## BACKDOOR

Une backdoor, ou porte dérobée, est un moyen d'accéder à un ordinateur en contournant les mécanismes de sécurité habituels. Elle peut être créée par un développeur pour résoudre des problèmes, mais elle peut également être installée par des hackers pour contrôler un ordinateur à distance. Les backdoors peuvent être très difficiles à détecter et peuvent être introduites de différentes manières, telles que des logiciels malveillants ou des erreurs de programmation.

## COMMENT LES REPERER ?

Vérifiez les processus en cours d'exécution. Recherchez des processus inconnus ou inhabituels, en particulier ceux qui écoutent sur des ports réseaux. Cela peut signaler une backdoor.

Examinez les fichiers système pour des modifications. Recherchez des fichiers système modifiés récemment, en particulier ceux liés à la sécurité comme les pare-feu, les listes de contrôle d'accès, etc. Cela peut indiquer qu'une backdoor a été installée.

HADJRAS MOHCINE, BOUANANI YACINE, BIABIANY THOMAS

# $> I'M THE CREEPER. CATCH ME IF YOU CAN! *

Le premier virus informatique de l'histoire s'appelait Creeper. Il a été créé en 1971 par Bob Thomas. Le virus se déplaçait sur le réseau Arpanet, ancêtre d'Internet, et signalait sa présence sans créer de dommage. Bien que considéré comme inoffensif, Creeper a été le premier exemple de programme malveillant à se déplacer sur un réseau d'ordinateurs.

*Creeper se baladait simplement entre les machines du réseau Arpanet en laissant le message "I'M THE CREEPER. CATCH ME IF YOU CAN"

## VIRUS INFORMATIQUE

## COMMENT SE PROTEGER ?

Il faut savoir que les failles sont rarement techniques car dans la majeure partie des cas, les failles sont humaines (phishing, ingénierie sociale, etc). Pour éviter ce genre d'infection, restez vigilants. Ne téléchargez que des fichiers provenant de sources de confiance et faites régulièrement des sauvegardes.


## RANSOMWARE

Un RANSOMWARE est un type de logiciel malveillant qui bloque l'accès à un ordinateur ou à des fichiers en les chiffrant, empêchant ainsi l'utilisateur d'y accéder. Il exige ensuite le paiement d'une rançon en échange de la clé de déchiffrement pour restaurer l'accès aux données. Les ransomwares sont souvent diffusés via des e-mails frauduleux, des sites web compromis ou des vulnérabilités logicielles non corrigées.

## J'AI ETE INFECTE !

- **Isoler l'ordinateur infecté**
  Déconnectez immédiatement l'ordinateur infecté du réseau local et d'internet pour éviter la propagation du ransomware à d'autres appareils connectés.
- **Ne pas éteindre l'ordinateur**
  Dans certains cas, il peut être préférable de ne pas éteindre immédiatement l'ordinateur infecté par un ransomware afin de permettre l'analyse de la mémoire RAM et de recueillir des preuves supplémentaires.
- **Signaler l'attaque**
  Informez les autorités compétentes, telles qu'un organisme de lutte contre la cybercriminalité. Signalez également l'incident à votre fournisseur de services Internet ou à votre département informatique si vous êtes dans un environnement professionnel.

IUT Lyon 1
l'excellence technologique