Le bon, la brute et le 'leecher' au pays des vulnérabilités !

Des sociétés comme iDefense ou Tipping Point – filiale de 3Com – ont inauguré, il y a quelques mois, un programme de « fidélisation » permettant aux chercheurs indépendants d'être rémunérés lorsqu'ils parviennent à découvrir une vulnérabilité.

En échange de la primeur de l'information, les auteurs de découvertes significatives peuvent se voir remettre une prime allant jusqu'à 5.000 dollars. D'autres sociétés comme ImmunitySec ou Core Technologies préfèrent opter pour une autre approche, plus subtile, et un modèle économique différent. Les deux entreprises commercialisent une plate-forme de tests accompagnée de nombreux exploits. La plate-forme est régulièrement mise à jour et les clients bénéficient ainsi, après signature d'un accord N.D.A (*Non disclosure agreement*, accord de confidentialité), d'exploits encore inconnus du grand public (0day). En France, un des derniers bastions à proposer en libre téléchargement une compilation d'exploits vient de tomber. En effet, cette semaine – l'autoproclamé CERT ? FrSiRT (ex K-otik) a annoncé qu'il allait désormais commercialiser l'accès à sa **base d'exploits**. La jeune entreprise de Montpellier aurait-elle subi les foudres d'un rappel à l'ordre de la part des autorités françaises ? Après avoir soutenu mordicus les effets néfastes de la LEN sur le *full-disclosure*, il semblerait que le FrSirt tombe sous le coup de l'article « 323-3-1 » et décide finalement de respecter la réglementation. Ce changement de politique soudain et forcé n'est malheureusement pas du goût de tout le monde. Tom Ferris, 'webmaster' du célèbre «Security-Protocols.com» n'accepte pas de voir le travail de chacun monnayé de la sorte. L'expert explique que la plupart des codes disponibles sur le site français sont en fait issus de plusieurs sites gratuits dont **milw0rm.com** et propose de récupérer plus de 600 exploits publiés sur FrSirt grâce aux fonctionnalités de cache de Google. Au passage, Security-Protocols.com enfonce le clou en accusant le site français de ne pas accorder les crédits appropriés aux véritables auteurs des exploits copiés publiés. *NB: 'Leecher': terme dérivé du mot anglais* 'leech' *signifiant sangsue.*