Le Web 2.0 a-t-il besoin d'une sécurité Web 2.0 ?
Par Leif Kremkow, Directeur Technique, Qualys France

Le Web 2.0, la deuxième génération de développement et de conception Web, est en plein essor, tout comme les applications qui s'appuient sur cette technologie. Des sites interactifs comme LinkedIn, Twitter, voire des sites Web d'entreprise, sont de plus en plus populaires. Et pourtant, de nombreux départements informatiques ne sont pas préparés aux menaces nouvelles et émergentes associées à ce phénomène. En effet, dans la mesure où toujours plus d'entreprises se reposent sur le Web pour développer leur activité, les possibilités d'attaque sont sensiblement multipliées. Les entreprises doivent donc réajuster leurs pratiques de sécurité face à l'univers du Web 2.0.

En règle générale, les failles de sécurité potentielles, ou vulnérabilités, ciblent les informations personnelles et économiques créées et stockées dans certaines applications Web 2.0, notamment Google Docs et Mobile Me. À l'aide de programmes JavaScript évolués spécifiquement développés pour capturer des données, les pirates peuvent rediriger les utilisateurs vers une parfaite copie du site qu'ils souhaitent visiter. Ensuite, une fois les informations d'identification saisies, elles sont transmises à leur insu aux pirates qui disposent ainsi des informations nécessaires pour accéder à des informations métier sensibles.

De nouvelles méthodes d'attaques sont régulièrement utilisées par les pirates qui profitent des technologies déjà déployées. Prenons l'exemple de Facebook qui permet à des tiers d'héberger leurs propres applications sur le site sous la forme de jeux ou de quizzes. Le code nécessaire est exécuté indépendamment de Facebook. En permanence, les pirates tentent de contourner les systèmes de sécurité déployés sur Facebook et d'accéder aux informations via le code exécuté sur le navigateur Web d'un tiers.

Le simple fait de remplir des formulaires en ligne permet à un pirate opportuniste d'obtenir des informations détaillées. En effet, même si le site est sécurisé, la technologie en arrière-plan qui suggère de saisir des informations déjà entrées auparavant peut être interceptée ainsi que les données concernant un particulier ou une entreprise.

Cependant, tous les pirates n'opèrent pas de la même manière. Certains choisissent d'exploiter des applications Web, notamment Twitter qui a essuyé une attaque en janvier

2009 ayant conduit au piratage de comptes de membres très actifs vers lesquels du contenu grotesque et choquant a été téléchargé. L'autre stratégie consiste à exploiter le navigateur Web. Dans ce cas, les pirates essaiment du code JavaScript sur un grand nombre de sites Web pour collecter au final des données sur les personnes visitant ces sites. Plutôt que de cibler des applications Web spécifiques, c'est le navigateur Web qui sert de vecteur à des liens qui permettent de rediriger les utilisateurs vers d'autres sites « bidons » ou de charger du contenu offensif depuis d'autres destinations.

La méthodologie de ces attaques évolue parallèlement à la motivation des pirates. Au temps des premières attaques Web, il s'agissait uniquement de défacer un site en éditant son contenu et en y ajoutant des messages ou des images choquantes. Désormais, il est important de ne pas être démasqué pour que le propriétaire du site ne sache pas que sa sécurité a été compromise. Grâce à JavaScript, les pirates utilisent ces attaques pour obtenir de l'argent plutôt que pour nuire par principe. En 2007, le site Web du Dolphin Stadium, stade où se déroule la finale du championnat de football américain (Super Bowl XLI), a été attaqué et du code JavaScript malveillant avait été déposé sur l'en-tête de sa page d'accueil. Un programme enregistrant les saisies au clavier (« key logger») ou un fichier de « backdoor » était téléchargé sur l'ordinateur de l'internaute qui visitait ce site, permettant ainsi au pirate d'accéder à l'ensemble de la machine infectée. L'acte de piratage est passé inaperçu jusqu'à ce qu'une société de sécurité parcourt le site dans le cadre d'une analyse globale. Même si le site du stade a probablement été piraté en raison de sa popularité et parce qu'il faisait l'actualité à ce moment-là, ce piratage s'inscrivait dans le cadre d'une attaque plus vaste qui visait 25 000 sites Web.

De nombreux personnes associent à tort le piratage à la fraude à la carte de crédit et à la fraude bancaire. En effet, toute information recèle toujours une certaine valeur pour quelqu'un. Le vol d'un identifiant par exemple permet non seulement de dépenser l'argent d'autrui, mais aussi d'ouvrir des comptes crédits chez des fournisseurs ou d'ouvrir de nouveaux locaux, le tout au dépend d'un tiers. Les données des clients et des employés peuvent également avoir de la valeur pour certaines entreprises.

Tandis que les pirates évoluent en permanence et s'adaptent aux nouvelles technologies telles que le Web 2.0, les entreprises réagissent à leur tour. Désormais, les employés, mais aussi les départements informatiques, sont sensibilisés aux risques de sécurité et la plupart

des entreprises ont déployé des politiques concernant le téléchargement d'applications Web. Des patches, des alertes et des mises à jour de sécurité sont publiés régulièrement par les fournisseurs. Ils doivent être téléchargés dès qu'ils sont disponibles.

En outre, plusieurs outils peuvent aider à prévenir de telles attaques, notamment l'analyse des applications Web. Cette analyse est un processus automatisé qui recherche les vulnérabilités logicielles sur les sites Web en lançant ses propres attaques afin d'en analyser les résultats. En s'appuyant sur ces données, l'analyse propose une liste d'actions à exécuter pour empêcher les pirates d'accéder à leurs systèmes. Cette analyse s'avère tout particulièrement utile pour les PME au sein desquelles la sécurité Web pose problème, mais pour laquelle il n'y a pas toujours de ressources en termes de personnel et de coût pour l'administrer en permanence.

Une analyse du code source et une supervision permanente du site sont également de précieuses méthodes pour se protéger contre les attaques de pirates.

La technologie continue de progresser à un rythme effréné traînant dans son sillage des individus qui cherchent à en exploiter d'autres par appât du gain. En s'informant sur les risques potentiels et en associant des méthodologies préventives testées et éprouvées, le département informatique est bien armé pour affronter la menace constante des attaques de type Web 2.0.