

EDITO

AGENDA

ACTUALITES P2

VEILLE P3

Flux RSS : la rançon du succès ?

ZOOM P4

L'année se termine mal pour Microsoft

L'ESSENTIEL P6

Autopsie du spam (1/2)

EDITORIAL

Récemment, le cabinet d'études IDC a souligné l'éclatante santé du marché de la sécurité. Rien qu'en France, ce marché a progressé d'environ 30% sur la période 2002-2004. L'explosion des projets de gestion des identités, des technologies mobiles et de RFID (entre autre), que nous avons traité et continuerons de traiter au travers de cette lettre d'information, confirme la poursuite de cette ascension irrésistible.

Cette dynamique est soulignée par les manœuvres de renforcement opérées par les grands éditeurs (Microsoft, Symantec, etc.) : acquisitions stratégiques d'acteurs de niches de la sécurité, annonces fracassantes, consolidation du secteur tendant vers une convergence inéluctable. Il ne faudrait pourtant pas sous-estimer les micros acteurs du marché que sont certaines PME/PMI, *start-up* et laboratoires de R&D, souvent peu connus du grand public, qui font réellement progresser les technologies de la sécurité.

Tandis que la menace demeure permanente, protéiforme et s'adapte instantanément, le choix des offres préventives et/ou curatives demeure pléthorique, plaçant de fait les décideurs dans une posture délicate : celle de l'art subtil de l'équilibre entre la maîtrise des coûts, les responsabilités légales et l'efficacité des moyens de protection mis en œuvre. La technologie se révèle efficace lorsqu'elle s'inscrit dans une démarche transversale et organisationnelle, le maillon faible restant toujours le facteur humain.

L'équipe ESEC vous présente ses meilleurs vœux et a le plaisir de vous annoncer que Sogeti-Transiciel s'appelle dorénavant SOGETI.

AGENDA - Sélection début d'année 2006

- ⇒ **Panorama de la cybercriminalité 2005 - CLUSIF**
Comme chaque année, le CLUSIF a présenté les faits marquants de la cybercriminalité pour l'année 2005. Le rapport est disponible à l'adresse ci-dessous.
Plus d'infos :.....<https://www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k5-fr.pdf>
- ⇒ **Solutions Linux + Solutions OpenSource2006 - 31 janvier, 1^{er} et 2 février 2006, CNIT, Paris La Défense**
Linux et les solutions Open Source ont désormais le vent en poupe et s'imposent de plus en plus dans les entreprises, les services publics et les administrations.
Plus d'infos :.....<http://www.solutionslinux.fr/fr/index.php>
- ⇒ **Conférence Normalisation et Certification en SSI, 7 mars 2006, Paris**
Deuxième conférence annuelle consacrée à la norme 7799/ISO 27001 organisée par ISSA France.
Plus d'infos :.....<http://www.issa-france.org/>
- ⇒ **Nouveaux enjeux préventifs de la sécurité pour les RSSI et CIO, 14 mars 2006, Forum LMI, Paris**
Un point sur la SSI dans les entreprises, panorama des technologies à venir et des meilleures pratiques de gestion des risques.
Plus d'infos :.....<http://www.lemondeinformatique.fr/forumdecideurs>



ACTUALITES

Gemplus et Axalto s'unissent pour créer Gemalto, leader mondial de la carte à puce

Alors que plus de 1,8 milliards de cartes à puce devraient avoir été écoulees en 2005 (en croissance de 23% par rapport à 2004), le phénomène de concentration des acteurs du secteur s'accélère avec le projet de fusion amicale de Gemplus et Axalto, présenté le 7 décembre. Respectivement n°1 et N°2 mondial (24,2% et 21.8% de part de marché en 2004 - Source : Frost & Sullivan), les deux sociétés produisent principalement les cartes SIM pour téléphones portables.

La téléphonie mobile s'est arrogée 72% du marché mondial des cartes à puce en 2005 (Source : Eurosmart) tandis que les cartes de crédit représentaient 18%. L'activité cartes d'identité électronique et de santé et cartes de décodeurs de télévision reste marginale (~1%) mais est en forte croissance. Une bonne nouvelle pour la France, berceau de la carte à puces, qui reste leader sur un marché dynamique et générateur de valeur ajoutée

Pour en savoir plus :

<http://www.zdnet.fr/actualites/informatique/0,39040745,39293501,0.htm>



BlueLane présente sa solution de patching virtuel : PatchPoint System

Alors que chaque semaine de nouvelles vulnérabilités, plus ou moins critiques, sont découvertes, le cycle de qualification puis de déploiement sur les systèmes en production demeure souvent long, délicat et coûteux. BlueLane, société américaine basée en Californie, aura mis trois années pour assurer la maturité et la pérennité de sa solution de patching virtuel. Basée sur une *appliance*, cette solution permet d'émuler les patches et autres correctifs de sécurité sur les flux, non pas sur les systèmes.

