

PRÉSENTATION DE PARII:

plateforme d'alerte risque intrusion interentreprises

INTRODUCTION

- L'application mobile doit remplir un double rôle: être un guide contre les menaces cyber et être un outil puissant en cas de cyberattaque.
- L'application est développée sous Xcode (version 12.4).
- Présentation sous Iphone 11.

ACCUEIL

Le bouton recouvre la totalité de l'écran donc on peut appuyer sur n'importe quelle zone de l'écran pour continuer.

10:47



GOUVERNEMENT

*Liberté
Égalité
Fraternité*

Bienvenue sur

**Plateforme d'alerte risque
intrusion interentreprise**

Appuyez pour continuer

MENU

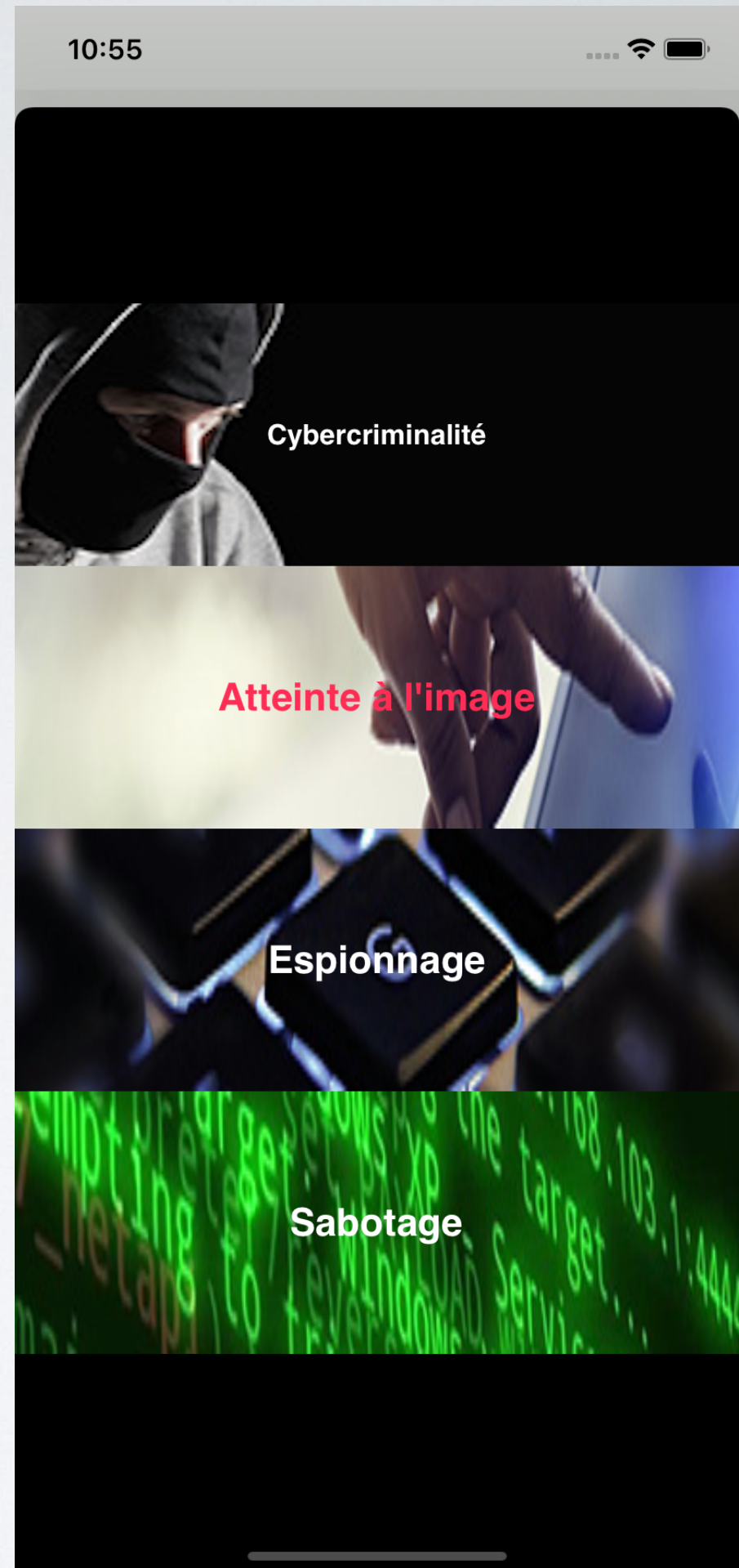
Nous avons au total sept boutons
dont trois principaux:
« Informations », « Organiser son
rendez-vous » et « Alerter une
cyberattaque ».



