

BOTNET C&C

3JSI

DA COSTA ALEXY | JULIEN DELAUNAY | NICOLAS TORRES-SANNIER

SOMMAIRE

1. Introduction
2. Partie Alexy
 - Fonctions
 - Réseau
 - Expérience
 - Evolution
3. Partie Julien
 - Gestion de projet
 - Infrastructure réseau
 - Retour d'expérience
4. Partie Nicolas
 - Gestion de projet
 - Développement du C&C
 - Expérience
 - Évolution
5. Conclusion

INTRODUCTION

Un Botnet axé sur la simplicité
d'utilisation mais également
sur le design épurée du
tableau de bord.

—BOTNET C&C



ALEXY

Developpement C Windows
Infrastructure réseaux
Gestion de projet
Javascript

01

FONCTIONS



Envoie de paquets répétitif
depuis plusieurs sources vers
une seule destination

DDOS TCP/UDP



Démarrage automatique
du malware à l'ouverture
d'une session

PERSISTANCE



Récupère tous les fichiers
dans un répertoire

ENUMERATION FICHIER



Suppression du dossier
des prefetch

SUPPRESSION PREFETCH



Récupération d'un fichier
via socket

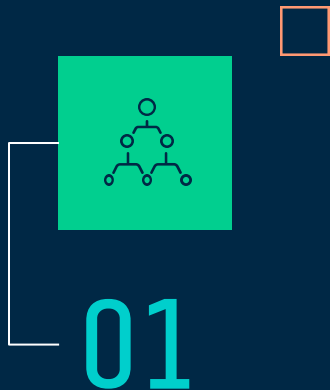
ENVOIE FICHIER



Récupération des
caractéristiques hardware

ENUMERATION HARDWARE

RESEAU



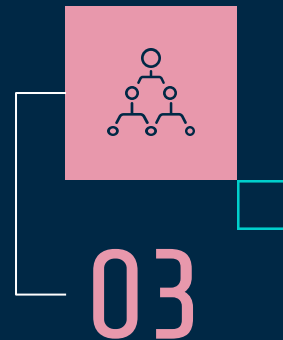
SERVEUR

Configuration des services
Mise en places des machines



ROUTAGE

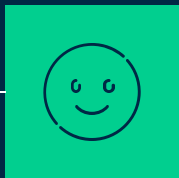
Routage des réseaux
Simulation d'internet



SECURITE

Hardening C&C
Règles du PFSense

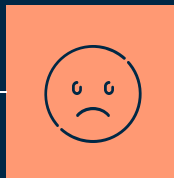
RETOUR D'EXPERIENCE



01

SUCCES

Partie fonctionnel
Fonction dynamique
Respect du cahier des charges
Epanouissement et apprentissage



02

ECHECS

Bug
Communication



03

CHANGEMENT

Coordination
Norme de code

EVOLUTION

ADS

Processus invisible

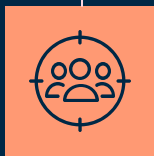


STATISTIQUES

Vue informatives sur
les zombies

PRIVILEGE

Fonction d'élévation
privilège



MISE A JOUR

Mise a jours des
zombies



Julien

Développement C
Infrastructure réseau
Gestion de projet

02



GESTION DE PROJET



Jira

- Confluence
- Jira Software



Trello



Github



APERCU JIRA

Feuille de route

Search bar with magnifying glass icon. User avatars: JD, DA, O, and two generic user icons. Filter: Catégorie d'état. Epic.

	'22	
Sprints		
> BOTNET-40 Méthodologie/Préparation		
BOTNET-56 Remise à niveau des connais...		
> BOTNET-42 Création de l'infrastructure ...		
BOTNET-44 Création du C&C		
BOTNET-43 Création du Malware		
BOTNET-54 Enrichissement de notre Ma...		
BOTNET-55 Préparation du rendu		
+ Créer Epic		

Projets / Botnet

Backlog

Search bar with magnifying glass icon. User avatars: JD and one generic user icon. Filter: Epic.

