Labo Sophos: une journée chez un traqueur de virus

Dans le saint des saints d'un éditeur d'anti-virus, lieu de tous les dangers, l'atmosphère est à la concentration et le silence est roi. Attention aux erreurs de manipulation…

Le '**virus lab**' de Sophos ou laboratoire de tests de virus, est constitué de trois entités géographiquement distinctes pour l'observation et l'identification des virus: Boston, aux Etats-Unis, Sidney, en Australie, et le plus important au siège à Oxford, en Grande-Bretagne. C'est un choix stratégique: le but est de couvrir la planète sur l'ensemble des créneaux horaires, soit trois fois 8 heures. **Ce qui rentre ne sort plus !** Pour pénétrer au coeur du '*virus lab*', vous êtes invité à laisser vos outils de travail à l'extérieur. Car hormis les humains, tout ce qui rentre ne ressort plus. Les '*virus labs*' figurent en effet parmi les lieux les plus exposés au monde – du moins dans cette matière? Si un ordinateur en sort, et qu'il renferme une souche virale, c'est l'ensemble des réseaux mondiaux qui risque d'en pâtir. Alors, les mesures de prophylaxie sont draconiennes: pas de PC portable ni de PDA! Et si vous souhaitez communiquer par e-mail, des ordinateurs vous attendent à l'extérieur du laboratoire. D'ailleurs, des ordinateurs s'entassent dans un coin du laboratoire, beaucoup de machines obsolètes ? nous avons revu avec nostalgie un Amstrad PC 1640 à disquettes 5 pouces, par exemple (*voir nos photos à la fin de l'artcile*) ? car la sacro-sainte règle demeure : ce qui rentre ne sort pas ! **Il y a virus et virus. Ne confondez pas !** Une première surprise nous attend ! Le laboratoire est un plateau de travail qui ressemble à tous les autres, avec des bureaux, des ordinateurs ? deux fois plus qu'ailleurs, certes – et des opérateurs qui s'activent. Nous nous attendions, image traditionnelle, à une salle blanche fréquentée par des individus vêtus de combinaisons isolantes? La confusion est classique, nous explique Vanja Svajcer, jeune *principal virus researcher* chez Sophos, elle provient de l'expression **virus**, beaucoup plus ancienne dans son contexte médical, et qui dans l'esprit des gens renvoie à l'image du virus biologique. En informatique, un virus n'est qu'un programme ! Pourtant en pénétrant dans ce lieu ultra-protégé, nous ne pouvons nous empêcher de ressentir comme un frisson. Certes, il n'y a pas de menace biologique ici, mais l'atmosphère très sécurisée et contrôlée vous laisse imaginer la réalité d'un danger physique ! **90% des virus ne seront jamais rendus publics** La seconde surprise provient des occupations menées par les traqueurs ('trackers'). Nous les imaginions surfant sur le Web ou consultant des masses de données à la recherche de souches virales numériques camouflées. Eh bien non! La chasse aux virus revêt un caractère plus prosaïque: nous apprenons qu'elle est essentiellement nourrie par la délation ! Autre information inédite: 90% des virus ne seront jamais rendus publics, et ne menaceront jamais personne ! Mettons à part les virus spammés, livrés avec les e-mails et qui peuvent être détectés simplement parce qu'ils vont envahir les messageries anonymes des chasseurs de virus et de spam. En réalité, la quasi-totalité des virus sont d'abord des macro-commandes ou de courts développements écrits en Visual basic, et sont révélés par leurs auteurs. Là aussi une explication s'impose : un virus reste un programme, et beaucoup de développeurs créent des programmes, sans toujours en maîtriser le résultat. En procédant innocemment à l'écriture d'un programme 'buggé' ou non conforme aux procédures de protection, ils peuvent être, à leur insu, les géniteurs d'un virus. D'autres développent sciemment des virus, mais dans un but purement technologique. D'autres enfin testent les applications du marché, et

