



MASTER 2 – TLS-SEC



Cybersécurité, cerner les menaces et se protéger

Lundi 30 septembre 2019



Fabrice CRASNIER

Doctorant en intelligence artificielle

Consultant expert senior - Responsable du pôle FORENSIC
Laboratoire SCASSI-CYBER - Société SCASSI Conseil

Fabrice CRASNIER

Senior Expert Consultant- Head of legal expertise activities (FORENSIC) - SCASSI-CYBER Laboratory - SCASSI Conseil - Doctoral student in artificial intelligence

- ▶ Après 27 ans au service des unités de recherche de la Gendarmerie Nationale, dont 17 années consacrées au suivi de la cyberdélinquance, j'ai rejoint SCASSI en tant que Consultant Expert Senior.
- ▶ Je suis responsable des activités d'expertise en informatique légale au laboratoire SCASSI-CYBER.
- ▶ Intéressé par les entreprises et les problématiques liées aux incidents de sécurité, je cherche à faire comprendre aux personnes et aux biens l'impact que cela a sur elles.

Expert en Cybersécurité





CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Thématiques abordées

Cerner les menaces

- La vulnérabilité du mot de passe
- L'usurpation d'identité
- Le phishing
- L'ingénierie sociale
- Les rançongiciels

Protection physique

- Le vol
- La compromission des outils communs

Les impacts sur l'entreprise

- Les obligations légales
- La eRéputation

L'escroquerie financière et la fraude

- Comprendre l'origine de certaines attaques
- Le darknet
- Les réseaux de communications sans fil
- Les smartphones
- L'internet des objets

Comment se protéger ?

- La formation des personnels
- Les principes fondamentaux de sécurité lors d'un développement
- Les services institutionnels
- Les bons réflexes de la DSI
- Les outils de sécurités pour les utilisateurs
- L'expertise en informatique légale

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Internet est devenu en quelques années un vecteur d'informations incontournables tant dans notre vie privée que dans notre sphère professionnelle.

Cette boulimie d'informations attise également toutes les convoitises, pour vous nuire directement ou bien atteindre à travers vous, votre environnement.



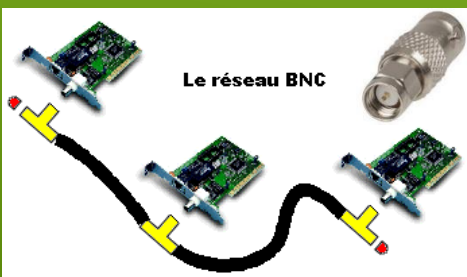
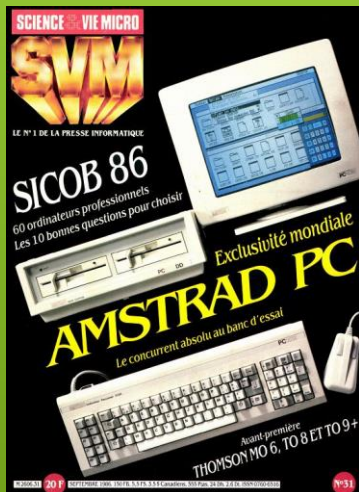
CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

SYSTEME D'INFORMATION ?



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

1986

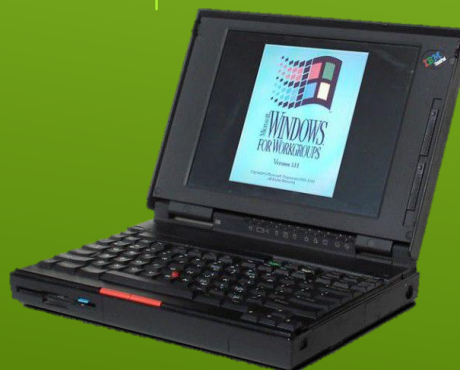
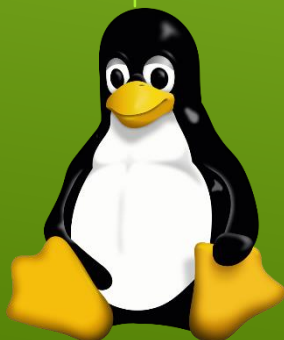


Le réseau BNC



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

————— 1996 —————





CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

————— 2016 —————



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

AUJOURD'HUI

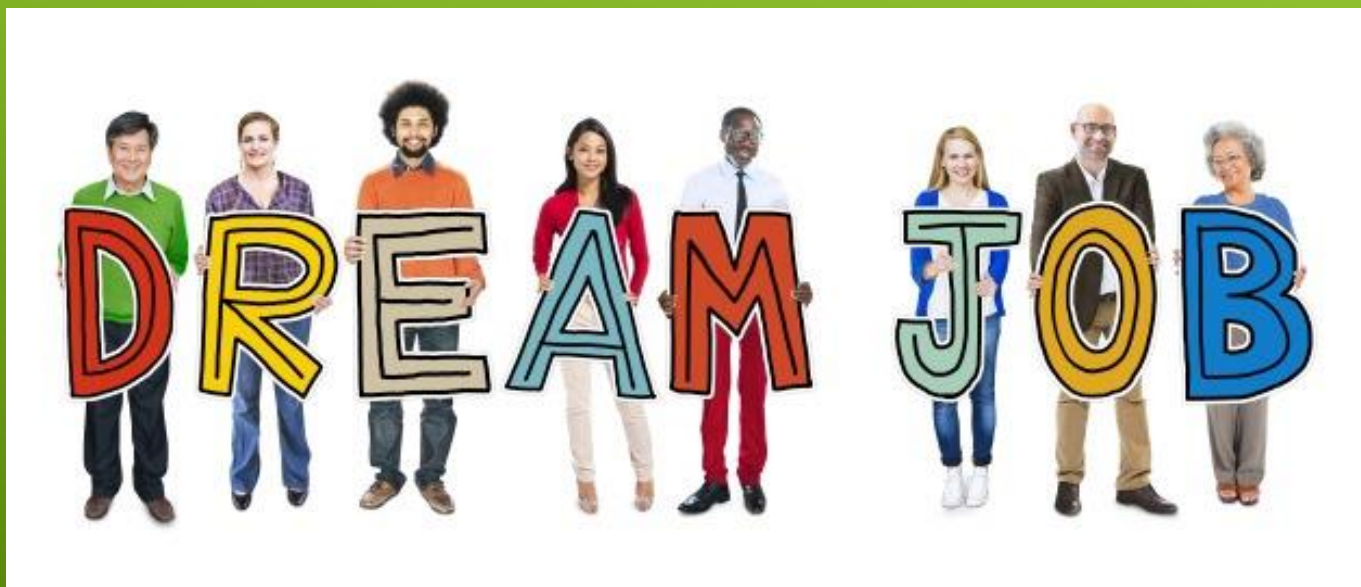


CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Un système d'information (SI)



Les métiers de cybersécurité



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER



Que risque-t-on ?



incident de sécurité

Le risque : c'est ça

Note : 18/20



Une mauvaise
estimation des
risques,



Film : le pion
1978



Ce qu'il faut éviter à tout prix

Une
destruction
des
preuves,



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Gouvernance des systèmes d'information

**ISO 27005
RISK MANAGER**

**Quelle solution ?
ÉVALUER LES RISQUES**



		Impacts				
Probabilité		Catastrophique 5	Majeur 4	Modéré 3	Mineur 2	Insignifiant 1
Très forte	5	10	9	8	7	6
Forte	4	9	8	7	6	5
Moyenne	3	8	7	6	5	4
Faible	2	7	6	5	4	3
Très faible	1	6	5	4	3	2
Niveau de risque encouru						
9 ≤ Risque extrême ≤ 10		7 ≤ Risque élevé ≤ 8		5 ≤ Risque moyen ≤ 6		1 ≤ Risque faible ≤ 4

L'évaluation
consiste à
hiérarchiser les
risques, en utilisant
des critères de
probabilité et
d'impact
préalablement
définis.

