L'information est votre meilleure arme

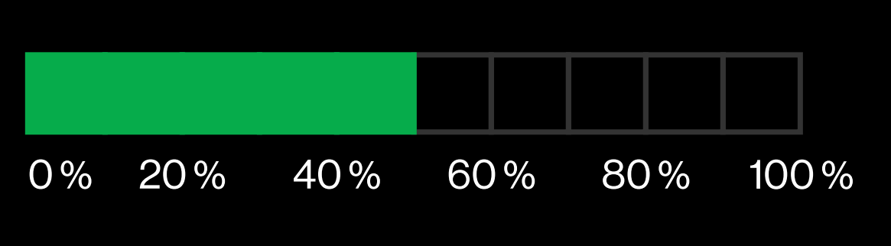
Principales conclusions de l'édition 2022
du Verizon Data Breach Investigations
Report (DBIR)

Cela fait déjà 15 ans que Verizon observe les modes opératoires des cyberattaquants. Ce rapport 2022 est le fruit de...

5 212	**23 896**	**87**
compromissions analysées	incidents de sécurité examinés	organisations participantes

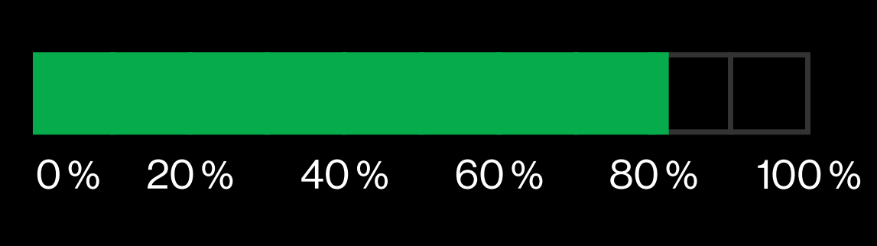
Nos conclusions :

> 50 %



Plus de la moitié des compromissions passent par l'utilisation d'un accès distant ou d'applications web.

82 %

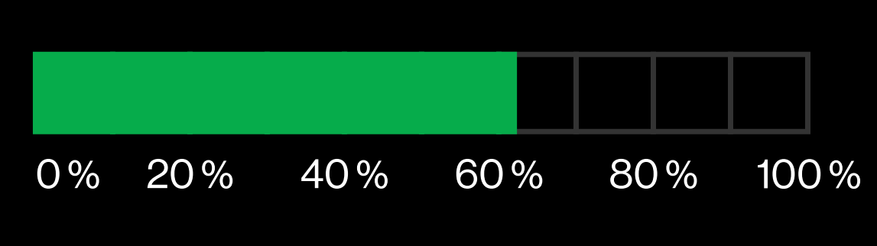


La plupart des compromissions sont imputables à des erreurs humaines.

20 %

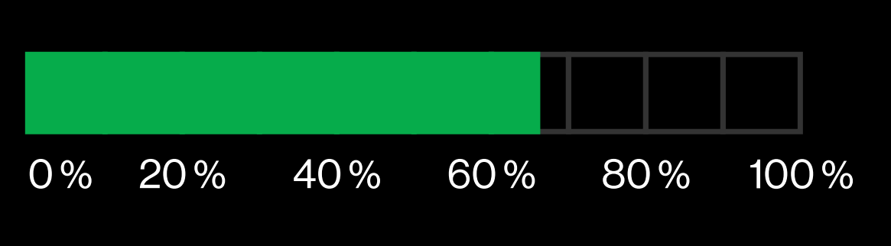
L'ingénierie sociale se retrouve dans 20 % des compromissions.

62 %



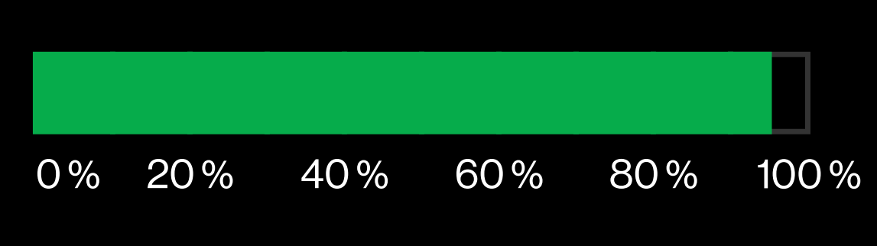
Les partenaires sont à l'origine de 62 % des incidents par intrusion de système, même s'il s'agit de compromissions d'un seul maillon de la supply chain dans la plupart des cas.

