Les attaques informatiques s’achètent sur le blackmarket | Le Net Expert Informatique

	Les attaques informatiques s’achètent sur le blackmarket

De 75 dollars le million d'adresses e-mail à plusieurs milliers de dollars pour une faille zero day exploitable… G Data a plongé dans le « blackmarket » pour en ressortir les principaux tarifs du marché de la cybercriminalité.

G Data s'est penché sur le marché de la cybercriminalité pour en étudier fonctionnement et offres de contenus. Baptisé « blackmarket », cet environnement construit autour de sites spécialisés, de forums privés, de structures d'anonymisation (proxy, VPN anonymes, réseau Tor…), de messageries protégées, de serveurs bulletproof (peu regardants sur la nature des fichiers stockés), de moteurs de recherche spécialisés et autres places de marchés de produits illicites, permet d'accéder à des montagnes de données personnelles, des kits de piratages en tout genre et de services d'attaques à la demande.
Au bout de son plongeon dans le blackmarket, les experts du SecurityLabs de l'éditeur allemand spécialisé en solutions de sécurité en a ressorti quelques informations éclairantes sur la vitalité du marché de la cybercriminalité. Un marché dont les tarifs évoluent entre une poignée de dollars et plusieurs centaines. La vente de données personnelles illégalement collectées se situe dans la zone basse des tarifs et, surtout, se commercialisent en volumes. Ainsi les accès aux comptes e-mails (adresse, nom d'utilisateur et mot de passe) se négocient 5 dollars le lot de 10 000. Les seules adresses e-mails, celles que se font notamment dérober les opérateurs et qui seront essentiellement exploitées pour des campagnes de phishing, ne se revendent pas plus de 10 dollars par poignées de 100 000, autour de 75 dollars le million. Les profils numériques qualifiés sont, eux, d'autant plus rentables qu'ils se revendent à l'unité : autour de 50 dollars pour une carte bancaire valide de type Gold ou Premier, un compte bancaire ou Paypal; 70 dollars l'identité complète dite Fullz (nom, prénom, adresse postale, données de cartes bancaires, comptes email, comptes bancaires).

Plusieurs milliers de dollars la faille zero day exploitable
Les cybercriminels financièrement plus ambitieux orienteront leurs activités vers la vente de produits et services. L'installation d'un Bot, bien utile pour prendre le contrôle d'un réseau de PC infectés, se négocie autour de 50 dollars les 1000 machines à la soldes des cyberattaquants. Lesquels pourront également exploiter ces Bots pour organiser des attaques par déni de service distribué (DDoS). Un service proposé entre 10 et 200 dollars l'heure d'attaque. Le tarif pour une campagne de spam, non traçable (via un service de diffusion hébergé sur un serveur bulletproof) tombe en revanche autour de 5 dollars les 20 000 envois.
La création et l'hébergement (sur un serveur piraté) d'une page web infectieuse dans le cadre d'une campagne d'hameçonnage (phishing) se facture entre 10 et 30 dollars. Mais on trouve également des outils d'attaques plus onéreux (car censés être plus efficaces). Par exemple, le kit d'exploitation Nuclear, qui exploite les bannières publicitaires Google Ads pour dérouter l'utilisateur vers un site infectieux, est disponible autour de 1500 dollars. La palme revient aux outils capables d'exploiter les failles zero day de Windows à raison de plusieurs milliers, voire plusieurs dizaines de milliers de dollars, selon G Data.

Source : http://www.silicon.fr/besoin-dune-attaque-ddos-comptez-entre-10-200-dollars-de-lheure-118545.html
Par Christophe Lagane