Le temps nécessaire est ainsi laissé aux équipes sécurité de tester la non régression des correctifs tout en permettant aux équipes d'exploitation de planifier leur mise en œuvre ainsi que leur déploiement. Cette solution fonctionne aussi bien pour Microsoft SQL, IIS, Exchange, Sendmail, Oracle, Solaris, Apache ou Linux.

Pour en savoir plus : <http://www.zdnet.fr/entreprise/service-informatique/poste-client/0,50007192,39279133,00.htm>



Certification CC EAL4+ : (vraie-fausse ?) opération séduction de Microsoft

La sécurité est LE grand chantier du géant de Redmond depuis plusieurs mois et nul doute que nous en reparlerons dans les prochaines lettres d'information. Dans cette optique, Windows Server 2003, XP SP2, Exchange Server 2003 et ISA Server 2004 ont obtenu la certification *Common Criteria* EAL4+. Ce résultat est la conséquence directe de l'engagement pris par Microsoft en 2002 (programme SDL - *Security Development Lifecycle*) d'améliorer la qualité et la sécurité des développements de ses produits.

Les Critères Communs sont une série de standards normalisés ISO qui permettent de procéder à l'évaluation du niveau de sécurité d'un logiciel (sur une échelle de 1 à 7), en fonction de critères stricts et précis.

Le niveau EAL4 est le niveau maximum qu'un logiciel puisse obtenir et est reconnu par les 22 pays signataires des CC. Le signe « + » renforce la certification obtenue puisqu'il signifie que les logiciels ont subi des tests de vulnérabilité.

Pourtant, cette annonce semble être davantage une tentative de séduction à destination des clients échaudés par les alertes, patches de sécurité et autres rustines qui font la « réputation » de Microsoft, qu'une réelle garantie de sécurité. Couplée, par exemple, à une certification du type CMM¹ (*Capability Maturity Model*) la démarche gagnerait en sérieux et en crédibilité.

Pour en savoir plus :

<http://www.silicon.fr/getarticle.asp?ID=12871>

¹ Modèle d'évaluation et d'évolution des processus logiciels qui comporte 5 niveaux de maturité : initial, reproductible, défini, maîtrisé et optimisé.

VEILLE TECHNOLOGIQUE

⇒ Flux RSS : la rançon du succès ?

📁 Syndiquer pour simplifier

En mars 1999, Netscape présentait la version 0.9 du format RSS (*Rich Site Summary* ou *Really Simple Syndication*) permettant la syndication de contenus issus de multiples sources d'information en un point unique. Sa simplicité d'utilisation et son utilité avérée expliquent sans doute le succès fulgurant des fils RSS : plus besoin de visiter

quotidiennement un site afin d'y rechercher de nouvelles informations. Une liste de sujets, rafraîchie et mise à jour, est affichée au format texte dans le lecteur dédié. Il suffit alors de cliquer sur le lien désiré et la page connexe s'affiche.

📁 L'apport du RSS aux entreprises

L'arrivée prochaine de Windows Vista et de la version 7 d'Internet Explorer devrait parachever l'utilisation grand public et au quotidien des lecteurs RSS. L'outil de veille par excellence est alors susceptible de devenir un puissant vecteur de *spywares* et autres codes malveillants.

Et ce qui apparaît aujourd'hui comme une application réellement utile en simplifiant le temps passé à la recherche d'informations, se révélera peut-être demain comme une faille supplémentaire des systèmes d'information, déjà bien « gâtés ».

Cette tendance est vraisemblable puisque de plus en plus d'entreprises commencent à mettre en œuvre les flux RSS dans le cadre de plates-formes de distribution de l'information sur leur intranet/extranet ou pour permettre l'échange automatique d'informations entre deux applications web (comme les services web).

Car le format RSS peut être abusé : écrit en XML et pointant vers des contenus HTML, il « embarque » les descriptions de ces derniers. Sa souplesse est telle que de nombreux objets, au premier rang desquels des scripts, peuvent être inclus. Le contenu est alors directement interprété par le lecteur dédié ou par le navigateur.

