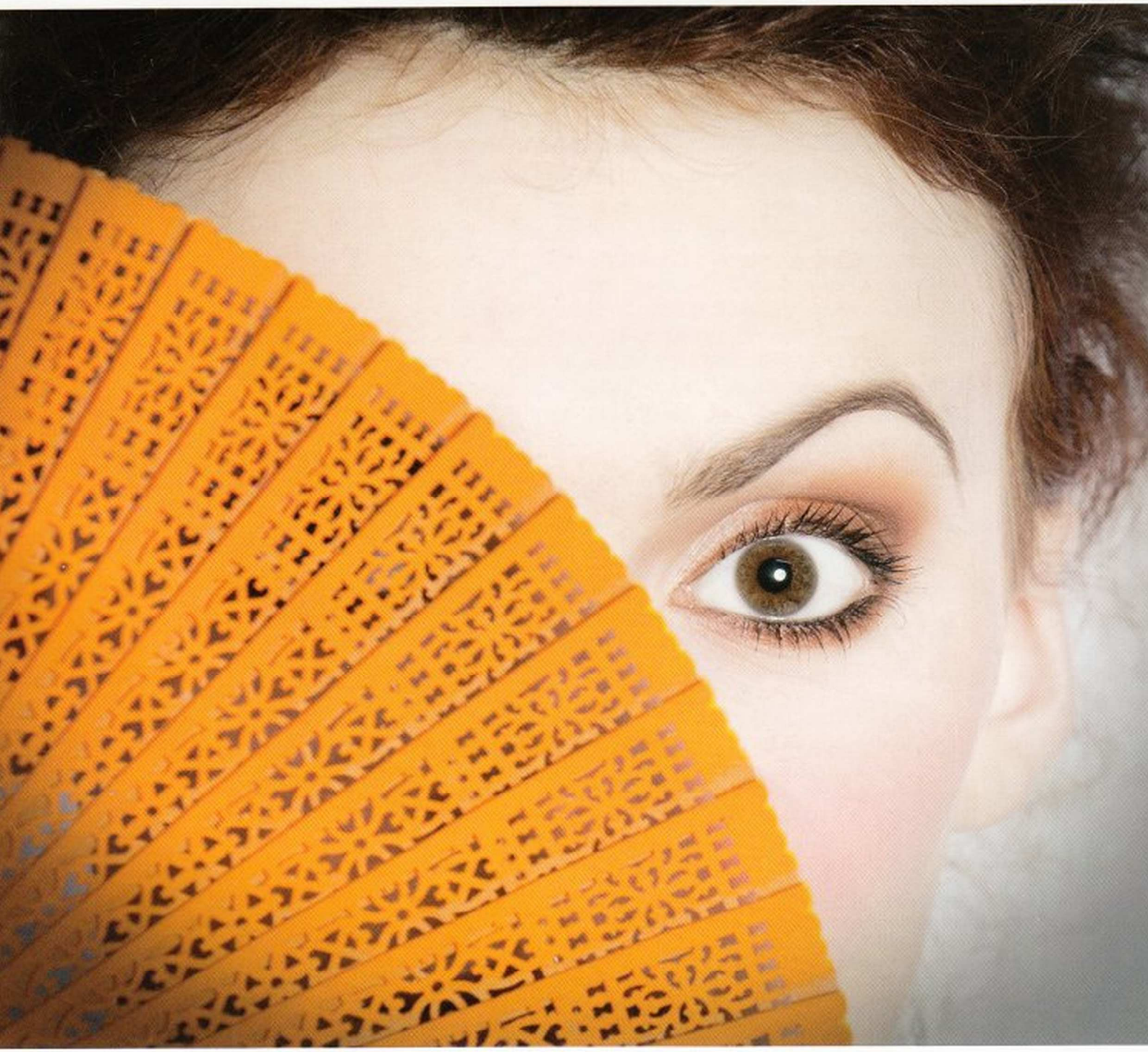
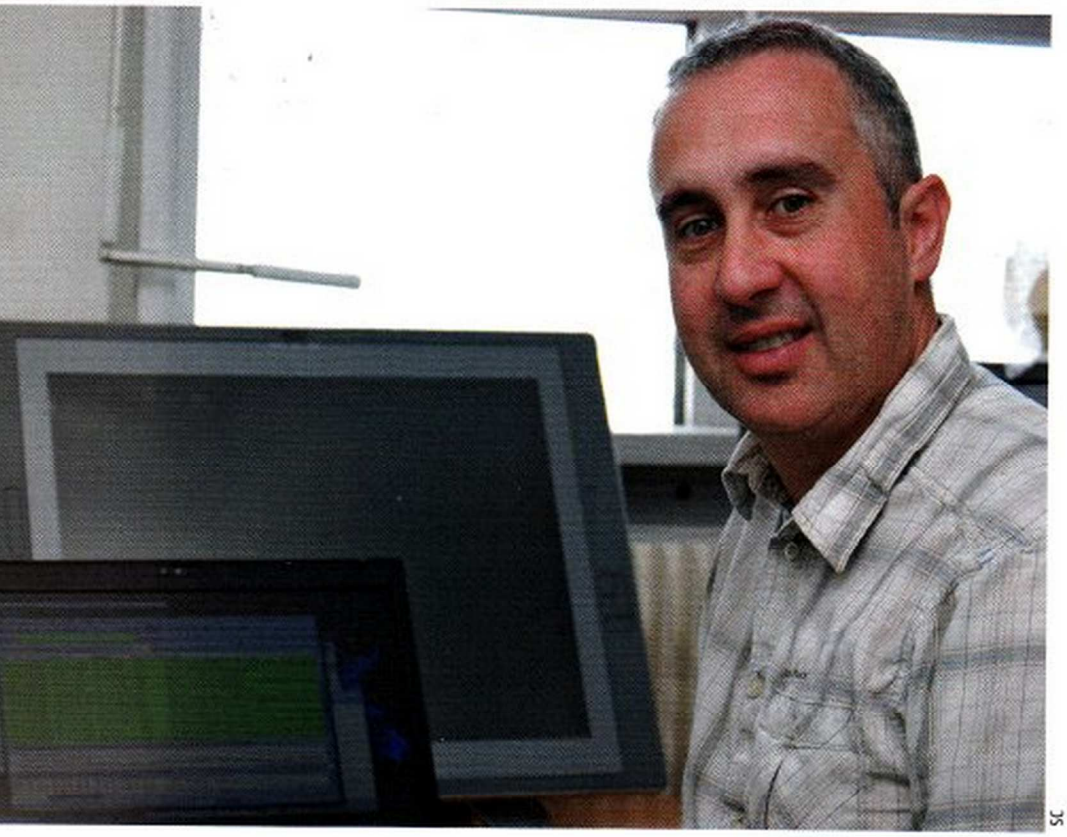
ForumEco
ACTUALITÉ ÉCONOMIQUE EN VERSION RÉGIONALE
La Gazette du Mid



