Microsoft : Les FranÃ§ais mis en garde contre la menace Conficker
Microsoft
PostÃ© par : JerryG
PubliÃ©e le : 26/4/2012 15:00:00

Microsoft dÃ©voile aujourdâ□□hui la 12Ã¨me Ã©dition de son **Security Intelligence Report** (SIRv12). Ce nouveau rapport rÃ©vÃ¨le la vivacitÃ© du ver Conficker, dÃ©tectÃ© prÃ¨s de 220 millions de fois dans le monde au cours des 30 derniers mois, ce qui en fait lâ□□une des menaces les plus persistantes pour les entreprises.

Lâ□□Ã©tude souligne Ã©galement les raisons de la propagation du ver liÃ©es principalement Ã la faiblesse ou lâ□□usurpation de mots de passe. Elle met Ã©galement en lumiÃ¨re des vulnÃ©rabilitÃ©s pour lesquelles une mise Ã jour de sÃ©curitÃ© existe pourtant dÃ©jÃ .

Un paysage de menaces en mouvement : les cybercriminels sâ□□appuient sur des attaques Ã la fois gÃ©nÃ©ralisÃ©es mais Ã©galement ciblÃ©es vers des entreprises et individus dÃ©finis.

Â« *Conficker reste lâ□□un des problÃ¨mes majeur de sÃ©curitÃ© que nous rencontrons aujourdâ□□hui, alors que nous avons tous les atouts en main pour le contrecarrer* Â», confie **Bernard Ourghanlian**, Directeur Technique et SÃ©curitÃ© chez Microsoft France. Â« *Conficker montre ainsi combien la technologie seule ne peut constituer une rÃ©ponse aux dÃ©fis posÃ©s en matiÃ¨re de sÃ©curitÃ© informatique. Il est essentiel que les diffÃ©rentes parties prenantes agissent ensemble. Les organisations en particulier doivent accentuer leurs efforts sur la mise Ã jour rÃ©guliÃ¨re et permanente de leurs systÃ¨mes et sur la rigueur de la gestion de leurs mots de passe afin de se protÃ©ger contre les menaces les plus courantes.* Â»

Des attaques en baisse en France

Bien quâ□□ayant enregistrÃ© une baisse de 10% au 4Ã¨me trimestre, la France reste particuliÃ¨rement touchÃ©e par les Adware* Ã 53% contre une moyenne mondiale de 37%. NÃ©anmoins, la bonne Ã©lÃ¨ve de lâ□□Europe en matiÃ¨re de sÃ©curitÃ© a connu une baisse du taux dâ□□infections entre le premier et le quatriÃ¨me trimestre de lâ□□annÃ©e 2011.

Des vecteurs dâ□□infections bien connus et qui peuvent Ãªtre stoppÃ©s

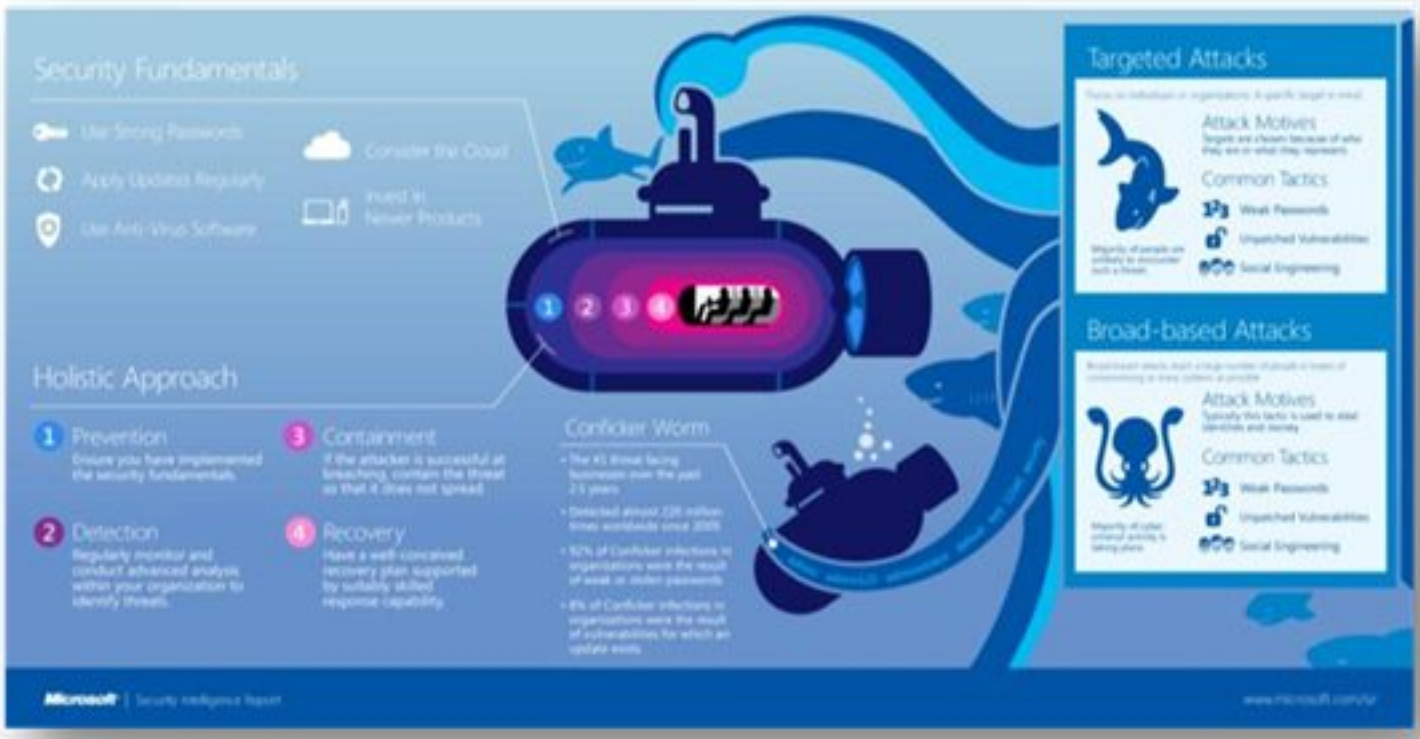
Microsoft recommande aux particuliers et aux entreprises franÃ§aises de suivre les principes de sÃ©curitÃ© suivants pour assurer leur protection :