66 %



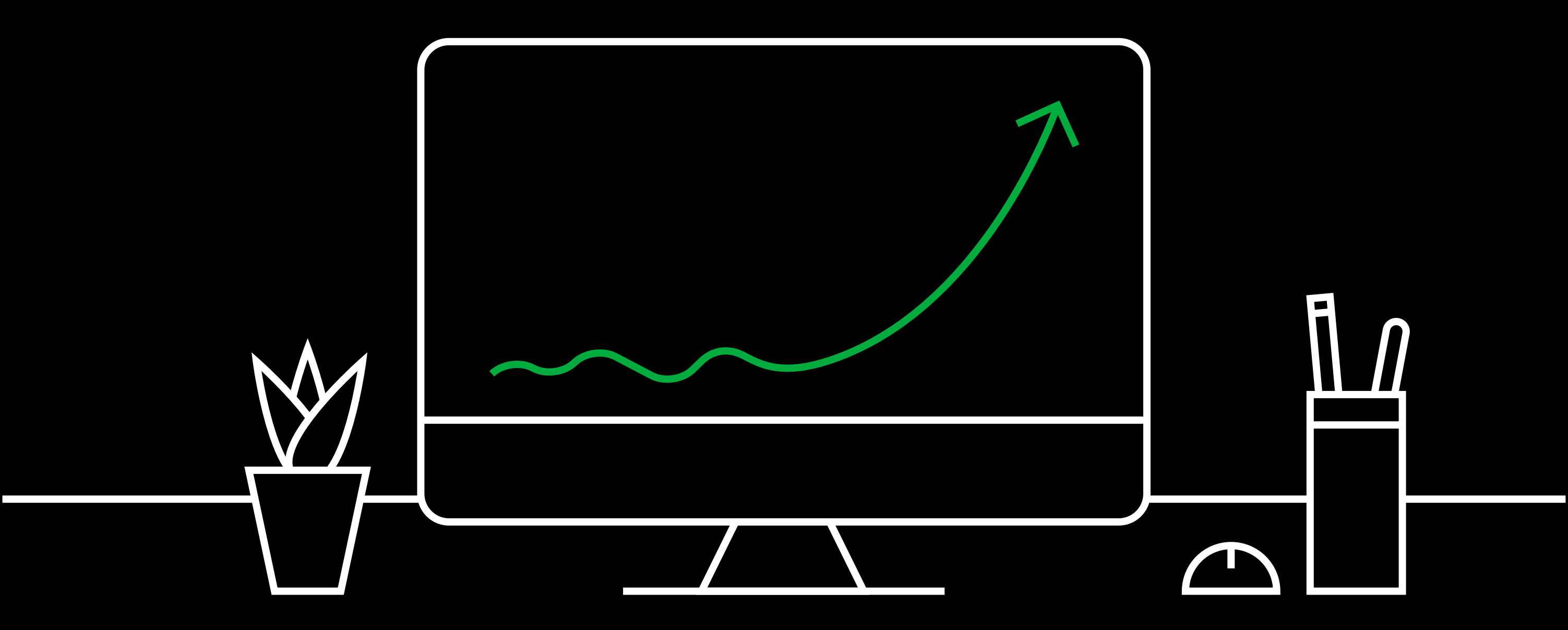
Près des deux tiers des compromissions reposent sur le phishing, des identifiants volés ou des ransomwares.

95 %



95 % des compromissions s'opèrent en cinq étapes ou moins.

Les ransomwares ont progressé de 13 % en un an, soit davantage que pendant les cinq dernières années réunies.



Les quatre grands vecteurs de compromission des données sont :

- Identifiants volés
- Phishing
- Exploitation de vulnérabilités
- Botnets

Chaque entreprise a besoin d'un plan pour s'en prémunir.

Qui sont les coupables ?

4/5	Près de quatre compromissions sur cinq sont imputables au crime organisé.
#1	La principale motivation est financière.
#2	Le deuxième motif est l'espionnage.

**Vous devez impérativement protéger votre entreprise.
Pour cela, le rapport DBIR constitue le point de départ idéal.**

Pour en savoir plus sur les dernières tendances en matière de compromissions de données, y compris par secteur et par région, téléchargez le rapport d'enquête Verizon 2022 sur le sujet.

Lire le rapport complet

verizon✓