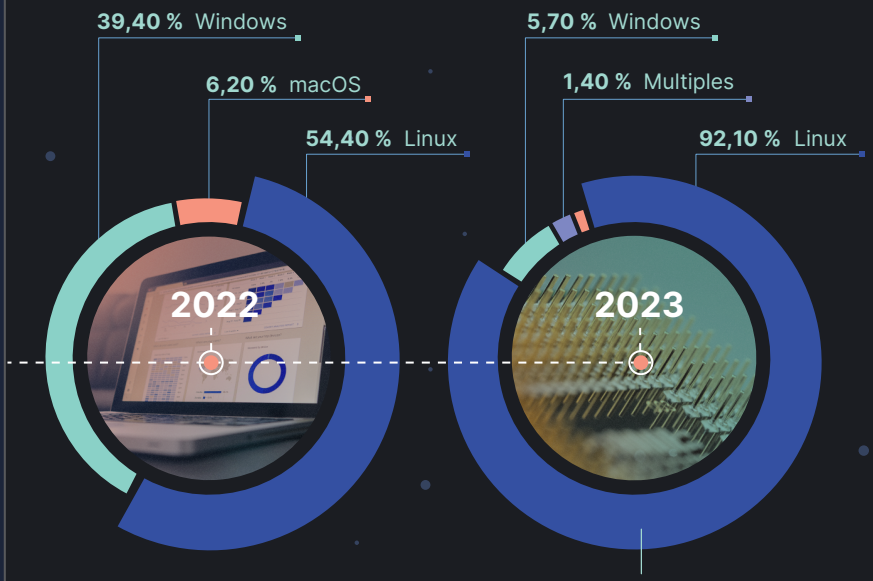
elastic security labs

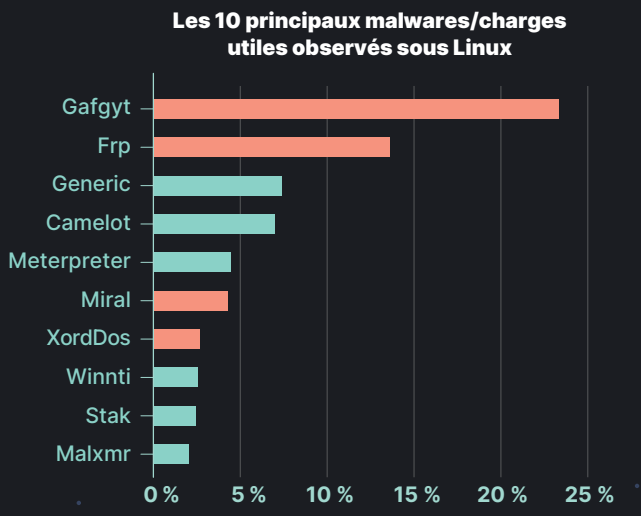
Méthodes des utilisateurs malveillants en 2023
Rapport d'Elastic sur les menaces mondiales

Notre rapport se fonde sur plus de **1 milliard de points de données**.

L'infrastructure Linux attire l'attention des utilisateurs malveillants.

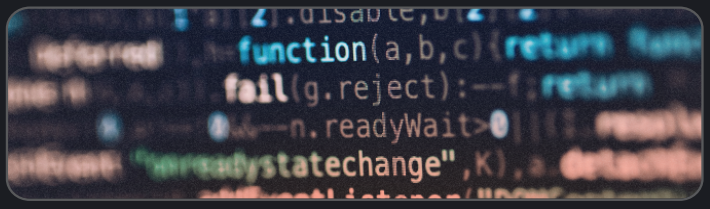


Le recours aux serveurs Linux a engendré une forte augmentation des signaux de malwares.



Les botnets sont souvent utilisés dans ce système d'exploitation. Ils tirent parti de la connectivité dans **environ 44 %** des attaques observées sur des systèmes Linux.

Le recours à l'Évasion par la défense sur les points de terminaison est une preuve de l'adaptation aux environnements hostiles.



Tactiques **MITRE ATT&CK** observées sur tous les points de terminaison	**ATTAQUES**
Évasion par la défense	**43,88 %**
Exécution	**29,20 %**
Persistance	**7,98 %**
Escalade des privilèges	**6,93 %**
Accès aux identifiants	**5,60 %**

Les utilisateurs malveillants s'appuient sur les défauts de conception du système d'exploitation, comme **BYOVD**, pour éviter les détections.

Les utilisateurs malveillants arrivent à leurs fins avec les techniques d'Accès aux identifiants dans les environnements cloud.

Tactiques **MITRE ATT&CK** observées sur l'ensemble des prestataires de services cloud	**% du signal**
Accès aux identifiants	**44,98 %**
Évasion par la défense	**23,02 %**
Exécution	**11,58 %**
Découverte	**6,04 %**
Persistance	**5,81 %**

Cette méthode s'avère fiable quand il est facile de collecter des données ou en l'absence de toute visibilité sur les utilisations frauduleuses.

Compréhension de la situation grâce au rapport d'Elastic sur les menaces mondiales

Étudiez en profondeur nos observations des signatures de malware, des comportements des points de terminaison et des fournisseurs cloud, mais aussi découvrez nos recommandations dans le rapport 2023 sur les menaces mondiales. Suivez Elastic Security Labs sur X (**@elasticseclabs**) et consultez notre blog afin de connaître les dernières nouveautés en matière de menaces, recherches et autres.