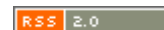
📁 Risques et menaces

Le panorama des attaques potentielles est digne d'une liste à la Prévert : insertion de scripts ou d'objets, attaque antédiluvienne de type *iframe* (faille I.E. 6 SP1 liée à une erreur au niveau de la gestion des tags) redirection sur une page piégée, exécution de code dans les définitions de style ou bien encore insertion de *web bugs* (image gif de 1 pixel donc invisible permettant d'enregistrer le comportement de navigation d'un internaute sur une page web donnée). Il semble donc probable que les lecteurs RSS aient à faire face aux mêmes problèmes de sécurité que les *webmails* il y a quelques années.


L'internaute croyant avoir affaire à sa revue préférée risque alors des surprises plus ou moins désagréables.

Ces risques potentiels sont clairement identifiés mais l'industrie commence tout juste à réagir afin de mettre la sécurité des lecteurs RSS à niveau.

Verisign envisage, par exemple, de fournir outils et services nécessaires à assurer la sécurité des flux RSS tandis que l'éditeur Reactivity propose une passerelle XML capable de contrôler les flux de ce format.



En bref

Le format RSS devient un outil indispensable améliorant le confort de navigation et apportant une réelle valeur ajoutée pour l'entreprise : agrégation des contenus informationnels, mises à jour en temps réel, présentation simplifiée. Même s'il est trop tôt pour savoir si le RSS sera victime de son succès (auprès des « pirates »), tout projet de déploiement du RSS doit être conduit comme un projet de sécurité à part entière. 



ZOOM

⇒ L'année se termine mal pour Microsoft

Et c'est reparti pour une alerte aux images malades : la dernière vulnérabilité en date pour Windows permettrait la prise de contrôle du PC à la simple lecture d'une image piégée. Cette fois-ci, ce sont les formats maison Windows Metafile (WMF) et Enhanced Metafile (EMF) qui sont à l'honneur.

Pas de trêve des confiseurs pour les pirates

Bien qu'il ne s'agisse pas des formats les plus couramment usités, leur utilisation à travers le système est suffisamment importante pour rendre une telle attaque rentable. Ces images peuvent en effet être intégrées à une page web (et donc automatiquement ouvertes par Internet Explorer à la lecture), ou dans un courrier au format HTML et c'est cette fois-ci Outlook (via le moteur d'I.E.) qui se chargera de les lire automatiquement. En outre, Windows interprétera les images (et sera donc compromis) en ouvrant un dossier qui en contiendrait.

L'attaquant peut aussi distribuer le piège dans une archive ZIP (par exemple avec une application copiée sur des réseaux P2P) ou tout simplement dans un dossier accessible via le réseau de l'entreprise. Enfin, il est également possible d'intégrer une image piégée à un document Office (Word ou PowerPoint par exemple) et donc de compromettre le système à son ouverture.

Les attaques...

Si la première génération des attaques WMF ne comprenait que des « downloaders » (codes intégrés à une page web chargés d'installer en catimini un code malicieux lors de sa visite), l'arsenal des pirates s'est considérablement sophistiqué depuis. Selon plusieurs FAI, une carte de vœux comportant une image piégée (extension au format JPG) aurait été largement diffusée par email. Lorsque l'image est manipulée (ouverte, prévisualisée ou même tout simplement indexée par Windows ou Google Search), le piège est activé et un trojan se télécharge et s'installe sur l'ordinateur.

Tout aussi inquiétant, un ver se propagerait actuellement via MSN et tenterait d'infecter les internautes en affichant un lien vers une image piégée. Les chatteurs enthousiastes qui suivraient innocemment le lien seraient alors infectés dès l'affichage de l'image et leur PC promptement détourné. Enfin, des sites de confiance (par exemple, selon l'Internet Storm Center, knoppix-std.org, réparé depuis) auraient été détournés et diffuseraient un code malicieux basé sur WMF.

La menace est donc critique puisque quasiment toutes les versions de Windows sont concernées (98, Millenium, 2000 SP4, XP SP1/SP2, Server 2000/2003).

Lors de tests menés en laboratoire, le lancement en ligne de commande de fichiers WMF piégés a permis d'infecter un PC sans aucune difficulté. Il est donc recommandé aux administrateurs réseaux de bloquer tout accès aux fichiers WMF mais cela n'est malheureusement qu'une cautère sur une jambe de bois : Windows XP exécutera tout fichier WMF, même s'il possède une extension différente ! En d'autres termes, prenez un fichier WMF, renommez-le avec une extension passe-partout (« .gif » ou « .jpg » par exemple), et vous voilà doté de l'arme absolue pour exploiter cette maudite faille.

