

Synthèse SSTIC 2005

Ce texte est © 2005 Bruno Kerouanton. Diffusion libre.

Introduction

Une fois de plus, la troisième édition du Symposium sur la Sécurité des Technologies de l'Information et des Communications ayant eu lieu ces derniers jours à l'ESAT aura été un très bon cru, tant de part la qualité des interventions que par le travail fourni par les organisateurs et l'ambiance générale due au public.

Durant ces trois jours, les différents intervenants ont pu brillamment présenter l'état de l'art en matière de lutte informatique, par le biais de présentations pratiques, retours d'expérience et résultats de travaux pour le moins impressionnants.

La recherche de vulnérabilités : un processus quasi industriel et lucratif.

Kostya Kortchinsky, responsable du CERT Renater et expert reconnu, démontre par le biais d'exemple concrets que malgré les efforts des éditeurs de logiciels à publier des correctifs de sécurité, il existera toujours un certain nombre de failles non résolues permettant d'attaquer des systèmes malgré tout un arsenal de contremesures, les « 0day exploits ». Un véritable marché parallèle concernant ces vulnérabilités s'est d'ailleurs développé dans les milieux souterrains et cybercriminels, chacune de ces failles sans correctif ayant une valeur estimée entre 10 et 50K\$.

Ce constat vient corroborer la présentation Halvar Flake qui a mis au point une méthode de comparaison structurelle permettant notamment de trouver des failles de sécurité dans les correctifs mis au point quelques heures auparavant par les éditeurs de logiciels, et ce de manière quasi automatisée. On rentre ainsi dans un processus d'industrialisation de la découverte des failles informatiques qui ne laisse pas insensible.

De plus, plusieurs présentations ont mis l'accent sur le manque de réactivité, voire carrément le désintérêt des éditeurs et concepteurs pour les vulnérabilités de leurs systèmes d'exploitation. Kostya Kortchinsky évoque un temps de réaction pouvant aller jusqu'à une année entre la découverte d'une faille et sa correction effective par l'éditeur. Le noyau Linux est lui aussi sur la sellette, Gaël Delalleau mentionnant des failles critiques liées à une mauvaise gestion de la mémoire des dernières versions de noyau Linux et surtout son incapacité à sensibiliser les auteurs du noyau face à ce problème. Même remarque pour Allain Yoann qui lors d'une Rump évoque une erreur fonctionnelle du noyau Linux lorsque Ipsec et Netfilter sont utilisés conjointement.. et qui n'a semble t'il toujours pas fait réagir leurs auteurs. Les systèmes de détection d'intrusion et les anti-virus ont également à ce titre un intérêt bien limité car ils détectent souvent les menaces bien trop tard.

Risque informationnel, cybercrime et légitime défense

L'expert en la matière, Christian Harbulot, a tiré la sonnette d'alarme en expliquant que de plus en plus d'entreprises étaient démunies face à l'accroissement réel d'attaques

informationnelles sous toutes leurs formes plus subtiles les unes que les autres. Il semble que cette activité lucrative rapporte (ou coûte suivant le côté où l'on se trouve) plus encore que les attaques informatiques classiques, mais les entreprises osant en parler sont extrêmement rares et il est difficile d'obtenir des chiffres. Ces attaques informationnelles peuvent parfaitement se combiner aux attaques informatiques classiques et font d'ailleurs souvent usage d'outils tels que les chevaux de troie, par exemple.

Dans le même ordre d'idées, Renaud Bidou cite un exemple intéressant d'une attaque informatique visant une entreprise russe, associée à du chantage et demande de rançon, pratique contre laquelle il existe finalement assez peu de solutions, et donc a tendance à augmenter.

Une initiative fort intéressante de part son aspect didactique a été présentée par Marc Dacier, il s'agit du projet Leurré.com. La mise en place d'un réseau de « pots de miel » mondialement distribué permettant de récupérer les tentatives d'attaque, puis la corrélation des événements associés a permis de démontrer quantitativement puis visuellement l'évolution des attaques, et l'influence de plus en plus importante des groupes cybercriminels organisés, notamment en mettant en évidence leurs relations et partenariats, ainsi que leurs méthodes sophistiquées de collecte d'informations puis d'attaque réparties dans le temps.

On pourrait imaginer des parades à de telles actions malveillantes, et pourquoi pas la riposte dans le cadre de la légitime défense, mais Thiébaud Devergranne nous présente la réalité juridique, qui est bien simple : cela reste une utopie et si une victime informatique se mettait à contre attaquer en évoquant la légitime défense, elle aurait bien des difficultés à justifier son action face au législateur. Quant aux systèmes de riposte automatisés, ils sont tout simplement à bannir car pouvant mettre en péril l'infrastructure et risquant d'attaquer à leur tour d'innocentes victimes.

Preuves informatiques ?