Backlog (5 tickets) Créer un sprint

BOTNET-30 Accéder à l'interface web	TERMINÉ(E)	
BOTNET-21 Mettre en place le C&C	À TESTER/CONFIRMER	JD
BOTNET-32 Attaques Alexy	À TESTER/CONFIRMER	
BOTNET-25 Mettre le Malware à jour sur les Zombies	EN COURS	
BOTNET-31 Fonction altération données	TERMINÉ(E)	

+ Créer un ticket



APERCU TRELLO

Botnet ☆ Privé Tableau

À faire
+ Ajouter une carte

En cours
+ Ajouter une carte

En test
+ Ajouter une carte

Finir

Créer la fonction de persistance en C
🕒 27 nov. 2022 DA

Attaques Julien
👁 18 déc. 2022 3/3 JD

Finir le C&C
🕒 31 déc. 2022 7/7

Préparer l'oral
👁 1 janv. 4/4 DA JD

Sécuriser serveur php
🕒 1 janv.

Attaques Alexy
🕒 18 déc. 2022 4/4 DA

Fusionner github
👁 17 déc. 2022 DA JD

+ Ajouter une carte



APERCU GITHUB

curity

Insights

main

3 branches

0 tags

Go to file

Add file

Code

About

No description, website,

Readme

0 stars

1 watching

0 forks

Releases

No releases published

[Create a new release](#)

Packages

No packages published

[Publish your first package](#)

Contributors 3

0xOxyDe 0xOxyDe

Skrliix

Nicolas-Torres-Sann

0xOxyDe Merge pull request #12 from Nicolas-Torres-Sannier/devAlexy

8f0791d 2 hours ago 67 commits

.vscode	Modifs	yesterday
Resources	Fonctions attaques	last month
README.md	ReadMe.MD	2 weeks ago
archive.c	Update archive.c	2 weeks ago
disable_defender.reg	Modifs	yesterday
installer.c	Malware ESGI V1.0.2	2 hours ago
installer.exe	modifs	3 hours ago
malware.c	Malware ESGI #1 - Socket files 1054 #V1.0.4	2 hours ago
malware.exe	modifs	3 hours ago
server.c	modifs	3 hours ago

