SÉCURITÉ INFORMATIQUE

numéro 48 avril 2004

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Rappel : le numéro de février a été supprimé, le bulletin ne paraît plus que quatre fois par an au lieu de cinq.

Dormez en paix braves gens, le CERT veille…

éditorial

Certes, certes..., le foisonnement des attaques sur Internet qui, depuis quelques mois, revêt des proportions inégalées, appelle une «réponse sécuritaire» à la hauteur des agressions. En termes de veille, d'analyses, de sensibilisation, d'information, d'alertes, la réponse sécuritaire est d'abord collective.

L'article de Kostya Kortchinsky, responsable du CERT Renater, illustre la manière dont Renater, en charge du réseau couvrant la recherche et les universités, entend répondre à ce défi.

Kostya Kortchinsky nous dévoile les missions et le travail de fourmis (ou d'abeilles, quand l'outil est le pot de miel) des équipes du CERT Renater avec l'appui de tous leurs correspondants.

Les bulletins réguliers du CERT Renater sont une source essentielle d'information et d'aide à la décision. On peut souhaiter que la plus grande diffusion et la plus large lecture en est faite. Ces bulletins doivent aussi faciliter le contact et la remontée d'informations, de la base vers le CERT. La sécurité est l'affaire de tous, comme le rappelle l'encadré dans l'article ; au-delà de la vigilance individuelle, la remontée et l'exploitation de l'information et le partage d'expérience facilitent aussi une appréhension collective de la sécurité.

Le CERT mis en place par Renater complète, pour la communauté scientifique et universitaire, le dispositif national de réponse reposant sur le CERTA (CERT dédié à l'administration française). Le CERTA qui, de «computer response team - administration» a francisé son nom en «centre d'expertise gouvernementale de réponse et de traitement des attaques informatiques» (www.certa.ssi.gouv.fr) est hébergé par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) du Secrétariat de la Défense nationale (SGDN). Créé début 2000, le CERTA a pour mission la protection des services de l'Etat contre les attaques. Le CERTA est particulièrement présent sur la détection des vulnérabilités, la protection et la réponse aux agressions.

Alors, dormons en paix, puisque les CERT veillent, mais les yeux grands ouverts, car chacun participe à la veille.

Joseph Illand
Fonctionnaire de Sécurité de Défense

Quelle utilité le bulletin *Sécurité informatique* a-t-il pour vous ? Doit-il continuer à paraître ? Le format électronique peut-il remplacer totalement l'édition papier ?

Vous qui le recevez chaque bimestre, que ce soit par la poste ou par le courrier électronique, donnez-nous votre avis. Vous pouvez nous aider en nous renvoyant, à l'adresse Robert.Longeon@cnrs-dir.fr, le questionnaire dûment rempli (une dizaine de cases à cocher) que vous trouverez sur la page http://www.cnrs.fr/infosecu/sondage.txt

Le CERT Renater

Sur le Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche, tout incident de sécurité peut avoir des conséquences désastreuses, aussi bien au niveau de l'épine dorsale, qu'au niveau des sites distants connectés à Internet via *cette dernière. Toute compromission d'un élément de l'infrastructure du réseau impliquerait le contrôle par l'attaquant du trafic transitant par l'équipement, qu'il s'agisse d'un ralentissement, d'une coupure totale (déni de service) ou de l'accès à son contenu, avec les conséquences particulièrement graves que cela aurait. Concernant les systèmes connectés à Renater, les implications sont tout aussi alarmantes, puisque le pirate pourrait avoir accès aux ressources des machines (espace de stockage, bande passante, puissance de calcul) ainsi qu'aux informations hébergées sur celles-ci ou transitant sur le réseau local. S'ajoutent à cela des soucis de conformité de l'utilisation du réseau (professionnelle, rationnelle et loyale) et de licéité des contenus, qui se doivent de respecter la charte de d'utilisation de Renater* [1].

La problématique de la sécurité sur le réseau Renater est complexe, puisque chaque site est, bien entendu, libre d'adopter la politique qu'il souhaite, que l'étendue des besoins exprimés par les utilisateurs du milieu académique est généralement très vaste, et que les capacités de l'épine dorsale, dont la plupart des liens sont maintenant à 2.5 Gigabits, présentent un intérêt certain pour tout délinquant ou criminel informatique, aussi bien débutant qu'expérimenté. C'est dans ce contexte que fonctionne le CERT Renater (2), chargé de la sécurité du réseau de la recherche français, qui offre ses services aux organismes raccordés.

