SENSIBILISATION CYBER : COMPRENDRE UNE CYBERATTAQUE

Aliénor DENISET (CSIRT-BFC, GIP ARNia)


LOCKBIT 2.0
ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!
All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.
Si vous voyez cela, c'est qu'il est déjà trop tard !
500 Internal Server Error
domain.com
Internal Server Error
The server encountered an internal error or misconfiguration
Libraries
Documents
Organize
Open
Share with
E-mail
New folder
Search Documents
Favorites
Libraries
Computer
Network
Documents library
Includes: 2 locations
Arrange by: Folder
Date modified
Type
50F94EC8A2462EAA5BB73EB8F178FDCF.CADB7
54A4F7652205EF0F1442044FC8A047E6.3B2CF
93AD590D3DD2461884A64065C7BE5EDE.FAB68
112B62E504B391474FADD4966FF04980.51486
140E5AE770D1147D85A4965176B66915.5DE82
708B58F71B9C15772C238DAA57100BD1.F13C6
134087DCA2ABB86E74B2C949F6DAF631.3BFF5
570403F25769647D5855725B56B75191.8565C
A29B874B80D9191619C0DBD3B29A0D59.FDD5A
C7959A4C407C8E2663C8B8478517187C.D1194
D3E9992C400E24A91352310140FD1FCE.107C9
37F74390AEFF9CF14D8F47A24A6DC590.0...
0728B File
Date modified: 10/8/2013 3:10 PM
Size: 62.0 KB
Date created: 3/17/2015 1:30 PM

De quoi parle-t-on ?

Selon vous, quelle est la définition d'une cyberattaque ?

Selon Le Robert, c'est un « Acte de piratage informatique sur Internet »


PC bloqué
Note de rançon
Message d'erreur
Réseau compromis
Vulnérabilité exploitée
Espionnage
Enquête sur les réseaux sociaux
Données altérées
Collaborateur corrompu

Quand arrive la cyberattaque ?

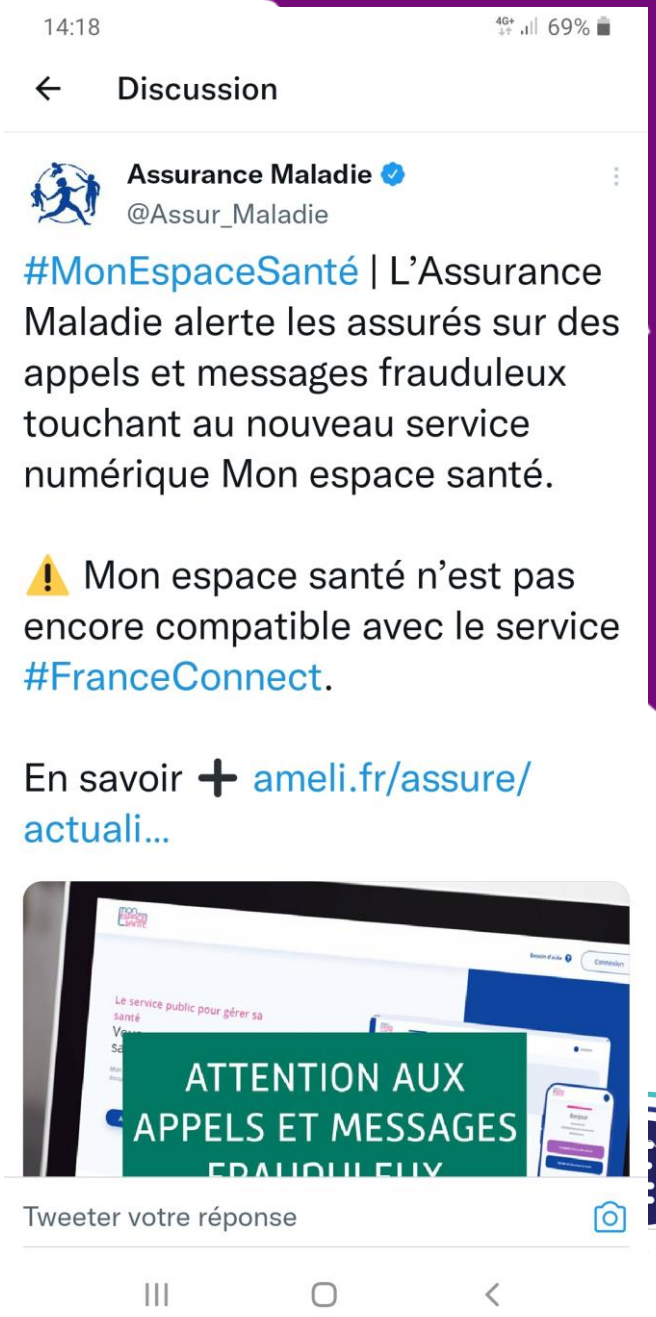
Difficile de prévoir…

Opportuniste

- Pas de règles
- Scan du web, phishing…

En lien avec l'actualité

- Lancement d'un nouveau service
  - *Exemple : Mon Espace Santé (courriels de phishing quelques jours après)*



Pourquoi ?

