



CASES articles

Le côté obscur

Les malwares d'aujourd'hui et de demain

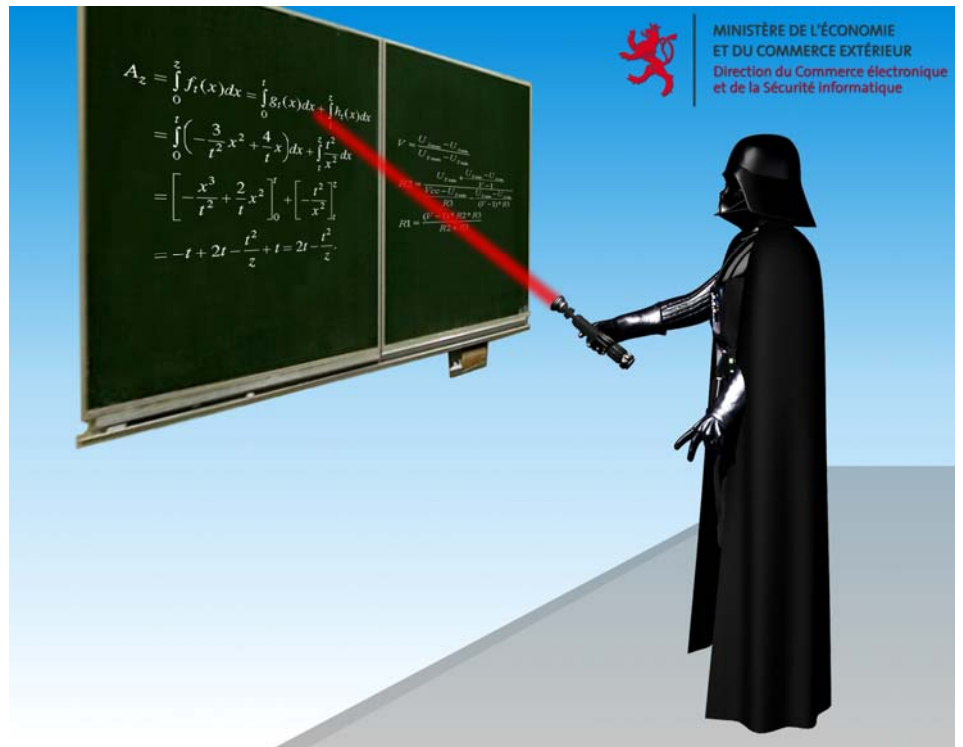
Pour plus de sécurité, adoptez les réflexes CASES !

Les avantages et les faiblesses du réseau des réseaux

Les utilisateurs privés ainsi que de nombreuses entreprises sont persuadés que leurs moyens techniques de protection informatique les mettent à l'abri des attaques. Mais ce sentiment de sécurité est trompeur. Ainsi, la direction d'une entreprise connaît-elle les formes d'attaque telles que la collecte automatique de données Web 2.0 visant à réaliser des profils de certains individus ou d'organisations complètes par exemple ? Les utilisateurs privés connaissent-ils les vulnérabilités des technologies qu'ils emploient à la maison ? Seule la connaissance des formes d'attaque permet d'évaluer le niveau de menace et les risques potentiels encourus, qu'ils soient d'ordre privé ou économique.

Les slogans des fournisseurs de logiciels de protection promettent souvent une protection à 100 % dès leur programme installé. C'est faux, il faut être conscient qu'une telle protection n'existe pas ! Pour les experts, il est souvent possible de mener à bien des attaques ciblées. En mettant à profit leurs connaissances techniques, ils sont, le cas échéant, en mesure de franchir avec succès un système sans se faire repérer. Ce genre d'attaque ciblée est en large augmentation à l'échelle mondiale.

Dans le monde informatique, la lutte entre le « bien » et le « côté obscur » atteint chaque année de nouveaux sommets. Les systèmes de protection actuels repoussent les attaques en cours, ou tentent de débarrasser un système des effets d'une attaque ayant déjà eu lieu.



