Informations stratégiques

34 %

Pourcentage d'attaques DDoS des couches 3 et 4 subies par les institutions de services financiers

Les services financiers restent le secteur le plus touché par les attaques par déni de service distribué (DDoS) sur les couches 3 et 4. Viennent ensuite le secteur des jeux vidéo avec 18 % et celui de la haute technologie avec 15 %. Cette menace croissante est probablement due aux tensions géopolitiques actuelles, en particulier les guerres entre Israël et le Hamas et entre la Russie et l'Ukraine, qui ont entraîné une forte hausse de l'activité des hacktivistes dans le monde entier.

La croissance des API entraîne une augmentation des attaques DDoS de la couche 7

Bien que les applications Web soient traditionnellement les cibles privilégiées des cyberattaques, les attaques DDoS de couche 7 contre les API ont atteint des sommets notables au cours de la période considérée. Cela s'explique en grande partie par l'adoption grandissante des API dans les services financiers pour répondre à l'évolution des exigences réglementaires et de conformité. Alors que les organisations s'appuient de plus en plus sur les API, leurs adversaires adaptent leurs tactiques, et la sécurité des API devient une priorité absolue pour les entreprises d'aujourd'hui.

Les pics de trafic soulignent la nécessité d'évaluer les attaques DDoS en fonction de leur fréquence et de leur volume

Les attaques DDoS dans les services financiers révèlent un aspect critique : la fréquence des événements n'est pas toujours corrélée avec l'intensité de l'attaque. En effet, bien que le nombre d'attaques est plus faible au cours de certains mois, leurs données en Gbit/s indiquent des pics de trafic importants, ce qui souligne la nécessité de prendre en compte à la fois la fréquence et le volume des attaques lors de l'évaluation des impacts des attaques DDoS.

36 %

Pourcentage de domaines suspects ciblant les institutions financières

Les attaques par hameçonnage ciblent de plus en plus les clients des services financiers, augmentant les risques d'usurpation d'identité et de piratage de comptes. Cette tendance expose les institutions financières à une surveillance accrue de la part des régulateurs, et les violations érodent la confiance des clients.

30 %

Pourcentage de visites de pages dirigées vers des sites d'hameçonnage et d'usurpation d'identité de marque

Les pirates réussissent à diriger du trafic vers des sites frauduleux en imitant des sites Web et des applications de services financiers légitimes. Ils continuent de perpétrer des attaques par hameçonnage contre les institutions financières afin de s'emparer des précieuses informations sensibles qu'elles détiennent.