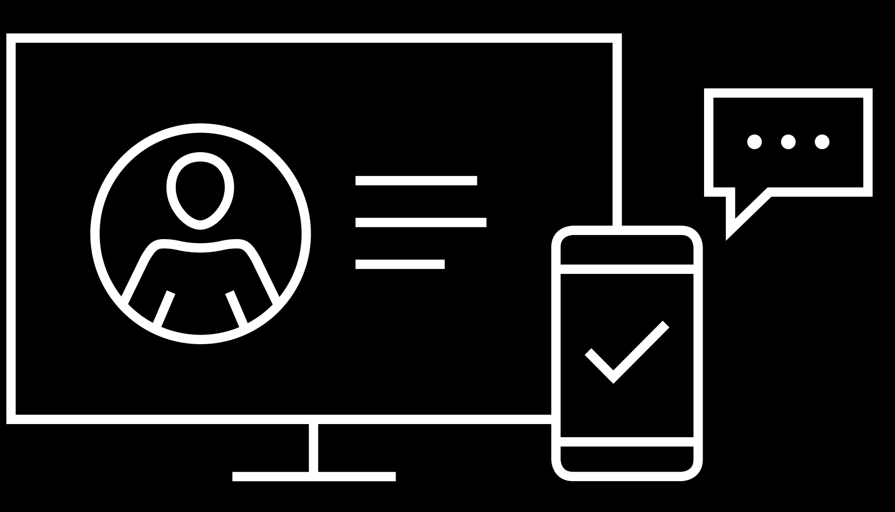
Le rapport qui fait autorité

Le Verizon Data Breach Investigations Report (DBIR) 2023 en sept points clés

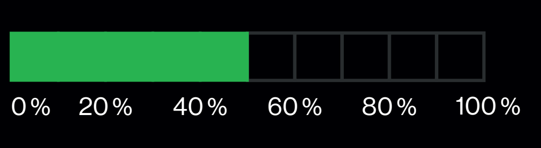
Les cybercriminels diversifient leurs attaques. Dans leur ligne de mire : les données d'entreprises comme la vôtre.

Tel est le principal enseignement de notre Data Breach Investigations Report 2023, qui passe au crible les tendances du cybercrime au cours des 12 derniers mois. Dans un style précis, mais non dénué d'un certain trait d'esprit, cette publication offre un éclairage pointu sur les schémas d'attaque qui dominent le champ des menaces.



Le pretexting gagne du terrain.

50 %

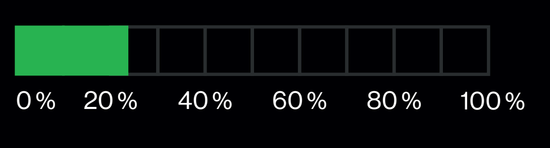


En 2022, 50 % des attaques par ingénierie sociale ont misé sur le pretexting, une technique visant à inciter la victime à divulguer des informations ou à accomplir une action susceptible d'aboutir à une compromission.

« Nous avons vos données. Vous devez payer. »

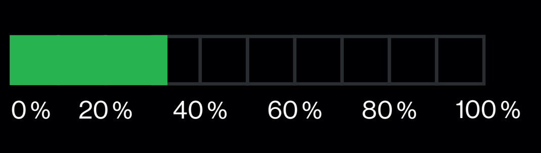
Dans le cadre d'une attaque par ransomware, l'entreprise victime voit ses données chiffrées et n'a d'autre choix que de payer une rançon pour les récupérer. Représentant 24 % de toutes les compromissions recensées, cette stratégie fait les beaux jours du crime organisé qui l'utilise dans plus de 62 % de ses attaques. Plus généralement, le ransomware est présent dans 59 % des incidents de sécurité avec comme motivation l'appât du gain.

