



17ème Congrès International EICAR

(European Institute for Computer Antivirus Research)

Organisé par l'ESIEA
du 3 au 6 mai 2008

REVUE DE PRESSE



Ouest-France du 29 avril 2008

Les spécialistes des virus informatiques réunis à Changé

L'école supérieure d'informatique électronique automatique (Esiea) accueillera les plus grands spécialistes mondiaux des virus informatiques à l'occasion d'un colloque international qui aura lieu à la salle des Ondines, à Changé, le lundi 5 et le mardi 6 mai. Il s'agit de la réunion

annuelle de l'institut européen de la recherche sur les antivirus (Eicar, selon les initiales en anglais).

Les spécialistes de la sécurité informatique parleront cette année de la lutte contre les virus et les codes malveillants, et des techniques virales émergentes, notamment

celles liées à la virtualisation. Une rencontre attendue alors que le marché des antivirus s'envole.

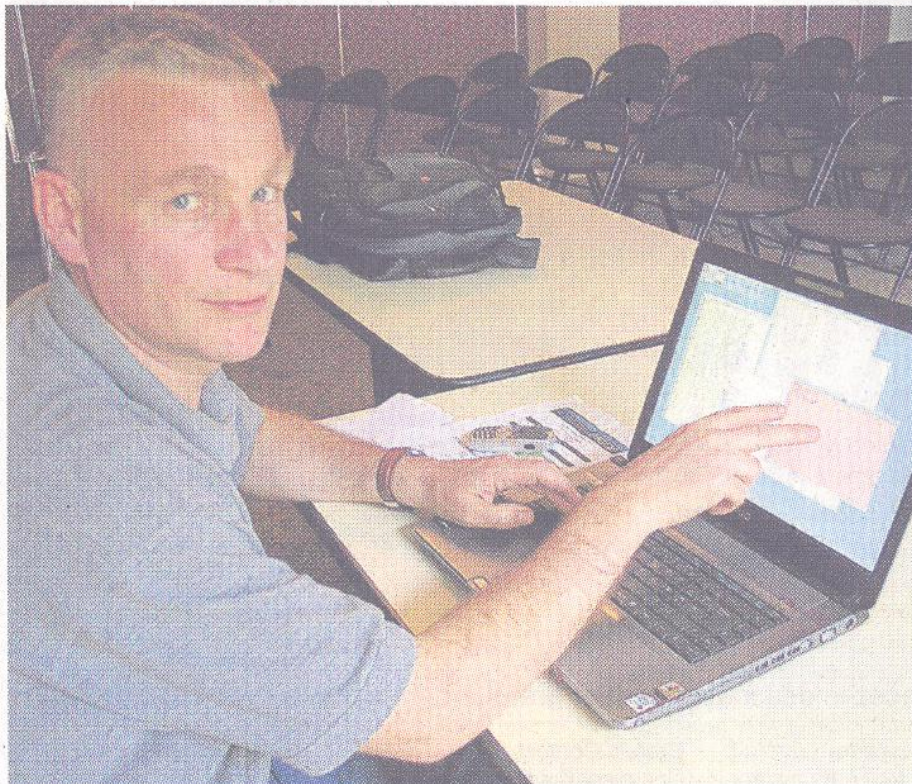
En 2007, il a atteint un nouveau record avec 2,4 milliards d'euros de chiffre d'affaires et devrait dépasser les 3,5 milliards d'euros d'ici trois ans.

Ouest-France du 6 mai 2008

70 experts des virus informatiques à Changé

Les grands spécialistes mondiaux des anti-virus sont présents en Mayenne depuis dimanche, à l'occasion d'un colloque international. L'événement, dont c'est la 17^e édition, se tient pour la première fois en France. Il est accueilli par l'Esiea, l'école d'ingénieurs de Laval. Objectif : présenter l'avancée de la recherche mondiale en terme d'anti-virus.

« Les pirates ne cessent de développer des systèmes d'infection de plus en plus élaborés » explique Éric Filiol, organisateur et enseignant à l'Esiea. Les virus se transmettent d'ordinateurs à ordinateurs lors des téléchargements, via les mails ou lorsqu'on ne remet pas à jour assez souvent les programmes et systèmes d'exploitation. « Il n'y a pas d'anti-virus infallible et il n'y en aura jamais, précise Éric Filiol. C'est l'utilisateur qui doit être prudent. » Selon des chiffres du FBI, un ordinateur sur quatre dans le monde serait accessible à des pirates.