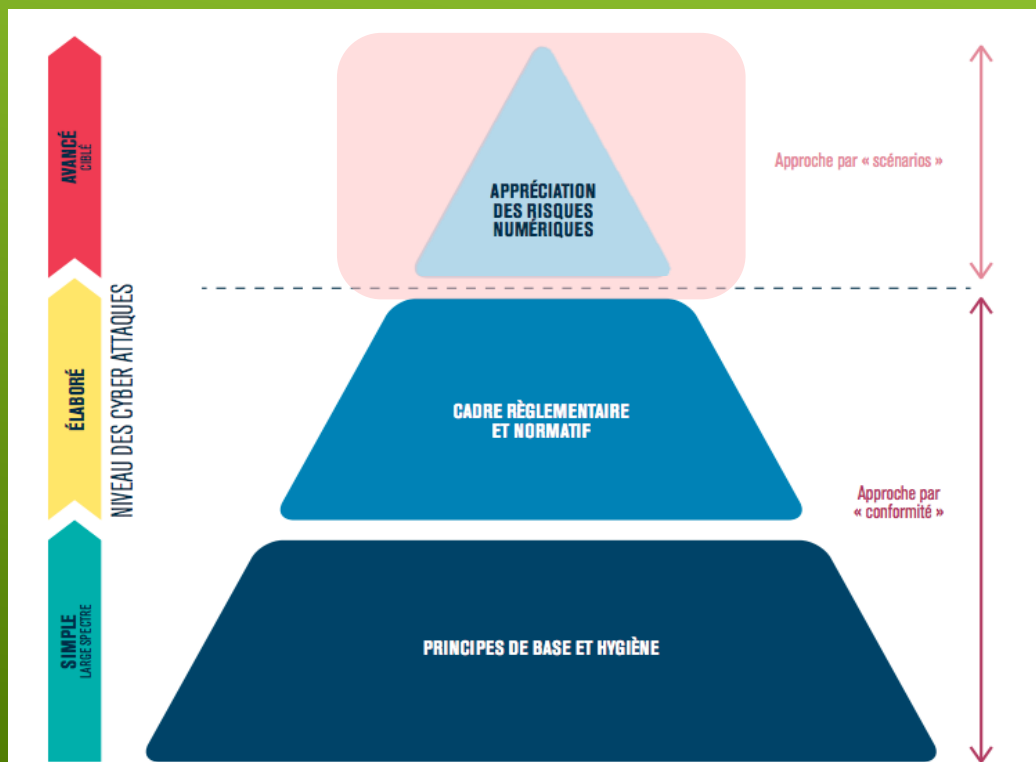


CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Gouvernance des systèmes d'information



ANTICIPER UN CYBER INCIDENT (MESURES CONSERVATOIRES, SENSIBILISATION, EXERCICES)



EBIOS Risk Manager

Version 1.0 - Octobre 2018,
Agence Nationale de la Sécurité des
Systèmes d'Information de l'Etat.

Expression des Besoins et Identification des Objectifs de Sécurité

Approche par « conformité »

Approche par « scénarios »

Gouvernance des systèmes d'information



Quelle solution ? L'accompagnement



La mise en œuvre de la gouvernance des systèmes d'information repose sur l'application d'un certain nombre de **bonnes pratiques** connues de tous les professionnels. Elles concernent quatre domaines :

- ☐ La conception des systèmes d'information,
- ☐ Le fonctionnement et le pilotage des systèmes d'information,
- ☐ Le pilotage des évolutions des systèmes d'information,
- ☐ L'évolution des systèmes d'information.

Gouvernance des systèmes d'information



Quelle solution ? **L'accompagnement**



La connaissance de ces bonnes pratiques permet d'évaluer le degré de maturité d'un système d'information et d'établir un plan d'action adapté. Cette démarche repose sur les étapes suivantes :

- ☐ Effectuer un audit du système d'information.
- ☐ Identifier les actions possibles.
- ☐ Déterminer les priorités.
- ☐ Fixer les responsabilités.
- ☐ Fixer des budgets d'investissement

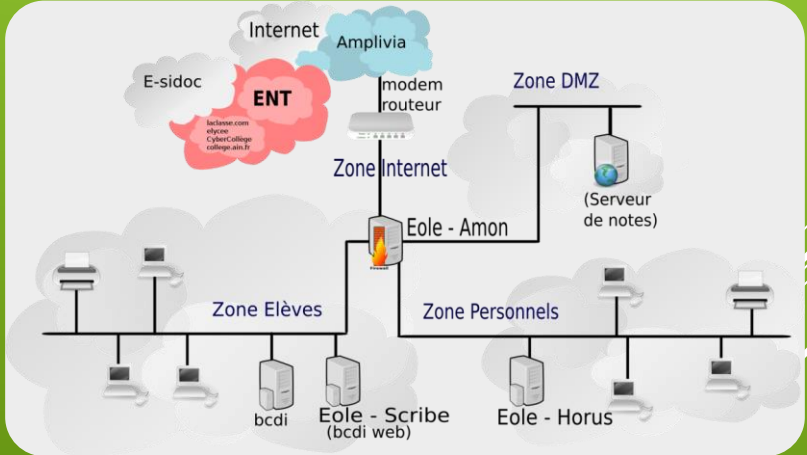


CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

L'architecture du système d'information



*Quelle solution ?
L'accompagnement*



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

L'architecture du système d'information



Quelle solution ? L'accompagnement

L'**architecte réseaux** répond aux besoins en communication numérique des utilisateurs (entreprises, administrations). Expert en **réseaux** et télécommunications, il conçoit, planifie, développe l'organisation générale (l'**architecture**) des **réseaux** de télécommunications et supervise leur mise en place... à moindre coût !

Son poste est **très technique**, Il doit analyser le réseau existant, déterminer à quoi va servir le réseau et qui va l'utiliser. Il propose des structures, des solutions qui répondent aux attentes de l'entreprise.

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

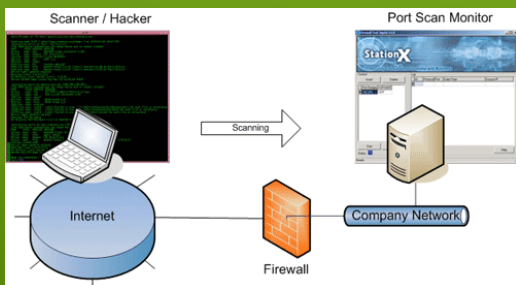
L'ingénieur infra sur le système d'information



Quelle solution ? **L'accompagnement**

Il s'assure de la sécurité de l'infrastructure du SI.

