ISOC MALI

Accès en ligne et utilisation de l’Internet

Atténuer les menaces sécuritaires et les vulnérabilités

#ShapeTomorrow

Abdrahamane Samba SIDIBE
samba@sidibe.org

Internet est partout !

Pour les uns, c’est un nouveau monde merveilleux qui va changer notre vie.
Pour les autres, c’est une calamité mondialiste qui menace notre culture et nos emplois.

Quoi qu’il en soit, les services accessibles sur Internet ne cessent de se multiplier : partout, à la télévision, dans les publicités sur les murs, dans les journaux, les entreprises de toutes natures indiquent leur adresse sur Internet en nous invitant à nous connecter.

Tous les jours, les sites de ventes sont de plus en plus nombreux.
Les partis politiques présentent leur programme. Les organisations de toutes sortes décrivent leurs objectifs et leur fonctionnement. Une bonne connaissance d’Internet est souvent même une condition de recrutement.

Internet est une réalité incontournable de la vie quotidienne et personne ne peut y rester indifférent.

Le réseau est totalement mondial : il est accessible dans tous les pays.

Internet est souvent désigné sous le terme WEB qui signifie toile d'araignée : en effet Internet se répand sur la terre entière comme une toile d'araignée. Internet est appelé aussi la Toile. Les initiales WWW, souvent utilisées signifient « world wide web » soit la toile d'araignée mondiale.
Internet est un outil qu'il faut apprendre à dominer.

Il est indispensable d'en avoir une connaissance suffisante pour l'utiliser et bénéficier de ses ressources.

Les gouvernements incitent à son développement et à la généralisation de son utilisation.

Pour bien comprendre Internet, il est nécessaire d'avoir quelques connaissances de ce qui l'a rendu possible :
- la révolution numérique,
- l'émergence de l'outil informatique et les réseaux.

La révolution numérique

L'expression révolution numérique désigne l'introduction progressive mais massive de la technologie numérique dans tous les domaines.

L'arrivée de la révolution numérique peut être considérée comme une évolution technique extrêmement rapide. Elle est directement associée à la naissance puis au développement de l'informatique, c'est-à-dire au fait que toute information (caractère d'imprimerie, son, forme, couleur, mot, texte, photographie, film, musique...) peut être numérisée puis stockée, modifiée, éditée, au moyen de toutes sortes appareils informatiques et transmises par l'intermédiaire du réseau informatique.

L'informatique en général peut se définir comme la science du traitement de l'information, élément de connaissance. Il s'agit d'un domaine d'activité scientifique, technique et industriel concernant le traitement automatique de l'information par des machines : des systèmes embarqués, des ordinateurs, des robots, des automates, etc. L'informatique couvre le secteur d'activité des technologies de l'information et de la communication.

Présentation d’internet, de ses composants, de ses principes de fonctionnement

Le réseau informatique permet d'échanger de l'information à une très grande vitesse dans le monde entier entre des millions de personnes en utilisant plusieurs types de distribution. La messagerie est la première application qui est apparue sur le réseau.
Des millions de messages sont échangés chaque jour sur le réseau entre individus. Des millions de pages sont proposées à la lecture de l'internaute par les serveurs d'informations. Il existe aussi d'innombrables listes de distributions et de groupes de discussion sur lesquels il est possible d'obtenir des informations sur toutes sortes de sujets.

Le réseau permet le partage de ressources. Vous pouvez mettre à disposition d'autres utilisateurs des sons, des images, des documents que vous avez créés et qui sont stockés sur votre micro-ordinateur. Le partage peut être soumis à des conditions d'accès comme par exemple la fourniture d'un mot de passe.

Internet est un réseau qui présente des points communs avec le réseau téléphonique.
Il transporte des données et de la voix. Il met en communication des terminaux qui ont une adresse individuelle qui ressemble au numéro de téléphone. Il vous permet de communiquer avec des interlocuteurs aux quatre coins du monde à travers les frontières et les océans avec la même facilité qu'avec un correspondant local et surtout au même prix. Ce sont les fournisseurs d'accès et les organismes de télécommunications qui gèrent le réseau Internet.

