Leurré.com : retour d'expérience sur plusieurs mois d'utilisation d'un pot de miel distribué mondialement

E. Alata[1], M. Dacier[2], Y. Deswarte[1], M. Kaâniche[1], K. Kortchinsky[3], V. Nicomette[1], V.H. Pham[2], and F. Pouget[2]

[1] LAAS/CNRS
7 Avenue du Colonel Roche
31077 Toulouse Cedex 4 - France
{ealata,deswarte,kaaniche,nicomett}@laas.fr
[2] Eurécom
2229 Route des Crêtes
BP 193
06904 Sophia Antipolis Cedex - France
{dacier,pham,pouget}@eurecom.fr
[3] CERT-RENATER
c/o ENSAM
151 Boulevard de l'Hôpital
75013 Paris - France
kostya.kortchinsky@renater.fr

Résumé L'environnement *Leurré.com* est le nom de l'infrastructure utilisée par le projet *CADHo* financé dans le cadre de l'Action Concertée Incitative (ACI) intitulée « sécurité et informatique » [1]. Cette plateforme est basée sur une collaboration entre de nombreux partenaires qui ont déployé un ensemble de pots de miel tous configurés de manière identique. Les données collectées sont rassemblées dans une base de données centralisée. Cet environnement unique, administré par l'institut Eurécom, offre à ses partenaires des données qu'ils peuvent analyser par le biais de techniques innovantes. Pour l'instant, près de trente plateformes sont en fonctionnement depuis plusieurs mois dans une vingtaine de pays couvrant les cinq continents.

Le projet *CADHo*, hormis la mise sur pied de cet environnement, a pour but d'analyser ces données et de fournir des modèles des attaques observées. Dans ce qui suit, nous offrons une synthèse des premiers résultats déjà obtenus. Par ailleurs, nous expliquons aussi la démarche poursuivie pour tirer parti de ces données afin de modéliser les phénomènes observés ainsi que le comportement des attaquants dès le moment où ils ont pris le contrôle d'une machine.

1 Introduction

Depuis les premières attaques de déni de service distribuées lancées contre plusieurs sites de commerce électronique en février 2000, de nombreux événements

du même ordre ont fait la une de l'actualité. Les vers, en particulier, connaissent un essor retentissant. Malgré les progrès spectaculaires des méthodes de protection, comme par exemple le déploiement de plus en plus systématique de garde barrières (« firewalls ») adaptés aux ordinateurs personnels, le nombre d'attaques ne semble pas diminuer. Face à cet apparent paradoxe, il est légitime de se poser les deux questions fondamentales suivantes. Premièrement, cette sensation d'accroissement est elle confirmée par des mesures objectives, irréfutables ? Deuxièmement, si tel est le cas, quels sont les processus d'attaques mis en œuvre qui permettent une telle diffusion des attaques ?

En l'état actuel des connaissances, il est malheureusement impossible de répondre, d'une manière précise, scientifique, à ces deux questions. En effet, force est de constater qu'aucun effort n'a été mené jusqu'à présent pour mesurer ces événements d'une façon stable, organisée, rationnelle. Il existe bien certains indicateurs qualitatifs, comme par exemple les enquêtes effectuées chaque année depuis 8 ans par le Computer Security Institute (CSI) et le Federal Bureau of Investigation (FBI). Ces rapports, cependant, ne rapportent que des tendances, obtenues de manière statistique sur un échantillon de données sans avoir une connaissance précise de l'environnement à partir desquels ces données sont recueillies et du comportement des attaquants qui ont généré le trafic malveillant. Par ailleurs, certaines grandes compagnies privées prennent en charge la gestion de la sécurité de leurs clients. Ce faisant, elles ont à leur disposition un très grand ensemble de données qui devraient, en théorie, leur permettre d'analyser de façon fine certains phénomènes, tels qu'ils sont vus depuis chez leurs clients. Cependant, pour avoir eu accès à certaines de ces données, nous pouvons témoigner de la difficulté d'utiliser ces sources d'information pour des analyses précises et non biaisées. En effet, les environnements des clients sont souvent très complexes et changeants. Il est, dès lors, difficile, pour ne pas dire impossible de tirer un quelconque parti des données ainsi collectées. Enfin, certaines initiatives ont vu le jour plus ou moins récemment, telles que la « honeynet research alliance » ou encore le site www.incidents.org. Ici encore, un des auteurs a une expérience de première main avec ces sources de données et force est de constater que ces initiatives sont très utiles par rapport aux objectifs qu'elles se sont fixées mais insuffisantes par rapport à l'analyse précise des menaces présentes sur l'Internet. Elles sont cependant complémentaires et ne doivent certainement pas être ignorées. Partant de ce constat, trois équipes françaises ont uni leurs forces pour bâtir un projet nommé *CADHo* financé partiellement dans le cadre de l'ACI sécurité [1]. Nous en livrons ici les objectifs et les premiers résultats.

