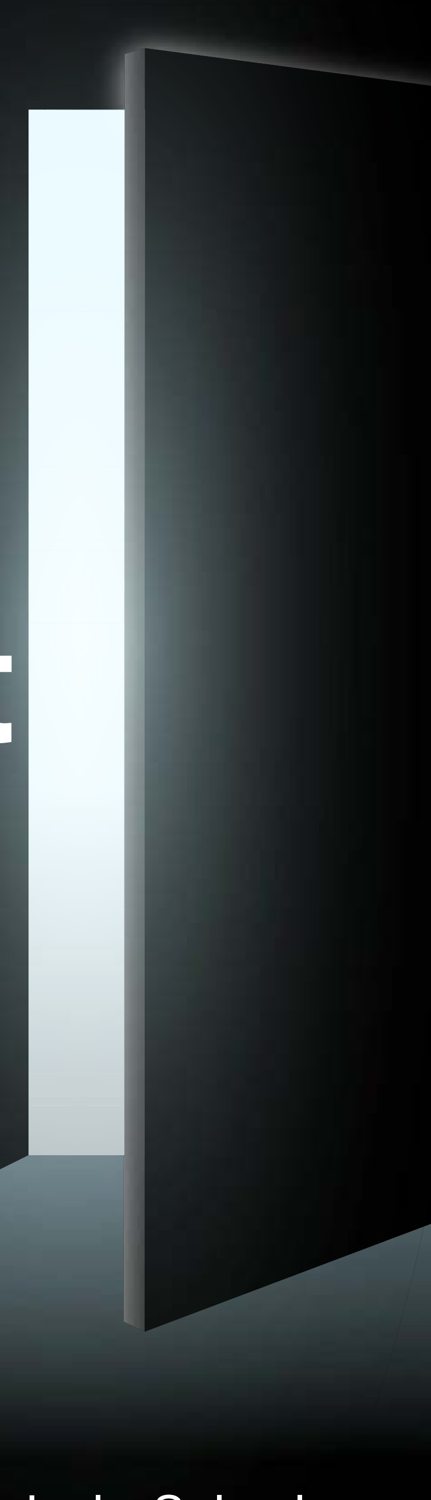
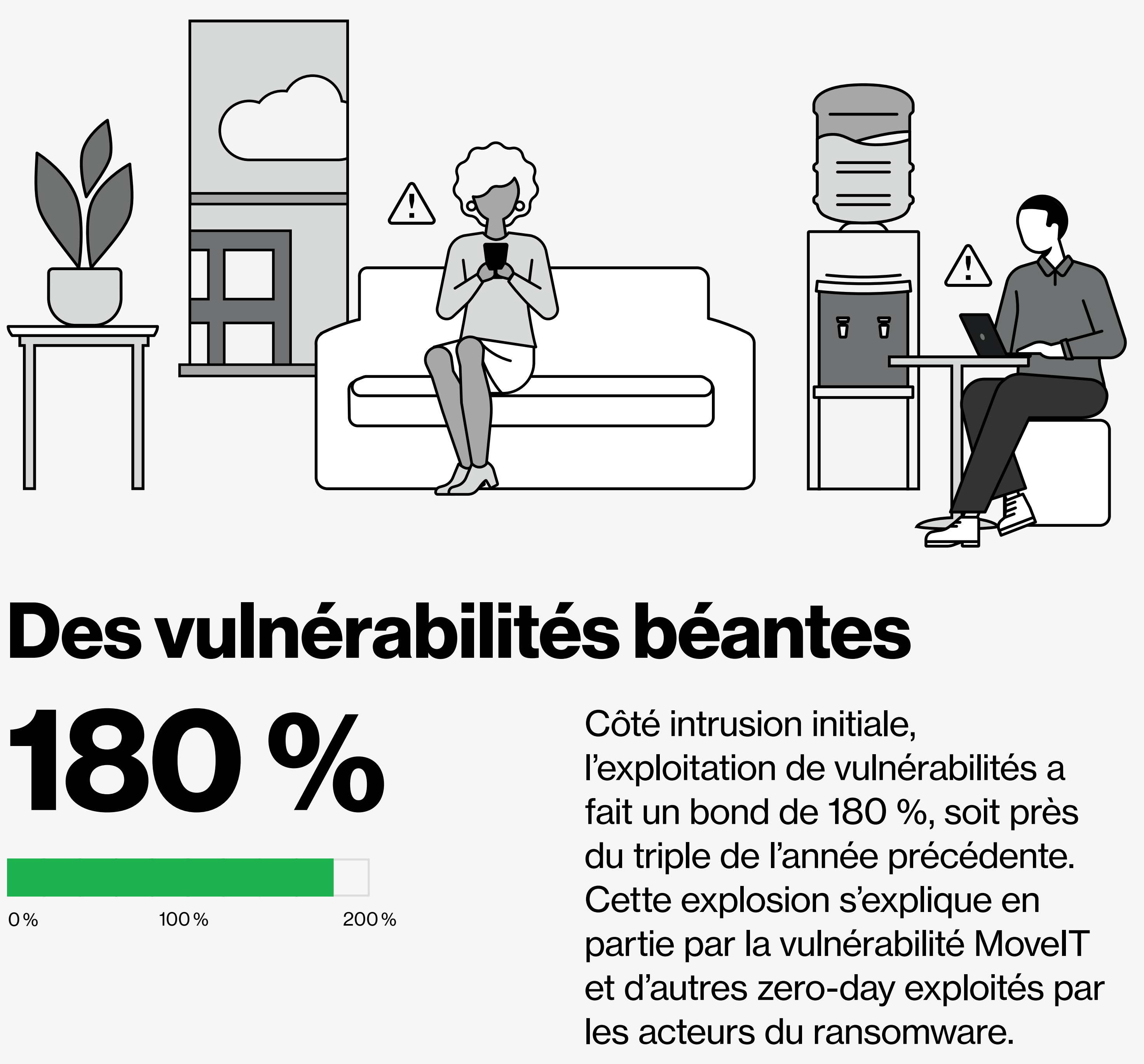
Les chiffres ont parlé. Découvrez comment ils parviennent à entrer.



