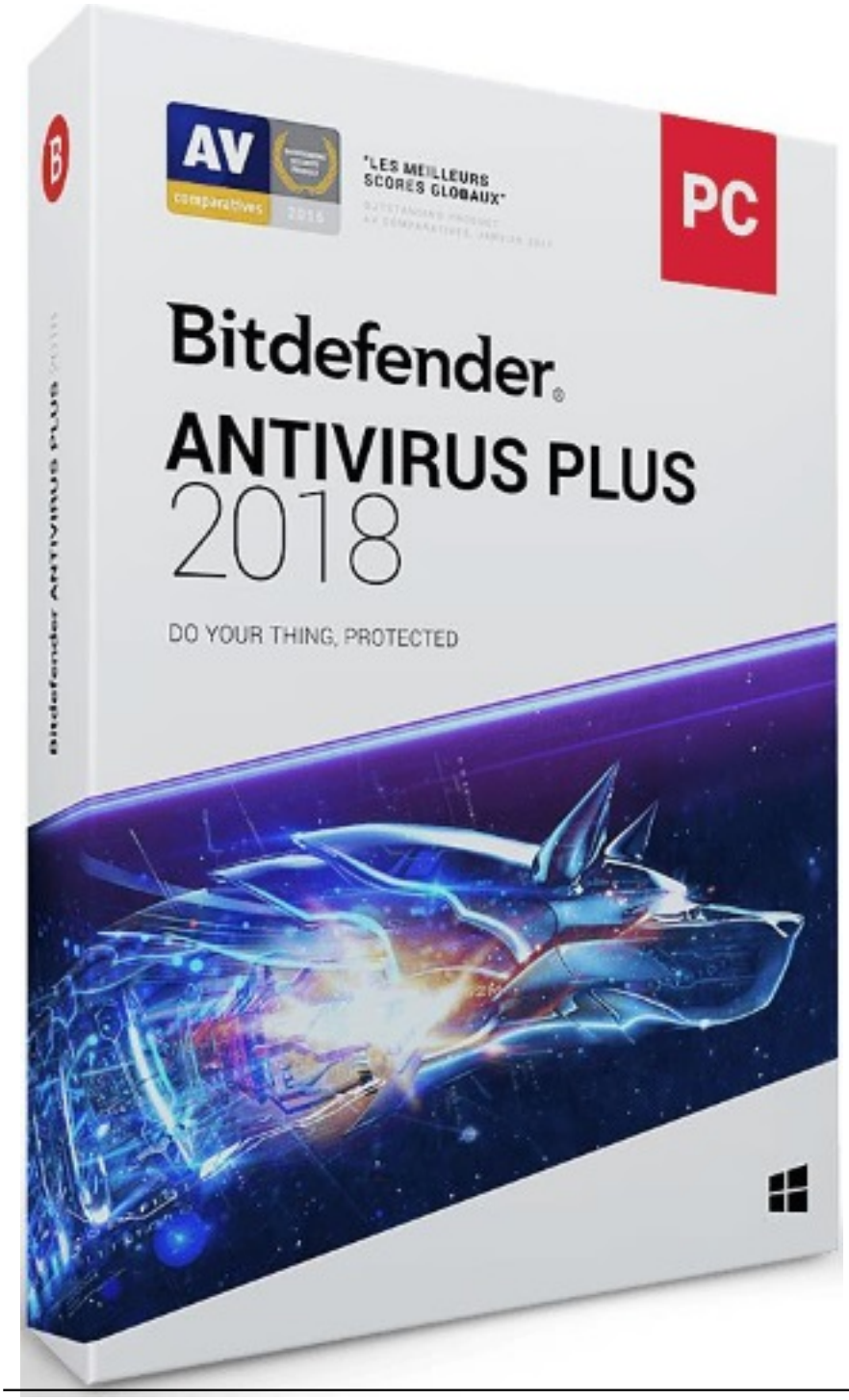
Bitdefender Labs : PrÃ©visions 2018, pas jolies jolies.
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 19/12/2017 13:30:00

Ransomware, attaques sans fichier, Machine learning, â¦ les cybercriminels passeront Ã la vitesse supÃ©rieure. En cette fin dâannÃ©e, les Bitdefender Labs envisagent dÃ©jÃ les prochaines Ã©volutions des cybermenaces qui vont faire des dÃ©gÃ¢ts au cours de l'annÃ©e Ã venir.

Les experts de Bitdefender prÃ©voient une croissance exponentielle des exploits de type Zero-day tirant parti de fuites issues dâagences de sÃ©curitÃ© au niveau mondial ainsi que des changements majeurs dans le fonctionnement des ransomwares.



AprÃ¨s des annÃ©es dâ□□attaques ciblant principalement les particuliers, les crÃ©ateurs des malwares vont dÃ©sormais cibler davantage les entreprises et les rÃ©seaux.

