

06 MAY

NEWS

ISSN 1377-0675
VOLUME 13 ISSUE 1

European Institute for
Computer Anti Virus
Research (eicar) e.V. Office
Rosenheimer Landstr. 41
D-85521 Ottobrunn

GERMANY

Editor: Eddy Willems
press at eicar dot org

CONSULTING EDITOR:

Rainer Fahs

CONTRIBUTORS:

Sarah Gordon,
Vlasti Broucek,
Frank Schnell, etc...

EDITORIAL ADDRESS:

Ter Borchstraat 17
B-1982 Elewijt (Zemst)
Belgium

- 1 From the Board –
Chairman's Corner
- 2 Editorial: 2006 And Beyond
... What Will Come?
- 3 Reports from the EICAR Taskforces
and Working Groups
- 4 EICAR Virus Prevalence Table
February 2006
- 5 User Education Letter from
David Perry (Trend Micro)
- 6 14th EICAR 2005 Conference:
Pictures and Comments
- 7 15th EICAR 2006 Hamburg:
The Programme

FROM THE BOARD CHAIRMAN'S CORNER

(By Rainer Fahs (RFA))

Diversity<>Assimilation?

EICAR is a truly international organisation with membership from all around the globe. The Board is an assembly of six representatives from four different nations and we are geographically situated in three different continents – Europe, North America and Australia. The annual conference is planned and managed with an international team from “down under”, while business development and administration resides in Germany. This situation bears some inherent challenges in terms of inter relationship and communication.

The diversity not only of Board members, AR, be it in the area of conference but also of key contributors within EIC preparation or paper review and selection, the management of the organisation as such or the outside representation via our web-page, requires a great deal of respect and consideration for the others. All these individuals with their specific backgrounds and expertise, with their own way of doing things, their interpretation, perception and way of communication deserve the full respect of the others.

Whenever we speak about diversity, we speak about gender, race, ethnic origin, nationality, age, religion, as well as background, education and behaviour. What we really speak about is the distinctions that make people different from each other. Everybody seems to agree that people are different and we hear people saying that we should embrace these differences because these differences are what really make us individuals.

The real issue than is the integration of single individuals into teams. How to esteem diversity without trying to assimilate, make them like us?

Diversity is foremost all about accepting that it concerns each and every one of us recognising that we are different to some and similar to others, meaning we are part of the mix.

It is a definitely challenge requiring quite a bit of sensibility to achieve common goals in an environ-

ment of great diversity. It is however very rewarding to be part of a team that despite of diversity works together towards a common goal.

Once we have agreed on common objectives we have to find the best way to convert objectives into individual goals and assign tasks and responsibilities in accordance to the expertise of each contributing individual. And here we are again, there are individuals, meaning we still have diversity. In consequence we (every one in the team) have to recognise the expertise of the others. This is inherently difficult since every individual knows what he/she is capable of, but that is an intangible asset that is not measurable. What we are calibrated for is our achievements, which are visibly.

I think for the last couple of years, we have managed pretty well. We where able to take new key players on board and we succeeded to integrate them into the complicated processes. This in return resulted in the exploitation of fresh expertise, which in return has changed the scope and objectives of EICAR as an organisation.

Still concentrating on our core business, we have managed to gain also considerable reputation in the area of security management. However, the visibility of related activities is associated with our very active task forces on RFID, Wireless LAN and Content Security, which are concentrated mainly in Germany. One of the reasons to get the EICAR conference back to Germany was to provide members of these active TF/WGs also a platform to represent their activities to a wider audience.

Recognising somewhat the consequences of that, I was very happy that we could get a PR professional on board who took on the responsibility of business development for EICAR.

Dealing with PR in a professional way was quite an experience for most of us over the past year, but if we

look back now, we can only conclude that it was worth going this maybe occasionally thorny path. Based on a number of activities and a great deal of networking, we have succeeded in promoting EICAR and its activities to a much wider audience than only the core AV researchers.

EICAR has gained a reputation, which again has become an obligation for us. At our conference this year we are bridging for the first time technically high quality and academic presentations to presentations of interest for the management level responsible for the implementation of security policy and mechanism.

