ÉTAT DE LA MENACE

RAPPORT D'INCIDENTOLOGIE
InterCERT France
2024

Panorama des phénomènes cybercriminels

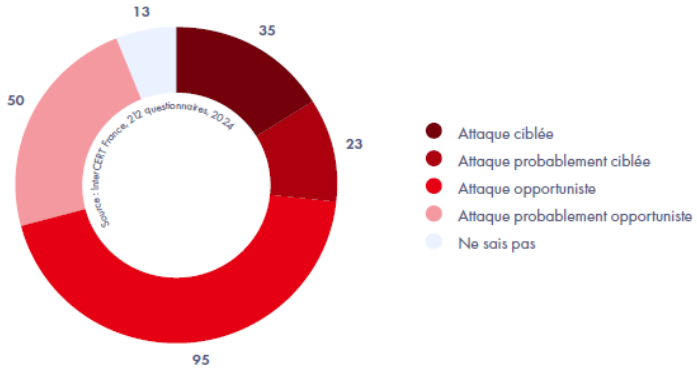
Mardi 26 novembre 2024

InterCERT FRANCE

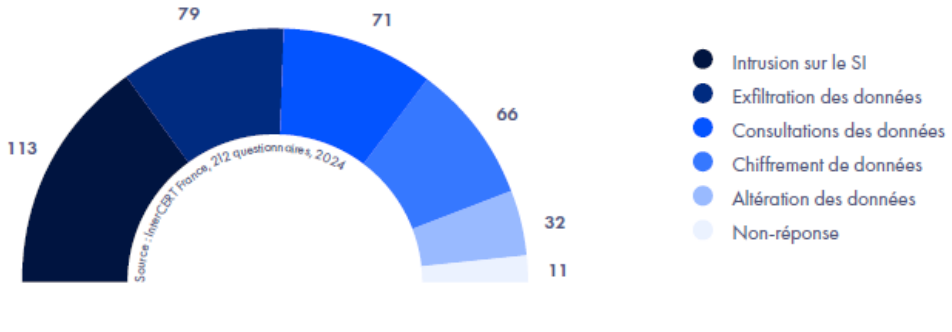
VUE D'ENSEMBLE

20%
des attaques sont revendiquées

Prenons un peu de recul sur les incidents observés par les différents membres de l'InterCERT France.



Près de 3 attaques sur 4 sont menées de manière opportuniste !



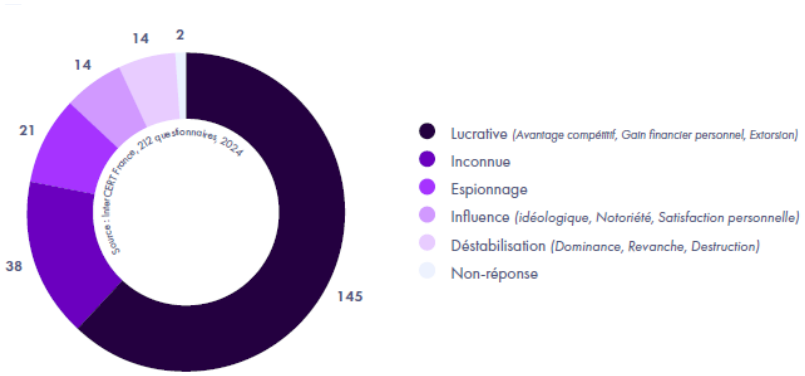
Un chiffrement ne vient que rarement seul, il est souvent accompagné d'une exfiltration de données !

InterCERT FRANCE

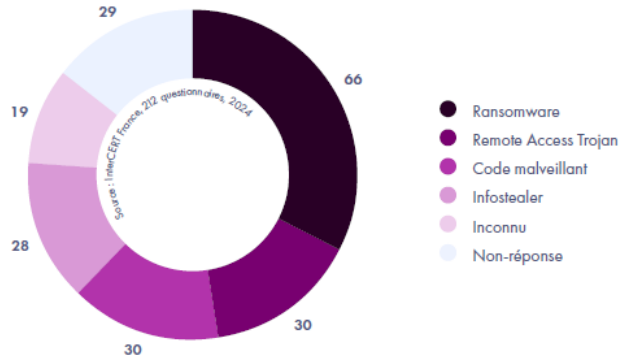
VUE D'ENSEMBLE

73%
de ces infrastructures compromises utilisaient Un système d'exploitation Windows

Sans aucun doute, la majorité des attaques sont conduites à des fins lucratives : l'appât du gain reste la principale motivation des attaquants.