README.md

INFRASTRUCTURE RESEAU



Serveur C&C



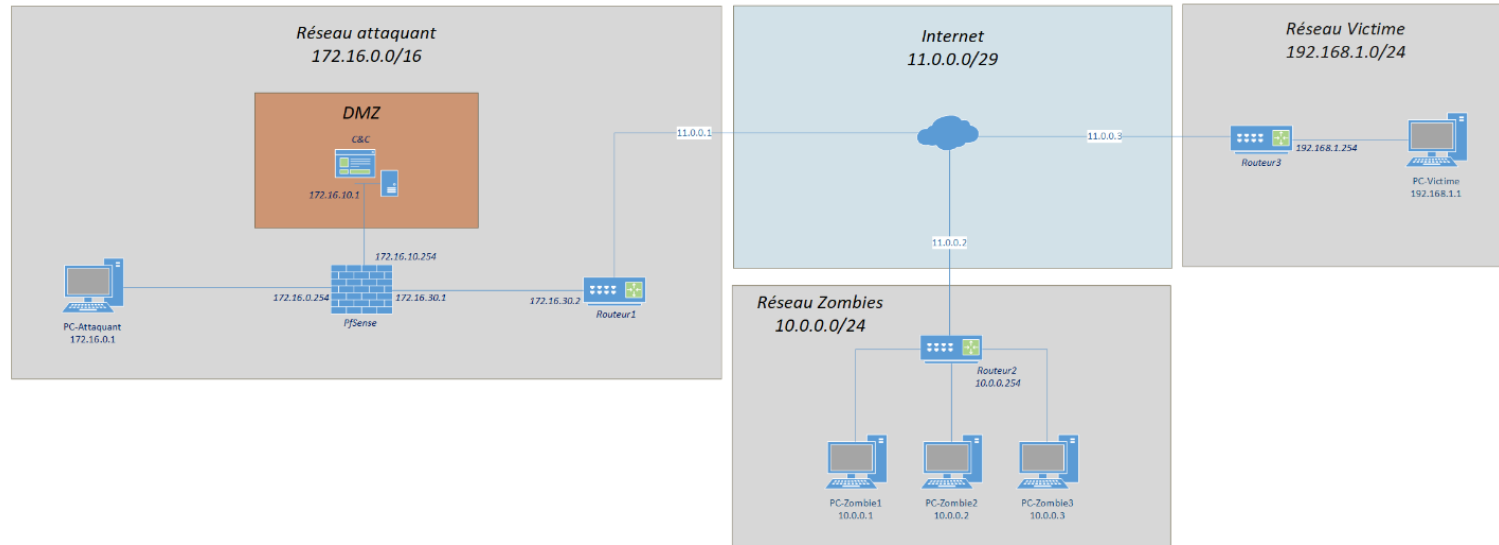
PfSense



Windows

PROJET BOTNET

Schéma technique



FONCTIONS DU MALWARE



BOMB FORK



EXECUTION FICHIER



SHUTDOWN



RESTART



LOCK



ALTERATION FICHIERS



LOGOFF



MODIFICATION
REGISTRE

RETOUR D'EXPERIENCE



01

SUCCES

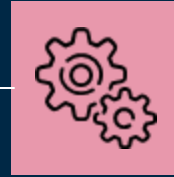
Nombreuses fonctions OK
Respect du cahier des charges
Apprentissage du C
Utilisation de nouveaux outils



02

ECHecs

Les bugs
Non respect des deadlines
Quelques fonctions non fonctionnelles
Manque de communication



03

CHANGEMENTS

Amélioration du code
Développer d'autres fonctions
Rendre les fonctions dynamique

Nicolas

1. Gestion de projet
 - Idées, outils, cahier des charges, infra...
2. Développement du C&C
 - MCD/MLD/Script SQL
 - MVC, routage
 - Modules
 - Processus de communication du Malware

03

Gestion de projet



Méthodologie

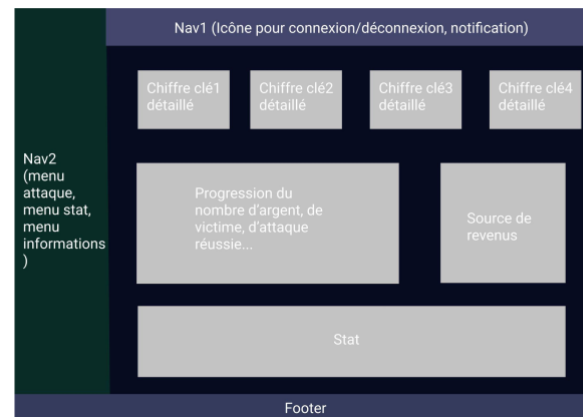
- Scrum (cahier des charges sur Jira, roadmap, Kanban)

Outils

- Jira
- Trello
- GitHub

Users stories

Fonction	Connexion
En tant que	Attaquant
Je veux	Me connecter au C&C
Afin de	Naviguer sur le C&C
Contraintes	Site responsive, UX Design user friendly
Niveau de priorité	1



Gestion de projet – Appercu GitHub



Nicolas-Torres-Sannier / Botnet-C2 Private

<> Code Issues Pull requests Actions Projects Security Insights Settings

main 2 branches 0 tags

Go to file Add file <> Code

Nicolas Torres-Sannier Merge branch 'main' of https://github.com/Nicolas-Torre... 35f505d yesterday 10 commits

config	Add files via upload	yesterday
css	first commit	4 days ago
fonts	first commit	4 days ago
images	module donnee + connexion avance	yesterday
include	module donnee + connexion avance	yesterday
js	accueil fini	3 days ago
modules	css	yesterday
node_modules	first commit	4 days ago
scss	first commit	4 days ago
vendors	first commit	4 days ago
.htaccess	first commit	4 days ago
README.md	first commit	4 days ago

About

No description, website, or topics provided.

