# Log4Shell : l'écosystème cyber structure sa réponse

Bientôt une semaine que la faille dite « Log4Shell » a éclaté au grand jour. Elle est critique autant par ses conséquences potentielles que par la multitude de ses vecteurs d'exploitation. Le composant problématique (la bibliothèque de journalisation Log4j) est effectivement très répandu dans l'écosystème Java. La liste des applications et des logiciels touchés en témoigne. En tout cas celle que tiennent les CERT européens. Elle s'accompagne d'indicateurs de compromission, de méthodes d'analyse et de solutions de contournement.

Ces solutions doivent parfois être combinées pour offrir une protection correcte. Il en est ainsi des règles de *firewall*. Les attaques sont susceptibles de les contourner aussi bien en exploitant des ports alternatifs qu'en mettant en œuvre des techniques d'obscurcissement.

## Log4j 2.16 : le correctif désormais complet ?

Le bulletin d'alerte du CERT-FR met l'accent sur ces techniques d'obscurcissement. En toile de fond, une recommandation aux entreprises : effectuer une analyse approfondie de leurs journaux réseau, à la recherche des chaînes de caractères utilisées pour déclencher l'attaque. Et faire, si possible, la corrélation avec les *logs* DNS. Puis, au niveau des logiciels affectés, filtrer et journaliser les flux sortants tout en vérifiant la disponibilité de correctifs. Les développeurs auront soin de passer à Log4j 2.15. Voire à la version 2.16. Publiée avant-hier, elle complète la correction en désactivant par défaut l'API JNDI et la fonction de *lookup*.

À son dernier pointage (mardi 14 décembre), Check Point recensait plus d'un million de tentatives d'exploitation de Log4Shell. Et fournissait un indicateur « brut » : à l'échelle mondiale, 44 % des réseaux *corporate* touchés. Principal objectif des assaillants : le minage de cryptomonnaies, assurait le groupe américain.

Les *cryptominers* sont aussi au premier rang dans l'analyse de Sophos. En la matière, la firme britannique mentionne entre autres le *botnet* Kinsing. Dans ce même rayon *botnet*, elle place Mirai et Tsunami. Tout en évoquant des tentatives de vol de données parmi lesquelles des secrets hébergés sur AWS. On retiendra, parmi ses statistiques, la suivante : 90 % des attaques se fonderaient sur le vecteur LDAP.

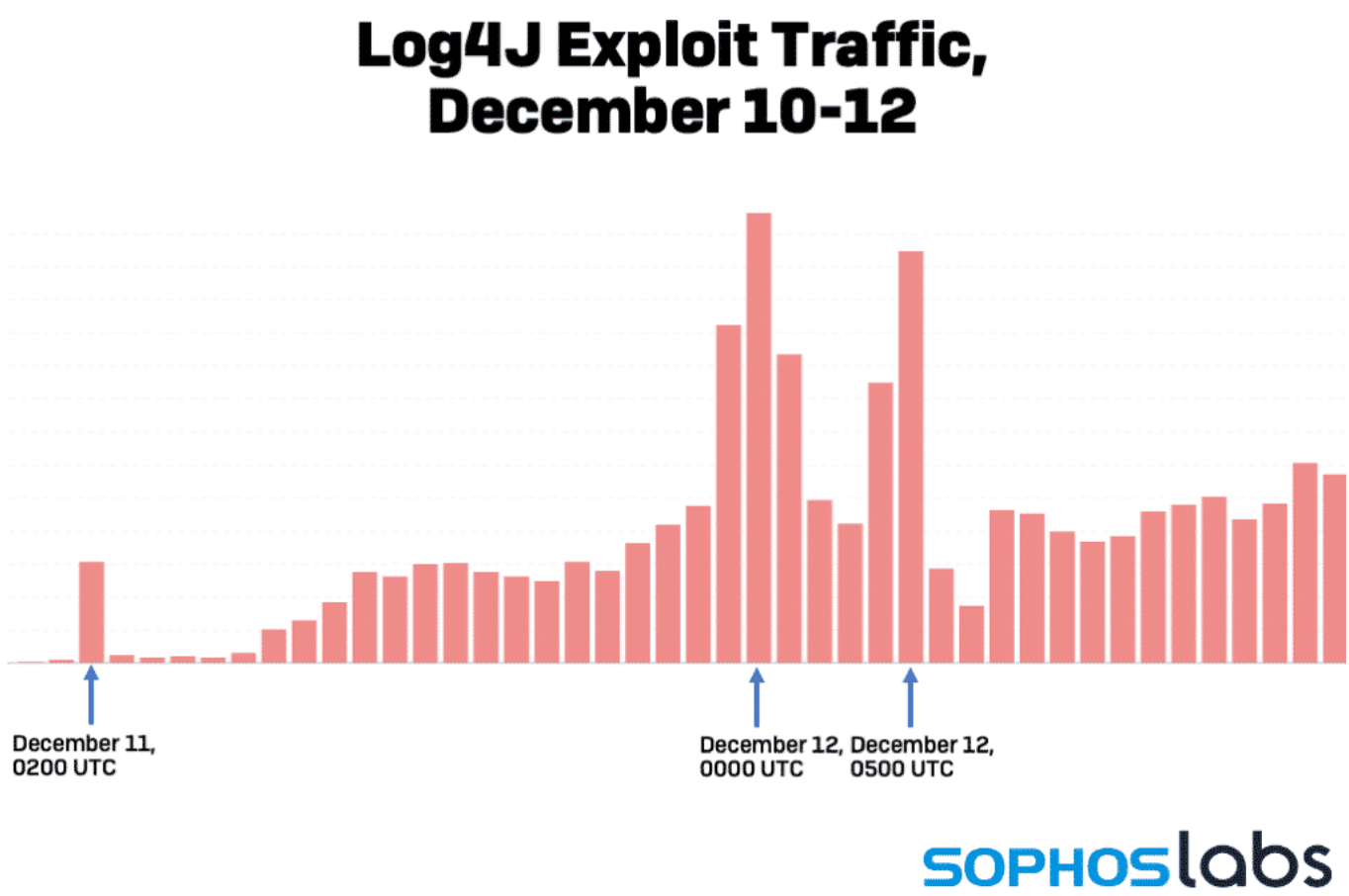


*Photo d'illustration © Quardia Inc. – Adobe Stock*