Un peu d'histoire

Le 2 novembre 1988, il y eut un changement majeur dans la façon dont les professionnels de l'informatique et le grand public envisageaient la sécurité sur Internet. En libérant sur le réseau un ver se propageant et se répliquant automatiquement, dont les conséquences furent de paralyser une bonne partie de l'Internet de l'époque, Robert T. Morris, étudiant de l'université de Cornell (le ver prit le nom de son créateur, le «Morris Worm») montra la sensibilité croissante des systèmes d'information aux attaques.

Une fois qu'un groupe de chercheurs des

suite page 2

(1) http://www.renater.fr/Telechargement/charte_v12.pdf

(2) C'est en 1995 qu'est créé le premier CERT français, à l'initiative du réseau Renater, ayant rejoint le FIRST cette même année.

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

suite de la page 1

communautés académique et gouvernementale eut réussi à contenir le ver, le «National Computer Security Center» américain (partie de la célèbre «National Security Agency») organisa une série de rencontres afin de discuter des façons de prévenir ou de répondre à de tels incidents à l'avenir. Peu après, la «Defense Advanced Research Projects Agency» annonça son intention de financer le développement d'un centre de coordination pour les incidents de sécurité sur Internet. La DARPA choisit alors le «Software Engineering Institute» de l'université de Carnegie Mellon pour héberger ce nouveau centre. Le CERT/CC, «Computer Emergency Response Team Coordination Center», premier CERT au monde, était né (3).

Depuis, d'autres équipes de réponses à incidents et de sécurité se sont développées à travers le monde, prenant le nom de CERT ou de CSIRT («Computer Security Incident Response Team»), dont une grande partie est aujourd'hui membre du FIRST («Forum of Incident Response and Security Team»)(4).

Les missions d'un CERT

La mission d'un CERT est d'assister ses adhérents en matière de sécurité informatique, et notamment dans le domaine de la prévention, la détection et la résolution d'incidents de sécurité. Sa fonction première est d'être un point de contact pour la communauté d'utilisateurs qu'il représente, c'est-à-dire la structure que l'on appelle à l'aide et qui organise les secours en cas d'incident. Cette structure doit pouvoir centraliser et diffuser l'information à des interlocuteurs identifiés par des canaux sûrs.

Les CERT, grâce à leur expérience, établissent des recommandations générales (pour les administrateurs de machines, de réseaux...) et font de la sensibilisation auprès des responsables et des utilisateurs.

Les CERT ne se substituent jamais aux autorités des organismes, encore moins aux autorités de police ou de justice. Ce sont les sites attaqués qui doivent (s'ils le jugent opportun) faire appel aux autorités de police. Néanmoins, les CERT maintiennent des liens de coopération avec ces autorités.

Le CERT-Renater ne déroge pas aux règles et principes qui régissent la vie des CERT et assure depuis quelques années, pour la communauté Renater, un rôle préventif et un rôle curatif. Depuis quelques mois, l'accent a été mis sur des aspects plus pro-actifs, répondant à la problématique de la détection précoce d'incidents de sécurité.

Les avis

Dans le domaine de la sécurité, la prévention est un domaine souvent négligé mais pourtant primordial. Se tenir au courant des problèmes de sécurité permet en effet d'anticiper bien des attaques et d'éviter bien des catastrophes. Cette activité requiert notamment une veille technologique permanente. La plupart des équipes techniques sur les sites Renater sont souvent débordées ou peu formées à la sécurité. Cette collecte d'informations est rarement faite ou du moins pas régulièrement. Le CERT-Renater se charge donc de diffuser aux sites Renater des informations jugées pertinentes et provenant de sources officielles (listes de diffusion des éditeurs par exemple). Existent quatre types de bulletins : vulnérabilité, alerte, information, statistiques. Ils sont diffusés vers les correspondants sécurité des sites (désignés par le chef d'établissement), qui ont la responsabilité de la diffusion en interne, conformément aux restrictions de diffusion que le CERT-Renater leur a communiquées.

En plus des notes de vulnérabilités distribuées par les équipementiers ou les autres CERT, le CERT-Renater dispose de moyens supplémentaires de collecte d'informations. Nous augmentons sans cesse le nombre de ces sources externes d'informations (sites Internet concernant la sécurité Internet, listes de discussion, forum de nouvelles (news), discussions IRC). Nous pouvons aussi glaner des renseignements susceptibles d'intéresser la communauté lors de l'analyse d'incidents, par le biais d'autres CERT, de relations privilégiées (ou non) avec certains correspondants sécurité au niveau des organismes, ou encore lors de la vérification d'informations provenant de sources non fiables (réseau de tests d'équipements en cours de déploiement, collaboration avec des membres d'autres CERT, etc.). Cette veille technologique des activités sur le réseau permet parfois de lancer des alertes ou de faire ressortir le niveau critique ou la persistance d'un problème de sécurité.