Le projet *CADHo* a été construit selon trois axes.

1. Il vise à développer et mettre à disposition de la communauté scientifique une plateforme simple et distribuée de collecte de données à même de permettre la mise en œuvre d'analyses fines des processus d'attaques visant les machines connectées à l'Internet

2. Il a également pour objectif de valider cette plateforme en montrant l'intérêt d'analyser les données ainsi acquises. Pour ce faire, nous mettons en œuvre

différentes techniques d'analyse et nous montrons les retombées pratiques que nos modèles peuvent avoir pour augmenter la sécurité globale du système.

3. Enfin, il vise à dépasser le stade de l'analyse des attaques automatisées pour parvenir à comprendre et modéliser les *modus operandi* des véritables attaquants humains une fois qu'ils sont parvenus à compromettre une machine cible. La constitution d'un environnement à même de permettre l'observation à la fois non biaisée, sécurisée et légale de ce genre de processus relève du challenge à l'heure actuelle. Une des difficultés principales à surmonter consiste à dépasser l'aspect purement anecdotique d'un attaquant dans ses œuvres. Une telle observation en tant que telle n'a que peu d'intérêt. Par contre, l'analyse des faits et gestes d'un attaquant dont nous pouvons dire avec confiance qu'il est représentatif d'une classe plus large d'attaquants est intéressante dans la mesure où elle permet de tirer des conclusions qui dépassent le cadre strict de l'environnement d'expérimentation et dont les enseignements peuvent s'appliquer de façon beaucoup plus large. Pour parvenir à résoudre ce problème de la représentativité, nous comptons nous appuyer sur les résultats obtenus dans les deux premiers axes décrits ci dessus.

Une plateforme a été développée et déployée dans le cadre du projet *CADHo*. Nous collectons aujourd'hui en temps réel des données issues d'une trentaine d'endroits différents situés dans une vingtaine de pays couvrant les cinq continents. Dans les sections qui suivent, nous décrivons notre environnement de collecte de données et nous offrons un bref résumé des résultats les plus importants déjà obtenus. De plus, nous montrons les premières pistes de réflexion déjà suivies en ce qui concerne la problématique de modélisation des attaquants.

Il est important de noter que toute institution qui accepte d'héberger une de nos plateformes obtient automatiquement l'accès à l'ensemble des données que nous avons déjà collecté.

La Section 2 décrit l'environnement de collecte distribuée *Leurré.com*. La Section 3 propose une synthèse des différentes analyses que nous avons réalisées et publiées au cours des derniers mois. La Section 4 s'intéresse plus particulièrement au problème de la modélisation des attaques observées sur chaque plateforme. La Section 5 offre des pistes de réflexion sur la façon de faire évoluer cette plateforme vers une architecture dite de haute interaction.

2 Environnement de collecte de données *Leurré.com*

Comme nous l'avons indiqué ci-dessus, un des objectifs avoués du projet *CADHo* est la mise en œuvre d'un environnement distribué de collecte de données pour l'analyse des attaques ayant lieu contre des machines connectées à l'Internet. Dans ce but, nous avons défini une structure évolutive qui peut s'enrichir de façon incrémentale. Les frais de gestion et de maintenance sont réduits afin de permettre à cette plateforme de perdurer dans le temps et de ne pas disparaître à la fin du projet *CADHo*. Le paradigme de fonctionnement est celui d'une assemblée collaborative. Toute équipe désireuse de bénéficier des données collectées par l'environnement doit en devenir partie prenante en installant chez

elle un des éléments constitutifs de la plateforme distribuée, à savoir un ensemble de 3 pots de miel.