ont fait de la découverte de failles, et des outils permettant d'en abuser, un sport international. A noter que ceux-là ne cherchent pas toujours à en tirer profit. La très grande majorité des virus sont donc détectés sur indication ou dénonciation ! Et ils ne franchiront jamais les limites des '*virus labs*' **De la curiosité, du flair et des outils** Autre surprise, démentant un lieu commun: il n'y a pas de 'hackers' (pirates informatiques) chez Sophos. L'image du pirate acheté à prix d'or pour qu'il livre ses dons et ses techniques, appartiendrait à la légende. Pourtant, comme dans toute légende, une partie de l'histoire est vraie, mais pas chez les éditeurs d'anti-virus -déclarent les responsables de Sophos. La tentation serait certainement trop grande de profiter de l'immense base de codes vérolés découverts par l'éditeur pour développer de nouveaux virus capables de contourner les méthodes développées afin de les repérer. Sophos ne veut pas prendre ce risque. Les traqueurs sont jeunes, de profil universitaire. On leur demande d'adopter plutôt une démarche scientifique, mathématique, de faire preuve de curiosité, mais aussi d'un sens du détail. Et d'imagination aussi, afin de pouvoir mimer l'action du virus. **Des machines vérolées, encore, encore, ?** Devant chaque traqueur, plusieurs ordinateurs s'additionnent. L'un d'entre eux est ceinturé d'un bandeau rouge, ce qui permet de l'identifier au premier coup d'?il. C'est le poste sain, celui sur lequel le virus sera décrit et à partir duquel partira l'information qui permettra d'assurer la mise à jour de l'anti-virus. Les autres postes, avec les systèmes d'exploitation multiples, car les virus concernent tout le monde, sont étiquetés en jaune avec la mention 'virus' (*voir notre photo*). C'est là que les fichiers suspects sont testés à l'aide d'un moteur de détection virale et d'une technologie maison brevetée: InterDeck. Le traqueur va isoler les fichiers à risque et ouvrir leur code. Les codes 'ascii' sont déchiffrés. Un bon traqueur est capable de repérer, dans les descriptions qui sont associées à ce code, des souches virales, ou alors les commentaires que les auteurs du virus ne manquent pas de faire figurer, histoire de signer leur ?uvre. Le processus de traitement anti-virus se révèle finalement assez simple: on extrait un échantillon du code douteux, on l'analyse, on détecte la présence de code frauduleux, on teste le code, et enfin on publie l'information. Si l'énigme n'est pas résolue, on recommence ! Si le programme ne présente pas de danger, on ne l'oublie pas pour autant: on le range, c'est tout ! **Signatures et coopération** Chaque virus possède sa signature, une partie de code qui sert à le différencier de ses petits copains. Tout du moins *chaque éditeur d'anti-virus définit la signature qui sera affectée au virus*. La nuance est d'importance ! La signature est l'indicateur du virus qui sera stocké dans le programme anti-virus ou dans sa mise à jour, et qui servira ensuite à le détecter. Si une même signature peut être associée à plusieurs virus, tant mieux, ce sera autant de code en moins qui n'alourdira pas l'anti-virus. Les signatures de virus sont donc spécifiques à chaque logiciel anti-virus, ou tout du moins éditeur. C'est la raison pour laquelle il peut être dangereux d'utiliser deux anti-virus sur un même poste. Ce qui définit un danger chez l'un peut marquer un programme sain chez l'autre ! En plus des incompatibilités et conflits, le risque est alors grand que les signatures se chevauchent, et plantent une application innocente ou même un poste ! Pourtant, les éditeurs coopèrent. L'information circule entre eux, mais pas les signatures? Les souches sont échangées afin que chacun puisse définir sa signature et protéger ses clients. Une problématique demeure, cependant: le nommage des virus. Un même virus découvert et annoncé en même temps par plusieurs '*virus labs*' pourra ainsi porter plusieurs noms. **Ici: 800 virus découverts et mis à jour chaque mois !** Les '*virus labs*' de Sophos découvrent en moyenne 800 virus par mois, soit environ 30 par jour! En fait, pour arriver à ce résultat, 3.000 analyses environ sont réalisées dans le mois, ce qui démontre que sur les fichiers '*à risque*' qui parviennent à Sophos ou sont détectés par lui, à peine un quart se révèlent présenter une menace. Ces fichiers doivent être détectés le plus rapidement possible, afin de renseigner les développeurs de l'anti-

virus qui vont mettre à jour leur programme. Il faut de quelques minutes à quelques semaines à un traqueur pour tester un exécutable et identifier la présence d'un virus. Il faudra ensuite le tester, découvrir son mode de fonctionnement et le documenter. Puis les développeurs vont définir sa signature, et l'intégrer dans leur programme. Il restera à valider la description et tester la désinfection avant de l'intégrer dans la mise à jour suivante, plusieurs quotidiennement. Ce temps est d'une demi-heure pour les macros ou les modules en Visual Basic. Il est porté à deux heures pour un virus sous Windows 32 bits, voire plusieurs jours si ce virus se révèle complexe. Un nouveau type de virus, comme ceux qui se lancent sans passer par un fichier exécutable, peuvent par contre demander plusieurs semaines. Quant à la disponibilité de la mise à jour, si la menace est d'importance et nécessite une procédure d'urgence, elle peut prendre moins de 2 heures. Chez Sophos, le '*virus lab*' est sans doute le lieu où la pression est la plus palpable, ne serait qu'en raison du silence de plomb qui y règne. Le traqueur y joue un rôle stratégique, car c'est lui qui est en charge du test et de la validation des virus. Une erreur, un détail qui lui échappe et c'est un monstre qui reste en liberté. On reste traqueur deux ans, voire trois ans chez Sophos. Car ensuite on passe à autre chose? La maintenance en ligne par exemple.