Balayage de port
« Portscanning »



Identification des ressources internes :

- ☐ Scan de plage d'adresses IP : découvrir le réseau, les machines connectées
- ☐ Scan de ports en écoute : découvrir les OS et versions de services utilisés
- ☐ Scan de vulnérabilités : découvrir les vulnérabilités des OS et services vulnérables

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

L'ingénieur infra sur le système d'information

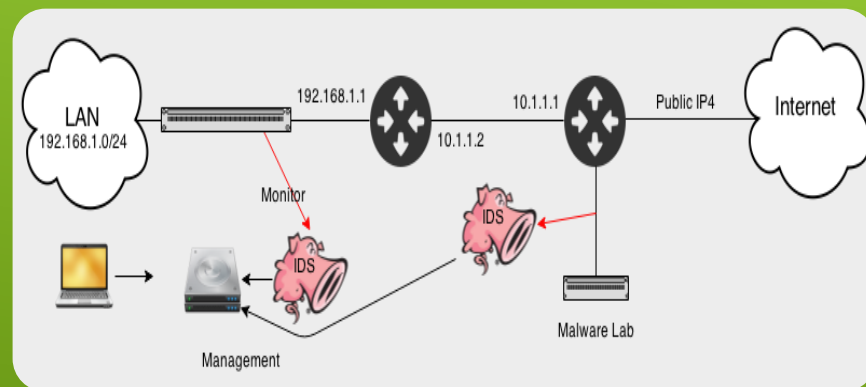


**Quelle solution ?
L'accompagnement**

Comment s'en protéger ?

Mettre en place de :

- ☐ firewalls,
- ☐ proxy,
- ☐ système de détection d'intrusion (IDS),
- ☐ système de prévention d'intrusion (IPS)
- ☐ security information and event management (SIEM)



Le Pentester - Test d'intrusion

Quelle solution ? L'accompagnement

Un test d'intrusion (« **pentest** », en anglais) est une **méthode d'évaluation** (« audit », en anglais) de la sécurité d'un système ou d'un réseau informatique ou un Système d'information; il est réalisé par un testeur, (« pentester », en anglais).

La différence avec un simple **audit de sécurité** est la motivation pour la personne à aller jusqu'à exploiter les failles, montrant ainsi la vulnérabilité. L'exploitation n'a bien sûr pas pour but de détruire ou endommager le système, mais elle permettra de situer le degré du risque lui étant associé.



OWASP
The Open Web Application
Security Project



RootMe
— hacking platform —

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

La réponse aux incidents de sécurité informatique



incident de sécurité



PASSI

PDIS

PRIS

FORENSIC

Gouvernance
Audit Technique



Pôle Architecture



CSIRT



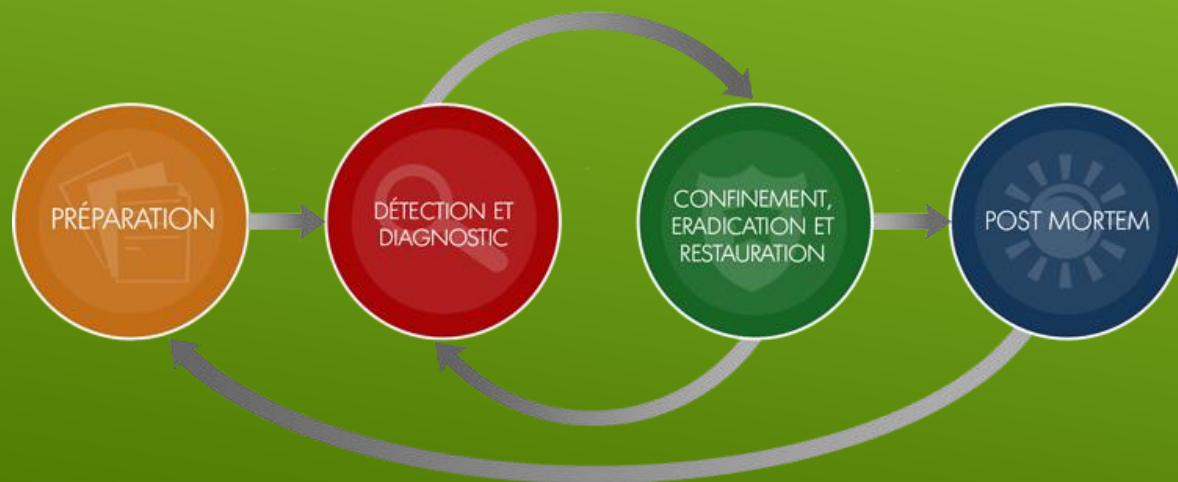
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
PDIS	Prestataire de détection d'incidents de sécurité
PRIS	Prestataire de réponse aux incidents de sécurité

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

La réponse aux incidents de sécurité informatique

Les types de prestations (ANSSI):

- ☐ - la recherche d'indicateurs de compromission IOC;
- ☐ - l'investigation numérique sur périmètre restreint ;
- ☐ - l'investigation numérique sur large périmètre.



Indicateur de compromission est une combinaison d'informations techniques représentatives d'une manifestation de compromission, dont la présence peut être identifiée à partir de l'analyse d'un système, d'un code malveillant ou de traces réseau.

Normes

ISO19011 - chapitre 7.2.3.4
 ISO27035 - Gestion des incidents de sécurité de l'information
 ISO27037 - l'identification, la collecte, l'acquisition et la préservation de preuves numériques

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Le personnel dédié à la RI

Missions et compétences attendues du personnel



La Team RI

Le
responsable
d'équipe
d'analyse



Analyste système



Analyste réseau



Gestion de crise
et communication



Le
responsable
d'équipe
technique



Analyste de codes
malveillants



Juriste





CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

L'expertise en informatique légale

L'EXPERTISE FORENSIC



L'expertise en informatique légale (*forensic*) est une investigation numérique légale qui a pour objet la **collecte de preuves numériques** afin de fournir la capacité à une personne de **soutenir une action en justice** ou de **faire reconnaître un droit**.

L'expertise en informatique légale

La prise en compte d'une situation forensique doit permettre la mise en place d'un processus juridique pour organiser une défense ou faire reconnaître un droit.

Quelles sont les difficultés rencontrées ?

- ☐ Le cadre de la collecte de la preuve numérique,
- ☐ L'accessibilité à la preuve numérique,
- ☐ La garantie de la preuve numérique,
- ☐ L'explicabilité de la preuve numérique.





CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Collecte de preuves

L'EXPERTISE FORENSIC



LE LITIGE ENTRE
PROFESSIONNELS

LE LITIGE
INTERNE

JUSTIFICATION
REGLEMENTAIRE

CADRE D'UNE CYBER
ATTAQUE

APPORTER SON CONCOURS
A LA JUSTICE



Recueil des preuves numériques

L'EXPERTISE FORENSIC

■ Analyse de disque dur :

- Analyse du système d'exploitation
- Analyse du système de fichiers
- Analyse de la navigation sur le réseau Internet
- Etude de logiciels spécifiques en vue d'extraire des documents formatés
- Recherche de points de compromission de la machine analysée

■ Analyse de téléphone :

- Exploitation de boîtier téléphonique
- Exploitation de carte SIM,
- Exploitation de carte amovible
- Exploitation de navigateurs GPS

■ Missions particulières :

- Analyse infrastructure réseau
- Analyse domotique
- Analyse Drone
- Analyse DIY (Do it yourself – Fabrication artisanale)
- Ré échantillonnage de fichiers vidéo (agrandissement, rotation, etc.)
- Extraction de piste audio
- Extraction d'images de fichiers vidéo



Que constate-t-on ?

- **Une mauvaise estimation des risques,**
Une absence de plan de réponse à incident, de gestion de crise et de prise en compte de la réponse à incident dans les PCA,
- **Une destruction des preuves,**
Une absence totale de collecte d'informations avant la crise et la disparition des éléments de preuve pendant de la crise.





CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Objectif ?