Depuis le début de l'année 2000, ces bulletins sont répartis en quatre catégories :

- VULN : elles informent les correspondants Sécurité des vulnérabilités découvertes sur les systèmes d'exploitation et les applications ;
- STAT : elles résument, tous les vendredis, l'ensemble des incidents traités au cours de la semaine écoulée et rappellent quelques recommandations appropriées. Le CERT-Renater utilise également les statistiques concernant les incidents traités comme indicateur pour mieux prévoir les évolutions dans les menaces et les failles utilisées ;
- INFO : elles décrivent, de la manière la plus détaillée et pédagogique possible, un phénomène lié à un problème de sécurité, mais sans caractère d'urgence ;
- ALER : elles donnent l'alerte sur un problème de sécurité qui touche l'ensemble du réseau ou qui menace de s'étendre rapidement à un grand nombre de sites.

Bien évidemment, pour que la prévention soit efficace, il faut que cette information parvienne rapidement à des contacts pertinents chargés de dispatcher l'information aux personnes responsables pour action. Il faut que son importance et sa pertinence soient reconnues et que des moyens soient mis en place pour la prendre en compte et déclencher des actions dès que cela s'avère nécessaire.

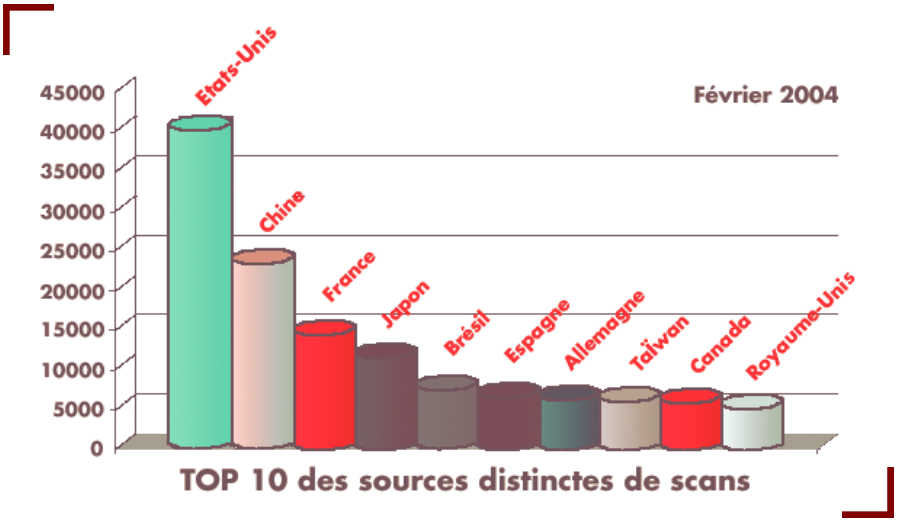
Kostya Kortchinsky
Responsable du CERT Renater
kostya.kortchinsky@renater.fr

L'année dernière, la championne toute catégorie des vulnérabilités découvertes a été la vulnérabilité RPC/DCOM n° 1 affectant les systèmes Windows NT, 2000, XP et 2003. Cette vulnérabilité était logée dans la portion de code qui gère les échanges de messages entre deux processus s'exécutant sur des machines distantes sous système d'exploitation Windows. De type «débordement de tampon», elle permet à un attaquant distant de prendre le contrôle d'un système vulnérable. L'annonce de cette vulnérabilité ainsi que la mise à disposition de correctifs pour tous les systèmes impactés a eu lieu le 16 juillet. Cette annonce, contrairement à beaucoup d'autres, tout autant prometteuse a priori, a été suivie des effets dévastateurs que l'on sait. En effet, cette faille de sécurité est le vecteur d'attaque de choix du sinistre ver Blaster qui a mis à mal le bon fonctionnement de nombreux réseaux et fait encore bien des victimes et perdre beaucoup de temps (et d'argent ?) à de nombreux organismes. Le 31 juillet, on notait déjà la publication d'un programme permettant de tirer parti de ce trou de sécurité et les premières compromissions étaient signalées. Mais l'exploitation à grande échelle de cette faille se situe deux semaines plus tard, aux alentours de 11 août avec le début de la propagation du ver Blaster. On voit donc bien qu'en très peu de temps, le pire peut arriver. On voit aussi qu'avec des moyens et/ou une bonne organisation, le pire peut aussi être évité. ■

(3) CERT Coordination Center http://www.cert.org/
(4) FIRST http://www.first.org/

Les remontées de sondages réseau

Le scan est une activité de reconnaissance qui permet à un individu de faire un audit des services offerts sur un réseau, des caractéristiques des systèmes accessibles, et des vulnérabilités potentielles de ces systèmes. Toutes les plages d'adressage d'Internet sont ainsi sondées en permanence à des fins plus ou moins légitimes.



