

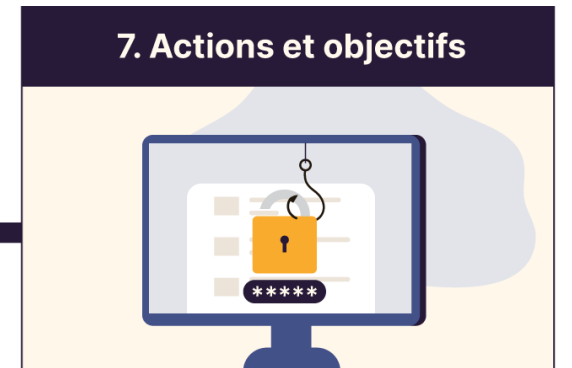
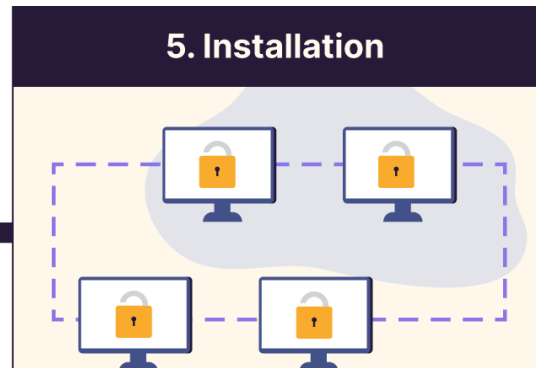
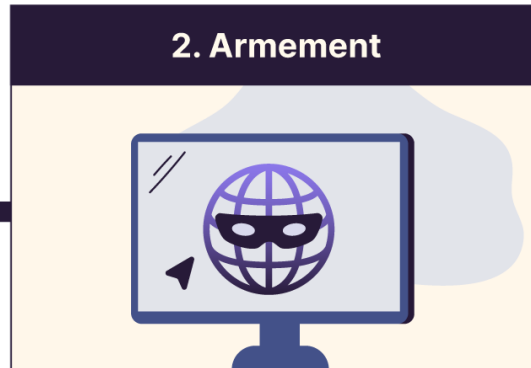
RSX112

Sécurité des réseaux

Stéphane LARCHER

A person wearing a Guy Fawkes mask and a dark hoodie is shown from the chest up. They are holding a laptop in front of them. The laptop screen displays a terminal window with green text on a black background, resembling a command prompt or a code editor. The text on the screen is partially legible and appears to be a mix of letters and numbers. The background is dark and out of focus.

Le scénario



L'attaque

The background of the slide is a dark, textured image. It features a Guy Fawkes mask, a symbol often associated with hacktivism, centered in the upper half. The mask is light-colored with dark eye sockets and a stylized mouth. Surrounding the mask and filling the background are faint, glowing patterns of binary code (0s and 1s) in a light blue or green hue, suggesting a digital or cyber theme.

Étape 1

Reconnaissance

l'attaquant recherche et identifie sa cible

L'attaque

The background of the slide features a Guy Fawkes mask, a symbol often associated with hacktivism, centered in the upper half. The entire background is overlaid with a pattern of binary code (0s and 1s) in a light green or yellow color, creating a digital or cyber-themed aesthetic.

Étape 2

Armement

l'attaquant crée ou achète son outil d'intrusion (un logiciel malveillant, ou malware) sur le dark web

Ce malware exploite une ou plusieurs vulnérabilités dans le système d'information cible

L'attaque



Étape 3

Livraison

le logiciel malveillant est transmis à la cible
(dans la pièce jointe d'un mail ou via une clé USB...)

L'attaque



Étape 4

Exploitation

le logiciel malveillant exploite la vulnérabilité identifiée au préalable

c'est-à-dire qu'il tire parti des faiblesses du système d'information cible.

L'attaque



Étape 5

Installation

l'attaquant s'introduit sur le système d'information cible et, via des “mouvements latéraux”, infecte d'autres éléments du système d'information

autres ordinateurs, autres comptes utilisateurs, etc.

