

cyclops

Security information for users
of Vet Anti-Virus software

autumn 05

exit X

print 

contents

- 2 Security Bytes
- 3 **Healthcheck** – MyDoom.AY
- 4 **Meet** Jakub Kaminski
- 5 Fraud schemes target banking websites
- 6 **Top 10** viruses
- 7 **Firewalls** burn up dangerous data
- 8 Vet FAQs

In this issue

Welcome to the Autumn edition of Cyclops. This quarter we look at firewalls, the Top 10 viruses and meet Jakub Kaminski, a technology veteran of 30 years who coordinates anti-virus research at CA.

Did you know a new cyber threat has emerged that can turn your computer into a device for sending spam email? How secure is your computer? Read on to learn about online fraud schemes that target people who are using

banking websites. Also, in response to reader requests from last issue, we answer some commonly asked questions about Vet software.

This issue of Cyclops is packed with security tips that I hope you find useful.

Happy reading and safe computing,

Michelle Micallef
Marketing Manager
eTrust

Cyclops is a quarterly publication of
Computer Associates Pty Ltd
ABN 20 001 146 345

Level 2, Bldg 10, 658 Church St, Richmond Vic 3121.

Email: feedback@vet.com.au Website: www.vet.com.au



Computer Associates™

Security bytes

1

Spammers avoid blacklists

Spam emailers have a new trick for increasing the volume of spam on the internet. Using the latest technology to disguise their email addresses, they're managing to avoid many of the blacklists used to filter spam mail-outs. The new technology works by changing a spam email to look as if it has been sent from the computer user's internet service provider.



Spam can be deceptive.

2

3

4

5

6

7

8

Virus writers to target mobile devices

Deloitte Touche Tohmatsu predicts that virus writers will focus more on mobile phones and portable internet technology in 2005. In a recent report it claimed that increasing use of wireless devices will result in even more complex viruses. The report says SPIM, the equivalent of spam email for mobile phones, is also set to rise.

Online bank fraud

UK Police have arrested a 21-year-old man from England on suspicion of committing online fraud. It's believed he swindled money from online bank customers using fraudulent email send-outs, a crime commonly known as phishing. While the man has been released on bail, a team of data forensic specialists is now investigating computer equipment found at his home for evidence.



Online bank fraud is increasing.

Virus healthcheck: MyDoom.AY

1

A new version of the MyDoom worm has the ability to turn your computer into a spamming device. MyDoom.AY is able to install 'backdoor' programs on your hard-drive, which hackers can use to send large amounts of spam email from your computer. This type of cyber attack is known as a spam relay.

2

3

4

5

6

7

8

Spread by email, MyDoom.AY is activated every time a computer user loads their Windows operating system. To locate target email addresses for spam relays, it scours the hard drives located on your computer and information stored on search

engines such as Lycos, Google and Alta Vista.

Attacks from MyDoom.AY normally imitate a message from your mail-domain provider that will try to convince you to open an attachment file, which infects your computer. To protect yourself, be wary of unfamiliar messages and avoid opening attachments without first turning on and updating your anti-virus software. If infected, seek help at CA's security advisor website by [clicking here](#).



Update anti-virus software before opening attachments.

Meet Jakub Kaminski

A keen contributor to e-security publications, Anti-Virus Research Manager, Jakub Kaminski, is passionate about understanding computer viruses.

1

2

3

4

5

6

7

8

Polish-born Jakub Kaminski moved to Australia in 1992. He now co-ordinates research at CA's anti-virus laboratory in Melbourne and has battled with computer viruses for more than 12 years as a researcher. A systems programming whiz with 30 years experience, Jakub relishes the daily challenge of containing new threats.

Jakub has a masters degree in electronics from Warsaw Technical University and rates Sobig.F, a worm spread to millions of PCs by email and file-sharing networks as the

most serious menace in his time at CA.

"Sobig was a real headache for computer users and administrators alike. The hardest thing to learn about a virus is where it's from and its purpose. Getting virus code to work under laboratory conditions is also difficult," he adds.

When not busy solving the latest cyber threat or managing researchers, Jakub enjoys reading and going bushwalking.



"... Getting virus code to work under laboratory conditions can be difficult."

Fraud schemes target banking websites

Cyber criminals continue to use elaborate phishing schemes to trick computer users into giving out important financial information before stealing their hard-earned savings. Hijacking well-known bank brands, the criminals send hoax emails that ask you to confirm banking usernames and passwords at bogus websites. And once this information is entered, they have everything needed to clean out your bank account.

The fake websites look and act exactly like those of the banks they're copying, so remember that the banks themselves will never ask for your personal information by email.

More sophisticated phishing attacks use viruses and trojans to install key logger computer programs that capture everything you type, sending your financial details out to cyber criminals. A mix of anti-virus, firewall and anti-spyware software is the best protection against these threats.



Banks will never ask for your personal information by email.