This is an opportunity for every one of us. The high standard of our conference is what gets experts from around the world to submit papers or sign up to participate. If we want to keep that high standard, we must continue to work as one team, respectful recognising diversity, but striving for common goals.

FROM THE DESK OF SCIENTIFIC DIRECTOR AND PROGRAM CHAIR

(Vlasti Broucek)

The EICAR 2006 call for papers have been published at the end of August 2005 and we have called for submissions in three categories – non-peer reviewed research papers (also called industry), peer reviewed papers (also called academic) and posters. Based on the submissions, well appointed program committee decided to accept 18 non-peer reviewed papers and after double/triple blind review of academic papers accepted 12 peer reviewed papers. Out of these twelve papers, seven were also offered journal publication. During the selection process, approximately about one third of submissions were rejected as either not suitable for the EICAR conference or for not being of sufficient research standard. Unfortunately, we have seen a significant drop in number of to 2005. On the other hand, the papers submitted by both academics and non-academics had generally higher standard than in 2005 and rejection rate was lower.

Unfortunately, only two posters have been submitted. One of them has been deemed not suitable for the conference and as a result poster session has been

cancelled. It suggests that there is not enough interest in this way of presenting in our field of expertise. The high quality and wide scope of the papers yet again confirm growing quality of the EICAR conference and broadening of it scope. While the majority of papers can still be classified as AV related, nearly all of them can also be classified in other categories such as Critical Infrastructure Protection, Legal, Privacy and Social Issues of ICT Security, ICT Security and Policy Management etc.

The program for the conference is nearly ready to be published. The selected papers have been grouped according to the topic and will be presented in these groups. Academic (peer reviewed) papers will be presented first in each relevant group followed by non-peer reviewed papers.

It also appears that the once successful Graduate Workshop is not attracting an adequate number of students. While there is still time to enrol, hitherto the program committee did not receive a single submission.

The program of the Professional Workshop also suffers fall off interest from speakers this year, but there has been interesting developments in the last few days. I can now confirm that we will have a very interesting session on „Security and Privacy Risks in Biometric Deployments“ by Elizabeth Bates and Dr Bill Hafner from USA. This should also help to form proposed TF on Biometrics proposed by Elizabeth and Bill. This should cover the Sunday morning session and another possible session, most probably on Network Traffic Visualisation, is currently being discussed with possible presenters.

TF AND WG REPORTS

(Manuel Hüttl)



RFID Task Force

The RFID Task Force has been very successful over the past two years. We saw an interest of different markets and the number of participants is still growing. The industry attends with leading companies like Microsoft, SUN Microsystems, SAP, Intel – not just typically IT-Security vendors. Officials like the Federal Data Protection Commissioner from Germany joined as well as huge retail organisations like Metro AG. We also welcomed standardisation specialists like GS1 (EPCGlobal).

So there is a nice mixture of different interest groups – an era sometimes not easy to handle by the way. We defined a first target: *to provide a guideline for organisations that do want to implement the RFID technology and we focused on data protection and related privacy issues. So for example, a company could use this guideline as an appendix for project contracts.*

The next step is related to the issue of person-related data connected to the communication between a RFID tag and reader. We are facing classical IT-Security issues here to protect this critical information – from access control to storage.

We are already working on a guideline that covers those IT-Security issues in RFID-scenarios from the perspective of technology, organisation, legislation and psychology.

One of our next goals is to extend the activities to a pan-European level. Because of the complicated legislation issues, we were starting in Germany.

Task Force „Content Security“

We are very pleased to announce that we finally have a new TF in place. After talking to industry and other experts, we noticed a growing demand for this platform. We can also happily report that we succeeded in winning Prof. Peter Bienert, a well known professional in IT security and project management as chairman for this TF. The first meeting concentrated on the question: *What is Content Security all about?* After intensive discussions, we defined three major pillars, on which Content Security is based:

1. *Data Protection and Integrity*
2. *Protection against unwanted data*
3. *Layer 7 (application level) issues*

We have been very content with the participation so far and could welcome companies that do cover the areas of audit and validation, phishing and spam, malware and access control. We had participation from Israel, Benelux and UK and can really say, that this will become an intentional TF. Among others, participants are: Finjan, Phoenix Technologies, CA, Aventail, Secure Computing, 3Com, SurfControl, Cross-beam systems and F-Secure.

