Les attaques web

WannaCry

Mirai

Réalisé par : GHARBI Wissal

Groupe : 4 ING-A

Annee scolaire : 2018/2019

Les attaques web

Introduction

Au meme titre qu'une application classique ou qu'un systéme d'exploitation, les applications Web peuvent presenter des failles de sécurité. Cela est d'autant plus grave que les applications Web manipulent parfois des donnees confidentielles (mots de passe, numéros de cartes bancaires) et qu'elles sont genéralement déployées sur Internet et donc exposées au public. Méme sur un serveur Web sécurisé tournant sur un systeme d'exploitation réputé sur (Apache sur OpenBSD, par exemple), des failles de sécurité peuvent subsister, car elles sont la plupart du temps dues a des fautes de programmation de l'application elle-meme, et non du serveur.

1. Le déni de service « DoS : Denial of Service»

Le déni de service est une attaque qui vise à rendre une application informatique incapable de répondre aux requêtes de ses utilisateurs. Les serveurs de messagerie peuvent être victimes de ces attaques. Le déni de service distribué (DDoS pour Distributed DoS) est une attaque de DoS émise depuis plusieurs origines distinctes. Ce type d'attaque est extrêmement complexe à bloquer, car il est souvent impossible de différencier une vraie requête d'une requête de DDos. L'attaque par DDos utilise très souvent une multitude de PC zombies infectés par des backdoors exploités à distance par un pirate et attaquant simultanément une cible unique.

2. La défiguration/défacement « Defacing »

La défiguration est l'altération visuelle de l'apparence d'un site Internet piraté. La nouvelle apparence du site peut être uniformément noire, blanche ou comporter des messages, des images, des logos et vidéos sans rapport avec l'objet initial du site, voire une courte mention comme « owned » ou « hacked ».

La défiguration est le signe visible qu'un site web a été attaqué et que le ou les attaquants en ont obtenu les droits, leur permettant ainsi d'en modifier le contenu.

La défiguration est un acte qui peut être d'une grande gravité pour l'organisation qui en est victime. Durant l'attaque, le site n'est souvent plus utilisable au moins partiellement, ce qui peut entraîner des pertes directes de revenus pour les sites marchands et des pertes de productivité. Par ailleurs, ce type d'attaque est visible publiquement voire médiatiquement et démontre que l'attaquant a pu prendre le contrôle du serveur, donc potentiellement accéder à toutes ses données y compris les plus sensibles (données personnelles, bancaires, commerciales…), ce qui porte directement atteinte à la notoriété, au sérieux, donc à la crédibilité du propriétaire du site auprès de ses utilisateurs, clients, usagers, partenaires, actionnaires…

3. Les injections SQL

Une injection SQL est un type d'exploitation d'une faille de sécurité d'une application interagissant avec une base de données. L'attaquant détourne les requêtes en y injectant une chaîne non prévue par le développeur et pouvant compromettre la sécurité du système.

C'est un cas particulier d'un type de vulnérabilité plus général qui peut se manifester lorsqu'un langage est imbriqué dans un autre.

Lorsqu'on évoque l'injection SQL, on parle tout le temps de faille dans un site Web, mais il n'y a pas que les sites qui sont touchés par cette faille: n'importe quelle application dialoguant avec une base de données en utilisant des requêtes sur lesquelles l'utilisateur a une influence peut être vulnérable aux injections SQL.

4. Le cross-site scripting « XSS»

Les attaques XSS ciblent le code (appelé également le script) d'une page web exécutée dans le navigateur de l'utilisateur plutôt que sur le serveur du site web. Lorsque vous êtes attaqué, des scripts malveillants essayant d'endommager votre ordinateur sont injectés dans votre navigateur. Il existe presque une variété infinie d'attaques XSS, mais la plupart essayent de récolter des données personnelles, de rediriger les victimes vers des sites web contrôlés par le pirate informatique ou de faire effectuer des actions à votre PC pour le compte du pirate informatique.