INFORMATIONS

INFORMATIONS

Lorsqu'on appuie sur le bouton, quatre rubriques apparaissent. Chaque rubrique contient un texte informatif. Les quatre rubriques sont à voir dans la page suivante.



Les pages suivantes sont munies d'un « scroller ». On peut dérouler la page vers le bas pour lire la suite.

CYBERCRIMINALITÉ

En pleine recrudescence, de nombreuses attaques ciblent les particuliers mais aussi les entreprises et les administrations. Elles visent à obtenir des informations personnelles afin de les exploiter ou de les revendre (données bancaires, identifiants de connexion à des sites marchands, etc.).

Hameçonnage (phishing) et « Rançongiciel » (ransomware) sont des exemples connus d'actes malveillants portant préjudices aux internautes. Pour s'en prémunir, des réflexes simples existent.

QUELS SONT LES DIFFÉRENTS TYPES D'ATTAQUES ?

Attaque par hameçonnage (phishing)
L'hameçonnage, phishing ou filoutage est une technique malveillante très courante sur Internet. L'objectif : opérer une usurpation d'identité afin d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel.

Le cybercriminel se « déguise » en un tiers de confiance (banques, administrations, fournisseurs d'accès à Internet...) et diffuse un mail frauduleux, ou contenant une pièce jointe piégée, à une large liste de contacts. Le mail invite les destinataires à mettre à jour leurs informations personnelles (et souvent bancaires) sur un site Internet falsifié vers

ATTEINTE À L'IMAGE

Lancées à des fins de déstabilisation contre des administrations et des entreprises et régulièrement relayées par les réseaux sociaux, les attaques de déstabilisation sont aujourd'hui fréquentes et généralement peu sophistiquées, faisant appel à des outils et des services disponibles en ligne. De l'exfiltration de données personnelles à l'exploitation de vulnérabilité, elles portent atteinte à l'image de la victime en remplaçant le contenu par des revendications politiques, religieuses, etc.

QUELS SONT LES DIFFÉRENTS TYPES D'ATTAQUES ?

Attaque par déni de service (ddos)

Le déni de service peut porter atteinte à l'image de la victime et constitue une menace pour toute organisation disposant d'un système d'information connecté à Internet. L'objectif : rendre le site internet, et donc le service attendu, indisponible. Les motivations des attaquants sont diverses, allant des revendications idéologiques à la vengeance, en passant par les extorsions de fonds.

Le cybercriminel peut :
exploiter une vulnérabilité logicielle ou matérielle
solliciter une ressource particulière du système d'information de la cible, jusqu'à « épuisement ». Cette ressource peut être la bande passante du réseau, la capacité de traitement globale d'une base de données, la puissance de calcul des processeurs, l'espace disque, etc.

ESPIONNAGE

Très ciblées et sophistiquées, les attaques utilisées pour l'espionnage à des fins économiques ou scientifiques sont souvent le fait de groupes structurés et peuvent avoir de lourdes conséquences pour les intérêts nationaux. De fait, il faut parfois des années à une organisation pour s'apercevoir qu'elle a été victime d'espionnage, l'objectif de l'attaquant étant de maintenir discrètement son accès le plus longtemps possible afin de capter l'information stratégique en temps voulu.

QUELS SONT LES DIFFÉRENTS TYPES D'ATTAQUES ?

Les modes opératoires de ces attaques rappellent ceux que les analystes américains ont baptisé APT (Advanced Persistent Threat) et qui touchent régulièrement des institutions et des industriels œuvrant dans des secteurs sensibles. Nombre de ces attaques sont très similaires, tant par leurs modes opératoires que par les techniques d'infiltration et d'exfiltration employées.

ATTAQUE PAR POINT D'EAU (WATERING HOLE)

La technique du « point d'eau » consiste à piéger un site Internet légitime afin d'infecter les équipements des visiteurs du secteur d'activité visé par l'attaquant. Objectif : infiltrer discrètement les ordinateurs de personnels œuvrant dans un secteur d'activité ou une organisation ciblée pour récupérer des données.

Le cybercriminel exploite une vulnérabilité d'un site web et y dépose un virus (malware).

SABOTAGE

Le sabotage informatique est le fait de rendre inopérant tout ou partie d'un système d'information d'une organisation via une attaque informatique.

QUELS SONT LES DIFFÉRENTS TYPES D'ATTAQUES ?