Il étudie le système de l'intérieur

L'attaque



Étape 6

Commandement et contrôle

l'attaquant s'installe de façon permanente dans le système d'information cible

L'attaque



Étape 7

Actions sur l'objectif

l'attaquant réalise ses objectifs initiaux, tels que le vol de données, la destruction de données, ou le chiffrement pour demander une rançon



Les protocoles à risques

Les protocoles à risques

SMTP (Simple Mail Transfert Protocol)

Envoyer et recevoir des mails	25 465 587	Utilisez une architecture proxy ce qui vous permet de vérifier le service SMTP	Utilisez des connexions chiffrées et sécurisées avec TLS ou SSL	Configurez votre serveur de mail, pour qu'il ne relaie que vos mails, et ce afin que les spammeurs n'utilisent pas votre serveur pour envoyer des mails (problème assez courant)
-------------------------------	------------------	--	---	--

Les protocoles à risques

SMTP (Simple Mail Transfert Protocol)

Protégez-vous
contre les attaques
DoS (dédi de
service)
fail2ban

Configurez
l'authentification,
afin qu'un
utilisateur sans login
et mot de passe ne
puisse utiliser le
serveur SMTP.

Mettez à jour vos
listes noires grâce
aux DNSBL
(Domain Name
System Blacklists)

Utilisez un antispam
SpamAssassin

Les protocoles à risques

HTTP (HyperText Transfert Protocol)

- Utiliser une architecture proxy, avec firewall type DPI.

Accès à distance

- N'autorisez que SSH et indiquez les adresses IP sources ayant le droit de se connecter.

Le transfert de fichier

- Utilisez FTPS qui est une combinaison de FTP et de SSL ou TLS
- Utilisez une architecture proxy (filtre DPI)
- Si seulement certaines personnes ou serveurs ont accès au serveur FTP, configurez les adresses sources dans vos règles firewall. Ainsi, aucune personne non autorisée n'y aura accès



Les attaques

Les attaques les plus courantes

Phishing

Malware

Attaques par déni
de service (DDoS)

Ingénierie sociale

Attaques de force
brute

Exploitation des
vulnérabilités
logicielles

Attaques
d'hameçonnage
par téléphonie
(vishing)

DDoS

Distributed Denial of Service

Le principe

- Saturation de requêtes un site pour le figer

Pourquoi ?

- Volonté politique
- Volonté économique avec échange d'une rançon pour récupérer le service
- visant à submerger les ressources du système cible, le rendant inutilisable

DDoS

Recrutement de botnets

- Les attaquants prennent le contrôle d'un grand nombre d'ordinateurs infectés
- Les zombies

Coordination du botnet

- Ils envoient des commandes aux ordinateurs zombies pour qu'ils génèrent et envoient du trafic vers la cible.

Inondation de trafic

- Les ordinateurs zombies inondent la cible avec un trafic excessif
- Requêtes DNS, UDP ...