Une présentation intéressante soumise par Laurent Roger visait à énumérer l'ensemble des mesures théoriques et réelles permettant de ralentir, voire de stopper les investigations post-mortem effectuées par des experts en recherches de preuves informatiques.

Deux aspects étaient évoqués : d'une part les techniques avancées de camouflage des traces sur un système en cours de fonctionnement afin de masquer une intrusion, et d'autre part les techniques permettant de cacher des données sur une mémoire de masse de manière efficace, tout en rendant les outils de récupération et d'analyse de disques inopérables ou inadéquats.

Cela met en valeur le danger potentiel lié au fait que la majorité des experts judiciaires s'appuient sur des outils et procédés bien connus mais faillibles, et que leur constat peut par conséquent être faussé, mettant à mal l'instruction judiciaire en cours. En extrapolant, il ne serait a priori pas plus difficile d'introduire de fausses preuves tout en masquant les siennes afin de brouiller les pistes. On imagine déjà avec stupeur l'erreur judiciaire...

Télécommunications, voix sur IP et téléphonie mobile

Michel Morvan détaille les motivations et pratiques courantes employées par les cybercriminels de tous types, leur permettant d'attaquer les téléphones mobiles pour les perturber, y introduire virus et chevaux de troie, les débloquent ou bien subtiliser carnets d'adresses et codes pin.

Un outil conçu et présenté par Nicolas Bareil a suscité la curiosité, puisqu'il permet d'intercepter des conversations utilisant la téléphonie sur IP (VoIP), d'injecter des fichiers sonores, de récupérer les informations de signalisation, y compris les touches pressées par l'utilisateur (pour récupérer un code PIN ou un numéro de carte bancaire par exemple). Il est clair que face à cette menace il vaut mieux utiliser des réseaux segmentés et du chiffrement...

Rump sessions et démonstrations

La fin de la seconde journée a été marquée par un grand nombre de mini présentations de qualité, les « Rump Sessions ». Celles-ci, au nombre de 14 cette année, ont eu pour but de présenter un thème, un point précis, des résultats de travaux etc, le présentateur n'ayant qu'une contrainte réelle, celle de finir en moins de cinq minutes. Parmi les Rump sessions les plus remarquées, on notera :

Un outil au nom sympathique ayant suscité l'hilarité lors de la présentation, « Oupa », qui a enregistré toutes les communications wifi au sein du Sstic deux jours durant, afin de présenter à l'aide de graphes et de tableaux les flux de communication hostiles entre les différents PC présents dans la salle. Instructif !

Toujours en Wi-Fi, un mécanisme sophistiqué d'insertion d'un PC dans un réseau sans fil ne nécessitant pas d'association au point d'accès et rendant par conséquent l'opération totalement invisible. Cela permet donc de lancer des attaques ou d'usurper un compte payant sur un hotspot, démonstration à l'appui.

Une démonstration d'un outil d'attaque des téléphones mobiles via bluetooth, permettant notamment de récupérer les carnets d'adresses stockés en temps réel et sans connaissance du mot de passe.

Un certain nombre de chevaux de Troie particulièrement perfides, le premier s'intégrant totalement dans le navigateur Internet et étant totalement furtif y compris au niveau de la transmission des flux réseaux, et le second capable d'analyser les codes saisis sur des claviers virtuels affichés à l'écran, mettant à mal les dernières solutions des banques qui pensaient déjouer les « keyloggers ».

Une sensibilisation au fait que de plus en plus de constructeurs intègrent des ressources et fonctions cachées dans du matériel, en l'occurrence ici dans les cartes mémoire SD, et permettant notamment de chiffrer les données ou d'authentifier les périphériques autorisés par le biais d'une PKI, l'utilisateur assumant le coût de ces fonctions dont il n'a pas le droit d'avoir l'usage.

Conclusion

A l'issue de ces trois jours denses en contenus et en émotions, force est de constater que la grande majorité des interventions étaient d'une haute qualité, mettant brillamment en exergue les capacités de certaines personnes à contourner l'ensemble des mesures de protection couramment employées dans les organismes privés ou publics, sans difficulté majeure et de manière parfois automatisée.

Anti-virus ou non, pare-feux ou non, correctifs appliqués ou non, cela ne fait presque aucune différence pour les personnes réellement intentionnées souhaitant pénétrer à l'intérieur d'un réseau privé pour y dérober, corrompre des données ou perturber l'activité sans même laisser de traces et rendre l'analyse et la recherche de preuves très difficile.

Les quelques managers présents dans la salle venus pour la première fois au Sstic ont certainement dû pâlir et repartir avec quelques cheveux blancs de plus ! En effet face à de telles menaces il ne semble pas exister de solution simple, la plupart des organismes et entreprises n'ayant pas les budgets, compétences et surtout la possibilité technique leur permettant de se protéger face à des attaquants déterminés. Leur priorité étant bien évidemment de maintenir la productivité au détriment de la sécurité.