Le sabotage s'apparente à une « panne organisée », frappant tout ou partie des systèmes, selon le type d'atteinte recherchée – désorganisation durable ou non, médiatisée ou non, plus ou moins coûteuse à réparer. Pour y parvenir, les moyens d'attaques sont d'autant plus nombreux que les organisations ne sont pas toujours préparées à faire face à des actes de malveillance.

Le sabotage et la destruction de systèmes informatiques peuvent avoir des conséquences dramatiques sur l'économie d'une organisation, sur la vie des personnes, voire sur le bon fonctionnement de la Nation s'ils touchent des secteurs d'activité clés. Afin d'éviter ce type de menace, l'ANSSI, l'Agence nationale de la sécurité des systèmes d'information, met l'accent sur la prévention.

A ce titre, elle :

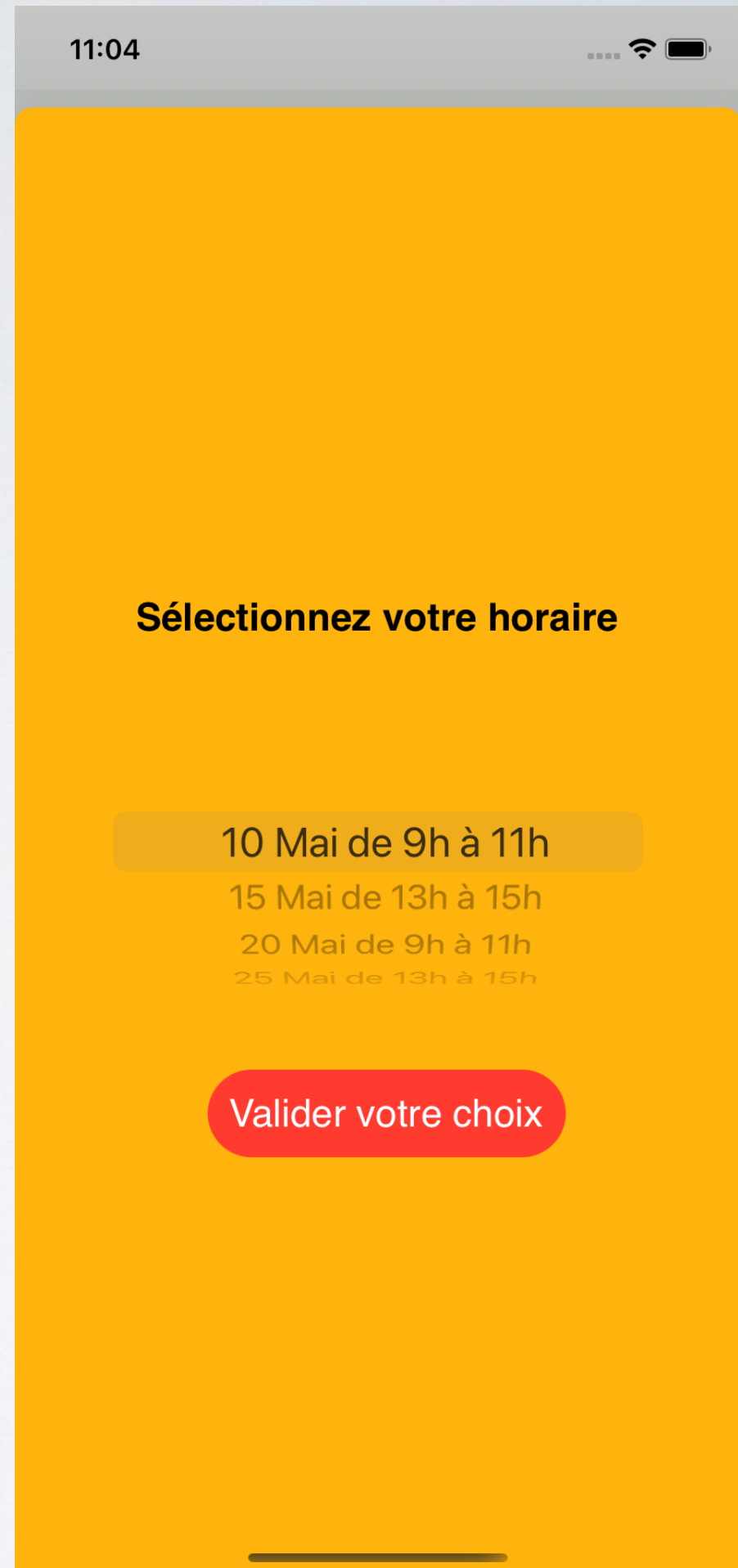
publie des recommandations de sécurité ;
labellise des produits et des prestataires de confiance ;
définit une réglementation permettant à

ORGANISER SON RENDEZ-
VOUS

ORGANISER SON RENDEZ-VOUS

Plusieurs dates sont proposées.