Readme

0 stars

1 watching

0 forks

Releases

No releases published
[Create a new release](#)

Packages

No packages published
[Publish your first package](#)

Languages

Développement du C&C – Technologies générales

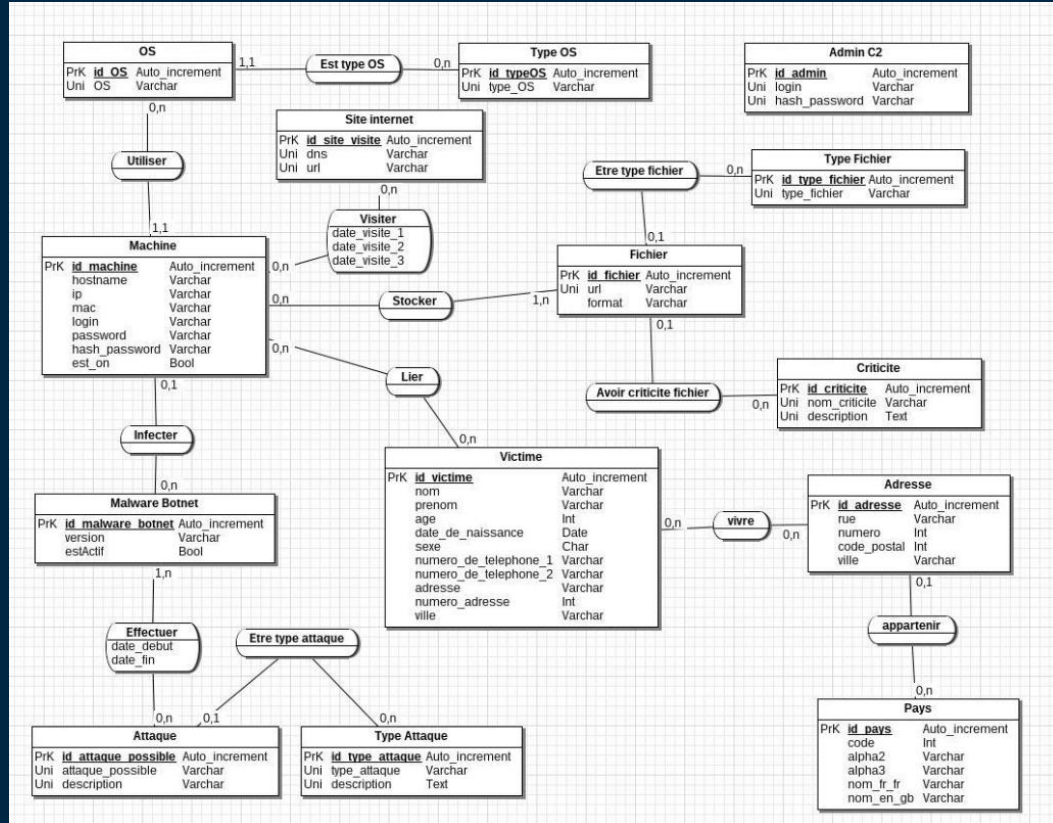


Bootstrap



Développement du C&C – BD

- MCD



1



Développement du C&C – BD – Script MySQL



```
▷ Execute
CREATE TABLE `Machine` (
  `id_machine` int(11) NOT NULL,
  `hostname` varchar(25) DEFAULT NULL,
  `ip` varchar(25) DEFAULT NULL,
  `mac` varchar(25) DEFAULT NULL,
  `login` varchar(45) DEFAULT NULL,
  `password` varchar(80) DEFAULT NULL,
  `hash_password` varchar(100) DEFAULT NULL,
  `est_on` tinyint(1) DEFAULT NULL,
  `id_OS` int(11) NOT NULL,
  `id_malware_botnet` int(11) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_general_ci;
```

```
--
-- Index pour la table `Machine`
--
▷ Execute
ALTER TABLE `Machine`
  ADD PRIMARY KEY (`id_machine`),
  ADD KEY `FK_Machine_id_OS` (`id_OS`),
  ADD KEY `FK_Machine_id_malware_botnet` (`id_malware_botnet`);
```