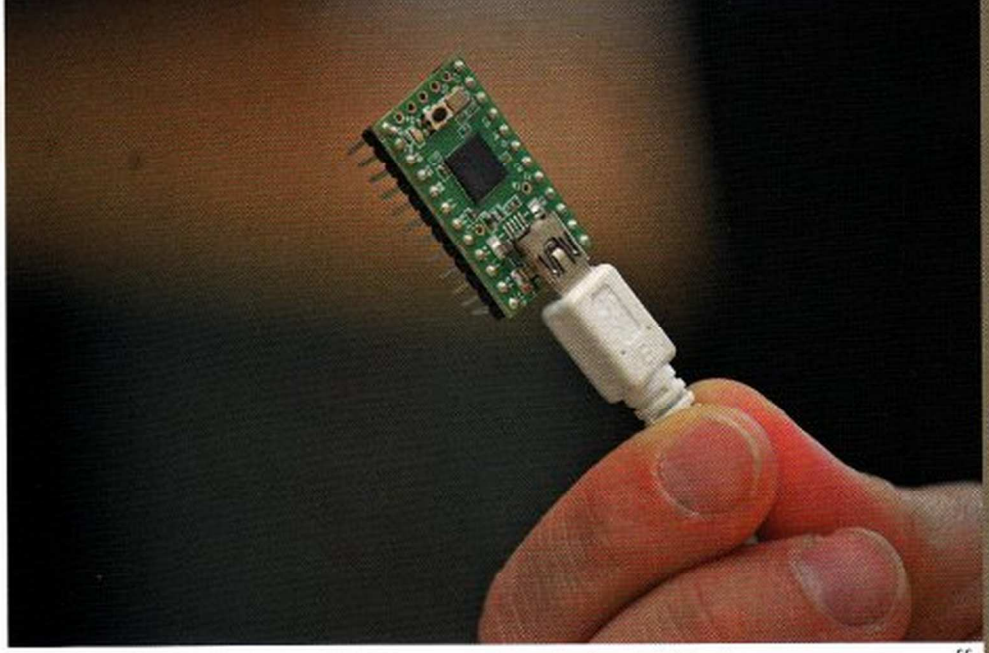
Intelligence économique, réputation, influence : un réflexe



