



Sécurité Informatique

ITAHRIOUAN Zakaria

z.itahriouan@umi.ac.ma



Sécurité Informatique

Chapitre 1: Notions fondamentales de sécurité

ITAHRIOUAN Zakaria

z.itahriouan@umi.ac.ma

1 - Introduction:

Le terme « système d'information » désigne tout système destiné à traiter l'information.

Les systèmes d'information s'appuient en règle général sur des systèmes informatiques pour leur mise en œuvre.

De tels systèmes se prêtent à des menaces de types diverses concernant:

- ▶ l'intégrité de l'information.
- ▶ la confidentialité de l'information.
- ▶ La disponibilité du système.
- ▶ ...

1 - Introduction:

Certaines de ces menaces peuvent aussi, indirectement, causer d'importants **dommages financiers**:

- ▶ 2,6 milliards de dollars ont été avancées suite à des dommages causés par des programmes malveillants comme le ver Code Red (serveur IIS).
- ▶ D'autres dommages à cause du vol des numéros de cartes de crédit
- ▶ ...

Outre les aspects financiers:

- ▶ des bris de sécurité informatique peuvent causer du **tort à la vie privée**
 - ▶ diffusant des informations confidentielles sur elle (entre autres ses coordonnées postales ou bancaires).

1 - Introduction:

certaines menaces peuvent **nuire à l'image** même du propriétaire du système d'information:

- ▶ Defacing :une refonte d'un site web.
 - ▶ diffuser de fausses informations sur son propriétaire (désinformation).
- ▶ Mettre en évidence des failles de sécurité sur un serveur web.

2- contexte et définitions

Qu'est-ce qu'un système d'information ?

- ▶ Ensemble organisé de ressources...
personnes, données, activités, ressources matérielles, etc.
- ▶ ...qui interagissent entre elles pour acquérir, stocker, transformer, diffuser, exploiter et gérer les informations en fonction des objectifs d'une organisation.

2- contexte et définitions

7

Que comprend un SI ?

- ▶ Matériel informatique.
- ▶ Périphériques.
- ▶ Logiciels.
- ▶ Documentation.
- ▶ Moyens de transmission.
- ▶ Des procédures et des règles de fonctionnement organisationnel.
- ▶ Ressources humaines qui les mettent en œuvre.

2- contexte et définitions

La sécurité des systèmes informatiques

- ▶ Le système informatique porte l'essentiel du système d'information.
- ▶ Ils sont devenus la cible de ceux qui convoitent l'information.
- ▶ Assurer la sécurité de l'information implique d'assurer la sécurité des systèmes informatiques.

2- contexte et définitions

Objectifs de la sécurité informatique

► Confidentialité

Une information doit être reçue uniquement par le(s) destinataire(s) prévu(s) (et pas par d'autres).

► Intégrité

Propriété assurant qu'une information ou un traitement n'a pas été modifié ou détruit de façon non autorisée.

► Disponibilité

Aptitude d'un composant ou d'un système à être en état de marche à un instant donné.

2- contexte et définitions

10

Objectifs de la sécurité informatique

► Authentification

Une information doit être acheminée exactement au destinataire souhaité.

► Non répudiation

Impossibilité de nier la participation au traitement d'une information.

► Imputabilité

Possibilité de faire porter la responsabilité d'une infraction à une personne.

2- contexte et définitions

11

Evolution des risques

- ▶ Croissance d'Internet et des appareils connectés.
- ▶ Croissance des attaques (vulgarisation des connaissances).
- ▶ Croissance des outils.
- ▶ Failles des technologies.
- ▶ Failles des configurations.
- ▶ Failles des politiques de sécurité.

2- contexte et définitions

12

Qui sont les pirates ?

- Peut être n'importe qui avec l'évolution et la vulgarisation des connaissances.
- Beaucoup d'outils sont disponibles sur Internet.

► Vocabulaire:

- « script kiddies »
- « hacktiviste »
- « hackers »:
 - « white hats »
 - « black hats »
 - « grey hats »
 - « cracker »
 - « carder »
 - « phreaker »



2- contexte et définitions

13

Motivations des attaques

- ▶ Vol d'informations
- ▶ Cupidité
- ▶ Modifications d'informations
- ▶ Vengeance/rancune
- ▶ Politique/religion
- ▶ Défis intellectuels
- ▶ ...