Un honeypot est une machine que l'on place dans un réseau mais dont personne ne se sert [2]. En théorie, aucune connexion de ou vers cette machine ne devrait être observée. Dans le cas contraire, il s'agit, au mieux d'une erreur accidentelle, au pire d'une tentative d'attaque intentionnelle. Récemment, plusieurs approches ont été proposées pour bâtir des environnements où cohabitent plusieurs honeypots. On parle alors de honeynet. Le projet le plus connu est sans doute celui mis en œuvre par les membres du Honeynet Research Alliance [3] dont certains des auteurs de cet article font partie de la branche française, le French Honeynet Project [4]. L'institut Eurécom a travaillé depuis plus d'un an sur la définition d'un environnement de collecte adapté aux besoins décrits ci-dessus. Un premier environnement a été déployé, basé sur la technologie VMware [5]. Au bout d'un an d'expérimentation et au vu des données collectées et analysées, nous sommes aujourd'hui en mesure d'affirmer qu'un environnement bâti autour de la technologie gratuite « *honeyd* » [6] plutôt que sur le logiciel payant VMware n'induira qu'un biais marginal dans les données collectées [7]. Cette affirmation, nous ne pouvions la faire il y a un an. En effet, il est bien connu que la technologie *honeyd* souffre de plusieurs défauts, le plus grave étant qu'un tel honeypot est identifiable à distance, dans certaines conditions, par un pirate déterminé. Si la majorité des attaquants passe par cette phase préliminaire d'identification, un honeypot qui utiliserait cette technique serait immanquablement repéré et ses données non représentatives puisqu'il y a fort à penser que l'attaquant ne s'y comporterait plus comme sur une machine 'normale'. Ayant collecté des données sur un environnement plus riche qui ne souffre pas de ces défauts, nous savons aujourd'hui que cette phase de test préalable n'existe que de façon très minoritaire. C'est pourquoi la plateforme bâtie utilise la technologie *honeyd*.

La plateforme de collecte distribuée consiste en un nombre potentiellement grand de honeynets configurés de façon rigoureusement similaire, déployés auprès de tous nos partenaires. Les données issues de chaque honeynet sont rapatriées au sein d'un serveur de bases de données maintenu par l'institut Eurécom. Les données, à savoir l'entièreté de tous les paquets émis ou reçus par tous les honeypots, y sont enrichies de données contextuelles (localisation géographique de la source, décalage horaire, type d'OS, etc.) et stockées de façon telle qu'il ne faille pas plus de quelques secondes pour répondre aux requêtes les plus courantes soumises à la base.

De façon concrète, l'environnement *Leurré.com* est constitué de trois éléments distincts [8] :

1. Un ensemble d'ordinateurs connectés directement à l'Internet en différents endroits du monde. Toutes ces machines utilisent le logiciel *honeyd* configuré de façon unique. Chaque ordinateur émule trois machines virtuelles. Il stocke dans un fichier tcpdump l'ensemble des paquets reçus sur, et émis depuis, la plateforme. Un garde barrière interdit d'initier des connections à partir de cet ordinateur mais le laisse répondre à toute sollicitation externe. Une fois

par jour, un service s'active durant une fenêtre de temps courte qui permet à une machine de confiance d'initier un transfert sécurisé des fichiers tcpdump de la journée. L'intégrité de la machine est également vérifiée à ce moment.

2. Un site centralisé où sont collectées toutes les données dans une base de données relationnelle. Tous les partenaires ont accès à l'ensemble des données par le biais d'une interface graphique sécurisée.
3. Un ensemble de logiciels qui permettent le rapatriement, le traitement et l'enrichissement des données collectées sur chaque plateforme. Par exemple, nous utilisons trois logiciels différents (*p0f, ettercap et disco*) pour déterminer de façon passive le système d'exploitation des machines qui ont attaqué les plateformes (Passive OS fingerprinting). Nous utilisons aussi les données fournies par le service commercial Maxmind pour déterminer l'origine géographique des attaques.

3 Synthèse des résultats obtenus

Les données collectées se montrent très riches d'enseignement. Au cours de l'année écoulée, nous avons publié un certain nombre de résultats dans différentes conférences internationales. Nous en offrons ci-après une synthèse rapide et nous invitons le lecteur intéressé à consulter les articles référencés pour de plus amples informations.

