 'virtual door' to the computer to put a halt to all viruses entering your system?

"Pre-warning and detection of viruses is called intrusion prevention. Intrusion prevention prevents an attack from the outside and blocks it before it enters the PC. This technology requires a very different approach from just detecting an attack. But that is a very technical story."

Can you give me an example of a virus that we really ought to worry about right now?

"A nasty example of a current virus is Gpcode.ak. It encrypts files with extensions such as .doc., .pdf., .xls., .jpg by using an RSA encryption algorithm with a 1024-bit key. After Gpcode.ak has encrypted those files on the victims computer, it changes the extension of this files to . _CRYPT and places a text file called '! _READ_ME!.Txt' in the same folder. In that text file, the cyber criminal explains to his victims that his files are now encrypted and they can buy a so called decryptor to get their files back. Then the virus removes itself, which makes it really hard for specialists to research it."

Nice guys!

"It took the author of Gpcode two years to improve his virus. Previous errors were corrected and the key was extended to 1024-bits instead of 660-bits. Up to now virus researchers have only been able to dismantle keys up to 660-bit. This was the result of detailed analysis of the RSA algorithm implementation. It would cost 1 PC with 2.2 GHz, 30 years to crack a 660-bit key, and only when the algorithm is executed flawlessly."

So what does it take to decrypt a 1024-bit key?

"The cracking is a very complicated cryptographic problem. In order to crack such a key you need at least fifteen million pc's to run for a full year."

What should someone do when his system gets infected with a virus?

"In case of infection we advise victims to contact Kaspersky. It's important to start using a different computer right away but also not to turn off the infected computer, nor to reboot it."

Are new generation smart phones with operating systems like Windows Mobile also vulnerable to the sort of threats that you mentioned?

"There are currently 500 threats for mobile phones. Compared to the overall number of malware it is negligible. Right now ☺"

we have one million active forms of malware. This number is growing rapidly every day."

Is there much similarity between the threats against PC's and against smart phones?

"The number of different forms of mobile phone malware now, is comparable with PC malware in the times of the rise of the personal computer in 1991, 1992. At that time there was around 500 forms of PC malware in circulation. And then all of a sudden an exponential growth in the number of PC threats occurred. The expectation is that the same will happen with mobile phone malware. Especially with the rapid emergence of smart phones and Windows Mobile operating systems, that are very similar to desktop operating systems."

So Kaspersky is ready to provide protection for phone malware?

To serve as a product specialist, it's very important to have a product for identifying malware for mobile phones. Of course there must be a relevance for it. The fact is that malware for mobile phones will probably evolve faster than was the case in the PC-market, because it is moving and growing to a size ultimately greater than that of the PC market." □



Kaspersky Lab to harmonise European Partner Program

THE "GREEN TEAM" PARTNER PROGRAM OFFERS COMPELLING BENEFITS FOR ALL PARTNERS

Following the restructuring of its European business into regional divisions, Kaspersky Lab has harmonized its European Partner Program. With the "Green Team" Partner Program, Kaspersky Lab offers partners an opportunity to grow sales revenue and profitability in Europe. The program is seen as a further step in strengthening the relationships with channel partners.

100% INDIRECT SALES MODEL

Kaspersky Lab is committed to a 100% indirect sales model and sells products exclusively via partners and resellers providing substantial support for their sales activities. This ranges from technical training and support to marketing material and lead generation. The new channel program offers partners the opportunity to join at one of four levels. These are "Accredited Reseller", "Certified Partner", "Enterprise Partner" and "Retail Partner". Each tier has its own level of commitment and benefits and is designed to accommodate partners of all sizes and skill sets.

ATTRACTIVE INCENTIVES

"The "Green Team" consolidates the best of our regional partner programs into a single European framework," says Frans Plantaz, Marketing Manager at Kaspersky

Lab Benelux. "Regardless of size, the program will make it easier for partners to generate revenue with Kaspersky Lab and consequently to grow their business." The program offers partners attractive financial incentives, extensive sales, marketing and technical support and lead generation. Furthermore it includes a complete technical training and certification course and an exclusive partner website.

HARMONIZED EUROPEAN PRICE LIST

Along with the harmonized Partner Program, Kaspersky Lab is also introducing a harmonized European price list designed to ensure consistency for multinational partners and customers based in the region. It offers clarity and consistency on the discounts available for volume license purchases and on the special terms available for vertical markets such as the public sector and education. New channel program "We've met with and listened to channel partners around Europe about what we can do to enhance our commitment to partnership and innovation," said Dick Gehéniau, Managing Director of Kaspersky Lab Benelux. "This resulted in a new channel program that will help our partners compete more effectively while helping their customers increase their level of security." □