Développement du C&C – Architecture – Routage

⚙️ .htaccess X

⚙️ .htaccess

```
1 RewriteEngine On
2
3 RewriteCond %{REQUEST_FILENAME} !-f
4 RewriteCond %{REQUEST_FILENAME} !-d
5 RewriteRule ^(.*)$ index.php?url=$1 [NC,L]
```

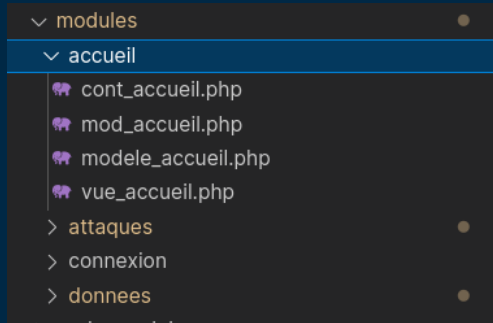
```
1 <?php
2 if (!isset($_SESSION['login'])) {
3     session_start();
4 }
5
6 $url = '';
7 if (isset($_GET['url'])) {
8     $url = explode('/', $_GET['url']);
9 }
10
11 if (isset($url[0])) {
12     $page = $url[0];
13 } else if (isset($_SESSION['login'])) {
14     $page = 'accueil';
15 } else {
16     $page = 'connexion';
17 }
18
```

```
39
40 if (in_array($page, array('connexion'))) {
41     ob_start();
42     require "modules/$page/mod_$page.php";
43     $pageContent = ob_get_clean();
44     require 'layout_connexion.php';
45 }
46 else if (in_array($page, array('accueil', 'attaques', 'donnees', 'connexion'))) {
47     ob_start();
48     require "modules/$page/mod_$page.php";
49     $pageContent = ob_get_clean();
50     require 'layout.php';
51 }
52 else {
53     http_response_code(404);
54     die;
55 }
```


Développement du C&C – Architecture – Layout

```
1 <!DOCTYPE html>
2 <html lang="fr">
3
4 <head>
5   <meta charset="utf-8">
6   <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
7   <title><?php echo $title ?></title>
8   <link rel="stylesheet" href="http://localhost/vendors/feather/feather.css">
9   <link rel="stylesheet" href="http://localhost/vendors/mdi/css/materialdesignicons.min.css">
10  <link rel="stylesheet" href="http://localhost/vendors/ti-icons/css/themify-icons.css">
11  <link rel="stylesheet" href="http://localhost/vendors/typicons/typicons.css">
12  <link rel="stylesheet" href="http://localhost/vendors/simple-line-icons/css/simple-line-icons.css">
13  <link rel="stylesheet" href="http://localhost/vendors/css/vendor.bundle.base.css">
14  <link rel="stylesheet" href="http://localhost/vendors/datatables.net-bs4/dataTables.bootstrap4.css">
15  <link rel="stylesheet" href="http://localhost/js/select.dataTables.min.css">
16  <link rel="stylesheet" href="http://localhost/css/vertical-layout-light/style.css">
17  <link rel="shortcut icon" href="http://localhost/images/favicon.png" />
18 </head>
19
20   <?php require 'include/inc_top.php' ?>
21   <?=(isset($pageContent)) ? $pageContent : $error = '403'; ?>
22   <?php require 'include/inc_footer.php' ?>
23
24  <script src="http://localhost/vendors/js/vendor.bundle.base.js"></script>
25  <script src="http://localhost/vendors/chart.js/Chart.min.js"></script>
26  <script src="http://localhost/vendors/bootstrap-datepicker/bootstrap-datepicker.min.js"></script>
27  <script src="http://localhost/vendors/progressbar.js/progressbar.min.js"></script>
28  <script src="http://localhost/js/off-canvas.js"></script>
29  <script src="http://localhost/js/hoverable-collapse.js"></script>
30  <script src="http://localhost/js/template.js"></script>
31  <script src="http://localhost/js/jquery.cookie.js" type="http://localhost/text/javascript"></script>
32  <script src="http://localhost/js/dashboard.js"></script>
33  <script src="http://localhost/js/Chart.roundedBarCharts.js"></script>
34  <script src="http://localhost/vendors/js/vendor.bundle.base.js"></script>
35
36 </body>
37 </html>
```