- Dans [9,10], nous nous intéressons exclusivement aux données collectées sur la plateforme initiale à haute interaction. Nous mettons en évidence l'existence d'une stabilité étonnante des phénomènes d'attaque observés au cours de 10 mois d'expérimentation. Nous mettons en exergue, à l'aide d'expériences simples, l'existence de deux ensembles disjoints de machines ciblant notre environnement. D'une part, certaines machines ne cherchent qu'à glaner de l'information. Elles ne réalisent pas d'attaque à proprement parler. Elles scannent notre réseau de façon systématique mais sur un nombre relativement faible de ports. D'autre part, un nombre pratiquement trois fois plus faible de machines nous attaquent directement. Ces machines ne visent que les seuls ports ouverts de nos différentes machines. Elles ont donc acquis une connaissance détaillée de notre environnement, sans doute grâce aux machines du premier groupe. Il est à noter que, à l'heure actuelle, nous observons toujours ce phénomène de deux communautés disjointes mais leurs proportions ont changé. Nous avons aujourd'hui plus d'*attaquants* que de *scanneurs*.
- Afin de pouvoir mieux tirer parti de la richesse des données collectées, nous définissons dans [11,12] un nouvel algorithme de clustering qui nous permet de regrouper ensemble les traces émises par différentes machines qui font usage d'un même outil d'attaque. Les résultats de l'application de cet algorithme à nos données révèlent l'apparition de phénomènes qui restent invisibles si l'on se contente de regarder simplement le nombre d'attaques par port sur une durée donnée.

- La structure de la base utilisée pour stocker les informations obtenues ainsi que la structure détaillée de l'environnement *Leurré.com* sont détaillés dans [8].
- Dans [7], nous étudions de façon précise, le biais possible introduit par l'utilisation de plateformes a basse interaction. Nous nous appuyons sur les deux types d'architecture déployée, haute et basse interaction, pour construire un système correctement étalonné, et en déduire éventuellement les modifications à effectuer pour affiner la configuration des plateformes basse-interaction.
- Enfin, dans [13], nous offrons les premières analyses obtenues à partir de plusieurs plateformes identiques réparties en différents endroits. Nous mettons en exergue les trois choses suivantes :
  1. Certains phénomènes d'attaques sont observés sur toutes les plateformes
  2. Certains phénomènes d'attaques ne sont observés que sur un sous ensemble, parfois très faible, de plateformes.
  3. Certains phénomènes d'attaques ne sont observés que sur une seule plateforme.

De façon surprenante, les phénomènes uniques à certaines plateformes représentent la majorité des attaques observées, toutes plateformes confondues. Il en résulte que l'on ne peut étudier les attaques sur la toile depuis un seul sous réseau, fut il très grand, et extrapoler à partir de là les résultats à l'ensemble de l'Internet. Sur base des informations que nous détenons à ce jour, il semble que cela ne soit possible que pour un sous ensemble, minoritaire, des attaques existantes. L'intérêt d'un système largement distribué s'en trouve d'autant plus justifié.

Armés d'un certain recul par rapport à l'amas de données collectées, nous avons entamé une démarche plus systématique de modélisation mathématique des phénomènes observés. Nous en livrons les premiers résultats, bien qu'embryonnaires dans la Section qui suit. Ils demandent à être affinés, validés et expliqués mais il nous semble important de les soumettre à une plus large audience en raison de leur caractère singulier. Nous espérons qu'ils généreront d'intéressantes interactions avec d'autres équipes à même de les confirmer ou au contraire de les invalider.

4 Modélisation à partir des données collectées

Les honeypots sont destinés à être la cible de plusieurs attaquants répartis géographiquement dans différents coins du globe. Généralement, on ne sait pas *a priori* à quels instants les attaques vont se produire, ni la source de ces attaques ni même leurs conséquences. Les vulnérabilités ciblées par ces attaques et les scénarios mis en œuvre pour les exploiter peuvent différer d'un attaquant à un autre. Par ailleurs, les résultats de ces scénarios peuvent dépendre de l'état dans lequel se trouve le système au moment de l'initialisation du processus d'attaque. Tous ces facteurs constituent des sources d'incertitude dont il faut tenir compte

dans les étapes d'analyse et de modélisation effectuées sur les données collectées. Les techniques statistiques et probabilistes sont bien adaptées pour prendre en compte ces incertitudes. Ceci justifie leur utilisation dans le cadre de ce projet, d'une part, pour caractériser le comportement des attaquants et les scénarios d'attaque, et d'autre part, pour construire des modèles et évaluer des mesures reflétant la capacité des systèmes à résister aux attaques.

