5 mois après : le bilan de la faille Heartbleed

Depuis sa divulgation, en avril dernier, la faille Heartbleed, touchant OpenSSL, alimente les spéculations dans les cercles de la sécurité informatique. Avec une interrogation récurrente : **la NSA américaine avait-elle connaissance de cette vulnérabilité** bien avant sa divulgation publique ? Une étude menée par des chercheurs de plusieurs universités américaines tend à **éloigner cette hypothèse**, leur analyse montrant que les attaques à grande échelle exploitant Heartbleed n'ont commencé qu'environ 24 heures après que l'information a été rendue publique.

« *Nous n'avons trouvé aucune preuve de l'exploitation de la faille avant sa divulgation publique, mais nous avons détecté des tentatives d'exploit ultérieures, émanant de près de 700 sources et commençant moins de 24 heures après la publication de l'information* », expliquent les auteurs, une dizaine de chercheurs issus de **quatre universités américaines différentes**, dont Berkeley. Pour mener cette analyse a posteriori, l'étude se base sur les traces collectées par trois systèmes passifs de collecte de données opérés par des universités ou des instituts de recherche américains ainsi que par un 'honeypot' hébergé sur Amazon EC2. Ce dernier disposant de l'historique le plus complet, remontant à novembre 2013.

Dans cette fenêtre allant de ce mois de novembre à avril 2014, « *aucun assaillant ayant connaissance de Heartbleed avant sa divulgation publique n'a mené de scan de grande ampleur à la recherche de serveurs vulnérables* », expliquent précisément les auteurs. Leur étude ne permet donc pas d'écarter des attaques ciblées exploitant Heartbleed avant avril dernier. Si la NSA semble ne pas avoir utilisé la faille d'OpenSSL pour se bâtir un catalogue de cibles potentielles, elle n'est donc pas totalement mise hors de cause.

44 sites du Top 100 touchés le jour J

L'étude américaine fournit également de très intéressantes statistiques sur l'ampleur de l'infection et la réaction des équipes d'administration. Selon les chercheurs, Heartbleed a affecté au maximum 55 % des sites HTTPS les plus populaires (figurant dans le premier million de sites attirant le plus de trafic selon le classement d'Alexa). Mais, en éliminant les sites qui utilisaient de vieilles versions de OpenSSL, moutures n'incluant pas le protocole Heartbeat (qui est à l'origine de la faille), les chercheurs estiment que, très probablement, **seul environ un quart de l'échantillon des sites HTTPS** – parmi le premier million du classement Alexa – étaient sensibles à la faille Heartbleed le

jour de divulgation, 44 des 100 sites les plus populaires (Google, Youtube, Yahoo, Pinterest, Instagram…). On est toutefois **loin des premières estimations** données par Codemicon, une des sociétés à l'origine de la découverte de la faille, qui estimait à l'époque que deux sites HTTPS sur trois étaient vulnérables. « *Ce chiffre représente la part de marché cumulée de Apache et Nginx (les deux principaux serveurs touchés, voir la liste complète ci-dessus, NDLR). Et il est surestimé car des opérateurs ont pu désactiver l'extension (Heartbeat, NDLR), utiliser des équipements dédiés SSL ou employer de vieilles versions d'OpenSSL non vulnérables* », raillent les auteurs de l'étude.

Web Servers		Mail Servers		Database Servers	
Apache (mod_ssl) [45]	Yes	Sendmail [62]	Yes	MySQL [62]	Yes
Microsoft IIS [46]	No	Postfix [62]	Yes	PostgreSQL [62]	Yes
Nginx [14]	Yes	Qmail [62]	Yes	SQL Server [46]	No
Lighttpd [62]	Yes	Exim [35]	Yes	Oracle [55]	No
Tomcat [17]	Yes	Courier [37]	Yes	IBM DB2 [38]	No
Google GWS [50]	Yes	Exchange [46]	No	MongoDB [47]	Yes
LiteSpeed [42]	Yes	Dovecot [35]	Yes	CouchDB [32]	No
IBM Web Server [38]	Yes	Cyrus [48]	Yes	Cassandra [6]	No
Tengine [13]	Yes	Zimbra [56]	Yes	Redis [35]	No
Jetty [51]	No				

Elle évalue également la **rapidité de réaction des administrateurs de sites**. Deux jours après la divulgation, la proportion de serveurs sites HTTPS vulnérables était tombée à 11 %, selon les chercheurs. Et à 6 % sur l'ensemble du parc des adresses IPv4. Sans surprise, la réaction des principaux services d'Internet a été la plus prompte : **24 heures après la divulgation, 95 des 100 premiers sites du classement Alexa** étaient patchés. Et l'ensemble du top 500 était protégé 48 heures après le vent de panique qui a soufflé sur le Web début avril.

Derrière, évidemment, la mise à niveau a été plus laborieuse, les chercheurs observant que **le déploiement du patch a plafonné après deux semaines**. Deux mois après la divulgation de la faille, 3 % des sites HTTPS faisant partie du premier million du classement Alexa restaient vulnérables. Un constat inquiétant. Signalons encore que l'étude affirme que la faille Heartbleed a rendu vulnérable « *plus de la moitié des nœuds Tor* » dans les jours qui ont suivi sa révélation.

Remplacement des certificats : peut mieux faire

Trois semaines après cet événement qui a tétanisé le Web, les chercheurs ont commencé à contacter les opérateurs de 200 000 sites toujours vulnérables, en se basant sur les contacts d'un annuaire Whois. « *Quand nous avons notifié les opérateurs réseau des sites non patchés dans leurs espaces d'adresses, le taux de mise à jour a progressé de 47 %* », se réjouissent les chercheurs, pour qui ce résultat montre que les **notifications massives de vulnérabilités** peuvent avoir des effets bénéfiques, n'en déplaisent à ceux qui trouvent ces opérations trop complexes ou inefficaces. « *De nombreux opérateurs notifiés ont expliqué qu'ils avaient essayé de patcher, mais qu'ils avaient oublié le système que nous avions détecté* », précisent les auteurs.

Si la réponse de la communauté Web est plutôt satisfaisante en matière de patching, elle l'est beaucoup moins en matière de certificats. Rappelons que l'exploitation de la faille permet, en théorie, de récupérer en mémoire des informations sensibles, comme des clefs cryptographiques. En avril dernier, Arnaud Soullie, auditeur chez Solucom, expliquait dans nos colonnes : « *Les découvreurs de Heartbleed ont dans un premier temps expliqué que les certificats n'étaient pas concernés par la faille. Mais, sur un environnement de test, deux assaillants sont parvenus à reconstituer la clef privée du serveur. Par mesure de précaution, il faut donc renouveler le certificat et régénérer une nouvelle clef privée ».* Dans les faits, **moins d'un quart des sites** faisant partie du premier million du classement Alexa ont remplacé leurs certificats dans la semaine suivant la divulgation. Si les sites les plus populaires ont réagi très vite, seul 10 % de ceux qui étaient encore vulnérables 48 heures après la divulgation

ont changé leurs certificats dans le mois qui a suivi. Et, parmi ces « *bons élèves* », 14 % ont 'oublié' de renouveler leur clef privée… annulant par là même le bénéfice provenant du remplacement des certificats.

A lire aussi :

Faille Heartbleed : la check-list pour s'en sortir
Piratage de l'hôpital US : Heartbleed fait des millions de victimes
La faille Heartbleed exploitée pour attaquer les VPN d'entreprise
Espionnage de la NSA : les 8 leçons d'Edward Snowden