ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) FASCICULE DE BREVET

(11) N° de publication :
MA 37591 A1

(51) Cl. internationale :
H04L 29/06

(43) Date de publication :
30.06.2016

(21) N° Dépôt :
37591

(22) Date de Dépôt :
28.11.2014

(71) Demandeur(s) :
UNIVERSITE INTERNATIONALE DE RABAT, PARC TECHNOPOLIS RABAT-SHORE,CAMPUS UNIVERSITAIRE UIR, ROCADE RABAT-SALE, 11100, (MA)

(72) Inventeur(s) :
younes moumen

(74) Mandataire :
BOUYA MOHSINE

(54) Titre : **POT DE MIEL POUR L'ENREGISTREMENT DE PREUVES LEGALES D'ACTES INFORMATIQUES MALVEILLANTS**

(57) Abrégé : Un pot de miel conçu pour simuler le fonctionnement exact d'un site Web et reproduire son activité. Il se comporte comme un proxy pour les requêtes entrantes. Sauf que les requêtes sortantes ne sont pas directement initiées depuis Le pot de miel mais relayés à travers des agents distribués sur Le réseau internet. L'objectif étant de tracer les activités des sites internet malveillants sans que cela ne soit détecté par leurs utilisateurs.

Dessins

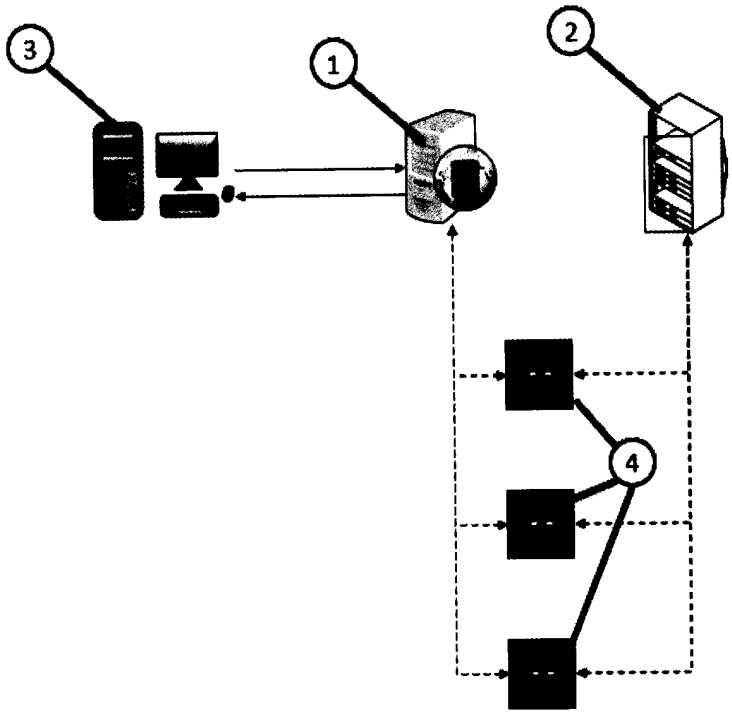

Figure 1

MA 37591A1

30 JUIN 2016

Pot de miel pour l'enregistrement de preuves légales d'actes informatiques malveillants

Description

L'invention est relative aux systèmes de sécurité informatique. En particulier, il s'agit d'un pot de miel.

Les pots de miel sont des outils informatiques à multiples usages dont l'objectif est généralement d'améliorer la sécurité internet. Ce sont des systèmes qui existent pour être testés, compromis et attaqués. En particulier, ils ont l'objectif commun d'enregistrer les activités malveillantes pour analyse. Nous retrouvons une multitude de pots de miel avec des utilisations très diverses.

Les pots de miel les plus répondus ont une fonction principale anti-spam. Ils détectent et traitent les requêtes indésirables dans les forums, les formulaires de contact, d'inscription, etc. Leur principe de fonctionnement est généralement l'utilisation de champs qui sont visibles pour les robots mais pas par les êtres humains. Lorsque ces champs sont remplis, le pot de miel signale qu'il s'agit d'un robot et traite la requête sur la base de cette information. Certains pots de miel ajoutent également le paramètre temps de remplissage du formulaire Web qui est généralement très rapide pour les robots et lent pour les êtres humains : Un humain ne peut pas remplir un formulaire en moins d'un seuil de temps fixé.

D'autres pots de miel dits avec haute interaction sont des systèmes exécutant des activités semblables à des systèmes en production où des vulnérabilités sont insérées volontairement pour attirer les hackers. Ces systèmes sont équipés d'outils de journalisation des activités du hacker pour analyse et post-traitement.