2- contexte et définitions

14

Cible des pirates

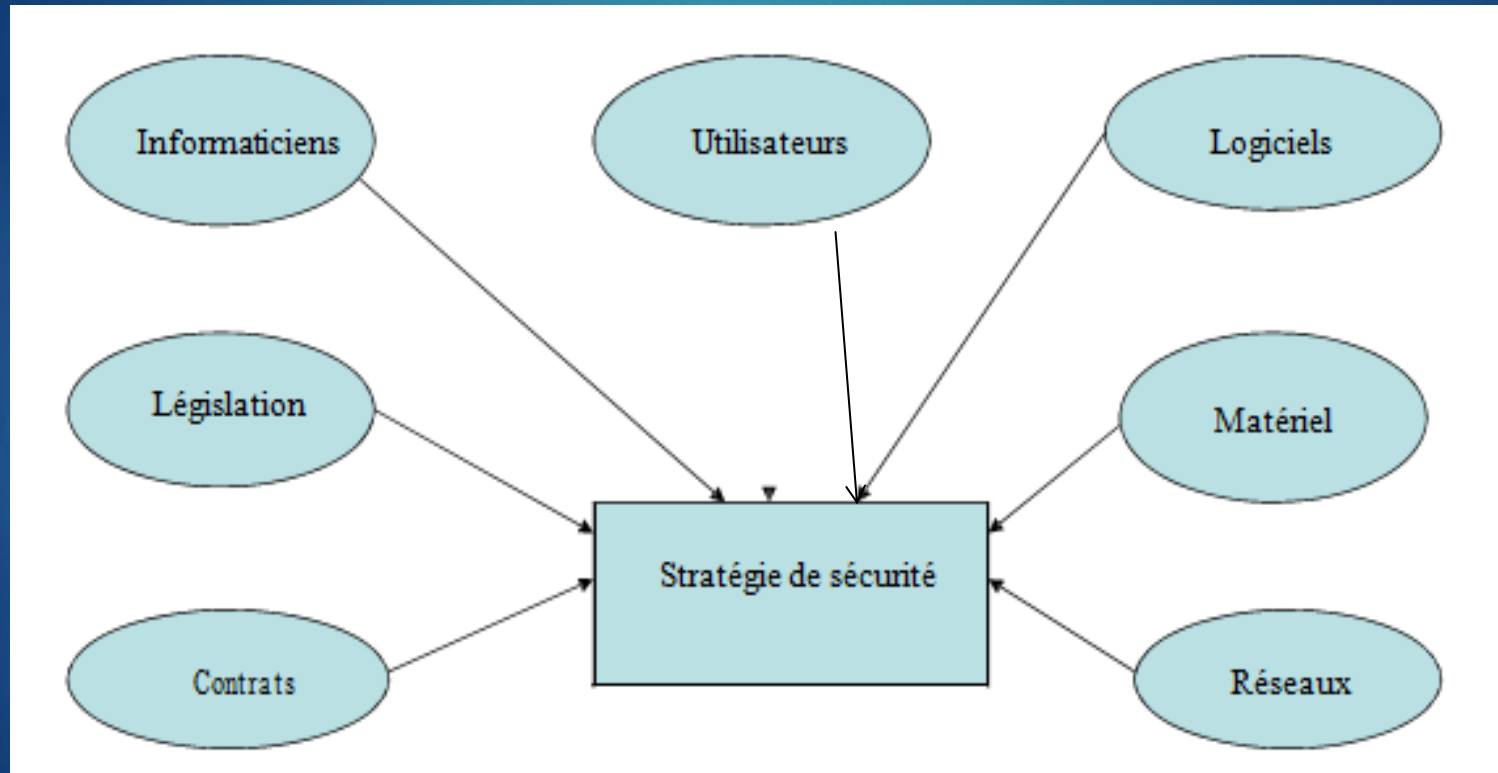
- ▶ Les états
- ▶ Serveurs militaires
- ▶ Banques
- ▶ Universités
- ▶ Tout le monde