- de faire **un gel des lieux numériques** sur un support de données par la fixation des preuves numériques dans le temps,
- de faire une **copie exacte des supports compromis** (copie bit à bit) en préservant le caractère inaltérable de la preuve,
- de **mettre en sécurité les données numériques** lors d'une cyberattaque avant la reprise d'activité,
- de s'assurer que la collecte **des données** à analyser pourra servir de **preuve légale dans le cadre d'un litige**,
- de s'assurer que les données prélevées seront de nature à **démontrer la « bonne foi »** de votre entreprise.

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

La cybersécurité



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Une sensibilisation pourquoi ?



**La sécurité est la
responsabilité
de tous !**

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Parlons Cyber ...

CYBER SÉCURITÉ

La cybersécurité est l'état recherché pour un système d'informations lui permettant de résister à des événements issus du cyberspace susceptibles de compromettre la **disponibilité**, l'**intégrité**, la **confidentialité**, la **non-répudiation** et la **traçabilité** des données stockées, traitées ou transmises.



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Parlons Cyber ...

CYBER DEFENSE

La **cyberdéfense** regroupe l'ensemble des moyens physiques et virtuels mis en place par un pays dans le cadre de la guerre informatique menée dans le cyberspace.



CYBERCRIMINALITÉ

La **cybercriminalité**, regroupe l'ensemble des infractions pénales qui se commettent via les réseaux informatiques, notamment sur le réseau Internet.



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Un monde en *HYPER-CONNEXION*

Ce monde en hyper-connexion cherchant à satisfaire nos besoins mais non sans danger à donner naissance à la cybersécurité.



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Mais qui sont ils ?



Entreprises concurrentes



Etats ennemis ou alliés



Les années 2010

Les années 2000

Geeks



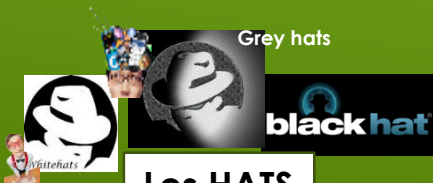
Les réseaux mafieux



*Quel est le visage du Cyber
délinquant aujourd'hui ?*



Escrocs du web



Les HATS



Prédateurs de web

Les menaces sont-elles réelles ?





Les menaces sont-elles réelles ?

Hausse de 32% sur les plaintes pour cybermenaces en France en 2017

Soit 63 500 plaintes en 2017

Les menaces sont-elles réelles ?

Plus inquiétant, le ministère de l'Intérieur cite une étude de Deloitte de janvier 2018 révélant que « **63 % des incidents de sécurité proviennent d'un collaborateur actif au sein des effectifs** ».

Le facteur humain reste encore et toujours le maillon faible dans la sécurité numérique d'une entreprise.

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

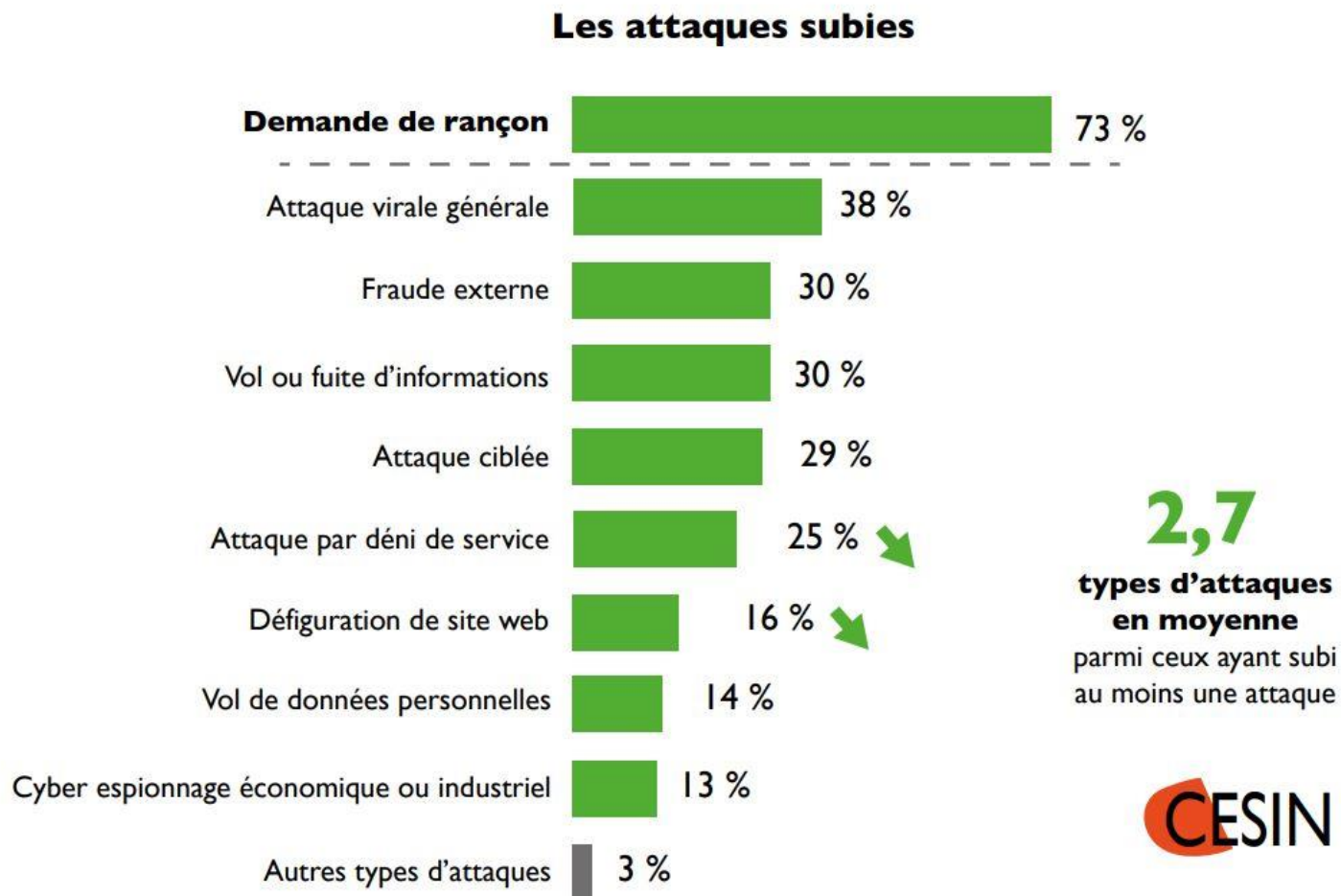
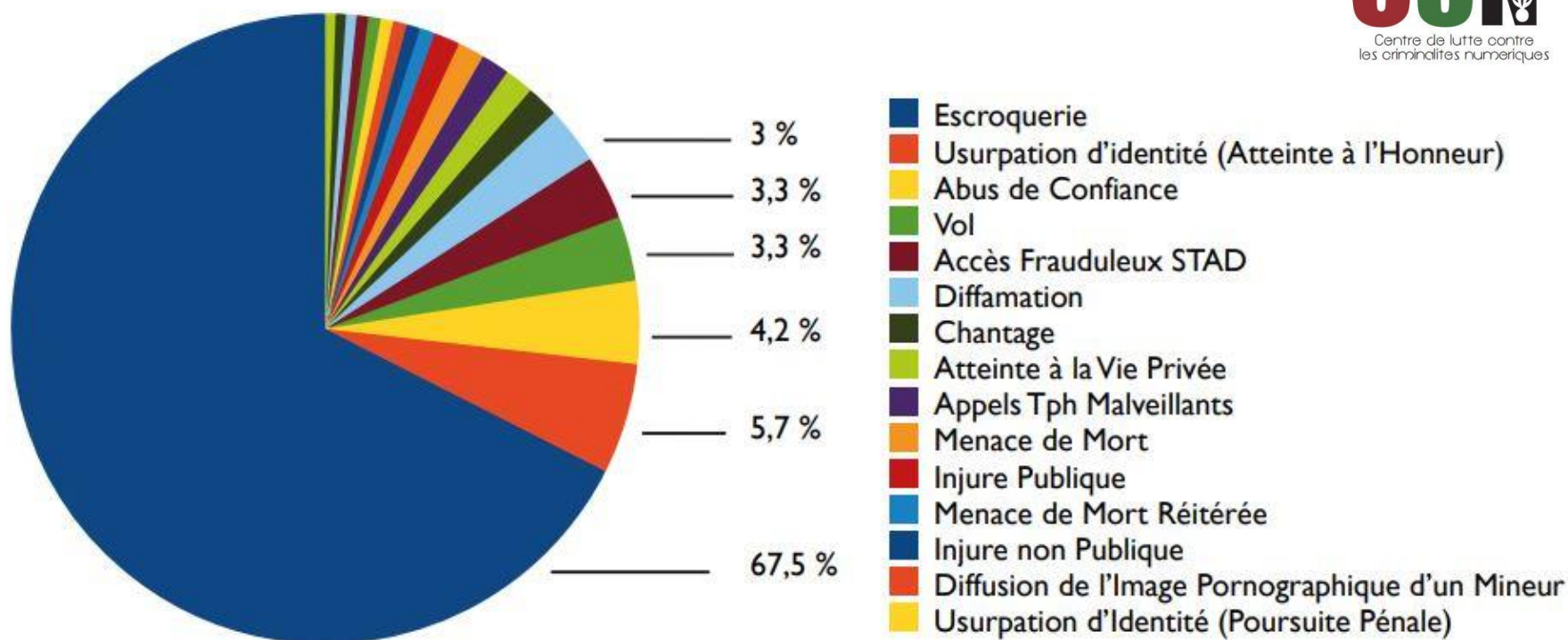