Internet n'est pas un réseau centralisé : il n'y a pas quelque part un gros ordinateur qui gère tout. Même si une partie du réseau s'arrête, tout le reste continue de fonctionner. Les documents qui décrivent tous les protocoles fondamentaux sont publics et consultables sur Internet. Internet est une association ouverte de milliers de réseaux et de millions d'ordinateurs qui se parlent entre eux pour partager de l'information. Sur Internet, les liaisons principales traitent la majeure partie du trafic.

Un réseau est constitué de trois composants de base :
- les moyens qui permettent la communication et le transfert d'informations entre les dispositifs
- les serveurs qui fournissent des services sur le réseau
- les dispositifs terminaux comme votre micro-ordinateur, votre tablette, votre téléphone qui vous permettent d'accéder aux services offerts sur le réseau

Lorsque vous vous connectez à Internet, vous ouvrez votre réseau au monde entier. Internet est plein de gens qui savent comment s'infiltrer dans votre système à travers une connexion Internet.

Aucune institution, aucun gouvernement, aucune entreprise ne contrôle seul, Internet : Internet est véritablement une entreprise collective coopérative. Beaucoup d'institutions et de société collabore au bon fonctionnement d'Internet. Beaucoup de gouvernements veulent légiférer autour d'Internet ; mais malgré leur souhait d'imposer le contrôle absolu de toute information, une sorte de censure, il reste un peu de liberté ! Mais pour combien de temps ?. Personne ne peut véritablement et heureusement à l'heure actuelle prendre le contrôle total d'Internet.

Pour obtenir l'accès à Internet, il existe deux moyens principaux, la liaison fixe filaire ou la connexion par ondes radios, WIFI ou Bluetooth.

Le fonctionnement des services et des explorateurs

Tous les services sur Internet fonctionnent en mode client-serveur : le client, en fait l'équipement terminal – PC ou Téléphone ou tablette…- envoie une demande à un serveur qui lui renvoie un bloc d'information en retour. Dans tous les cas, la requête va être traitée par le service concerné et le résultat est renvoyé à l'adresse de l'expéditeur sur le réseau.

S'il s'agit d'un courrier, c'est le programme de courrier qui va le traiter, s'il s'agit d'une requête HTML, c'est le serveur WEB.

Le courrier électronique un outil très répandu dans Internet aussi bien pour les entreprises que pour les particuliers. C'est le premier service qui s'est développé sur Internet auprès de tous les particuliers ; il a accéléré son développement. La messagerie permet d'acheminer des courriers électroniques entre personnes éloignées par l'intermédiaire du réseau.

Menaces et vulénrabilités

Une menace fait référence à un incident susceptible de nuire à un système ou à l'ensemble de votre organisation. Il existe trois principaux types de menaces:
1. les menaces naturelles (par exemple, les inondations ou une tempête),
2. les menaces non intentionnelles (par exemple, un employé qui accède par erreur à une information erronée)
3. les menaces intentionnelles.

Il existe de nombreux exemples de menaces intentionnelles comprenant des logiciels espions, des logiciels malveillants, des sociétés de logiciels publicitaires ou les actions d'un employé mécontent. D'ailleurs, les vers et les virus sont également considérés comme des menaces, car ils pourraient potentiellement nuire à votre organisation en les exposant à une attaque automatisée, par opposition à une attaque perpétrée par des humains.

Une vulnérabilité fait référence à une faiblesse connue d'une ressource pouvant être exploitée par un ou plusieurs attaquants. En d'autres termes, il s'agit d'un problème connu qui permet à une attaque de réussir. Par exemple, lorsqu'un membre de l'équipe démissionne et que vous oubliez de désactiver son accès aux comptes externes, de modifier ses identifiants, votre entreprise reste ouverte aux menaces intentionnelles. Cependant, la plupart des vulnérabilités sont exploitées par des attaquants automatisés et non par un humain.