Différentes motivations

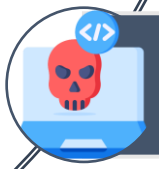

Votre argent *(rançon)*


Vos données *(récupération, destruction, modification)*


Enjeux politiques ou idéologiques


Espionnage


Augmentation de la notoriété du hacker


Utiliser votre système comme rebond, comme puissance de calcul ou comme ressource *(minage de cryptomonnaies, téléchargement illégal…)*

Par qui ?

L'importance de connaître son adversaire

- Savoir définir :
  - Son niveau technique
  - Ses motivations

	Niveau technique	Motivations	Impact	Vraisemblance	Risque
Opposant politique	Faible à moyen	Créer une interruption de services, espionner	Fort	Moyenne à Elevée	Très élevé

Prendre en compte la menace interne

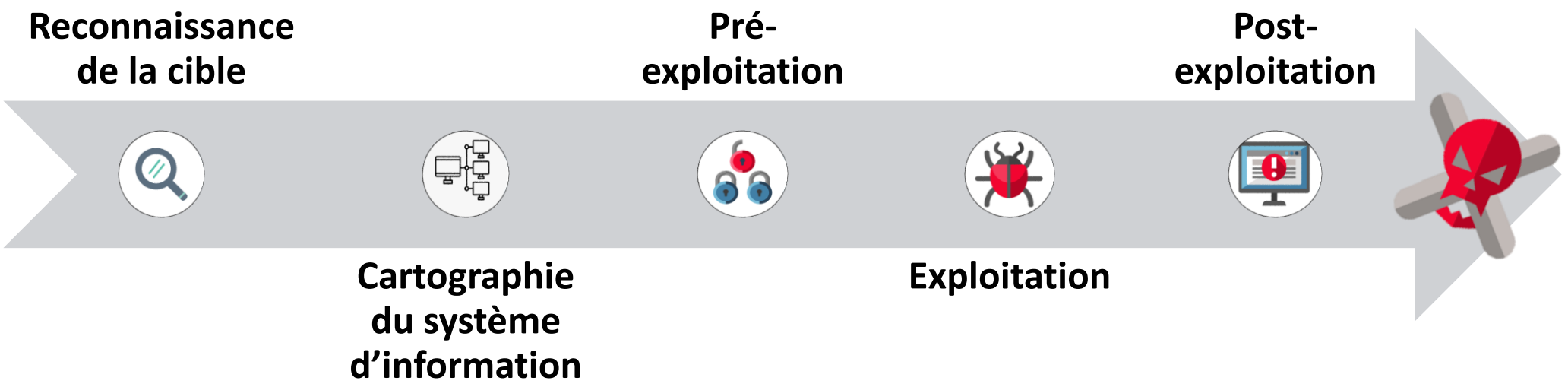
- Plus difficile à détecter
- Action voulue ou accidentelle
- Risque accru de divulgation de secret professionnel / données personnelles

→ Vigilance au moment du recrutement

→ Donner l'information uniquement aux personnes qui en ont besoin

Comment ça se passe ?

Le parcours du cyberattaquant



Ce processus peut durer de quelques heures à plusieurs mois/années

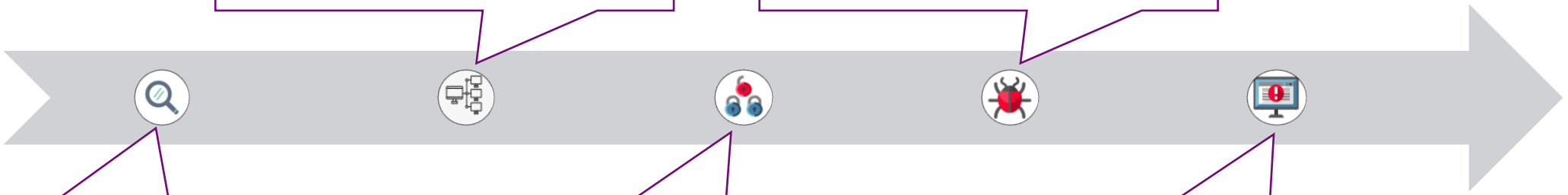
Contrairement à nous, les cybercriminels ont tout leur temps !