Passionné des questions de cybersécurité, le chercheur et informaticien de l'Irit (université Toulouse III Paul-Sabatier) Philippe Truillet livre ici quelques clés pour éviter les intrusions malveillantes dans les systèmes informatiques.

PHILIPPE TRUILLET : « LA CONFIANCE, C'EST LE MOTEUR DU PIRATAGE »

Philippe Truillet a beau sourire, le constat qu'il livre sur les réseaux informatiques a de quoi glacer le sang : « On n'est en sécurité nulle part ! Aujourd'hui, quand on consulte internet, l'important est d'obtenir le service que l'on recherche, comme accéder à ses mails ou à ses comptes bancaires, mais vous ne voyez jamais par où transitent vos informations, et de quelle manière : autant dire que vous ne pouvez pas savoir si vos transferts de données sont bien sécurisés ! » Pour preuve, l'enseignant-chercheur du Laboratoire de recherche en informatique de Toulouse (Irit), au sein de l'université Toulouse III Paul-Sabatier, a récemment réalisé une petite expérience sur la confiance que nous accordons aux réseaux publics. En installant une fausse borne wi-fi au sein de l'université Toulouse I Capitole, qui fonctionnait comme un routeur, il a pu ainsi récupérer les mots de passe des étudiants qui s'y étaient connectés ! Comment ? La réponse ne tarde pas : Philippe Truillet allume son ordinateur et lance un simple logiciel, baptisé Wireshark. En quelques secondes, cet outil d'analyse des protocoles des réseaux affiche… toutes les connections informatiques qui transitent par le routeur du laboratoire ! Révélant, en temps réel, quelles sont les machines connectées, les adresses internet et les fichiers qu'elles consultent, et même les identifiants et les mots de passe qui ont été enregistrés ! « Wireshark est un outil gratuit, facile à trouver et à utiliser quand on s'y connaît un peu, mais de manière générale, il n'y a pas besoin d'être informaticien pour faire tomber un système ou récupérer des informations », souligne Philippe Truillet. Alors, comment se protéger ? « Il faut utiliser des protocoles sécurisés, symbolisés par la lettre "s" : https, ftps, SSH… cela permet de crypter les communications entre celui qui demande un accès et celui qui le donne, dont les logins qui autrement apparaîtraient en clair. Mais bien sûr le système n'est pas parfait, les attaques sont toujours possibles ! » Pour ne rien arranger, « rien ne dit que la personne ou la



