Les cyber-attaques changent de forme…| Le Net Expert Informatique

	Les cyber-attaques changent de forme…

Akamai constate une évolution du profil des attaques informatiques par déni de service distribué (DDoS), mais aussi des assauts contre les services Web.

Le profil des attaques informatiques par déni de service distribué (DDoS, visant à rendre des ressources indisponibles en les saturant de requêtes) a fortement évolué en un an, tandis que de nouvelles menaces sont nées de l'adoption du protocole IPv6.
Telles sont les principales conclusions émises par Akamai dans la dernière édition de son baromètre Internet Security – document PDF, 93 pages – portant sur le 1er trimestre 2015.
Sur le volet DDoS, le constat est sans appel : les assauts se multiplient (+ 116,5 % d'une année sur l'autre). Les attaques sur la couche applicative (Layer 7) augmentent de 60 %, mais ne représentent encore qu'un cas sur dix.
Le reste des offensives se concentre sur l'infrastructure (Layers 3 & 4 ; + 125 %), qui permet de maximiser plus facilement la puissance des attaques tout en nécessitant moins de ressources.
Alors qu'un DDoS s'échelonnait en moyenne sur 17 heures au 1er trimestre 2014, la durée a avoisiné les 25 heures un an plus tard (+ 43 %). Des attaques plus longues, donc, mais aussi moins virulentes : 5,95 Gbit/s de bande passante moyenne, contre 9,7 Gbit/s un an plus tôt ; quant au nombre moyen de paquets envoyés par seconde, il baisse de 89 % (2,21 millions).
Akamai a tout de même relevé 8 attaques d'un volume supérieur à 100 Gbit/s.
Encore quasiment inexploité début 2014, le SSDP (« Simple Service Discovery Protocol ») est devenu, en l'espace d'un an, le principal facteur déclencheur des attaques DDoS (plus d'un cas sur cinq). Implémenté et activé par défaut sur des millions d'équipements (routeurs, webcams, imprimantes, TV connectées) pour leur permettre d'interagir sur un réseau local, ce protocole est souvent mal – ou pas du tout – sécurisé.
L'industrie du jeu vidéo concentre à elle seule 35 % des dénis de services répertoriés entre le 1er janvier et le 31 mars. Suivent le secteur IT (25 %), les télécoms (14 %), la finance (8,4 %), les médias (7,5 %), l'éducation (5 %), la distribution (2,3 %) et le secteur public (2 %).
Pour la première fois, Akamai inclut dans son baromètre les attaques contre les applications Web. Les analyses réalisées sur environ 180 millions d'échantillons ont permis de dégager 7 vecteurs de piratage.
Dans les deux tiers des cas, les cybercriminels ont exploité une faille de type LFI (« Local File Inclusion ») leur permettant d'accéder, en lecture, à des fichiers hébergés sur un serveur Web. On notera cette campagne massive venue d'Allemagne contre deux grands noms du secteur de la distribution via une vulnérabilité dans le plugin WordPress RevSlider.

SQL, HTTPS et IPv6
29 % des attaques recensées sont liées à des injections SQL* ; c'est-à-dire à l'exploitation d'une brèche dans une application qui interagit avec une base de données en introduisant une requête SQL non prévue par le système. Illustration avec cette campagne issue essentiellement d'Irlande et visant une société de l'industrie du voyage.
Les autres types d'attaques (inclusion de fichiers distants sur des serveurs Web, injection de code PHP, exécution de commandes shell sur le système visé…) n'ont été repérées que dans environ 5 % des cas. Sachant toutefois qu'au global, près de 10 % ont été menées sur des sites « sécurisés » en HTTPS…
Parmi les grandes tendances de l'année, Akamai pointe la menace grandissante des sites dits « booters » ou « stressers » et qui permettent de simuler des attaques DDoS. Alors qu'il y a encore un an, leur ampleur se limitait à 10 ou 20 Gbit/s, ils peuvent désormais lancer des assauts dévastateurs à plus de 100 Gbit/s, en exploitant notamment des techniques de réflexion du trafic.
Autre enjeu à surveiller : l'adoption du protocole IPv6, qui permet d'élargir l'espace d'adressage réseau… mais dont l'architecture est dite « imparfaite » par Akamai : il est possible de passer outre certaines protections implémentées dans IPv4. Il existe d'ailleurs « plusieurs signes » montrant que les cybercriminels mènent bien des recherches sur le sujet.
* Documentées depuis 1998, les attaques par injection SQL vont désormais bien au-delà du simple vol de données. Elles permettent aussi l'élévation de privilèges, l'exécution de commande, la corruption de systèmes…

Source : http://www.itespresso.fr/securite-it-cyber-attaques-changent-forme-97172.html