5. Attaque CSRF « Cross-site Request Forgeries»

Les attaques de type cross-site request forgery (ou CSRF) sont mal connues et trop souvent non prises en compte par les développeurs de sites Internet. Elles sont également souvent confondues avec les attaques de type injection de code indirecte (cross-site scripting ou XSS) alors que le principe est quelque peu différent.

En français, un cross-site request forgery est une injection de requête(s) illégitime(s) par rebond. Concrètement, pour un attaquant, cela consiste à effectuer des opérations sur un site sans le consentement d'un utilisateur.

L'attaque consite à provoquer l'envoi de requêtes (par exemple, GET ou POST) par une victime vers un site vulnérable (V), à son insu et en son nom. L'envoi des requêtes se fait lorsque la victime visite un site malveillant ou compromis (M), ou clique sur un lien. L'attaque cible toujours un ou plusieurs sites en particulier qui sont vulnérables. Le CSRF se fait toujours en aveugle, car l'attaquant provoque l'envoi d'une ou plusieurs requêtes sans obtenir de réponse.

6. L'hameçonnage « Phishing »

L'hameçonnage est une approche détournée qu'utilisent les cyber-escrocs pour vous pousser à révéler des informations personnelles, comme des mots de passe ou des numéros de carte de crédit, de sécurité sociale ou de compte bancaire. Ils le font en vous envoyant des e-mails contrefaits ou en vous dirigeant sur un site web contrefait.

Conclusion

Le meilleur moyen de protéger nos données contre de telles attaques malveillantes consiste à faire une sauvegarde complète de tous les fichiers dans un système séparé.

Les "Malicious Ransomware" peuvent être envoyés par diverses sources telles que les courriels, les publicités, en créant des sites Web et bien d'autres choses pouvant partager le ransomware malveillant avec les utilisateurs de l'ordinateur.

Il faut assurer que la gestion des vulnérabilités est toujours sur une priorité élevée, y compris la gestion des correctifs et l'analyse des vulnérabilités, ce qui est essentiel pour la sécurité de nos données et de notre système.

WannaCry

Introduction

Le vendredi 12 mai 2017, WannaCry a commencé à affecter les ordinateurs dans le monde entier. L'épidémie a commencé en Asie au début de la matinée et s'est répandue dans la journée. Plus de 200 000 ordinateurs auraient été infectés. A titre d'exemple, seize hôpitaux britanniques n'ont pas pu accéder à leurs systèmes. Des entreprises comme Renault, Deutsche Bahn et Telephonica ont également été touchées. Le 14 mai, les effets de WannaCry se faisaient sentir sur tous les continents.

1. Fonctionnement de WannaCry

Baptisé WannaCry, ce logiciel malveillant fait partie de la famille des « rançongiciels ». Une fois installé sur un ordinateur, il chiffre son contenu pour le rendre inaccessible à son propriétaire, et réclame une rançon de 300 dollars, à payer en bitcoins, pour le déverrouiller.

Ces logiciels sont plutôt courants. Ce qui distingue WannaCry des autres, c'est l'extrême rapidité de sa diffusion. Selon la police française, plus de 75 000 ordinateurs ont été infectés dans le monde et ce nombre « devrait très vraisemblablement s'alourdir dans les jours qui viennent ». Cela en fait déjà la plus importante diffusion d'un logiciel de ce type de l'histoire.

2. Conséquences de WannaCry

WannaCry a été la plus grande attaque de rançongiciel de l'histoire. Son effet a été global avec, selon les estimations, des ordinateurs infectés dans plus de 150 pays en seulement 72 heures. La Russie, l'Ukraine et plus généralement les pays de l'ancienne Union Soviétique ont été particulièrement touchés. Les ordinateurs des ministères de l'Intérieur de la Russie et de la Chine ont été infectés.

Cependant, les autorités conseillèrent le public de ne pas payer la rançon et ce conseil a été largement suivi. Les comptes Bitcoin mis en place par les pirates informatiques

ont reçu un peu plus de 100 000 dollars et ce montant n'a pas été transféré jusqu'à présent. Si la motivation était financière, WannaCry a été un échec.