Tips to avoid a phishing attack:

- never click on links in strange emails
- be careful of urgent requests for personal information
- always enter the correct web address from your browser
- keep a regular check on your finances to spot attacks early
- update your web browser frequently with the latest security fix.

If attacked, seek help at CA's **security advisor** website and quickly change your online passwords. Immediately report stolen card numbers and close all affected accounts, keeping a record of conversations and correspondence in case your actions are later questioned.

1

2

3

4

5

6

7

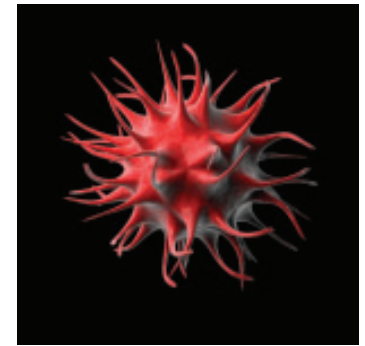
8

Top 10 viruses

reported to CA's Anti-Virus Research Team

These are the 10 most frequently reported viruses for the week commencing March 2005. You can find the latest list of the most active viruses by [clicking here](#).

1. Win32.Netsky.P – worm spread via email and file sharing
2. Win32.Lovgate.AB – worm spread via email, network shares and Kazaa
3. Win32.Netsky.D – worm spread via email
4. Win32.Lovgate.AO – worm with backdoor functionality spread via e-mail, network shares and file sharing
5. Win32.Netsky.Z - worm spread via email
6. Win32.Mydoom.O – worm spread via email with backdoor functionality
7. Win32.Mydoom.AU - worm spread via email
8. Win32.Netsky.C - worm spread via email and peer-to-peer networks
9. Win32.Sober.K – worm spread by email
10. Win32.Mydoom.BA - worm spread via email



Computer viruses come in many shapes and sizes.

1

2

3

4

5

6

7

8

cyclops

exit X

print □

Firewalls burn up dangerous data

1

There's no one-size-fits-all solution for handling all of the threats lurking in cyberspace. For staying truly safe, you need to take a holistic approach using a mix of software protection.

2

3

A firewall is the electronic equivalent of having a security guard camped outside your front door to control who enters or leaves. Filtering online data it identifies and rejects unwanted traffic including spam email. Yet it's much more than a simple spam filter. Without a good firewall, skilled hackers can use your internet connection to take control of your computer.

4

5

6

7

8



A firewall's job is to:

- filter and reduce spam email
- protect you from backdoor attacks that are made possible using trojans
- examine packets of data before they enter your computer system, weeding out the threats
- prevent hackers from controlling your computer to steal data, read personal files or run programs.

If you're not sure whether your firewall is adequate for your needs, use a vulnerability assessment tool such as a port scanner to run some tests. Remember to regularly download the latest security updates and renew your firewall subscription annually.

Use a mix of software for maximum protection.

Security research organisation, the SANS Institute, claims a typical unprotected PC will be attacked within 20 minutes of being connected to the internet!

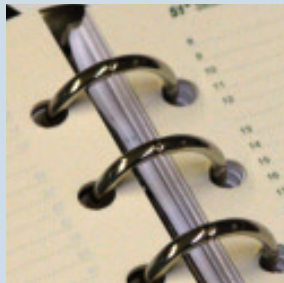
Protect your PC and network using CA's eTrust Firewall 2005. It provides complete industrial-strength hacker and privacy protection and protects your PC from both known and unknown cyber threats. Its easy-to-use interface and pre-loaded settings take the guesswork out of managing security. **Click here** to learn more about eTrust Firewall 2005.



Frequently asked questions (FAQs)

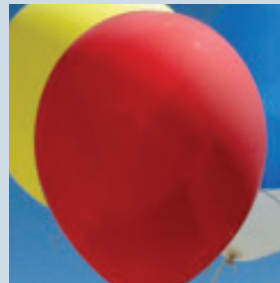
How do I schedule a Vet scan?

Firstly, you should ensure you have installed the latest version of Vet. To schedule Vet scanner, click on the Vet icon located on the system tray, next to the time display, then select Option/Program/Scheduled Scan. From here, you can schedule Vet to scan at any time or date.



Why do Vet updates gradually increase in size?

Vet virus signature files store all previous virus patches. As new updates are added, the file size increases. New updates protect you against the latest viruses and previous updates against earlier strains that may still be active.



When I start my computer, Vet displays the out-of-date warning message, even though I'm using the latest release?

Always ensure you've properly installed the latest Vet release from our website at Vet/Help and About. Vet determines when to display the out-of-date error message by monitoring your system date. Double click the time display located in the bottom right corner of your screen to correct the date.



To view more FAQs, [click here](#)

Reader feedback

Does Cyclops provide relevant information for your security needs? Are there other topics you'd like to see covered in future editions? Please [click here](#) to email us your feedback on Cyclops.

1

2

3

4

5

6

7

8