30 minutes pour pirater un Mac Mini, oui mais…

Oui, mais la presse oublie juste de donner plusieurs détails qui ont leur l'importance.

Tout commence par un concours de hacking lancé par un jeune Suédois certain du niveau de sécurité de son OS fétiche : Mac OSX. Il met donc à disposition sur Internet un ordinateur Mac Mini – à jour – qui est censée résister aux attaques de pirates volontaires. À peine six heures après le début du concours, la machine est compromise ! L'auteur du piratage démonstratif, contacté par Zdnet Australie, explique qu'il a utilisé une vulnérabilité encore inconnue du grand public (une faille 0-day) pour obtenir les droits du 'root' et qu'il lui aurait fallu à peine 30 minutes pour s'emparer du système. Effrayant ! Mais certains sites Internet à forte audience se sont empressés de reprendre l'information et ont oublié d'expliquer qu'un compte SSH (service qui n'est pas activé par défaut), avec certes des privilèges limités, était mis à disposition des challengers. Exit donc la faille distante dont personne ne connaît encore l'existence. L'exploit du jeune pirate prend une tout autre dimension, il s'agit en réalité d'une 'escalation de privilèges' en local et non de l'exploitation d'une vulnérabilité critique à distance qui aurait pu aboutir à l'exécution de commandes arbitraires comme certains articles le laissent penser. **Trop peu d'informations pour être crédible** Malheureusement pour la communauté Mac, trop peu d'informations transparaissent sur les conditions de ce concours. L'organisateur n'a pas précisé s'il avait utilisé une version 'server' ou 'client' de MacOSX et ne dit pas non plus si des logiciels tiers étaient installés sur la machine. Les conditions du challenge restent donc relativement obscures, ce qui ne tend pas à crédibiliser les résultats. **Des motivations financières ?** Quelles pourraient être les motivations de l'organisateur anonyme ? Une piste se dévoile lorsqu'on visite son site Internet du concours : la publicité au clic. Prenez un sujet à la mode, laissez planer l'ombre du doute et ajoutez une pincée de 'menace communautaire'. Vous obtenez un cocktail marketing détonnant qui génère une couverture presse étonnante et bien évidemment des centaines milliers de visites rémunératrices en provenance du monde entier. CQFD. De là à dire que le piratage faisait en fait partie d'une stratégie commerciale bien échafaudée… Il y en a bien qui gagnent 1 million de dollars en vendant des pixels sur une page web !