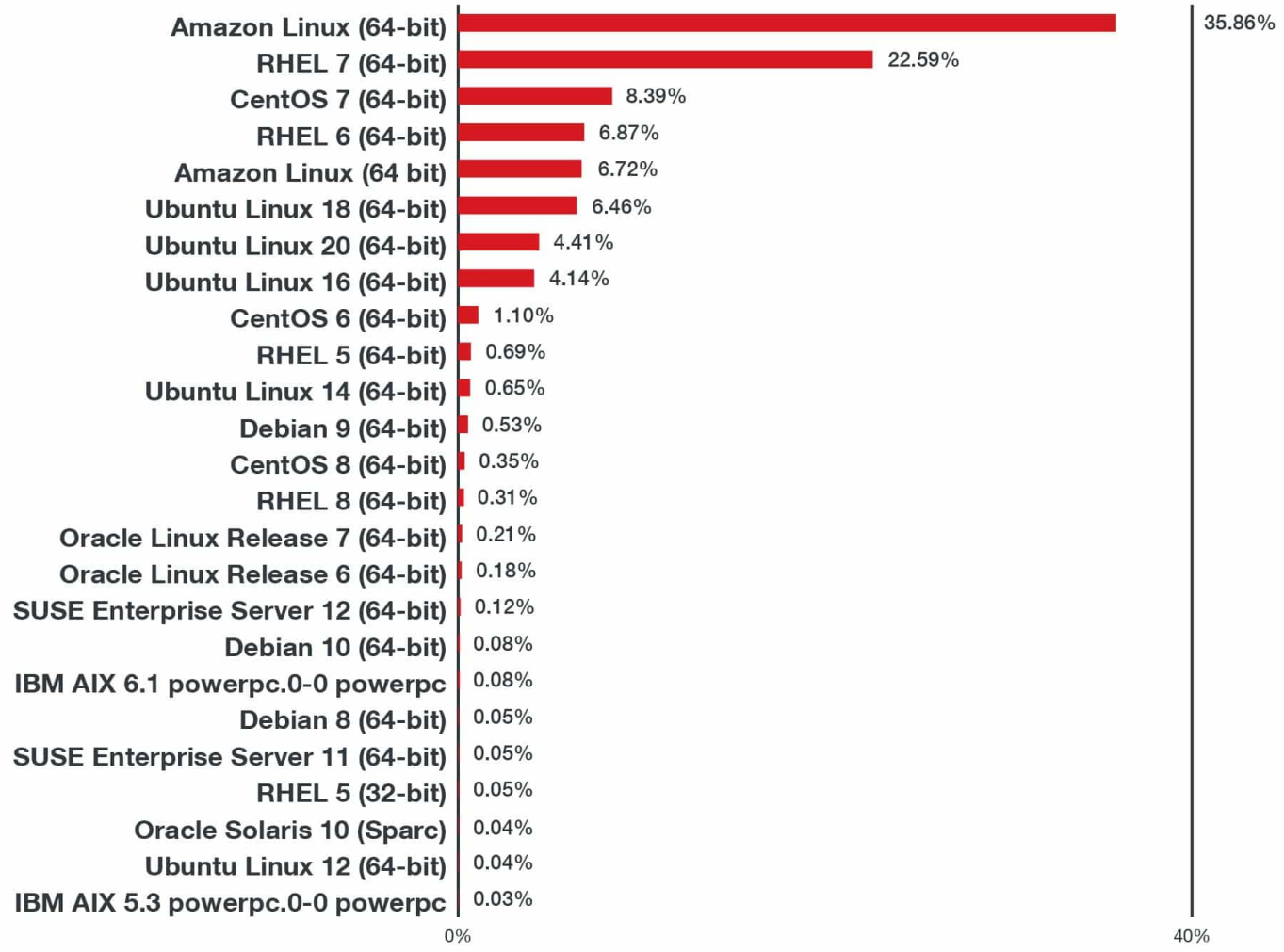
Serveurs Linux : beaucoup de distributions obsolètes ?

Les distributions obsolètes, monnaie courante sur les serveurs Linux ? Les éléments que communique Trend Micro ne permettent pas de l'affirmer. Ils donnent cependant quelques tendances.

L'indicateur le plus significatif provient des outils de prévention d'intrusion de l'éditeur américain. Sur quelque 50 millions d'événements détectés au premier semestre 2021, une part non négligeable sont survenus sur des OS approchant de leur fin de vie. Voire l'ayant atteinte. En l'occurrence :

- 22,59 % sur **RHEL 7**
  Le support complet de cette distribution a pris fin en août 2019. Elle est désormais en phase dite « maintenance » (correctifs de sécurité, mais plus de mises à jour de fonctionnalités), jusqu'au 30 juin 2024. Deux ans supplémentaires seront possibles… moyennant paiement. On est déjà à ce stade pour les versions Arm, POWER9 et System z.
- 8,39 % sur **CentOS 7**
  Le support complet s'est terminé le 6 août 2020. La phase de maintenance prendra fin le 30 juin 2024.
- 6,87 % sur **RHEL 6**
  Là, on est déjà passé sur le support étendu payant, jusqu'au 30 juin 2024. La phase « maintenance » a pris fin le 30 novembre 2020.



Les serveurs Linux, cibles des cryptomineurs

Le deuxième indicateur ne se fonde pas sur le volume de tentatives d'intrusion, mais sur celui des détections de menaces (13 millions d'événements de sécurité). Dans la catégorie « anciens OS », CentOS domine (les versions 7.4 à 7.9 regroupent près de 44 % du total des détections). Suivent CloudLinux Server (environ 40 %) et Ubuntu Server (7 %).

En se focalisant sur les dix principales familles de menaces, les détections se répartissent ainsi :

- 24,56 % de cryptomineurs
- 19,92 % de *webshells*
- 11,56 % de *ransomwares* (DoppelPaymer en tête, les serveurs Linux faisant souvent office de relais pour infecter des systèmes Windows)
- 9,65 % de *trojans*
- 3,15 % d'autres souches

Concernant les tentatives d'exploitation de failles, les volumes sont particulièrement élevés sur :

- CVE-2017-5638 (RCE sur Struts)
- CVE-2017-9805 (*idem*, mais dans le *plug-in* XStreams)

- CVE-2018-7600 (RCE sur Drupal)
- CVE-2020-14750 (RCE sur Oracle WebLogic)
- CVE-2020-25213 (RCE sur le *plug-in* File Manager de WordPress)

Photo d'illustration © ArtushFoto – Adobe Stock