ByteDefender, Un faux antivirus qui se fait passer pour BitDefender
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 21/5/2010 15:00:00

OpportunÃ©ment nommÃ© Â« **ByteDefender** Â», lâ□□application malicieuse se comporte exactement comme **un faux antivirus** (ou Â« Rogue Â») avec un â□□cadeau bonusâ□□

BitDefender a dÃ©tectÃ© ByteDefender, ce Rogue tente de leurrer les internautes pour quâ□□ils lâ□□installent en pensant quâ□□il sâ□□agit du produit BitDefender.

Contrairement Ã la majoritÃ© des Antivirus Rogue, Bytedefender ne se contente pas de sâ□□appuyer sur la mÃ©thode classique du Â« Drive-by Â» qui lance des tÃ©lÃ©chargements involontaires, comme le font souvent ce type dâ□□applications, mais sâ□□appuie dâ□□avantage sur la popularitÃ© des solutions de sÃ©curitÃ© BitDefender en reprenant leur identitÃ© visuelle pour tromper les utilisateurs.

Le site web qui diffuse ce Virus est situÃ© Ã lâ□□adresse hxxp://www.bytedefender.in (***URL volontairement tronquÃ©e pour Ã©viter les infections accidentelles***), il utilise un design proche de la charte graphique de BitDefender et reprend mÃªme les vrais visuels des produits pour tromper les utilisateurs en leur faisant croire quâ□□il sâ□□agit des vraies versions des solutions de sÃ©curitÃ©. Le nom de domaine a Ã©tÃ© enregistrÃ© en Ukraine.

Le scÃ©nario dâ□□infection est simple et efficace : un utilisateur Ã la recherche dâ□□un produit BitDefender peut faire une faute de frappe sur la vÃ©ritable adresse et Ãªtre redirigÃ© vers la page web malveillante et croire quâ□□il est sur la page de lâ□□Ã©diteur.

Une fois installÃ© sur le systÃ¨me, ce logiciel Â« scareware Â» commence Ã afficher des faux messages dâ□□alerte simulant des infections pour pousser lâ□□utilisateur Ã acheter la â□□version complÃ¨teâ□□ afin de se dÃ©barrasser des soit-disant menaces en question.

Il est intÃ©ressant de noter que le processus de paiement de lâ□□Antivirus Rogue ByteDefender est gÃ©rÃ© par une entreprise digne de confiance : Plimus, qui a suspendu ses ventes en raison des fraudes constatÃ©es.

Â« *Les cybercriminels nâ□□ont aucune limite quand il sâ□□agit de distribuer et commercialiser leurs faux produits de sÃ©curitÃ©. Ã□vÃ¨nements sensationnels, applications ou sites Internet contenant des chevaux de Troie ou mÃªme crÃ©ation minutieuse de â□□produits de sÃ©curitÃ©â□□ â□□ inutiles - ne sont quâ□□une petite partie de la multitude des mÃ©thodes utilisÃ©es pour tromper les*

utilisateurs imprudents Â», dÃ©clare Catalin Cosoi, Chercheur des Laboratoires BitDefender.

En ce qui concerne la partie plus technique, lâ□□antivirus Rogue ByteDefender est protÃ©gÃ© par un logiciel de compression UPX avec de multiples couches de dissimulation qui non seulement tente dâ□□empÃªcher lâ□□analyse statique, mais aussi bloque tout type dâ□□exÃ©cutions dans une machine virtuelle. Il essaie de fermer les services Windows connus pour appartenir Ã certains Ã©diteurs dâ□□antivirus, afin dâ□□ouvrir lâ□□accÃ¨s Ã ses propres fichiers.

BitDefender a ajoutÃ© une protection contre cette nouvelle menace (dÃ©tectÃ©e sous le nom de Trojan.FakeAV.KZO) et a dÃ©veloppÃ© un outil gratuit de suppression pour automatiquement nettoyer lâ□□infection sur les ordinateurs qui nâ□□utilisent pas les produits de sÃ©curitÃ© BitDefender.

Afin de rester en sÃ©curitÃ©, BitDefenderÂ® vous recommande de tÃ©lÃ©charger, installer et mettre Ã jour

une suite antimalware avec antivirus, antispam, antiphishing et pare-feu et vous incite Ã la prudence lorsque vous Ãªtes invitÃ© Ã ouvrir des fichiers dont vous ne connaissez pas la provenance.

Pour plus dâ□□informations concernant les produits BitDefender.