Des formes d'attaque simples comme bonjour

Les attaques ciblant des appareils dont la fonction Bluetooth est activée, comme les téléphones mobiles, peuvent de nos jours être lancées par des enfants. Ils utilisent alors des malwares afin, entre autres, de téléphoner gratuitement par le biais de téléphones mobiles étrangers. Les propriétaires de ces appareils ne le remarquent qu'à la lecture de leur facture téléphonique.

Les cybercriminels ont également la possibilité d'obtenir des données commerciales importantes, car ils ont alors accès au carnet d'adresses de la victime.

Lors d'un test d'une durée d'une heure, effectué le 15.10.2008 sur le Boulevard Royal à Luxembourg-Ville, le portail de la sécurité de l'information CASES a répertorié plus de 200 ap-

pareils dont la fonction Bluetooth était activée.

« L'équipement utilisé ainsi que le logiciel mis en œuvre ont été réalisés par nos soins, en seulement quelques jours. Les mesures ont été effectuées à une distance assez importante : à partir du 7^e étage d'un immeuble de bureaux. Nous avons répété ce test à l'occasion de la Foire d'automne 2008, cette fois sur le site Luxexpo. Les appareils dont la fonction Bluetooth est activée sont apparus sur des écrans placés à proximité de l'entrée principale de l'exposition, près du stand CASES. Grâce à ces actions, nous souhaitons sensibiliser la population et les entreprises aux vulnérabilités induites par la technologie et aux mesures de protection des données personnelles et commerciales qu'il est nécessaire d'appliquer. Lorsque la fonction Bluetooth n'est pas nécessaire, elle doit être désactivée. Ceci est

valable aussi bien pour le kit mains libres dans une voiture, que pour le téléphone mobile, l'ordinateur ou tout autre appareil », explique Pascal Steichen, collaborateur de CASES.

Les chevaux de Troie les plus courants permettent de prendre le contrôle à distance d'un ordinateur sans protection. Dès que le malware est installé sur l'ordinateur de la victime, l'attaquant peut surveiller toutes les opérations effectuées par celle-ci : introduction de données bancaires, rédaction de documents, ou toute autre tâche réalisée sur l'ordinateur. Pourtant, n'importe quel logiciel antivirus mis à jour régulièrement est en mesure d'empêcher toute tentative d'attaque effectuée à l'aide de chevaux de Troie courants.

Enfants et adolescents utilisent ces malwares par exemple pour activer la webcam de camarades de classe ou pour faire toutes sortes de bêtises sur l'ordinateur de leur victime. Les visiteurs du stand d'exposition CASES lors de la Foire d'automne 2008 ont eu la possibilité d'observer un cheval de Troie ainsi que son fonctionnement. Il leur a été alors toutefois précisé que l'utilisation de tels malwares est sévèrement punie en Europe.

Hack.lu 2008 – les formes d'attaque des professionnels

Alors que les cybercriminels exécutent de plus en plus souvent des attaques très ciblées, par exemple à l'aide de modèles mathématiques sophistiqués, les scientifiques et experts en sécurité de l'information tentent de mettre au point des boucliers de protection adéquats. À l'occasion de la conférence luxembourgeoise sur la sécurité hack.lu 2008, du 22.10. au 24.10.2008, plus de vingt formes d'attaques modernes, ainsi que les moyens de s'en protéger, ont été présentés. La conception et les fonctionnalités des navigateurs sont par exemple responsables de bon nombre de vulnérabilités et les nouvelles vagues d'attaques lancées actuellement par les pirates se concentrent principalement sur celles-ci.

La divulgation d'informations personnelles ou de données d'entreprise par

le biais du World Wide Web peut également être exploitée par des individus malveillants. À l'aide de logiciels spécifiques, les criminels sont en mesure de collecter et de corréliser des données. Il leur est ainsi rapidement et aisément possible d'établir des profils de personnes ou même d'organisations entières. Ces profils leur permettent ensuite de cibler leurs attaques. Les visiteurs ont pu assister à une présentation en direct de cette forme d'attaque au cours de hack.lu 2008.