Différentes analyses peuvent être effectuées sur les données issues des honeypots pour caractériser les attaques et effectuer des évaluations prévisionnelles. Par exemple, on peut élaborer des modèles caractérisant les processus d'occurrence des attaques dans le temps et dans l'espace en tenant compte de la localisation géographique des attaquants, de la source de ces attaques, des outils utilisés pour mettre en œuvre les attaques, du type de vulnérabilités ciblées, etc. Des prévisions peuvent être effectuées et mises à jour régulièrement par extrapolation à partir de l'analyse des données observées. Pour que ces prévisions soient possibles et valides, il est nécessaire d'avoir des données représentatives et une représentation fidèle des différents paramètres et hypothèses caractérisant le processus d'attaque.

Plusieurs questions peuvent être soulevées :

1. Quelles sont les distributions de probabilité qui caractérisent au mieux le, ou les, processus d'occurrence des attaques ?
2. Existe-t-il des processus réguliers d'apparition, de diffusion et de disparition de vagues d'attaques nouvelles ?
3. Existe-il une corrélation dans le temps entre les attaques qui proviennent de plusieurs sources (ou au contraire qui visent plusieurs destinations) et comment expliquer ces corrélations éventuelles ?
4. Les données observées sur des sites différents font-elles apparaître des comportements similaires ou différents ?

Notre démarche dans le cadre du projet *CADHo* consiste à explorer des méthodes qui sont traditionnellement utilisées dans le domaine de l'analyse et de l'évaluation de la sûreté de fonctionnement des logiciels et matériels à partir des données issues de l'observation opérationnelle. Nous les adaptons pour analyser les données issues des honeypots dans une optique d'analyse et d'évaluation de la sécurité. Ces méthodes reposent sur l'utilisation combinée de techniques statistiques d'analyse de données et de modèles stochastiques intégrant les résultats issus des analyses statistiques.

A titre d'illustration, nous présentons dans la suite quelques exemples de modélisations préliminaires que nous avons effectuées en utilisant les données collectées à partir des honeypots déployés jusqu'à présent. Ces exemples portent sur l'élaboration de modèles simples décrivant l'évolution dans le temps du nombre d'attaques enregistrées sur les honeypots et l'étude de corrélations éventuelles entre les courbes observées sur les différents honeypots, en considérant en particulier l'origine géographique de la source des attaques et la contribution relative des différents honeypots à l'activité d'attaque globale.

La période considérée pour l'exemple correspond à 65 semaines d'observations durant laquelle 23 honeypots ont été déployés progressivement. Le nombre total

d'attaques observées sur l'ensemble des honeypots est de 959802. Ces attaques ne sont pas réparties de façon uniforme entre les honeypots, en particulier en raison de la différence de la période d'observation et de l'intensité de l'activité d'attaque ciblant chacun d'eux. Par exemple, on peut noter que le honeypot correspondant à la période d'observation la plus longue (65 semaines) ne représente que 4,8% de l'activité d'attaque globale observée sur toute la période. En revanche, un autre honeypot qui a été observé pendant 36 semaines seulement représente plus de 20% de l'activité globale.

Considérons d'abord la courbe $Y(t)$ décrivant l'évolution du nombre total d'attaques par semaine enregistrées à partir de l'ensemble des honeypots, et par $X_j(t)$ la courbe donnant l'évolution du nombre total d'attaques par semaine enregistrées à partir de l'ensemble des honeypots en considérant uniquement les attaques dont la source provient du pays j. En considérant un modèle de régression linéaire [14], nous avons étudié si la courbe globale $Y(t)$ pour la période considérée peut être estimée à partir de la combinaison linéaire des courbes correspondant à un sous-ensemble de pays d'origine uniquement. On note par $Y^*(t)$ le modèle estimé à partir de la régression linéaire.

Formellement, il s'agit de trouver le modèle $Y^*(t)$ qui offre la meilleure adéquation avec les données observées et qui s'écrit sous la forme suivante :

$$Y^*(t) = \sum \alpha_j X_i(t) + \beta, j = 1, 2, ..k \tag{1}$$

Les constantes α_j et β correspondent aux paramètres du modèle linéaire et k est le nombre de pays considérés dans le modèle.