Une fois la date choisie, on appuie sur le bouton « Valider votre choix ». Ici, quatre dates sont à choisir. Ces dates sont des éléments du tableau « Horaires » dans le code.



11:04

Sélectionnez votre horaire

10 Mai de 9h à 11h

15 Mai de 13h à 15h

20 Mai de 9h à 11h

25 Mai de 13h à 15h

Valider votre choix

The image shows a mobile application interface for scheduling an appointment. At the top, there is a status bar with the time 11:04 and icons for signal strength, Wi-Fi, and battery. The main background is a solid orange color. In the center, the text 'Sélectionnez votre horaire' is displayed in bold black font. Below this, there are four selectable options, each represented by a light orange rounded rectangle containing the date and time range: '10 Mai de 9h à 11h', '15 Mai de 13h à 15h', '20 Mai de 9h à 11h', and '25 Mai de 13h à 15h'. At the bottom, there is a red rounded button with the text 'Valider votre choix' in white. A thin horizontal line is visible at the very bottom of the screen, likely representing the home indicator bar on an iPhone.

ORGANISER SON RENDEZ-VOUS

Lorsqu'on appuie sur le bouton, une nouvelle page s'ouvre confirmant la date choisie. De plus, on affiche « choix validé » dans la console. Aussi, on déclare une variable qui prend en valeur la date choisie que l'on va afficher. Ces données peuvent ainsi être envoyées vers une base de données pour être traitées.



```
2021-02-27 11:13:00.078665+0100 PARI[1874:106842] [Storyboard] Unknown  
class RDVValide in Interface Builder file.
```

```
choix validé  
15 Mai de 13h à 15h
```

All Output ↕

Filter



ALERTER UNE CYBERATTATQUE

ALERTER UNE CYBERATTACHE

Plusieurs champs de texte sont à remplir. Nous écrivons un exemple. Ensuite, appuyons sur le bouton « Valider ».

11:20

Veillez renseigner les informations suivantes

Nom de l'entreprise

Adresse

Telephone

Description de l'attaque

Valider



11:22

Veillez renseigner les informations suivantes

Nom de l'entreprise

Adresse

Telephone

Description de l'attaque

Valider

On va récupérer cette donnée dans la page suivante

ALERTER UNE CYBERATTATQUE

Une nouvelle page de confirmation s'ouvre. Cette page a la particularité de récupérer le nom de l'entreprise. En effet, il y a une transmission de données entre deux pages. Pour ce faire, du code a été nécessaire pour réaliser cela.

Ensuite, ces données peuvent être envoyées vers une base de données pour être traitées.

11:24



**Merci pour votre
confiance
Google France !**

**Nous avons bien
reçu votre alerte,
nous allons
immédiatement
vous contacter.
Veuillez patienter.**

PLUS

Les pages sont courtes et munies d'un effet de transparence.

LIENS UTILES

11:31

Menu



GOUVERNEMENT

Liberté
Égalité
Fraternité

Où se renseigner contre la cybermalveillance

<https://www.cybermalveillance.gouv.fr>

En cas de tentative d'intrusion

Alerter une cyberattaque

Où se renseigner contre les risques cyber

<https://www.gouvernement.fr/risques/risques-cyber>

Liens utiles

Paramètres

Confidentialité

A propos - Nous contacter

PARAMÈTRES

11:32

Menu



GOUVERNEMENT

Liberté
Égalité
Fraternité

Notifications "informations"

Recevez une notification quand de nouvelles informations sont disponibles.

Me notifier



Alerter une cyberattaque

Plus

Liens utiles

Paramètres

Confidentialité

A propos - Nous contacter

CONFIDENTIALITÉ

11:32

Menu



GOUVERNEMENT

Liberté
Égalité
Fraternité

Vos données sont protégées

L'application est conforme à la réglementation qui garantit la protection de vos données.

En cas de tentative d'intrusion

Alerter une cyberattaque

Plus

Liens utiles

Paramètres

Confidentialité

A propos - Nous contacter

A PROPOS - NOUS CONTACTER

11:32

Menu



GOUVERNEMENT

Liberté
Égalité
Fraternité

Nous contacter par téléphone (ANSSI)

+33 (0)1 71 75 84 00

En cas de tentative d'intrusion

Alerter une cyberattaque

Nous contacter par e-mail (ANSSI)

[secretariat.anssi\[at\]ssi.gouv.fr](mailto:secretariat.anssi[at]ssi.gouv.fr)

Liens utiles

Paramètres

Confidentialité

A propos - Nous contacter