IUT LYON 1

Etude des risques

Livrable GPI

« Cuisine de chez vous »
14/01/2022

Table des matières

Événements redoutés : 2
Sources de risques et objectifs visés : 3
Valeurs métier et biens supports : 4
Scénarios de risques 5
Un cyber attaquant pirate des utilisateurs via la messagerie 5
Un cyberattaquant test ses capacités en détournant une session 6
Un membre se fait voler son identité par un pirate 7
L'hébergeur subit un incident technique 7
Un utilisateur poste du contenue non conforme dans l'espace commentaire 7
Plan d'action 8
Un cyber attaquant pirate des utilisateurs via la messagerie 8
Un cyberattaquant test ses capacités en détournant une session 8
Un membre se fait voler son identité par un pirate 8
L'hébergeur subit incident technique 8
Un utilisateur poste du contenue non conforme dans l'espace commentaire 9

Événements redoutés :

Le tableau suivant présente les principaux événements redoutés par rapport au site « Cuisine de chez vous » :

	Dispo	Intégrité	Confidentialité	Gravité	Retenu ?
Fuite de données personnelles			X	**Significative**	**OUI**
Altération de données		X		**Importante**	**OUI**
Base de données injoignable	X			**Importante**	**OUI**
Usurpation des données d'identification d'un membre		X	X	**Significative**	**OUI**
Hébergeur est hors service, pour une courte période	X			**Significative**	**NON**
Hébergeur est hors service, pour une longue période	X			**Importante**	**OUI**
Contenus non-conformes		X		**Minimale**	**NON**

Sources de risques et objectifs visés :

Le tableau suivant présente les sources de risques et leurs objectifs visés, jugés comme pertinents par rapport au site « Cuisine de chez vous »:

Source de risque	Objectif visé	Motivation	Ressources	Pertinence	Retenu ?
Cyberattaquant	Tester ses capacités, nuire à l'image du site, cibler un utilisateur.	Peu motivé	Importante	Plutôt pertinente	OUI
Administrateur informatique	Saboter les services, modifier la base de données, par vengeance.	Très peu motivé	Illimitées	Très pertinente	OUI
Sites concurrents	Dénigrer le site web, appelle au boycott.	Peu motivé	Faible	Peu pertinente	NON

Valeurs métier et biens supports :

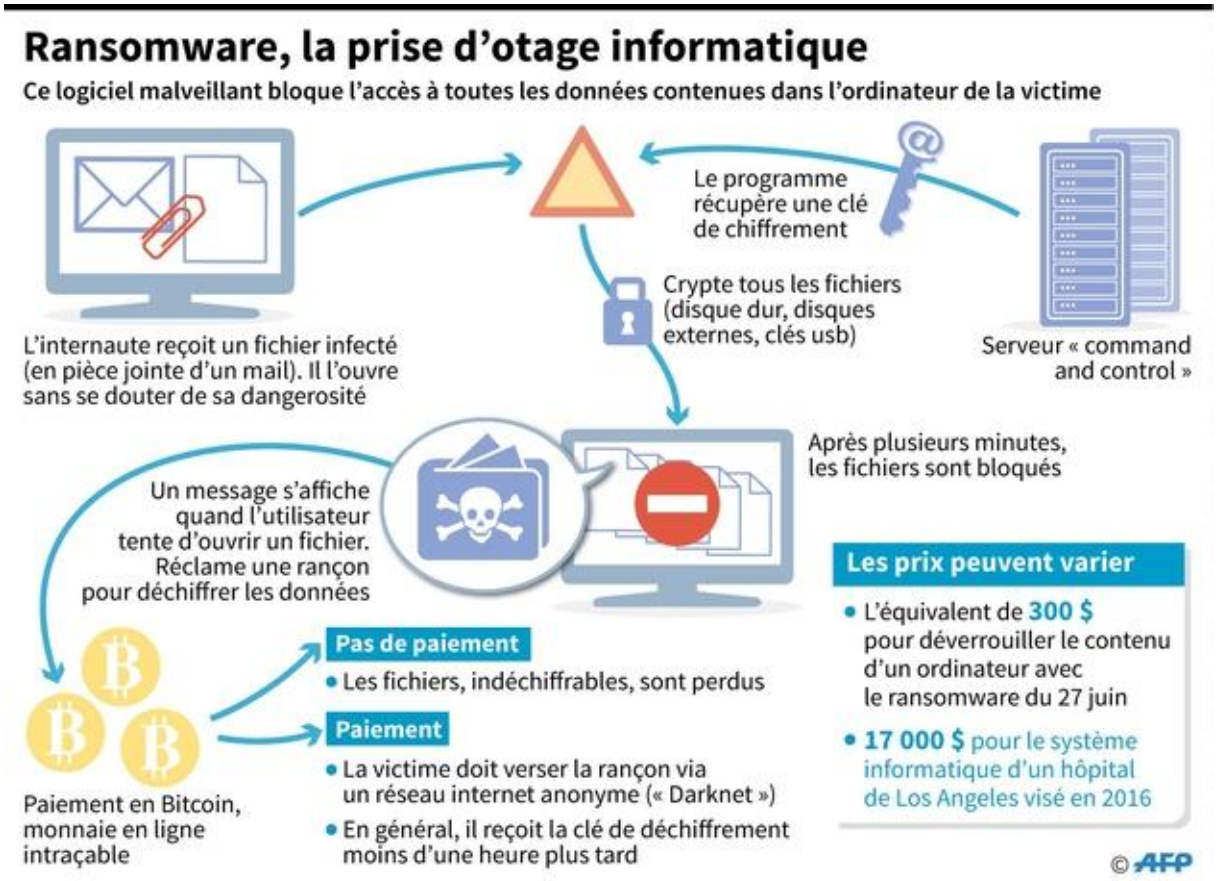
Le tableau suivant montre sur quels biens supports reposent les valeurs métier :

