RECHERCHE, ENQUETE ou Comment effacer vos traces.

Problématique :

Pour illustrer le sujet et comprendre les actions à effectuer, imaginons un exemple :

Un de vos employé a installé un site Web pirate sur un des vos serveur pour vendre de la drogue en ligne.
Pour identifier le coupable vous devez trouver à partir de quel micro de votre entreprise ce site Web a été installé sur un de vos serveurs.

Première action.

Avant toute chose il faut prendre des copies d'écrans du site Web incriminé et surtout faire une copie du code source de la page d'accueil.

Sur la page Web incriminée sélectionner :

Outil
Outil de navigateur
Code source de la page
Puis copier le code source dans Notepad ++
Faire cela sur toutes les pages accessibles du site Web.

Si on prend comme exemple le site internet du Lycée Saint Joseph on voit

Qu'il a été construit à base Joomla un open source de création de site Web.
Qu'un outil de type Gandry5 a été utilisé.
Il a probablement utilisé un outil de type FizeZilla pour le charger sur le serveur.
Et surtout on a le nom d'images et de vidéos : logo-saint-jo1.png ; video-internat ; video-cdi ; video-restaurant-scolaire etc..

Ce sont toutes ces références qui, si elles sont retrouvées dans un ordinateur, servirons comme faisceau de preuves contre son utilisateur.

Mais dès que vous allez commencer votre investigation le coupable va détruire le site Web et effacer le maximum trace sur son ordinateur.

La première question que vous devez vous poser et pourquoi le port 80 du votre routeur (ou de votre box) d'entrée est ouvert et qui à accès à la configuration du routeur. --> Responsabilité du mot de passe du routeur.

Deuxième étape : Analyser tous les micros pour essayer d'identifier le coupable.

Imaginons que pour finir de préparer le site web avant de le charger sur un serveur monsieur X a eu besoin des logiciels Gantry5 et de FileZila.
Il les a probablement dé-installés mais s'il n'a pas pris la précaution de nettoyer son micro il reste des traces de leurs installations.

Quand on désinstalle un logiciel il reste beaucoup de trace de son installation.
Vérifier :

Directement dans les répertoires dur le disque C :

Programme, Programmes data, et programmes (86).

Puis dans utilisateur : XXXX

App data

Local

Etc..

Faire une recherche sur l'ensemble du disque C avec comme critère de recherche :

FileZilla.*

Ou : logo-saint-jo1.*

Enfin lancer REGEDIT

Rechercher : FileZilla (ou Gantry)

Si une instance est trouvée bien faire attention à la date d'installation ce qui peut vous aider dans votre recherche.

A contrario :

Si vous êtes le pirate et que vous voulez installer un site Web à partir d'une clef USB, sur un serveur de votre entreprise en vous servant de votre propre micro.

If faut :

1 Faire une sauvegarde du registre.
2 Installer les logiciels nécessaires pour uploader le site Web.
3 Uploader le site Web et vérifier sa disponibilité.
4 Modifier le routeur. (Tester l'accès du site Web de l'extérieur).
5 Désinstaller les logiciels installés en 2. (Puis redémarrer)
6 Vérifier s'il ne reste pas de traces avec l'option recherche sur le disque C.
7 Re installer la sauvegarde du registre faite en 1.

Si vous n'avez pas fait la partie 1 (et donc pas la 7) essayer de nettoyer le registre avec CCleaner avant de faire des recherches avec REGEDIT.