RAPID7

rapid7.com

Rapport 2024 relatif aux renseignements sur les attaques (Attack Intelligence Report) :

analyse de quatre années sur les vulnérabilités et l'exploitation des données

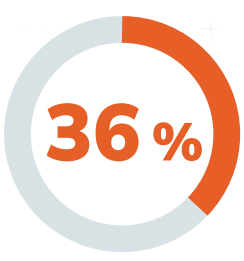
Dans son rapport de 2024 faisant état des renseignements sur les attaques, Rapid7 analyse quatre années de données sur les vulnérabilités et le comportement des attaquants. L'objectif est d'aider les professionnels de la sécurité à comprendre les risques, ainsi que les motivations et les tactiques des attaquants qui agitent le contexte actuel des cybermenaces. Voici quelques informations clés.

Un taux élevé d'attaques « zero day » est devenu la norme

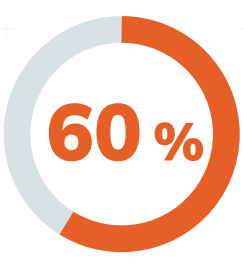
Le délai médian avant l'exploitation connue des CVE (vulnérabilités et expositions communes) selon des analyses menées par Rapid7 depuis 2020

des incidents de compromission de masse liés aux CVE suivis par Rapid7 entre janvier 2023 et février 2024 étaient dus à une attaque de type zero-day

Les exploits d'équipements de périphérie de réseaux ont explosé, à un rythme jamais constaté à ce jour.

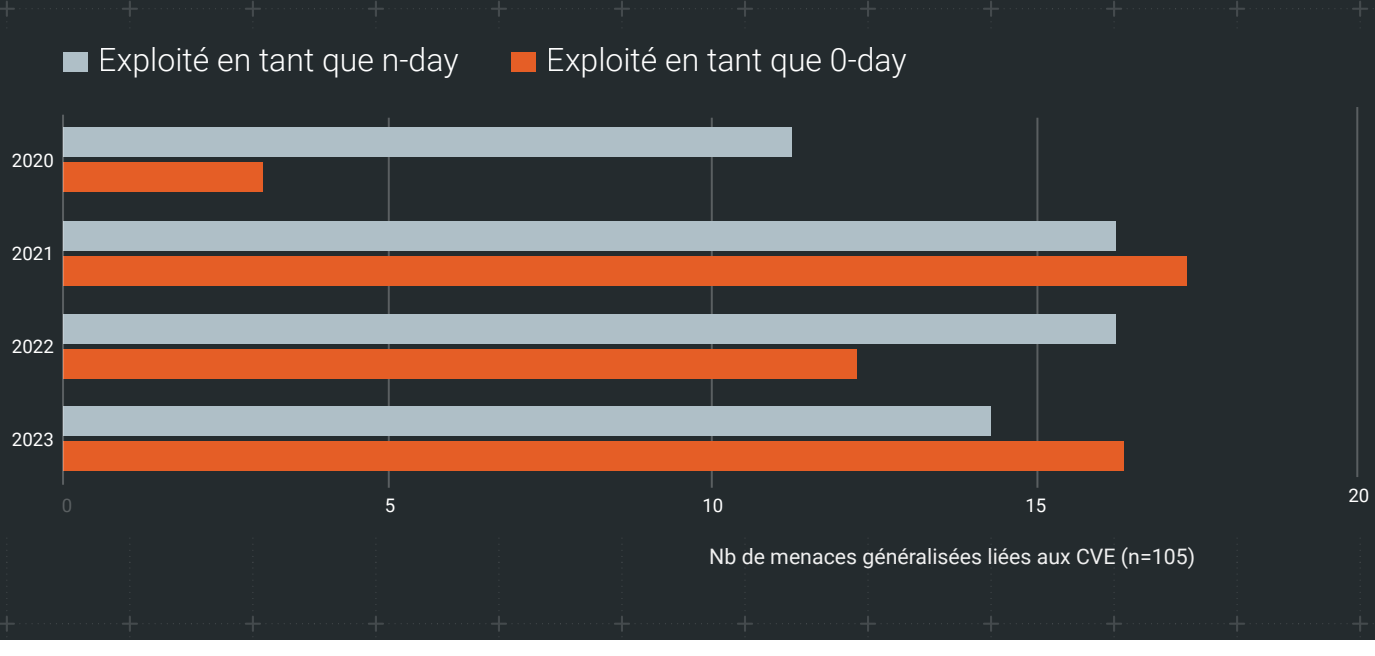


des menaces les plus répandues en 2023 ont affecté des **technologies de périphérique réseau**