Éric Filiol, directeur de laboratoire et enseignant à l'Esiea : « Les piratages informatiques sont aujourd'hui dus en grande partie à des mafias chinoises et russes. La seconde grande menace est terroriste. »

Virus informatiques : comment se protéger ?

À Laval la semaine dernière, un colloque a réuni 70 experts mondiaux des antivirus. Éric Filiol, spécialiste, explique comment se prémunir.

Entretien

Aujourd'hui, existe-t-il des anti-virus plus fiables que d'autres ?

Bien sûr. Mais il faut d'abord rappeler qu'il n'y a pas d'antivirus infaillible. Et cela n'existera jamais. Un chercheur, Fred Cohen, l'a prouvé en 1986. Ce qui compte beaucoup, c'est l'attitude de l'utilisateur. Ce n'est pas nécessaire d'être un grand technicien mais il faut être prudent. Quand on veut télécharger un programme, c'est bien par exemple de taper son nom dans Google avant. Si c'est un programme normal, on va tomber sur des sites officiels. Si c'est un programme dangereux, on va le voir tout de suite dans les portails affichés. On trouve aussi des indications dans les forums. Mais c'est vrai qu'on ne peut pas avoir de garantie. Si on possède un logiciel douteux dans son ordinateur, on peut l'envoyer par mail à son antivirus pour qu'il le vérifie. C'est le seul moyen d'être sûr. Il suffit d'aller dans la rubrique « contact » qu'on trouve sur le site Internet de chaque antivirus. Cette procédure est gratuite.

À part l'antivirus, peut-on se protéger autrement ?

Il y a trois règles simples à respecter. En ce qui concerne les mails, il

ne faut jamais ouvrir ceux qui paraissent douteux. Il faut se méfier en priorité des messages qui ont des titres racleurs. La seconde règle est d'éviter certains téléchargements, sur les sites pornographiques bien sûr, mais aussi sur les sites où les internautes mettent en commun des logiciels. Appelés « peer to peer », ils sont dangereux car on ne sait pas d'où viennent les logiciels qui y sont proposés. Enfin, il faut remettre à jour régulièrement le système d'exploitation de l'ordinateur et les programmes. Ce n'est pas une manipulation difficile. La plupart du temps, l'ordinateur affiche un message vous disant : « Une nouvelle mise à jour est disponible ». Dans ce cas, c'est très important d'accepter le message pour les effectuer. Sinon, cela crée des failles dans le dispositif de sécurité.

Est-ce risqué d'effectuer des paiements en ligne ?

C'est risqué car on peut être piraté sans s'en rendre compte, sans que l'antivirus l'ait détecté. Surtout, il ne faut jamais donner son code de carte bancaire à quatre chiffres. Il faut savoir que même la banque ou la police ne peuvent pas le demander sur Internet. Lorsqu'on paye en ligne, on donne seulement ses identifiants bancaires. Mais le risque existe. On pense même que beau-

coup de personnes ne se rendent pas compte qu'on leur a volé leurs identifiants bancaires. Les pirates ne retirent que des petites sommes : moins de 20€ par mois. Mais ils opèrent sur beaucoup de machines et gagnent donc énormément d'argent. La seule manière de savoir si on est piraté ou pas est de surveiller ses comptes attentivement. Si on découvre des retraits qu'on n'a pas fait, on peut porter plainte.

Les risques se développent-ils ?

Des formes de prises en otage numérique se développent. Des pirates cryptent vos données puis vous demandent 50€ pour vous les restituer. La plupart des petites entreprises préfèrent payer ces sommes modiques et ne portent pas plainte. Avant, les pirates concurrençaient les entreprises ou étaient tout simplement malveillants. Depuis 2003, le piratage s'est professionnalisé. Aujourd'hui, ce sont des mafias chinoises et russes, très bien organisées, qui veulent faire de l'argent. La menace est aussi terroriste. Selon des chiffres du FBI, un quart des ordinateurs dans le monde serait tombé sous le contrôle de pirates. Il faut donc redoubler de vigilance.

Recueilli par
Raphaëlle REMANDE.

Éric Filiol est directeur du laboratoire de virologie et cryptologie à l'ESIEA, l'école supérieure d'informatique électronique automatique de Laval.



