Compte-rendu de réunion

Référence RéSIST/2011-03

31 mars 2011

Table des matières

1 Tour d'horizon

La réunion a débuté par un rapide tour d'horizon de M. Fabrice Prigent sur quelques événements récents sur le plan de la sécurité informatique. Il a notamment parlé de la compromission de certificats SSL produits par Comodo, au travers d'un des fournisseurs de ce dernier (RapidSSL).

Au moins neuf certificats « significatifs » ont été compromis, dont `login.live.com`, `mail.google.com`, `www.google.com`, `login.skype.com` et `addons.mozilla.org`. Les certificats compromis ont été révoqués par des listes noires dans les navigateurs, mais pas via OCSP (Online Certificate Status Protocol). Cela signifie implicitement que les certificats compromis ne seront reconnus comme tels que si l'utilisateur met à jour son navigateur. Deux greffons pour Firefox ont été évoqués (`perspectives` et `certpatrol`), qui réalisent un ensemble de contrôles sur les certificats (valides ou non).

Fabrice a ensuite évoqué la compromision de RSA et SecurID, les failles XSS sur le site de McAfee et quelques autres informations.

2 Nomadisme et sécurité

La première présentation a été faite par M. Clément Saad, de la société Pradéo (`www.pradeo.net`).

M. Saad a commencé par évoquer la « situation » des travailleurs nomades[1]. Ces derniers seraient potentiellement un milliard en 2012. En 2009,

1. Au sens informatique du terme.

Rédigé par Pierre-Yves Bonnetain -– pyb@ba-consultants.fr
ReSIST -– http://www.ossir.org/resist
Comptes-rendus -– http://www.ossir.org/resist/supports/index.htm

le nombre d'ordinateurs portables vendus en une année a dépassé celui des ordinateurs fixes. Il est estimé qu'en 2013 il se vendra deux fois plus d'ordinateurs portables que d'ordinateurs fixes. Ces chiffres ne prennent pas en compte le nombre de *smartphones* vendus (525 millions en 2010).

Les ordinateurs portables Les situations de sécurité, entre un ordinateur fixe et un ordinateur mobile, sont très contrastées :

sur le plan de la protection un ordinateur fixe dispose d'une dizaine de modules de protection, y compris dans l'architecture qui l'accueille. Un ordinateur mobile, notamment en situation de mobilité, n'en a guère que deux (l'anti-virus et le pare-feu locaux)

sur le plan de la supervision les ordinateurs fixes peuvent être suivis et supervisés en temps réel ou presque, avec levée d'alertes en cas d'incidents. À l'inverse, il est nécessaire d'attendre qu'un ordinateur mobile reviennent au sein de l'entreprise pour qu'il puisse être supervisé et contrôlé.

Il existe de très nombreux exemples de systèmes mobiles qui se font attaquer en situation de mobilité, et attaquent l'entreprise lorsqu'ils reviennent au sein de cette dernière.

Le schéma classique d'utilisation d'un VPN pour toutes les connexions des ordinateurs mobiles revient à centraliser (sur le serveur VPN) tous les traitements de sécurité. Si une telle solution présente d'indéniables avantages, elle a aussi de nombreuses limites.

La société Pradéo développe des logiciels (PradeoKey et Smart-NS notamment) dont l'objectif est de ramener les contrôles et traitements de sécurité au plus proche du poste nomade. La PradeoKey, orientée mono-utilisateur, est une clé USB « tout-en-un » offrant un ensemble de logiciels de sécurité et de supervision – et interdisant tout accès au réseau lorsqu'elle n'est pas branchée. Smart-NS offre les mêmes fonctionnalités, mais pour un parc d'ordinateurs, avec une plate-forme de pilotage à distance.

Dans les deux cas, il s'agit de mettre en œuvre sur les ordinateurs à protéger des machines virtuelles (sous GNU/Linux, avec Snort, ClamAV, netfilter, squid, squidguard…). Vis-à-vis du réseau, ces machines virtuelles se substituent totalement au poste de travail. Elles servent, en coupure, de relais et passerelle entre le réseau et le poste local. Au démarrage, ces machines virtuelles reconfigurent l'interface réseau du poste de travail afin de garantir l'interception de tous les paquets par la machine virtuelle.

Les deux produits permettent aux administrateurs de définir des *seuils d'hostilité* au-delà desquels le poste de travail va perdre un certain nombre de ses possibilités d'utilisation du réseau. Il ne s'agit pas de « punir » l'utilisateur du poste, mais de reconnaître que son ordinateur se trouve dans un environnement hostile et d'agir en conséquence. Cette isolation peut aller jusqu'au blocage de l'accès au réseau (et de l'accès du réseau au poste de

travail) dans les cas les plus sérieux. L'isolation du nomade peut n'être que partielle, en fonction de la configuration définie par l'administrateur.

Dans le cadre d'utilisation de Smart-NS, ces seuils d'hostilité et leurs franchissement sont remontés vers la plate-forme de pilotage, permettant aux administrateurs de connaître très rapidement le niveau d'hostilité de chacun des ordinateurs ainsi supervisés.

Et les *smartphones* ? La sécurisation des *smartphones* pose des difficultés particulières, car les constructeurs signalent tous que l'installation de programmes usant de privilèges étendus annule la garantie de l'équipement. Cela implique qu'un logiciel de sécurité, si l'utilisateur souhaite conserver la garantie associée à son terminal, ne pourra jamais « tout voir » sur le *smartphone*. Typiquement, un anti-virus ne pourra pas voir un fichier système infecté, puisqu'il ne disposera pas des droits d'accès appropriés.