Figure 18 : Type d'attaque subies par les entreprises

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Répartition des infractions cyber les plus représentées par NATINF *



(*) NATINF : Nature infraction



NORSE

ATTACK ORIGINS

COUNTRY	#	PORT	SERVICE TYPE
China	85	8080	http-proxy
United States	43	23	telnet
MDGov	10	445	microsoftrds
Russia	12	3389	win-remote-viewer
Venezuela	11	11211	ssh-tunnel
Japan	9	5000	ssh-tunnel
Taiwan	7	33445	vnc
Vietnam	7	33446	ssh-tunnel

ATTACK TYPES

ATTACK TARGETS

COUNTRY	#
United States	292
MDGov	75
Philippines	30
Cyprus	25
Laos	18
Russia	13
Taiwan	7
Singapore	5
Bulgaria	5

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
17:44:03.382	CHINANET HUBEI PROVINCE NETWORK	116.211.0.90	Wuhan, CN	milgov	http-proxy	8080
17:44:03.392	CHINANET HUBEI PROVINCE NETWORK	116.211.0.90	Wuhan, CN	milgov	http-proxy	8080
17:44:03.401	CHINANET HUBEI PROVINCE NETWORK	116.211.0.90	Wuhan, CN	milgov	http-proxy	8080
17:44:03.409	CHINANET HUBEI PROVINCE NETWORK	116.211.0.90	Wuhan, CN	milgov	http-proxy	8080
17:44:03.427	CHINANET HUBEI PROVINCE NETWORK	116.211.0.90	Wuhan, CN	milgov	http-proxy	8080
17:44:03.436	CHINANET HUBEI PROVINCE NETWORK	116.211.0.90	Wuhan, CN	milgov	http-proxy	8080
17:44:03.479	University of Michigan College of Engineering	141.212.122.88	Ann Arbor, US	Seattle, US	ssh	443
17:44:03.561	CHINANET Yunnan PROVINCE NETWORK	182.246.164.73	Kunming, CN	St. Louis, US	telnet	23
17:44:03.563	Isalady Networks	216.209.233.85	Englewood, US	Englewood, US	ssh-tunnel	1842

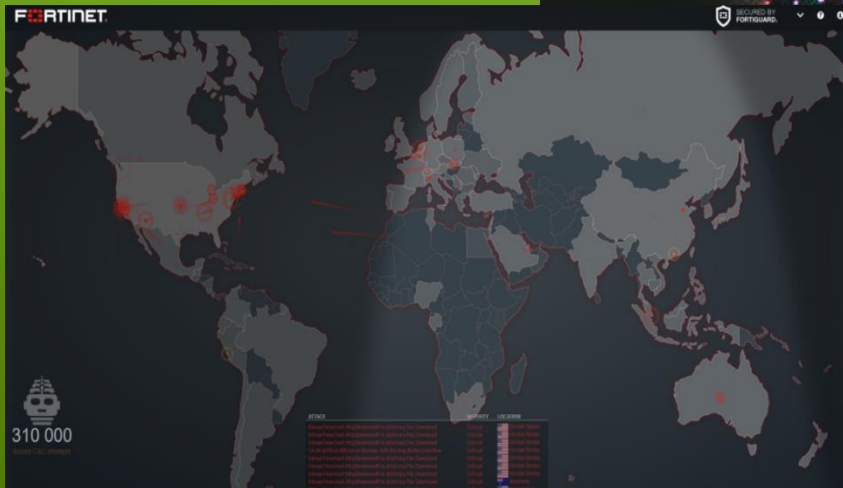
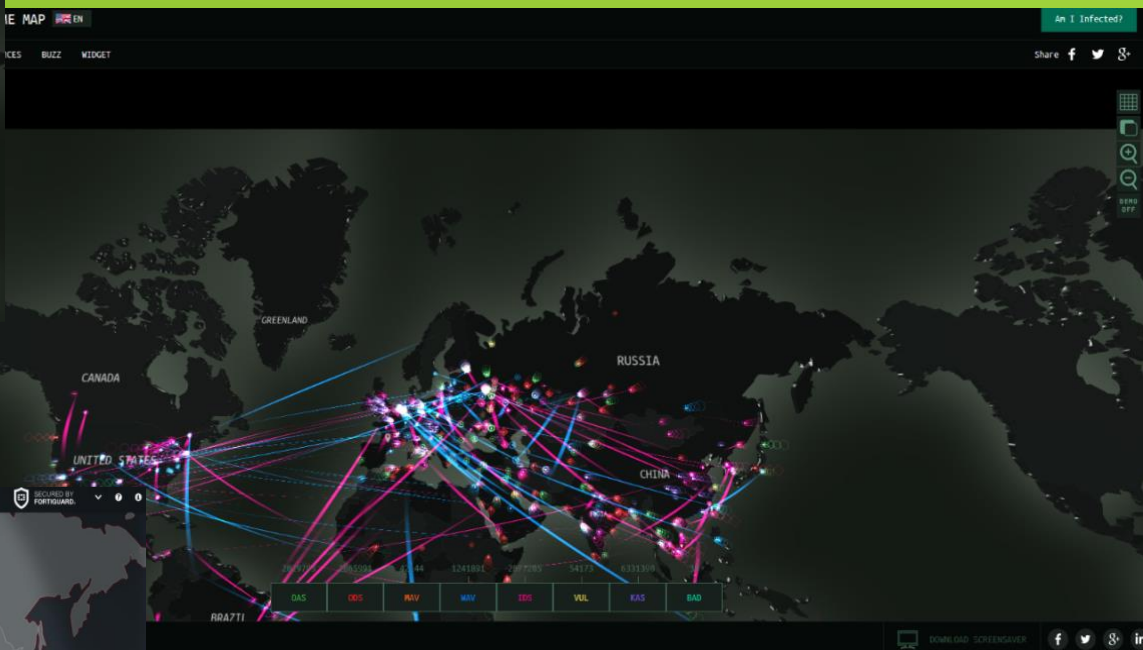
5:42 PM

Jul 30 2015

NEW NORSE MAP

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Un monde en *HYPER-CONNEXION*



SOURCE :

<https://cybermap.kaspersky.com/>

<https://www.fireeye.com/cyber-map/threat-map.html>

<https://threatbutt.com/map/>

<https://threatmap.fortiguard.com/>

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Conséquences ?



