Le vendredi 24 juillet 2009

Harry Potter et le Prince de sang-mêlé disponible gratuitement sur Internet ?

Pas vraiment, à moins que vous ne vouliez abîmer votre ordinateur

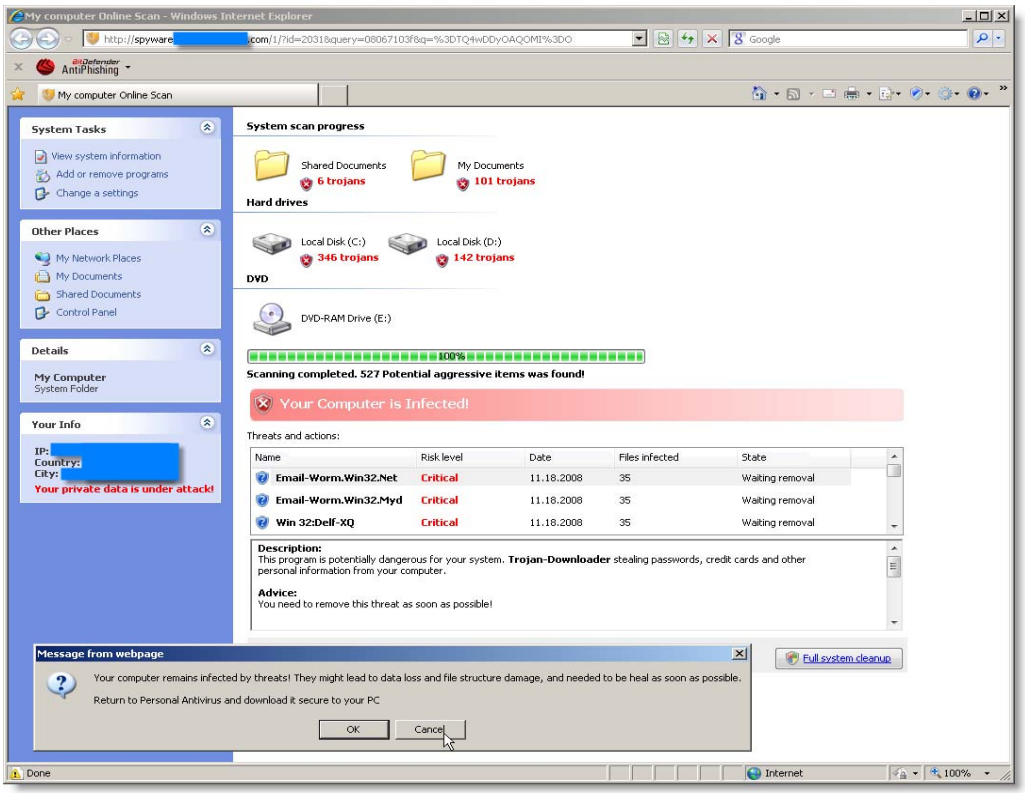
Si vous souhaitez voir les dernières aventures des élèves de Hogwarts, nous vous conseillons d'acheter une entrée de cinéma afin d'éviter d'être victime du dernier malware, qui dépose un cheval de Troie, vide les comptes bancaires et fait perdre beaucoup de temps à ses victimes. C'est en tout cas ce que les fans de Harry Potter (sans protection antivirus ou crédules) obtiennent en cliquant sur des liens supposés permettre de visionner gratuitement le dernier volet cinématographique de l'œuvre de J.K Rowling.

La diffusion du malware comprend cinq étapes simples et implique au moins deux types de charges utiles malveillantes :

