Le Cyber cambriolage. Via les Cyber RAT.

(Remote Access Trojan)

De tout temps des personnes ont voulu voler des informations que ce soit pour les revendre, pour effectuer un chantage ou pour s'offrir un avantage particulier.

L'arrivé de l'informatique a multiplié les possibilités et l'arrivé des smartphones à multiplié le marché potentiel de ces escrocs.

Si, dans l'actualité récente les américains accusent les chinois d'avoir laissé des Backdoor dans le logiciel TicTok, il y a plus de 20 ans, les européens accusaient la CIA d'avoir utilisé des Backdoor dans les Smartphones du Canadien « Blackberry » pour gagner des marchés avec Boeing contre Airbus. (Car, à cette époque, le téléphone portable Blackberry était le téléphone le plus utilisé par les chefs d'entreprises ou les politiciens du monde entier).

Je ne vous parlerai pas des RAT dans les smartphones mais des RAT dans les centres informatiques où la défense contre les « Cyber RAT » est un enjeu majeur.

En premier il faut savoir que des Backdoor sont découvertes régulièrement dans des logiciels mais les risques qu'elles soient utilisées sont faibles à condition que vous mainteniez tous vos logiciels à jour régulièrement.

Le risque majeur pour vous, qui serez un jour responsable d'un système d'information, est qu'une personne mal intentionnée installe une Backdoor pour pirater votre système. Dans ce cas votre responsabilité sera directement mise en cause.

Pour comprendre comment se défendre il faut comprendre comment un Cyber Cambrioleur va s'y prendre pour vous pirater. Imaginons que le pirate veule installer une Backdoor permanente pour pirater votre informatique quand il en aura besoin.

Démonstration avec un logiciel de piratage « QUASAR » qui installe un RAT.

(Voir les vidéos sur YouTube).

L'avantage de ce logiciel est qu'il est écrit en langage C donc facilement modifiable.

Même si vous lui donnez un autre nom du type « framework-upgrade.exe » et que vous l'installez dans c:\windows\system ; l'antivirus vas reconnaitre la signature du logiciel et va le rejeter.

Par contre si vous rajouter dans le programme C quelques lignes comme : int a=1 et… (qui ne servent à rien), à la compilation la signature va changer et l'antivirus ne le verra pas.

Toute la difficulté sera de trouver un poste de travail disponible, qui sera allumé sans personne devant, et dont son utilisateur possède des droits suffisants pour accéder aux serveurs visés.

Et, suivant que le routeur d'accès soit oui ou non modifiable, la stratégie change.

Vous voyez que vous pouvez toujours être vulnérable à une cyberattaque via un RAT.

Et ce RAT peut être amené simplement par un utilisateur lambda qui a cru judicieux de télécharger sur son poste de travail un logiciel spécifique (non fourni, ni agréé par l'entreprise) et qui malheureusement contient un RAT caché à l'intérieur.

D'où l'intérêt fondamental de savoir exactement et en permanence quels sont les logiciels installés sur les PC de l'entreprise en utilisant des analyseurs automatiques de type Solar Win ou Landsweper.

(Voir démo : SolarWin ou LanSweper)

Toutes les règles élémentaires de sécurité que l'on a vues précédemment vont freiner ou même bloquer ce type d'attaque.

Ne pas oublier qu'une attaque HID à souvent que le seul but d'installer un RAT.