Perte de disponibilité



Pertes
financières



Impact sur l'image

Conséquences ?

Cout moyen d'une intrusion
en 2017

**3,62 millions
de dollars**



**35% des utilisateurs
Ont des mots de
passe faible**



**72% des intrusions
liées à des emails frauduleux**



**60% des attaques en 2016
Menées par des
personnes internes**



**Délai de détection de
compromission en 2016**

191 jours



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Un monde en *HYPER-CONNEXION*

Manifeste du Cyberspace

**Vous n'êtes plus à TOULOUSE !
Vous êtes dans le CYBERESPACE !**

4,3 \overline{M}



+ 50 \overline{M}







CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Le mot de passe

**Premier rempart
de la sécurité informatique**



Le mot de passe

Qui compose son mot de passe avec moins 8 caractères (chiffre/lettre/caractère) ?



Qui change ses mots de passe tous les 6 mois ?

Qui utilise une fenêtre de navigation privée dans son navigateur pour faire des achats ?

Qui enregistre ses mots de passe dans son navigateur ?

Qui utilise des conteneurs chiffrés ?

Qui enregistre ses mots de passe dans un document Word ?

Qui utilise plusieurs fois le même mot de passe ?

Qui utilise une messagerie chiffrée avec signature ?

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Construire son mot de passe



Construire son mot de passe



COMMENT RENFORCER MON MOT DE PASSE ?

Une question qui se pose fréquemment est : mais quels critères dois-je employer pour mes mots de passe ? Huit caractères, dix caractères, des chiffres, des majuscules, etc ?

Une première règle à savoir est qu'il est souvent plus efficace d'allonger un mot de passe que de chercher à le rendre plus complexe. Mais pour s'en rendre compte, le mieux est d'utiliser le petit calculateur ci-dessous :

Longueur : caractères. Alphabet :

Un mot de passe avec ces caractéristiques est à peu près équivalent à une clé de bits.

QUELQUES RÉSULTATS TYPIQUES

Type de mot de passe	Taille de clé équivalente	Force	Commentaire
Mot de passe de 8 caractères dans un alphabet de 70 symboles	49	Très faible	Taille usuelle
Mot de passe de 10 caractères dans un alphabet de 90 symboles	65	Faible	
Mot de passe de 12 caractères dans un alphabet de 90 symboles	78	Faible	Taille minimale recommandée par l'ANSSI pour des mots de passe ergonomiques ou utilisés de façon locale.
Mot de passe de 16 caractères dans un alphabet de 36 symboles	82	Moyen	Taille recommandée par l'ANSSI pour des mots de passe plus sûrs.
Mot de passe de 16 caractères dans un alphabet de 90 symboles	104	Fort	
Mot de passe de 20 caractères dans un alphabet de 90 symboles	130	Fort	Force équivalente à la plus petite taille de clé de l'algorithme de chiffrement standard AES (128 bits).

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Construire son mot de passe



Oui mais tout cela on connaît !

Mais alors pourquoi continuer à utiliser des protocoles comme FTP ou TELNET ?



tcpdump



- capturer les mots de passe FTP :



```
tcpdump -XX -s0 -i eth0 tcp and port 21 | grep -A1 PASS
```

Restons humble face aux cybermenaces

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Le mot de passe des comptes utilisateurs





CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Le mot de passe des comptes utilisateurs

Campagne Hack Academy - JENNY (2015)



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Le mot de passe

Je n'écirai pas mon mot de passe sur un post-it
Je n'écirai pas mon mot de passe sur un post-it
Je n'écirai pas mon mot de passe sur un post-it
Je n'écirai pas mon mot de passe sur un post-it
Je n'écirai pas mon mot de passe sur un post-it
Je n'écirai pas mon mot de passe sur un post
Je n'écirai pas mon mot de passe sur un po
Je n'écirai pas mon mot de passe sur un post-it
Je n'écirai pas mon mot de passe sur un post-it
Je n'écirai pas mon mot de passe sur

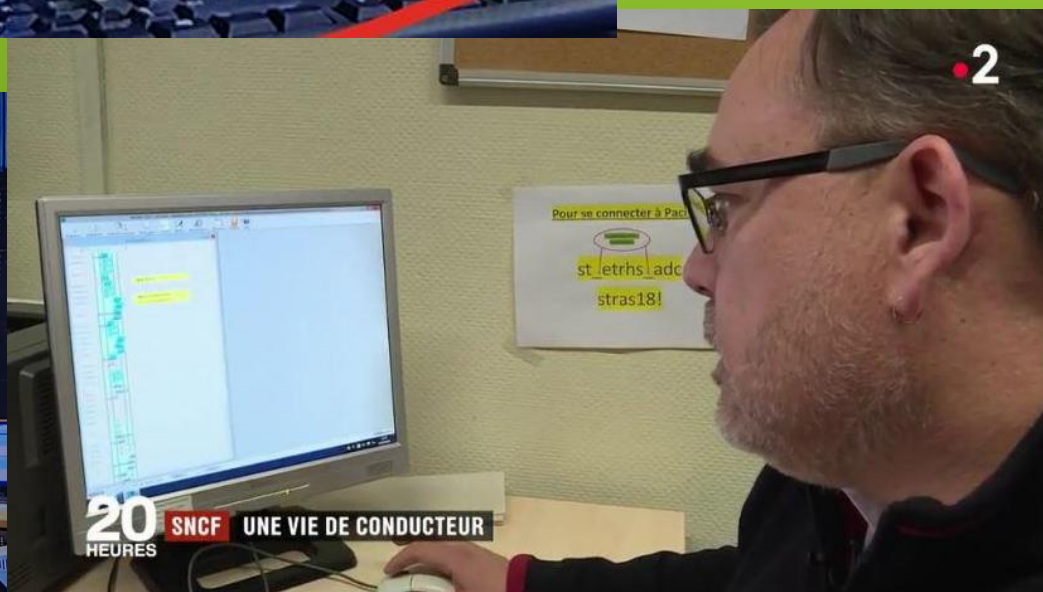
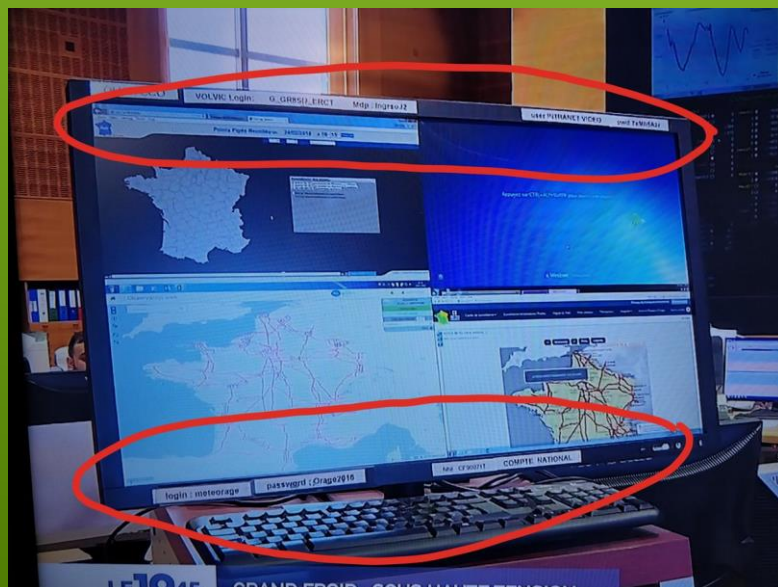
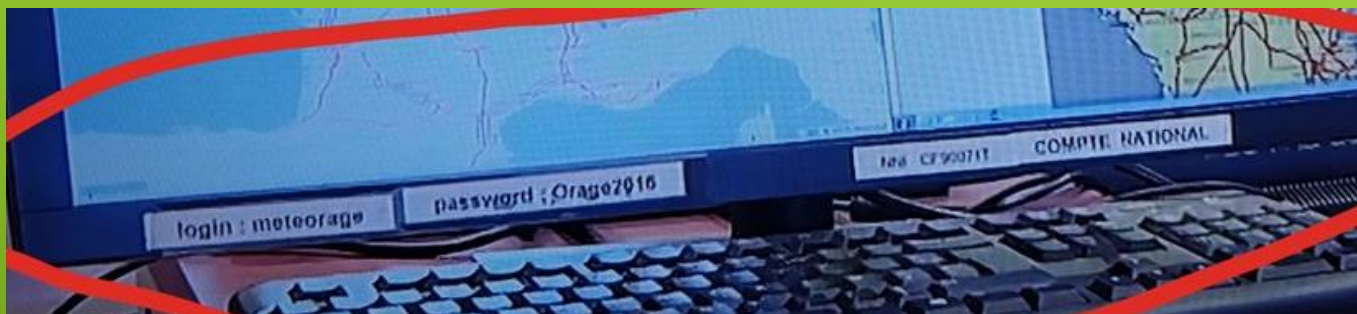


