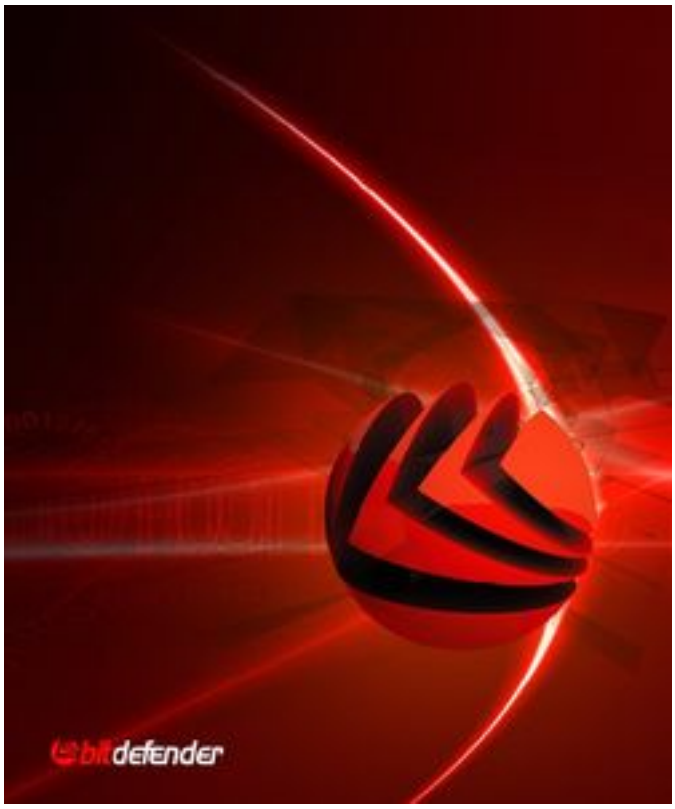
BitDefender Des malwares furtifs redirigent vers de faux sites Internet
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 12/6/2009 0:00:00

Bitdefender dÃ©couvre des scammeurs imitant des sites de paiement en ligne pour obtenir des informations personnelles de leurs victimes
Les chercheurs BitDefenderÂ® confirment que les services de paiement en ligne font toujours partie des dix identitÃ©s les plus souvent usurpÃ©es dans le monde du spam et du phishing, conformÃ©ment au dernier rapport BitDefender sur l'Ã©tat des e-menaces.

La derniÃ¨re campagne de phishing ciblant les utilisateurs de services bancaires et de paiements en ligne comporte plusieurs Ã©lÃ©ments caractÃ©ristiques propres aux malwares. D'abord, le message non sollicitÃ© diffusant le malware prÃ©tend proposer la meilleure Solution Antivirus Open Source et demande aux utilisateurs de visiter une page Web oÃ¹ ils peuvent tÃ©lÃ©charger le produit.

Pourtant, une fois que l'utilisateur a cliquÃ© sur le lien, il ne reÃ§oit pas la suite de sÃ©curitÃ© promise, mais un faux exÃ©cutable, setup.exe, une archive auto-extractible qui sâ□□exÃ©cute bien comme telle.



Son but est de remplacer le contenu du rÃ©pertoire C:WINDOWSSystem32driversetc et de modifier le comportement du navigateur Web, en chargeant automatiquement des pages Web spÃ©cialement conÃ§ues Ã des fins de phishing imitant des sites de paiement en ligne tels que PayPal, Abbey ou Halifax.

Puis, Ã chaque fois que l'utilisateur tape dans son navigateur une adresse appartenant Ã l'une de ces institutions financiÃ¨res, il est automatiquement redirigÃ© vers les fausses pages.

Ses donnÃ©es d'authentification (nom d'utilisateur, mot de passe, code de sÃ©curitÃ©) et d'autres donnÃ©es sensibles (nom, prÃ©nom, adresse e-mail, adresse postale, numÃ©ro et date d'expiration de la carte, code de vÃ©rification de la carte et mÃªme, le code confidentiel) sont rÃ©cupÃ©rÃ©es via des scripts PHP. Toutes les autres options du menu disponibles sur les pages redirigent l'utilisateur vers les sections appropriÃ©es des vÃ©ritables sites Web.

L'analyse a rÃ©vÃ©lÃ© que ces fausses pages Web se chargeaient Ã partir de domaines enregistrÃ©s en Chine et en CorÃ©e.

Â« *La situation Ã©conomique actuelle a inÃ©vitablement conduit Ã la prolifÃ©ration des dÃ©lits informatiques* Â» explique **Vlad Valceanu**, Directeur de la Recherche Antispam des Laboratoires BitDefender. Â« *Les derniÃ¨res tendances observÃ©es par BitDefender rÃ©vÃ¨lent plusieurs aspects alarmants : d'abord, depuis le dÃ©but de l'annÃ©e, les scams et les actes de phishing suivent une courbe ascendante. Ensuite, la complexitÃ© et l'agressivitÃ© de ces attaques ont augmentÃ© considÃ©rablement ainsi que le nombre de victimes de ces attaques. Les utilisateurs doivent non seulement faire plus attention aux e-mails qu'ils reÃ§oivent, mais il est Ã©galement important qu'ils installent une solution de sÃ©curitÃ© fiable sur leurs systÃ¨mes, afin d'Ã©viter de prochaines attaques* Â».

Pour Ãªtre informÃ© au sujet des e-menaces inscrivez-vous aux flux RSS BitDefender.

Ã propos de BitDefenderÂ®

BitDefender est la sociÃ©tÃ© crÃ©atrice de lâ□□une des gammes de solutions de sÃ©curitÃ© la plus complÃ¨te et la plus certifiÃ©e au niveau international reconnues comme Ã©tant parmi les plus rapides et les plus efficaces du marchÃ©. Depuis sa crÃ©ation en 2001, BitDefender nâ□□a cessÃ© dâ□□Ã©lever le niveau et dâ□□Ã©tablir de nouveaux standards en matiÃ¨re de protection proactive des menaces.

Chaque jour, BitDefender protÃ¨ge des dizaines de millions de particuliers et de professionnels Ã travers le monde â□□ en leur garantissant une utilisation sereine et sÃ©curisÃ©e de lâ□□univers informatique. Les solutions de sÃ©curitÃ© BitDefender sont distribuÃ©es dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiÃ©s.

Dans les pays francophones, BitDefender est Ã©ditÃ© en exclusivitÃ© par Ã□ditions Profil. Plus dâ□□informations sur BitDefender et ses solutions sont disponibles via le Centre de presse .

Retrouvez Ã©galement sur le site **MalwaresCity** les derniÃ¨res actualitÃ©s au sujet des menaces de sÃ©curitÃ© qui permettent aux utilisateurs de rester informÃ©s des derniÃ¨res Ã©volutions de la lutte contre les malwares.