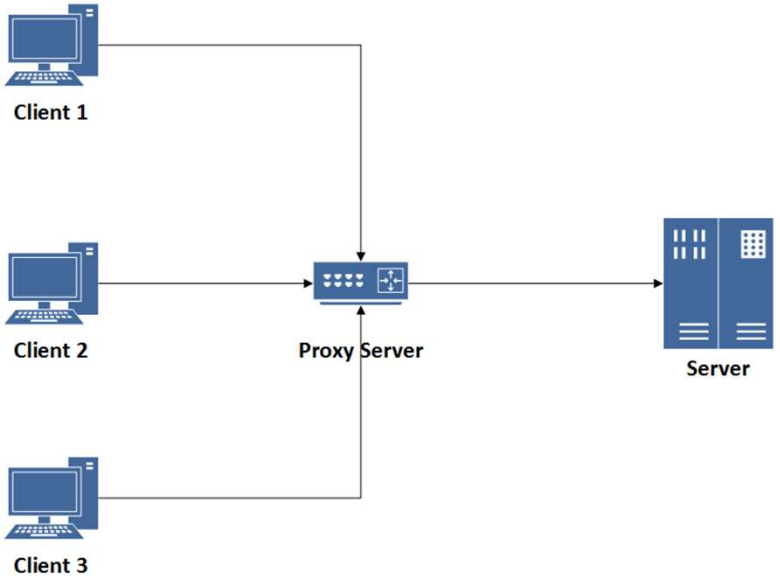
Sécurisation Client Windows

Proxy



Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges. Il sert d'intermédiaire pour accéder à un autre réseau, généralement Internet.

Par extension, on appelle aussi « proxy » un matériel comme un serveur mis en place pour assurer le fonctionnement de tels services.

Fonction

L'utilité des serveurs proxys est importante, notamment dans le cadre de la sécurisation des systèmes d'information.

Par exemple, il est presque systématique en entreprise ou dans les établissements scolaires que l'accès Internet se fasse à travers un serveur proxy.

L'internaute ne voit pas la différence, sauf quand il tente de naviguer sur un site interdit, auquel cas il pourra recevoir un message d'erreur : un tel proxy est appelé proxy filtrant.

Il se peut aussi qu'une boite de dialogue s'ouvre et demande un identifiant et un mot de passe avant de pouvoir surfer sur Internet.

Un proxy peut aussi servir à contourner les filtrages.

Supposons le cas d'un pays qui bloque l'accès à certains sites considérés comme « subversifs », mais qui effectue ce filtrage uniquement en se basant sur l'adresse du site que l'on souhaite visiter.

Dans ce cas, en utilisant un proxy comme intermédiaire (situé dans un autre pays donc non affecté par le filtrage), on peut s'affranchir du filtrage (sauf bien sûr si l'adresse du proxy est elle-même interdite).

Le principe fonctionne également dans l'autre sens.

Supposons qu'un site web n'accepte que les internautes d'un certain pays (exemple concret : un site de campagne présidentielle américain qui n'accepte que les connexions venant des États-Unis).

Dans ce cas, en passant par un proxy situé aux États-Unis, un internaute français pourra visiter le site.

Un troisième rôle du proxy est de compliquer la remontée vers l'internaute (anonymisation) .

Dans l'exemple précédent, on a trompé le site américain qui n'était pas capable de remonter jusqu'à l'internaute à travers le proxy.

Certaines techniques avancées permettent de remonter à travers le proxy.

Dans ce cas, un internaute pourra utiliser de nombreux proxys en chaîne comme le réseau Tor et stopper la connexion avant que ceux qui le ne soient appréhendé.

Anti-virus

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique ne sont qu'une catégorie).

Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation).

Fonctionnement

Un logiciel antivirus vérifie les fichiers et courriers électroniques, les secteurs de démarrage (afin de détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.), les données qui transitent sur les éventuels réseaux (dont internet), etc.

Différentes méthodes sont possibles :

- les principaux antivirus du marché se concentrent sur des fichiers et comparent alors la signature virale du virus aux codes à vérifier ;
- la méthode heuristique est la méthode la plus puissante, tendant à découvrir un code malveillant par son comportement. Elle essaie de le détecter en analysant le code d'un programme inconnu. Parfois de fausses alertes peuvent être provoquées ;
- l'analyse de forme repose sur du filtrage basé entre des règles regexp ou autres, mises dans un fichier junk. Cette dernière méthode peut être très efficace pour les serveurs de messagerie électronique supportant les regexp type postfix puisqu'elle ne repose pas sur un fichier de signatures.

Les antivirus peuvent balayer le contenu d'un disque dur, mais également la mémoire vive de l'ordinateur. Pour les antivirus les plus modernes, ils agissent en amont de la machine en scrutant les échanges de fichiers avec l'extérieur, aussi bien en flux descendant (téléchargement) que montant (téléversement ou upload).

Ainsi, les courriels sont examinés, mais aussi les fichiers copiés sur ou à partir de supports amovibles tels que cédéroms, disquettes, connexions réseau, clefs USB…

Les Méthodes d’analyses

Dictionnaire

Les créateurs de logiciels antivirus ayant préalablement identifié et enregistré des informations sur des virus, comme le ferait un dictionnaire, le logiciel antivirus peut ainsi détecter et localiser la présence d’un virus.

On appelle ce dictionnaire la base de définition virale qui contient les signatures de virus.

Lorsque cela se produit, l'antivirus dispose de trois options, il peut :

- effectuer la suppression du fichier contaminé ;
- tenter de réparer le fichier endommagé en éliminant le virus ;
- déplacer le fichier dans une zone de quarantaine afin qu’il ne puisse être accessible aux autres utilisateurs et logiciels. Ceci permet d'éviter que le virus se répande (par autoréplication), et permet éventuellement de réparer le fichier ultérieurement.

Afin de maximiser le rendement de l'antivirus, il est essentiel d’effectuer de fréquentes mises à jour en téléchargeant des versions plus récentes. Des internautes consciencieux et possédant de bonnes connaissances en informatique peuvent identifier eux-mêmes des virus et envoyer leurs informations aux créateurs de logiciels antivirus afin que leur base de données soit mise à jour.

Généralement, les antivirus examinent chaque fichier lorsqu'il est créé, ouvert, fermé ou lu. De cette manière, les virus peuvent être identifiés immédiatement. Il est possible de programmer le système d’administration pour qu’il effectue régulièrement un examen de l'ensemble des fichiers sur l'espace de stockage (disque dur, etc).

Les Méthodes d’analyses

Liste blanche

La « liste blanche » est une technique de plus en plus utilisée pour lutter contre les logiciels malveillants.

Au lieu de rechercher les logiciels connus comme malveillants, on empêche l'exécution de tout logiciel à l'exception de ceux qui sont considérés comme fiables par l'administrateur système.

En adoptant cette méthode de blocage par défaut, on évite les problèmes inhérents à la mise à jour du fichier de signatures virales. De plus, elle permet d'empêcher l'exécution de logiciels indésirables.

Étant donné que les entreprises modernes possèdent de nombreuses applications considérées comme fiables, l'efficacité de cette technique dépend de la capacité de l'administrateur à établir et mettre à jour la liste blanche.

Cette tâche peut être facilitée par l'utilisation d'outils d'automatisation des processus d'inventaire et de maintenance.

Les Méthodes d’analyses

Comportements suspects

Une autre approche pour localiser les virus consiste à détecter les comportements suspects des programmes.

Par exemple, si un programme tente d’écrire des données sur un programme exécuté, modifier/supprimer des fichiers système l’antivirus détectera ce comportement suspect et en avisera l’utilisateur qui choisira les mesures à suivre.

Contrairement à l’approche précédente, la méthode du comportement suspect permet d’identifier des virus très récents qui ne seraient pas encore connus dans le dictionnaire de l'antivirus.

L'intelligence artificielle des nouveaux antivirus leur permet de choisir la décision à prendre sans en avertir l'utilisateur, ce qui permet d'utiliser à nouveau cette méthode.

De plus les filtres se sont considérablement améliorés et les faux positif sont moins nombreux.

Les Méthodes d’analyses

L’analyse heuristique

Utilisée par quelques antivirus.

Par exemple, l’antivirus peut analyser le début de chaque code de toutes les nouvelles applications avant de transférer le contrôle à l’usager. Si le programme semble être un virus, alors l’usager en sera averti.

Toutefois, cette méthode peut également mener à de fausses alertes.

La méthode heuristique permet de détecter des variantes de virus et, en communiquant automatiquement les résultats de l'analyse à l'éditeur, celui-ci peut en vérifier la justesse et mettre à jour sa base de définitions virales.

Les différents types de virus

Il existe une grande quantité de virus aussi différents les uns que les autres :

- Virus Informatique
- Vers
- Adware
- Spyware (Logiciel espion)
- Ransomware
- Robot (ou Botnet)
- Rootkits
- Trojan (Cheval de troie)

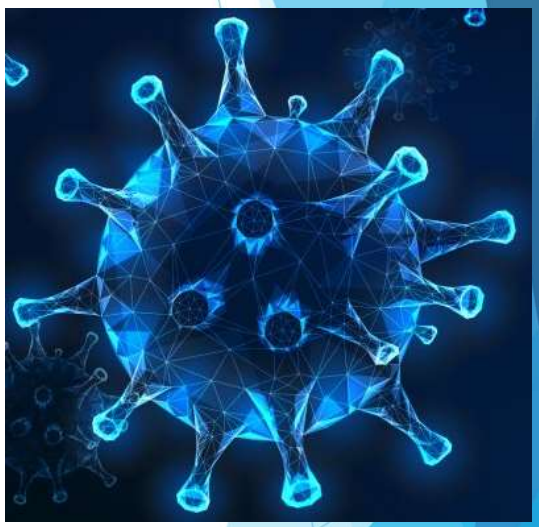
Virus Informatiques

Les virus informatiques ont acquis ce nom en raison de leur capacité à «infecter» plusieurs fichiers sur un ordinateur.

Ils se propagent sur les autres machines lorsque des fichiers infectés sont envoyés par e-mail ou lorsque des utilisateurs les transportent sur des supports physiques tels que des clés USB ou des disquettes (au début).

Selon le National Institute of Standards and Technology (NIST), le premier virus informatique, appelé « Brain », a été développé en 1986.

Lassés de voir les clients pirater les logiciels de leur magasin, deux frères(Amjad Farooq Alvi et Basit Farooq Alvi) prétendent avoir conçu le virus permettant d'infecter le secteur d'amorçage des disquettes des voleurs, propageant ainsi le virus lors de leur copie.



Vers

Contrairement aux virus, les vers ne nécessitent pas d'intervention humaine pour se propager et infecter les ordinateurs.

Un vers est un programme capable d'utiliser des réseaux informatiques pour infecter les autres machines connectées sans l'aide des utilisateurs.

En exploitant les vulnérabilités des réseaux telles que les failles des programmes de messagerie électronique, les vers peuvent se répliquer des milliers de fois en vue d'infecter de nouveaux systèmes dans lesquels le processus se reproduira. Bien que de nombreux vers utilisent simplement les ressources système, réduisant ainsi les performances.

La plupart d'entre eux contiennent des «charges utiles» malveillantes conçues pour dérober ou supprimer des fichiers.

Adware

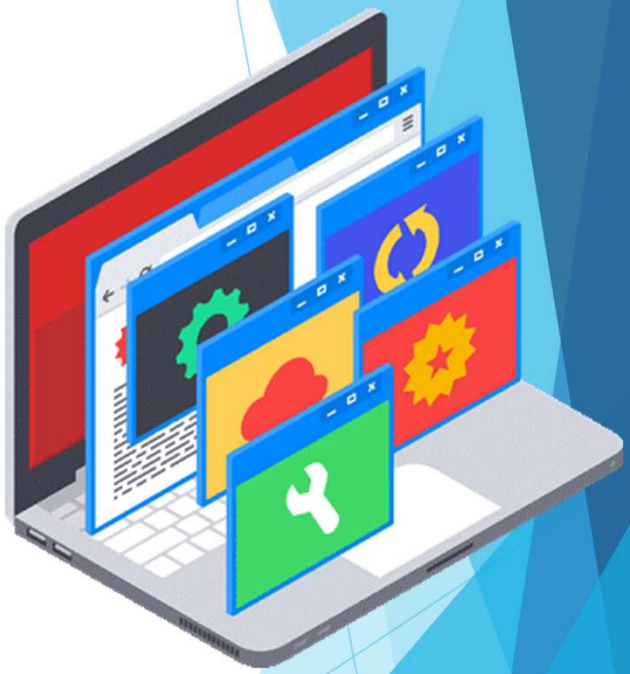
Les adware représentent l'une des nuisances les plus couramment rencontrées en ligne.

Les programmes envoient automatiquement des publicités aux ordinateurs hôtes.

Les types de programmes adware courants incluent des publicités contextuelles sur les pages Web et des publicités intégrées au programme qui accompagnent bien souvent un logiciel « gratuit ».

Bien que certains adware soient relativement sans danger, d'autres variantes utilisent des outils de suivi permettant de récupérer des informations sur votre site ou sur votre historique de navigation et affichent des publicités ciblées sur votre écran. Comme le fait observer BetaNews, une nouvelle forme d'adware capable de désactiver votre logiciel antivirus a été détectée.

Le programme adware étant installé avec le consentement des personnes après les en avoir informé, de tels programmes ne peuvent donc pas être appelés programmes malveillants : ils sont généralement identifiés en tant que «programmes potentiellement indésirables».



Spyware (Logiciel espion)

Un logiciel espion agit comme son nom l'indique, à savoir, espionner ce que vous faites sur votre ordinateur.

Il recueille des données telles que les saisies clavier, vos habitudes de navigation et vos informations de connexion qui sont alors envoyées à des tiers, généralement des cybercriminels.

Il peut également modifier des paramètres de sécurité spécifiques sur votre ordinateur ou interférer avec les connexions réseau.

TechEye révèle que de nouvelles formes de logiciels espions peuvent permettre à des entreprises de suivre le comportement des utilisateurs sur plusieurs appareils, à leur insu.

Ransomware

Les ransomware infectent votre ordinateur, puis chiffrent des données sensibles telles que des documents personnels ou des photos, puis demandent une rançon pour les récupérer.

Si vous refusez de payer, les données sont supprimées.

Certaines variantes de ransomware verrouillent l'accès à votre ordinateur.

Ils peuvent prétendre provenir d'organismes légitimes chargés de faire appliquer la loi et suggérer que vous vous êtes fait prendre pour avoir mal agi.

En juin 2015, Internet Crime Complaint Center du FBI a reçu des plaintes d'utilisateurs signalant 18 millions de dollars de pertes dues à un ransomware courant appelé CryptoWall.

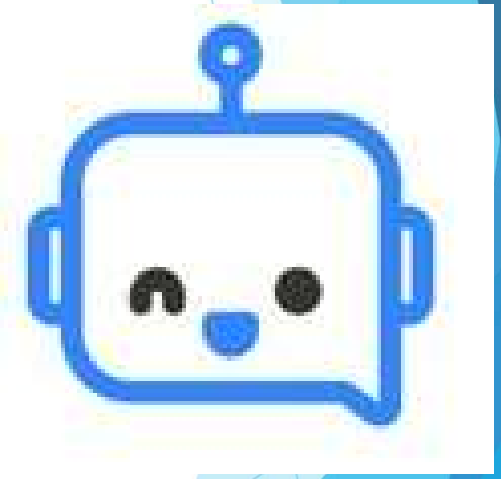
Robot (Botnet)

Les robots sont des programmes conçus pour exécuter automatiquement des opérations spécifiques.

Ils sont utilisés à de nombreuses fins légales, mais ont été redéfinis comme un type de programme malveillant.

Une fois dans l'ordinateur, les robots peuvent faire en sorte que la machine exécute des commandes spécifiques sans que l'utilisateur ne les autorise ou n'en soit informé.

Les pirates informatiques peuvent également tenter d'infecter plusieurs ordinateurs avec le même robot afin de créer un « botnet » (contraction des termes « robot » et « network » (réseau), qui peut alors être utilisé pour gérer à distance des ordinateurs infectés (pour dérober des données sensibles, espionner les activités de la victime, distribuer automatiquement des spams ou lancer des attaque DDoS dévastatrices sur des réseaux informatiques).



Rootkits

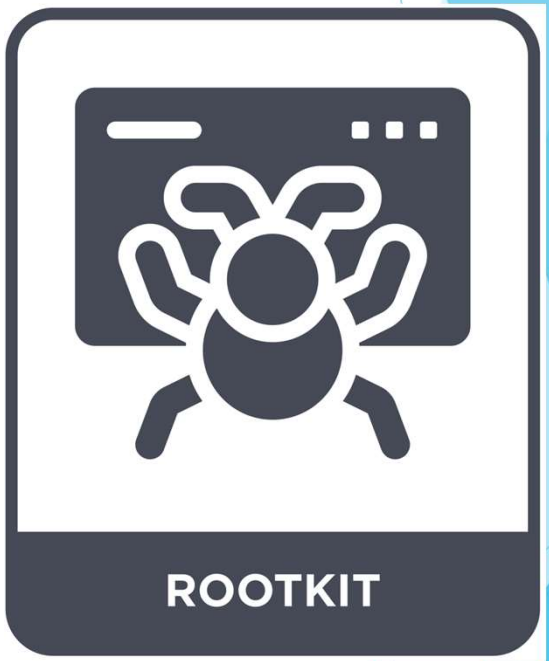
Les rootkits autorisent un tiers à accéder ou contrôler à distance un ordinateur.

Ces programmes permettent aux professionnels de l'informatique de résoudre à distance des problèmes de réseau mais ils peuvent également devenir malveillants.

une fois installés sur votre ordinateur, les pirates peuvent prendre le contrôle de votre machine pour dérober des données ou installer d'autres composants du programme malveillant.

Les rootkits sont conçus pour passer inaperçus et masquer activement leur présence.

La détection de ce type de code malveillant nécessite la surveillance manuelle de comportements inhabituels ainsi que l'application régulière de correctifs sur votre système d'exploitation et vos logiciels afin d'éliminer les chemins d'accès potentiels d'infection



Trojan (Chevaux de Troie)

Ces programmes se fondent en se faisant passer pour des fichiers ou des logiciels légitimes.

Une fois téléchargés et installés, ils modifient un ordinateur et conduisent des activités malveillantes, à l'insu de la victime.

TP 1 Installation d'un anti-virus

- Faites l'installation de Kaspersky Anti-Virus sur votre VM

https://www.kaspersky.fr/downloads

- Lancé une première analyse-virale
- Plannifiez l'analyse viral tous les Mardi à 14h

Stratégie de groupe

GPO

Group policy Objects

Les **stratégies de groupe** (En anglais, *Group Policy* ou *GP*) sont des fonctions de gestion centralisée de la famille Microsoft Windows.

Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory.
Les stratégies de groupe font partie de la famille des technologies IntelliMirror, qui incluent la gestion des ordinateurs déconnectés, la gestion des utilisateurs itinérants ou la gestion de la redirection de dossiers ainsi que la gestion des fichiers en mode déconnecté.
Les stratégies de groupe sont gérées à travers des objets de stratégie de groupe communément appelés GPO (Group Policy Objects).

Les entreprises utilisent les stratégies de groupe pour restreindre les actions et les risques potentiels comme le verrouillage du panneau de configuration, la restriction de l'accès à certains dossiers, la désactivation de l'utilisation de certains exécutables, etc.

Création et édition des stratégies de groupe

Les stratégies de groupe peuvent être éditées au travers de deux outils – le Group Policy Object Editor (Gpedit.msc) et la Group Policy Management Console (gpmc.msc).

GPEdit est utilisé pour créer et éditer une stratégie de groupe de façon unitaire. La GPMC simplifie grandement la gestion des stratégies de groupe en fournissant un outil permettant une gestion centralisée et collective des objets.

La GPMC inclut de nombreuses fonctionnalités telles que la gestion des paramètres, un panneau pour la gestion du filtrage par groupe de sécurité, des outils de sauvegarde et de restauration et d'autres outils graphiques intégrés à la MMC.

Le nom d'une stratégie de groupe peut être déterminé en utilisant l'outil GPOTool.exe.

Les stratégies de groupe locales

Les stratégies de groupe locales sont une version plus basique des stratégies de groupe utilisées avec Active Directory.

Dans les versions antérieures à Windows Vista, les stratégies de groupe locales peuvent être utilisées sur un ordinateur local, mais ne peuvent pas être utilisées pour des comptes utilisateur ou des groupes.

La limitation liée aux utilisateurs peut être contournée en utilisant l'éditeur de base de registre pour modifier les clés sous HKCU ou HKU

Les stratégies de groupe locales réalisent des modifications sous la clé HKLM, ce qui affecte tous les utilisateurs ; les mêmes changements peuvent être effectués sous HKCU ou HKU pour affecter uniquement certains utilisateurs.

Microsoft fournit des informations complémentaires sur son site Technet.

Windows Vista supporte les stratégies de groupe locales multiples, qui permettent de positionner les paramètres pour les utilisateurs individuels.

Quelques commandes

Il est possible de vérifier l'application des GPO manuellement avec les commandes

gpresult (Windows 2003 et Windows XP)

GPResult

rsop.msc (Windows 2000 à 8 ; serveurs Windows 2000 à 2012) offre une interface graphique "Jeu de stratégie résultant".

Il est possible de forcer l'application des GPO manuellement avec les commandes

gpupdate (Windows 2003 et Windows XP ainsi que sous Windows Vista, Windows 7, 8 et 10).

GPUpdate /Force

Info: gpupdate ne déploie pas les GPO aux membres du domaine. Elle doit être exécutée sur chaque poste concerné.

secedit (Windows 2000)

Secedit /RefreshPolicy machine_policy /ENFORCE pour les GPO s'appliquant aux ordinateurs

Secedit /RefreshPolicy user_policy /ENFORCE pour les GPO s'appliquant aux utilisateurs

TP2 GPO

Créez une GPO pour faire du fon d’écrans suivant le fond d’écrans par default de tous les utilisateurs.