VIRUS INFORMATIQUE

Un **virus informatique** est un **programme malveillant** capable de se **répliquer** et de se **propager** de manière autonome d'un ordinateur à l'autre. Son objectif principal est de perturber le fonctionnement normal d'un système informatique, pouvant aller de la simple nuisance à des dommages graves.

Le malware (logiciel malveillant)

Le terme générique définissant **les virus** est **malware**, le **terme virus** est utilisé couramment de manière abusive pour désigner l'ensemble des malwares**.**

Differents tpes de malware :

- **Virus**
  Un virus informatique est un petit programme logiciel qui se propage d'un ordinateur à un autre et interfère avec le fonctionnement de l'ordinateur. Un virus d'ordinateur peut endommager ou supprimer des données sur un ordinateur, utiliser un programme de messagerie pour propager le virus à d'autres ordinateurs, ou même supprimer tout ce qui se trouve sur le disque dur.
- **Ver : Un ver informatique** est un logiciel malveillant, tout comme un virus, mais un ver prend une copie de lui-même et la propage à d'autres utilisateurs. Les vers se propagent alors automatiquement via les messages électroniques, les réseaux ou les vulnérabilités du système d'exploitation, souvent écrasant ces systèmes avant que la cause ne soit connue. Les vers ne sont pas toujours destructeurs pour les ordinateurs, mais ils causent généralement des problèmes de performances et de stabilité de l'ordinateur et du réseau.
- **Rançongiciel - Ransonware**
  Un rançongiciel est un type de logiciel malveillant qui crypte vos fichiers, les rendant inaccessibles. Les attaquants de ransomware exigent ensuite le paiement d'une rançon en échange du décryptage de vos fichiers**.**
- **Cheval de troie : trojan**
  Un cheval de Troie est un programme logiciel malveillant qui se cache à l'intérieur d'autres programmes. Il entre un ordinateur masqué à l'intérieur d'un programme légitime, tel qu'un économiseur d'écran. Ensuite, il place le code dans le système d'exploitation qui permet à un pirate informatique d'accéder à l'ordinateur infecté. Chevaux de Troie ne se propagent généralement pas par eux-mêmes. Ils sont propagés par des virus, des vers ou des logiciels téléchargés

- **Logiciel espion - spyware**
  Les logiciels espions peuvent être installés sur votre ordinateur à votre insu. Ces programmes peuvent modifier la configuration de votre ordinateur ou collecter des données publicitaires et des informations personnelles. Les logiciels espions peuvent suivre les habitudes de recherche Sur Internet et peuvent également rediriger votre navigateur web vers un autre site web que celui vers lequel vous envisagez d'accéder.
- **rootkit**
  Ce malware permet au pirate d'installer une série d'outils pour accéder à distance à l'ordinateur hacké. Le malware, habituellement caché dans l'OS, n'est pas détecté par les logiciels anti-virus et autres outils de sécurité. Le rootkit peut capturer les mots de passe, voler les informations de cartes et de comptes bancaires en ligne, mener des attaques DDoS (Denial of Service), désactiver les logiciels de sécurité…
- **Logiciel publicitaire** :**Adwar**e
  Un logiciel publicitaire est un logiciel qui affiche des publicités indésirables sur votre ordinateur.Bien que les logiciels publicitaires ne soient généralement pas considérés comme aussi nuisibles que d'autres types de logiciels malveillants, ils peuvent être ennuyeux et intrusifs.
- **Hameçonnage**
  L'Hameçonnage est une methode qui concisye à vous piéger pour que vous partagie vos mots de passe, numeros de cartes bancaire et autres informations sensibles en pretendant etre une institution de confiance dans un e-mail ou un appel
- **Cryptojacking**
  le cryptojacking est une forme emrrgente de malware qui se cache fdans votre appareil et qui vole ses ressources informatiques afin de miner les devices de valeur comme le bitcoin
- **Emotet**
  Emotet est un cheval de Troie qui se propage principalement par des e-mails de spam (malspams). L'infection peut provenir d'un script malveillant, de fichiers document qui prennent en charge les macros, ou des liens malveillants. Les e-mails d'Emotet peuvent contenir des supports de marques connues pour prendre l'apparence d'e-mail légitimes. Emotet peut essayer de persuader les utilisateurs à cliquer sur des fichiers malveillants en utilisant un discours ayant pour but de tenter l'utilisateur, avec « Votre facture

trois principales familles de de virus informatiques :

#1 Les virus “chaotiques”, moins fréquents aujourd’hui, suppriment des données et/ou font dysfonctionner les ordinateurs :
Symptômes classiques : messages d’erreur ou écran bleu au démarrage, système instable, plantages. Dans le meilleur des cas, on peut restaurer et réinstaller sons système. Dans le pire, on risque de perdre des fichiers importants (et très souvent aussi, du temps…).

#2 Les virus “à valeur ajoutée” utilisent les ordinateurs-hôtes pour générer du revenu :
Certains affichent par exemple de la publicité non-sollicitée. Chaque vue rapporte un petit bénéfice qui, multiplié à grande échelle, peut vite grossir. D’autres, plus discrets, misent sur le vol de données. Ils “scannent” l’ordinateur pour trouver des informations intéressantes. Ce type de malware parcourt par exemple les tableurs ou les fichiers textes à la recherche de syntaxes ressemblant à des relevés bancaires ou des numéros de téléphone. Les données sont ensuite vendues. L’utilisateur imprudent s’expose alors à un risque bancaire, au spam, ou encore à des appels non sollicités.

#3 Les virus “preneurs d’otages” bloquent l’accès au système ou aux fichiers, et exigent le paiement d'une rançon.
Aussi appelé “malwares de rançonnage”, cryptovirus, ransomwares, rançonwares ou rançongiciels, ce type de virus cherche à piéger l’utilisateur. L’infection de l’ordinateur résulte souvent d’un comportement à risque : ouverture d’une pièce jointe douteuse, clic sur un faux lien, etc. Le programme malveillant vient alors crypter tout ou partie des données puis propose l’achat d’une clé de déchiffrement, souvent contre plusieurs centaines d’euros. On estime que 80 % des virus en circulation aujourd’hui sont des ransomwares.

1 – differents types de virus

Il existe **neuf grands types de virus**, dont certains peuvent être associés à d’autres logiciels malveillants pour augmenter les risques d’infection et de dommages.

Les neuf principales catégories de virus sont les suivantes :

1 -1 Virus visant le secteur de démarrage

Le disque dur de votre ordinateur possède un secteur (Master Boot Record - MBR)uniquement chargé de pointer vers le système d’exploitation afin qu’il puisse démarrer dans l’interface.
. Lorsque l'ordinateur est allumé, le BIOS recherche le MBR sur le disque dur. Si le MBR est infecté par un virus, le virus est alors exécuté avant le système d'exploitation. Le virus peut ensuite infecter d'autres fichiers du système ou afficher un message d'erreur.

Les attaquants diffusent généralement ce type de virus à l'aide d'un périphérique USB malveillant. Le virus est activé lorsque les utilisateurs branchent le périphérique USB et démarrent leur machine.

En cas d'infection par un virus du secteur de démarrage :

- Déconnecter l'ordinateur du réseau.
- Démarrer l'ordinateur à partir d'un CD ou d'une clé USB de secours.
- Analyser l'ordinateur avec un antivirus.
- Réparer le MBR ou restaurer le système à partir d'une sauvegarde.

Conclusion

Le secteur de démarrage est une cible privilégiée pour les cybercriminels. En prenant les mesures de sécurité adéquates, les entreprises et les particuliers peuvent se protéger contre les virus du secteur de démarrage et les dommages potentiels qu'ils peuvent causer.

1 – 2 -Virus des scripts Web

Comprendre la menace et se protéger

Un virus de script web, parfois appelé simplement "**script malveillant**", est un type de malware qui exploite le code des navigateurs web et des pages web pour infecter les ordinateurs des utilisateurs.