La qualité des estimations est appréciée à travers le calcul de la statistique R^2 définie comme suit :

$$R^2 = \sum (Y^*(i) - Y_{moy})^2 / \sum (Y(i) - Y_{moy})^2 \tag{2}$$

$Y(i)$ et $Y^*(i)$ correspondent respectivement aux valeurs observées et estimées du nombre d'attaques pour la semaine i toutes sources confondues.

En fait, R représente le facteur de corrélation entre le modèle estimé et les valeurs observées. Plus R^2 se rapproche de 1, meilleure est l'adéquation.

Nous avons étudié ce modèle en considérant des combinaisons linéaires, impliquant un, deux ou plusieurs pays. Les résultats obtenus sont très surprenants. Ils montrent que généralement en ne considérant que deux pays le modèle fournit une très bonne adéquation avec les valeurs observées ! Ce résultat se confirme dans le cas où on analyse la courbe décrivant l'évolution des attaques observées sur l'ensemble des honeypots, et aussi dans le cas où on considère les attaques observées sur chacun des honeypots pris de façon indépendante des autres. A titre d'illustration, le meilleur modèle estimé en considérant les attaques observées à partir de l'ensemble des honeypots est obtenu à partir de la combinaison linéaire des attaques provenant de la Russie et de la Chine. Le modèle estimé est le suivant :

$$Y^*(t) = 38,44X_1(t) + 2,29X_2(t) + 1041 \tag{3}$$

où $X_1(t)$ et $X_2(t)$ représentent l'évolution du nombre d'attaques issues de la Russie et de la Chine respectivement. La valeur du R^2 associée est égale à 0,989, ce qui exprime une très bonne adéquation du modèle aux données observées. Il est à noter que ces deux pays ne représentent pas une grande proportion des attaques observées. Les pourcentages sont respectivement de 1,84% pour la Russie et 9,41% pour la Chine !

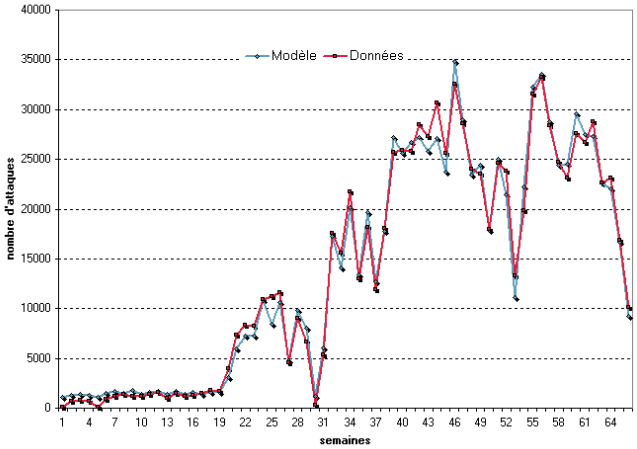

Fig. 1. Nombre d'attaques par semaine observées sur l'ensemble des honeypots et modèle estimé associé

Les modèles estimés en considérant chaque honeypot séparément sont résumés dans le tableau 1. On peut constater que tous les modèles obtenus présentent une bonne adéquation avec les données observées, reflétée par une valeur élevée du facteur de corrélation proche de 1. Néanmoins, chaque honeypot à un modèle particulier qui lui est associé et on ne retrouve pas toujours les mêmes pays qui interviennent dans le modèle de régression qui offre la meilleure adéquation.

Les résultats ci-dessus restent à confirmer dans la durée et surtout il est important de leur associer une justification pour valider leur pertinence. Par ailleurs, des modèles plus élaborés sont en cours d'exploration pour analyser des phénomènes de propagation d'attaques entre environnements et également pour aboutir à des évaluations prévisionnelles.

5 Honeypots "haute interaction"

Les honeypots actuellement déployés dans le cadre du projet sont dits de "faible interaction" dans le sens où ils contraignent le type d'actions qui peuvent être effectuées par les attaquants. En particulier, par conception, ces systèmes ne permettent pas aux attaquants de prendre le contrôle de la machine attaquée. Les attaquants n'ont pas accès à un système d'exploitation ou des services qu'ils