2- contexte et définitions

15

La sécurité : une nécessité

Sécurité Informatique



2- contexte et définitions

16

Niveaux de sécurisation

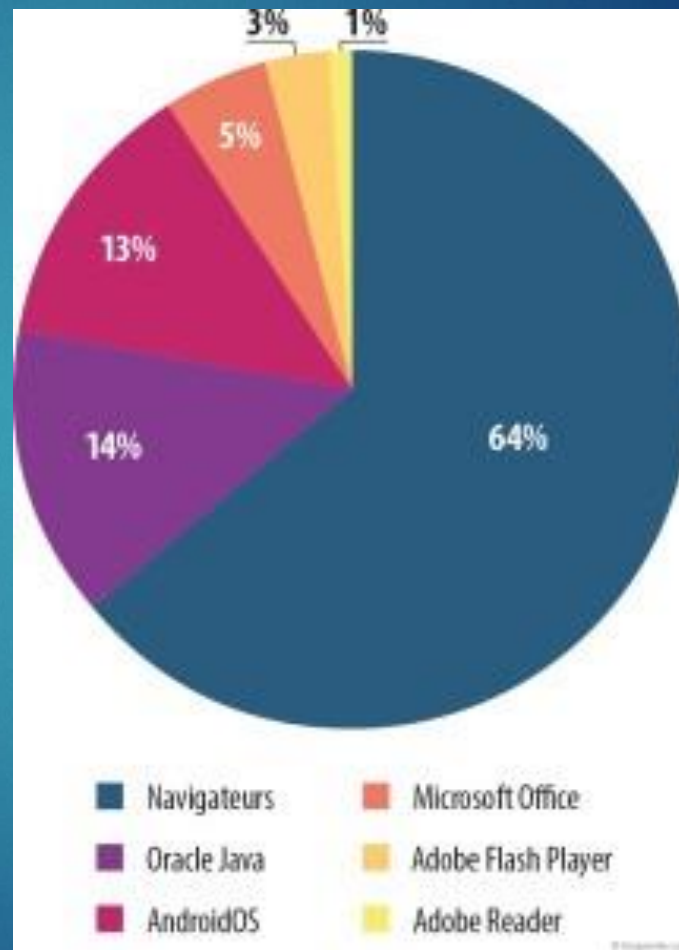
- ▶ Sensibilisation des utilisateurs aux problèmes de sécurité.
- ▶ Sécurisation des données, des applications, des systèmes d'exploitation.
- ▶ Sécurisation des réseaux.
- ▶ Sécurisation physique du matériel et des accès.

3- Statistiques:

17

Répartition, par type d'application ciblée, des codes d'exploitation utilisés par les individus malveillants dans les attaques, 2021

[kaspersky labs, 2021]