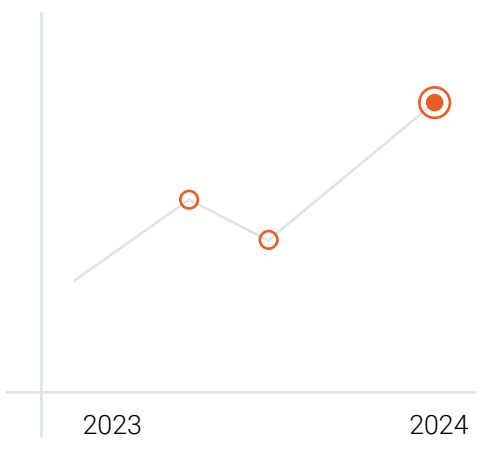


des vulnérabilités analysées par Rapid7 au niveau des équipements réseaux et de sécurité sont **exploitées par des attaques de type zero-day**

Menaces généralisées liées aux CVE 2020-2024



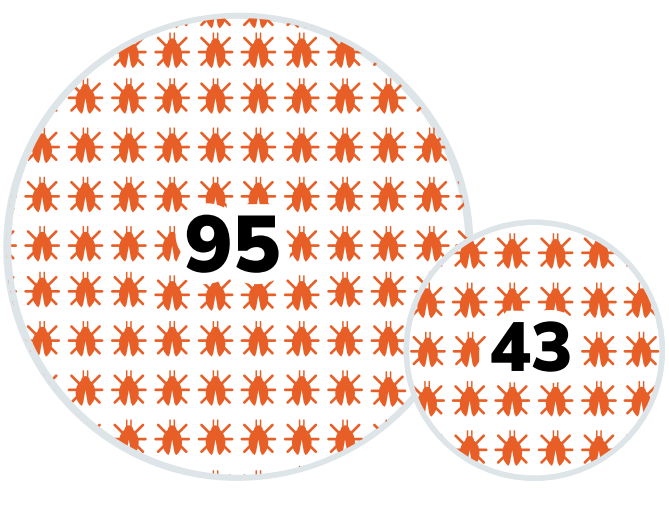
Les attaques par ransomware sont rapides, violentes et plus dévastatrices que jamais



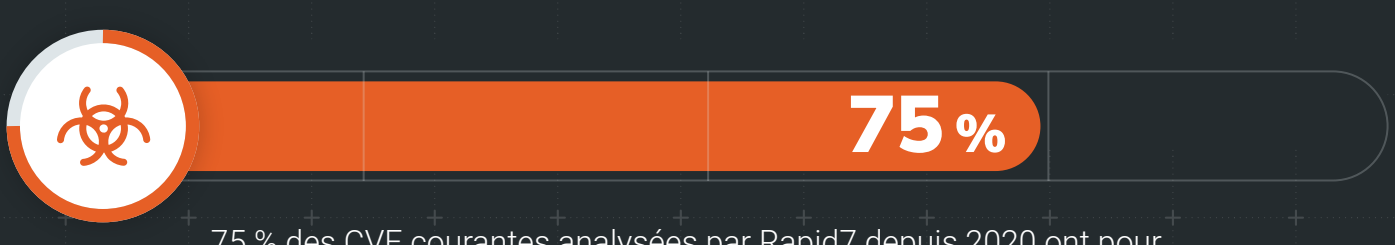
Rapid7 Labs a réalisé un suivi de plus de **5 600 incidents liés à des ransomwares entre janvier 2023 et février 2024***

*Ce nombre ne prend pas en compte les incidents non signalés

Le nombre de nouvelles familles de ransomwares a été réduit de moitié, ce qui indique que les modèles et capacités préexistants restent rentables pour les attaquants.