3 Méthodes d'identification de fichiers connus

La seconde présentation a été faite par M. Pierre-Yves BONNETAIN, de la société B&A CONBSULTANTS (www.ba-consultants.fr).

Cette présentation a eu pour objectif d'illustrer une extension des méthodes de recherches de fichiers connus sur des supports de stockage. La méthode proposée peut être étendue afin de détecter l'échange, au travers d'un réseau, de fichiers particuliers.

La recherche de fichiers connus correspond par exemple à une enquête lorsque l'on pense qu'un collaborateur a fait une copie d'un fichier de l'entreprise (fichiers clients, documents confidentiels, etc.) sur un support identifié (clé USB, ordinateur personnel, smartphone...).

Techniques classiques de recherche La présentation a débuté par un rappel des techniques « courantes » pour rechercher des fichiers connus. Il s'agit de recherche qui peuvent reposer sur le système de fichiers (fichiers présents), ou qui traitent tout l'espace de stockage (fichiers présents ou effacés).

Dans le premier cas, la recherche repose sur une caractéristique (ou plusieurs) des fichiers, souvent le nom ou le contenu (via un condensat de celui-ci). Ces techniques de recherche se heurtent à deux écueils importants. Si le fichier a transité sur l'ordinateur inspecté mais a été effacé, il ne sera pas trouvé. Et si la caractéristique sur laquelle repose la recherche a été modifiée (nom, contenu, etc.), le fichier ne sera pas trouvé non plus.

Dans le second cas, des outils spécialisés comme `photorec` extraient du support de stockage des fichiers, typiquement en identifiant leurs en-têtes (JPEG, MP3, ODT...). Charge ensuite d'examiner ces fichiers pour voir s'ils correspondent à ceux que l'on recherche. Ces techniques de *data-carving* sont

efficaces notamment si le fichier a été effacé, mais présentent un taux de faux positifs élevé : le nombre de fichiers à examiner et à valider est significatif. En outre, l'extraction de données repose sur des hypothèses comme la continuité des blocs de stockage (qui peut ne pas être vérifiée, auquel cas seul le début du fichier est correct), la non-compression, etc. Enfin, plus le transit du fichier recherché est ancien, plus la probabilité d'en retrouver l'en-tête (qui déclenche l'extraction des données) diminue.

Recherche par blocs La recherche par blocs repose sur le constat de l'existence de « blocs discriminants » dans des fichiers. Un bloc discriminant est un bloc à forte entropie, dont on considère qu'il est unique et distinctif. Si le fichier englobant est lui-même le produit d'un processus à forte entropie (photographie, vidéo, compression ou chiffrement sont de bons exemples), il est très probable qu'il contienne des blocs discriminants. Il se peut même que tous les blocs du fichier soient discriminants.

Il suffit alors d'identifier, sur le support examiné, un seul bloc discriminant du fichier originel pour avoir la certitude que le dit fichier a transité sur le support. Il peut d'ailleurs toujours y être présent (auquel cas de nombreux autres blocs seront identifiés) ou avoir été effacé (si tous ses blocs de stockage n'ont pas été recyclés).

Il convient de s'assurer que les blocs que l'on identifie sont réellement discriminants. Un bloc rempli de zéros ne répond pas à ce critère.

La recherche de fichiers connus revient alors à un pré-calcul des condensats des blocs constituant les fichiers concernés. Seuls ces condensats doivent être fournis aux investigateurs, les fichiers originaux n'ont pas à être fournis. Cela peut se révéler important, selon le contenu des fichiers en question.

Optimisation statistique Une recherche extensive sur un support de stockage de 1To peut se révéler particulièrement longue. Si l'on considère qu'il suffit d'un seul bloc trouvé pour permettre de conclure au transit de l'un des fichiers recherchés sur le support de stockage, une recherche par échantillonnage bien calibrée peut apporter la réponse. Il suffit donc, plutôt que de lire séquentiellement tous les blocs de stockage du support, de lire aléatoirement un certain nombre de blocs.

En ne lisant pas l'intégralité du support, le risque de faux négatif (qui reviendrait à dire de façon erronée que le fichier n'est pas présent et n'a pas transité sur le support) devient le critère prépondérant du travail. Il faut maîtriser cette probabilité.

La troisième partie de la présentation a présenté les éléments statistiques permettant de déterminer, pour une taille de support et une taille des fichiers recherchés, le nombre d'échantillons à prendre sur le support pour atteindre une certaine probabilité de succès (ou pour passer la probabilité de non-détection en dessous d'un certain seuil).

Les calculs montrent par exemple que la recherche du transit d'un fichier de 100 Mio sur un support de 1,5 Tio peut se faire en moins de deux secondes, avec une probabilité de faux négatif inférieure à 0,005% (cela suppose une excellente performance du disque, ce qui est rarement le cas sur des accès aléatoires).

Des mesures réalisées sur un support de 100 Gio, pour rechercher des traces d'un fichier de 100 Mio, donnent des résultats en une minute environ, avec une probabilité de faux négatif de l'ordre de 0,007%.

En cas de résultat positif, l'investigation technique peut être terminée en quelques minutes (surtout si les outils identifient de nombreux blocs). En cas de résultat négatif, si l'enquêteur craint que ce soit un faux négatif, il demeure toujours la possibilité de réaliser une recherche complète sur tous les blocs du support de stockage.