Valeurs métiers / Biens supports	Gérer les services web	Enregistrer des recettes	Télécharger une recette	Gérer la publication de recette	Gérer l'espace commentaire	Gérer les membre
Site web public	X	X		X	X	X
Utilisateur	X	X	X	X	X	X
Chat (commentaire)	X				X	X
Base de données	X	X	X	X	X	X

Scénarios de risques

Cette partie présente l'analyse des risques déclinée en scénario opérationnel.

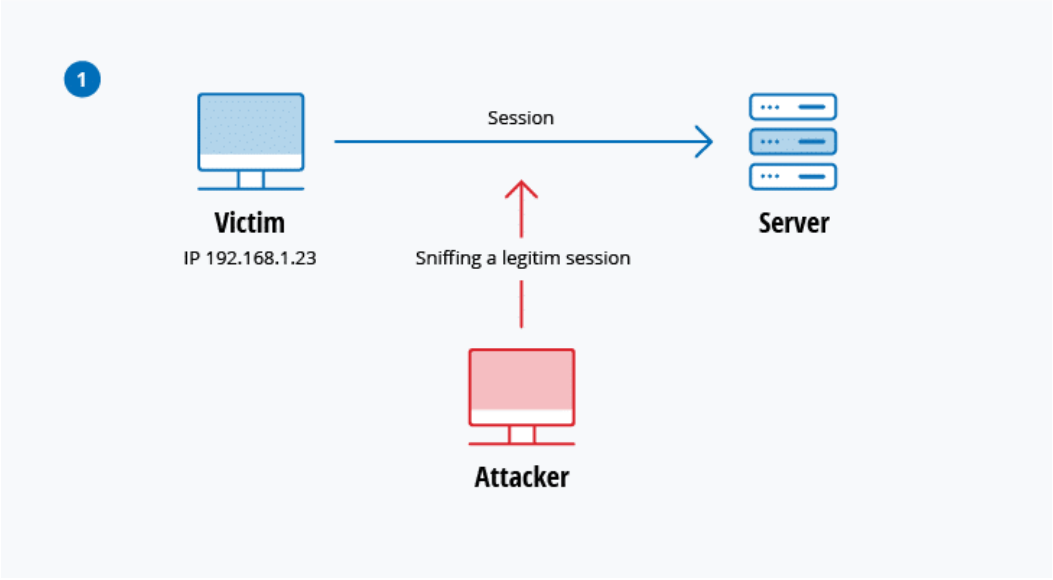
Un cyber attaquant pirate des utilisateurs via la messagerie