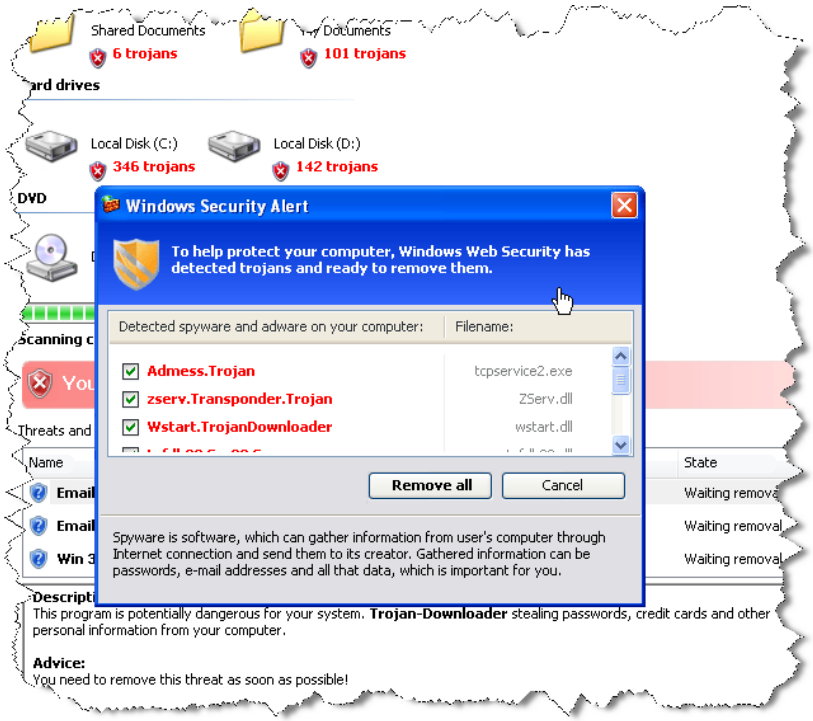
1. Le faux lien ne conduit pas vers une page Web présentant le film, mais redirige automatiquement le navigateur vers un site Web contenant des malwares. La fenêtre du navigateur est réduite et en même temps, un message s'affiche, signalant à l'utilisateur la présence de plusieurs infections sur son ordinateur et lui proposant d'utiliser Personal Antivirus pour supprimer les menaces.

2. S'il clique sur le bouton OK ou sur Annuler, l'utilisateur lance un faux processus d'analyse qui s'affiche dans la fenêtre du navigateur qui a été restaurée. Ce processus est censé détecter les malwares présents sur le système. Pour plus de crédibilité, les cyber-criminels ont ajouté un panneau d'informations à gauche de la fenêtre « My Computer Online Scan » (Analyse en ligne du Poste de travail), qui affiche des détails concernant l'adresse IP, le pays et la ville de l'ordinateur de l'utilisateur.

Une fois l'analyse terminée (après environ 10 secondes), on recommande à l'utilisateur de télécharger et d'installer le faux logiciel antivirus afin de supprimer plus de 500 fichiers endommagés par différents types de malwares.