Comment ça se passe ?

Exemple : L'attaque d'un site web

CARTOGRAPHIE
- Version du gestionnaire de contenu obsolète

EXPLOITATION
La vulnérabilité découverte grâce au bug est exploitée



RECONNAISSANCE
Repérage d'un bug sur le site web
- erreur de conception
- faille logicielle…

PRE-EXPLOITATION
Cette version est concernée par une vulnérabilité

POST-EXPLOITATION
- Intrusion dans le système
- Obtention de privilèges administrateur ou éditeur du site
- Effacement des traces

- Modification du contenu du site
- Redirection des visiteurs vers un domaine malveillant
- Mise hors ligne du site…

Les principaux vecteurs d'intrusion

Le logiciel

- Logiciels obsolètes
- Logiciels vulnérables

Le matériel

- Intrusion physique
- Utilisation de matériel corrompu
- Composants vulnérables

Le réseau

- Connexion à distance
- Connexion via un réseau public/non sécurisé

L'humain

- Hameçonnage
- Ingénierie sociale
- Mauvaises pratiques
- Inattentions

La plus grosse faille : l'humain

Les attaquants cherchent à exploiter les émotions humaines :

- Peur
- Sentiment d'urgence
- Avidité
- Curiosité
- Entraide

Quelques exemples d'attaques ayant recours à l'ingénierie sociale

Le tailgating (ou talonnage)

- Objectif : entrer dans une zone protégée
- Mode opératoire : suivre un collaborateur
- Conséquences : vol/destruction de matériel, accès à des informations sensibles….

Demander l'identité et la fonction aux personnes extérieures

Entraide

Quelques exemples d'attaques ayant recours à l'ingénierie sociale

Clé USB piégée

- Objectif : compromettre un poste de travail/serveur
- Mode opératoire : offrir une clé, laisser une clé abandonnée en évidence…
- Conséquences : destruction de matériel, accès à des informations sensibles, espionnage, compromission du réseau entier….

Proscrire l'utilisation de clés USB extérieures

Curiosité

Quelques exemples d'attaques ayant recours à l'ingénierie sociale

Arnaque au faux support informatique

- Objectif : compromettre un poste de travail/serveur
- Mode opératoire : pousser à appeler un numéro frauduleux
- Conséquences : accès à des informations sensibles, espionnage, vol de données….

Eviter d'agir dans l'urgence

Sentiment d'urgence

Peur

Qu
à l

A

:(

Votre ordinateur a été verrouillé

Votre ordinateur nous a averti qu'il était infecté par un virus et un logiciel espion. Les données suivantes sont à risque:

- Identifiant Facebook, identifiants de messagerie
- Information de carte de crédit, accès bancaires
- Fichiers sur cet ordinateur

Ne redémarrez pas votre ordinateur et contactez Windows, sinon nous ne pourrons garantir la sécurité de vos données.

Pour plus d'informations sur ce problème et sur les solutions possibles, consultez le site https://www.windows.com/stopcode