TOP 10 des sources distinctes de scans

En fonction du nombre de systèmes et des services visés par un scan, il est possible de dégager certains comportements suspects. Des messages d'alerte sont alors envoyés aux contacts sur les sites, charge aux administrateurs réseau locaux de vérifier la légitimité des traces fournies. La prise en compte et l'analyse de ce type d'activité permet ainsi de détecter bon nombre de machines corrompues, et ce, souvent avant que les équipes techniques sur place ne se rendent compte d'un quelconque problème.

Par le passé les remontées d'incident de ce type étaient essentiellement effectuées par le biais de la messagerie électronique : des administrateurs contactaient le CERT-Renater pour lui communiquer des traces capturées illustrant des tentatives de connexion illicites. La collecte des traces était issue d'un processus manuel, nécessitant beaucoup d'efforts de la part de certains correspondants. Bien sûr, ce surcroît de travail n'encourageait pas de nouveaux correspondants à soumettre régulièrement des traces. Or, pour que ce travail de surveillance soit un minimum efficace, il faut travailler sur un grand nombre de classes d'adresse IP, et si possible, bien réparties sur l'ensemble d'adressage IPv4.

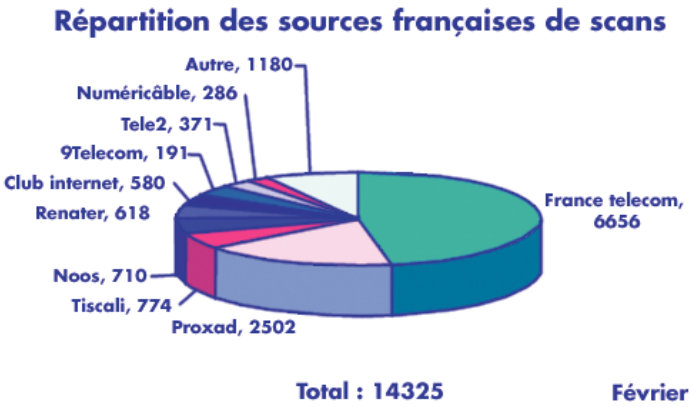
Au niveau du CERT, les rapports soumis nécessitaient aussi une analyse longue et fastidieuse. Qui plus est, il était assez difficile d'affecter des priorités aux différentes alertes à envoyer. Le mode de traitement adopté était assez séquentiel. L'expérience aidant, il s'avère que ce traitement est loin d'être efficace. On perd du temps à examiner des traces concernant des communautés peu enclines à collaborer alors que, noyées dans la masse, on passe à côté de machines compromises sur le réseau Renater ou sur d'autres réseaux avec lesquels le CERT entretient les meilleures relations de collaboration.

Dans le but d'améliorer la détection et le traitement des scans sur le réseau Renater, une nouvelle architecture et deux outils successifs ont été mis en place. Les messages sont maintenant envoyés à une adresse spéciale (certs-can@renater.fr), puis enregistrés et stockés dans une base de données. Ils sont consultables selon le mode client/serveur depuis le poste de chaque membre de l'équipe. Un premier client aux fonctionnalités limitées a été mis en place pour effectuer des requêtes sur la base. Courant juillet 2003, cet outil a cédé le pas à un système de consultation par interface graphique plus maniable et intégrant un plus grand nombre de requêtes standard (ainsi que la possibilité pour l'utilisateur de créer lui-même ses requêtes).

Il est ainsi maintenant possible de repérer assez rapidement tous les scans en provenance de machines de Renater, le but étant de repérer le maximum d'incidents et d'alerter les sites afin de faire en sorte qu'ils soient réglés le plus rapidement possible.

Il est donc possible de fouiller la base selon des critères prédéfinis et de traiter les résultats en fonction de différents profils :

- traiter d'abord les incidents mettant en cause des sites Renater (AS2200 principalement) ;
- traiter ensuite les incidents mettant en cause des systèmes appartenant à des communautés de confiance (couvertes par des CERT français, des CERT académiques, des CERT membres de la TF-CSIRT ou du FIRST) ;
- traiter ensuite le maximum de cas choisis en fonction des dernières vulnérabilités publiées et des programmes d'attaque mis à disposition.



