Deep dive dans le métier de pentester

Pablo Bondia-Luttiau (GLiCID)
pablo.bondia-luttiau@ec-nantes.fr

CV

- Cursus Ingénieur Cybersécurité (ESIEA)
  - Reverse engineering
  - Forensic
  - Sécurité physique
  - OSINT
  - ....
- Actuellement CSSI + Admin Système pour GLiCID
- 3 Pentests et 2 audits sur 5 mois

Introduction

La Sécurité, c'est l'affaire de tout le monde.

Une seule défaillance dans toute une chaîne peut provoquer des réactions catastrophiques sur toute une infrastructure.

La première cause d'incidents de sécurité est humaine (volontaire ou involontaire, des utilisateurs ou des administrateurs)

Bases

✅ **Douter de tout**
✅ **Douter tout le temps**
✅ **Douter avec tout le monde**

❌ Je le ferai plus tard
❌ C'est pas si grave
❌ Mais il me l'avait demandé

Mon métier c'est d'être parano

Déroulement d'un pentest réel

- OSINT
- Cartographie des lieux
- Campagne massive de phishing
- Récupération de documents d'architecture
- Pivot, extraction de l'AD et cassage de mots de passe
- Audace
- Bingo

Notre but

1. Entrer physiquement dans les bâtiments
2. Placer des implants réseau
3. Récupérer un maximum de mots de passe d'utilisateurs pour faire chanter le patron

OSINT

Mots-clés

- Deep/Dark Web
- Identité numérique
- Fuite de données
- Social engineering
- Scans de réseaux

OSINT

Généralités

Récupérer un maximum d'informations sur les composants du SI, et sur les personnes de l'entreprise.

Durant cette phase, nous partons simplement du nom de l'entreprise.