Premier
rempart de la
sécurité
informatique



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

NE PAS DIVULGUER son mot de passe



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

NE PAS DIVULGUER son mot de passe





CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

NE PAS DIVULGUER son mot de passe

La SNCB Europe divulgue x La SNCB vous emmerde x Piratage: Les mots de pas x Un pirate informatique de x

www.tdg.ch/monde/mots-tv5monde-diffuses-13heures-france2/story/24338918

Les mots de passe de TV5Monde dévoilés

Piratage
des mots

YOUTUBE
Mdp :
lemotdepassedeyoutu
be

13 HEURES **DAVID DELOS**
JOURNALISTE TV5 MONDE

Sur le mur, derrière le journaliste, on aperçoit clairement une feuille de papier avec le mot Youtube et sous lequel figurent les mots de passe pour accéder au compte de la chaîne.
Image: DR

Cyberattaque La chaîne francophone TV5Monde, piratée mercredi soir par des hackers se réclamant de l'Etat islamique, peut à nouveau diffuser ses programmes originaux. Plus



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Le vol de mots de passe



LinkedIn
167 millions de
mots de passe
volés

32 millions de
mots de passe
volés



272 millions
d'e-mails et
de mots de
passe



500 millions/1 milliard
de mots de passe volés



Dropbox
60 millions
de comptes

MySpace
427 millions de
mots de passe
volés



5 millions de
mots de passe
du service d'e-
mails de Google



Dailymotion
87 millions
de comptes



57 millions de
comptes Uber



Le vol de mots de passe, un sport international

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Le vol de mots de passe

Gaming Collection/3,6кк Заточка под PSN.txt

```
69063: [redacted]@equipement.gouv.fr:nicolas
69190: [redacted]@equipement.gouv.fr:NYZU95
69611: [redacted]@dircom.finances.gouv.fr:BAVE85
69731: [redacted]@equipement-agriculture.gouv.fr:vatbey09
79452: [redacted]@agriculture.gouv.fr:madrono
84261: [redacted]@dd-38.travail.gouv.fr:VATU71
84322: [redacted]@interieur.gouv.fr:lucche
90421: [redacted]@education.gouv.fr:truffe
96843: [redacted]@orne.pref.gouv.fr:573200
11410: [redacted]@developpement-durable.gouv.fr:QWERTY
116345: [redacted]@developpement-durable.gouv.fr:merde99
118697: [redacted]@cher.gouv.fr:NADOUR
125599: [redacted]@seine-maritime.gouv.fr:olifin
135310: [redacted]@ardennes.gouv.fr:luc877
138376: [redacted]@douane.finances.gouv.fr:concorde
138907: [redacted]@correze.gouv.fr:Christophe.1
268617: [redacted]@jeunesse-sports.gouv.fr:ALT06162
295494: [redacted]@douane.finances.gouv.fr:kimiak974
682418: [redacted]@jeunesse-sports.gouv.fr:ALEXBO
```

VIP Collection/VIP раздел слитый (43).txt

```
135670: [redacted]@sante.gouv.fr:maddalen
137673: [redacted]@developpement-durable.gouv.fr:entreprise
203164: [redacted]@sante.gouv.fr:tnerual
249034: [redacted]@culture.gouv.fr:infoy
303556: [redacted]@diplomatie.gouv.fr:vas
303923: [redacted]@diplomatie.gouv.fr:vas
307780: [redacted]@diplomatie.gouv.fr:vas
308042: [redacted]@diplomatie.gouv.fr:vas
387893: [redacted]@developpement-durable.gouv.fr:leonberg
400706: [redacted]@developpement-durable.gouv.fr:lanka
452365: [redacted]@sante.gouv.fr:195016
491932: [redacted]@aviation-civile.gouv.fr:DERF
609678: [redacted]@drjcs.gouv.fr:bateaux
621265: [redacted]@interieur.gouv.fr:4223
```

Trading Collection/600к.txt

```
61275: [redacted]@cp.finances.gouv.fr:oiseau
335604: [redacted]@cepc-mailly.terre.defense.gouv.fr:dauphins
```

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Le vol de mots de passe



Un mot de passe efficace

«dadada»



"123456",
"password",
"abcdef"

Les hackers ont réussi à trouver le mot de passe dans une fuite de données provenant de LinkedIn.

Les comptes Twitter et Pinterest de Mark Zuckerberg ont été piratés.

Instagram piraté par un garçon de 10 ans qui empoche au passage 10 000 dollars

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Le vol de mots de passe



Uber a caché le vol de données de 50 millions de clients et 7 millions de chauffeurs

Vol de données en octobre 2016 assumé le 21 novembre 2017 et à payer la somme de 100 000 dollars aux hackers pour qu'ils gardent le silence.

<https://www.usine-digitale.fr/article/uber-a-cache-le-vol-de-donnees-de-50-millions-de-clients-et-7-millions-de-chauffeurs.N617393>



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Le vol de mots de passe

Votre adresse mail est-elle mentionné sur des sites qui ont été compromis ?

<https://haveibeenpwned.com/>

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

fabrice.crasnier@wanadoo.fr

pwned?

Oh no — pwned!

Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)

Le vol de mots de passe

Votre adresse mail est-elle mentionné sur des sites qui ont été compromis ?

<https://haveibeenpwned.com/>

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Domino's: In June 2014, Domino's Pizza in France and Belgium was hacked by a group going by the name "Rex Mundi" and their customer data held to ransom. Domino's refused to pay the ransom and six months later, the attackers released the data along with troves of other hacked accounts. Amongst the customer data was passwords stored with a weak MD5 hashing algorithm and no salt.

