Plateforme distribuée de pots de miel haute-interaction et résultats expérimentaux

Ivan Studnia[1,2], Vincent Nicomette[1,3], Mohamed Kaâniche[1,2] et Eric Alata[1,3]
[1]CNRS, LAAS, 7 Avenue du colonel Roche, F-31400 Toulouse, France,
[2]Univ de Toulouse, LAAS, F-31400 Toulouse, France
[3]Univ de Toulouse, INSA, LAAS, F-31400 Toulouse, France
Email: {studnia,nicomett,kaaniche,ealata}@laas.fr

***Résumé*—La multitude d'activités malveillantes s'exécutant sur le réseau Internet est aujourd'hui un problème crucial. Afin de mieux comprendre les objectifs et modes opératoires des attaquants, il est nécessaire de collecter des données relatives à leurs activités. Leur analyse permet ensuite de mieux anticiper de nouvelles menaces et de mieux adapter les mécanismes de défense correspondants. Cet article propose une plateforme distribuée de pots de miel haute-interaction déployée dans cet objectif. Nous décrivons 1) le fonctionnement de cette plateforme, 2) la façon dont les données relatives aux activités malveillantes sont collectées, et 3) les premières analyses faites à partir de ces données.**

I. Introduction

Le développement très rapide d'Internet (près de deux milliards d'utilisateurs en 2010 selon l'Internet World Stats[1]) a fait apparaître de nombreux services accessibles en ligne, ainsi que de nombreuses communautés d'internautes. L'importance prise par ce réseau est telle que des règles et même des lois ont été créées afin d'assurer son bon fonctionnement. En effet, certains utilisateurs détournent l'outil informatique à des fins malveillantes en exploitant des failles matérielles ou logicielles. Ces pirates informatiques veulent ainsi pouvoir accéder à des données confidentielles, prendre le contrôle de machines ou diffuser des logiciels malveillants (vers, chevaux de Troie…). Par conséquent, des contre-mesures ont été développées pour tenter de combler ces failles et contrer les attaques, obligeant continuellement les pirates à rechercher de nouvelles vulnérabilités et imaginer de nouvelles attaques pour les exploiter. Ainsi, attaquants et experts en sécurité sont dans une perpétuelle course de type attaque-défense[1].

Il est donc primordial de connaître les stratégies utilisées actuellement par les pirates afin de parer au mieux les prochaines attaques et d'élaborer des nouveaux mécanismes de protection adaptés. Il faut pour cela collecter le plus d'informations possibles sur les pirates informatiques. Un certain nombre de techniques sont aujourd'hui employées dans cet objectif. On peut citer par exemple :

1) Les initiatives de centralisation de données recueillies par des sondes qui récupèrent les données fournies par divers équipements comme des routeurs ou des pare-feux[2][3].
2) La mise en place de "leurres", d'abord manuellement [2], puis de manière automatique, afin de piéger un pirate pour pouvoir l'observer.

C'est l'automatisation de ce dernier aspect qui nous intéresse ici, à travers la notion de "pot de miel" (*honeypot*). La définition généralement admise est celle de L. Spitzner[3] : *A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.* Ici, nous employons ce terme pour parler d'un système informatique connecté au réseau Internet, volontairement vulnérable dans le but d'attirer les attaques et d'analyser des informations sur leurs caractéristiques (protocoles employés, failles exploitées, programmes utilisés…). Il existe une grande diversité d'implémentations de pots de miel [4], [5]. Historiquement regroupées en deux catégories : haute [6] ou basse [7] interaction, selon les possibilités offertes à l'attaquant de nouvelles tendances font leur apparition (comme celles décrites dans [8], [9] ou [10]). Nous proposons dans cet article une description d'une plateforme de collecte de données utilisant différents pots de miel haute interaction répartis sur différents sites géographiques, ainsi que les premières analyses des données collectées. Ce déploiement fait suite à une première expérimentation qui avait été menée dans le seul contexte du LAAS avec le même pot de miel (cf. [11]). Il a pour but de vérifier si les conclusions obtenues de la première expérimentation sont bien généralisables ou si le comportement des attaquants varie selon la localisation du pot de miel attaqué.

Cet article est construit comme suit. Nous présentons le pot de miel haute interaction que nous avons conçu et implémenté dans le cadre de ces expériences. Les données collectées et la façon dont elles sont gérées et stockées sont ensuite présentées dans la section III. La section IV détaille l'architecture et le fonctionnement de la plateforme distribuée de pots miel que nous avons conçue et déployée pour cette expérimentation. La section V présente les résultats des premières analyses qui ont été faites sur les données collectées. Enfin, la section VI propose une conclusion à ce travail.

II. Le pot de miel haute interaction

Le pot de miel n'étant pas le point central de cet article, nous en donnons seulement ici les caractéristiques principales.

[1]www.internetworldstats.com/stats.htm
[2]www.dshield.org
[3]www.symantec.com/about/profile/universityresearch/sharing.jsp

Nous invitons le lecteur à consulter [11] pour de plus amples informations.

Le pot de miel développé au LAAS a pour but d'enregistrer les activités malveillantes effectuées par des êtres humains principalement, en plus des activités pouvant être mises en oeuvre par des outils automatiques. C'est pourquoi la décision a été prise de choisir des vulnérabilités plus facilement exploitables par des êtres humains. La vulnérabilité retenue est la création dans un système `GNU/Linux` de comptes utilisateurs ayant des mots de passe simples à deviner et accessibles via le service `ssh`.

Afin d'obtenir le plus haut niveau d'interaction possible, plusieurs machines sont disponibles pour les attaquants. Les systèmes physiques étant coûteux et complexes à administrer, nous avons opté pour l'utilisation de machines virtuelles. Les informations retenues afin de pouvoir reconstituer les scénarios d'attaques sont :

- Les couples (nom d'utilisateur, mot de passe) tentés par l'attaquant.
- Les caractères tapés par l'attaquant ainsi que ceux qui s'affichent sur son terminal. Cela permet de connaître les commandes entrées par l'attaquant.
- Les fichiers exécutés par le système d'exploitation, dans le cas où la liste des caractères ne suffirait pas à déterminer cela (raccourcis clavier ou programme en appelant d'autres par exemple).