Quels sont les motivations des attaquants ?

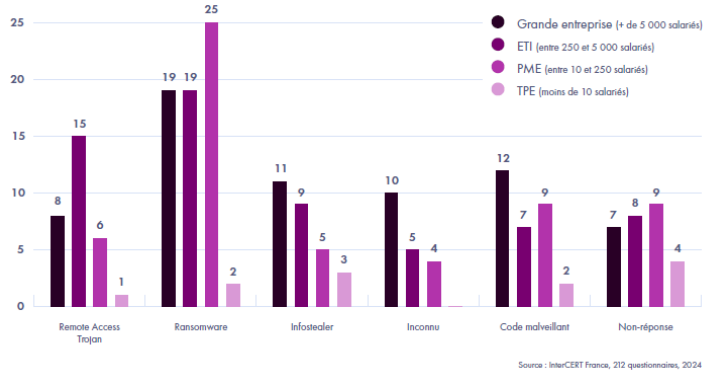


Quels outils ont été le plus observés ?

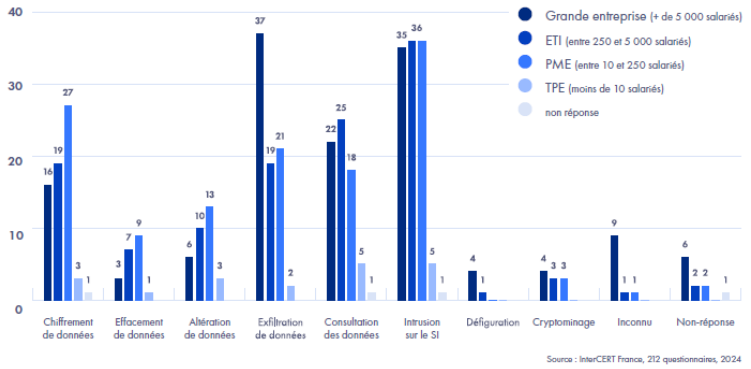
InterCERT FRANCE

GRANDES TENDANCES

Des disparités notables en fonction du type d'organisation victime de la cyberattaque.



Répartition des outils malveillants rencontrés lors des réponses à incidents en fonction de la taille de l'entreprise