Comment fonctionnent les virus de scripts web ?

Ces virus sont généralement écrits dans des langages de script comme JavaScript, VBScript ou PowerShell. Ils peuvent être injectés dans des pages web légitimes de plusieurs manières, notamment :

- **Attaques par injection SQL** : injection de code malveillant dans une base de données pour récupérer des informations sensibles.
- **Cross-site scripting (XSS)** : injection de code JavaScript malveillant dans une page web légitime, capable d'infecter l'ordinateur de la victime lorsqu'elle consulte la page.
- **Sites web compromis** : des sites web piratés peuvent héberger des scripts malveillants.

Une fois exécuté, le script malveillant peut effectuer diverses actions néfastes, telles que :

- **Vol de données sensibles** : informations de connexion, numéros de carte de crédit, etc.
- **Installation de logiciels malveillants supplémentaires** : chevaux de Troie, ransomwares, etc.
- **Redirection vers des sites web frauduleux** : pour inciter les utilisateurs à saisir des informations personnelles.
- **Perturbation du fonctionnement du navigateur web** : affichage de publicités indésirables, ralentissements, etc.

Comment se protéger contre les virus de scripts web ?

- Installer un **antivirus** et **un anti-malware** sur tous les appareils utilisés pour naviguer sur Internet.
- Mettre à jour régulièrement le système d'exploitation, les logiciels et les navigateurs web.
- Utiliser un bloqueur de publicités pour empêcher l'affichage de publicités potentiellement malveillantes.
- Se méfier des liens et des sites web suspects : ne jamais cliquer sur un lien provenant d'une source inconnue.
- Saisir ses informations personnelles uniquement sur des sites web sécurisés : l'URL doit commencer par "https://" et un cadenas doit être présent dans la barre d'adresse.
- Activer les paramètres de sécurité du navigateur : désactiver les scripts Java et JavaScript si possible (à utiliser avec prudence).
- Se familiariser avec les techniques **de phishing** et apprendre à les identifier.

En cas d'infection par un script malveillant :

- Analyser l'ordinateur avec un antivirus et un anti-malware.
- Modifier les mots de passe de tous les comptes en ligne.
- Contacter la banque ou l'organisme de crédit en cas de vol de données bancaires.
-

Points à retenir :

Les virus de scripts web sont une menace sérieuse pour la sécurité des utilisateurs en ligne.
En prenant des mesures de sécurité simples, on peut se protéger efficacement contre ces menaces.
Restez vigilant et méfiez-vous des activités suspectes en ligne.

1 – 3 - Virus résident

Un virus résident est un type de malware qui s'installe et se cache dans la mémoire vive (RAM) de l'ordinateur. Cette persistance lui permet d'infecter tous les programmes et fichiers exécutés par la suite, sans nécessairement être activé par l'utilisateur.

Types de virus résidents :

- **Virus à infection rapide** : Se propagent rapidement en infectant un grand nombre de fichiers, provoquant des dommages importants.
- **Virus à infection lente** : Se propagent plus lentement, mais restent inactifs plus longtemps, ce qui rend leur détection plus difficile.

Modes d'infection des virus résidents :

- **Pièces jointes infectées**: Ouverture de pièces jointes malveillantes dans des emails.
- **Téléchargements infectés**: Téléchargement de fichiers provenant de sources non fiables.
- **Logiciels piratés**: Installation de logiciels piratés contenant du code malveillant.
- **Lecteurs amovibles infectés**: Insertion de clés USB ou de CD/DVD infectés dans l'ordinateur.

Impact des virus résidents :

- **Perturbation du fonctionnement du système**: Ralentissements, plantages, messages d'erreur.
- Vol de données sensibles: Informations personnelles, mots de passe, données bancaires.
- **Espionnage des activités de l'utilisateur**: Enregistrement des frappes au clavier, capture d'écrans.
- **Détournement de l'ordinateur pour des attaques** : Envoi de spam, propagation de malwares, etc.

Protection contre les virus résidents :

- Installer un **antivirus** et **un anti-malware** performants: Assurez-vous que les définitions de virus sont à jour.
- Effectuer des analyses régulières du système: Analysez votre ordinateur à la recherche de virus et de malwares.
- Mettre à jour le système d'exploitation et les logiciels: Installez les correctifs de sécurité pour combler les vulnérabilités.
- Être vigilant sur internet: Ne cliquez pas sur des liens suspects et ne téléchargez pas de fichiers provenant de sources non fiables.
- Utiliser un pare-feu: Bloquez les accès non autorisés à votre ordinateur.
- Effectuer des sauvegardes régulières: Sauvegardez vos données importantes pour les restaurer en cas d'infection.

En cas d'infection par un virus résident :

- Déconnectez l'ordinateur d'internet.
- Démarrez l'ordinateur en mode sans échec.
- Analysez l'ordinateur avec un antivirus et un anti-malware.
- Supprimez le virus si possible.
- Rétablissez l'ordinateur à partir d'une sauvegarde si nécessaire.

En conclusion, les virus résidents constituent une menace sérieuse pour la sécurité des ordinateurs. En prenant les mesures de protection adéquates et en restant vigilant, vous pouvez réduire le risque d'infection et minimiser les dommages potentiels.

1 – 4 - Virus à action directe

Un virus à action directe est un type de virus informatique qui infecte un ordinateur et exécute son code malveillant immédiatement, sans période de latence. Les virus à action directe sont également connus sous le nom de virus à infection rapide ou de virus à action rapide.

Les virus à action directe se propagent généralement lorsqu'un utilisateur exécute un fichier infecté, tel qu'une pièce jointe à un e-mail ou un fichier téléchargé à partir d'Internet. Une fois le fichier exécuté, le virus s'installe sur l'ordinateur et commence à exécuter son code malveillant.

Le code malveillant d'un virus à action directe peut effectuer un certain nombre d'actions différentes, notamment :

- Supprimer ou corrompre des fichiers
- Formater le disque dur de l'ordinateur
- Voler des informations personnelles ou financières
- Envoyer des e-mails de spam
- Détourner l'ordinateur vers un site Web malveillant

Les virus à action directe peuvent être très dangereux et peuvent causer des dommages importants aux ordinateurs et aux réseaux. Il est important d'avoir un antivirus installé et mis à jour sur votre ordinateur pour vous protéger contre les virus à action directe.

Voici quelques conseils pour vous protéger contre les virus à action directe :

- N'ouvrez pas les pièces jointes des e-mails provenant de personnes que vous ne connaissez pas.
- Ne téléchargez pas de fichiers à partir de sites Web non fiables.
- Installez un antivirus et maintenez-le à jour.
- Utilisez un pare-feu pour bloquer les accès non autorisés à votre ordinateur.

Soyez prudent lorsque vous cliquez sur des liens dans des e-mails ou sur des sites Web. En suivant ces conseils, vous pouvez aider à protéger votre ordinateur contre les virus à action directe.

1 – 5 - virus polymorphe

Un virus polymorphe est un type de virus informatique qui modifie son code à chaque infection, ce qui rend sa détection par les logiciels antivirus traditionnels plus difficile.

Fonctionnement:

- Le virus contient un moteur de mutation qui génère de nouvelles copies du virus avec des structures de code différentes.

- Le code du virus reste fonctionnellement identique, mais son apparence change, ce qui le rend indétectable par les logiciels antivirus qui s'appuient sur des signatures de virus statiques.

Différences avec les virus classiques:

- **Difficile à détecter**: Les signatures de virus ne correspondent pas à toutes les copies du virus.
- **Difficile à bloquer**: Les logiciels antivirus basés sur les signatures ne peuvent pas bloquer toutes les variantes du virus.

Méthodes de détection:

- **Analyse heuristique**: Détecte les comportements suspects du virus.
- **Analyse émulative**: Exécute le virus dans un environnement virtuel pour observer son comportement.
- **Vaccins antiviraux**: Empêchent le virus de modifier son code.