OSINT

Elements en entrée

Le nom de l'entreprise

OSINT

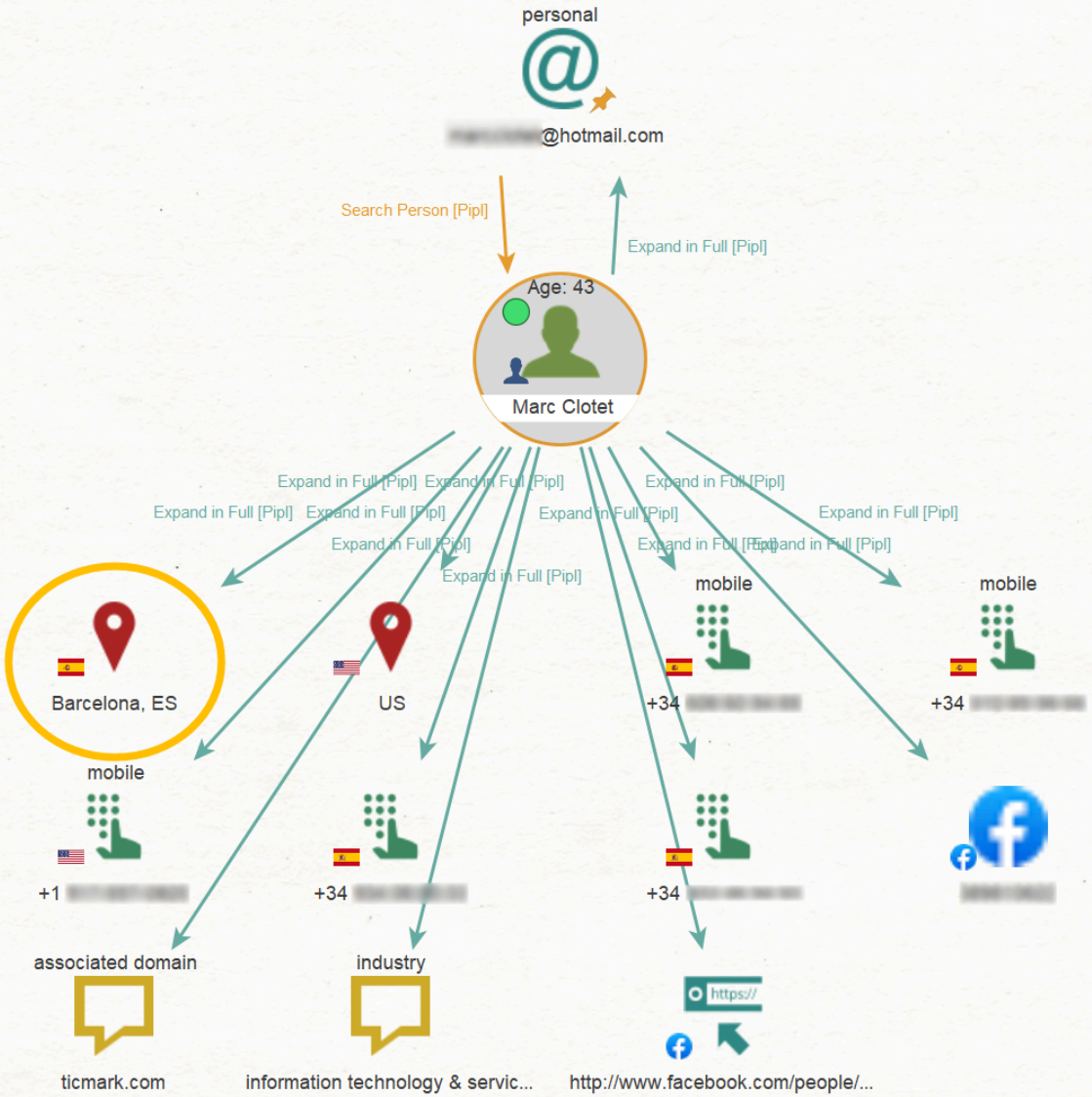
Elements en sortie

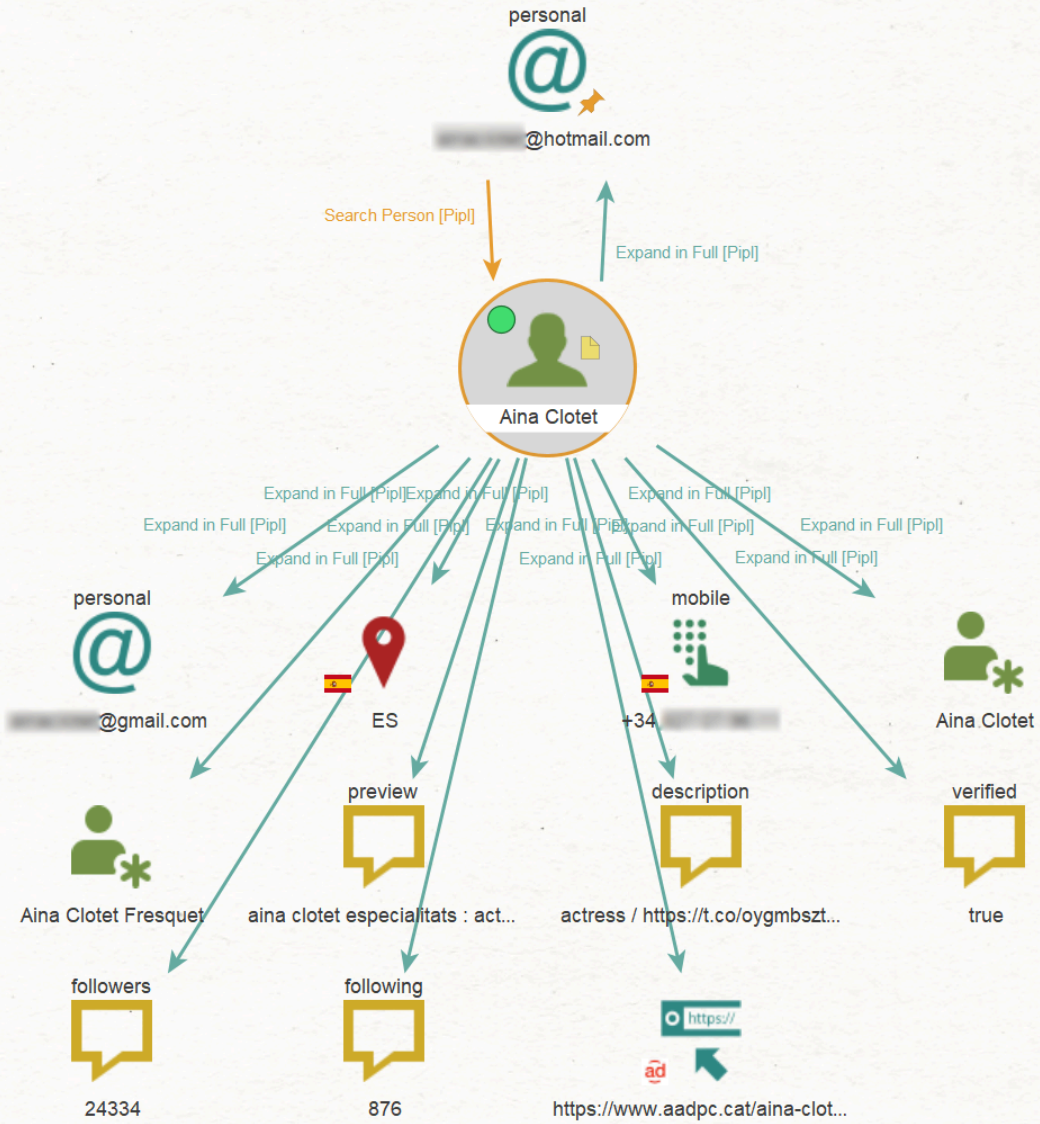
- Qui sont les différents dirigeants ou personnes importantes, le nom de leur femme, de leurs enfants, famille proche ou éloignée, adresses et numéros de téléphone personnels
- Qui sont les potentiels administrateurs, qui sont les utilisateurs les moins à l'aise avec la technologie, quelles traces ont-ils laissé
- Quelle est la politique de l'entreprise, ses relations client, sa domiciliation, à quoi ressemble l'entreprise de l'extérieur, etc.