DDoS

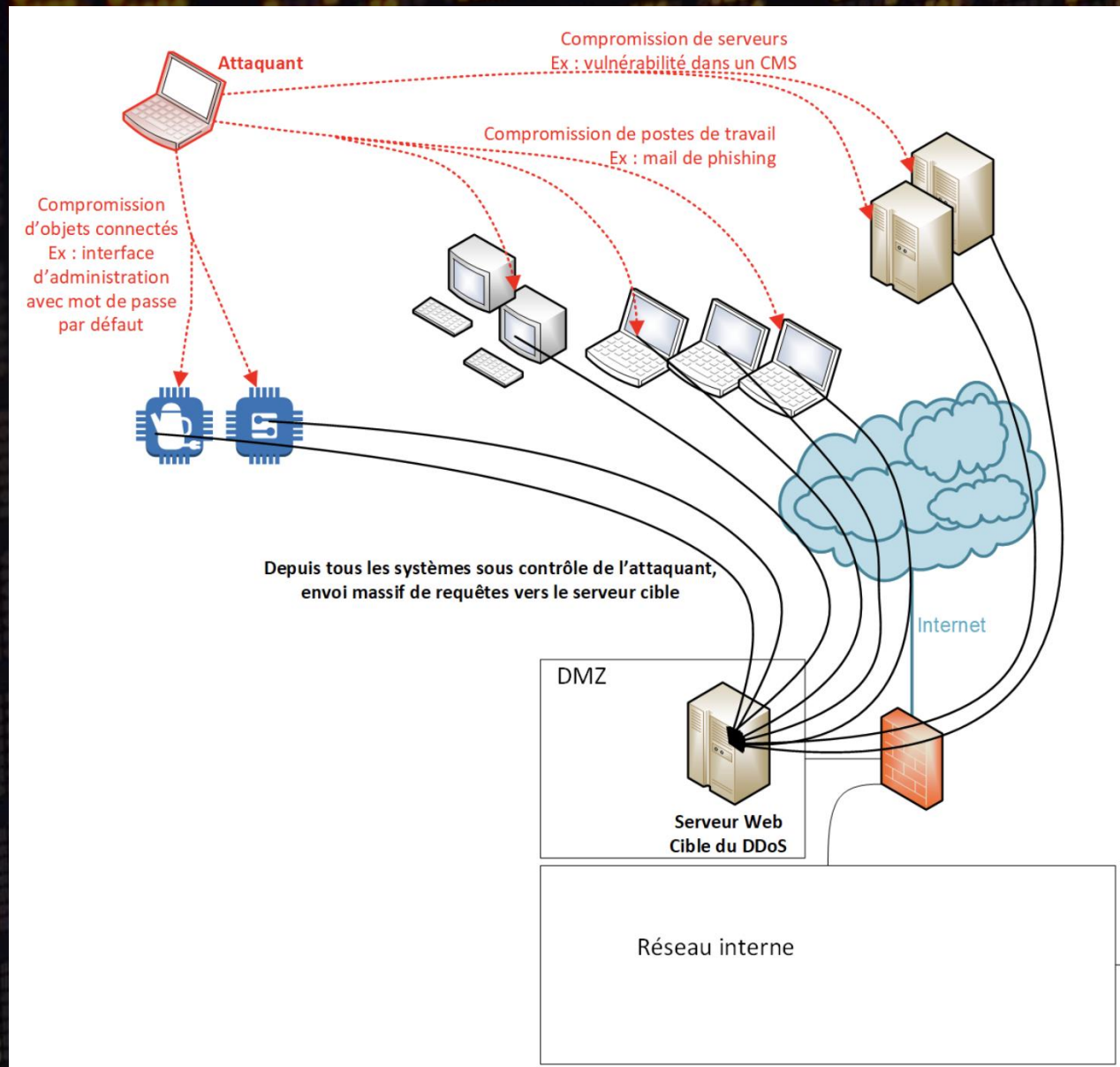
Surcharge du système cible

- congestion ou un épuisement des ressources, rendant le service ou le site web indisponible pour les utilisateurs légitimes.

Impact sur la disponibilité

- L'objectif principal d'une attaque DDoS est de perturber ou de paralyser les services de la cible

DDoS



Injection SQL

Fonctionne sur un modèle d'application comportant une base de données

Connexion sur l'interface web avec l'aide d'une requête SQL, dans le champ mot de passe

La requête SQL sera interprétée

L'automatisation de cette attaque est possible

Injection SQL

Vulnérabilité de l'application

- L'attaque par injection SQL est possible lorsque l'application web ne valide pas correctement les entrées fournies par l'utilisateur ou ne gère pas correctement les caractères spéciaux dans les requêtes SQL.

Injection de code malveillant

- L'attaquant utilise les failles de l'application pour injecter des fragments de code SQL malveillants dans les champs de saisie ou les paramètres de requête de l'application web.

Injection SQL

Exécution de commandes SQL non autorisées

- Lorsque les instructions SQL malveillantes sont injectées avec succès, elles peuvent être interprétées et exécutées par le serveur de base de données.

Conséquences de l'attaque

- la divulgation d'informations sensibles, la modification
- la suppression de données, l'usurpation d'identité, voire la compromission complète du système.