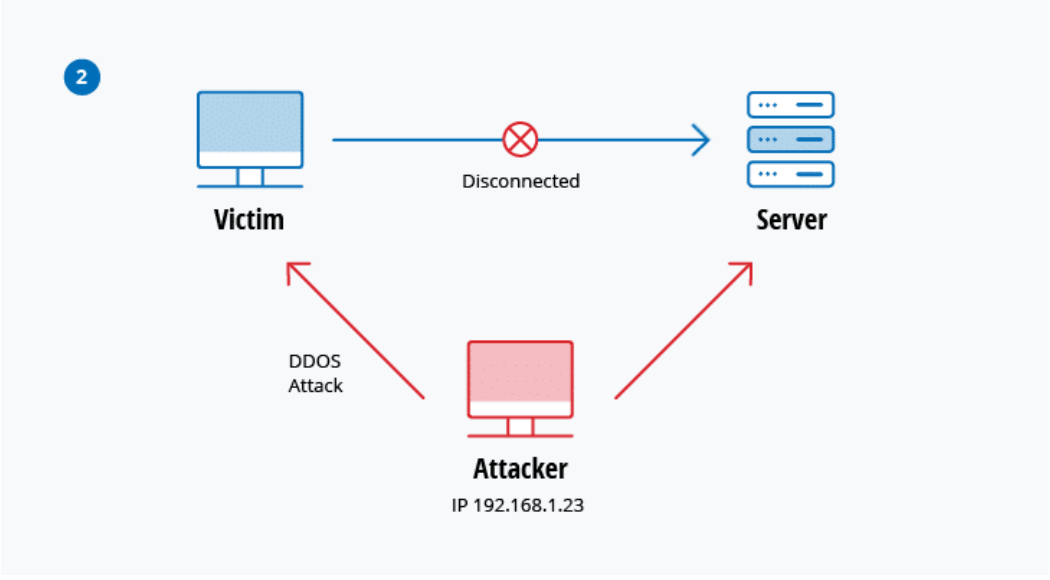


Un cyberattaquant test ses capacités en détournant une session

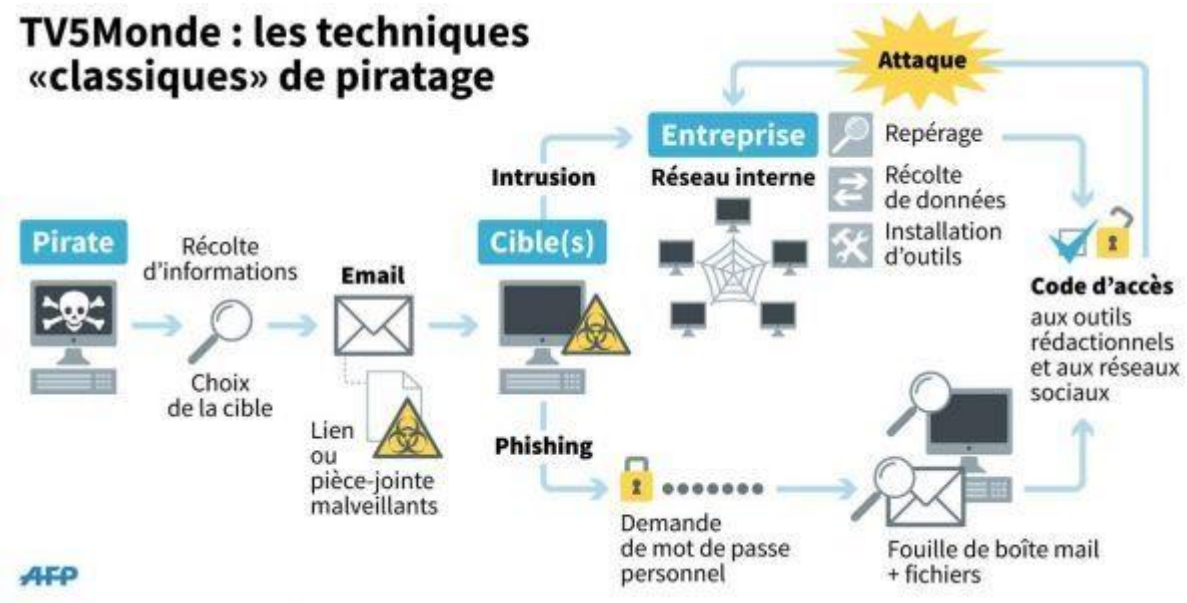
Dans ce type d'attaque MitM (Man In The Middle), un attaquant détourne une session entre un client de confiance et un serveur réseau. L'ordinateur attaquant substitue son adresse IP au client de confiance pendant que le serveur poursuit la session, croyant qu'il communique avec le client. Par exemple, l'attaque pourrait se dérouler ainsi :