Honeypot	α_1	Pays 1	α_2	Pays 2	β	R^2
H1	14,9681	CA	3,9171	KR	17,34	0,9126
H2	7,9203	DE	1,8930	US	54,55	0,9450
H3	2,8879	DE	2,6169	FR	385,03	0,8785
H4	18,0555	BG	0,8341	YU	286,57	0,9472
H5	7,3315	FR	3,7627	US	148,33	0,9586
H6	1,0413	TW	2,4610	US	86,60	0,9940
H7	11,7527	FR	4,5351	KR	36,11	0,9940
H8	7,5020	DE	9,4870	TR	92,87	0,9318
H9	2,4173	CN	1,5676	US	49,11	0,9635
H10	8,4599	DE	1,7484	US	110,24	0,8869
H11	5,7164	DE	6,1320	NL	82,09	0,9230
H12	47,6553	DK	18,8589	PL	213,65	0,9302
H13	20,3369	GB	5,3688	JP	542,06	0,9544
H14	7,0876	DE	1,5926	US	58,85	0,9819
H15	43,5248	AR	2,3384	CI	-15,15	0,9962
H16	1,2438	CN	3,0631	US	40,28	0,9924
H17	18,6355	FR	1,4165	US	56,53	0,9009
H18	10,1001	FR	1,5866	US	79,97	0,9416
H19	1,1266	CA	12,3471	TW	-0,75	0,9973
H20	6,0909	DE	1,6114	US	220,22	0,9797
H21	11,1849	BE	5,0981	US	42,99	0,9881
H22	1,5656	CH	1,0505	KR	5,15	0,9989
H23	26,2325	IL	4,1914	US	-5,51	0,9926

Tab. 1. Tableau des corrélations pour chaque Honeypot

peuvent compromettre réellement. Ils ne peuvent que “frapper à la porte” sans jamais pouvoir entrer. En particulier, les attaquants peuvent uniquement interroger des ports ou envoyer des requêtes à des serveurs fictifs sans jamais avoir la possibilité d'y accéder directement.

Dans le cadre du projet *CADHo*, nous envisageons également de mettre en œuvre un environnement de honeypots plus sophistiqué, dit de “haute interaction”, dans le but de faire des analyses plus poussées des étapes qui succèdent à la prise de contrôle d'une machine attaquée. Il ne s'agit pas de leur laisser la possibilité de lancer des attaques vers d'autres machines sur le réseau Internet, qui sont extérieures à l'environnement qui est sous notre contrôle, mais plutôt de les laisser progresser à l'intérieur d'un Intranet et étudier les scénarios d'attaque qu'ils mettent en œuvre. Nous nous rapprochons en cela de l'architecture préconisée par le Honeynet Project [3]. Cependant, une caractéristique spécifique importante de l'environnement qui sera développé sera d'offrir la possibilité de sélectionner les attaquants ou les types d'attaques que nous souhaiterions observer et analyser en détail. En effet, notre objectif n'est pas d'observer toutes les attaques qui sont susceptibles de prendre pour cible notre honeypot, mais de considérer uniquement celles qui sont représentatives d'une large classe d'attaquants de telle sorte que les résultats des analyses issues des données collectées

soient généralisables, ou bien de focaliser sur les attaques manuelles réalisées par des attaquants humains.

Le honeypot de haute interaction qui sera mis en œuvre dans le cadre du projet *CADHo* sera déployé sur un nombre limité de sites qui seront hautement contrôlés. Les expérimentations et les analyses qui seront effectuées à partir des données collectées nous permettront de poursuivre deux objectifs. Le premier est de mieux comprendre les processus d'attaque, en particulier ceux réalisés par des attaquants expérimentés. Ces connaissances nous permettront d'apporter des réponses concrètes pour améliorer les techniques et outils de détection d'intrusions ciblant ce type d'attaques et pour lesquelles aucune solution valable n'existe encore. Le second objectif est d'apporter une réponse concrète pour l'évaluation de l'impact de ce type d'attaques sur la sécurité des systèmes cibles. Dans ce sens, nous proposons d'utiliser les observations opérationnelles pour valider un modèle théorique que nous avions initialement proposé lors de nos travaux dans le cadre de l'approche d'évaluation quantitative de la sécurité [15,16]. Il s'agissait d'une méthode d'évaluation probabiliste de la sécurité qui se démarquait des démarches traditionnelles basées sur des critères qualitatifs (livre rouge, ITSEC, critères communs, etc.). Notre méthode est basée sur la représentation par un graphe de privilèges des vulnérabilités identifiées sur les systèmes cibles et des différents scénarios d'exploitation de ces vulnérabilités par des attaquants éventuels pour mettre en défaut la sécurité. L'interprétation de ce graphe sous forme d'un modèle probabiliste permet d'évaluer des mesures quantitatives caractérisant la capacité des systèmes à résister à des attaques éventuelles. Dans nos travaux antérieurs, la génération du processus d'attaque à partir du graphe des privilèges était basée sur des hypothèses sur le comportement des attaquants qui n'ont pas pu être validées en raison de l'absence d'observations opérationnelles. Le développement d'un environnement de honeypots de "haute interaction" et la mise en œuvre de cet environnement en menant des expérimentations ciblant un sous-ensemble d'attaques bien choisies, nous permettra de disposer des données nécessaires pour valider ces hypothèses et de proposer ainsi une solution novatrice à l'analyse opérationnelle des scénarios d'attaque et l'évaluation de leur impact sur la sécurité.