Ainsi par exemple, on observait très peu de scans sur le port 135/tcp avant la publication par Microsoft de la vulnérabilité RPC/DCOM (bulletin MS03-026). L'observation des évolutions des scans nous a permis de détecter une très forte activité sur ce port après la date de la publication. Il était ensuite intéressant de contacter un maximum de sites sources de scans afin d'essayer de savoir ce qui se tramait (analyser des machines compromises permet d'en savoir plus sur le modus operandi des attaquants afin d'émettre des alertes). Les sites contactés sont choisis dans toute communauté pour laquelle le

suite page 4

suite de la page 3

CERT estime que la démarche a une chance d'aboutir. L'expérience permet d'identifier les types d'interlocuteurs, fournisseurs d'accès ou autres, susceptibles d'être sensibles à nos messages. Ces choix sont absolument nécessaires car la quantité d'informations à passer en revue chaque jour est énorme et par conséquent, on ne peut pas tout traiter.
À l'heure actuelle, le CERT compte 27 contributeurs journaliers, ce qui représente :

- une couverture de 2000 classes C (environ 10% des adresses de Renater);
- 150 à 200 messages reçus par jour;
- en moyenne plus de 10000 adresses IPs source de scans enregistrées par jour;
- plus de 100000 adresses destination scannées par jour.

Les informations collectées sont extraites de fichiers journaux de routeurs. Les rejets de tentatives de connexion illicites sont enregistrés dans ce fichier. Un tri automatique préalable à l'envoi est nécessaire pour réduire la masse d'informations à envoyer et écarter d'emblée des informations peu pertinentes (réduire le nombre de faux-positifs). Plusieurs outils sont disponibles pour faire ce travail de remontée dans un format immédiatement exploitable par les outils du CERT : Detescan (1), Vigilog (2), Anapirate (3).
La mise en place de ces outils est assez simple, et les bénéfices de la surveillance, inestimables. Une fois l'outil choisi mis en place, les remontées se font de façon automatique et l'administrateur n'est pas constamment sollicité par ce travail. Le CERT-Renater recommande des remontées quotidiennes, un délai supérieur empêchant un traitement correct des incidents et faussant les statistiques hebdomadaires. Outre la détection de machines compromises, cette collecte permet aussi de tirer des statistiques sommaires sur les tendances d'attaque. Ces chiffres alimentent le bulletin «STAT» que le CERT-Renater publie tous les vendredis.
Le CERT-Renater continue de solliciter les sites Renater pour augmenter le nombre de contributeurs journaliers. Le but poursuivi est de couvrir les attaques survenant sur l'ensemble des classes d'adresses de Renater et donc de capturer plus d'éléments intéressants, notamment des attaques généralisées et d'obtenir des statistiques plus fiables.

Kostya Kortchinsky

(1) Detescan http://www.igh.cnrs.fr/denis.pugnere/detescan/detescan.html
(2) Vigilog http://www.ensmp.fr/~martins/vigilog/
(3) Anapirate http://www.orleans.ird.fr/pub/anapirate/anapirate-site.html

Trafic contraire à la charte

En étroite synergie avec le personnel du GIP chargé de la supervision du réseau, le CERT a entrepris la surveillance des flux de trafic en transit sur le réseau Renater. Il ne s'agit pas, bien sûr d'espionner les communications des clients Renater, c'est-à-dire de faire une analyse du contenu des paquets en transit. Il s'agit plutôt d'essayer de détecter plus d'incidents sur le réseau Renater, de réduire le nombre d'activités illicites sur Renater, et de faire respecter la charte Renater.
Des informations au format Netflow5 en provenance de l'ensemble des Points de Présence (PoP) de Renater sont collectées, traitées et archivées. L'analyse se base sur la nature du trafic en transit sur les liens Renater : flux, adresses IPs, index de routeurs, taille des flux...
Une analyse quantitative du trafic permet de repérer des transferts potentiellement suspects et des dénis de service. Une analyse de la taille des flux permet de mettre en évidence des transferts potentiellement illicites. Certains gros transferts peuvent ainsi être symptomatiques de la présence d'un serveur de transfert de fichiers (FTP) pirate ou détourné de sa fonction première, ou bien encore de l'utilisation d'un outil P2P. Une analyse par seuil des flux permet aussi de mettre en évidence des dénis de service.
Les clients/serveurs P2P et les serveurs FTP pirates sont deux moyens très utilisés (1) aujourd'hui pour l'échange de fichiers illicites. Dans les deux cas, il s'agit le plus souvent de rapatrier et/ou mettre à disposition des fichiers contenant des jeux ou du contenu audio ou vidéo protégé par une licence ou des droits d'auteur. Ce type de trafic n'est pas conforme à la charte de bon usage du réseau Renater. Or, tout site connecté à Renater signe cette charte qui stipule que le trafic généré ou reçu doit essentiellement être à but éducation/recherche. Qui plus est, la présence de tels contenus sur des systèmes engage la responsabilité du responsable de ces systèmes. Or, depuis quelque temps, des associations d'éditeurs se forment et intentent des actions en justice contre les propriétaires de systèmes engagés dans de telles activités. En conséquence, dès qu'un transfert suspect est détecté, le CERT Renater se met en contact avec l'administrateur du site Renater concerné, lui signale l'incident et demande vérification et action lorsqu'il y a lieu. Le CERT Renater est aussi susceptible d'étendre son action et d'indiquer à un certain nombre d'autres sites un problème éventuel de ce type.
Cette année a été marquée par une croissance importante des incidents concernant des systèmes Windows. En effet, depuis l'an 2000 et la vulgarisation de l'utilisation de noyaux NT, les systèmes Windows sont très attractifs pour les pirates. Ils sont très largement déployés et leurs nouvelles fonctionnalités permettent de manipuler à distance le système avec la même souplesse qu'un système de type Unix/Linux.
Obtenir le contrôle d'un tel serveur sur Renater présente plusieurs avantages :