Le contexte du Covid 19 :

- ✓ Le télétravail, adopté en réponse à la pandémie de Covid-19, devrait s'installer durablement dans les habitudes
- ✓ Défis de taille en termes de cybersécurité : utilisation des équipements professionnels à des fins personnelles et vice versa, multiplication des accès à distance, recours au cloud, etc.


Menace
?

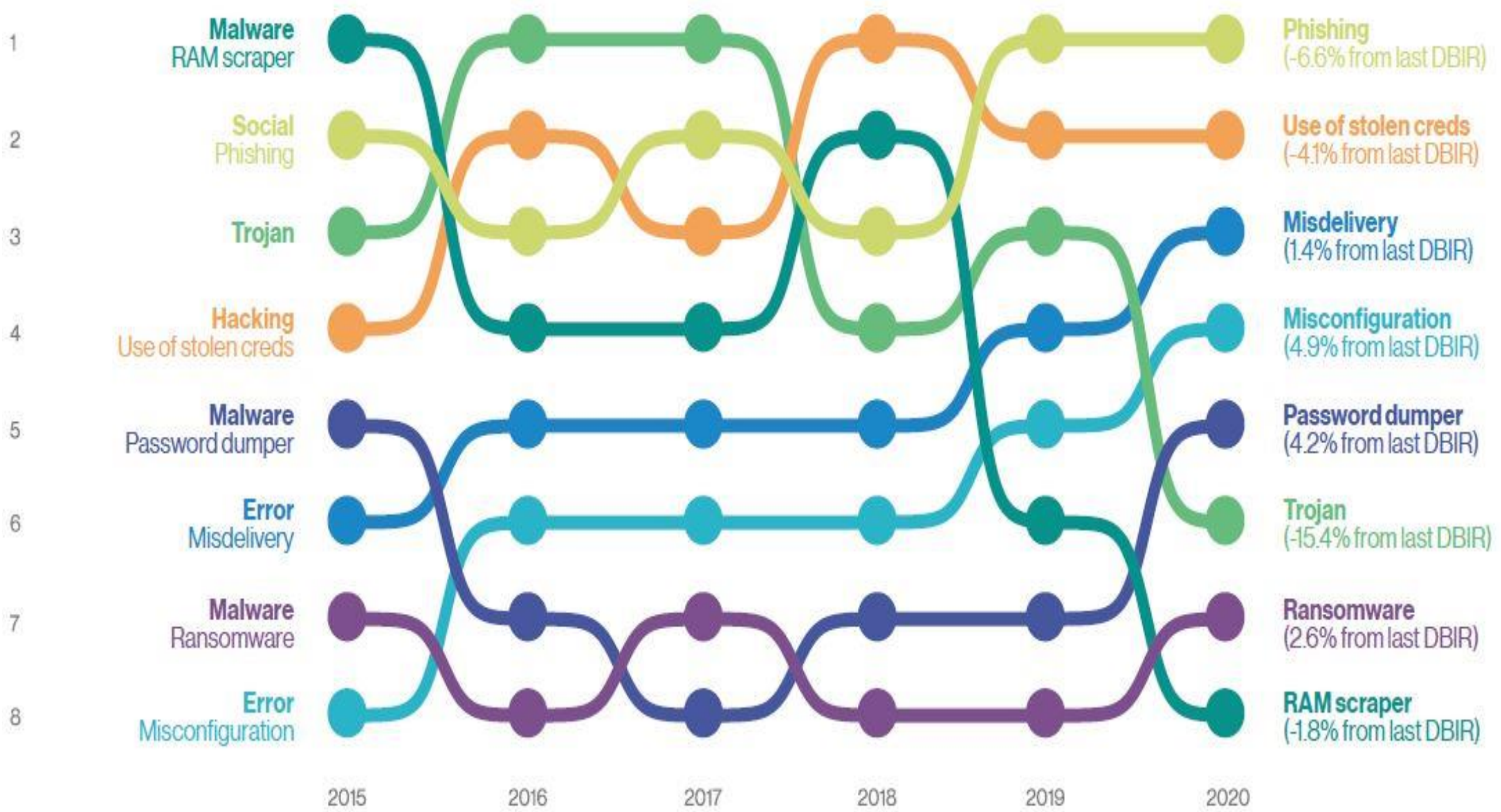
Les différents types de menaces informatiques qui visent les entreprises

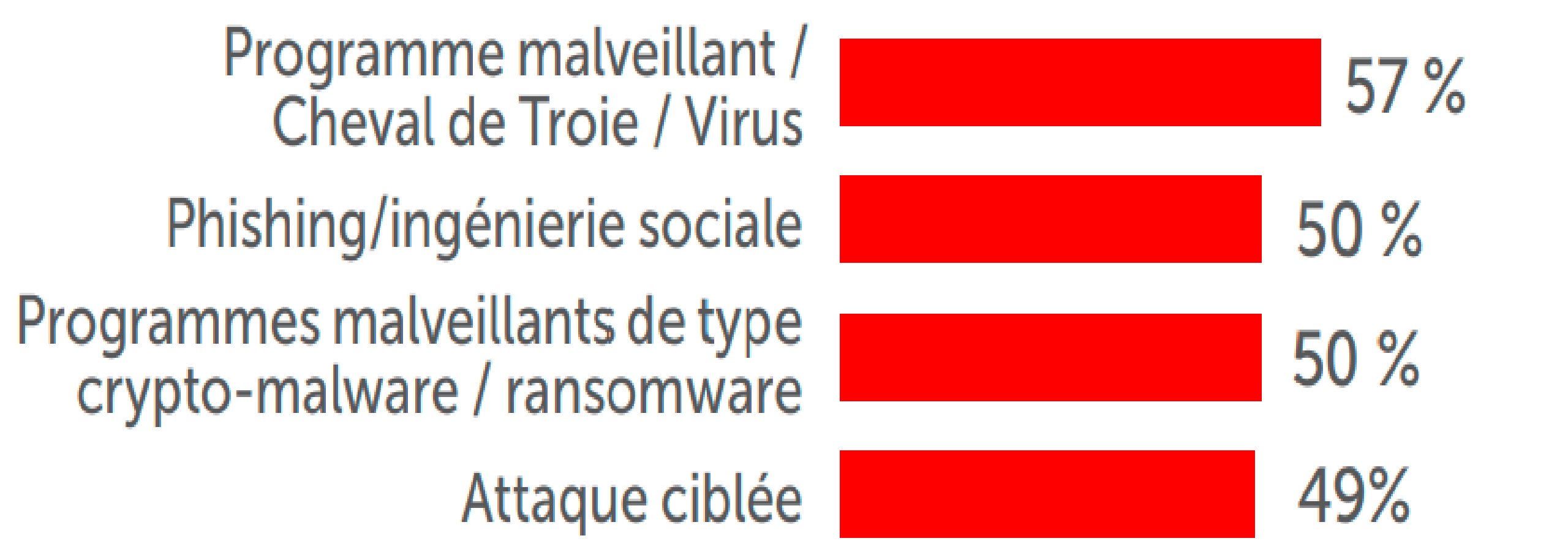
- ✓ Les ransomwares, une menace informatique très répandue. ...
- ✓ Le phishing, une menace informatique sournoise. ...
- ✓ La fuite de données, une menace informatique externe comme interne. ...
- ✓ Les attaques DDos, une menace informatique paralysante.