Once again, the first step will be the development of a guideline identifying the methods of attack and describing common defence mechanism, which will help business and private user to better understand the issues of Content Security and the appropriate defence mechanism.

NEW Task Forces

Awareness and Education

Issues that have a tremendous complexity and after our initial ideas during the conference 2005 in Malta, we have been in contact with other experts around the world. To somehow order the complexity and to establish goals and objectives for a Task Force is what we would like to achieve.

Dr. Johannes Wiele, a German Journalist, who is currently writing a book about awareness and education and Manuel Hüttel, who has published a book on the interrelationship between reputation and success, will chair the new TF.

Members and other interested experts are invited to join us at the inaugural meeting on 3rd May in Hamburg.

Biometrics

It might be that for the first time EICAR will established yet another Task Force and for the first time, this one will have its home in the US instead of Europe. Dr William Haffner and Elisabeth Bates had the idea to set up a TF to look further into the problems around biometrics.

Both will be at the conference in Hamburg and we will be able to discuss goals, objectives and operating procedures there.

2006 AND BEYOND... WHAT WILL COME?

By Eddy Willems, EICAR Director Press and Information

Spyware and adware

Spyware looks set to rise in 2006 and we see hackers now using zombies to install adware and potentially unwanted software across the network. While adware is not necessarily always illegal, the legal status is being subverted and exploited to create revenue streams. As the threat from spyware and adware continues to grow, 2006 and beyond is likely to see businesses looking for integrated, centrally controllable solutions rather than home user software.

No end in sight for spam

In the beginning of 2004, Bill Gates predicted that spam would be "a thing of the past" within two years. However we believe that the rumors of spam's death have been greatly exaggerated. The threat remains alive and kicking despite the increased action against spammers and constantly improving anti-spam software.

Host Intrusion Prevention Systems (HIPS)

HIPS covers a wide array of security approaches including behavioural containment and application inspection along with traditional approaches such as virus protection and a personal firewall. We believe that customers should consider carefully what mix of protection they need to defend their enterprises. HIPS is definitely the next generation Anti-Virus and Anti-Malware.

Mobile viruses and mobile devices

More and more organizations will promote and support remote working – whether at home or on the road – and this effectively extends the corporate network to an environment beyond the control of the IT manager. According to IDC, 69 million workers will be mobile by 2009 across Europe. As we begin to see more trains and planes being furnished with Wi-Fi, the risks for businesses also increases. Hence controlling the flow of traffic to and from the internet is more important in order to secure the workstation and therefore the business network. A VPN does not

secure the computer from the internet, so once the laptop is exposed, the VPN is also exposed. Securing mobile devices will certainly become a higher priority as they become an omnipresent part of the workplace. Theft or misplacement of such devices will inevitably increase, thus we may see increased adoption of biometric or fingerprint-type security to protect them. With more and more businesses rolling out Blackberry solutions or something similar, it is more important than ever to filter the increasing amount of spam from the corporate inbox, as any spam that reaches the inbox will also reach the mobile users – rendering the devices almost useless if the spam is not controlled. The other issue that mobile devices present is securing devices being brought into the organization, bypassing the firewall. The challenges of authenticating and securely managing these devices will prove difficult. The rise and increase of mobile viruses however will become a much larger problem; maybe then we can imagine ...

Microsoft

Microsoft's venture into producing anti-virus software for consumers is likely to be a thorn in the side of those security vendors who protect home users. Microsoft will, however, face considerable challenges in presenting itself as a credible security vendor for enterprises. Furthermore, it is likely that a large number of future viruses will be designed to specifically subvert Microsoft's anti-virus product, just as their anti-spyware and firewall products have been targeted.

Malware authors

Virus writers will continue to use more methods to make money from their malware – whether it be stealing confidential information, using exploited computers as spam factories or for DDoS attacks, or planting adware on infected PCs. Increasingly, we expect to see fewer traditional email worms making an impact, and an increase in the use of Trojan horses in targeted attacks against specific victims.

Vulnerability exploitation

Although Microsoft will continue to have its vulnerabilities exploited by malware authors, we will see an increase in attacks taking advantage of security holes in other products (for instance, desktop tools, alternative web browsers, email gateway software, etc) which are widely used.