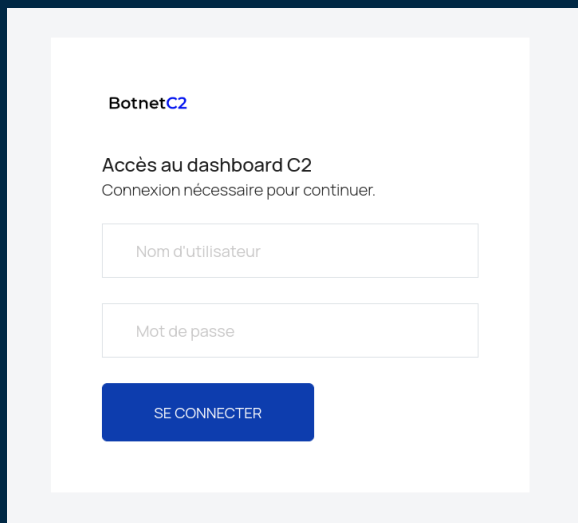
Développement du C&C – Architecture – MVC



```
1 <?php
2 require_once 'cont_accueil.php';
3
4 class ModAccueil
5 {
6
7     public function __construct($url)
8     {
9         $controllAccueil = new ContAccueil();
10         if (isset($_SESSION['login'])) {
11             $controllAccueil->accueil();
12         } else {
13             http_response_code(404);
14             die;
15         }
16     }
17 }
18 ?>
19
20 <?php
21 $modAccueil = new ModAccueil((isset($url)) ? $url : null);
22 ?>
```

```
1 <?php
2 require_once 'vue_accueil.php';
3 require_once 'modele_accueil.php';
4
5 class ContAccueil
6 {
7     function __construct()
8     {
9         $this->modele = new ModeleAccueil();
10        $this->vue = new VueAccueil();
11    }
12
13    public function accueil()
14    { ...
15    }
16 }
```

Développement du C&C – Module Connexion



BotnetC2

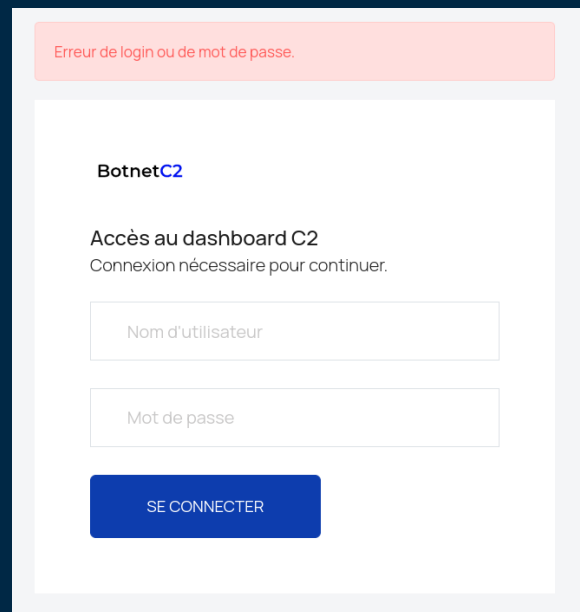
Accès au dashboard C2
Connexion nécessaire pour continuer.

Nom d'utilisateur

Mot de passe

SE CONNECTER

This is a login form for BotnetC2. It features a white background with a light gray border. At the top, the text 'BotnetC2' is displayed in a bold, black font. Below it, the heading 'Accès au dashboard C2' is followed by the instruction 'Connexion nécessaire pour continuer.' in a smaller font. There are two input fields: 'Nom d'utilisateur' and 'Mot de passe', both with light gray borders and placeholder text. A blue button with the text 'SE CONNECTER' is positioned at the bottom.



Erreur de login ou de mot de passe.

BotnetC2

Accès au dashboard C2
Connexion nécessaire pour continuer.