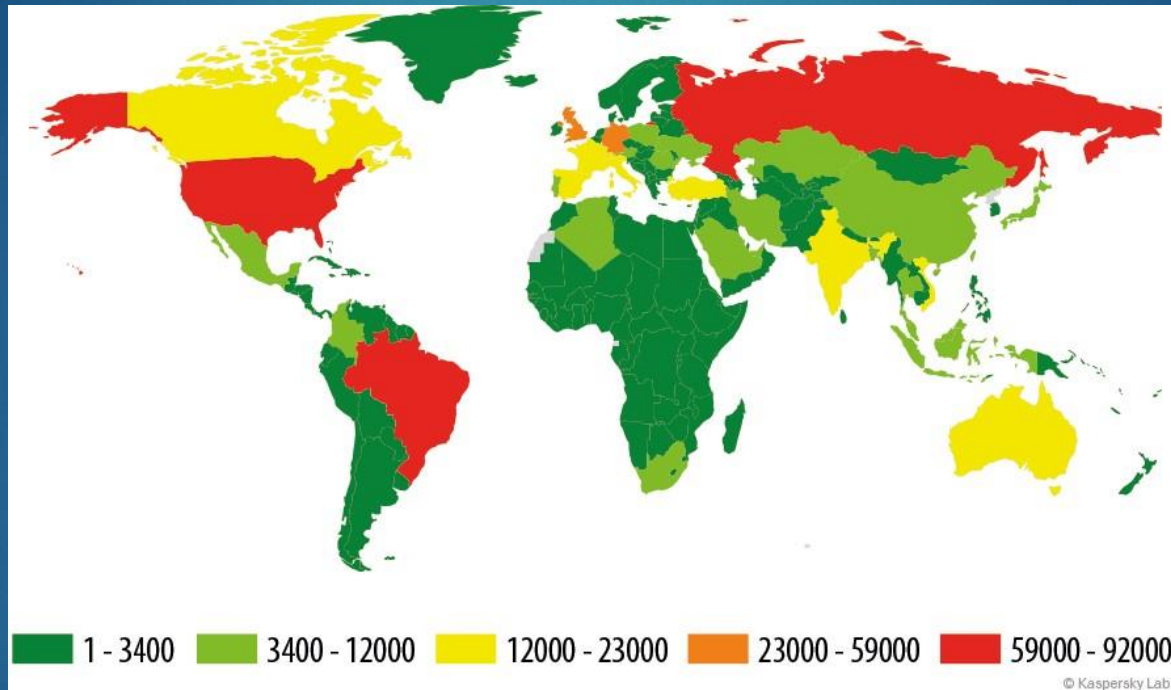


3- Statistiques:

18

Secteur Bancaire

- augmentation du nombre d'attaques de malwares financiers.
- explosion du nombre d'attaques de ce genre en mars 2021.



Répartition géographique des attaques
[kaspersky labs, 2021]

3- Statistiques:

19

Secteur Bancaire

Top 10 des pays selon le nombre d'utilisateurs attaqués:

Sécurité Informatique

	Pays	Nombre d'utilisateurs attaqués
1	Brésil	91 893
2	Russie	85 828
3	États-Unis	66 699
4	Allemagne	51 670
5	Royaume-Uni	25 269
6	Inde	22 085
7	Turquie	21 397
8	Australie	18 997
9	Italie	17 663
10	Espagne	17 416

[kaspersky labs, 2021]

3- Statistiques:

Secteur Bancaire

Top 10 des familles de malwares utilisés dans le cadre d'attaques contre les utilisateurs de services de banque électronique 2021 (sur la base du nombre d'utilisateurs attaqués) :

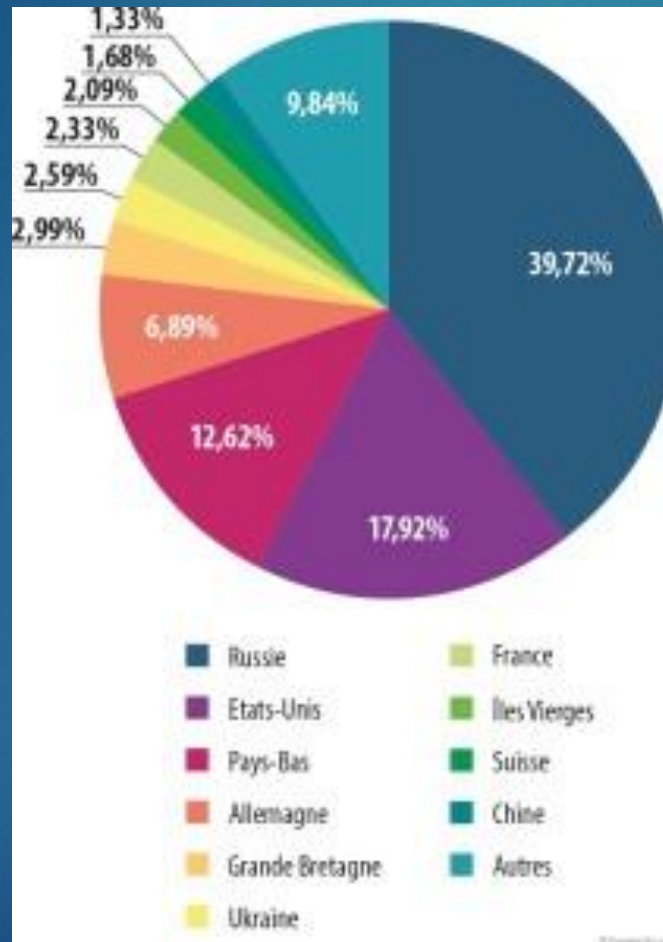
Nom	Nombre de notifications	Nombre d'utilisateurs attaqués
Trojan-Downloader.Win32.Upatre	3 127 365	349 574
Trojan-Spy.Win32.Zbot	865 873	182 966
Trojan-Banker.Win32.ChePro	355 735	91 809
Trojan-Banker.Win32.Banbra	35 182	16 363
Trojan.Win32.Tinba	94 972	15 719
Trojan-Banker.Win32.Agent	44 640	12 893
Trojan-Banker.Win32.Shiotob	60 868	12 283
Trojan-Banker.Win32.Banker	39 728	12 110
Trojan-Spy.Win32.SpyEyes	57 418	9 168
Backdoor.Win32.Papras	56 273	3 062