Zombies

As more and more home users switch to Windows XP SP2 and benefit from its improved security (basic firewall, automatic downloading of security patches), hackers will no longer be able to rely solely on internet worms blasting their way onto computers to compromise them. Instead, they will use social engineering to enter the computer and turn off the protection from within, allowing a zombie component to be downloaded.

ADVICE FOR USERS TO AVOID BEING AFFECTED BY MALWARE IN 2006

For companies and corporations:

• Deploy HTTP scanning methods.

Many modern threats utilize the Web protocol to spread. It is highly recommended to implement a Web virus scanning system, much in the same way that administrators started deploying email scanning long ago. Detecting and stopping threats before any infected file can reach the end user adds a new layer of protection in the corporate network infrastructure. Spyware protection in the network layer is a bonus because these threats use HTTP exclusively to enter the corporate environment.

• Block unnecessary protocols from entering the corporate network

The most dangerous of them are IM P2P communication protocols and IRC (chat). These two are part of the bot arsenal of weapons to propagate and communicate with their botmaster and should be disallowed in the corporate firewall.

• Deploy vulnerability scanning software

and Host Intrusion Protection Systems in the network.

Being constantly up-to-date can minimize the impact of any new network vulnerability and diminish the risk of being infected by this kind of worm. HIPS covers a wide array of security approaches including behavioral containment and application inspection along with traditional approaches such as virus protection and a personal firewall.

• Do not give administrator privileges to all users

The most dangerous of all privileges is "load and unload device drivers". This is the most recommended measure to prevent being affected by rootkits. Usually rootkits are implemented as device drivers, in order to have access to all operating systems internals. Redesigning the user policy to limit users in this fashion can be one of the most useful ways to secure a network. If the administrator deprives users of admin rights, there is an added bonus: aggressive malware would not be able to kill antivirus processes in the system.

• Deploy corporate anti-spyware scanning.

As they are becoming prevalent threats for corporate businesses, the administrators need to deploy specific software to detect and stop them.

• Educate users; enforce a strict security policy within the network.

Not only do software and defence systems help fight against malware. Most of the time, the user needs to take some kind of action to infect the machine. Be it a Web page that installs spyware or an infected email, the user needs to know in advance the ways new malware attack users. User awareness is the key to a clean network, and administrators should conduct ongoing education initiatives to keep users informed and protected with updated malware technology. This is especially important with newer users, as they are the ones malware writers typically target.

For home users:

1. Beware of pages that require software installation. Do not allow new software installation from your browser unless you absolutely trust both the Web page and the provider of the software.
2. Scan with an updated antivirus and anti spyware software any program downloaded through the Internet. This includes any downloads from P2P networks, through the Web and any FTP server regardless of the source.
3. Beware of unexpected strange-looking emails, regardless of their sender. Never open attachments or click on links contained in these email messages.
4. Enable the "Automatic Update" feature in your Windows operating system and apply new updates as soon as they are available.
5. Always have an antivirus real-time scan service. Monitor regularly that it is being updated and that the service is running.

VIRUS PREVALENCE TABLE

TOP 10

FEBRUARY 2006 VERSION

1. W32/Netsky
2. W32/Sober
3. W32/Mytob
4. W32/Bagle
5. W32/Mydoom
6. W32/Sdbot
7. W32/Lovgate
8. W32/Funlove
9. W32/Brebipot
10. W32/Mywife

- Virus Families -

(By Eddy Willems, EICAR WildList Reporter)

QUESTIONS & ANSWERS



eicar

Within this new column you can get answers from the specialists themselves. If you have some questions or some problems related to Anti-Virus or Security please send them to

newsletter@eicar.org

and we will try to give your questions to the most respected specialists in the Anti-Virus and Security world.

No questions received this time.

(By Eddy Willems, EICAR News Editor)

WHAT MEMBERS COULD DO!

We ask you to send your statistics or incidents to us. Also, if you are looking at a new undetected specimen or if you have some problems with a document, spreadsheet or executable which could be infected, please send us this in a zipped file to the address `vsample@wavci.com`. We can provide you with a solution within a few days from receiving this sample in case of infection. The samples or reporting of the statistics or incidents will be used for input for our report to the WildList.