Et ce n'est pas terminé. Récemment, une nouvelle version de l'exploit (le « mode d'emploi » de la faille qui permet aux pirates les moins doués d'en bénéficier également) a été publiée. Jugée plus avancée et surtout plus difficile à détecter, elle pourrait donner lieu à une troisième vague d'attaques beaucoup plus perfectionnées. Toutes, bien sûr, reposeront alors sur le même principe : forcer l'ordinateur à afficher une image piégée. Cette attaque permettrait la lecture automatique par I.E., affichée dans un courrier avec Outlook Express ou Lotus Notes qui utiliserait la même librairie pour afficher les images WMF, visualisées à l'aide de Paint, de l'outil de fax de Windows ou encore via un autre navigateur (en acceptant cette fois son ouverture car seul I.E. ne demande pas la permission d'affichage à l'utilisateur).

Il existe de nombreuses opportunités d'infection, et toutes sont silencieuses, invisibles et parfaitement opérationnelles. Bien entendu, la quasi-totalité des attaques WMF observées à ce jour sont utilisées pour installer des *adwares* ou des *bots* chargés de « zombifier » les PC.



📁 Les parades

Une semaine d'attaques massives plus tard, Microsoft a (de nouveau) tardé à réagir. L'éditeur se contente d'affirmer en substance qu'il « étudie la situation » et offrira, peut-être, un correctif s'il « estime la situation suffisamment grave ». De quoi prêter le flanc à la critique car Microsoft a la fâcheuse tendance à communiquer tardivement. Quelles que soient les – bonnes ou mauvaises – raisons qu'il pourra invoquer, ce ratage ne va guère aider l'éditeur à renforcer l'image sécurité qu'il cherche à se donner depuis plusieurs mois.

Heureusement, la communauté s'organise : le temps que le correctif sorte (le 6 janvier)², un expert indépendant (Ilfak Guilfanov) a pallié le risque en développant un correctif capable de patcher en mémoire la librairie vulnérable pour permettre d'afficher les images WMF sans danger. Le patch a été examiné et testé par l'Internet Storm Center. Raffinement

² <http://www.microsoft.com/downloads/results.aspx?pocId=&freetext=KB912919&DisplayLang=fr>

📁 La détection

Les éditeurs de logiciels anti-virus se sont lancés dans la course avec du retard. Si la plupart des produits détectent désormais les premières versions de l'exploit, ce n'était pas le cas aux premières heures de l'alerte. Un test sur un fichier infecté réalisé le 28 décembre dernier, grâce au service Virustotal, indique que sur les 24 moteurs anti-virus testés, seuls Avast, BitDefender, Fortinet, Kaspersky, NOD32 (v2) et Panda identifiaient alors une menace. Par ailleurs l'éditeur français Sunbelt donnait l'alerte le 27 décembre et F-Secure faisait état d'attaques dès le 28.

suprême : ce correctif peut être désinstallé proprement, via l'interface d'ajout et de suppression des programmes.

Du côté des fournisseurs d'IDS/IPS (sondes réseau) et d'anti-virus, chacun y va de ses mises à jour des bases de signatures. Problème toutefois puisque les exploits WMF évoluent très vite, et depuis la publication de la seconde génération du code d'attaque, les signatures sont rapidement obsolètes. Les administrateurs réseaux et responsables de la sécurité doivent veiller à s'assurer des mises à jour régulières de leurs IDS/IPS et, bien entendu, de leurs passerelles anti-virus. Pour finir sur les parades, l'activation de la protection DEP³ est recommandée pour les processeurs qui la supportent (AMD 64 bit, par exemple). Elle empêcherait l'exécution de l'attaque.

³ Fonction de sécurité intégrée au processeur empêchant l'exécution de codes de programmes dissimulés.

Mais il s'agissait là de la première version de l'exploit. Depuis, plusieurs variantes ont vu le jour mais c'est surtout la seconde génération qui pourrait permettre le développement d'attaques plus difficiles à détecter selon l'Internet Storm Center. Notons toutefois que lorsque la faille WMF est utilisée pour installer un parasite connu, ce dernier est à *priori* détecté par l'anti-virus, même si l'exploit WMF utilisé ne l'est pas.

Conclusion

Malgré l'armada de mesures appliquées pour lutter contre les codes malveillants, les failles les plus évidentes conservent un riche potentiel d'instabilité et de criticité. D'autant que les pirates développent une vraie capacité à exploiter les failles techniques des outils de protection tout comme celles, organisationnelles, des éditeurs : aucune fuite n'avait été détectée sur cette nouvelle attaque avant son activation massive et simultanée.

L'astuce des pirates rejoint les stratégies marketing sophistiquées des grandes marques !