Afin de pouvoir collecter toutes ces données, les noyaux des machines virtuelles ont été modifiés : 1) modification du pilote `tty` qui fournit les routines de lecture et d'écriture sur le terminal d'un utilisateur distant (de façon à pouvoir sauvegarder le contenu des terminaux) ; 2) modification de la routine d'exécution des programmes, afin de récupérer la liste des fichiers exécutés par l'attaquant ; et 3) création d'un nouvel appel système qui permet au serveur `ssh` s'éxécutant dans l'espace utilisateur de stocker des données dans l'espace noyau (les couples logins/mots de passe notamment).

Les données capturées sont temporairement stockées dans la mémoire du noyau des machines virtuelles. Ces informations sont ensuite récupérées périodiquement sur la machine hôte et stockées dans des fichiers. Ces fichiers sont ensuite transférés sur un serveur de base de données pour analyse.

La figure 1 présente l'architecture de notre pot de miel.

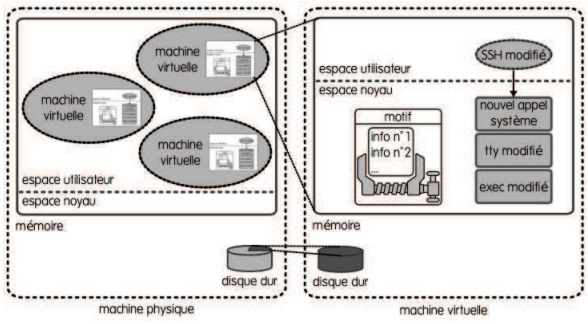

Fig. 1. Implémentation du pot de miel

III. Collecte et stockage des données

Les données extraites des pot de miel sont stockées dans une base de données dans un format permettant de faciliter l'accès aux données et les analyses qui vont suivre. La structure de la base de données est brièvement représentée en figure 2. Nous allons simplement ici décrire les tables les plus importantes pour nos analyses. Nous invitons le lecteur à consulter [12] pour plus de détails.

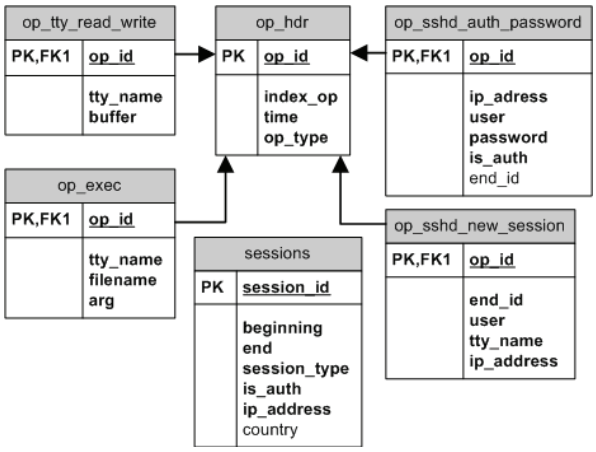

Fig. 2. Schéma de la base de données d'un pot de miel

La table `op_sshd_auth_password` contient les données relatives à toutes les tentatives de connexion `ssh`. La signification des différents champs est la suivante :

- `ip_address` est l'adresse IP source de l'attaque.
- `user` est l'identifiant utilisé lors d'une tentative.
- `password` est le mot de passe tenté avec l'identifiant
- `is_auth` indique si la tentative de connexion a réussi
- `end_id` indique, si la connexion a réussi, l'identifiant de la dernière action répertoriée lors de cette attaque.

La table `op_sshd_new_session` est renseignée quand une connexion `ssh` a abouti. Relativement similaire à `op_sshd_auth_password`, elle ne contient que des informations sur les attaques pendant lesquelles l'ouverture d'un terminal a été requise. La colonne `tty_name` indique le terminal attribué à l'attaquant. Cette information va nous servir à relier les données fournies par le pilote `tty` modifié à celles collectées par le serveur `ssh`.

La table `op_tty_read_write` contient toutes les informations enregistrées par le pilote `tty`. Une ligne contient ainsi le contenu du buffer de `tty` ainsi que le terminal auquel il est destiné. Lorsque les données concernent des entrées faites au clavier par l'attaquant, le buffer ne contiendra qu'un caractère à la fois. En revanche, si le texte a été copié/collé, le buffer contiendra plusieurs caractères. Il est ainsi facile de faire une première observation du comportement de l'attaquant.

La table `op_exec` contient les données concernant les programmes exécutés par la machine lors d'une intrusion. Une entrée correspond au nom du programme exécuté, aux arguments qui lui sont passés et au terminal dans lequel il s'est exécuté.

Une fois la base remplie, des tables `sessions` peuvent être créées et mises à jour. Ces tables contiennent les données issues du regroupement des connexions `ssh` en sessions d'attaques. Le principe de ce regroupement est le suivant : les connexions `ssh` issues d'une même adresse IP et rapprochées dans le temps sont regroupées[4] en sessions afin de reconstituer l'activité d'un attaquant. Trois catégories de sessions sont ensuite distinguées :

- L'attaquant a réussi à se connecter et des commandes ont été exécutées sur le pot de miel. Ce sont des *intrusions*.
- Il n'y a pas eu de commandes exécutées, mais une grande quantité de couples (identifiant, mot de passe) ont été tentés. Ce sont des *attaques par dictionnaire*.
- Les sessions ne rentrant pas dans les deux cas précédents sont regroupées dans la catégorie *autres*. Elles correspondent probablement à des "erreurs de connexions".

Les tables `sessions` vont ainsi contenir :

- `beginning` et `end` indiquent les identifiants des évènements de début et de fin d'une session.
- `session_type` indique si l'attaque est une intrusion, une attaque par dictionnaire ou aucune des deux.
- `is_auth` vaut 1 si au moins une tentative de connexion a réussi lors de la session, 0 sinon.
- `ip_address` est l'adresse IP source de l'attaque.
- `country` indique le pays correspondant à cette IP.