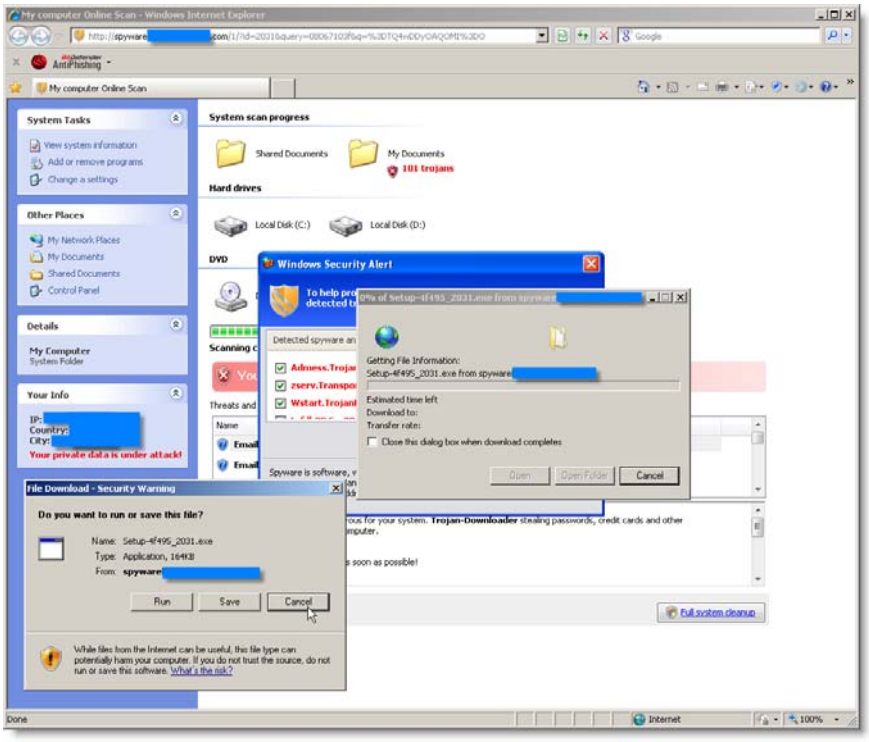


3. Que l'utilisateur clique sur OK ou sur Annuler, il active une fausse alerte de sécurité Windows® (notez le bouclier doré dans le coin supérieur gauche) qui est en fait une simple capture d'écran déclenchant le téléchargement du faux antivirus (voir le curseur en forme de main sur l'image ci-dessous).



4. Si l'utilisateur clique à l'intérieur de la fausse fenêtre, il lance le téléchargement du malware.

5. Lorsque le téléchargement se termine, si aucune suite de sécurité n'est installée et si le binaire s'exécute, le système de l'utilisateur est alors infecté avec Trojan.Downloader.PersonalAntivirus.A. Une fois installé, ce malware à l'accord de licence crypté tente de télécharger l'un des nouveaux membres de la famille des faux antivirus, Personal Antivirus, en se connectant à plusieurs serveurs enregistrés dans des domaines .com et .cn. Pour ne pas être détecté, il termine le processus



Windows Defender.

Sans doute pour réaliser d'autres attaques à l'avenir, il collecte également des données sur la machine qui sera compromise : la date d'installation de Microsoft® Windows® et le numéro de sa version, le type de navigateur par défaut, le nombre de processus en cours, l'espace disque disponible et la taille de la mémoire RAM, ainsi que le nombre de programme installés.

Une fois que le composant chargé de l'installation termine le téléchargement de Personal Antivirus, il se connecte à la page de remerciement de Microsoft® Windows® Update, pour faire croire que le logiciel provient d'une source de confiance et est sûr.

Personal Antivirus modifie les paramètres du registre, demande à l'utilisateur d'acheter/de renouveler une licence et télécharge des malwares supplémentaires à l'origine des fausses alertes qu'il affiche. Ces alertes ne sont plus visibles lorsque l'utilisateur visite les pages Web qui hébergent le faux logiciel antivirus, lesquelles sont incluses dans une liste cryptée du cheval de Troie.

À propos de BitDefender®

BitDefender est la société créatrice de l'une des gammes de solutions de sécurité la plus complète et la plus certifiée au niveau international reconnues comme étant parmi les plus rapides et les plus efficaces du marché. Depuis sa création en 2001, BitDefender n'a cessé d'élever le niveau et d'établir de nouveaux standards en matière de protection proactive des menaces. Chaque jour, BitDefender protège des dizaines de millions de particuliers et de professionnels à travers le monde – en leur garantissant une utilisation sereine et sécurisée de l'univers informatique. Les solutions de sécurité BitDefender sont distribuées dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiés. Dans les pays francophones, BitDefender est édité en exclusivité par Éditions Profil. Plus d'informations sur BitDefender et ses solutions sont disponibles via le Centre de presse. Retrouvez également sur le site www.malwarecity.fr les dernières actualités au sujet des menaces de sécurité qui permettent aux utilisateurs de rester informés des dernières évolutions de la lutte contre les malwares.

À propos des Editions Profil

Editions Profil, société indépendante créée en 1989, développe, édite et diffuse des logiciels sur différents secteurs d'activités, professionnel et grand public. L'éditeur a constitué un large catalogue de solutions dans de nombreux domaines, par exemple sur les segments de la bureautique et de la productivité. Editions Profil s'est plus particulièrement spécialisée ces dernières années dans l'édition et la distribution d'outils de sécurité informatique et la protection des données en général. Editions Profil édite notamment les solutions de sécurité BitDefender et Parental Filter, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.