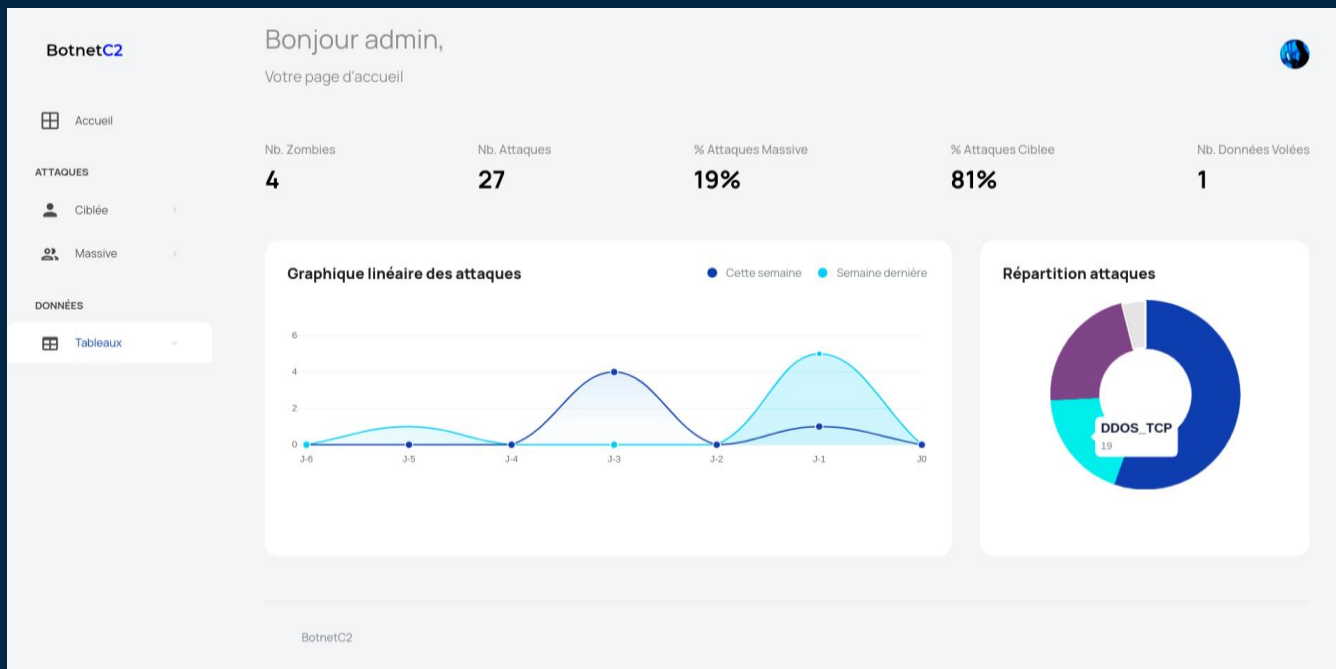
Nom d'utilisateur

Mot de passe

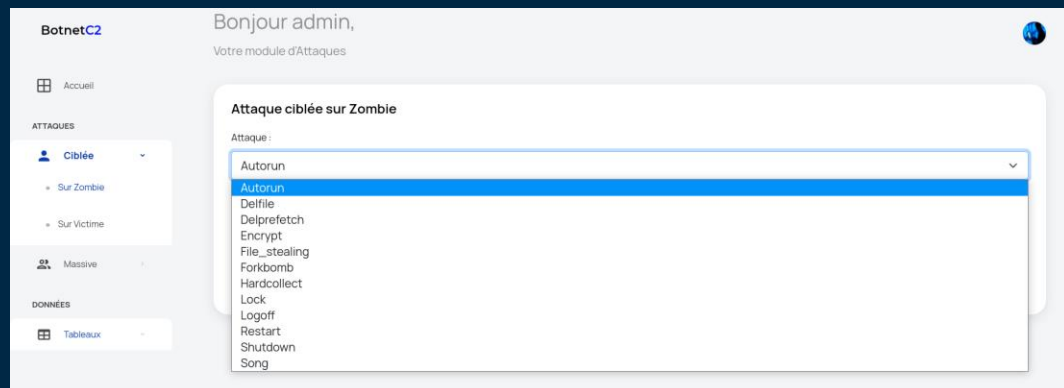
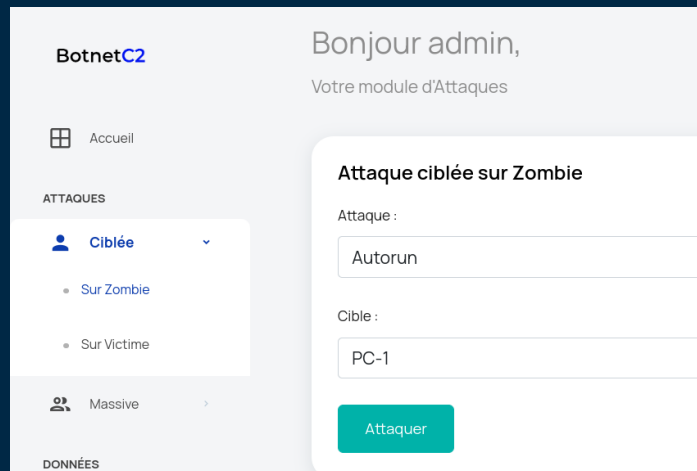
SE CONNECTER