XSS : Cross-Site Scripting

Polluer un site avec des bouts de codes malicieux

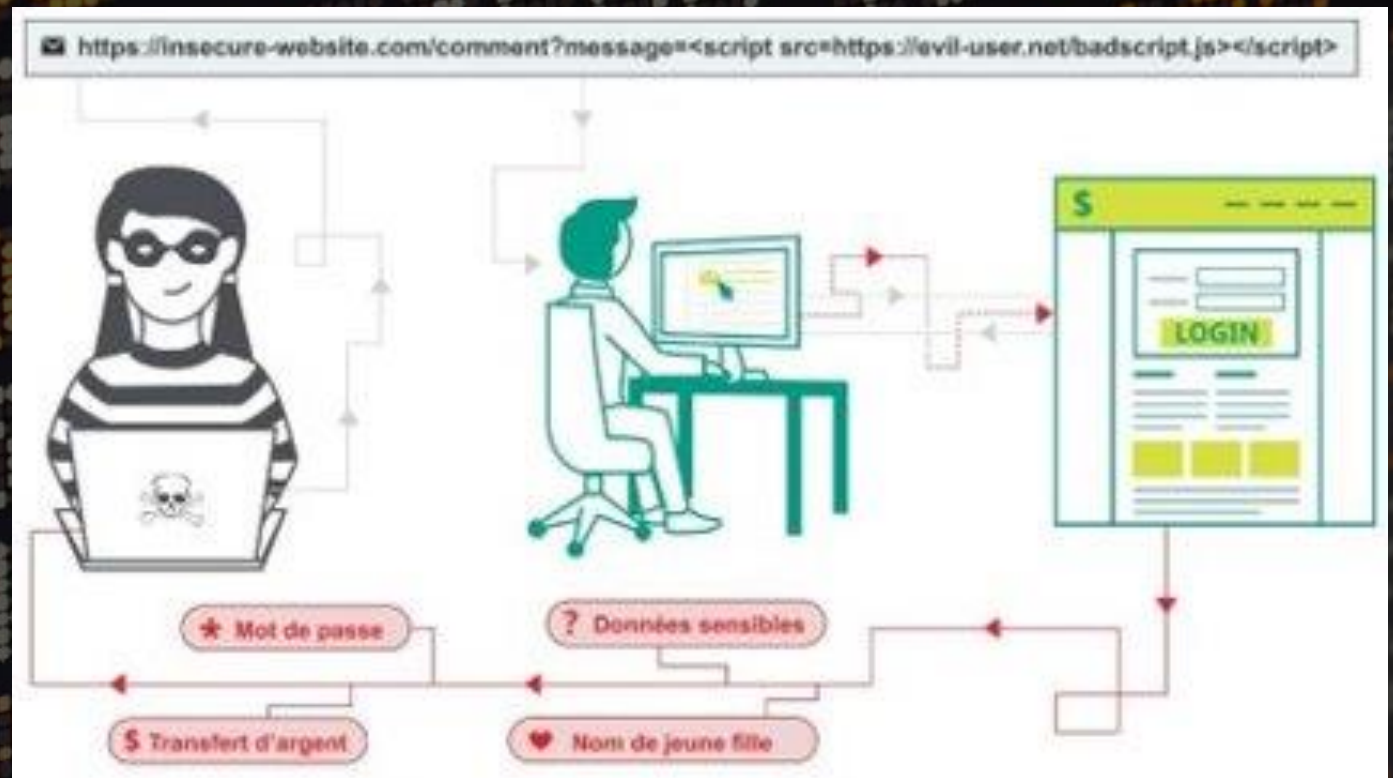
- Forum
- Commentaire

Langage le plus souvent utilisé JavaScript

Rediriger l'utilisateur vers une autre page

- phishing

XSS : Cross-Site Scripting



Le défacement

Modifie le contenu d'un site Web



Message

Politique

Religieux

Contestataire

Le défacement

Rechercher le compte et mot de passe d'accès à une interface d'administration ou à un service d'échange de fichiers

Exploiter une vulnérabilité dans le serveur Web, le serveur d'application, le CMS utilisé ou l'application elle-même

Compromettre un hébergeur pour défacier les sites de l'ensemble de ses clients

Sidejacking

La démarche :

- Connexion à un site avec identifiant et mot de passe
- Vérification du site et dépose d'un cookie sur le poste client
- Ce cookie peut être récupérer car non chiffré la plus part du temps
- L'authentification n'est plus nécessaire alors

Peut-être possible sur des connexion Wifi non sécurisée :

- Hôtel
- Gare ou aéroport
- Wifi public

Sidejacking

Utilisation des cookies volés

- usurper l'identité de l'utilisateur légitime. En utilisant ces cookies volés, l'attaquant peut se connecter au site web ciblé sans avoir besoin de connaître les identifiants de connexion de l'utilisateur

Les Conséquences

- accéder à ses informations personnelles
- effectuer des transactions financières
- modifier les données

Sidejacking

Réseau sans fil non sécurisé

Sniffing des paquets réseau

- L'attaquant utilise des outils de sniffing de paquets réseau, tels que Wireshark

Intercepter les cookies de session

- L'attaquant peut capturer ces cookies de session à l'aide d'outils de sniffing réseau

Buffer Overflow

Débordement de tampon

Écraser les informations nécessaires au fonctionnement d'un programme

Tout le code pirate sera exécuté comme émanant d'une source sûre

Technique assez difficile à mettre en place

Existence d'outil "clé-en-main"

Buffer Overflow

Allocation de mémoire

Entrée de données

Débordement du tampon

Modification de l'exécution

Exécution du code malveillant



Le phishing

Se faire passer pour quelqu'un de confiance via un e-mail

Proposer un lien pour récupérer éventuellement login et mot de passe sur une fausse page institutionnelle

Cryptojacking

Utilisation des ressources de votre PC

Utilisation du portefeuille virtuel de votre PC pour la création de la cryptomonnaie

Cryptojacking

Injection de code malveillant

- injection de scripts JavaScript malveillants dans des sites web, des publicités ou des extensions de navigateur compromis.

