F5 Labs : L'Europe sous le feu des attaques DDoS

février 2018 par F5

F5 Labs publie ses derniers chiffres montrant comment les attaques DDoS continuent de croître et d'évoluer dans la région EMEA. Selon les données du Security Operations Center (SOC) de F5 Networks en Pologne, 2017 a vu une augmentation de 64 % du nombre d'attaques. L'EMEA concentre plus de 51 % des attaques DDoS signalées au niveau mondial.

Parallèlement, F5 a enregistré une croissance de 100 % de déploiement de sa technologie de Web Application Firewall (WAF) par ses clients EMEA au cours de l'année écoulée. L'adoption de solutions anti-fraude a quant à elle augmenté de 76 %, et celle de lutte contre les DDoS de 58 %.

Des attaques moins puissantes, mais plus nombreuses et diversifiées L'une des tendances a été la baisse relative de la puissance des attaques. L'an dernier, le SOC a enregistré plusieurs attaques de plus de 100 Gbps, dont certaines dépassaient les 400 Gbps. En 2017, l'attaque la plus élevée enregistrée était de 62 Gbps. Cela suggère une évolution vers des attaques DDoS de niveau 7 plus sophistiquées, potentiellement plus efficaces et nécessitant moins de bande passante. 66 % des attaques DDoS signalées étaient d'ailleurs multi-vecteurs et nécessitaient des outils et des connaissances sophistiquées en matière d'atténuation pour pouvoir y faire face.

« La région EMEA est un point névralgique pour les attaques au niveau mondial », précise Laurent Pétroque, expert cybersécurité chez F5 Networks. « Il est essentiel que les organisations prennent en considération les évolutions de typologie si elles souhaitent s'assurer de bénéficier des bonnes solutions pour stopper les attaques DDoS avant qu'elles n'atteignent leurs applications ».

Les quatre saisons du renseignement sur la menace

Le premier trimestre 2017 a démarré en force, puisque les entreprises se sont trouvées confrontées à la gamme d'attaques perturbatrices la plus diversifiée observée à ce jour. Les attaques de type UDP Floods se sont distinguées et ont représenté à elles seules 25 % de l'ensemble des attaques (les cybercriminels envoient généralement de gros paquets UDP (User Diagram Protocol) vers une destination précise ou des ports aléatoires, se déguisant en entités de confiance afin de pouvoir exfiltrer des données sensibles). En deuxième position, on retrouve les attaques par Réflexion DNS (18 %) et SYN Flood (16 %).

Le 1er trimestre a été le point culminant des attaques par Internet Control Message Protocol (ICMP), durant lesquelles les cybercriminels submergent les entreprises de paquets de "demande d'échos" (ping) sans attendre les réponses. En contraste frappant, les attaques du 1er trimestre de 2016 se divisaient à 50/50 entre UDP Floods et Simple Service Discover Protocol (SSDP) Floods.

Le deuxième trimestre s'est avéré tout aussi intense, les attaques de type SYN Floods se plaçant en tête du peloton d'attaques (25 %), suivies par les attaques Network Time Protocol Floods et UDP Floods (20 % chacune).

L'élan des attaquants s'est poursuivi au 3ème trimestre avec des attaques de type UDP Floods occupant la première place (26 %). Les attaques NTP Floods ont également été particulièrement nombreuses (passant de 8 % durant la même période en 2016 à 22 % en 2017), suivies par les attaques par réflexion DNS (17 %).

2017 s'est terminée par une large prédominance des attaques UDP Floods (25 % de toutes les attaques). C'était également la période la plus chargée au niveau des attaques par réflexion DNS, qui représentaient 20 % de l'ensemble des attaques (contre 8 % en 2017 au cours de la même période).

Une autre découverte clé observée au cours du quatrième trimestre, et qui souligne de façon frappante la capacité des cybercriminels à se réinventer avec agilité, a été la façon dont le cheval de Troie Ramnit a considérablement étendu sa portée. S'il était initialement conçu pour frapper les banques, F5 Labs a constaté que 64 % de ses cibles pendant la période des Fêtes étaient des sites de e-commerce basés aux Etats-Unis. Parmi les autres nouvelles cibles, mentionnons les sites internet liés aux voyages, aux divertissements, à la nourriture, aux rencontres et à la pornographie. Parmi les autres chevaux de Troie bancaires observés qui étendent leur rayon d'action, Trickbot est également sorti du lot. Il infecte ses victimes grâce à des attaques d'ingénierie sociale, telles que le phishing ou le malvertising (l'utilisation de la publicité en ligne pour diffuser des logiciels malveillants), destinées à tromper les utilisateurs et les inciter à cliquer sur des liens malveillants ou à télécharger des programmes malveillants.

« Il ne fait aucun doute que les vecteurs et les tactiques d'attaques continueront de fortement évoluer dans la région EMEA en 2018 », précise Laurent Pétroque. « Il est essentiel que les entreprises disposent des bonnes solutions et des bons services pour protéger leurs applications où qu'elles se trouvent. 2017 a montré qu'une part grandissante du trafic Internet est désormais chiffré SSL/TLS et qu'il est donc impératif que les solutions d'atténuation DDoS soient en mesure d'examiner la nature de ces attaques de plus en plus sophistiquées. Une visibilité complète et un meilleur contrôle de la sécurité à chaque niveau sont essentiels pour que les entreprises restent pertinentes et crédibles aux yeux de leurs clients. Cela sera particulièrement important en mai 2018 lorsque le règlement général de l'UE sur la protection des données (RGPD) entrera en vigueur. »