OSINT

Elements en sortie

- Domaines internet possédés par l'entreprise, serveurs DNS, serveurs de mail, format des adresses mail, adresses mail de collaborateurs, sites web accessibles, tutelles potentielles


personal
@hotmail.com
Search Person [Pipl]
Expand in Full [Pipl]
Age: 43
Marc Clotet
Barcelona, ES
US
mobile
+34
mobile
+34
mobile
+1
+34
+34
associated domain
ticmark.com
industry
information technology & servic...
https://
http://www.facebook.com/people/...


personal
@hotmail.com
Search Person [Pipl]
Expand in Full [Pipl]
Aina Clotet
personal
@gmail.com
ES
mobile
+34
Aina Clotet
Aina Clotet Fresquet
preview
aina clotet especialitats : act...
description
actress / https://t.co/oygmbszt...
verified
true
followers
24334
following
876
https://
https://www.aadpc.cat/aina-clot...

Cartographie des lieux

Mots-clés

- Sécurité physique
- Vidéosurveillance
- Fuite de réseaux sans fil

Cartographie des lieux

Généralités

Après avoir fait notre petite enquête sur l'entreprise sur internet, nous avons sauté dans une voiture pour se rendre sur place.

Après quelques heures de planque...

Cartographie des lieux

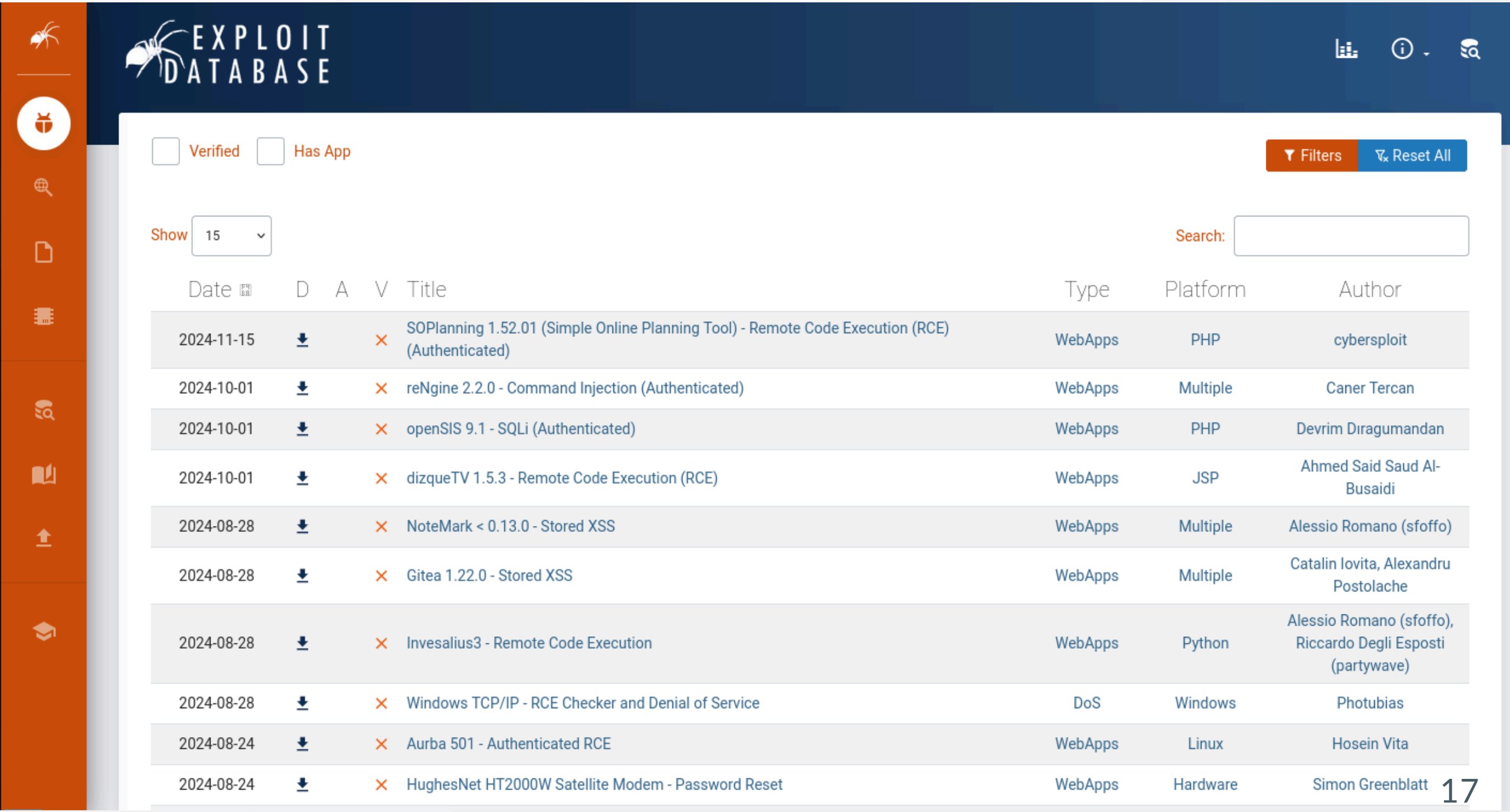
Elements en entrée

OSINT et l'adresse de l'entreprise

Cartographie des lieux

Elements en sortie

- Une cartographie complète de la couverture Wi-Fi de l'entreprise, en situant avec précision les différents réseaux Wi-Fi présents, et leur position géographique via une triangulation
- De nombreux portraits robots de personnes entrants et sortants de l'entreprise, les différents habits utilisés par les prestataires et utilisateurs... Pas de badge visiteur, et une tenue reconnaîssable ...
- Un prestataire de service informatique bien connu est sur les lieux