SC

nachine avec laquelle je commu-ique soient sécurisées ! Car elle éberge peut-être des virus qui récu-èrent l'information directement hez elle... »

Limiter la diffusion des informations sur internet

Autre risque auquel s'exposent les ntreprises, celui qui consiste à proposer des services ou des documents sur internet au prétexte que leur accès est restreint et bien protégé. Mais la confiance, c'est le moteur du piratage ! Il y a clairement des informations qui n'ont rien à faire sur internet ; et même si on ne connaît pas l'adresse URL qui mène à ces documents, les moteurs de recherche feront ce tra-ail très bien à votre place. » Ne reste plus qu'à s'introduire par effraction, ce qui, du fait de la profusion de logi-iels de piratage sur internet, ne pré-sente plus une grande difficulté, même pour des hackers amateurs. Un autre bon moyen de récupérer des codes informatiques est de créer une copie du site informatique visé, et d'y amener les usagers qui, en toute bonne foi, vont enregistrer leurs logins et mots de passe. Aussi Philippe Truillet défend-il l'idée qu'une entreprise, au lieu de propo-ser des informations à partir d'un site nternet, « devrait plutôt permettre à 'utilisateur de rentrer dans le sys-ème informatique interne de l'entre-prise, à condition qu'il soit protégé, de part et d'autre, par un réseau privé virtuel (virtual private network, VPN) ». Un système qui, chez l'utili-sateur et son destinataire, crypte toutes les informations entrantes et sortantes, rendant presque impossi-ble toute interception.

Le bon sens comme règle de sécurité

« En fait, pour éviter la plupart des risques informatiques, il suffit parfois juste d'un peu de bon sens, et se demander : est-ce que je livrerais sans contrôle ces mêmes informations dans la vie réelle ? », souligne Philippe Truillet. Ce qui suppose, par exemple, de se méfier des réseaux publics gratuits, comme on en trouve dans les fast-foods et certains espaces publics. Attention également aux objets électroniques, comme les clés USB, les tablettes et les smartphones que l'on utilise désormais sans discernement, par simple commodité : encore en vogue récemment dans les entreprises, la mode du bring your own device (BYOD, « amenez vos propres outils ») qui poussait les employés à utiliser leurs propres objets communicants se voit de plus en plus encadrée, « car cela pose la question de la limite entre information publique et privée et de leur sécurisation ». Même un outil apparemment aussi innocent qu'une souris informatique peut représenter un risque de sécurité ! En témoigne une société américaine qui s'était vantée d'être parfaitement impénétrable. Son sous-traitant en sécurité informatique, Netragard, l'a pris au mot : mais au lieu de l'attaquer par le réseau, comme l'aurait fait n'importe quel hacker, les faux pirates choisirent d'envoyer de faux cadeaux promotionnels aux employés de l'entreprise-cible, en l'occurrence des souris de la marque Logitech. Caché à l'intérieur, se trouvait un microcontrôleur relié à une mémoire flash qui, au bout d'une minute d'inactivité de la souris, déclencha l'envoi d'un logiciel malveillant qui permit de prendre le contrôle de l'ordinateur ! Moralité : ne jamais faire trop confiance, car même les meilleurs s'y feront toujours prendre.

Un master cybercriminalité ?

Philippe Truillet, qui est également lieutenant de réserve dans la gendarmerie nationale, coordonne un projet de master sur la cybercriminalité qui pourrait voir le jour en septembre 2014 au sein de l'université Toulouse III Paul-Sabatier. L'objectif de cette nouvelle formation, d'abord accessible en formation continue, sera « d'associer les aspects juridiques et techniques de la sécurité informatique », dont par exemple la cryptographie et l'analyse des protocoles réseaux. Des entreprises comme Airbus et Thales songeraient d'ailleurs à soutenir le financement de ce nouveau master car, comme le note PhilippeTruillet, « ces deux sociétés manquent cruellement de techniciens spécialisés dans ce domaine. »