6 Conclusions

La plateforme de collecte d'informations distribuée *Leurré.com* basée sur des honeypots est opérationnelle depuis plusieurs mois. Nous encourageons toute équipe désireuse d'avoir accès à nos données à nous contacter afin de connaître les modalités pour pouvoir héberger une de nos plateformes.

Les données recueillies jusqu'à présent offrent une vision plus précise des phénomènes d'attaque qui se déroulent sur l'Internet. Leur analyse offre de nombreuses justifications pour le déploiement d'une telle plateforme distribuée. Les premiers modèles mathématiques utilisés pour modéliser les phénomènes d'attaques font ressortir des relations que nous ne nous expliquons pas encore mais qui semblent prometteurs pour l'éventuelle obtention de modèles prédictifs à

même de détecter rapidement toute nouvelle attaque qui apparaitrait sur la toile.

Références

1. *ACI Sécurité et Informatique*, `http ://acisi.loria.fr`
2. L. Spitzner, *Honeypots : Tracking Hackers*, Add.-Wesley, ISBN from-321-10895-7, 2002
3. Home Page du projet Honeynet, `http ://www.honeynet.org/`, dernière visite 03/2005
4. *French Honeynet Project*, http ://honeynet.rstack.org
5. VMware Corporation Home Page, `http ://www.vmware.com`
6. Honeyd Home page, `http ://www.citi.umich.edu/u/provos/honeyd`
7. F. Pouget, T. Holz, "A Pointillist Approach for Comparing Honeypots", *Proc. Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2005)*, Vienne (Autriche), Juillet 2005.
8. F. Pouget, M. Dacier, H. Debar, "Honeynets : Foundations for the Development of Early Warning Systems", *Proc. Cyberspace Security and Defense : Research Issues (NATO ARW Series)*, Gdansk (Pologne), 2005.
9. M. Dacier F. Pouget, H. Debar, "Honeypots : Practical Means to Validate Malicious Fault Assumptions on the Internet", *Proc. 10th IEEE International Symposium Pacific Rim Dependable Computing (PRDC10)*, Mars 2004, pages 383-388.
10. M. Dacier, F. Pouget, H. Debar, "Attack Processes found on the Internet", *Proc. NATO Symposium IST-041/RSY-013*, Toulouse (France), Avril 2004.
11. F. Pouget, M. Dacier, "Honeypot-based Forensics", *Proc. AusCERT Asia Pacific Information Technology Security Conference (AusCERT'2004)*, Brisbane (Australia), Mai 2004.
12. F. Pouget, M. Dacier, V.H. Pham, "Towards a Better Understanding of Internet Threats to Enhance Survivability", *Proc. International Infrastructure Survivability Workshop (IISW'04)*, Lisbonne (Portugal), Décembre 2004.
13. F. Pouget, M. Dacier, V.H. Pham, "Leurre.com : On the Advantages of Deploying a Large Scale Distributed Honeypot Platform", *Proc. E-Crime and Computer Evidence Conference (ECCE 2005)*, Monaco, Mars 2005.
14. G. Saporta, *Théories et méthodes de la statistique*, Editions TECHNIP, ISBN 2.7 108-0351-8,1978
15. M. Dacier, Y. Deswarte, M. Kaâniche, "Models and tools for quantitative assessment of operational security", *Proc. 12th International Information Security Conference (IFIP SEC'96)*, Samos (Greece), Mai 1996, pages 177-186
16. R. Ortalo, Y. Deswarte, M. Kaâniche, "Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security", *IEEE Transactions on Software Engineering*, Vol.25, N°5, pages 633-650, Septembre/Octobre 1999.