EXPLOIT DATABASE
Verified
Has App
Filters
Reset All
Show 15
Search:
Date D A V Title Type Platform Author
2024-11-15 SOPlanning 1.52.01 (Simple Online Planning Tool) - Remote Code Execution (RCE) (Authenticated) WebApps PHP cybersploit
2024-10-01 reNgine 2.2.0 - Command Injection (Authenticated) WebApps Multiple Caner Tercan
2024-10-01 openSIS 9.1 - SQLi (Authenticated) WebApps PHP Devrim Diragumandan
2024-10-01 dizqueTV 1.5.3 - Remote Code Execution (RCE) WebApps JSP Ahmed Said Saud Al-Busaidi
2024-08-28 NoteMark < 0.13.0 - Stored XSS WebApps Multiple Alessio Romano (sfoffo)
2024-08-28 Gitea 1.22.0 - Stored XSS WebApps Multiple Catalin Iovita, Alexandru Postolache
2024-08-28 Invesalius3 - Remote Code Execution WebApps Python Alessio Romano (sfoffo), Riccardo Degli Esposti (partywave)
2024-08-28 Windows TCP/IP - RCE Checker and Denial of Service DoS Windows Photubias
2024-08-24 Aurba 501 - Authenticated RCE WebApps Linux Hosein Vita
2024-08-24 HughesNet HT2000W Satellite Modem - Password Reset WebApps Hardware Simon Greenblatt

Campagne massive de phishing

Mots-clés

- Phishing mail
- Spear phishing
- Faux sites web
- Typosquatting
- Macros de documents / Trojan / Keyloggers

Campagne massive de phishing

Généralités

Grâce aux informations collectées lors de l'OSINT, nous savions que l'entreprise à l'habitude de poster ses résultats d'expérience, ses nouveaux contrats avec des fournisseurs, et les évènements en cours sur Linkedin.

Tiens donc, un séminaire à XXX dans 3 jours... Merci Linkedin ;)

Après 10 minutes d'effort de rédaction d'un mail crédible proposant du covoiturage pour le séminaire...