Une interface graphique de gestion a été développée de façon à faciliter le traitement et l'analyse des données stockées dans notre base de données.

IV. Plateforme de pots de miel

Notre objectif vise le déploiement des pots de miel à divers endroits dans le monde afin de pouvoir comparer les comportements des différents attaquants observés. Nous voulons déterminer si des tendances globales se dessinent ou si les activités sont, au contraire, très dépendantes de la situation géographique du pot de miel. Pour cela, nous avons pu avoir accès à trois machines, chacune possédant une adresse IP publique, installées en trois sites différents : une à Toulouse, une à Rennes et une à College Park, Maryland (Etats-Unis). Afin d'avoir un site dont nous contrôlons tous les paramètres, nous avons également installé un pot de miel identique au LAAS. Cette section présente l'architecture de déploiement des pots de miel.

A. Architecture

Le déploiement de pots de miel haute interaction peut être réalisé selon deux approches. Une première approche pourrait être de déporter l'architecture des pots de miel utilisés lors de l'expérimentation précédente, c'est-à-dire d'installer nos machines virtuelles modifiées sur un ordinateur en ces différents sites. Cette approche pose trois problèmes majeurs. Tout d'abord, le déploiement d'un pot de miel haute interaction reste une opération risquée (puisqu'il est destiné à laisser réellement un attaquant opérer sur le système). Il est donc soumis à de nombreuses contraintes de sécurité. Par conséquent, multiplier les systèmes revient à multiplier ces contraintes, d'autant plus que nous ne connaissons pas exactement la configuration des réseaux sur lesquels nous souhaitons installer les pots de miel. Ensuite, tous les pots de miel doivent être déployés dans des conditions identiques pour éviter que des différences de paramétrage nuisent à l'expérimentation. Notre architecture doit donc être pensée en fonction de ce besoin. Enfin, nous ne souhaitons pas que les réseaux des partenaires sur lesquels vont se connecter les attaquants puissent être compromis. Il est donc exclu de permettre l'exécution des instructions de l'attaquant sur des machines qui ne sont pas les nôtres. Notre système devra donc faire croire à un attaquant qu'il se connecte sur un ordinateur situé à Toulouse, Rennes ou College Park alors qu'il interagira en fait avec une machine du LAAS.

Ainsi, nous avons adopté une approche pour laquelle les connexions d'un attaquant vont être redirigées vers des machines virtuelles installées sur une machine du LAAS. Cette approche nous permet de garder un contrôle suffisamment important sur les pots de miel pour garantir un niveau de sécurité satisfaisant ainsi qu'une meilleure capacité de réaction en cas de problème (les éléments "sensibles" de l'infrastructure étant faciles d'accès). De plus, cela nous permet de minimiser l'influence du matériel et des réseaux mis à notre disposition dans les lieux de déploiement en utilisant les machines distantes uniquement comme des relais vers notre installation locale.

La figure 3 présente un aperçu global de l'architecture de ce déploiement. Nous avons ainsi trois machines situées sur des réseaux distants, plus une installée au LAAS. Chacune possède une IP publique. Elles vont servir de relai vers nos machines virtuelles, notées VM1 à VM4. Ces dernières sont installées sur un même hôte qui simule également un environnement de réseau local distinct pour chacune des machines virtuelles. Des tunnels `GRE` (*Generic Routing Encapsulation*, décrit dans la RFC 2784[5]) sont créés entre les relais et l'hôte, qui se charge de faire le lien entre ses extrémités de tunnels et les machines virtuelles. Nous devrons toutefois faire en sorte que les réponses envoyées par les machines virtuelles aux attaquants suivent bien le même chemin que les requêtes lancées par ces attaquants (à savoir passer par les tunnels pour ressortir par le relai), sinon elles risquent d'être rejetées par des pare-feux d'Internet. Enfin, l'établissement de règles de routage au niveau des relais et de l'hôte va permettre à une partie du trafic ciblant les IP publiques des relais d'être redirigée par ceux-ci vers les machines virtuelles.

B. Contrôle du trafic

Le contrôle des connexions intervient au niveau des machines relais et au niveau de la machine hôte du LAAS. Nous effectuons ce contrôle au moyen de l'outil `iptables` qui nous permet d'établir des règles de filtrage sur les paquets

[4] Ce regroupement est réalisé en fonction d'un seuil que nous avons fixé à 20 secondes, suite à des analyses que nous ne détaillons pas ici (voir [12]).

[5] www.ietf.org/rfc/rfc2784.txt.

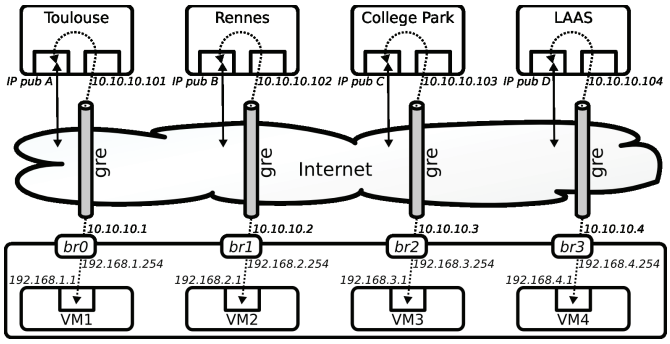

Fig. 3. Schéma de l'architecture du système de pots de miel

entrants et sortants d'une machine administrée par un système d'exploitation Linux. La politique de sécurité associée aux machines relais est la suivante :

- Les connexions entrantes sur le port 22 sont autorisées. C'est le port par défaut pour `ssh`, et donc celui sur lequel les attaquants vont pouvoir se connecter.
- Les connexions sortantes sur les ports 53 (`dns`) et 123 (`ntp`) sont autorisées pour que nos machines virtuelles puissent utiliser ces services.
- Un port supplémentaire `plaas` est ouvert uniquement pour les machines possédant une IP du LAAS et permet ainsi d'administrer la machine à distance.
- Le protocole `GRE` est autorisé en entrée et en sortie.
- Toutes les autres tentatives de connexions sont rejetées.