L'ESSENTIEL

⇒ Autopsie du spam (1/2) : « ça vous chatouille ou ça vous gratouille ? »

Au début « ça chatouillait » et nombre d'internautes pouvait s'en accommoder mais, de plus en plus, « ça gratouille » de manière généralisée et il faut envisager, si cela n'est pas déjà fait, de traiter ce phénomène au même titre que les virus. Il est effectivement très difficile de considérer cette pandémie avec un sourire aux lèvres à la lecture d'une *publicité* pour des pilules bleues aux effets tellement vantés ! Dans ce numéro, nous allons vous faire découvrir l'origine et le fonctionnement du spam. Le mois prochain, nous tâcherons de décliner les parades (techniques et législatives) de ce fléau planétaire.

📁 Un peu d'étymologie

En 1937, SPAM est une marque déposée de jambon épicé (*SPiced hAM*) qui nourrira les GI's de l'armée américaine pendant la seconde guerre mondiale. En 1970, l'épisode 25 du *Monty Python's Flying Circus* se passe dans un restaurant, et consacre l'un de leurs plus célèbres sketches. On trouve cet aliment dans tous les plats de la carte : « œufs au Spam, salade au Spam, frites au Spam, Spam tomates, etc. ». Déguisés en Vikings amateurs de Spam, les joyeux drilles se lancent alors dans une chanson de leur crû : « Spam Spam Spam Spam Spam ... ». La chanson, interminable, est interprétée crescendo et finit pas couvrir les propos des autres protagonistes : la réputation du SPAM est faite !

📁 Comment ça marche ?

Le spam est une manifestation intempestive, massive et non sollicitée de messages qui s'attaquent aux différents médias électroniques dont nous disposons. Cette manifestation est généralement à caractère publicitaire avec escroquerie ou non à la clé. Le spam ne circule pas uniquement au travers de la messagerie. Forums de discussion, moteurs de recherche (référencement abusif), navigation Internet (*pop up*), messageries instantanées, téléphonie par Internet (à surveiller dans un avenir proche), commentaires des blogs... en sont aussi victimes !

Mais la messagerie demeure le vecteur le plus « exploité » à l'heure actuelle, et de très loin ; ce qui fait que dans les esprits et même dans sa définition, le terme spam soit exclusivement rattaché à la messagerie électronique. C'est cet aspect qui est abordé dans la suite de cet article.

Le contenu des spams est généralement publicitaire. C'est un moyen facile, rapide et peu onéreux pour communiquer. Bien souvent, les produits vantés sont des médicaments (dopage sexuel ou produits de jouvence), des crédits financiers, des services pornographiques ou des escroqueries en tout genre. Parfois, il s'agit aussi de messages d'entreprises ignorantes des règles de bonne conduite (« la Nétiquette »), qui voient là un moyen peu coûteux de s'assurer une quelconque promotion. Récemment, un parti politique n'a eu aucun scrupule à recruter des militants par ce biais, en utilisant des adresses email « non

Enfin, en mars et avril 1994, le cabinet *Canter & Siegel* pollue les groupes de discussion *Usenet* par les deux premiers spams officiels de l'histoire. L'un des participants, qui se sent alors gêné par ce parasitage, se fâche en répondant : « *Send coconuts and cans of Spam to Canter & Co. Be sure to drop the can of Spam on its seam first !* ». Traduction : envoyez des noix de coco et les boîtes de Spam à Canter et Co. Veillez à laisser tomber la boîte de Spam en plein sur sa soudure.

Le spam dans sa définition actuelle était officiellement né : une chose immonde dont personne ne veut mais qui finit par s'imposer à vous jusqu'à couvrir tout dialogue intelligible.

qualifiées » et « douteuses » (pour reprendre les termes de la presse qui s'en est fait l'écho).

Le *phishing* (hameçonnage), dans sa phase d'approche et de prise de contact, peut lui aussi être assimilé à une forme de spam. Cette technique consiste à tromper le destinataire en faisant passer un email d'apparence officielle (banque, organisme de certification de paiement électronique, ...) pour le rediriger sur un site piégé chargé de récupérer les données personnelles, en particulier les numéros de comptes et les mots de passe.

Les spammeurs, pour trouver leurs victimes, utilisent des logiciels (« robots ») spécialement conçus pour récupérer un maximum d'emails (dans les forums, sites Internet, groupes de discussion, etc.) et constituent ainsi d'impressionnantes bases de données. Les envois massifs de spam se font généralement à partir de machines corrompues (« zombifiées »), contrôlées à distance, rendant extrêmement difficile toute tentative de remonter la piste vers les criminels.

[Suite de l'article au prochain numéro]