Courrier de la Mayenne - du 15 mai 2008

Un laboratoire lavallois traque les virus et pirates du net

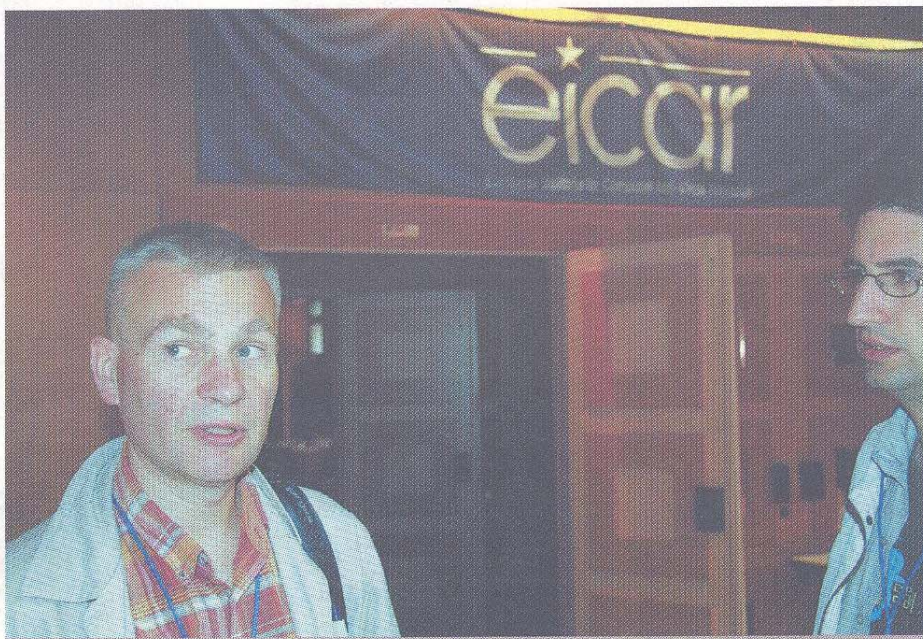
« Professionnalisation des attaquants »

L'Institut européen de la recherche sur les anti-virus a organisé son colloque annuel en France, à Changé, sur la lutte contre les "virus et codes malveillants".

Pour la première fois depuis sa création en 1991, l'Institut européen de la recherche sur les anti-virus a organisé son colloque annuel en France. 70 des plus grands spécialistes mondiaux de la virologie informatique se sont retrouvés à Changé pour évoquer la lutte contre les virus et codes malveillants liés à la virtualisation.

Les virus suivent le développement de la net économie. Plus le logiciel est utilisé, plus il est la cible des pirates. « Il y a plus de chances de se faire infecter en utilisant Internet Explorer que Firefox ou Opera. Or 90 % des gens qui ont un PC utilisent Internet Explorer qui est diffusé sous Windows », rappelle Boris Sharov, P-dg de Doktor web, une société moscovite spécialisée dans les solutions anti-virus. Baptisé Rustock.A, le plus important rootkit récemment décelé a contaminé 300 000 ordinateurs dans le monde avec une capacité de délivrer 60 milliards de spams par jour. Derrière les infections se cachent l'espionnage, l'escroquerie et l'extorsion de fonds en échange de la restitution des données.

Pour Eric Filiol, directeur du Laboratoire de Virologie et Cryptologie Opérationnelles à l'Esiea, installé à Laval, la situa-



Spécialiste mondialement reconnu, Eric Filiol entend bien développer l'activité du laboratoire de virologie et cryptologie lavallois de l'Esiea créé voici un an.

tion est d'autant plus grave que l'on manque vraiment d'experts indépendants. « Les utilisateurs sont pris en otages par les vendeurs de logiciels. Ce sont ceux qui diffusent qui définissent aussi les besoins. Il faut trouver des nouveaux moyens pour évaluer les risques. Et

pour garantir cette indépendance, il n'y a que la recherche académique ». D'où l'intérêt du laboratoire de virologie et cryptologie opérationnelles de l'Esiea et de l'institut européen. « Depuis 2003, on assiste à une professionnalisation des attaquants qui peuvent être des

groupes mafieux, des terroristes, voire des pirates étatiques », confirme ce militaire de carrière qui quittera prochainement l'armée pour se consacrer entièrement à sa nouvelle mission.