La politique de sécurité au niveau de l'hôte des machines virtuelles est la suivante :

- Le protocole `GRE` est autorisé en entrée et en sortie.
- Les connexions `ssh` sur le port `plaas` sont autorisées depuis le LAAS, pour administrer la machine.
- Les connexions `ssh` sur le port 22 sont autorisées, des tunnels vers les machines virtuelles.
- `dns` et `ntp` sont autorisés depuis les machines virtuelles vers les tunnels.

Ainsi, un attaquant ne peut se connecter sur nos pots de miel que par `ssh` (et copier des fichiers depuis sa machine via `scp`) sur le port 22 et toutes ses tentatives de nouvelles connexions sortantes depuis ce pot de miel sont alors bloquées. De cette manière, nous limitons les risques liés à l'utilisation de notre pot de miel par les attaquants pour rebondir et cibler d'autres systèmes sur Internet.

V. Analyse des données

Notre expérimentation s'est déroulée en deux phases. Tout d'abord, nous avons déployé nos pots de miel sans créer de comptes sur ceux-ci, pendant un mois. Cette première phase s'est déroulée du 1^{er} au 30 juin. L'analyse des données collectées durant cette phase a permis d'avoir un aperçu des couples identifiant/mot de passe tentés par les attaquants ainsi que leur fréquence. Ces résultats ont été utilisés pour constituer une liste de comptes que nous savions régulièrement tentés. La seconde phase a débuté par la création des comptes précédents sur tous les pots de miel. Grâce à l'utilisation de ces comptes fréquemment tentés, nous espérions pouvoir observer rapidement des intrusions. Cette deuxième phase a commencé le 1^{er} juillet et a duré 5 mois. Dans cette partie, nous allons d'abord donner un aperçu d'ensemble des résultats obtenus lors de ces deux phases, en les distinguant si besoin. Ensuite nous nous intéresserons à quelques analyses plus poussées sur ces données.

A. Activités observées

Dans cette partie, nous analysons les résultats des observations sur les différents pots de miel en amont de tout traitement des données. Ces analyses concernent les deux phases de l'expérimentation.

1) Connexions `ssh`

TABLE I
RÉPARTITION DES CONNEXIONS `ssh` OBSERVÉES SUR LES POTS DE MIEL.

Pot de miel	Nb. connexions	Nb. connexions réussies	Nb. IP différentes
Toulouse	301948	58	385
Rennes	397462	119	387
College Park	10737	42	197
LAAS	150027	298	421
Total	860174	517	1207

a) Aperçu Le tableau I donne la répartition des connexions observées sur les différents pots de miel à la date du 1^{er} décembre. Chacune de ces connexions correspond à l'envoi d'un couple identifiant/mot de passe au serveur `ssh`.

Le nombre d'adresses distinctes obtenu en considérant tous les pots de miel (1207) étant plus faible que la somme des nombres obtenus pour chaque machine (1390), certaines IP se sont donc connectées sur plusieurs d'entre elles. Il faudra donc tenir compte de ces intersections lors de nos analyses transversales.

Le tableau II donne les couples les plus tentés lors de ces attaques sur chaque pot de miel. Sans surprise, le compte `root` (le compte administrateur sous Linux) est la cible privilégiée des attaques, et ce quel que soit le pot de miel considéré. Pour le reste, nous voyons que les couples les plus tentés sont simples, avec un mot de passe souvent identique au nom d'utilisateur. Ce point confirme les observations faites il y a quatre ans dans [11]. On peut donc supposer que l'emploi de tels mots de passe pour protéger ses données est encore très répandu (un attaquant n'aurait pas d'intérêt à tester de telles combinaisons si elles étaient très rares). De plus, il semble y avoir un attrait pour les identifiants correspondant à des comptes créés pour le besoin de certains programmes (oracle, mysql, postgres, nagios, etc.). Les mots de passe associés sont ceux utilisés par défaut lors de l'installation de ces applications. Il serait intéressant de savoir si ces applications sont ciblées seulement parce qu'elles sont très répandues ou si l'intérêt est également d'accéder aux fichiers qu'elles utilisent et aux données qu'elles manipulent.

En comparant les résultats obtenus sur chaque pot de miel, nous constatons des variations du classement, avec toutefois certains couples présents dans les premières positions sur tous les pots de miel.

TABLE II
LISTE DES 5 COUPLES LES PLUS TENTÉS SUR CHAQUE POT DE MIEL

	Ordre	Toulouse Couple	Nb.	Rennes Couple	Nb.	College Park Couple	Nb.	LAAS Couple	Nb.
root inclus	1	root 123456	347	root 123456	386	root 123456	70	root 123456	247
	2	oracle oracle	282	root password	327	root root	61	root root	221
	3	root password	271	oracle oracle	304	root password	58	root password	203
	4	root qwerty	250	test test	297	root qwerty	47	root qwerty	201
	5	test test	247	root root	282	test test	36	oracle oracle	174
root exclu	1	oracle oracle	282	oracle oracle	304	test test	36	oracle oracle	174
	2	test test	247	test test	297	oracle oracle	32	test test	150
	3	mysql mysql	197	mysql mysql	257	admin admin	19	postgres postgres	140
	4	postgres postgres	193	postgres postgres	251	postgres postgres	16	mysql mysql	120
	5	test test123	159	user user	224	mysql mysql	13	admin admin	103

TABLE III
ENSEMBLE DES COMPTES CRÉÉS

Compte	*login*	*pass*
C1	adam	adam
C2	alex	alex123
C3	apache	apache
C4	cary	cary
C5	eric	eric
C6	michael	michael
C7	mysql	mysql
C8	nagios	123456
C9	postgres	postgres
C10	test	test123
C11	user	password

b) Paramétrage A la fin de la première phase, nous avons regardé quels étaient les couples les plus tentés sur chaque pot de miel. En nous basant sur les éléments de cette liste (qui exclut `root`), nous avons déterminé une liste de couples identifiant/mot de passe qui a été utilisée sur les quatre pots de miel. Les couples composant cette liste ont été choisis selon plusieurs critères :

- Des couples parmi les plus tentés sur un pot de miel mais pas sur les autres.
- Des couples fréquemment tentés sur tous les pots de miel.
- Des couples pour lesquels l'identifiant est différent du mot de passe.
- Des couples pour lesquels l'identifiant est identique au mot de passe.
- Des couples dont l'identifiant correspond à une application pouvant être installée sur la machine (`apache`, `mysql`, etc.).