- espace de stockage gratuit et anonyme,
- une bande passante souvent importante et à coût nul.

Une étude comportementale de ce type de transfert illicite a permis de mettre en évidence une taille de fichiers caractéristique à rechercher, les captures se font donc en fonction de ce paramètre. Cette taille correspond à celle du fichier image ISO d'un disque compact (CD), découpé grâce à un logiciel de compression (RAR ou ACE la plupart du temps).
Bien sûr, la masse de trafic capturé abrite aussi des transferts légitimes. La plupart des logiciels P2P n'ont pas été, à l'origine, créés pour permettre la circulation de fichiers pirates. Il existe des utilisations tout à fait licites de ces logiciels : échanges entre chercheurs, etc. Cependant on estime qu'aujourd'hui, ces transferts sont loin de représenter la majorité des flux capturés (moins de 5% pour être plus précis). La charge générée constitue donc une occupation non justifiée et non négligeable de bande passante et, il ne faut pas l'oublier, cela a un coût.

(1) « La sécurité réseau au quotidien vue de l'intérieur» et «Témoignage sur un site piraté». Cf. http://www.cnrs.fr/Infosecu/num43.pdf

Les dénis de service

BIEN évidemment, la palme médiatique des attaques contre les systèmes d'information, juste après les virus (et quelquefois liées à eux) revient aux attaques de type DoS (Denial of Service) et DDoS (Distributed Denial of Service), qui ont rendu le jeune mafiaboy tristement célèbre en février 2000, et ont fait couler de l'encre plus récemment avec MyDoom et ses conséquences attendues sur les sites de SCO et Microsoft (soit dit en passant, il n'y a pas eu la moindre hausse du trafic sur Renater aux dates annoncées). Le principe en est simple : saturer les ressources réseaux ou systèmes d'un organisme afin qu'il ne puisse plus joindre Internet ni être joint :

- les réseaux, en saturant le lien ou le routeur d'accès du site en question ;
- les systèmes, en saturant les ressources du noyau de la machine cible, ou bien de façon plus précise, les ressources de l'application que l'on désire rendre injoignable.

Contrairement aux gros sites commerciaux dont le chiffre d'affaire dépend étroitement de l'accessibilité du site vis-à-vis du reste d'Internet, il n'existe pas de modèle financier aux attaques en déni de service sur Renater (je ne vois pas bien la menace «donnez-nous 10000 euros ou nous vous coupons du reste du monde» fonctionner convenablement). Ainsi, lorsqu'un site est la cible d'un déni de service, c'est qu'il héberge quelque chose ou quelqu'un qui a énervé le possesseur d'un réseau de machines compromises (dans 95% des cas, cela a un rapport avec IRC d'une façon ou d'une autre). L'intérêt est bien supérieur lorsqu'il s'agit d'utiliser une machine comme source, et les découvertes de BotNets (réseaux de clients de déni de service fonctionnant sur la base de drones IRC contrôlés) sur Renater sont en recrudescence, principalement sous systèmes d'exploitation Windows. Toujours en s'appuyant sur l'infrastructure de Métrologie mise en place au sein du GIP Renater, des outils ont été développés afin de signaler en temps réel tout déni de service potentiel survenant sur le réseau. Les critères de détection demeurent simples pour l'instant, mais efficaces : il s'agit principalement de seuils sur le nombre de flux envoyés ou reçus par un site (attaque par un grand nombre de petits paquets) ou sur le débit généré ou absorbé par un site (attaque par un petit nombre de gros paquets). En cas de dépassement des seuils, un mail est envoyé à une personne du CERT, et des flux extraits du trafic du site impliqué sont sauvegardés pour analyse ultérieure.

Cette méthodologie a permis de mettre à jour des machines compromises faisant partie de réseaux de dénis de service distribués, et ainsi de démanteler ces derniers.