3. Qui était derrière WannaCry :

L'attribution de la responsabilité de WannaCry reste incertaine à ce stade et repose largement sur des preuves circonstancielles. WannaCry possède deux composantes, le vecteur d'infection des réseaux (la partie qui installe le logiciel malveillant dans les ordinateurs) et le crypto-verrouilleur (la partie qui crypte les fichiers). La première composante peut être attribuée directement à la fuite provenant de la NSA. Divers acteurs ont noté des similitudes dans la deuxième composante avec des codes informatiques qui ont été utilisés dans le passé par un groupe baptisé « Lazarus ». On a déjà attribué la responsabilité d'incidents cyber à ce groupe, probablement lié aux services de renseignement nord-coréens.

Mirai

Introduction

Un pirate a publié le code source de Mirai, le botnet qui s'est appuyé sur l'internet des objets pour lancer l'attaque de déni de service qui a mis hors ligne le site KrebsOnSecurity le mois dernier. Mirai se déploie sur des dispositifs vulnérables en analysant en continu internet pour rechercher des systèmes connectés protégés par les identifiants attribués par défaut ou codés directement dans les systèmes. Les dispositifs vulnérables sont alors attaqués par le logiciel qui les transforme en bots, les obligeant à communiquer avec un serveur de contrôle central qui peut être utilisé comme lieu de préparation pour lancer des attaques DDoS puissantes qui peuvent entre autres paralyser un site.

1. Fonctionnement de Mirai

Mirai recherche les services ouverts, dont Telnet, un protocole d'application utilisé pour l'accès à distance. Telnet

est utilisé et installé sur l'IoT et d'autres appareils depuis des décennies. Le botnet utilise ensuite une attaque par force brute,

exploiter une série d'informations d'identification pour accéder au périphérique (par exemple, une caméra, un enregistreur numérique, un routeur ou un autre matériel connecté).

Une fois à l'intérieur d'une machine, le malware tentera de tuer et de bloquer tout ce qui tourne sur les ports 22 (SSH), 23

(Telnet) et 80 (HTTP), qui sont des ports Internet et de connectivité standard. Cette action empêche le propriétaire

de reprendre le contrôle de l'appareil. Il corrige également le périphérique contre les logiciels malveillants externes, ce qui permet acteurs de la menace de posséder la machine.

2. Le code Mirai

Le virus est conçu pour plusieurs architectures de processeurs différentes (x86, ARM, Sparc, PowerPC, Motorola) afin de couvrir les différents processeurs déployés dans des périphériques IoT. L'image elle-même est petite et utilise plusieurs techniques pour

rester inconnue et pour masquer ses mécanismes internes résultant de tentatives d'ingénierie inverse.

Une fois que le virus est chargé en mémoire sur le BOT, il se supprime de son disque. Le virus restera actif jusqu'au redémarrage du BOT. Immédiatement après un redémarrage, l'appareil n'est plus infecté par le virus. Toutefois, il ne faut que quelques minutes avant qu'il soit à nouveau découvert et réinfecté.

Les vecteurs d'attaque sont hautement configurables à partir du CnC mais par défaut, Mirai a tendance à randomiser les différents champs (numéros de port, numéros de séquence, ident, etc.) dans les paquets d'attaque afin qu'ils changent à chaque paquet envoyé.

3. Comment se défendre contre les attaques par DDoS de Mirai Botnets

Mirai continuera à être une menace jusqu'à ce que les dispositifs mal protégés soient sécurisés. Cependant, le maintien de ces dispositifs n'est pas quelque chose que les victimes d'attaques de Mirai n'ont aucun contrôle.

Le système de défense contre les menaces (TDS) Corero SmartWall offre diverses protections contre les attaques de type Mirai. L'équipe Corero Security Operations Team (SOC) possède également une expérience approfondie de la gestion des attaques Mirai et peut activer des fonctions d'atténuation supplémentaires pour les clients ne bénéficiant pas déjà de l'offre de services gérés SecureWatch.