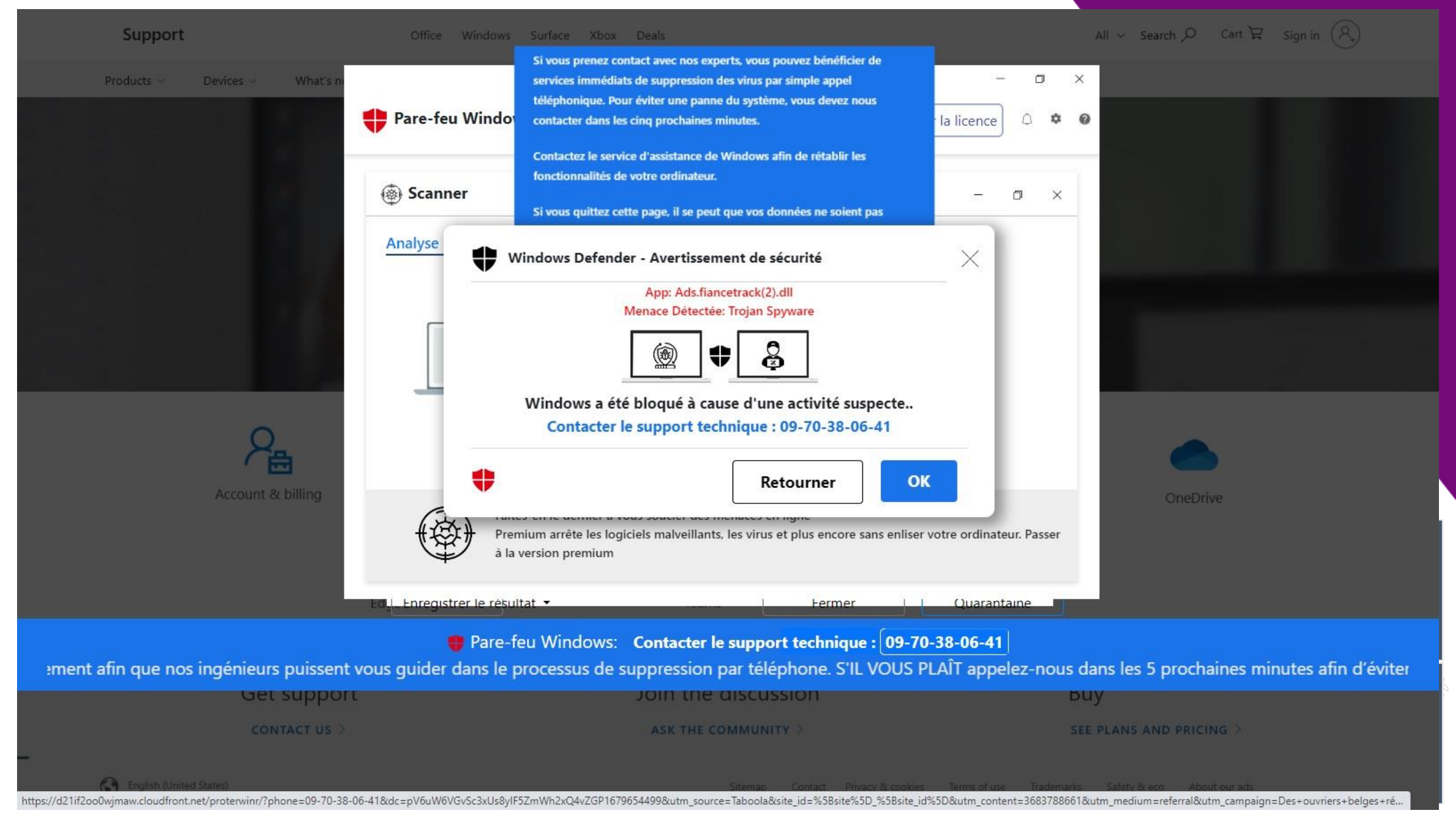
Si vous contactez l'assistance, transmettez-leur ces informations:

Code d'arrêt: SPYWARE

Appelez le support technique Windows: 09 77 19 94 56 (Appel gratuit)

nent
nce

r


Support
Office
Windows
Surface
Xbox
Deals
All
Search
Cart
Sign in
Products
Devices
Si vous prenez contact avec nos experts, vous pouvez bénéficier de services immédiats de suppression des virus par simple appel téléphonique. Pour éviter une panne du système, vous devez nous contacter dans les cinq prochaines minutes.
Contactez le service d'assistance de Windows afin de rétablir les fonctionnalités de votre ordinateur.
Si vous quittez cette page, il se peut que vos données ne soient pas
Pare-feu Windo
la licence
Scanner
Analyse
Windows Defender - Avertissement de sécurité
App: Ads.fiancetrack(2).dll
Menace Détectée: Trojan Spyware
Windows a été bloqué à cause d'une activité suspecte..
Contacter le support technique : 09-70-38-06-41
Retourner
OK
Premium arrête les logiciels malveillants, les virus et plus encore sans enliser votre ordinateur. Passer à la version premium
Enregistrer le résultat
Fermer
Quarantaine
Account & billing
OneDrive
Pare-feu Windows: Contacter le support technique : 09-70-38-06-41
ement afin que nos ingénieurs puissent vous guider dans le processus de suppression par téléphone. S'IL VOUS PLAÎT appelez-nous dans les 5 prochaines minutes afin d'éviter
Get support
CONTACT US
Join the discussion
ASK THE COMMUNITY
Buy
SEE PLANS AND PRICING
English (United States)
Sitemap
Contact
Privacy & cookies
Terms of use
Trademarks
Safety & eco
About our ads
https://d21if2oo0wjmaw.cloudfront.net/proterwinr/?phone=09-70-38-06-41&dc=pV6uW6VGvSc3xUs8yIF5ZmWh2xQ4vZGP1679654499&utm_source=Taboola&site_id=%5Bsite%5D_%5Bsite_id%5D&utm_content=3683788661&utm_medium=referral&utm_campaign=Des+ouvriers+belges+ré...