Kostya Kortchinsky

Vendredi 23 janvier 2004 - Une augmentation anormale du nombre de flux en provenance d'un site connecté à Renater est détectée. Les informations extraites du Netflow de nos routeurs mettent en évidence une attaque en déni de service, utilisant un grand nombre de paquets SYN TCP (peu coûteux en bande passante), à destination d'une adresse IP et d'un port précis. La provenance exacte reste encore indéterminée puisque les adresses source des paquets ont été modifiées pour utiliser de façon aléatoire l'ensemble des adresses du sous-réseau incriminé. Les informations sont transmises au site en question ainsi qu'au réseau régional, afin que puisse être identifiée la machine à l'origine de l'attaque. D'autres dénis de service seront déclenchés pendant deux jours, ciblant différentes machines et services. L'ensemble du trafic est alors analysé à la recherche de traces suspectes, notamment de connexions IRC (couramment utilisées pour la constitution de réseaux de machines compromises). Une machine suspecte sort du lot suite à des connexions vers un serveur situé chez un fournisseur d'accès DSL américain, et une connexion au serveur révélera un unique canal non protégé regroupant l'ensemble des machines piratées. Les adresses IP des machines constituant le réseau sont chiffrées, mais il aura fallu moins d'une heure pour implémenter un programme se basant sur les sources d'UnrealIRCd permettant de recouvrer les adresses déchiffrées, qui ont été communiquées par la suite à leurs propriétaires respectifs. ■

La sécurité, c'est l'affaire de tous

Pour reprendre le titre de la présentation de David Crochemore sur le CERT Renater [1], la sécurité, c'est l'affaire de tous. Ainsi il appartient à chacun d'apporter sa pierre à l'édifice. Plusieurs moyens pour cela. Le premier : nous tenir informés de tout incident lié à la sécurité de votre système d'information ; de précieux renseignements se cachent dans toute compromission, que ce soit la méthodologie, les outils utilisés, le but recherché, autant d'éléments qui pourront aider d'autres sites par la suite. Vous pouvez aussi nous remonter de façon automatisée vos rapports de scans, les statistiques de vos plateformes antivirales, nous transmettre des informations sur des vulnérabilités potentielles, nous envoyer les disques durs de machines compromises pour analyse, et bien entendu, répondre à nos sollicitations lorsque nous vous contactons.

N'hésitez pas à nous contacter :
- par téléphone : 01 53 94 20 44 ;
- par courriel : certsvp@renater ;
- clé PGP du CERT Renater :
id d754e8cd fingerprint 021f9a79a180885bcd7a3e94718b34e0

[1] Renater en vidéo http://www.renater.fr/Video/CERT/Index.htm ■

Les évolutions

AFIN de développer une expertise plus spécifique dans le domaine de la sécurité des systèmes d'information, et apporter un peu de nouveauté aux initiatives similaires, nous nous sommes penchés sur quelques activités annexes : les pots de miel (honeypots), les tests d'intrusion, les formations (cette année, investigations de machines compromises), la recherche de vulnérabilités.

Depuis peu, le CERT Renater est membre du French HoneyNet Project (1), pendant français au projet américain HoneyNet Project. Le concept d'un honeypot, ou pot de miel en version française, est ludique et intéressant : il s'agit de mettre en place des systèmes ou réseaux de systèmes, virtuels la plupart du temps, dont la seule finalité est d'être compromis. Il est alors possible d'observer le compor- réponse page 6

La biométrie (suite)

Suite à l'article de Philippe Wolf sur la biométrie paru dans le numéro 46, M. Jacky Person nous écrit. (http://biometrie.online.fr/)

Il faut noter tout d'abord la grande difficulté de récupérer une image correcte d'empreinte à l'insu de l'intéressé. Les policiers en font l'amère expérience chaque jour quand ils doivent identifier le criminel à partir de traces d'empreintes trouvées sur le lieu de crimes. De plus, il faut trier parmi toutes les traces laissées par l'utilisateur dont on veut usurper l'identité, pour ne garder que l'empreinte du doigt à utiliser pour l'accès.

Par ailleurs, il existe des techniques permettant de déterminer si un doigt est vrai (n'est pas une copie) et vivant (n'est pas un doigt coupé) : oxymétrie, mesure de la résistance, etc. Ces techniques sont déjà largement répandues et opérationnelles dans d'autres contextes (service d'urgence d'hôpitaux, par exemple, pour l'oxymétrie). Cela devrait suffire à lever l'objection théorique sur la falsification des empreintes digitales. Si ces techniques ne sont pas encore implantées dans les produits vendus, c'est que cela augmente leur coût, qui ne correspondrait plus alors aux exigences du marché de la biométrie à ce jour. Il y a beaucoup d'usages pour lesquels le niveau de sécurité apporté par la biométrie dans l'état actuel est largement suffisant : accès à son PDA, son téléphone, dans certains cas son poste de travail, etc.