Emmanuel Blois

Repères

• **Un rootkit** est un programme ou un ensemble de programmes qui masque l'activité des pirates dans un système de données leur permettant d'utiliser celui-ci comme relayeur de spams par exemple sans que l'utilisateur même averti s'en rende compte.

• **Un chiffre** atteste de l'inflation des virus : en 2007, le marché des anti-virus a atteint un nouveau record avec **2,4 milliards d'euros** de chiffre d'affaires et devrait dépasser les 3,5 milliards d'euros d'ici trois ans.

• **Sur Second Life**, des pirates donnent vie à des codes ou virus qui franchissent la barrière du monde réel pour s'infiltrer dans les ordinateurs des particuliers, mais aussi des entreprises.

Quatre conseils pour limiter les risques de virus

- **Primo** : ne jamais utiliser de logiciel piraté. C'est le meilleur moyen d'installer des codes malveillants, en plus du logiciel.
- **Secundo** : éviter d'aller visiter certains sites de téléchargement de jeux piratés ou de sites pornographiques.
- **Tertio** : entretenir régulièrement son ordinateur équipé d'une version officielle d'anti-virus. La sécurité doit être mise à jour régulièrement.
- **Quatro** : développer une hygiène informatique signifie se former en permanence. L'utilisateur doit être l'acteur de sa propre sécurité. Il existe des anti-virus gratuits très bons. Pour se former, le meilleur outil c'est Google.

www.lamayenne.fr - mai 2008

L'ESIEA Ouest accueillera la 17e conférence internationale EICAR

Dans le cadre de l'ouverture à LAVAL, en septembre 2008, d'un nouveau pôle de recherche en Cryptologie-Virologie, l'ESIEA accueillera les plus grands spécialistes mondiaux de la virologie informatique à l'occasion du colloque EICAR qui aura lieu à la salle des Ondines à CHANGE, le 5 et 6 mai 2008.

Pour la première fois depuis sa création en 1991, l'Institut Européen de la Recherche sur les Anti Virus (EICAR) organise son colloque annuel en France. Scientifiques, chercheurs et industriels, les spécialistes de la sécurité informatique se réunissent à Laval. EICAR est la plus ancienne conférence scientifique sur la virologie. Cette année, la thématique principale est **la lutte contre les virus et les codes malveillants face aux techniques virales émergentes et notamment celles liées à la virtualisation**. Une rencontre attendue alors que le marché des anti-virus s'envole. En 2007, il a atteint un nouveau record avec 2,4 milliards d'euros de chiffre d'affaires et devrait dépasser les 3,5 milliards d'euros d'ici 3 ans.

Lors de ce congrès mondiale de virologie, les thèmes du "Rapt numérique et cyber-guerre" seront abordés.

Le développement du rapt numérique

« Le rapt numérique se développe fortement. Il y a urgence pour trouver les moyens de lutte contre ce fléau » explique Eric Filiol, Directeur du Laboratoire de Virologie et Cryptologie Opérationnelles à l'ESIEA. C'est le thème abordé par un chercheur de la société Sogeti, qui a analysé les virus d'extorsion de fond. En clair, des pirates s'introduisent dans un ordinateur et accèdent au disque dur. Ils aspirent alors l'ensemble des données et prennent contact avec le propriétaire. Ils font alors monter les enchères en fonction de la confidentialité des données. La victime doit verser une forte somme pour récupérer l'ensemble du contenu de son disque dur.

Attentat numérique : les industriels en dangers

L'autre sujet du colloque sera la cyber-guerre. Les experts scientifiques présenteront les conclusions de leurs dernières recherches sur la collecte de l'information préalable à une attaque électronique. L'approche sera résolument psychologique et portera notamment sur la manipulation des personnes. Les industriels sont en dangers face aux risques croissant d'attentat numérique. Mc Afee, Sophos, Computer Associates, Sogeti, IBM, les grands noms de l'informatique ont pris conscience de l'enjeu économique de la cyber criminalité. Les spécialistes de Mc Afee, un des leaders de la sécurité numérique et de l'édition d'anti-virus, ont également planché sur l'impact de la virtualisation. Ils ont ainsi mis en évidence des passerelles entre le monde réel et le monde virtuel. Sur Second Life, des pirates donnent vie à des malwares (codes malveillants ou virus) qui franchissent ensuite la barrière du monde réel pour s'infiltrer dans les ordinateurs des particuliers, mais aussi des entreprises.