D'autres pots de miel dits de faible interaction simulent des vulnérabilités spécifiques sans offrir un environnement d'exécution complet.

Certains open proxys sont également des pots de miel. Les open proxys sont des relais entre l'utilisateur et les systèmes auxquels il se connecte. Les proxys servent entre-autres à contrôler les accès et la distribution des bandes passantes d'un réseau fermé par exemple. Les open proxys servent principalement à cacher l'identité de l'utilisateur en cachant son adresse IP. Ces pots de miel de type open proxy proposent au hacker de cacher son identité alors qu'en réalité, ils traquent toutes ses activités.

Chaque type de pot de miel a une utilité spécifique selon son utilisation. Toutefois, les pots de miel restent des systèmes principalement passifs qui attendent l'intrusion du hacker ou du robot pour faire un traitement ou pour journaliser l'activité pour un traitement postérieur. Ils sont utilisés comme moyen défensif dans la sécurité internet. Notre invention propose un pot de miel qui sert à identifier et tracer l'activité des hackers dans leurs propres domaines et sites Web qu'ils utilisent. Les sites web doivent être soupçonnés au préalable d'activité malveillante (terrorisme, vol d'identités, contrefaçon, etc). En vue de son caractère intrusif, ce pot de miel devra être utilisé uniquement après décision judiciaire.

Notre invention est constituée d'un pot de miel proxy modifié (1). Il doit être déployé après modification de l'aiguillage DNS pour passer de l'adressage vers le site ciblé (2) à l'adressage vers le proxy (1). Ce dernier intercepte les requêtes émanant des hackers (3) destinées vers le site ciblé (2). Les requêtes sont journalisées et traitées au niveau du proxy pour identifier les hackers ou les proxys utilisés par ces derniers. De l'autre côté le proxy envoie les requêtes sortantes à des relais (4) distribués dans le réseau internet. Ces relais renvoient les requêtes vers le site Web ciblé (2) qui les traite et renvoie les réponses vers le hacker. Ceci est effectué en toute transparence pour le hacker.

Ainsi lorsque le hacker (3) envoie une requête au site Web ciblé (2), le pot de miel l'intercepte par modification ou redirection DNS. Il effectue les traitements de journalisation et apporte les modifications nécessaires à la requête qui est renvoyée à l'un des agents (4) déployés dans le réseau internet. L'agent (4) ayant reçu la requête la transmet ensuite au site Web. Les agents sont déployés pour simuler une activité quasi-normale dans le site Web.

La figure 1 illustre la structure de déploiement du pot de miel.

Revendications

1- Un pot de miel informatique caractérisé par le procédé de traitement suivant : à chaque fois que le hacker (3) envoie une requête au site Web ciblé (2), le pot de miel (1) l'intercepte par modification ou redirection DNS. Il effectue les traitements de journalisation et apporte les modifications nécessaires à la requête qui est renvoyée à l'un des agents (4) déployés dans le réseau internet. L'agent (4) ayant reçu la requête la transmet ensuite au site Web.

Abrégé

Un pot de miel conçu pour simuler le fonctionnement exact d'un site Web et reproduire son activité. Il se comporte comme un proxy pour les requêtes entrantes. Sauf que les requêtes sortantes ne sont pas directement initiées depuis le pot de miel mais relayés à travers des agents distribués sur le réseau internet. L'objectif étant de tracer les activités des sites internet malveillants sans que cela ne soit détecté par leurs utilisateurs.

MA 37591A1

ROYAUME DU MAROC
****
OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
****

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية

RAPPORT DE RECHERCHE AVEC OPINION SUR LA BREVETABILITE

(Conformément aux articles 43 et 43.2 de la loi 17-97 relative à la protection de la propriété industrielle)

Renseignements relatifs à la demande	
N° de la demande : 37591	Date de dépôt : 28/11/2014
Déposant : UNIVERSITE INTERNATIONALE DE RABAT	
Intitulé de l'invention : POT DE MIEL POUR L'ENREGISTREMENT DE PREUVES LEGALES D'ACTES INFORMATIQUES MALVEILLANTS	

Le présent document est le rapport de recherche avec opinion sur la brevetabilité établi par l'OMPIC conformément aux articles 43 et 43.2, et notifié au déposant conformément à l'article 43.1 de la loi 17-97 relative à la protection de la propriété industrielle telle que modifiée et complétée par la loi 23-13.