24 %



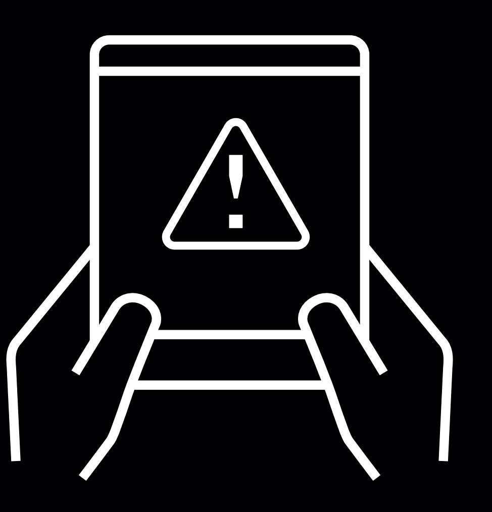
Le rythme des menaces s'accélère.

> 32 %



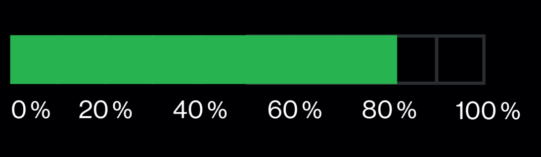
En 2021, une faille critique a été découverte dans Log4j, un utilitaire Java très répandu. Une fois exploitée, cette vulnérabilité permet aux hackers de prendre le contrôle des serveurs exposés. Dès la publication de la CVE, une déferlante de scans de vulnérabilités s'est abattue sur le web, au point que plus de 32 % de tous les scans effectués ont eu lieu dans les 30 jours suivant l'annonce.

Cet exemple montre la rapidité entre la découverte et l'exploitation généralisée.



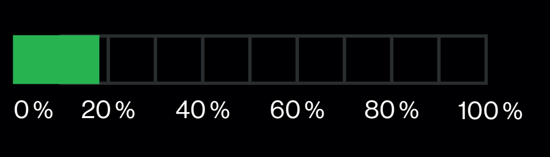
Si la plupart des menaces viennent de l'extérieur, les acteurs internes sont tout aussi dangereux.

83 %



83 % des compromissions impliquent des acteurs externes, principalement issus de bandes organisées motivées par l'appât du gain.

19 %

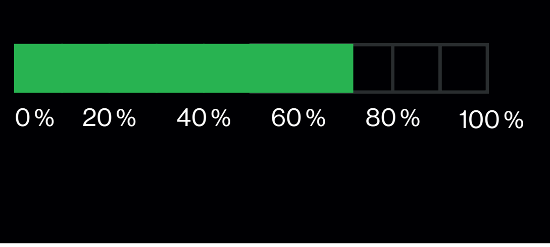


19 % impliquent des acteurs internes qui provoquent des dommages volontaires ou accidentels à la suite d'abus ou de simples erreurs humaines.

L'humain, tendon d'Achille de la sécurité.

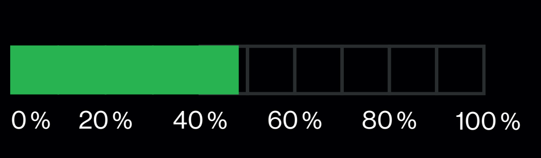
Erreurs, abus de privilèges, utilisation d'identifiants volés, ingénierie sociale… le facteur humain est présent dans 74 % des compromissions.

74 %



Aussi habiles que déterminés, les attaquants arrivent trop souvent à leurs fins.

49 %



Les acteurs externes misent sur différents vecteurs d'attaque : utilisation d'identifiants volés (49 %), phishing (12 %) et exploitation de vulnérabilités (5 %).

Cet exemple démontre à quel point il est important d'anticiper divers scénarios d'attaque.

L'argent, (presque) toujours l'argent.

95 % des compromissions sont motivées par l'appât du gain.

95 %

La protection de votre entreprise passe d'abord par une bonne compréhension des menaces auxquelles elle est confrontée. C'est là toute la clé d'une détection rapide d'une compromission, de sa neutralisation et d'un retour rapide à la normale.

Pour approfondir ces thématiques, lisez le Verizon Data Breach Investigations Report (DBIR) 2023 en intégralité. Pour découvrir comment Verizon peut vous aider à renforcer les défenses de votre infrastructure, contactez votre représentant Verizon local.

Consultez le rapport sur verizon.com/business/fr-fr/resources/reports/dbir/.