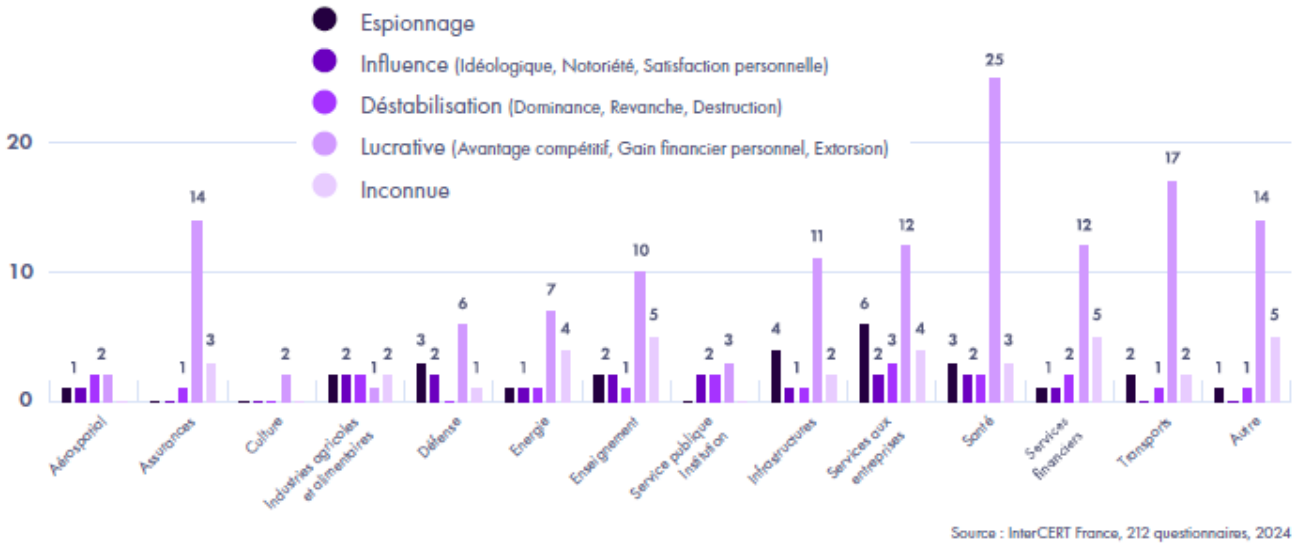


Répartition des types d'attaques rencontrées, selon la taille de l'entreprise

InterCERT FRANCE

MOTIVATIONS

Il apparaît que les secteurs dits critiques, tels que la défense, l'aérospatial, la santé, l'énergie et le secteur public, sont particulièrement vulnérables au cyber-espionnage.

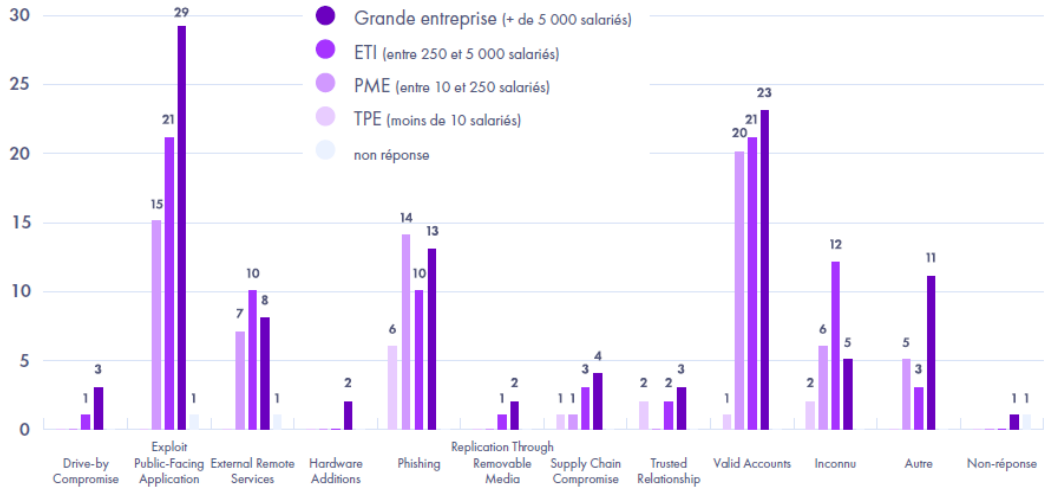


Source : InterCERT France, 212 questionnaires, 2024

InterCERT FRANCE

VECTEURS DE COMPROMISSIONS

Les profils de risques varient selon les types de structure : les besoins cyber des uns ne sont pas forcément ceux des autres !



Dans près d'un cas sur 10, il n'a pas été possible d'identifier d'outil malveillant spécifique, corroborant d'autres études comme le rapport de l'ANSSI soulignant une utilisation de plus en plus forte de LOLbins (Living Off the Land Binaries, des exécutables et des scripts légitimes déjà présents sur un système).

InterCERT FRANCE

Durée des incidents

Des disparités fortes apparaissent néanmoins en fonction du type de structure. En effet, plus la structure est importante et complexe...

1. Plus le temps de détection est long ; contrairement aux plus petites structures, où les impacts sont généralement plus rapidement visibles... malgré l'absence de moyens de détection.

2. Plus le temps de résolution est long, notamment à cause de systèmes d'information plus complexe et d'une distribution plus importante de la connaissance et des compétences que dans les structures plus petites où quelques individus centralisent la capacité de gestion et de relance du SI.

27
le nombre de jour moyen entre l'intrusion et la détection

Structure	Temps de détection en moyenne (en jours)	Temps de résolution en moyenne (en jours)
TPE	10,1	3
PME	21	11,5
ETI	27	19,7
Grandes Entreprises	32,3	28,5

InterCERT FRANCE