Black Hat : des données personnelles expurgeables des serveurs cache

La conférence Black Hat ouvre ses portes aujourd'hui à Las Vegas. Et les chercheurs en sécurité s'apprêtent à dévoiler vulnérabilités et nouvelles méthodes d'attaques informatiques. C'est notamment le cas d'Omer Gil qui détaillera l'attaque Web Cache Deception, ou tromperie du cache web, ainsi que les moyens de s'en protéger.

Selon la fiche descriptive de la session, *« Web Cache Deception est un nouveau vecteur d'attaque Web qui expose diverses technologies et frameworks. En manipulant les comportements des serveurs Web et des mécanismes de mise en cache, les attaquants anonymes peuvent obtenir les informations sensibles des utilisateurs authentifiés de l'application et même, dans certains cas, prendre le contrôle de leurs comptes »*.

Concours actif de la victime

Expert en sécurité pour EY Advanced Security Center, Omer Gil avait précédemment évoqué cette méthode d'attaque sur son blog. Il y rappelle que, pour économiser de la bande passante, les serveurs Web tirent parti des fonctionnalités de mémoire cache qui stockent les fichiers statiques non sensibles (feuilles de style, scripts, textes, images, etc.), à travers les services de CDN (proposés par Akamai, CloudFlare, etc.), les systèmes d'équilibrage de charge (load balancer) et les proxy inverses (reverse proxy) qui peuvent gérer des caches locaux. Il s'avère qu'un attaquant pourrait tirer parti de ce système d'optimisation du réseau en interrogeant directement le serveur cache pour espérer en extraire les données précédemment enregistrées suite à une requête légitime.

« Un attaquant qui parvient à attirer un utilisateur connecté pour accéder à http://www.example.com/home.php/logo.png entraînera la mise en cache de cette page -contenant le contenu personnel de l'utilisateur- et le rendra donc accessible au public, considère le chercheur. *Cela pourrait être pire encore si le corps de la réponse contient (pour une raison quelconque) l'identifiant de la session, les réponses de sécurité ou les jetons CSRF (Cross-Site Request Forgery, une faille des services d'authentification, NDLR). Tout ce que l'attaquant doit faire alors est d'accéder à cette page et afficher ces données. »* Autrement dit, l'attaque nécessite le concours actif de la victime qui doit initier la première requête avant que l'attaquant puisse ensuite accéder au serveur cache.

Paypal affecté

Une méthode qui avait notamment affecté les services de Paypal, alertait Omer Gil en février dernier. Un attaquant pouvait ainsi potentiellement récupérer les noms d'un utilisateur du service, son crédit en cours, les quatre derniers chiffres de sa carte bancaire, les données de transaction, son numéro de passeport, ses adresses mails et postales ou encore son numéro de téléphone. Si Paypal a corrigé la vulnérabilité avant la publication du billet, et remercié au passage le chercheur de 3 000 dollars pour sa découverte, les risques d'attaques similaires persistent sur d'autres applications qu'Omer Gil n'entend pas rendre publiques. *« Dans ces cas, il était possible de prendre le contrôle total de l'application de l'utilisateur*, écrit-il. *Cela était possible car l'ID de la session ou les réponses*

de sécurité pour récupérer le mot de passe d'un utilisateur étaient inclus dans le code HTML des pages vulnérables. »

Le chercheur souligne encore qu'une quarantaine de formats de fichiers sont exploitables pour tirer parti de la vulnérabilité. Autant d'éléments qu'il entend détailler plus amplement à Las Vegas.

Lire également

Comment la CIA suit les PC à la trace à l'aide du Wifi
Un malware furtif est passé inaperçu pendant des années sur Mac
Suède : scandale national après l'exposition de données secrètes sur le Cloud

Photo credit: Skley via Visual hunt / CC BY-N