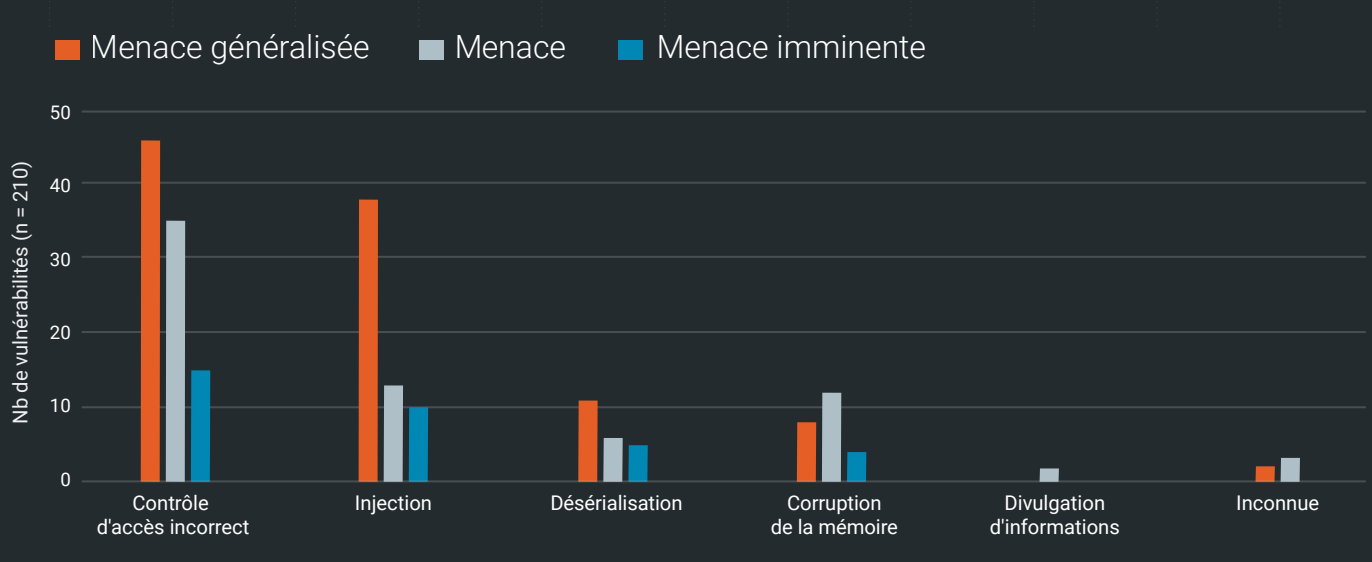


L'analyse des causes premières montre que les adversaires préfèrent exploiter des classes de vulnérabilité simples



75 % des CVE courantes analysées par Rapid7 depuis 2020 ont pour origine un contrôle d'accès inapproprié et des situations d'injection

Classes de vulnérabilité et statut des menaces 2020-2024



Comment agir ?

Comment améliorer notre résilience et notre préparation dans le contexte actuel des cybermenaces ? Quelques conseils :

40 %

des incidents sont dus à l'absence ou à aux incohérences de la MFA (authentification multifacteur). Celle-ci doit être une priorité absolue

Appliquer les principes du moindre privilège : autoriser la publication de la liste des accès standard ; mettre en œuvre un contrôle d'accès granulaire ; vérifier et mettre régulièrement à jour la liste des utilisateurs

Mettre en œuvre un solide programme proactif de gestion des risques de vulnérabilité dans le cloud et sur site

Créer des procédures d'application de correctifs zero-day pour les technologies critiques, en particulier les appareils de périphérie du réseau

En renforçant leur stratégie de sauvegarde hors site, les organisations résistent mieux aux risques d'attaques par ransomware

Téléchargez le rapport complet à l'adresse suivante : www.rapid7.com