Exploitation de la puissance de calcul

- exécute des opérations de minage de cryptomonnaies en utilisant la puissance de calcul de l'ordinateur de l'utilisateur.
- pour effectuer les calculs nécessaires à la génération des cryptomonnaies

Discrétion de l'attaque

- Le Cryptojacking vise à rester furtif et à passer inaperçu

Cryptojacking

Extraction des cryptomonnaies

- Les calculs effectués par le code malveillant génèrent des blocs de cryptomonnaies qui sont ensuite ajoutés à la blockchain correspondante
- Les récompenses générées, sous forme de cryptomonnaies, sont envoyées aux attaquants

Impact sur la victime

- Utilisation excessive des ressources de l'ordinateur

The background of the slide is a dark, blurred image of a digital display, likely a stock market ticker or a data feed. It features numerous yellow and orange digits and symbols, such as plus and minus signs, arranged in a grid-like pattern. The text "Sniffing" is positioned in the upper left corner of this background.

Sniffing

Lire ou enregistrer des
paquets transitant par un
réseau

Sniffing

Capture des paquets

- L'attaquant utilise des outils de sniffing, tels que Wireshark, tcpdump ou d'autres logiciels similaires, pour capturer les paquets de données qui transitent sur le réseau

Analyse des paquets

- Une fois les paquets capturés, l'attaquant peut les analyser pour extraire des informations sensibles

Sniffing

Exploitation des vulnérabilités

- L'analyse des paquets peut révéler des vulnérabilités ou des faiblesses dans les protocoles ou les applications utilisés sur le réseau.
- Exploiter ces vulnérabilités pour effectuer des attaques supplémentaires, telles que l'injection de code malveillant ou l'usurpation d'identité

Risques pour la confidentialité et la sécurité

- confidentialité et la sécurité des données qui transitent sur le réseau
- Usurpation d'identité
- Le vol d'informations confidentielles



Les contrer

Les contrer

Utiliser des requêtes préparées ou des paramètres liés pour les requêtes SQL.

Valider et filtrer rigoureusement les entrées utilisateur.

Échapper correctement les caractères spéciaux dans les requêtes SQL

Les contrer

Limitier les privilèges de l'utilisateur de la base de données pour minimiser les risques.

Maintenir les applications et les systèmes à jour avec les correctifs de sécurité

Les contrer

Utiliser des réseaux Wi-Fi sécurisés et chiffrés, tels que des réseaux WPA2 ou WPA3 avec des mots de passe forts

Éviter de se connecter à des sites web sensibles ou d'effectuer des transactions financières sur des réseaux Wi-Fi publics non sécurisés

Utiliser des connexions HTTPS sécurisées (reconnaissables par le préfixe "<https://>" dans l'URL) chaque fois que possible, car elles chiffreront le trafic entre l'utilisateur et le site web

Utiliser des VPN (Virtual Private Network) pour établir une connexion sécurisée et chiffrée entre l'utilisateur et le réseau auquel il se connecte

Les contrer – Services de la sécurité

Contrôle d'accès au système

- protection physique du matériel
- correctifs éditeurs
- communications filtrées
- Antivirus
- IDS (Intrusion Detection System)

Gestion des habilitations

- ACL pour les systèmes de fichiers
- gestions des identités

Les contrer – Intégrité

Hachage

- algorithme générant un texte de longueur fixe

MD5 (Message Digest 5)

- empreinte de 128 bits
- 32 caractères décimaux
- Méthode AND, OR, XOR ou encore NOT

SHA (SH1)

- Empreinte de 160 bits
- Utilisation de 5 variables

Les contrer – Services de la sécurité

Non-répudiation

- Signature électronique
- Calcul d'intégrité par hachage

Authentification

- Certificat électronique
- Confiance d'un tier
- Doit être reconnu par tous les systèmes
- CA – Certificat Authority

Les contrer – Services de la sécurité

Confidentialité

- Clés symétriques
 - Même clé pour le chiffrement et déchiffrement
- Clés asymétriques
 - Clés publiques
 - Clés privées
 - SSL, HTTPS
 - TLS (Transport Layer Security)