Les chercheurs se mobilisent

Plusieurs chercheurs universitaires interviendront au colloque EICAR. Parmi eux, Cédric Lauradoux, de l'Université de Princeton, essaye de détecter les techniques de virtualisation responsables du développement exponentiel des malwares. Sébastien Josse, est lui à l'école doctorale de Polytechnique. Il termine sa thèse sur les liens entre la cryptologie et la virologie informatique. «La virologie et la cryptologie deviennent interdépendantes » explique Eric Filiol. C'est un des objectifs de ce colloque. C'est aussi celui de l'ESIEA qui compte désormais sur la complémentarité de ses deux laboratoires de recherche lavallois (un laboratoire de Virologie et Cryptologie Opérationnelles et un laboratoire de Réalité Virtuelle et Systèmes Embarqués).

Lors de ce colloque, il sera possible d'interviewer Eric FILIOL, Directeur du Laboratoire de Virologie et Cryptologie Opérationnelles à l'ESIEA et membre du Comité directeur du Colloque EICAR 2008.

<http://www.infohightech.com/> - mai 2008

Rapt numérique et cyber-guerre

lundi 28 avril 2008, par [Bernard](#)

Paris, le 28 avril 2008 - Pour la première fois depuis sa création en 1991 l'Institut Européen de la Recherche sur les Anti Virus organise son colloque annuel en France. Scientifiques, chercheurs et industriels, les spécialistes de la sécurité informatique se réunissent à Laval. EICAR est la plus ancienne conférence scientifique sur la virologie.

Cette année, le thème principal est la lutte contre les virus et les codes malveillants face aux techniques virales émergentes et notamment celles liées à la virtualisation. Une rencontre attendue alors que le marché des anti-virus s'envole. En 2007, il a atteint un nouveau record avec 2,4 milliards d'euros de chiffre d'affaires et devrait dépasser les 3,5 milliards d'euros d'ici 3 ans.

Le développement du rapt numérique

*« Le rapt numérique se développe fortement. Il y a urgence pour trouver les moyens de lutte contre ce fléau » explique **Eric Filiol, Directeur du Laboratoire de Virologie et Cryptologie Opérationnelles à l'ESIEA.***

C'est le thème abordé par un chercheur de la société Sogeti, qui a analysé les virus d'extorsion de fond. En clair, des pirates s'introduisent dans un ordinateur et accèdent au disque dur. Ils aspirent alors l'ensemble des données et prennent contact avec le propriétaire. Ils font alors monter les enchères en fonction de la confidentialité des données. La victime doit verser une forte somme pour récupérer l'ensemble du contenu de son disque dur.

Attentat numérique : les industriels en dangers

L'autre sujet chaud du colloque sera la cyber-guerre. Les experts scientifiques présenteront les conclusions de leurs dernières recherches sur la collecte de l'information préalable à une attaque électronique. L'approche sera résolument psychologique et portera notamment sur la manipulation des personnes. Les industriels sont en dangers face aux risques croissant d'attentat numérique. Mc Afee, Sophos, Computer Associates, Sogeti, IBM, les grands noms de l'informatique ont pris conscience de l'enjeu économique de la cyber criminalité.

Les spécialistes de Mc Afee, un des leaders de la sécurité numérique et de l'édition d'anti-virus, ont également planché sur l'impact de la virtualisation. Ils ont ainsi mis en évidence des passerelles entre le monde réel et le monde virtuel. Sur Second Life, des pirates donnent vie à des malwares (codes malveillants ou virus) qui franchissent ensuite la barrière du monde réel pour s'infiltrer dans les ordinateurs des particuliers, mais aussi des entreprises.

Les chercheurs se mobilisent

Plusieurs chercheurs universitaires interviendront au colloque EICAR. Parmi eux, Cédric Lauradoux, de l'Université de Princeton, essaye de détecter les techniques de virtualisation responsables du développement exponentiel des malwares. Sébastien Josse, est lui à l'école doctorale de Polytechnique. Il termine sa thèse sur les liens entre la cryptologie et la virologie informatique. « La virologie et la cryptologie deviennent interdépendantes » explique Eric Filiol. C'est un des objectifs de ce colloque. C'est aussi celui de **l'ESIEA** qui compte désormais sur la complémentarité de ses deux laboratoires de recherche lavallois (un laboratoire de Virologie et Cryptologie Opérationnelles et un laboratoire de Réalité Virtuelle et Systèmes Embarqués).