USER EDUCATION

By David Perry (Global Director of Education, TrendMicro)

We all assume so much. We assume that everyone shares our world view. We assume that everyone understands not only our language but our idiom. We assume too much, especially in the world of computer users.

We employ an entire industry of help desk and tech support analysts, and among the people of this world, there is a saying. "Mostly you are not fixing the computer, mostly you are fixing the user." Not only does the user need help finding specific instructions or installation, frequently the user does not understand the actual goals and functions of the products he uses. Having spent some years in software support—I can tell you that there is still vast misunderstanding between the users and the industry that helps to protect them. Here are some examples of user misunderstanding:

that helps to protect them. Here are some examples of user misunderstanding:

1.
Everything that goes wrong with my system is caused by a computer virus.

This is a very common misunderstanding—users think 'bug' and 'virus' are the same thing.

2.
I bought AV software already, why should I ever buy it again?

Again, this is a very very common misapprehension. Many users go for years without ever updating their av software and are quite surprised to find out that they need an internet connection and daily updates.

3.
I ran the virus to see what it would do but it didn't do anything I could see.

Years of movies and television shows have conditioned users into believing that viruses should produce instant and dramatic effects, and these users

frequently *intentionally infect themselves out of curiosity, or worse, desire to stop their employer's network.*

What can be done about this?

How can we possibly hope to protect an enterprise where users bring disks from home, give away their passwords to strangers and buy pills from spammers? I have long maintained that the future of computer security rests on four pillars:

1.

System design needs to be more secure from the ground up

2.

Security apps need to be better

3.

Users need to be better informed and take better actions

4.

Legislation and international cooperation must support a world safe for data exchange

INVITATION TO THE EICAR MEMBERS MEETING

2006

TO BE HELD THE EICAR CONFERENCE IN HAMBURG
ON MONDAY, 1ST MAY 2006 COMMENCING AT 17:30 hrs

AGENDA

1. Welcome and acceptance of the agenda
2. Minutes of last members meeting
3. Board reports
 - 3.1. Chairman's report
 - 3.2. Report from the eicar office
 - 3.3. Treasurer report
 - 3.4. Audit report
4. Exoneration of the board
5. EICAR future strategy
6. Election of new board members
7. Membership and fees
8. Election of auditors
9. Conference 2006
 - 9.1. Conference venue
 - 9.2. Conference Organisation
10. Any other business

THE MEMBERS MEETING SHALL ONLY ADDRESS MOTIONS FROM THE AGENDA.
ADDITIONAL MOTIONS FOR CONSIDERATION HAVE TO BE SUBMITTED IN WRITING AT THE
LATEST BY 15TH APRIL 2006 (DATE OF RECEIPT) TO THE EICAR OFFICE.

Signed: Rainer Fahs Chairman of the Board

2005

★
eicar14th CONFERENCE*(By Eddy Willems)*

More pictures and impressions of the conference at the www.eicar.org !

The conference 2005 was a great success. The choice of the venue is hard to top; a marvellous place, which will be remembered by the attendees. Sorry for those who missed it!

Let us try to make Hamburg also a remarkable event.



EUROPEAN EXPERT GROUP FOR IT-SECURITY

★
eicar

06

29. APRIL
BIS 2. MAIHOTEL HAFEN HAMBURG
HAMBURG
GERMANY

Conference Theme:

"Technical, Legal and Social and Management Aspects of IT Security"

Malware and Anti-Virus, Cybercrime, Data Protection and Privacy, Critical Infrastructure Protection, INFOSEC Management and sociological aspects of security and data protection will be topics of discussion at the conference.

ATTENTION!

Because of the large number of high quality presentations the conference will already start on Sunday 30th April, at 14:00 We will have the usual pre-conference program with Student WS and Professional Clinic starting on Saturday, 29th April.

You will find the latest information about the program here:
<http://conference.eicar.org/2006/programme/schedule.htm>

OUR SPONSORS!**METRO** Group symantec.**G DATA**
SECURITY phoenix
technologies CLEARSWIFT™ F-SECURE®
BE SURE. Aventail
More secure. More access. It's that simple. TREND
MICRO™15th EICAR
ANNUAL CONFERENCE