Les mouvements latÃ©raux deviendront la norme pour la plupart des malwares, soit via des utilitaires de dÃ©tournement de mot de passe tels que Mimikatz, soit en exploitant des vulnÃ©rabilitÃ©s en ayant un comportement identique Ã celui des vers.

Le nombre de piÃ¨ces jointes malveillantes dans les spams augmentera, en particulier ceux Ã©crits dans des langages de script tels que PERL ou Python.

Les attaques sans fichier augmenteront Ã©galement fortement Ã mesure que l'adoption de Windows 10 deviendra universelle, en utilisant des outils tels que PowerShell ou Linux Bash.

Lâ□□environnement des cybermenaces restera concentrÃ© principalement sur les malwares les plus rentables financiÃ¨rement.

Les ransomwares, les chevaux de Troie bancaires et les mineurs de monnaie virtuelles seront donc toujours plus prÃ©sents, mais ces menaces subiront des changements majeurs dans leur mode opÃ©ratoire.

On sâ□□attend par exemple Ã ce que les ransomwares tentent de tirer parti de la puissance de calcul des GPU (processeurs des cartes graphiques) pour infecter et chiffrer plus rapidement les donnÃ©es des machines ciblÃ©es et tenter de contourner les protections des solutions de sÃ©curitÃ©.

Â« Les ransomwares sont de plus en plus lucratifs et peuvent rapporter aujourdâ□□hui plus de 1400 fois la somme investie par un cybercriminel. Ces derniers vont donc chercher Ã perfectionner encore plus ce type de menaces. Â» commente Gauthier Vathaire, Brand manager pour Bitdefender France

Les experts de Bitdefender prÃ©voient Ã©galement des changements importants sur le marchÃ© du PaaS (Polymorphism as a Service), une tendance qui se consolidera tout au long de l'annÃ©e 2018. Les cybercriminels utilisent dÃ©jÃ des moteurs polymorphes avancÃ©s disponibles dans le cloud pour inonder le marchÃ© de variantes uniques de malwares connus.

Les avantages qu'ils offrent aux cybercriminels sont particuliÃ¨rement intÃ©ressants. La vente de licences dâ□□utilisation de ces moteurs personnalisÃ©s gÃ©nÃ©rera probablement des profits importants pour ces revendeurs.

Ces attaques menÃ©es par des moteurs polymorphes seront Ã©galement renforcÃ©es par lâ□□utilisation dâ□□algorithmes de Machine Learning utilisÃ©s Ã des fins de cybercriminalitÃ©.

En 2018, les cybercriminels se focaliseront beaucoup plus sur le dÃ©veloppement de techniques : crÃ©er et diffuser des codes entraÃ®nant la dÃ©tection de faux positifs de la part des Ã©diteurs ou manipuler la charge utile du malware jusqu'Ã ce qu'elle ne soit plus dÃ©tectÃ©e.

En 2018, les attaquants rechercheront Ã©galement des vulnÃ©rabilitÃ©s utilisables dans des composants situÃ©s sous les systÃ¨mes d'exploitation, tels que les firmwares.

Les protocoles Wi-Fi et Bluetooth feront lâ□□objet d'une attention particuliÃ¨re de la part des attaquants car toutes les vulnÃ©rabilitÃ©s potentielles identifiÃ©es Ã leur niveau offrent une porte dÃ©robÃ©e furtive trÃ¨s difficile Ã dÃ©tecter et Ã bloquer puisque intÃ©grÃ©es directement lors de leur conception.

Les attaques liÃ©es Ã des botnets massifs exploitant des objets connectÃ©s deviendront trÃ¨s

courantes en 2018. Le code source de nombreux bots IoT (Internet of Thing) est dÃ©jÃ disponible gratuitement sur Internet et les groupes cybercriminels dÃ©sireux de compromettre la sÃ©curitÃ© des appareils connectÃ©s disposent ainsi dÃ©jÃ d'une solide plateforme pour les personnaliser selon leurs propres besoins.

Bitdefender prÃ©voit que ce code source sera amÃ©liorÃ© en 2018 pour permettre les mouvements latÃ©raux Ã l'intÃ©rieur du rÃ©seau corrompu pour la diffusion de ransomwares ou l'envoi de spams.

DerniÃ¨re prÃ©vision, mais non des moindres, nous prÃ©voyons un net accroissement de la cybercriminalitÃ© visant le systÃ¨me dâ□□exploitation OS X. Pour les particuliers, les malwares se concentreront vraisemblablement sur des techniques de â□□scarewaresâ□□, consistant Ã effrayer les utilisateurs pour les lâ□□inciter Ã acheter des outils inutiles.

Les entreprises seront probablement victimes dâ□□attaques plus ciblÃ©es et de charges utiles malveillantes utilisÃ©es dans les menaces persistantes avancÃ©es.

Retrouvez Bitdefender en ligne et restez au fait de lâ□□actualitÃ© des e-menaces