- Un client se connecte à un serveur.
- L'ordinateur de l'attaquant prend le contrôle du client.
- L'ordinateur de l'attaquant déconnecte le client du serveur.
- L'ordinateur de l'attaquant remplace l'adresse IP du client par sa propre adresse IP et son propre nom de domaine et usurpe les numéros de séquence du client.
- L'ordinateur de l'attaquant poursuit le dialogue avec le serveur, le serveur croit qu'il communique toujours avec le client.





Un membre se fait voler son identité par un pirate



L'hébergeur subit un incident technique

Un incident peut rendre les serveurs d'un hébergeur inexploitables. Par exemple, un incendie peut brûler la salle des serveurs qui permet l'hébergement en ligne du site, mais aussi la sauvegarde de toutes les bases de données et le code du site. Un tel incident aurait pour conséquence la perte totale de toutes les données et de tout le code du site.

Un utilisateur poste du contenue non conforme dans l'espace commentaire

Via l'espace commentaire, des utilisateurs peuvent chercher à faire parler d'eux en mettant des liens vers leur contenu ou autre. L'espace commentaire peut alors vite ne plus rien à voir avec la recette. Dans le pire des cas, des utilisateurs peuvent poster du contenu insultant, voir effectuer du harcèlement. L'anonymat que procure le pseudonyme peut leur permettre de répéter de telles actions sans être particulièrement inquiétés.

Plan d'action

Cette partie présente les mesures qui seront mises en place, pour éviter les scénarios de la partie précédente, et donc pour s'occuper des risques suivant leur niveau de pertinence.

Un cyber attaquant pirate des utilisateurs via la messagerie

Ce scénario est vraiment pertinent. C'est pourquoi il est important de mettre en place des mesures de sécurités

- Premièrement, on peut installer une vérification à la création du compte, qui vérifierait si l'utilisateur est un humain, et ainsi bloquerait une majorité des bots.

- Deuxièmement, on peut installer un programme qui vérifierait les messages. Il faut empêcher l'envoie d'URL, et de pièce jointe. Aucun de ces 2 types de messages n'a d'importance au bon fonctionnement du site. On peut ainsi empêcher totalement leur envoie.

Un cyberattaquant test ses capacités en détournant une session

Bien que hypothétiquement pertinent, ce risque ne peut pas être géré& au niveau du site. La seule chose qui pourrait être faite, est d'afficher un message conseillant aux utilisateurs de n'utiliser que des connexions internet de confiance. En conclusion, ce scénario n'est pas très pertinent, et donc n'est pas retenu.

Un membre se fait voler son identité par un pirate

Il est difficile de vérifier que l'utilisateur soit bien le détenteur du compte et pas un pirate qui lui aurait volé son mot de passe. Cependant, un système permettant de modifier le mot de passe à partir de l'adresse électronique peut être une solution pour permettre aux utilisateurs de régulièrement changer leur mot de passe, notamment dans le cas où ils se rendent compte que leur identité a été volée.

L'hébergeur subit un incident technique

La meilleure des solutions serait de prendre un hébergeur qui a des sauvegardes de ses données dans un autre lieu géographique. Cette solution semble simple à mettre en place est peut se révéler fort utile. Il est donc important de la mettre en place

Un utilisateur poste du contenue non conforme dans l’espace commentaire

On peut mettre en place un vérificateur de mots, pour être sûr qu’aucun propos injurieux ne soit envoyé. De plus on peut mettre en place, la possibilité de signaler un commentaire, pour ajouter une autre vérification.