This is the same login form as the one on the left, but it includes an error message at the top. The error message, 'Erreur de login ou de mot de passe.', is displayed in a red box with a white border. The rest of the form, including the BotnetC2 logo, the dashboard access heading, the input fields, and the 'SE CONNECTER' button, remains identical to the previous version.

Développement du C&C – Module Accueil



Développement du C&C – Module Attaques



Développement du C&C – Module Données

Bonjour admin,

Votre module de données

Historique des attaques

Hostname	IP	Nom de l'attaque	Status	Date
PC-1	192.168.1.51	Autorun	FINIE	2023-01-04
PC-1	192.168.1.51	Autorun		
PC-1	192.168.1.51	Autorun		

Liste des Fichiers collectés

Hostname	IP	Nom fichier	Date de collecte	Lien
PC-1	192.168.1.51	photo_de_famille.png	2023-01-03	photo_de_famille.png

Liste des Machines Zombies

Hostname	IP	Login	PASSWD	HASH	ON/OFF	MAC	Version du Botnet
PC-1	192.168.1.51	PC-1			JOIGNABLE		1.0
PC-2	192.168.1.52	PC-2	PC-2		JOIGNABLE	00:1B:44:11:3A:B8	1.0
PC-3	192.168.1.40	PC-3	PC-3		INJOIGNABLE	D4-FB-6A-7C-31-B4	1.0
PC-4	192.168.1.41	PC-4	PC-4		INJOIGNABLE	D4-FB-6B-7C-31-B4	1.0

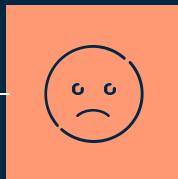
RETOUR EXPERIENCE



01

SUCCES

- Résultat fonctionnel et de bonne qualité
- Respect global du cahier des charges
- Expérience en terme de savoir-faire et savoir-être



02

ECHECS

- Manque de rigueur (méthodologie, code)
- Le résultat aurait donc pu être meilleur



03

CHANGEMENT

- Respect commun des engagements
- Mieux communiquer et être plus sérieux

EVOLUTION

Amélioration de la communication avec le Malware

- Récupération de plus d'informations

Ajout de fonctionnalités :

- Pouvoir filtrer les données du module accueil et données
- Pouvoir mieux sélectionner les attaques sur certains zombies/victimes
- Ajout d'interactivité avec les attaques



CONCLUSION

1. Résultat obtenu
2. Expérience très enrichissante
3. Méthodologie solide mais non suffisamment suivie
4. Des évolutions possibles, rapides à mettre en place maintenant que les fondements du projet et expériences sont là

The background is a dark blue gradient. It features several thin, vertical white lines of varying lengths. Scattered across the slide are numerous small squares in three colors: light pink, light orange, and light teal. Some squares are solid, while others are outlined. The text is centered on the slide.

Merci de votre écoute !

Des questions ?