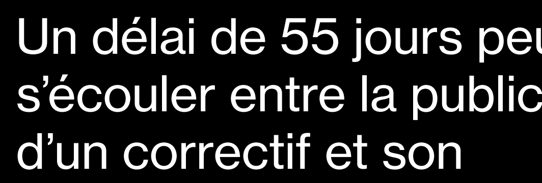
Les points clés du Verizon Data Breach Investigations Report (DBIR) 2024

2023 a été une très belle année pour les cybercriminels. Selon les données du Verizon Data Breach Investigations Report (DBIR) 2024, le nombre de compromissions a atteint un niveau record : plus de 10 000, réparties sur 94 pays. Fruit d'un suivi et d'une analyse minutieuse de ces données, cette nouvelle édition du DBIR dresse un bilan des principaux schémas d'attaque pour vous aider à renforcer vos défenses face à des menaces en perpétuelle évolution. Voici nos principales conclusions.



Des vulnérabilités béantes

180 %



Côté intrusion initiale, l'exploitation de vulnérabilités a fait un bond de 180 %, soit près du triple de l'année précédente. Cette explosion s'explique en partie par la vulnérabilité MoveIT et d'autres zero-day exploités par les acteurs du ransomware.

Une défense trop lente

Un délai de 55 jours peut s'écouler entre la publication d'un correctif et son application sur 50 % des vulnérabilités critiques. Un temps de retard terriblement délétère pour les entreprises.

