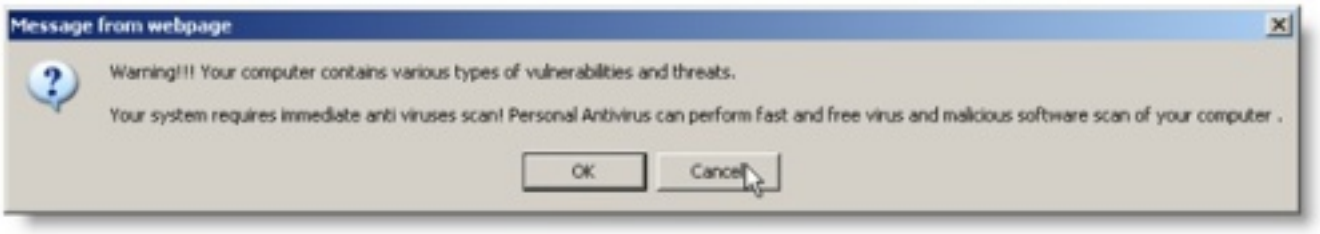
BitDefender, Harry Potter et le Prince de sang-mÃªlÃ©, gratuitement sur Internet ?
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 27/7/2009 0:00:00

Pas vraiment, Ã moins que vous ne vouliez abÃ®mer votre ordinateur
Si vous souhaitez voir les derniÃ¨res aventures des Ã©lÃ¨ves de Hogwarts, nous vous conseillons dâ□□acheter une entrÃ©e de cinÃ©ma afin dâ□□Ã©viter d'Ãªtre victime du dernier malware, qui dÃ©pose un cheval de Troie, vide les comptes bancaires et fait perdre beaucoup de temps Ã ses victimes.

Câ□□est en tout cas ce que les fans de Harry Potter (sans protection antivirus ou crÃ©dules) obtiennent en cliquant sur des liens supposÃ©s permettre de visionner gratuitement le dernier volet cinÃ©matographique de lâ□□Å□uvre de J.K Rowling.



Â

Â

2. S'il clique sur le bouton OK ou sur Annuler, l'utilisateur lance un faux processus d'analyse qui s'affiche dans la fenÃªtre du navigateur qui a Ã©tÃ© restaurÃ©e. Ce processus est censÃ© dÃ©tecter les malwares prÃ©sents sur le systÃ¨me.

Pour plus de crÃ©dibilitÃ©, les cyber-criminels ont ajoutÃ© un panneau dâ□□informations Ã gauche de la fenÃªtre Â« My Computer Online Scan Â» (Analyse en ligne du Poste de travail), qui affiche des dÃ©tails concernant l'adresse IP, le pays et la ville de l'ordinateur de l'utilisateur.

Â

Â

4. Si l'utilisateur clique Ã l'intÃ©rieur de la fausse fenÃªtre, il lance le tÃ©lÃ©chargement du malware.

Â

Â

Sans doute pour rÃ©aliser d'autres attaques Ã l'avenir, il collecte Ã©galement des donnÃ©es sur la machine qui sera compromise : la date d'installation de MicrosoftÂ® WindowsÂ® et le numÃ©ro de sa version, le type de navigateur par dÃ©faut, le nombre de processus en cours, l'espace disque disponible et la taille de la mÃ©moire RAM, ainsi que le nombre de programme installÃ©s.

Une fois que le composant chargÃ© de lâ□□installation termine le tÃ©lÃ©chargement de Personal Antivirus, il se connecte Ã la page de remerciement de MicrosoftÂ® WindowsÂ® Update, pour faire croire que le logiciel provient d'une source de confiance et est sÃ»r.

Personal Antivirus modifie les paramÃ¨tres du registre, demande Ã lâ□□utilisateur dâ□□acheter/de

renouveler une licence et tÃ©lÃ©charge des malwares supplÃ©mentaires Ã lâ□□origine des fausses alertes qu'il affiche. Ces alertes ne sont plus visibles lorsque lâ□□utilisateur visite les pages Web qui hÃ©bergent le faux logiciel antivirus, lesquelles sont incluses dans une liste cryptÃ©e du cheval de Troie.