Les documents cités par l'examinateur dans la partie rapport de recherche sont joints au présent document

Le présent rapport contient des indications relatives aux éléments suivants :

Partie 1 : Considérations générales
- ☒ Cadre 1 : Base du présent rapport
- ☐ Cadre 2 : Priorité
- ☐ Cadre 3 : Titre et/ou Abrégé tel qu'ils sont définitivement arrêtés

Partie 2 : Rapport de recherche

Partie 3 : Opinion sur la brevetabilité
- ☐ Cadre 4 : Remarques de clarté
- ☒ Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle
- ☐ Cadre 6 : Observations à propos de certaines revendications dont aucune recherche significative n'a pu être effectuée
- ☐ Cadre 7 : Défaut d'unité d'invention

Examinateur: BAMI MOHAMMED	**Date d'établissement du rapport** : 03/03/2015
Téléphone: **212 5 22 58 64 14/00**	

Partie 1 : Considérations générales

Cadre 1 : base du présent rapport

Les pièces suivantes de la demande servent de base à l'établissement du présent rapport :

- Description
  2 Pages
- Revendications
  1
- Planches de dessin
  1 Pages

Partie 2 : Rapport de recherche

Classement de l'objet de la demande :

CIB : H04L29/06

Bases de données électroniques consultées au cours de la recherche :

EPOQUE, Orbit

Catégorie*	Documents cités avec, le cas échéant, l'indication des passages pertinents	N° des revendications visées
X	EP1900172 A1 19/03/ 2008 Gatesweeper solutions inc.	1
A	http://searchsecurity.techtarget.com/feature/Honeypot-technology-How-honeypots-work-in-the-enterprise 10/11/2013 Lance Spitzner	1

***Catégories spéciales de documents cités :**

-« **X** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
-« **Y** » document particulièrement pertinent ; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
-« **A** » document définissant l'état général de la technique, non considéré comme particulièrement pertinent
-« **P** » documents intercalaires ; Les documents dont la date de publication est située entre la date de dépôt de la demande examinée et la date de priorité revendiquée ou la priorité la plus ancienne s'il y en a plusieurs
-« **E** » Éventuelles demandes de brevet interférentes. Tout document de brevet ayant une date de dépôt ou de priorité antérieure à la date de dépôt de la demande faisant l'objet de la recherche (et non à la date de priorité), mais publié postérieurement à cette date et dont le contenu constituerait un état de la technique pertinent pour la nouveauté

Partie 3 : Opinion sur la brevetabilité

Cadre 5 : Déclaration motivée quant à la Nouveauté, l'Activité Inventive et l'Application Industrielle

Nouveauté (N)	Revendications 1 Revendications aucune	Oui Non
Activité inventive (AI)	Revendications aucune Revendications 1	Oui Non
Possibilité d'application Industrielle (PAI)	Revendications 1 Revendications aucune	Oui Non

Il est fait référence aux documents suivants. Les numéros d'ordre qui leur sont attribués ci-après seront utilisés dans toute la suite de la procédure

D1 : EP1900172 A1

1. **Nouveauté (N) :**

Aucun des documents cités ci-dessus, ne divulgue l'ensemble des caractéristiques techniques énoncées dans la revendication 1.
Par conséquent, l'objet de la revendication 1 est nouveau au sens de l'art. 26 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

2. **Activité inventive (AI) :**

Le document D1 est considéré comme l'état de la technique le plus proche de l'objet de la revendication 1, et divulgue un procédé caractérisé par les étapes suivantes :
L'interception de la requête générée par le hacker
La redirection de la requête vers un pot de miel déployé sur internet
Le pot de miel effectue les traitements de journalisation des activités du hacker
Par conséquent, l'objet de la revendication 1 diffère de D1 en ce que :
L'interception est faite par modification ou redirection DNS
La requête est renvoyée à l'un des agents déployés dans le réseau internet.
Le problème objectif que la présente demande se propose de résoudre peut être considéré comme : un pot de miel pour l'analyse des activités des hackers.
La solution proposée par la présente demande n'est qu'une alternative à la solution proposée dans le document D1. En effet, les caractéristiques distinctives de la revendication 1 ne constituent que l'une des options que l'homme du métier sélectionnerait, selon le cas, parmi plusieurs possibilités évidentes, afin de résoudre le problème posé sans faire preuve d'esprit inventif.
Par conséquent, l'objet de la revendication 1 n'implique pas une activité inventive au sens de l'art.28 de la loi 17/97 telle que modifiée et complétée par la loi 23/13.

3. **Possibilité d'application industrielle (PAI) :**

L'objet de la présente invention est susceptible d'application industrielle au sens de l'article 29 de la loi 17-97 telle que modifiée et complétée par la loi 23-13, parce qu'il présente une utilité déterminée, probante et crédible.