

Cyber-criminalité : les « creepwares » ou « furtiviciels ».

Sécurité

Posté par : JulieM

Publié le : 13/12/2013 13:00:00

Ces chevaux de Troie, des « RAT » (pour Remote Access Trojan), permettent de prendre insidieusement le contrôle à distance de l'ordinateur de leurs victimes et exécutent différentes opérations comme :

- Le détournement de la webcam pour espionner et prendre les victimes en photo à leur insu ;
- Suivre la trace des activités en ligne des victimes ;
- Ecouter les conversations à l'aide du micro de l'ordinateur ;
- Accéder aux comptes protégés par mot de passe.

Certains cas ont été fortement médiatisés, notamment aux Etats-Unis, comme le piratage de Miss Teen USA ou de Cassidy Wolf, mais la France est particulièrement touchée, puisqu'elle totalise 12 % des cas recensés dans le monde, arrivant en 3^e place.

Les utilisateurs de ces maliciels ont des profils très divers : il peut s'agir d'individus malveillants, familiers des escroqueries et cherchant à gagner de l'argent via l'extorsion de fonds ; ou bien encore d'utilisateurs cherchant à vivre une expérience « divertissante » avec ce qu'ils croient être un programme inoffensif, voulant simplement vanter leurs succès pour s'amuser.

La relative disponibilité de ces outils, leur prix modique ainsi que leur facilité d'utilisation en font une menace très préoccupante. Les pirates ont un accès direct aux données privées de leurs victimes, allant même jusqu'à fanfaronner sur des forums où ils comparent à leurs prises et incitent d'autres internautes à les imiter.

Ce [blog](#) post établit un panorama du phénomène des Creepwares en décrivant cette nouvelle menace, sa nature, ce qui est ou peut être fait avec. Il vise également à présenter les conséquences pour les victimes comme pour les utilisateurs de ces outils malveillants, ainsi que l'économie souterraine connexe générée par la vente de ces programmes et la monétisation des données volées. Enfin, l'ensemble des modes de diffusion et des protections adaptées y est détaillé.

[Visionnez une vidéo.](#)