L'accès à des informations et à des services de commerce électronique par le biais du World Wide Web fait désormais partie de notre quotidien. L'Internet nous permet par exemple de réserver des billets d'avion, de commander des livres ou encore de consulter les liaisons ferroviaires. Bien que ces applications Internet protègent l'accès à leurs systèmes internes et aux réseaux adjacents, des connaissances spécifiques peuvent permettre, sous certaines conditions, de contourner les mécanismes de protection actuels. Un nouvel outil aux mains des attaquants permet par exemple de compromettre ce genre d'applications Internet courantes en quelques minutes. Une démonstration en direct de ce genre d'attaque a été également présentée à l'occasion de hack.lu. Dans ce cadre, il est important d'intégrer les concepts de sécurité adéquats.

Les formes d'attaque ciblant les systèmes embarqués d'applications à usage personnel ou pour les petites entreprises sont également à la hausse. Presque chaque entreprise moyenne et chaque foyer disposent désormais d'un routeur. Or, bien peu d'importance est accordée à ces petits appareils – et aux vulnérabilités qu'ils laissent apparaître.

La liste des mesures de protection nécessaires ne cesse de croître, en particulier pour les entreprises. Ceci est dû, entre autres, à des technologies telles que WiFi, Voice over IP ou les réseaux GPRS. Les cybercriminels, à l'intérieur et à l'extérieur de l'entreprise, exploitent les points faibles de ces technologies afin de s'introduire dans les réseaux.

Conseil de sécurité :

Agenda de la sécurité de l'information pour octobre 2008.

Au cours de la Foire d'automne, du 18.10. au 26.10.2008, sur le site Luxexpo et sous la devise de la « Protection de la vie privée », le portail de la sécurité de l'information CASES a offert aux visiteurs la possibilité d'en savoir plus au sujet de la sécurité de l'information. Des réglages sécurisés de l'application Facebook, en passant par le bon paramétrage d'un pare-feu, jusqu'au mode de fonctionnement d'un cheval de Troie ou l'explication des escroqueries actuelles sur l'Internet – des spécialistes de la sécurité de l'information ont été à la disposition des visiteurs pour répondre à toutes leurs questions. Les visiteurs de la foire ont également pu tester leurs connaissances en matière de sécurité de l'information et ainsi gagner, toutes les deux heures, des prix intéressants.

Spécialistes, experts en sécurité de l'information, scientifiques et cadres ont pu assister du 22.10. au 24.10.2008 à la conférence de sécurité luxembourgeoise de renommée mondiale hack.lu. Ils ont pu à cette occasion obtenir des informations sur des thèmes relevant de la sécurité de l'information, tels que les formes d'attaque, les vulnérabilités et mécanismes de protection. Plus de 20 thèmes dans les domaines les plus divers y ont été abordés par des experts. De nombreux exposés ont par ailleurs été associés à des « démonstrations en direct ». Le Ministère de l'Économie et du Commerce extérieur soutient, avec d'autres partenaires issus de l'industrie et de l'économie, cette conférence spécialisée.

Cofondateur de l'organisme public luxembourgeois CIRCL (Computer Incident Response Centre Luxembourg – véritable rempart de la sécurité informatique), Pascal Steichen conseille d'adopter une approche lucide des formes d'attaque et des mécanismes de protection : « Que ce soit pour les entreprises ou les personnes privées, il est important de connaître et de comprendre les différentes formes d'attaque. La sécurité à 100 % n'existe pas, mais des mécanismes et réflexes de sécurité adéquats peuvent néanmoins réduire fortement les risques. Assister à une conférence de sécurité comme hack.lu représente assurément pour les cadres, les spécialistes de l'informatique, les scientifiques et les experts en sécurité de l'information un bon investissement sur le long terme. »

Définitions :

Bluetooth

Bluetooth est un standard de communication par ondes radio.

navigateur

Un navigateur est un programme informatique permettant aux utilisateurs de visualiser des pages Internet sur le World Wide Web. Internet Explorer, Mozilla Firefox et Opera sont des navigateurs populaires.

routeur

Les routeurs sont des appareils reliant les réseaux informatiques entre eux ou les isolant les uns des autres. Les routeurs analysent les paquets de données entrant en fonction de leur adresse de destination et les bloquent ou les acheminent, selon les cas.

Voix sur IP (« voice over IP »)

Le terme de voix sur IP désigne la téléphonie via les réseaux informatiques par le biais du protocole Internet.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu