Pirates informatiques

[sommaire]

1. **Objectifs**

- Connaitre les hackers, les types de pirates et les types de piratage

- **Qu'est-ce qu'un hacker ?**



- Le terme hacker est souvent utilisé pour désigner un pirate informatique.
- Les victimes de piratage sur des réseaux informatiques aiment à penser qu’ils ont été attaqués par des pirates chevronnés ayant soigneusement étudié leur système et ayant développé des outils spécifiquement pour en exploiter les failles.
- Le terme hacker a eu plus d’une signification depuis son apparition à la fin des années 1950. À l’origine ce nom désignait d’une façon méliorative les programmeurs émérites, puis il servit au cours des années 1970 à décrire les révolutionnaires de l’informatique, qui pour la plupart sont

devenus les fondateurs des plus grandes entreprises informatiques.

- C’est au cours des années 1980 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.
- Aujourd’hui, ce mot est souvent utilisé à tort pour désigner les personnes s’introduisant dans les systèmes informatiques.

> *Un **Hacker** est un informaticien qui utilise ses connaissances et ses compétences pour mettre en défaut un système informatique. Les termes "Fouineur" ou "Bidouilleurs" sont les plus appropriés en langue française. Au fil des années, le terme a été mal employé en désignant un pirate informatique ayant un but nocif à un site web ou un système informatique.*

Les types de pirates

- En réalité, il existe de nombreux types d'attaquants catégorisés selon leur expérience et selon leurs motivations :

- **Les white hat hackers**



  - Les **white hat hackers**, hackers au sens noble du terme, dont le but est d’aider à l’amélioration des systèmes et technologies informatiques, sont généralement à l’origine des principaux protocoles et outils informatiques que nous utilisons aujourd’hui. Les objectifs des white hat hackers sont en règle générale un des suivants :
    - l'apprentissage ;
    - l'optimisation des systèmes informatiques ;

apcpedagogie.com

        - la mise à l’épreuve des technologies jusqu’à leurs limites afin de tendre vers un idéal plus performant et plus sûr.
    - Les **white hat hackers**, ce sont les "gentils", des experts en sécurité informatique qui se spécialisent dans les tests d’intrusion et d’autres méthodes pour s’assurer que les systèmes d’information d’une entreprise sont sécurisés. Ces professionnels de la sécurité informatique comptent sur un arsenal technologique en constante évolution pour combattre les "mauvais" pirates informatiques.

- **Les black hat hackers**

    - Les **black hat hackers**, plus couramment appelés pirates informatiques, c’est-à-dire des personnes s’introduisant dans les systèmes informatiques dans un but nuisible. Les motivations des **black hat** hackers peuvent être multiples :



        - l’attrait de l’interdit ;
        - l’intérêt financier ;
        - l’intérêt politique ;
        - l’intérêt éthique ;
        - le désir de la renommée ;
        - la vengeance ;
        - l'envie de nuire (détruire des données, empêcher un système de fonctionner).

- **Les grey hat hackers**

apcpedagogie.com



- Pirates "grey hat" Ces pirates informatiques n’utilisent pas leurs compétences pour servir leur intérêt personnel, mais n’agissent pas non plus dans la plus grande honnêteté.
- Par exemple, un pirate informatique qui pénètre dans le système d’une entreprise pour révéler une vulnérabilité et en parler sur Internet peut en fin de compte agir dans l’intérêt des clients de l’entreprise. Cependant, par son action, il compromet également un système sans autorisation.
- Si le même pirate exige de l'argent à l'entreprise pour ne pas révéler la vulnérabilité, il passe alors dans la catégorie des pirates "black hat", agissant uniquement pour son enrichissement personnel.
- Comme la logique le suggère, un hacker au chapeau gris se situe quelque part entre les hackers au chapeau blanc et au chapeau noir. Contrairement au piratage éthique certifié, le piratage au chapeau gris est toujours illégal, car le pirate n'a pas reçu l'autorisation d'une organisation pour tenter d'infiltrer ses systèmes, mais les intentions des pirates au chapeau gris ne sont pas aussi gênantes que leurs homologues au chapeau noir.
- Le piratage du chapeau gris est parfois effectué dans l'intention de l'intérêt public, bien que très souvent, si un chapeau gris identifie un défaut et le signale à une entreprise, l'entreprise travaillera avec le pirate informatique pour corriger l'exploit - en le récompensant souvent comme lui. serait un chapeau blanc. Si un pirate est suffisamment récompensé pour avoir signalé une vulnérabilité plutôt que de l'exploiter, il est plus susceptible de le faire.
- Cependant, la différence entre les pirates au chapeau gris et les pirates au chapeau blanc est que si l'entreprise décide d'ignorer un pirate au chapeau gris, le pirate n'est pas lié par des règles de piratage éthique ou un contrat de travail. Au lieu de cela, ils pourraient décider d'exploiter la faille eux-mêmes ou de partager les connaissances en ligne pour que d'autres pirates puissent en profiter.
- Lorsqu'un hacker au chapeau gris réussit à accéder illégalement à un système ou à un réseau, il peut suggérer à l'administrateur système qu'il ou un de ses amis soit engagé pour résoudre le problème moyennant des frais. Cependant, cette pratique est en déclin

apcpedagogie.com

en raison de la volonté croissante des entreprises d'intenter des poursuites.
- Parfois, si les organisations ne répondent pas rapidement ou ne se conforment pas, les hackers chapeaux gris peuvent devenir des chapeaux noirs en publiant le point d'exploitation sur Internet ou même en exploitant eux-mêmes la vulnérabilité.

- **Les script kiddies**



- Les **script kiddies** (traduisez "gamins du script", parfois également surnommés **crashers, lamers** ou encore **packet monkeys**, soit "les singes des paquets réseau") sont de jeunes utilisateurs du réseau utilisant des programmes trouvés sur Internet, généralement de façon maladroite, pour vandaliser des systèmes informatiques afin de s'amuser.
- Un **script kiddie**, ou "**skiddie**", est une personne qui manque de connaissances en programmation et utilise un logiciel existant pour lancer une attaque. Souvent, un **script kiddie** utilisera ces programmes sans même savoir comment ils fonctionnent ou ce qu'ils font.
- Par exemple, imaginez qu'un enfant reçoit son premier ordinateur. L'enfant regarde un film sur le piratage, puis télécharge une copie de Kali Linux. Ils commencent à jouer avec les différents programmes tout en recherchant des tutoriels en ligne. Au début, ils peuvent être perçus comme rien de plus qu'un troll ou un noob sur Internet, en raison de leur manque d'expérience et de leur rapidité à se vanter et à se vanter. Parfois, ils auront même recours au cyberharcèlement ou à l'intimidation. Cependant, cela peut simplement être une couverture pour d'autres activités plus néfastes.
- Un **Script Kiddie** , également connu sous le nom de **skiddie** ou **dérapage** ; est une personne non qualifiée qui utilise des scripts ou des programmes développés par d'autres personnes pour attaquer des systèmes informatiques et des réseaux ainsi que

pour dégrader des sites Web.
- Ces utilisateurs sont généralement des mineurs qui n'ont pas les compétences nécessaires pour écrire leurs propres programmes ou exploits et utilisent ces scripts pour impressionner les gens ou pour gagner du crédit dans les communautés de cybersécurité.

- **Les phreakers**



- Les **phreakers** sont des pirates s’intéressant au réseau téléphonique commuté (RTC) afin de téléphoner gratuitement grâce à des circuits électroniques (qualifiés de box, comme la blue box, la violet box...) connectés à la ligne téléphonique dans le but d’en falsifier le fonctionnement. On appelle ainsi **phreaking** le piratage de ligne téléphonique. Ce type de pirate connaît un renouveau avec l’accroissement de l’utilisation de la voix sur IP (VoIP) comme moyen de transport des communications téléphoniques grand public.
- Le **phreaking** (contraction des mots « phone » et « freak ») est plus communément appelé piratage téléphonique. Il s’agit de la prise de contrôle des postes téléphoniques, conduite par un hacker ou un « phreaker » dans un but malveillant.
- Les intrusions les plus courants consistent à passer une multitude d’appels locaux ou internationaux surtaxés aux frais de l’entreprise. Suite à ce type d’attaque, les factures téléphoniques peuvent dépasser les milliers d'euros.
- Le **phreaking** peut également se traduire par le blocage des systèmes, la saturation des lignes ou encore l’écoute téléphonique. Ces actes entrainent une gêne dans le cycle de production, parfois même une interruption d’activité impactant considérablement l’entreprise.

- **Les carders**

apcpedagogie.com



- Les **carders** s'attaquent principalement aux systèmes de cartes à puce (en particulier les cartes bancaires) pour en comprendre le fonctionnement et en exploiter les failles. Le terme **carding** désigne le piratage de cartes à puce.
- Le **carding** est un processus par lequel un utilisateur ou un carder achète des marchandises en utilisant des informations de carte de crédit piratées ou volées. Les pirates volent les détails des cartes de crédit, puis achètent des trucs en utilisant ces détails de carte de crédit.
- Le **Carding** est un art ou une technique permettant d'acheter gratuitement quelque chose sur un site d'achat en ligne. En tant que tel, attendez-vous à échouer plusieurs fois pendant que vous démarrez. La clé du succès est de ne pas abandonner et d'essayer différents sites, méthodes, etc.
- La plupart des **cardeurs** ont enduré des périodes inlassables d'essais et d'erreurs. C'est ainsi qu'ils ont découvert des méthodes spécifiques qui leur conviennent.
- Les cardeurs professionnels ne sont disponibles que sur le marché noir et ils le font uniquement pour eux mêmes. Ainsi, quand une personne de la région voudra connaître le carding , elle vous demandera de l'argent environ 100$, ce qui est très élevé pour les noobs.

- **Les crackers**

apcpedagogie.com



- Les **crackers** ne sont pas des biscuits apéritifs au fromage mais des personnes dont le but est de créer des outils logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels payants.
- Un crack est ainsi un programme créé exécutable chargé de modifier (patcher) le logiciel original afin d'en supprimer les protections.
- Le **cracker**, ou déplombeur de logiciels, est spécialisé dans le cassage des protections des logiciels. Il possède de très bonnes connaissances en assemblage ainsi que dans les outils (désassembleur, débogueur…) qui lui permette d'analyser le code d'un programme transmis au processeur. Cela lui permet de neutraliser ou contourner les mesures de protections d'un logiciel en créant un patch (ou crack), ou bien un « keygen » dans le cas de logiciels protégés par des clefs. Les motivations des crackers sont multiples : renommée, exploit, ou tout simplement par intérêt personnel. Crackers célèbres :
  - **DeVianCe** : groupe de crackers.
  - **MYTH** : un autre groupe de crackers.

- **Les hacktivistes**

  - Les **hacktivistes** (contraction de hackers et activistes que l'on peut traduire en cybermilitant ou cyberrésistant), sont des hackers dont la motivation est principalement idéologique. Ce terme a été largement porté par la presse, aimant à véhiculer l'idée d'une communauté parallèle (qualifiée généralement d'underground, par analogie aux populations souterraines des films de science-fiction).
  - Le **hacktivisme** est une forme d'activisme numérique non violent dont le motif n'est pas, principalement, un gain financier personnel. Au contraire, les campagnes hacktivistes visent à obtenir une justice politique, sociale ou religieuse conforme à la cause du groupe.
  - **Les différents types de hacktivisme**
    - Les hacktivistes effectuent des violations de données pour autre chose que l'argent. Au lieu de cela, leurs actions sont menées dans un but politique, pour la justice sociale, au nom de la religion ou l'anarchie.

- **Politique** : le hacktivisme en tant que forme de mobilisation politique vise à orienter ou influencer la population dans le sens des idées du pirate.
- **Social** : La justice sociale dans le hacktivisme vise à provoquer un changement sociétal.
- **Religieux** : le hacktivisme pour un programme religieux vise à recruter ou à désavouer une entité religieuse.
- **Anarchiste** : les pirates peuvent avoir un but anarchiste pour accéder ou contrôler les infrastructures civiles, l'équipement militaire ou la population en général.

- **Les pirates soutenus par un Etat**

  - Les gouvernements du monde entier se rendent compte qu'il est militairement avantageux d'être bien positionné sur le Web. On disait « Celui qui commande la mer commande le monde », puis « Celui qui commande les airs commande le monde ». Il s'agit désormais de commander le cyberespace. Les pirates informatiques financés par des États ont accès à des ressources illimitées pour cibler des civils, des entreprises et des gouvernements.

- Ce qu'il faut retenir, c'est que ces dernières années ont vu une professionnalisation du secteur de l'insécurité. Des organisations criminelles se sont mises en place et utilisent les outils de piratage pour gagner de l'argent1. Comme exemple de cette structuration, on peut citer :
  - les réseaux de machines piratées (botnet) que l'on peut louer pour des activités illégales (spamming, phishing…) ;
  - les sites d'enchères de failles de sécurité ;
  - la vente de pack de malware, de listing de données sensibles (numéros de carte bancaire…) ;
  - l'automatisation du cybersquattage ;
  - le rançonnage d'entreprises avec pour moyen de pression des attaques DDOS ou le cryptage de données par des malwares.

Les types de piratage

- **La contrefaçon**

  - Copie, distribution ou vente illégale d'oeuvres protégées par des droits d'auteur dans l'intention d'imiter le produit protégé. Dans le cas des logiciels en pack, il est courant de trouver des copies contrefaites des disques comprenant non seulement les programmes, mais aussi le packaging, des manuels, des contrats de licence, des étiquettes, des fiches d'enregistrement et des fonctions de sécurité.

apcpedagogie.com

- **Le piratage Internet**
    - Intervient lors du téléchargement sans autorisation d'un logiciel via Internet. Les règles d'achat sont identiques pour les logiciels achetés en ligne et ceux achetés sur CD. Ci-dessous les techniques de piratage via Internet les plus courantes :
        - Sites Web permettant de télécharger des logiciels gratuitement ou moyennant un échange avec d'autres
        - Sites de vente aux enchères proposant des logiciels contrefaits ou hors circuit
        - Réseaux poste-à-poste (ou "peer-to-peer") permettant le transfert non autorisé de programmes protégés par des droits d'auteur

- **Le piratage par les utilisateurs finaux**
    - Cas dans lequel une personne reproduit des copies de logiciels sans autorisation En voici quelques exemples :
        - L'utilisation d'un exemplaire sous licence pour installer un programme sur plusieurs ordinateurs
        - La copie de CD-ROM à des fins d'installation ou de distribution
        - Le fait de profiter d'offres de mise à niveau sans posséder une copie légale de la version antérieure du produit
        - L'acquisition d'un logiciel d'enseignement ou autre programme non disponible dans le commerce/limité sans licence appropriée
        - L'échange de CD sur le lieu de travail ou en dehors

- **L'abus d'utilisation client/serveur**
    - Ce type de piratage intervient lorsqu'un trop grand nombre d'utilisateurs exécute simultanément une copie centrale d'un programme sur un réseau. Si vous disposez d'un réseau local et souhaitez installer sur le serveur des programmes destinés à plusieurs utilisateurs, vous devez vérifier au préalable que votre licence vous y autorise. Si le nombre d'utilisateurs est supérieur à celui autorisé par la licence, on parle d'abus de licence.

- **Le "Hard-Disk Loading"**
    - Cas dans lequel une entreprise vend de nouveaux ordinateurs équipés de copies illicites de logiciels, chargées sur les disques durs pour inciter à l'achat des machines.

apcpedagogie.com

- ## Comment se protéger des pirates

1. **Utilisez des mots de passe uniques et complexes**

- Un mot de passe fort n'est pas facile à deviner et se compose idéalement d'une combinaison de lettres majuscules et minuscules, de caractères spéciaux et de chiffres. Les gens laissent souvent les mots de passe inchangés pendant des années, ce qui réduit leur sécurité.
- En violant un mot de passe, les pirates informatiques se rapprochent un peu plus de vos données. Évitez d'écrire vos mots de passe sur un morceau de papier et ne les partagez pas avec d'autres. Un outil de gestion de mots de passe est un excellent moyen de gérer vos mots de passe.

- **Ne cliquez jamais sur des liens envoyés dans des e-mails non sollicités**

- Ils peuvent faire partie d'une escroquerie par hameçonnage , d'une tentative d'obtention de vos mots de passe, numéros de carte de crédit, coordonnées bancaires, etc. En cliquant sur ces liens, vous pourriez télécharger des logiciels malveillants – des logiciels malveillants – sur votre appareil.

- **Utilisez des sites Web sécurisés**

- Utilisez des sites Web commerciaux dotés du cryptage Secure Sockets Layer (SSL). Pour vérifier si un site Web l'a installé, regardez l'URL - elle doit commencer par "HTTPS://" au lieu de "HTTP://". Le "s" signifie "sécurisé". Il y aura également une icône de verrouillage à proximité, et son emplacement dépend de votre navigateur. Essayez d'éviter d'enregistrer les informations de paiement sur les sites Web d'achat - si des fraudeurs compromettent le site, ils auront accès à vos informations.

- **Activer l'authentification à deux facteurs**

- Cela ajoute une couche de sécurité au processus de connexion. Lors de la configuration, vous devrez toujours saisir votre nom d'utilisateur et votre mot de passe, mais vous devrez également vérifier votre identité grâce à un deuxième facteur d'authentification - souvent un code PIN envoyé à votre téléphone portable. Cela signifie qu'un voleur d'identité aurait besoin de connaître vos informations de connexion et d'être en possession de votre téléphone portable, ce qui est un scénario moins probable.

apcpedagogie.com

- **Soyez prudent lorsque vous utilisez des réseaux Wi-Fi publics**
    - Ils peuvent être non cryptés et non sécurisés, vous laissant vulnérable aux pirates qui cherchent à voler toute information qui passe entre vous et les sites Web que vous visitez. Vos informations personnelles, telles que les mots de passe ou les données financières, sont alors vulnérables à l'usurpation d'identité. L'utilisation d'un VPN peut vous aider.
- **Désactiver l'option de remplissage automatique**

    C'est une fonctionnalité qui permet de gagner du temps, mais si cela vous convient, cela l'est également pour les pirates. Toutes les informations de remplissage automatique doivent être conservées quelque part, par exemple dans le dossier du profil de votre navigateur. C'est le premier endroit où un pirate informatique ira chercher votre nom, votre adresse, votre numéro de téléphone et toutes les autres informations dont il a besoin pour voler votre identité ou accéder à vos comptes.
- **Choisissez judicieusement les applications**

    Téléchargez uniquement des applications à partir de sources fiables telles que l'App Store d'Apple ou Google Play. Assurez-vous de mettre régulièrement à jour votre logiciel et vos applications et de vous débarrasser des anciennes applications que vous n'utilisez pas.
- **Tracer ou effacer**
    - Assurez-vous que vos données sont sécurisées si votre appareil mobile est volé ou perdu. Vous pouvez installer un logiciel qui peut effacer votre téléphone s'il est perdu. Vous pouvez également configurer votre appareil pour qu'il se verrouille après un nombre prédéfini de tentatives de connexion infructueuses.
- **Désactiver et gérer les autorisations des tiers**

    Sur les téléphones mobiles, certaines autorisations sont activées pour les applications tierces que les utilisateurs téléchargent sur leurs appareils sans en informer le propriétaire du gadget. Par conséquent, les services de localisation, les téléchargements automatiques, la sauvegarde des données et même l'affichage public des numéros de téléphone personnels sont tous des autorisations définies sur le vert lors de l'installation. La gestion de ces paramètres et des autorisations sur le plateau, en particulier ceux

apcpedagogie.com

connectés au cloud, est essentielle pour protéger vos données des pirates.

- **Installez une cybersécurité de confiance sur tous vos appareils**
  - Comme la cybersécurité, Kaspersky Internet Security bloque les virus et les logiciels malveillants en temps réel et empêche les pirates de s'emparer de votre PC à distance. Ainsi, vous et votre famille serez toujours protégés , quel que soit l'appareil que vous utilisez pour accéder à Internet.

- ## Exercice d'application

  [h5p id="60"]

Cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/pirates-informatiques · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com