Il est vrai que sur un plan théorique, si la donnée biométrique est volée et publiée, elle est « grillée » à tout jamais, au contraire d'un mot de passe qui peut être régénéré. Mais sur un plan pratique, le mot de passe n'est pas un moyen totalement efficace : la fréquence des changements de mots de passe imposés par les systèmes, et le grand nombre de mots de passe (en moyenne quatre par utilisateur bureautique) amènent des comportements déviants. Dans toutes les campagnes de sensibilisation à la sécurité, il est recommandé de ne pas noter son mot de passe près de l'endroit où il est utilisé (post-it sous la souris, etc.), ce qui prouve bien que ce genre de comportements existe. Un autre comportement déviant est d'utiliser des mots de passe faciles à retenir, et donc faciles à craquer.

À l'analyse théorique de Philippe Wolf, j'oppose donc une analyse sur le plan pratique, qui met bien en évidence la faculté des outils biométriques de renforcer la sécurité d'un système existant, à condition bien sûr de les assembler de manière cohérente avec les autres éléments du système de sécurité existants.

JPIERSON@bouyguestelecom.fr
Jacky Pierson chef de projet SI Bouygues Telecom

RÉPONSE

Les réserves exprimées par l'article sur l'authentification biométrique proviennent du fait que l'authentifiant biométrique est une donnée publique (ce que n'est pas, par exemple, un bon mot de passe) et non révocable en cas de compromission (un mot de passe ou une clé se changent régulièrement).

Certains commentaires suscités par cet article soulignent les risques liés à ces deux caractéristiques (voir par exemple http://www.cecurity.com/cecurity/html/article_biometrique_donnee_publique.php) : « L'analyse de Philippe Wolf peut être confortée par l'observation du très grave phénomène d'usurpation d'identité aux États-Unis. Les banques avaient pris l'habitude d'accorder des crédits en ligne aux interlocuteurs qui étaient en mesure de communiquer leur numéro de sécurité sociale (avec le nom de jeune fille de leur mère). Or, ce numéro de sécurité sociale a vocation à être communiqué et enregistré en de multiples endroits et il ne peut pas être modifié. On a donc utilisé comme mot de passe ce qui était par nature un identifiant. Cette mauvaise approche sur le plan de la sécurité a été à l'origine d'une fraude phénoménale. »

Quant au leurrage des capteurs biométriques, dont vous admettez la faisabilité actuelle, des pistes (décrites, par exemple dans http://www.securiteinfo.com/conseils/biometrie.shtml et http://www.schneier.com/crypto-gram-0311.html) indiquent que le coût de ces leurres est de l'ordre du coût des capteurs, ce qui n'est pas acceptable (le faux doigt en gélatine alimentaire qui m'a été démontré et qui leurre certains capteurs du commerce est même d'un coût très inférieur). Seuls des travaux scientifiques sérieux (comme les travaux menés en cryptographie par la communauté internationale) sur ce sujet permettront d'évaluer les potentialités d'attaque de ces dispositifs et d'en mesurer l'apport réel dans la sécurisation des systèmes d'information.

Robert Longeon

suite de la page 5

tement du pirate in vivo, de suivre ses agissements, de récupérer ses outils. Le CERT Renater participe activement aux initiatives sur le sujet.

Concernant les tests d'intrusion, deux sites de la communauté Renater ont joué aux cobayes pour ce type de prestation qui consiste, entre autres, à tenter de s'introduire au sein d'un réseau, et compromettre un grand nombre de machines. Le test d'intrusion diffère fondamentalement d'un audit de sécurité classique puisque ne prenant en compte que les aspects techniques de l'architecture systèmes et réseaux, et en rien les aspects humains. Son succès requiert des compétences d'autant plus pointues. Les résultats ont été très positifs dans les deux cas, puisque soulignant de nombreux trous de sécurité dans les réseaux concernés permettent d'obtenir des accès privilégiés à des machines importantes, ainsi que l'obtention d'informations sensibles.

Organisée conjointement avec le CINES, une formation CiRen (2) de 3 jours sur le thème des investigations de machines compromises (investigations « forensiques ») s'est déroulée cette année à Montpellier. Le principe en était de fournir aux stagiaires des bases dans ce domaine en alliant une partie théorique et une partie pratique basée sur l'étude de machines compromises issues de nos travaux sur les HoneyNets.

Kostya Kortchinsky

(1) French HoneyNet Project
http://www.frenchhoneynet.org/
(2) Formations CiRen
http://www.cines.fr/textes/ciren.html

SÉCURITÉ INFORMATIQUE
numéro 48 avril 2004
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 4 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conseil et coordination : CNRS - DIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45210961