55 jours

Un manque de formation

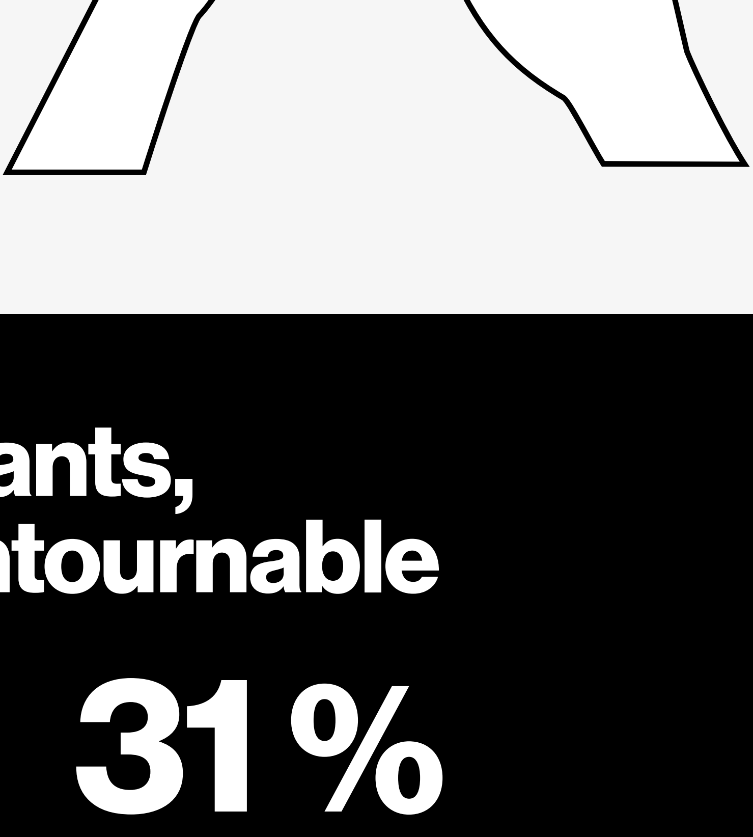
68 %

68 % des compromissions ont une origine humaine involontaire, allant de la simple erreur au collaborateur piégé par l'ingénierie sociale.

Le phishing – Vite fait, bien fait

< 60 sec.

Un utilisateur mord à l'hameçon du phishing en moins de 60 secondes (délai médian).



Le vol d'identifiants, classique incontournable

Au cours des 10 dernières années, 31 % des compromissions se sont appuyées sur le vol d'identifiants.

31 %

L'importance du choix de ses partenaires

15 %

15 % des compromissions ont impliqué un intermédiaire : dépositaire de données, infrastructures d'hébergement, supply chain logicielle (directement ou indirectement), etc.

« Pas mal, vos données. Ce serait tellement dommage qu'il leur arrive quelque chose. »

En 2023, 32 % des compromissions se sont appuyées sur une technique d'extorsion, notamment les ransomwares.

32 %

46 000 $

Dans les cas d'extorsion par ransomware ou autre, la perte financière médiane s'élève à 46 000 $.[11]

Un coût faramineux pour l'entreprise

50 000 $

La perte financière médiane associée aux compromissions de messagerie professionnelle (BEC) s'est chiffrée à environ 50 000 $ en 2022 et 2023.[1]

Les cybermenaces se font toujours plus complexes et dangereuses.

Connaître l'ennemi et ses nouveaux modes opératoires, c'est prendre une sérieuse option pour renforcer la protection de votre entreprise. C'est pourquoi nous vous invitons à lire la version complète du Verizon Data Breach Investigations Report (DBIR) 2024, la référence incontournable sur les compromissions de sécurité.

N'hésitez pas à contacter votre conseiller Verizon pour découvrir comment nos solutions de sécurité peuvent venir renforcer votre organisation pour l'aider à faire face à des cyberattaques en perpétuelle évolution.

Consultez le rapport sur verizon.com/dbir.

verizon business

---

1. Données du FBI (IC3 – Internet Crime Complaint Center)