A partir de ces critères, nous avons créé les comptes listés dans le tableau III sur tous les pots de miel.

c) Premières connexions Appelons τ_1 la durée écoulée entre la création d'un compte et la première tentative de connexion à ce compte réussie et τ_2 la durée écoulée depuis cette tentative jusqu'à la première connexion avec saisie de commandes sur ce compte. Les valeurs τ_1 et τ_2 pour l'ensemble des comptes créés sur les pots de miel sont données dans la table IV. Sur certains pots de miel, un attaquant s'étant connecté sur un des 11 comptes créés a réussi à obtenir les droits `root` en exploitant une faille du système d'exploitation. Quand cela a été le cas, nous donnons le temps qui s'est écoulé entre la création des comptes et cet évènement.

TABLE IV
DURÉES τ_1 ET τ_2 POUR CHAQUE COMPTE ET CHAQUE POT DE MIEL

Compte	Toulouse		Rennes		C.P.		LAAS	
	τ_1	τ_2	τ_1	τ_2	τ_1	τ_2	τ_1	τ_2
C1	65h	-	48h	81h	80j	61h	25j	40j
C2	61h	-	48h	15j	81j	6h	14j	40j
C3	32h	-	72h	15j	73j	8j	33h	37h
C4	-	-	7j	14j	-	-	53j	30j
C5	65h	-	72h	99h	82j	-	6j	48j
C6	65h	70h	64h	7h	60j	-	6j	11j
C7	50h	1h	72h	6j	71j	-	55h	1h
C8	7j	19h	99h	99h	87j	-	100h	10j
C9	65h	70h	72h	28h	23h	6h	60h	2h
C10	56h	-	72h	9j	81j	-	55h	1h
C11	65h	-	72h	16j	-	-	7j	6j
root	6j		-		-		25j	

Le tableau montre des valeurs τ_1 bien plus grandes sur le pot de miel de College Park. Il y a plusieurs raisons possibles à cela. En premier lieu, l'activité sur ce pot de miel depuis la création des comptes a été bien plus faible que sur les trois autres. Cela aurait pu être dû à une configuration des paramètres du réseau, qui pourrait par exemple rejeter les connexions générant un trafic trop important (on parle de *rate limiting*) comme dans le cas d'une attaque par dictionnaire. Différents tests indiquent que ce n'est pas le cas et ceci a été confirmé par l'administrateur du site. On peut également imaginer que le délai de quelques secondes induit par la redirection des connexions depuis les Etats-Unis vers la France a pu être assez important pour décourager une partie des attaquants. Enfin, il n'est pas exclu qu'un attaquant ait trouvé un moyen de démasquer le pot de miel, mettant alors l'adresse IP correspondante sur une "liste noire" des machines à ne pas attaquer.

Nous voyons sur ce tableau que tous les comptes ayant été trouvés (τ_1 est fini) n'ont pas nécessairement été attaqués par la suite. Cela peut être dû à plusieurs raisons. Tout d'abord, comme nous avons délibérément choisi des couples fréquemment tentés, il arrive que lors d'une même session d'attaque plusieurs couples soient trouvés (une attaque par dictionnaire sur le pot de miel de Toulouse a ainsi trouvé 10 couples valides). Il est arrivé que l'attaquant ne se connecte que sur un de ces comptes et modifie alors le mot de passe des autres depuis celui-ci, empêchant d'autres attaquants de s'y connecter à leur tour. Nous avons ainsi observé un attaquant changeant successivement 6 mots de passe. De plus, nous avons eu deux cas où un attaquant a réussi à prendre le contrôle du compte `root`. Ici aussi, il a ensuite modifié les mots de passe des comptes qu'il a détectés sur la machine. Etant devenu `root`, il possédait tous les droits sur la machine attaquée et n'avait même plus besoin de connaître le mot de passe original du compte à modifier. Dès lors, ces nouveaux mots de passe étant relativement complexes, ils ne seront pas trouvés lors de futures attaques par dictionnaire. Ici aussi, nous avons vu un attaquant changer 4 mots de passe d'un coup. Ce genre de comportements spécifiques sera détaillé dans la partie V-C2.

Concernant les résultats obtenus, on constate que la découverte des comptes s'est faite rapidement (à l'exception de College Park et du compte C4), comme prévu, puisqu'en une semaine tous les identifiants et mots de passe sauf un ont été découverts. En revanche, le temps avant une première

intrusion sur ces comptes est bien plus variable, allant d'une heure à plus de deux semaines.

2) Répartition géographique Les connexions enregistrées provenaient de 1207 adresses IP distinctes, issues de 78 pays. Le tableau V donne les 5 pays pour lesquels le nombre d'adresses IP différentes ayant été aperçues sur chaque pot de miel est le plus important.

TABLE V
ORIGINE DES ATTAQUES LES PLUS OBSERVÉES SUR CHAQUE POT DE MIEL

Ordre	Toulouse	Rennes	College Park	LAAS
1	Chine 83	Chine 80	Chine 40	Chine 98
2	Etats-Unis 50	Etats-Unis 56	Etats-Unis 39	Etats-Unis 60
3	Allemagne 18	Corée du Sud 37	Brésil 12	Roumanie 34
4	France 18	Allemagne 14	Japon 7	Russie 16
5	Pays-Bas 18	Royaume-Uni 13	Royaume-Uni 7	Allemagne 14
Nb. IP distinctes	385	387	197	421

La Chine et les Etats-Unis se démarquent nettement, et ce sur les quatre pots de miel. Ensuite, nous observons que les mêmes pays apparaissent sur les trois pots de miel situés en France alors qu'ils sont absents sur celui des Etats-Unis. Cependant, en restant à ce haut niveau d'abstraction les écarts ne sont pas suffisamment significatifs pour pouvoir conclure.