Campagne massive de phishing

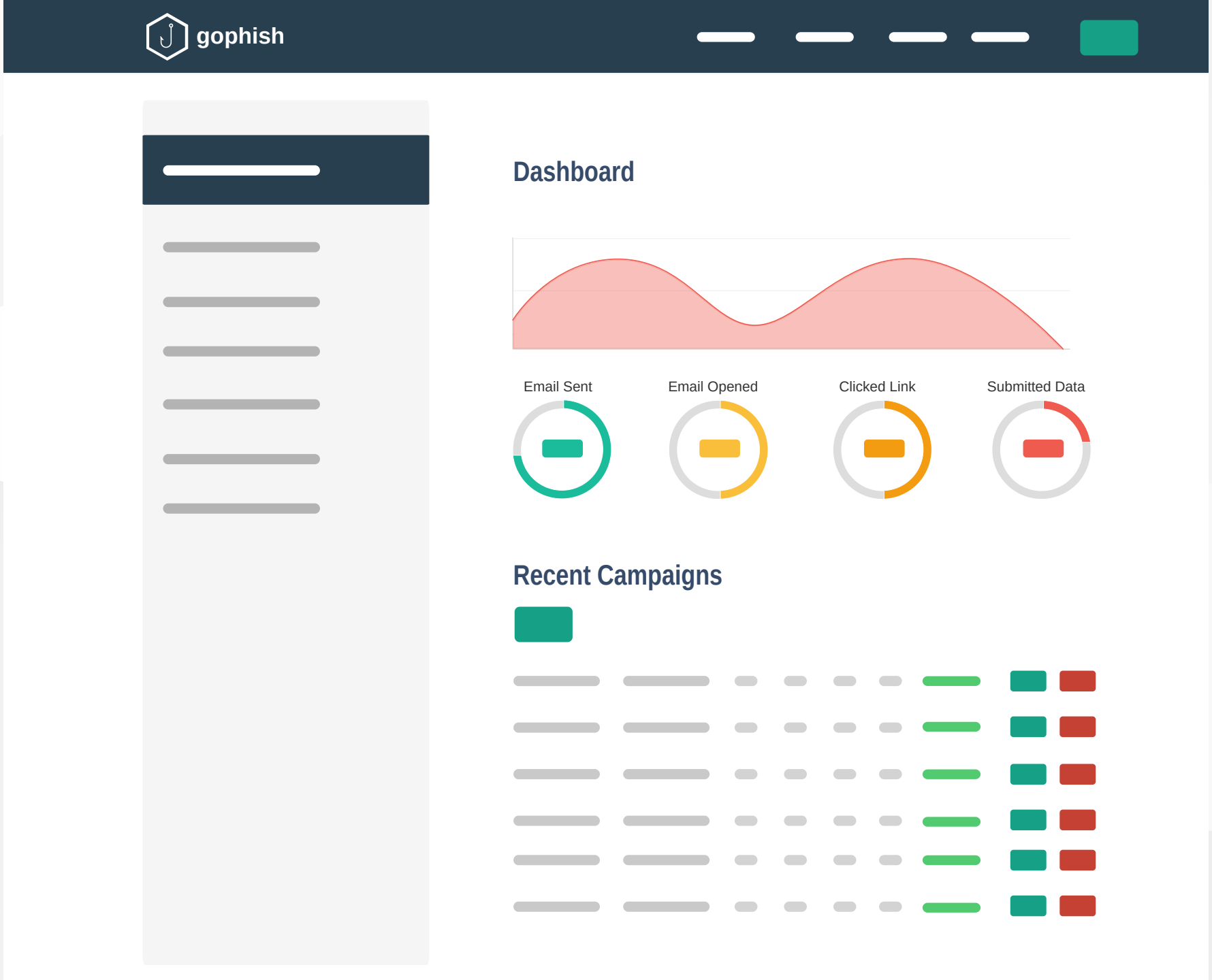
Elements en entrée

- Adresses mail de tous les collaborateurs de l'entreprise
- Mail crédible de covoiturage pour le séminaire avec un lien truqué

Campagne massive de phishing

Eléments en sortie

- 80% de l'entreprise à rempli ses identifiants sur la page de phishing
- Environ X mots de passe en clair récupérés


gophish
Dashboard
Email Sent
Email Opened
Clicked Link
Submitted Data
Recent Campaigns

Tips : On a mis 2 pages consécutives avec un faux "mot de passe erroné" pour forcer les utilisateurs à bien taper leur vrai mot de passe... Vicieux

Récupération de documents d'architecture

Mots-clés

- Broken Access Control
- **Chiffrement** des postes et supports
- Data leaks
- Vol de postes
- Clés USB
- Double authentification

Récupération de documents d'architecture

Généralités

Super, on a récupéré le mot de passe d'un vieil utilisateur que nous avions repéré en OSINT, il faisait partie de la DSI il y a quelques années...

On en a profité pour fouiller dans les dossiers de son service de partage de fichier grâce à son mot de passe.

Récupération de documents d'architecture

Elements en entrée

Accès à un partage de fichiers

Récupération de documents d'architecture

Eléments en sortie

- Un document s'appellant "passwords.keepass2" contenant des fleurs et des paillettes

Pivot, extraction et cassage

Mots-clés

- Etanchéité réseau
- Vulnérabilités et exploits (injections, etc.)
- Complexité et renouvellement des mots de passe
- Double authentification (Passwords managers !)

Pivot, extraction et cassage

Généralités

Bon, vu le fichier, il semblerait que notre ex-informaticien ait décidé d'utiliser un mot de passe présent dans une brèche d'il y a quelques temps, qu'il n'a jamais changé en 8 ans.

Avec ça, accès à tous les mots de passe de la DSI !

Pivot, extraction et cassage

Elements en entrée

Accès au mot de passe de l'Active Directory

Pivot, extraction et cassage

Eléments en sortie

- Dump complet de l'Active Directory avec les mots de passe hachés
- Cassage offline des mots de passe de l'Active Directory
- Récupération du mot de passe maître du directeur de l'entreprise


esiea
ASUS

Audace

Super, avec le mot de passe du directeur, on va envoyer un message à l'accueil qui filtre les entrées. On a qu'a dire que des personnes de chez <insérez nom du prestataire> vont devoir accéder à la salle serveur demain dans la journée.

Le lendemain, déguisé en faux technicien avec fausse carte de visite, je me présente à l'accueil. On me donne généreusement les clés de la salle serveur, et on me laisse installer mon implant dans le réseau administrateur général.

Mon collègue, dans la voiture, voit en temps réel l'implant se connecter, et lui donner un accès au réseau d'administrateurs de l'entreprise.

Bingo

On a réussi.

Maintenant, il va falloir passer l'étape douloureuse d'expliquer comment nous sommes rentrés à toute l'équipe DSI...

Merci pour votre attention

Questions !