[kaspersky labs, 2021]

3- Statistiques:

21

Pays source des attaques Internet :



[kaspersky labs, 2021]

3- Statistiques:

22

Pays dont les internautes ont été les plus exposés au risque d'infection via Internet

Sécurité Informatique

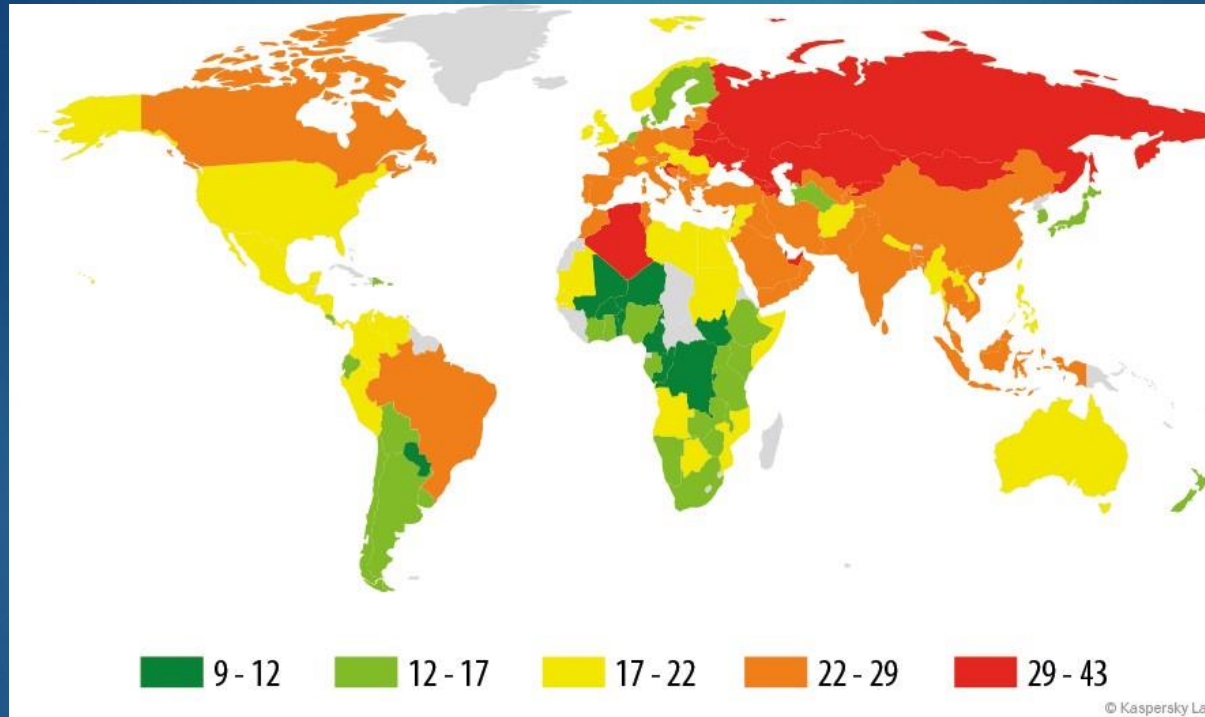
	Pays*	% d'utilisateurs uniques attaqués**
1	Kazakhstan	42,37%
2	Russie	41,48%
3	Azerbaïdjan	38,43%
4	Ukraine	37,03%
5	Croatie	37,00%
6	Arménie	35,74%
7	Mongolie	33,54%
8	Moldavie, République de	33,47%
9	Biélorussie	33,36%
10	Kirghizstan	32,20%
11	Algérie	32,12%
12	Qatar	31,15%
13	Géorgie	30,69%
14	Emirats arabes unis	29,36%
15	Lettonie	28,69%
16	Tadjikistan	28,36%
17	Bosnie et la Herzégovine	28,00%
18	Grèce	27,55%
19	Tunisie	27,54%
20	Bulgarie	27,44%

[kaspersky labs, 2021]

3- Statistiques:

23

les pays les plus sûrs en terme de navigation sur Internet:



Sécurité Informatique

En moyenne, 26,3% des ordinateurs des Internautes à travers le monde avaient été exposés au moins une fois à une attaque sur Internet.

[kaspersky labs, 2021]