Par ailleurs, en comparant les IP collectées par ces quatre pots de miel avec celles collectées par le pot de miel précédemment déployé au LAAS [11] (3230 adresses différentes répertoriées entre janvier 2006 et août 2010), seulement 4 d'entre elles ont été vues lors des deux expériences et ce uniquement sur les pots de miel situés en France. Par conséquent, il semble que les adresses IP, utilisées pour ces attaques ne le soient que pendant une durée limitée.

B. Attaques par dictionnaire

1) Généralités Nous appelons attaque par dictionnaire une session pendant laquelle au moins 9 tentatives de connexion `ssh` ont eu lieu. Cela nous permet d'éliminer de manière relativement sûre les cas où une attaque s'avèrerait en fait être une erreur de connexion. Parmi les sessions obtenues avec un seuil de 20s, nous obtenons un total de 1479 attaques par dictionnaire. Celles-ci ont été lancées depuis 825 adresses distinctes, provenant de 71 pays différents.

2) Vocabulaires

a) Définition Nous appelons vocabulaire d'une session l'ensemble des couples identifiant/mot de passe utilisés lors de cette session. Chaque couple constitue un mot de ce vocabulaire. Nous appelons dictionnaire un regroupement de vocabulaires qui ont des caractéristiques communes[11].

b) Observations Nous avons créé un dictionnaire général pour chaque pot de miel qui est en fait l'union de tous les vocabulaires observés sur ce pot de miel. Nous appelons ainsi $D1, D2, D3$ et $D4$ les dictionnaires généraux des pots de miel respectivement situés à Toulouse, Rennes, College Park et au LAAS. Nous appelons $D1', D2', D3'$ et $D4'$ les dictionnaires créés à partir de $D1$, $D2$, $D3$ et $D4$ contenant les mots apparaissant uniquement dans ces dictionnaires :

$$Di' = \{m \in Di / \forall j \neq i, m \notin Dj\}$$

Ce sont les parts exclusives de ces dictionnaires. Le tableau VI montre le nombre de mots ces dictionnaires ont en commun.

Malgré les fortes différences de taille entre les différents dictionnaires, nous pouvons faire quelques observations. Tout d'abord, il est clair qu'il existe une base de couples communs assez importante, même si elle est variable selon les pots de miel. En effet, les parts exclusives des dictionnaires $D1$, $D2$, $D3$ et $D4$ s'élèvent respectivement à 57%, 62%, 14% et 44% de leur taille totale.

TABLE VI
INTERSECTIONS DES DIFFÉRENTS DICTIONNAIRES GÉNÉRAUX

Dictionnaire	Nombre de mots	Dictionnaire	Nombre de mots
$D1$	127226	$D1 \cap D2 \cap D3$	3732
$D2$	142956	$D1 \cap D2 \cap D4$	29277
$D3$	5953	$D1 \cap D3 \cap D4$	3172
$D4$	76102	$D2 \cap D3 \cap D4$	3224
$D1 \cap D2$	46893	$D1 \cap D2 \cap D3 \cap D4$	3025
$D1 \cap D3$	4218	$D1'$	72598
$D1 \cap D4$	36673	$D2'$	89463
$D2 \cap D3$	4546	$D3'$	825
$D2 \cap D4$	35262	$D4'$	33348
$D3 \cap D4$	3467		

De la même manière, nous construisons $D0$, le dictionnaire contenant tous les couples tentés lors de l'expérimentation effectuée dans [11] et $D0'$, sa part exclusive par rapport à $D1, D2, D3$ et $D4$. Le tableau VII nous permet ainsi d'avoir un aperçu de l'évolution des vocabulaires actuels par rapport à ceux observés lors des années précédentes. On constate que moins de 50% du contenu des dictionnaires observés récemment (sauf D3, bien plus petit) se retrouve dans $D0$. Il est difficile encore de conclure à l'heure actuelle compte tenu de la courte période de collecte mais il semble que ces analyses tendent à montrer que les vocabulaires se diversifient.

TABLE VII
COMPARAISONS ENTRE ANCIENS ET NOUVEAUX DICTIONNAIRES

Dictionnaire	Nombre de mots
$D0$	253287
$D0 \cap D1$	56333
$D0 \cap D2$	51219
$D0 \cap D3$	4653
$D0 \cap D4$	33675
$D0 \cap D1 \cap D2 \cap D3 \cap D4$	2720
$D0'$	172708

3) Répartition géographique

a) Origine des attaques Le tableau VIII donne les 5 pays les plus impliqués dans les attaques par dictionnaire de nos pots de miel sachant que nous comptabilisons chaque adresse IP une seule fois. En comparant ces chiffres avec le tableau V, il apparait que les adresses IP chinoises et américaines sont majoritairement utilisées pour mener des attaques par dictionnaire. Globalement, en plus de ces deux pays, d'autres sont présents dans le haut du classement sur les trois machines situées en France, comme la Corée du Sud, le Canada ou la Russie. En revanche, ils n'apparaissent pas dans les premières positions à College Park. Les machines situées dans ces régions (ou du moins utilisant des adresses IP situées dans ces régions) semblent donc dédiées à l'attaque d'une plage d'adresses incluant nos trois pots de miel français.