Situation des menaces dans le monde

Dans le passé, la perception commune était que les cybermenaces ne concernaient principalement que les grands conglomérats tels que les banques, les institutions financières, les entreprises technologiques et les institutions gouvernementales. La réalité d'aujourd'hui est quelque peu différente - tout le monde est également en danger.

Depuis 14 ans, la société Verizon publie un rapport sur les fuites de données, le Data Breach Investigations Report ou DBIR, réputé pour sa rigueur scientifique et sa richesse statistique.


1
2
3
4
5
6
7
8
Malware
RAM scraper
Social
Phishing
Trojan
Hacking
Use of stolen creds
Malware
Password dumper
Error
Misdelivery
Malware
Ransomware
Error
Misconfiguration
Phishing
(-6.6% from last DBIR)
Use of stolen creds
(-4.1% from last DBIR)
Misdelivery
(1.4% from last DBIR)
Misconfiguration
(4.9% from last DBIR)
Password dumper
(4.2% from last DBIR)
Trojan
(-15.4% from last DBIR)
Ransomware
(2.6% from last DBIR)
RAM scraper
(-1.8% from last DBIR)
2015
2016
2017
2018
2019
2020



Les 4 préoccupations principales en matière de sécurité informatique pour les entreprises du monde entier portent sur les menaces directes[1].