Evolution des logiciels malveillants et potentiellement dangereux en France en 2011

â□¢ Utilisation de mots de passe forts** et sensibilisation des collaborateurs Ã leur importance

â□¢ Maintien des systÃ¨mes Ã jour en appliquant rÃ©guliÃ¨rement les mises Ã jour disponibles pour lâ□□ensemble des produits

â□¢ Utilisation dâ□□un logiciel antivirus de confiance



â□¢ Investissement dans les produits les plus rÃ©cents afin de bÃ©nÃ©ficier dâ□□une protection logicielle de qualitÃ©

â□¢ Envisager le Cloud comme une solution dâ□□hÃ©bergement bÃ©nÃ©ficiant dâ□□une gestion efficace de la sÃ©curitÃ©

Le rapport SIR de Microsoft rÃ©vÃ¨le Ã©galement que bien des menaces, connues sous le nom de Â« menaces persistantes avancÃ©es Â», ou APT (Advanced Persistent Threats), ne sont gÃ©nÃ©ralement pas aussi Ã©voluÃ©es quâ□□elles le paraissent. Dans la plupart des cas, ces attaques passent par des vecteurs dâ□□infection bien connus (mots de passe faibles ou usurpÃ©s

et vulnÃ©rabilitÃ©s pour lesquelles une mise Ã jour de sÃ©curitÃ© a Ã©tÃ© publiÃ©e). Leur rÃ©ussite tient principalement Ã une forte volontÃ© de perdurer et de compromettre la cible visÃ©e. Câ□□est pour cette raison que Microsoft prÃ©fÃ¨re parler dâ□□attaques ciblÃ©es menÃ©es par des adversaires dÃ©terminÃ©s.

Evolution du ver Conficker depuis 2009 dans le monde

Â« *Qualifier les menaces informatiques ciblÃ©es et persistantes dâ□□Â« Ã©voluÃ©es Â» peut parfois Ãªtre trompeur. En gÃ©nÃ©ral, ces attaques ne sâ□□appuient en effet sur aucune technique ou technologie trÃ¨s Ã©voluÃ©e, contrairement Ã ce que le terme APT pourrait faire croire. Dans la majoritÃ© des cas, elles exploitent simplement un mot de passe faible ou usurpÃ©, des vulnÃ©rabilitÃ©s pour lesquelles il existe pourtant une mise Ã jour de sÃ©curitÃ© ou encore lâ□□ingÃ©nierie sociale.* Â» prÃ©cise Bernard Ourghanlian, Directeur Technique et SÃ©curitÃ© chez Microsoft France.

Une approche plus globale de la gestion des risques

Comme lâ□□a soulignÃ© **Scott Charney**, vice-prÃ©sident de Microsoft Trustworthy Computing lors de son discours dâ□□ouverture Ã la confÃ©rence RSA 2012, en fÃ©vrier dernier, Microsoft recommande aux entreprises dâ□□adopter une approche plus globale de la gestion des risques. Objectif : mieux lutter contre les attaques ciblÃ©es ou Ã grande Ã©chelle et agir aux niveaux suivants :

â□¢ PrÃ©vention : respect des principes de sÃ©curitÃ© fondamentaux et attention particuliÃ¨re Ã la gestion des configurations et au dÃ©ploiement rÃ©gulier des mises Ã jour de sÃ©curitÃ©

â□¢ DÃ©tection : surveillance attentive et analyses poussÃ©es afin dâ□□identifier les menaces. Les entreprises doivent se tenir informÃ©es des Ã©vÃ©nements de sÃ©curitÃ© et sâ□□appuyer sur des analyses de sÃ©curitÃ© dignes de confiance

â□¢ Isolation : lâ□□entreprise visÃ©e doit configurer son environnement pour faire face Ã dâ□□Ã©ventuelles attaques ciblÃ©es menÃ©es par des adversaires dÃ©terminÃ©s. Il est possible dâ□□isoler les activitÃ©s de lâ□□attaquant afin de prendre le temps dâ□□identifier et de contrecarrer lâ□□attaque pour en minimiser lâ□□impact. Pour isoler une attaque, il convient de concevoir des modÃ¨les dâ□□administration du domaine qui prÃ©servent les informations dâ□□identification de lâ□□administrateur et dâ□□appliquer les technologies disponibles (comme le chiffrement IPsec du rÃ©seau) de maniÃ¨re Ã limiter toute interconnexion inutile sur le rÃ©seau.

â□¢ RÃ©cupÃ©ration : Il est important de disposer dâ□□un plan de rÃ©cupÃ©ration rÃ©flÃ©chi, accompagnÃ© de processus de rÃ©ponse aux incidents bien adaptÃ©s. Lâ□□entitÃ© visÃ©e doit rÃ©unir un Â« comitÃ© de crise Â» pour dÃ©finir les prioritÃ©s dâ□□intervention et tester la capacitÃ© de lâ□□entreprise Ã se rÃ©tablir aprÃ¨s plusieurs scÃ©narios dâ□□attaques diffÃ©rents.