TABLE VIII
PAYS LES PLUS OBSERVÉS SUR CHAQUE POT DE MIEL : ATTAQUES PAR DICTIONNAIRE

Classement	Toulouse		Rennes		College Park		LAAS	
1	Chine	32	Chine	25	Etats-Unis	8	Chine	28
2	EItats-Unis	20	Etats-Unis	14	Chine	4	Etats-Unis	11
3	Russie	8	Corée du Sud	11	Argentine	4	France	5
4	Corée du Sud	8	Turquie	5	Taiwan	2	Canada	5
5	Inde	6	Canada	5	Thailande	2	Russie	4

b) Cibles des attaques par dictionnaire Le tableau IX dénombre les adresses IP ayant effectué des attaques par dictionnaire sur plusieurs machines. Nous constatons que deux adresses seulement ont attaqué les quatre pots de miel. En revanche, il y a un nombre important d'adresses ayant visité au moins deux pots de miel en France mais au contraire très peu d'adresses observées en France et aux Etats-Unis. Il est à noter que les adresses IP correspondant aux pots de miel français sont assez rapprochées entre elles mais plus éloignées de celle de College Park. De plus, les séquences de couples testés par une même adresse sur plusieurs de nos pots de miel sont très similaires, voire identiques. Il semble donc que des machines dédiées à ces attaques se voient attribuer des plages d'IP à attaquer plutôt que de balayer tout le spectre possible et se contentent de répéter la même séquence de couples à tester sur chaque machine avant de passer à la suivante, voire de recommencer cette séquence sur toute la plage, comme nous l'avons observé plusieurs fois.

TABLE IX
RÉPARTITION DES IP SOURCES DES ATTAQUES PAR DICTIONNAIRE

Ensemble	Nombre d'attaques	IP distinctes
Toulouse	358	297
Rennes	529	308
College Park	197	93
LAAS	395	225
Toulouse ∩ Rennes	120	54
Toulouse ∩ College Park	21	12
Toulouse ∩ LAAS	108	55
Rennes ∩ College Park	12	7
Rennes ∩ LAAS	84	37
College Park ∩ LAAS	9	6
Toulouse ∩ Rennes ∩ College Park	8	2
Toulouse ∩ Rennes ∩ LAAS	71	24
Toulouse ∩ College Park ∩ LAAS	6	2

C. Intrusions

Cette section est consacrée aux connexions réussies par les attaquants et suivies par une saisie de commandes de leur part.

1) Identification des attaquants Nous avons observé que quasiment la moitié des 131 intrusions que nous avons enregistrées sont issues du même pays européen P1 (62 intrusions au total). Ces résultats confirment ici ce que nous avions déjà observé lors de l'expérimentation précédente [11]. Il est toutefois possible que certaines de ces adresses ne soient en fait que des relais utilisés par l'attaquant pour brouiller les pistes. Cependant, l'analyse des données fournies par les terminaux utilisés par les attaquants a montré qu'ils tentaient souvent de télécharger des programmes sur des sites hébergés dans le pays P1, mais surtout que parmi les programmes effectivement exécutés, plusieurs affichaient du texte dans la langue du pays P1.

De plus, nous avons vu dans la partie V-A1a que des adresses IP avaient été observées sur plusieurs machines. Les résultats de l'analyse des recoupements d'adresses visibles dans le tableau X nous montrent que les intrusions sont rarement menées depuis les mêmes adresses. En effet, seules cinq adresses IP ayant effectué des intrusions ont été vues sur plusieurs pots de miel, plus spécifiquement sur ceux situés en France. En observant plus en détail le contenu des intrusions réalisées par ces adresses, il apparait que pour quatre d'entre elles, vues à la fois à Toulouse et à Rennes, le mot de passe modifié utilisé lors de l'appropriation du compte (cf V-C2a) est toujours le même (la cinquième adresse n'a pas changé le mot de passe du compte attaqué). Ces quatre adresses appartiennent donc au même individu ou au même groupe d'individus. Par ailleurs, le nombre d'adresses distinctes est relativement proche du nombre total d'intrusions répertoriées mais bien supérieur au nombre de comptes attaqués, ce qui signifie que la plupart des attaquants ne se connectent pas plusieurs fois avec la même adresse sur un compte. Dans le cas des comptes ayant été visités par plusieurs adresses, deux hypothèses (ne s'excluant pas mutuellement) sont alors envisageables :

- L'attaquant change d'adresse à chaque connexion pour brouiller les pistes.
- Il y a en fait une communauté d'attaquants se partageant des informations à propos des machines qu'ils ont attaquées, ce qui leur permet par exemple de se relayer si l'un d'entre eux ne parvient pas à prendre le contrôle d'une machine par manque de connaissances techniques.

TABLE X
RÉPARTITION DES ADRESSES IP SOURCES DES INTRUSIONS

Ensemble	Nombre d'intrusions	IP distinctes	Nb. comptes attaqués
Toulouse	22	13	4 + root
Rennes	26	21	11
College Park	7	7	4
LAAS	76	51	11 + root
Toulouse ∩ Rennes	11	4	2 + 2
Toulouse ∩ College Park	0	0	-
Toulouse ∩ LAAS	0	0	-
Rennes ∩ College Park	0	0	-
Rennes ∩ LAAS	3	1	1 + 1
College Park ∩ LAAS	0	0	-

2) Activités des attaquants

a) Tendances globales Lors des 131 intrusions observées, plusieurs comportements communs à un grand nombre d'attaquants ont été régulièrement observés :

- Souci de discrétion : l'attaquant vérifie s'il est le seul connecté sur la machine et efface souvent les fichiers d'historique des commandes.

- Exploration de la machine : l'attaquant cherche à récupérer des informations sur la machine attaquée : nom et version de l'OS, caractéristique du processeur, etc.
- Appropriation du compte : Lors de la première connexion à un compte, l'attaquant change toujours le mot de passe de celui-ci par un autre plus complexe afin de s'approprier le compte, prenant ainsi le risque de se faire détecter lorsque l'utilisateur légitime voudra utiliser sa machine.
- Scan d'adresses IP : l'attaquant installe un scanner de plage d'adresses IP afin de déterminer lesquelles sont accessibles via le service `ssh` depuis la machine attaquée.
- Installation de client `IRC` : ce client de messagerie est utilisé pour recevoir et exécuter des instructions envoyées par un attaquant depuis un serveur distant. L'objectif ici semble être de rattacher la machine compromise à un *botnet*, le serveur envoyant alors ses ordres à des centaines de machines en même temps.
- Tentatives d'acquisition de privilèges d'administrateur : certains attaquants cherchent à obtenir les privilèges d'administrateur afin d'obtenir un contrôle total sur la machine compromise. Pour cela, ils tentent d'exploiter des failles de sécurité de l'OS via divers programmes spécialisés appelés `rootkit`.

b) Pleins pouvoirs sur le système Une fois les privilèges d'administrateur obtenus, les deux attaquants ont aussitôt changé le mot de passe `root` de la machine. Ils ont ensuite installé des programmes modifiés afin d'obtenir des informations sur les utilisateurs "légitimes" de la machine ainsi que pour ouvrir un nouveau port afin de pouvoir continuer à communiquer avec la machine s'ils venaient à perdre l'accès via le port 22 (on parle de *porte dérobée*).