Compromised data: Email addresses, Names, Passwords, Phone numbers, Physical addresses



Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

Le vol de mots de passe



Se connecter en tant que **Fabrice Crasnier**

fabrice.crasnier@wanadoo.fr · Ce n'est pas vous ?

Vous avez saisi un ancien mot de passe

Votre mot de passe a été modifié à partir de cet ordinateur il y a environ 6 mois

[Demander un nouveau mot de passe.](#)

Connexion

Récupérer votre compte

[S'inscrire sur Facebook](#)

facebook [Inscription](#)

Piratage de Facebook:
**5 millions de comptes
concernés en Europe**

Publié le 02/10/2018 à 12:22

Au total, Facebook a remis à zéro les «token d'accès» de 90 millions de comptes, par mesure de précaution.

**Une amende potentielle de
1,6 milliard de dollars**

CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Le vol de mots de passe

Attaques
non techniques

Premier rempart de la
sécurité informatique

1. Attitude de l'humain
2. Ingénierie sociale
3. Phishing
4. Espionnage humain



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Le vol de mots de passe

Attaques techniques

1. Camera de surveillance
2. Attaques de sites (autorités d'authentification)
3. Attaques par sniffing
4. Attaques par sniffing sur protocole https
5. Attaques "Man in the Middle"
6. Attaques "Man in the Middle" Authentification frauduleuse
7. Attaques par keylogger
8. Attaques par keylogger acoustiques
9. Attaques par keylogger électromagnétiques
10. Attaque en "Force brute"
11. Attaque en "Dictionnaire"
12. Attaque "Tables Arc en ciel" (Rainbow tables)

Premier rempart de la sécurité informatique

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^3)

m – Million (1,000,000 or 10^6)

bn – Billion (1,000,000,000 or 10^9)

tn – Trillion (1,000,000,000,000 or 10^{12})



qd – Quadrillion (1,000,000,000,000,000 or 10^{15})

qt – Quintillion (1,000,000,000,000,000,000 or 10^{18})

L'usurpation d'identité

Nintendo France : toutes les données du SAV volées par des hackers

Nintendo France annonce avoir été victime d'un piratage de son SAV. Toutes les données client ont été dérobées par des hackers, et ces derniers envoient de fausses propositions de remboursement afin de s'emparer des coordonnées bancaires des victimes.

 Bastien L  31 mai 2018  Sécurité  Ecrire un commentaire

A l'heure où la confidentialité des données personnelles préoccupe de plus en plus les consommateurs, Nintendo France s'offre un très mauvais coup de pub. Sur Twitter, l'entreprise annonce que son SAV a été piraté et que les hackers sont parvenus à **s'emparer de toutes les données client** stockées sur les serveurs.

Adresses mail et postales, noms, prénoms et numéros de téléphone : toutes les coordonnées de contact des milliers de clients enregistrés dans la base de données du SAV ont été récupérées. Pire encore, les pirates utilisent ces informations pour **contacter toutes les victimes en se faisant passer pour Nintendo**.



L'usurpation d'identité

Nintendo France : les hackers tentent de récupérer les informations bancaires des clients



noreply@nintendo-sav.fr ▾

Votre demande de remboursement nintendo-sav

À :

Répondre à : noreply@nintendo-sav.fr



Bonjour M.

Votre demande de remboursement a bien été prise en compte.
Pour finaliser votre demande merci de cliquer sur le lien ci-dessous :

[Lien Remboursement](#)

Récapitulatif du remboursement

Email :
Nom :
Prenom :
Adresse :
Code Postal :
Montant : 97 EUR

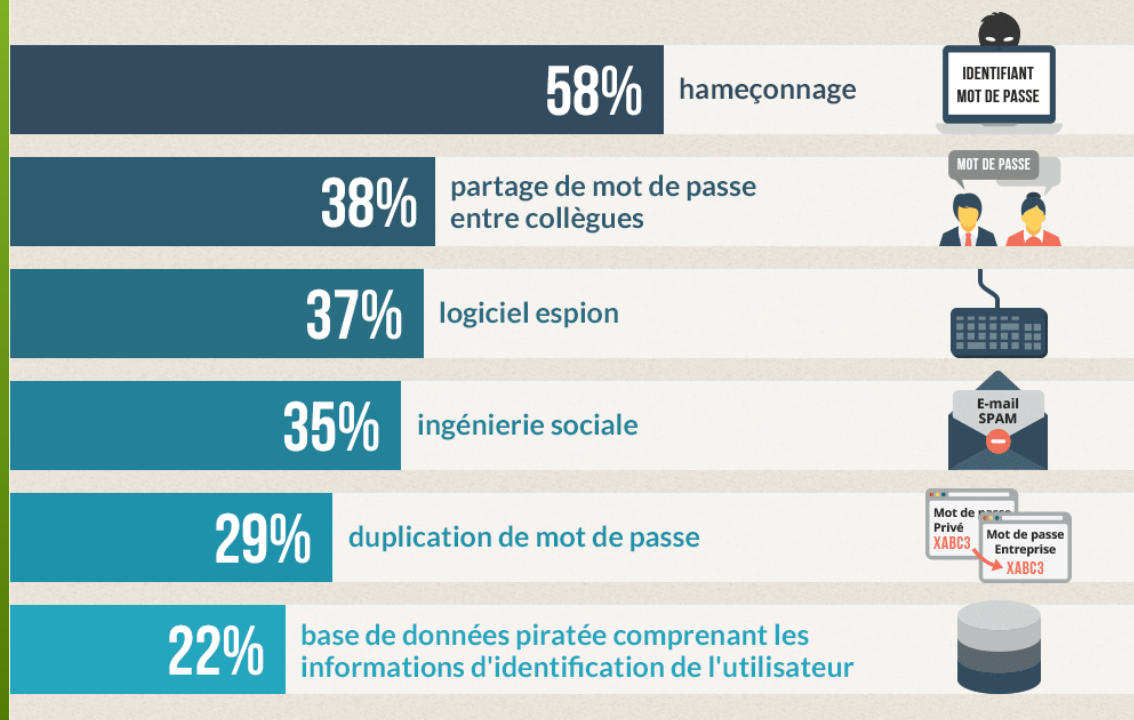
Nous vous remercions de votre confiance .

Pour toute information, merci de nous contacter à info_remboursement@nintendo-sav.fr.

L'usurpation d'identité

COMMENT LES IDENTIFIANTS DE CONNEXION — SONT FACILEMENT COMPROMIS —

Ce sont vos utilisateurs finaux qui mettent souvent votre réseau en danger.



Quelles
sont les
conséquences
?



CYBERSÉCURITÉ, CERNER LES MENACES ET SE PROTÉGER

Merci de votre attention

Fabrice CRASNIER

Consultant expert senior

Responsable du pôle FORENSIC

Laboratoire SCASSI-CYBER

Tel : 06.24.49.39.20

Courriel : fabrice.crasnier@scassi.com



Société SCASSI

Bâtiment AGORA 1

209 Rue Jean Bart

31670 Labège, France

tél : +33 (0)5 61 17 08 54

fax : +33 (0)5 61 54 50 02

courriel : contact@scassi.com



Doctorant en intelligence artificielle

Ecole doctorale MITT Mathématiques Informatique

Télécommunications de Toulouse.

Laboratoire IRIT - Equipe SMAC

Systèmes Multi-Agents Coopératifs

Avenue de l'étudiant, 31400 Toulouse

Tel : 06.24.49.39.20

Courriel : fabrice.crasnier@irit.fr



neccampus