Quelques exemples d'attaques ayant recours à l'ingénierie sociale

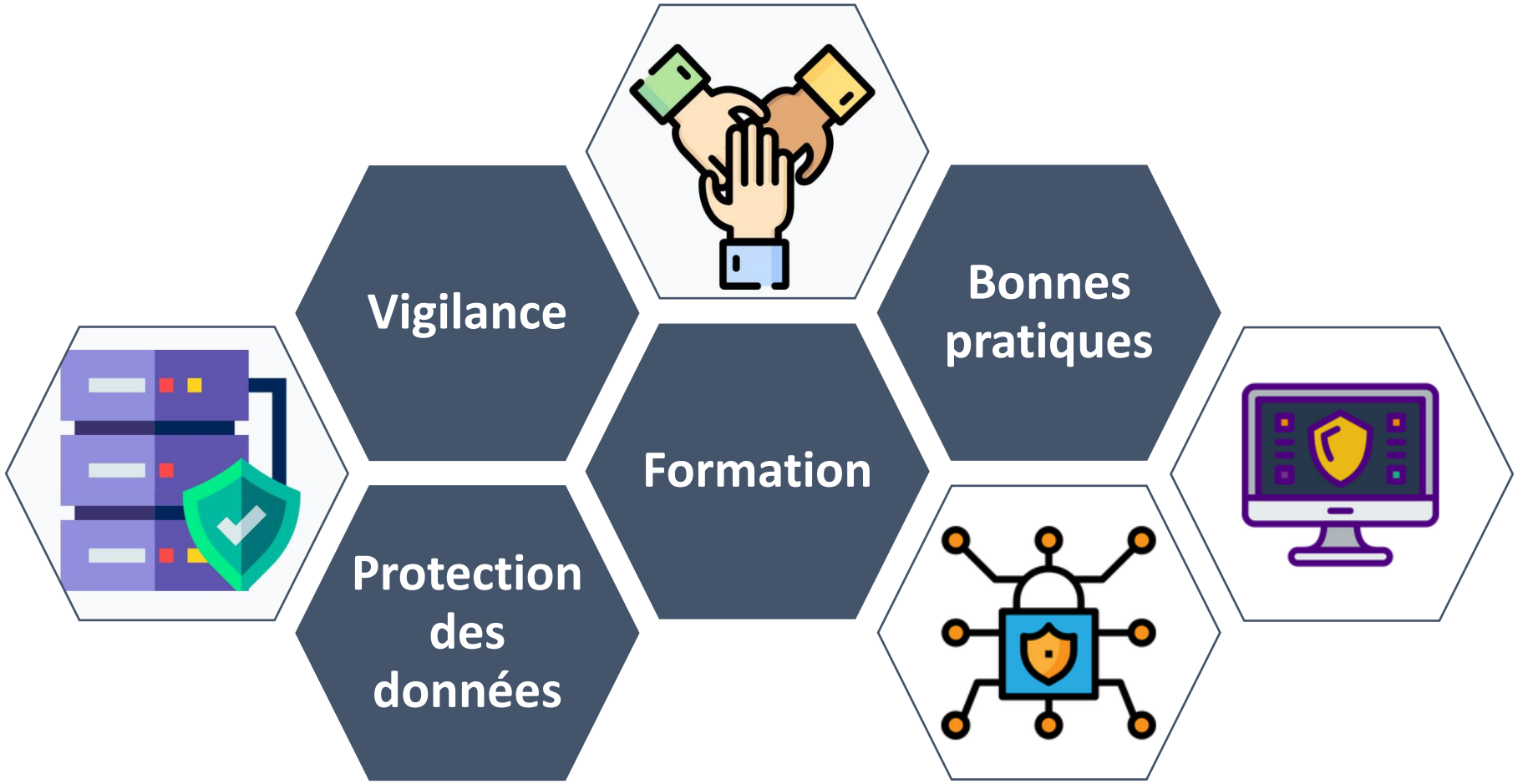
Faux point d'accès WiFi

Utiliser le partage de connexion de son smartphone

Mauvaises pratiques

Restez vigilants

La sécurité en ligne est une responsabilité partagée



En résumé

Une cyberattaque, c'est...

Imprévisible	Dévastateur	Un ensemble d'éléments bien combinés
Un vecteur d'intrusion	Exploitation de vulnérabilité(s)	Une série d'étapes

Merci pour votre attention

CSIRT-BFC

Tél : 0970 609 909 (choix 1)

https://www.csirt-bfc.fr

Pôle Cyber : cyber@arnia-bfc.fr (PGP : 0x169AB32B)

Aliénor Deniset – adeniset@arnia-bfc.fr (PGP : 0xAB63C97C3E6AB32B)