Le premier a ainsi installé le `rootkit` SHV4[6], qui installe un serveur `ssh` s'il n'y en a pas déjà un présent, modifie l'exécutable du client `ssh` pour qu'il enregistre les couples identifiant/mot de passe tentés lors de connexions vers d'autres hôtes et surtout installe un grand nombre de versions modifiées d'exécutables du système qui pourraient permettre de détecter sa présence afin de rester indétectable. Cet attaquant cherche donc vraisemblablement à obtenir facilement de nouvelles cibles pour de futures attaques. Cependant, il a également modifié le mot de passe de tous les comptes qu'il a pu trouver sur la machine grâce à son attaque par dictionnaire précédant l'intrusion, ainsi qu'en listant les dossiers du répertoire `/home` (mais sans consulter la liste des comptes existants, par exemple dans `/etc/passwd`). Il semble ainsi étrange que l'attaquant cherche à couvrir ses traces et à récupérer les mots de passe fournis par les personnes pouvant utiliser la machine tout en bloquant l'accès au plus grand nombre de comptes possibles.

Le second a également remplacé le binaire du client `ssh` par une autre version mais nous n'avons pas de certitude quant aux modifications réellement apportées. Il n'a en revanche pas changé les mots de passe d'autres comptes existants, mais en a créé un nouveau, nommé "backup" et possédant les droits d'administrateur. Il s'est depuis reconnecté via ce compte mais n'a pour l'instant rien modifié de plus. En revanche, il continue d'utiliser le compte "user" pour installer de nouveaux clients `IRC`, probablement car établir un contact avec ceux précédemment installés lui est impossible du fait de notre verrouillage du réseau.

[6]http://web.fhnw.ch/plattformen/ns/vorlesungsunterlagen-1/network-analysis-tools/shv4-analysis

VI. Conclusion

Nous avons présenté dans cet article une plateforme de déploiement de pots de miel haute interaction ainsi que les premiers résultats des analyses des données collectées.

Ces premiers résultats viennent confirmer pour la plupart les conclusions que nous avions tirées d'une précédente expérience menée avec un seul pot de miel au LAAS. Ainsi, on constate que sont confirmés : 1) la spécialisation des adresses IP qui sont utilisées, soit pour l'attaque par dictionnaire, soit pour l'intrusions, mais jamais les deux ; 2) les activités et objectifs des attaquants et 3) le principal pays d'origine des intrusions. Nous avons également tiré de nouvelles conclusions de cette expérimentation 1) le fait que les adresses IP qu'utilisent les attaquants sont quasiment toutes renouvelées régulièment (seulement 3 adresses IP ont été "vues" à la fois lors de cette expérimentation et lors de la précédente) et 2) le fait que les dictionnaires utilisés pour les attaques par dictionnaire semblent se diversifier. Bien sûr, ces analyses, encore préliminaires, demandent à être confirmées par les nouvelles collectes de données que nous poursuivons.

Références

[1] B. McCarty, "The honeynet arms race," *IEEE Security and Privacy*, vol. 1, pp. 79–82, 2003.

[2] B. Cheswick, "An evening with berferd in which a cracker is lured, endured, and studied," in *Proceedings of the Winter 1992 USENIX Conference*, 1992, pp. 163–174.

[3] L. Spitzner, *Honeypots: Tracking Hackers*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2002.

[4] F. Maggi and S. Zanero, "Analysis of the state of the art," *WOMBAT Project Worldwide Observatory of Malicious Behaviors and Attack Threats*, 2008, http://wombat-project.eu/workpackages/wp2-analysis-of-state-of-the-a/.

[5] NOAH, "Do1.1: Survey on the state of the art," *Deliverable of the European Network of Affined Honeypots*, 2005, http://www.fp6-noah.org/publications/deliverables/D0.1.pdf.

[6] E. Balas, "Know your enemy : Sebek," *The Honeynet Project*, 2003, www.honeynet.org/papers/.

[7] N. Provos, "A virtual honeypot framework," *Proceedings of the 13th conference on USENIX Security Symposium*, 2004.

[8] C. Leita, K. Mermoud, and M. Dacier, "Scriptgen: an automated script generation tool for honeyd," in *Proceedings of the 21st Annual Computer Security Applications Conference*. IEEE, 2005.

[9] G. Wagener, R. State, A. Dulaunoy, and T. Engel, "Self adaptive high interaction honeypots driven by game theory," in *SSS*, ser. Lecture Notes in Computer Science, R. Guerraoui and F. Petit, Eds., vol. 5873. Springer, 2009, pp. 741–755.

[10] P. Baecher, M. Koetter, M. Dornseif, and F. Freiling, "The nepenthes platform: An efficient approach to collect malware," in *In Proceedings of the 9 th International Symposium on Recent Advances in Intrusion Detection (RAID)*. Springer, 2006, pp. 165–184.

[11] V. Nicomette, M. Kâaniche, E. Alata, and M. Herrb, "Set-up and Deployment of a High Iinterfaction Hhoneypot: Experiment and Lessons Learned," *Journal in Computer Virology*, vol. 7, no. 2, pp. 143–157, Mai 2011.

[12] I. Studnia, E. Alata, M. Kâaniche, and V. Nicomette, "Observation et Analyse d'Attaques sur Internet," LAAS CNRS, Tech. Rep. RL 1160, 2011.