Exemples de virus polymorphes:

- Dark Avenger
- Elkin
- Narcissus

Protection contre les virus polymorphes:

- Utiliser un logiciel antivirus performant avec des technologies de détection avancées.
- Mettre à jour régulièrement le logiciel antivirus.
- Être prudent lors de l'ouverture de fichiers provenant de sources inconnues.
- Ne pas télécharger de logiciels à partir de sites Web non fiables.

Conclusion:

Les virus polymorphes représentent une menace importante pour la sécurité informatique. Il est important de prendre des mesures pour se protéger contre ces virus en utilisant des logiciels antivirus performants et en adoptant des pratiques de sécurité informatique saines.

1 – 6 - Virus infecteur de fichiers

Un virus infecteur de fichier est un type de logiciel malveillant qui s’attaque directement aux fichiers exécutables (.exe, .Com etc.) d’un ordinateur. Son objectif principal est de se propager en infectant d’autres fichiers, causant ainsi divers dommages au système et aux données.

Fonctionnement:

- **Infection**: Le virus infecte un fichier exécutable en s’y injectant.

- **Exécution**: Lorsque l'utilisateur exécute le fichier infecté, le code du virus est également exécuté.

- **Propagation**: Le virus recherche d'autres fichiers exécutables sur le système et les infecte à son tour**.**
    - **Dommages**: Le virus peut causer divers dommages, tels que la suppression de fichiers, le vol de données, le cryptage des données (ransomware), ou encore le ralentissement du système.

Types de virus infecteurs de fichier:

- Virus de secteur d'amorçage : Infectent le secteur d'amorçage du disque dur, ce qui les rend actifs dès le démarrage de l'ordinateur.
- Virus de macro: Infectent les documents Microsoft Office et se propagent via les macros.
- Virus furtifs: Modifient le comportement du système pour éviter d'être détectés par les antivirus.

Protection contre les virus infecteurs de fichier:

- Installer un antivirus performant et le maintenir à jour.
- Analyser régulièrement votre ordinateur avec l'antivirus.
- Être prudent avec les fichiers provenant de sources inconnues.
- Ne pas ouvrir les pièces jointes suspectes.
- Mettre à jour régulièrement le système d'exploitation et les logiciels.

En résumé, les virus infecteurs de fichier sont des logiciels malveillants qui peuvent causer de graves dommages à votre ordinateur et à vos données. Il est important de se protéger contre ces virus en utilisant un antivirus performant et en adoptant des pratiques de sécurité informatique.

1 – 7 - virus multipartite – un type complexe de malware

Un virus multipartite est un type particulier de logiciel malveillant qui combine les caractéristiques des virus de fichier et des virus de boot secteur.

Caractéristiques:

- **Genome segmenté**: Son matériel génétique est divisé en plusieurs segments, chacun pouvant se trouver dans une particule virale distincte.
- **Double infection**: Il peut infecter à la fois les fichiers exécutables et le secteur d'amorçage du disque dur.
- **Multiplication de la propagation** : Se propage grâce aux deux méthodes d'infection, augmentant sa capacité de diffusion et de persistance.

Fonctionnement:

- **Infection initiale**: Le virus peut infecter un ordinateur via un fichier exécutable infecté ou en exploitant une vulnérabilité du système.
- **Propagation par fichier**: Lorsqu'un fichier infecté est exécuté, le code du virus s'active et recherche d'autres fichiers exécutables pour les infecter à leur tour.

- Infection du secteur d'amorçage : Une partie du virus peut également infecter le secteur d'amorçage du disque dur. Ce segment se charge dès le démarrage du système, garantissant la persistance du virus même après la suppression des fichiers infectés.

Complexité et danger:

Les virus multipartites sont souvent considérés comme plus dangereux que les virus classiques en raison de leur double capacité d'infection. Ils peuvent être plus difficiles à détecter et à éliminer complètement, car une partie du virus peut persister même si les fichiers infectés sont supprimés.

Exemples:

- Moutons lapidés : L'un des premiers virus multipartites connu, infectant à la fois les fichiers et le secteur d'amorçage.
- Form : Un autre exemple de virus multipartite capable d'infecter les fichiers COM et le secteur d'amorçage.

Prévention:

Les mêmes mesures de protection contre les virus infecteurs de fichier s'appliquent aux virus multipartites :

- Utiliser un antivirus performant et le maintenir à jour.
- Analyser régulièrement votre ordinateur.
- Être prudent avec les fichiers provenant de sources inconnues.
- Ne pas ouvrir les pièces jointes suspectes.
- Mettre à jour régulièrement le système d'exploitation et les logiciels.

En conclusion, les virus multipartites sont des logiciels malveillants complexes et potentiellement dangereux. Une vigilance accrue et des pratiques de sécurité informatique strictes sont essentielles pour se protéger contre ce type de menace

1 – 8 - Virus macro

Les fichiers Microsoft Office peuvent exécuter des macros, et ces macros peuvent être utilisées pour télécharger des logiciels malveillants supplémentaires ou exécuter du code malveillant.

Les virus de macro délivrent une charge utile lorsque le fichier est ouvert et que la macro est exécutée.

De quoi s'agit-il ?

Les virus de macro sont un type de logiciel malveillant qui exploite la fonctionnalité de macro de certaines applications, principalement des produits Microsoft Office comme Word, Exceller et l'accès. Les macros sont essentiellement des séquences automatisées de commandes intégrées dans des documents qui peuvent effectuer diverses tâches.

Comment fonctionnent-ils ?

Les virus de macro se propagent généralement par le biais de documents infectés partagés via des pièces jointes à des e-mails, téléchargé à partir de sources non fiables, ou ouvert à partir d'un support externe. Lorsque le document infecté est ouvert et que les macros sont activées, le code malveillant de la macro s'exécute, pouvant causer des dommages.

Que peuvent-ils faire ?

Les macrovirus peuvent avoir toute une série d'effets nocifs, notamment :

- Corrompre ou supprimer des fichiers
- Voler des informations sensibles comme des mots de passe ou des données financières
- Perturber le fonctionnement du système en désactivant des processus ou en modifiant les paramètres
- Téléchargement et installation de logiciels malveillants supplémentaires

Protégez-vous :

Voici quelques mesures essentielles que vous pouvez prendre pour protéger votre système contre les virus de macro :

- **Désactiver les macros par défaut** : dans les paramètres de vos applications compatibles avec les macros, configurez-les pour désactiver automatiquement les macros, sauf si vous faites explicitement confiance à la source et au contenu du document.
- **Faites preuve de prudence avec les macros** : n'activez les macros qu'en cas d'absolue nécessité et à partir d'une source en laquelle vous avez entièrement confiance. Méfiez-vous des invites d'activation des macros, en particulier dans des situations inattendues.
- **Utilisez une solution antivirus robuste** : choisissez un programme antivirus fiable qui offre une protection en temps réel contre les logiciels malveillants, y compris les macrovirus. Maintenez-le à jour avec les dernières définitions de virus pour vous assurer qu'il peut détecter et bloquer les menaces émergentes.
- **Maintenez les mises à jour logicielles** : mettez régulièrement à jour votre système d'exploitation, vos applications et votre logiciel antivirus pour corriger les failles de sécurité qui pourraient être exploitées par des logiciels malveillants.
- **Faites attention aux courriels et aux pièces jointes** : Évitez d'ouvrir les courriels ou les pièces jointes provenant d'expéditeurs inconnus ou ceux qui semblent suspects. Si vous n'êtes pas sûr de la légitimité d'un e-mail, n'hésitez pas à contacter directement l'expéditeur pour vérifier son authenticité.
- **Analyser les fichiers téléchargés** : les fichiers téléchargés : Avant d'ouvrir les fichiers téléchargés,, en particulier de sources non fiables, Analysez-les avec votre logiciel antivirus pour identifier les menaces potentielles.
- **Sauvegardez vos données** : vos données : sauvegardez Sauvegardez régulièrement vos données critiques dans un emplacement sécurisé au cas où votre système serait compromis par des logiciels malveillants. Cela vous permet

d’avoir une copie de vos fichiers essentiels au cas où ils seraient endommagés ou perdus.

En suivant ces mesures de sécurité complètes, vous pouvez réduire considérablement le risque d’infections par macrovirus et protéger votre système contre les dommages potentiels. Si vous rencontrez une activité suspecte ou si vous soupçonnez une infection par un macrovirus, demandez l’aide immédiate d’un professionnel de l’informatique qualifié ou d’un expert en cybersécurité. Ils peuvent aider à diagnostiquer le problème, supprimer le logiciel malveillant, et rétablissez la sécurité de votre système.

1 – 9 – Detourneur de navigateur (browser hijacker)

Un détourneur de navigateur est un type de logiciel malveillant qui modifie les paramètres de votre navigateur web sans votre consentement. Son objectif principal est de générer des revenus publicitaires pour son créateur en vous redirigeant vers des sites web spécifiques.

Impact:

- **Redirection vers des sites web indésirables**: Vous êtes redirigé vers des sites web que vous ne souhaitez pas visiter, souvent remplis de publicités ou de contenu malveillant.
- **Modification de la page d’accueil et du moteur de recherche** par défaut : Votre page d’accueil et votre moteur de recherche par défaut sont remplacés par des options indésirables.
- **Ajout de barres d’outils et d’extensions indésirables** : Des barres d’outils et des extensions indésirables sont installées sur votre navigateur, qui peuvent collecter vos données personnelles et ralentir votre système.
- **Collecte de données personnelles**: Le détourneur de navigateur peut collecter vos données personnelles, telles que votre historique de navigation et vos habitudes de recherche, et les vendre à des tiers.

Exemples de détourneurs de navigateur:

- Rechercher Baron : Modifie la page d’accueil et le moteur de recherche par défaut en [URL non valide supprimée]
- **MyStartSearch**: Redirige les utilisateurs vers mystartsearch.com lorsqu’ils effectuent une recherche.
- **CoolWebSearc**h: Ajoute une barre d’outils et modifie la page d’accueil et le moteur de recherche par défaut en [URL non valide supprimée]

Protection contre les détourneurs de navigateur:

- Installer un antivirus performant et le maintenir à jour.
- Être prudent avec les logiciels gratuits et les sites web non fiables.
- Ne pas télécharger de fichiers à partir de sources inconnues.
- Lire attentivement les conditions d’utilisation avant d’installer un logiciel.
- Supprimer les extensions et les barres d’outils que vous n’utilisez pas.

- Réinitialiser les paramètres de votre navigateur si vous pensez être infecté.

En résumé, les détourneurs de navigateur sont des logiciels malveillants qui peuvent causer de nombreux désagréments et mettre en danger vos données personnelles. Il est important de se protéger contre ces logiciels en adoptant des pratiques de sécurité informatique strictes.

1 -10 – Virus réseau

Un virus réseau est un type de logiciel malveillant qui se propage d'un ordinateur à l'autre via un réseau informatique, sans avoir besoin de s'installer sur un ordinateur individuel. Contrairement aux virus classiques qui infectent des fichiers, les virus réseau exploitent les failles de sécurité des logiciels et des protocoles réseau pour se propager.

Fonctionnement:

Propagation via les paquets réseau: Le virus se propage en s'insérant dans les paquets de données qui circulent sur le réseau. Il peut infecter d'autres ordinateurs en exploitant des vulnérabilités logicielles ou en utilisant des techniques d'ingénierie sociale pour inciter les utilisateurs à exécuter du code malveillant.

Pas de fichier infecté: Contrairement aux virus classiques, les virus réseau ne s'installent pas sur les ordinateurs infectés. Ils exploitent les ressources du réseau pour se propager et infecter d'autres machines.

Différents types de virus réseau:

Il existe plusieurs types de virus réseau, tels que les vers, les chevaux de Troie et les ransomwares. Chaque type de virus a ses propres caractéristiques et peut causer différents types de dommages.

Exemples de virus réseau:

- **Ver Slammer**: Ce ver a exploité une vulnérabilité dans le service Microsoft SQL Server en 2003, infectant plus de 75 000 ordinateurs en quelques minutes.
- **Cheval de Troie Zeus**: Ce cheval de Troie a été utilisé pour voler des informations bancaires à des millions d'utilisateurs entre 2007 et 2011.
- **Ransomware WannaCry**: Ce ransomware a crypté les données de centaines de milliers d'ordinateurs dans le monde en 2017, exigeant une rançon en échange de la clé de décryptage.

Comment se protéger contre les virus réseau ?

- **Mettre à jour les logiciel**s: Il est important de maintenir tous les logiciels à jour, y compris le système d'exploitation, les navigateurs web et les logiciels antivirus.

- **Utiliser un pare-feu**: Un pare-feu peut bloquer les connexions non autorisées à votre ordinateur et empêcher les virus réseau de se propager.
- **Être prudent avec les emails** et les sites web: Ne cliquez pas sur les liens suspects et ne téléchargez pas de fichiers provenant de sources non fiables.
- **Utiliser un antivirus performant**: Un antivirus performant peut détecter et bloquer les virus réseau avant qu'ils ne puissent infecter votre ordinateur.

En résumé, les virus réseau sont un type de logiciel malveillant qui peut causer de graves dommages aux ordinateurs et aux réseaux. Il est important de prendre des mesures pour se protéger contre ces menaces en mettant à jour les logiciels, en utilisant un pare-feu, en étant prudent avec les emails et les sites web et en utilisant un antivirus performant.

2 – Comment detecter un virus

La présence d'un virus informatique peut être mise en évidence grâce à différents **signes**, parmi les suivants :

- **Modifications de votre page d'accueil**. Votre page d'accueil habituelle peut être modifiée, et vous amener vers un autre site Web.
- **Présente des fenêtres pop-up**. Ces pop-ups peuvent vous inciter à télécharger un nouvel antivirus ou un autre logiciel, ou vous mener vers des sites malveillants.
- **Accidents de disque dur fréquents**. La présence d'un virus peut également entraîner des dommages sur votre disque dur, pouvant causer l'arrêt de votre appareil, ou l'empêcher de se rallumer.
- **Envoi d'emails depuis votre messagerie**. Certains hackers peuvent se servir des virus pour prendre le contrôle de votre boîte de messagerie. Ils utilisent alors votre boîte mail pour envoyer des emails malveillants à d'autres cibles.
- **Ralentissement des performances de l'ordinateur**. Lors d'un changement soudain de la vitesse de fonctionnement de votre ordinateur, vous devrez vous alerter de la présence d'un virus.
- **Activités inhabituelles**. Toute activité inhabituelle peut aussi vous mettre la puce à l'oreille, comme le changement de mots de passe, technique qui vise à vous empêcher de vous connecter à votre appareil.
- **Présence de programmes inconnus**. Lorsque vous démarrez votre ordinateur, des programmes inconnus apparaissent, souvent sans explications.

3 – Comment eviter un virus malveillant

Les cybercriminels ont beaucoup appris au fil des années et il est plus difficile de prévoir d'où va venir le prochain virus. Si vous suivez ces six conseils, vous aurez une meilleure idée de la manière de reconnaître un virus sur Internet.

3 – 1 -Installez un logiciel antivirus

Appelons un chat un chat : si vous souhaitez éviter les virus sur Internet, un logiciel **antivirus** est une solution essentielle. Les cybermenaces ont évolué et les activités du quotidien telles que la gestion des opérations bancaires, les achats et la navigation sur Internet peuvent vous rendre plus vulnérable aux cybermenaces.
Les virus font partie des cybermenaces, c'est pourquoi il est essentiel de protéger votre appareil contre elles. Vous trouverez une fiche Asprom concernant les antivirus , qui decrits l'ensemble des antivirus disponibles avec leurs caractéristiques et niveaux de protection pour votre appareil, le tout dans une seule et même solution. Vous bénéficiez d'une protection contre les virus et les ransomwares, mais aussi contre le phishing et les autres menaces en ligne lorsque vous réalisez des opérations bancaires, effectuez des achats et naviguez en ligne.

3 – 2 - Méfiez-vous des pièces jointes

Les fournisseurs de messagerie comme Gmail et Outlook vous demandent la permission avant de télécharger une pièce jointe pour une bonne raison : elles peuvent être dangereuses. Si ces services ont souvent une protection antivirus intégrée à leur logiciel, les messages électroniques avec des virus en pièces jointes peuvent tout de même passer à travers leurs défenses.

Les cybercriminels qui cherchent à répandre un virus peuvent recourir à l'envoi d'un message spam avec une pièce jointe malveillante au plus grand nombre de personnes possible, en espérant que l'un des utilisateurs l'ouvrira. Une fois ouvert et exécuté, le virus s'installe immédiatement en arrière-plan et commence son travail.
Si vous ne connaissez pas la personne qui vous a envoyé une pièce jointe, ou si le message ressemble à une tentative de phishing, l'ignorer est probablement la meilleure option. Ne téléchargez les fichiers dans vos messages électroniques que si vous faites confiance à la source.
De même, désactivez les aperçus d'image dans votre logiciel de messagerie. Vous trouverez cette option dans les options ou réglages de votre programme. Certains virus peuvent s'attacher à des images et s'installer automatiquement dès que le message est ouvert. La configuration de vos réglages pour ne montrer que les images de source sûre peut permettre d'éviter qu'une imprudence ne se transforme en déclaration de virus.

3 – 3 - Appliquez les correctifs à votre système d'exploitation et vos applications

Les fournisseurs comme Microsoft et Adobe sortent régulièrement des mises à jour logicielles afin de rendre l'utilisation des ordinateurs ou logiciels plus sécurisée. Sans

elles, les cybercriminels peuvent exploiter ces failles de sécurité et forcer un appareil à télécharger un virus.
Ces vulnérabilités logicielles sont dissimulées dans les ordinateurs de nombreux utilisateurs qui font tout leur possible pour éviter les virus sur Internet. Le seul moyen de vous assurer que vous avez couvert ce risque est de régulièrement mettre votre logiciel à jour, à chaque fois qu'un correctif est disponible.

3 – 4 - Évitez les sites web douteux

Les gens passent beaucoup de temps à naviguer sur Internet. Selon un rapport d'Ofcom, une personne passe en moyenne un jour par semaine en ligne au Royaume-Uni.
Tout ce temps passé à rechercher le meilleure mème ou la prochaine série à regarder peut vous mener dans des endroits intéressants sur le web, mais parfois douteux. Il existe plus de 1,5 milliard de sites web dans le monde, et tous n'ont pas les meilleures intentions. Les sites malveillants utilisent une variété d'outils pour télécharger un virus sur votre ordinateur, comme les téléchargements non sollicités, l'hébergement de publicités malveillantes et les incitations à cliquer sur des liens trompeurs.
Évitez de cliquer sur les liens vers des sites web aux noms suspects, par exemple composés de mélange de lettres et de nombres qui ne ressemblent pas à des mots. Faites également attention aux sites web qui portent le même nom que des marques reconnues, telles que Norton ou Google, mais qui présentent une variation dans l'URL. S'il comporte quelques symboles supplémentaires, il y a des chances pour que le site web soit faux.

3 – 5 -Tenez-vous à distance des logiciels piratés

Nous ne sommes pas là pour discuter de questions morales autour du piratage de logiciel, qui consiste à obtenir une copie gratuite d'un jeu, d'un film ou d'une application pour laquelle tous les autres doivent payer. Le fait est que les gens qui téléchargent des versions piratées ou illégales de logiciels devraient savoir que cela présente des risques pour leur ordinateur.
Les logiciels piratés proviennent soit de sites web difficiles à trouver, soit du partage de pair à pair, qui attirent aussi bien ceux qui cherchent simplement leur film préféré que ceux qui cherchent à répandre un virus.
Sans une protection antivirus intégrée au contenu téléchargé, il est facile pour un cybercriminel de glisser un virus dans une application gratuite. Parfois, le logiciel gratuit n'est même pas présent dans le contenu téléchargé qui contient juste un virus.

Faites preuve de prudence lorsque vous téléchargez quelque chose de gratuit et, si vous téléchargez malgré tout des fichiers piratés, assurez-vous d'utiliser un logiciel antivirus.

3 – 6,- Sauvegardez votre ordinateur

En effectuant régulièrement une sauvegarde cloud, vous pouvez garder des copies de tous vos fichiers et dossiers importants dans un emplacement qui ne sera pas touché par le virus. Ainsi, si vous êtes victime d'un virus informatique dont il est difficile de se débarrasser sans endommager vos fichiers, vous pouvez simplement effacer le contenu de votre appareil et le restaurer au point le plus récent avant l'infection.
Assurez-vous d'opter pour un forfait de sauvegarde cloud suffisant pour ne rien laisser de côté. La Sauvegarde cloud pour PC, qui est comprise dans les solutions d'antivirus de qualité peut prendre en charge jusqu'à 75 gigaoctets de fichiers. Cela est plus que suffisant pour permettre à la plupart des gens de stocker leurs dossiers personnels et financiers en toute sécurité.

3 – 7 – Conseils évidents

1 -Ne pas répondre aux e-mails indésirables ou spontanés.

2- Ne rien acheter qui a été recommandé par un e-mail indésirable.

3- Ne jamais cliquer sur les liens d'e-mails pressants.

4- Ne jamais répondre à un e-mail demandant des informations personnelles ou confidentielles.

5- Savoir que sa banque ne demandera jamais d'informations personnelles par e-mail.

6- Utiliser des mots de passe compliqués (mélanges de chiffres et de lettres, de minuscules et de majuscules).

7- Utiliser des mots de passe différents pour chacun de ses comptes.

8- Ne jamais enregistrer ses mots de passe sur des ordinateurs étrangers.

9- Ne pas installer de programmes suggérés.

10- Ne pas utiliser n'importe quel USB tombant sous la main.

11- Verrouiller l'accès à son ordinateur.

12- Protéger l'accès à son smartphone et le configurer pour qu'il s'autoverrouille.

13- Considérer comme "spam" toutes les demandes d'inconnus sur les réseaux sociaux.

14- Se méfier des bannières sur les sites web clamant que l'on est "le millionième visiteur" ou le vainqueur d'un "prix incroyable".

4 - Comment de debarasser d'un virus

Les virus informatiques sont presque toujours invisibles. Sans protection antivirus, il se peut que vous ne sachiez pas que vous avez un. C'est pourquoi il est essentiel d'installer une protection antivirus sur tous vos appareils.

Si votre PC est infecté par un virus, suivre ces **dix étapes simples** vous aidera à vous en débarrasser **:**

Étape 1 : Télécharger et installer un scanner antivirus

Téléchargez un scanner antivirus ou une solution de sécurité Internet complète. Nous vous recommandons de consulter le docuùent virus de l'asprom.

Étape 2 : Se déconnecter d'Internet

Lorsque vous supprimez un virus de votre PC, il est judicieux de vous déconnecter d'Internet afin de prévenir d'autres dommages : certains virus informatiques utilisent la connexion Internet pour se propager**.**

Étape 3 : Redémarrer votre ordinateur en mode sans échec

Pour protéger votre ordinateur pendant que vous supprimez le virus, redémarrez-le en mode sans échec. Vous ne savez pas comment procéder ?

Voici des indications simples :

- Éteignez votre ordinateur et rallumez-le.
- Lorsque l'écran s'allume, appuyez sur F8 pour faire apparaître le menu « Options de démarrage avancées ».
- Cliquez sur « Mode sans échec avec prise en charge réseau ».
- Restez déconnecté d'Internet**.**

Étape 4 : Supprimer les fichiers temporaires

Ensuite, vous devez supprimer tous les fichiers temporaires en utilisant l'option de nettoyage du disque.

Voici comment procéder :

- Cliquez sur « Démarrer ».
- Sélectionnez « Tous les programmes ».
- Cliquez sur « Accessoires ».
- Choisissez « Outils système ».
- Choisissez « Nettoyage du disque ».
- Recherchez « Fichiers temporaires » dans la liste « Fichiers à supprimer ».
- Sélectionnez « Fichiers temporaires » pour les supprimer.

Certains virus sont programmés pour se lancer lorsque votre ordinateur démarre. La suppression des fichiers temporaires peut entraîner la suppression du virus. Toutefois, vous ne pouvez pas vous contenter de cela. Pour assurer la suppression des virus sur votre ordinateur, il est prudent d'effectuer les étapes suivantes.

Étape 5 : Lancer une analyse antivirus

C'est le moment de lancer une analyse antivirus à l'aide de l'antivirus de votre choix ou d'un logiciel de sécurité Internet.,

sélectionnez et exécutez « Scan » (Analyser).

Étape 6 : Supprimer ou mettre en quarantaine des virus

Si un virus est découvert, il peut affecter plusieurs fichiers. Sélectionnez « Supprimer » ou « Quarantaine » pour supprimer le ou les fichiers et vous débarrasser du virus. Effectuez une nouvelle analyse de votre ordinateur pour vérifier qu'il n'y a pas d'autres menaces. Si des menaces sont détectées, supprimez les fichiers ou mettez-les en quarantaine.

Étape 7 : Redémarrer votre ordinateur

Maintenant que le virus est supprimé, vous pouvez redémarrer votre ordinateur. Il vous suffit de l'allumer comme vous le feriez normalement. Le mode sans échec n’est plus nécessaire.

Étape 8 : Modifier tous vos mots de passe

Pour protéger votre ordinateur contre de nouvelles attaques, modifiez tous vos mots de passe au cas où ils auraient été compromis. C'est strictement nécessaire uniquement si vous avez des raisons de croire que vos mots de passe ont été capturés par un programme malveillant, mais mieux vaut prévenir que guérir.
Vous pouvez toujours vérifier le mode de fonctionnement du virus sur le site Web de votre fournisseur antivirus, ou auprès de son équipe d'assistance technique si vous n'êtes pas sûr.

Étape 9 : Mettre à jour votre logiciel, votre navigateur et votre système d'exploitation

La mise à jour de votre logiciel, du navigateur et du système d'exploitation permettra de limiter le risque que des failles dans le code ancien ne soient exploitées par des criminels pour installer des programmes malveillants sur votre ordinateu

Suppression d'un virus informatique sur un Mac

Si vous utilisez un Mac, vous avez peut-être l'impression que votre ordinateur ne peut pas être infecté par un virus. Malheureusement, c'est une idée reçue. Les virus qui ciblent les Mac sont beaucoup moins nombreux que ceux qui ciblent les PC, mais ils existent.

Certains virus Mac sont conçus pour piéger les utilisateurs en se faisant passer pour des produits antivirus. Si vous avez accidentellement téléchargé un virus de ce type, votre ordinateur peut être infecté. Voici trois exemples de virus Mac de ce type : « MacDefender », « MacProtector », et « MacSecurity ».

Si vous pensez que votre Mac est infecté par un virus, voici les six étapes à suivre pour le supprimer :

1. Fermez l'application ou le logiciel qui semble être affecté(e).
2. Accédez au « Moniteur d'activité » et recherchez des virus Mac connus, comme « MacDefender », « MacProtector » et « MacSecurity ».
3. Si vous découvrez l'un de ces virus, cliquez sur « Quitter l'opération » avant de fermer le « Moniteur d'activité ».
4. Ensuite, accédez à votre dossier « Applications » et faites glisser le fichier dans votre corbeille.
5. N'oubliez pas de vider le dossier « Corbeille » par la suite pour supprimer définitivement le virus.
6. À présent, assurez-vous que vos logiciels et applications sont à jour pour bénéficier des derniers correctifs de sécurité.

5- Historique des virus informatiques

5– 1 - historique

Les virus informatiques existent depuis presque aussi longtemps que les ordinateurs eux-mêmes. Le premier virus, **Creeper**, a été créé en 1971 par Bob Thomas, un chercheur chez BBN. Creeper était un programme inoffensif qui se propageait d'un ordinateur à l'autre sur le réseau ARPANET, ancêtre d'Internet.

Le premier virus malveillant, **Elk Cloner**, a été créé en 1982 par Richard Skrenta, un adolescent de 15 ans. Elk Cloner infectait les disquettes Apple II et s'affichait à l'écran lorsque l'utilisateur démarrait son ordinateur.

Dans les années 1980 et 1990, les virus informatiques sont devenus de plus en plus nombreux et sophistiqués**. Certains virus, comme **Michelangelo** et **Chernoby**l, ont causé des dommages importants aux ordinateurs du monde entier.

L'apparition d'Internet a contribué à la propagation des virus informatiques. Les virus peuvent désormais se propager d'un ordinateur à l'autre en quelques secondes par le biais de courriels, de pièces jointes et de sites Web infectés.

Aujourd'hui, les virus informatiques constituent une menace majeure pour la sécurité informatique. Les entreprises et les particuliers doivent utiliser des logiciels antivirus et des pratiques de sécurité informatique pour se protéger contre les virus.

Voici quelques dates importantes dans l'histoire des virus informatiques:

1971: Bob Thomas crée **Creepe**r, le premier virus informatique. le virus Creeper est détecté sur ARPANET, un réseau informatique de l'armée américaine,

prédécesseur d'Internet. Programmé pour Tenex, un système d'exploitation populaire à l'époque, ce virus est capable d'accéder seul à un système distant via un modem et de s'y copier. Les systèmes infectés affichent alors le message : « I'M THE CREEPER : CATCH ME IF YOU CAN. »

1974,,Un virus baptisé **Rabbit** fait son apparition : il doit son surnom de Rabbit (lapin) au simple fait qu'il ne faisait rien d'autre que de se multiplier et de se propager aux autres machines. Ce nom fait allusion à la vitesse à laquelle ce programme se multiplie. Il encombre le système avec ses propres copies, ce qui nuit aux performances. Une fois que Rabbit avait atteint un certain niveau sur une machine infectée, le virus plantait.

1975 .**Pervading Animal**, un autre jeu écrit cette fois-ci pour un Univac 1108 apparaît en 1975. Les experts d'aujourd'hui se demandent encore s'il s'agissait d'un autre virus ou du premier cheval de Troie.

1982: Richard Skrenta crée **Elk Cloner**, le premier virus malveillant. Elk Cloner se propage en infectant le système d'exploitation d'Apple II enregistré sur des disquettes. Lors du démarrage de l'ordinateur au départ d'une disquette infectée, une copie du virus démarre automatiquement. Le virus n'interfère pas avec le fonctionnement de l'ordinateur, si ce n'est qu'il contrôle l'accès au disque. En cas d'accès à une disquette saine, le virus se copie sur celle-ci afin de l'infecter. Ainsi, le virus se propage petit à petit, de disquette en disquette.

1983 Len Eidelmen utilise le terme » virus » la première fois pour désigner un programme informatique qui se reproduit automatiquement. Le 10 novembre 1983, lors d'un séminaire sur la sécurité informatique organisé à l'université de Lehigh, l'aïeul de la virologie informatique moderne réalise une démonstration avec un programme semblable à un virus sur un système VAX11/750.

1986: Le virus **Brain** infecte les disquettes 5,25 pouces. C'est cette année que la première épidémie de virus compatible avec IBM est détectée. Brain, qui infecte le secteur d'amorçage, se répand dans le monde entier en l'espace de quelques mois. Le succès de Brain peut s'expliquer par le fait que la communauté informatique n'avait aucune idée de ce qu'était un virus. En fait, la diffusion d'un nombre d'ouvrages de science-fiction sur le sujet ne fit que renforcer la sensation de panique au lieu d'informer les gens sur la sécurité.

1988 : **Morri**s

Nommé en l'honneur de son créateur Robert Morris et considéré comme le premier ver informatique, Morris exploitait les vulnérabilités des commandes Unix (sendmail, rsh et finger). Bien que Morris aurait pu causer d'énormes dégâts, il n'a en fait rien détruit, puisque Robert Morris voulait simplement découvrir la taille et la portée d'Internet.

1991: Le virus **Michelangelo** infecte les ordinateurs du monde entier.

Il a été configuré pour s'activer le 6 mars de chaque année, date à laquelle il écraserait les 100 premiers secteurs sur les périphériques de stockage avec des zéros - les empêchant de démarrer. Pourquoi le 6 mars? Parce que c'était l'anniversaire de Michaelangelo (l'artiste).

1999: **Le virus *Chernobyl*** cause des dommages importants aux ordinateurs du monde entier. Créé par l'étudiant taiwanais Chen Ing-hau, CIH a infecté 60 millions d'ordinateurs dans le monde, causant (selon le Dr Evil voice) 1 milliard de dollars de dégâts]. Conçu pour infecter les ordinateurs utilisant les systèmes d'exploitation MS-Windows 9x, CIH a écrasé les informations cruciales et, dans certains cas, détruit le BIOS.

1999 : **Melissa.** À la veille du nouveau millénaire,], de nombreuses personnes dans le monde paniquaient à cause du virus Melissa. Ce virus envoyait des mots de passe pour des adhésions érotiques aux 50 premières personnes du carnet d'adresses Outlook d'une victime. Les choses sont devenues tellement incontrôlables que les serveurs de messagerie se sont écrasés à cause du trafic. Ça, c'est sans parler des coups de fil malaisants de grand-maman et grand-papa…

2000: Le virus **ILOVEYOU** se propage par le biais de courriels Vous souvenez-vous du dinosaure mauve nommé Barney, qui chantait: « I love you, you love me »?, en 2000, beaucoup de gens ne ressentaient pas ce sentiment d'amour envers la chanson, merci à un ver informatique appelé iloveyou, qui a infecté des millions de machines Windows dans le monde en quelques heures. Parce qu'il s'est propagé par le biais d'un courriel chargé de logiciels malveillants avec pour objet « ILOVEYOU », il est considéré comme l'un des premiers virus mondiaux à utiliser des techniques d'ingénierie sociale..

2004 : **Netsky**. Créé par Sven Jaschan en juin 2004, Netsky comptait 29 variantes qui ont provoqué de nombreuses attaques DDoS. Le ver informatique s'est

propagé par courriel et se copiait sur le disque dur local de la victime, ainsi que sur les lecteurs réseau mappés (si disponibles).

2001 : **Nimda**. Alors que les gens pensaient qu'il était sécuritaire de naviguer sur le Web, Nimda a infecté des milliers d'ordinateurs dans le monde grâce à une vulnérabilité dans Windows. Nimda a également ciblé les serveurs Internet et a entraîné un ralentissement des performances et, dans certains cas, un arrêt complet.

2004 : **MyDoom**. 2004 n'a pas été une bonne année pour les attaques DDoS, et MyDoom était une autre menace massive. Le ver a atteint des milliers d'ordinateurs par les réseaux P2P et les courriels. À l'époque, c'était le ver de messagerie le plus rapide de l'histoire.

2004: Le virus **Sasser** infecte les ordinateurs Windows.

Vous vous souvenez de Sven Jaschan et de la renommée (ou de l'infamie) de Netsky? Eh bien, en 2004, Jaschan était occupé à créer le ver informatique Sasser. Contrairement à Netsky, ce virus ne se propageait pas par courriel. Il se stationnait plutôt dans une machine infectée à la recherche d'autres systèmes vulnérables. Une fois les systèmes trouvés, il contactait ces systèmes et leur disait de télécharger le viru

2009: Le virus **Conficke**r infecte des millions d'ordinateurs dans le monde.

Tirant son nom des mots « configuration » et « ficker » (l'équivalent d'un juron en allemand), le ver informatique Conficker a exploité les vulnérabilités de Windows et a utilisé le dictionnaire standard pour casser les mots de passe administrateur. Conficker a infecté des millions d'ordinateurs dans plus de 200 pays et n'a épargné personne

2010 : **Stuxnet**. Considéré comme la première cyberarme publique, Stuxnet est soupçonné (mais ça n'a pas été prouvé) d'avoir été créé par les gouvernements américain et israélien pour attaquer des installations nucléaires en Iran.

2011 : **Gameover ZeuS** (GOZ). On estime qu'un million d'ordinateurs Windows ont été infectés par Gameover ZeuS, qui était principalement utilisé pour voler des informations bancaires. Le même maliciel que celui dans Gameover ZeuS a été utilisé dans la première attaque de rançongiciel connue,

2012 : **Flame**. Lorsque Flame a été lancé au début de 2012, certains experts le considéraient comme le logiciel malveillant le plus complexe jamais créé en

raison de sa capacité à enregistrer le trafic réseau, les captures d'écran, l'activité du clavier, l'audio et même les conversations Skype

2015 : **BASHLITE**. Initialement appelé Bashdoor, BASHLITE a infecté des systèmes Linux dans le monde entier et a lancé des attaques DDoS qui ont atteint un niveau incroyable de 400 gigaoctets par seconde. Holy speed, Batman!

016 : MEMZ, Locky, Tiny Banker et Mirai. Tout comme il y a des millésimes pour les bons vins, 2016 a été (malheureusement) un millésime pour les virus. Il y avait d'abord le cheval de Troie MEMZ avec ses symptômes inhabituels (comme déplacer légèrement le curseur de la souris). Ensuite, il y a eu le rançongiciel Locky, suivi du cheval de Troie Tiny Banker (alias Timba) qui ciblait des dizaines de grandes banques aux États-Unis.

2017/2018 : **WannaCry**, Petya, Xafecopy et Kedi RAT. Le rançongiciel WannaCry a effectivement fait pleurer des millions de personnes dans le monde. Il a infecté plus de 200 000 machines dans plus de 150 pays et accumulé des centaines de millions de dollars en rançon. Petya, un autre rançongiciel crypté, a causé environ 10 milliards de dollars de dommages dans le monde.

2020: La pandémie de COVID-19 a conduit à une augmentation du nombre de cyberattaques, y compris les ransomwares.

Les virus informatiques sont une menace constante pour la sécurité informatique. Il est important de rester vigilant et de prendre des mesures pour se protéger contre les virus.

5– 2 – Top 10 des pires virus

1- I LOVE YOU

I love you est le virus considéré comme le plus marquant de l'histoire. Se propageant par la messagerie Microsoft Outlook, il envoyait de nombreux mails sous forme de déclarations d'amour aux utilisateurs Outlook, infectant instantanément leur ordinateur en renommant tous les fichiers contenus dedans. Le virus a touché environ 10% des ordinateurs connectés à Internet dans le monde pour un coût estimé à 5 milliards de dollars.

2- CRYPTOLOCKER

C'est un cheval de Troie apparu en 2003 qui s'attaque aux ordinateurs sous Windows : une fois introduit dans les machines, il crypte les données et demande une rançon pour pouvoir les récupérer.

3- JIGSAW

C’est un rançongiciel inspiré de la marionnette des films d’horreur « Saw ». Personne ne sait à ce jour comment le virus s’introduit dans les ordinateurs, mais nous savons qu’il n’infecte qu’en passant par Windows. Comme Cryptolocker, il crypte les fichiers de l’ordinateur et exige une rançon. Des fichiers sont supprimés toutes les heures si vous ne payez pas. Fort heureusement, des chercheurs ont réussi à créer une clé pour décrypter ses fichiers.

4- PETYA

Encore un rançongiciel, mais celui-ci ne s’attaque pratiquement qu’aux services de ressources humaines des entreprises en dissimulant un malware dans un CV en pièce jointe. Il prend ensuite le contrôle total de l’ordinateur et demande une rançon.

5- LOCKY

C’est lui aussi un rançongiciel spécifique à Windows qui se diffuse par email. Il a fait beaucoup de victimes en Allemagne et en France. Il a la spécificité de se déplacer dans le réseau de l’entreprise et d’infecter tous les ordinateurs.

6- HEARTBLEED

Celui-ci n’est pas vraiment un virus, c’est plutôt une vulnérabilité logicielle. Cette faille présente dans la bibliothèque OpenSSL depuis mars 2012 permettait à un cybercriminel de récupérer certaines données d’un serveur ou d’un ordinateur spécifique. Quand on a découvert cette faille, environ 500 000 serveurs étaient déjà touchés !

7- FREAK

Freak est une faiblesse cryptographique situé dans le protocole SSL/TLS utilisé pour l’HTTPS. C’est une ancienne faille introduite par la NSA qui lui permettait de casser le chiffrement RSA avec moins de 512 bits.

8- REGIN

Ringin est un malware de cyber espionnage ciblant avant tout les grandes organisations. Il permettait de voler des mots de passe, faire des captures d’écran ou de prendre carrément le contrôle d’un ordinateur dans le but d’espionner ces grandes organisations.

9- WALEDAC

Waledac est un ver qui se transmettait dans la pièce jointe d’un email. Ce ver pouvait envoyer jusqu’à 1,5 milliards de messages par jour ! Même si Microsoft a rapidement combattu ce virus, on estime qu’environ plus 1 million d’ordinateurs zombie sont restés infectés depuis.

10- CABIR

C’est le premier malware à infecter les appareils mobiles. Pour se répandre, il utilisait Bluetooth. Il n’était pas néfaste car il était utilisé en test, mais il s’est répandu très rapidement via cet ingénieux moyen.

6 – Scanner un virus

Voici les deux principales méthodes que vous pouvez utiliser :

6-1. Utilisez un scanner antivirus :

Si vous avez un PC Windows :

Vous pouvez utiliser l’antivirus Windows Defender intégré. Pour analyser votre ordinateur, ouvrez le menu Démarrer, tapez « Sécurité », puis cliquez sur « Sécurité Windows ».« Cliquez sur « Protection contre les virus et les menaces », puis sur « Analyse rapide."

Vous pouvez également utiliser un scanner antivirus tiers, tel qu’Avast, Bitdefender ou Kaspersky. Ces scanners antivirus proposent généralement un essai gratuit, vous pouvez donc les essayer avant de les acheter.

Si vous avez un Mac :

Vous pouvez utiliser l’antivirus macOS intégré, appelé XProtect. XProtect analyse automatiquement votre Mac à la recherche de logiciels malveillants, vous n’avez donc rien à faire pour l’activer.

Vous pouvez également utiliser un scanner antivirus tiers, tel qu’Avast, Bitdefender ou Kaspersky

.

6-2-. Utilisez un scanner en ligne :

Les scanners de virus en ligne sont une bonne option si vous n’avez pas d’antivirus installé sur votre ordinateur, ou si vous souhaitez analyser un fichier ou un site Web spécifique.

Il existe de nombreux scanners de virus en ligne gratuits, tels que VirusTotal et Metadefender.

Pour utiliser un antivirus en ligne, il suffit de télécharger le fichier ou d’entrer l’URL du site Web que vous souhaitez analyser. Le scanner analysera ensuite le fichier ou le site Web à la recherche de logiciels malveillants.

Voici quelques conseils supplémentaires pour la recherche de virus :

- **Maintenez votre scanner antivirus à jour**. Les scanners antivirus sont constamment mis à jour pour détecter les nouvelles menaces de logiciels malveillants, il est donc important de garder votre scanner à jour.
- **Analysez régulièrement votre ordinateur**. C'est une bonne idée d'analyser votre ordinateur à la recherche de virus au moins une fois par semaine.
- **Faites attention à ce sur quoi vous cliquez**. Ne cliquez pas sur des liens et n'ouvrez pas de pièces jointes provenant d'expéditeurs inconnus.
- **Faites attention à ce que vous téléchargez**. Ne téléchargez que des fichiers provenant de sources fiables.

Principaux scanner en ligne :

1. Scanneur de vulnérabilités connues **SafetyDetectives** – Meilleur scanner en ligne global.

2**. VirusTotal** – Compare les résultats de plus de 70 antivirus pour analyser vos fichiers individuels.

3. **Norton Power Eraser** — Version de base du meilleur antivirus avec détection à 100 % des malware.

4. **ESET Online Scanner** — Analyses complètes et très approfondies du système.

5. **Bitdefender Virus Scanner for Mac** —

Meilleur scanner léger pour les utilisateurs de Mac.

- **Prime. Norton 360** — Meilleur antivirus global en 2024.
- **Prime. Bitdefender Total Security** — Protection avancée + large éventail de fonctionnalités.

6 – 3 – Scanner en ligne pour USB

Virus USB : Deux choses à savoir

Vous utilisez peut-être tous des périphériques USB pour vous connecter au système informatique, car ils sont très utiles pour transférer des données d'un PC à un autre. Mais une utilisation importante est le stockage de données précieuses, de chansons ou de vidéos.

Cependant, ce que beaucoup de gens ne savent pas, c'est que, lorsque vous branchez la clé USB sur un système infecté, le virus se déplace et infecte d'autres PC.

Il arrive donc un moment où le lecteur USB infecté fait planter tout le système. Le système ne fonctionnera pas à cause de l'attaque du virus. C'est pourquoi vous avez besoin d'un outil d'analyse des virus USB. Avant de commencer à analyser les virus sur votre PC, vous devez comprendre deux choses sur le virus USB.

Question 1 : Les clés USB peuvent-elles véhiculer des virus ?

Oui, les clés USB **sont porteuses de virus** et peuvent infecter plusieurs systèmes. Certains virus ne se transmettent que par les clés USB. Ainsi, chaque fois que vous utilisez une clé USB infectée sur un autre système, ce dernier est automatiquement infecté. Essayez d'éviter d'utiliser les clés USB d'utilisateurs tiers. Vous pouvez également utiliser un outil antivirus fiable pour analyser le lecteur flash USB.

Question 2 : Comment vous assurer que votre clé USB est sûre ?

Certains virus et fichiers malveillants sont transférés par des clés USB vers un système PC. Petit à petit, les fichiers du système seront affectés et votre système commencera à se comporter bizarrement. Chaque fois que vous branchez une clé USB sur un port, ve10 meilleurs scanners de virus USB à essayer

les 10 meilleurs logiciels pour scanner les clés USB :

- Adaware Live CD
- Panda USB Vaccine
- ESET SysRescue
- Bitdefender USB Immunizer
- Kaspersky Free Rescue Disk
- USB Threat Defender
- USB Disk Security
- Avast
- BullGuard
- McAfee VirusScan

Annexe ; bibliographie

- https://www.proofpoint.com/fr/threat-reference/computer-virus
- https://www.kaspersky.fr/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store
- https://www.pandasecurity.com/fr/mediacenter/virus-informatiques-top-10/
- https://encyclopedia.kaspersky.fr/knowledge/history-of-malicious-programs/#:~:text=Les%20premiers%20virus
- https://blog.devolutions.net/fr/2019/04
- https://nordvpn.com/fr/blog/un-virus-informatique/
- https://fr.norton.com/blog/how-to/avoid-getting-a-virus-on-the-internet
- https://www.lemondeinformatique.fr/actualites/lire-15-recommandations-pour-eviter-les-virus-53055.html
- https://www.kaspersky.fr/resource-center/threats/how-to-get-rid-of-a-computer-virus
- https://recoverit.wondershare.fr/usb-tips/bootable-usb-virus-scanners.html?source=8