DBIR 2021 : Motivation des attaques

Figure 15. Top threat actor motive over time in breaches

DBIR 2021 : Auteurs des attaques

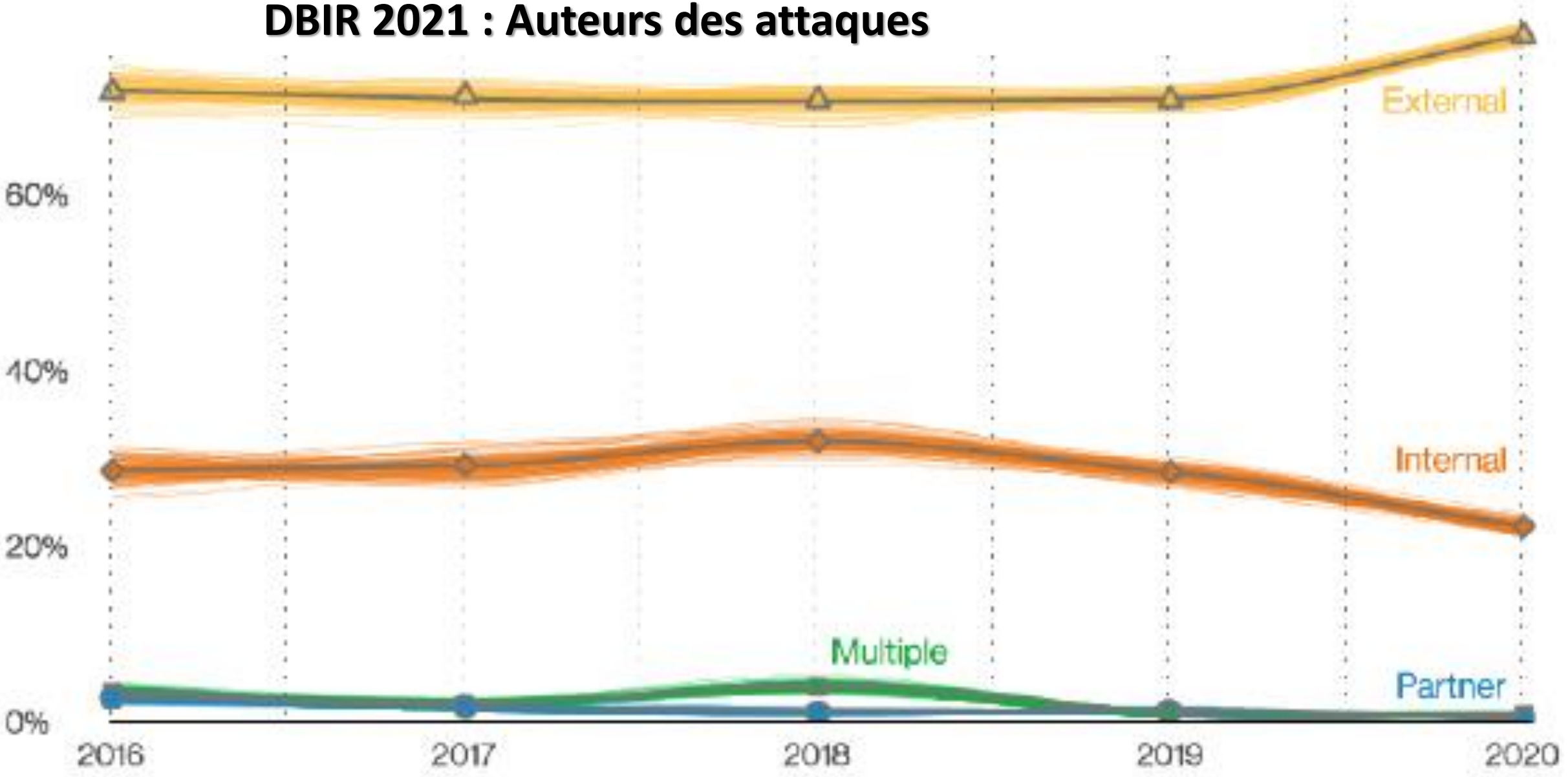


Figure 14. Threat actor over time in breaches

Attaque de type ransomware

Au cours de la prochaine décennie, le coût des attaques de ransomware dépassera 265 milliards de dollars.

En 2020 on a noté une attaque de ransomware toutes les 10 secondes

Source : https://www.infosecurity-magazine.com

2020 a vu la première mort connue d'une cyberattaque liée à un ransomware (la clinique universitaire de Düsseldorf en Allemagne)

Source : Magazine de sécurité

Attaque de pipeline causé par le groupe DarkSide : Colonial Pipeline confirme avoir payé 4,4 millions de dollars de rançon

Menaces liées au COVID-19

- ✓ Domaines malveillants : selon Palo Alto Networks, 2 022 nouveaux domaines enregistrés malveillants et 40 261 présentant un risque élevé avaient été découverts à la fin mars 2020;
- ✓ Escroqueries en ligne et hameçonnage : 1 000 000 d'un million de messages non sollicités envoyés depuis janvier 2020 selon Trend Micro avaient un rapport avec le COVID-19
- ✓ Logiciels malveillants visant à obtenir des données
- ✓ Logiciels malveillants visant à désorganiser (rançongiciels et attaques par déni de service distribué)
- ✓ Vulnérabilité du télétravail

Situation des menaces en Afrique

- ✓ 28 millions de cyberattaques ont eu lieu sur le continent entre janvier et août 2020. (source: Kaspersky)
- ✓ Les banques et les administrations sont de plus en plus ciblées par les hackeurs;
- ✓ 85% des banques ont déjà été victimes d'une ou de plusieurs cyberattaques : fraudes sur les cartes bancaires, phishing et « core banking » (intrusions dans les systèmes d'information pour rançongiciels ou infections virales); (source : Dataprotect)
- ✓ L'Afrique du Sud, le Nigéria, le Kenya payent un lourd tribut au fléau.

Les entreprises africaines sont exposées aux dix attaques les plus communes identifiées par l'ONG Open Web Application Security Project (OWASP).

Tout particulièrement à trois d'entre elles :

- ✓ l'injection SQL, qui permet aux pirates d'avoir accès à toute la base de données d'une entreprise ;
- ✓ l'exposition de données sensibles mal protégées due à des défauts de configuration des systèmes ;
- ✓ et le rançongiciel (ransomware), qui consiste à chiffrer les données d'une entreprise et d'exiger un rançon en échange de leur restitution.