DE L'ÂGE DE PIERRE À L'ÂGE DES MACHINES

CYBER CRIMINALITÉ

L'ÂGE DE PIERRE

Les débuts primitifs, années 1960 - 1980)

Les premières formes de cyber-criminalité se manifestent de manière artisanale et expérimentale. Les hackers de cette période, comme les phreakers, explorent les systèmes sans intention nécessairement malveillante. Les premiers virus informatiques comme Creeper (1971) et les activités de phreaking symbolisent cette époque.

L'ÂGE DE BRONZE

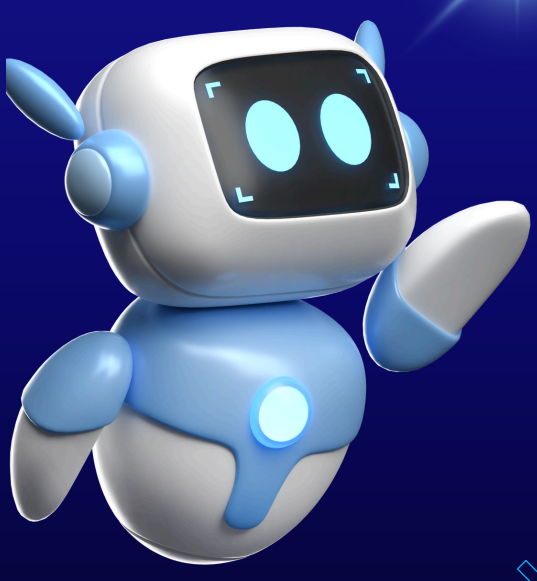
Années 1990 - 2000

Avec l'essor d'Internet, la cybercriminalité se structure. Les virus destructeurs comme ILOVEYOU (2000) et les premières attaques de type phishing apparaissent. La cybercriminalité devient plus organisée, et des plateformes comme le Dark Web se développent pour monétiser ces attaques.

L'ÂGE DE FER

Années 2000 - début 2010s

Cet âge voit l'apparition des cyber-attaques sophistiquées et ciblées, comme Stuxnet (2010), et l'uti-lisation des premières cyberarmes. Les attaques deviennent massi-vement destructrices, et les États commencent à utilise le cyberespace comme un champ de bataille pour la guerre numérique et l'espionnage. Les cybercriminels s'organisent davantage avec des infrastructures criminelles plus élaborées.



L'ANTIQUITÉ

Années 2010s - 2018

L'Antiquité de la cybercriminalité est l'époque où les attaques deviennent une véritable arme géopolitique, et où les cybercriminels organisés, parfois étatiques, lancent des campagnes de cyberespionnage à grande échelle et des attaques contre des infrastructures critiques. Les rançongiciels, sur des grandes entreprises ciblées se multiplient.

ARTIFICIAL INTELLIGENCE IMPACT

L'ÂGE INDUSTRIEL

2018 à Aujourd'hui

Tout juste avant l’automatisation complète des cyber-attaques. C’est une ère de professionnalisation accrue, où la cybercriminalité se transforme en une véritable industrie du crime. Il est possible de louer des logiciels malveillants pour mener des attaques. Cet âge est marqué par des attaques massives, mais toujours orchestrées par des humains avec l’aide de processus semi-automatisés. Les exemples incluent les cyberattaques contre Colonial Pipeline (2021) et SolarWinds (2020)

L'ÂGE DES MACHINES

2025 ?

l’automatisation prend le dessus. Les cyberattaques sont largement autonomisées, et les criminels utilisent des outils d’IA pour lancer des attaques de phishing automatisées, des malwares polymorphes, et des campagnes massives. L'IA est utilisée non seulement pour concevoir des attaques, mais aussi pour optimiser et personnaliser les tactiques d'attaque à grande échelle.

D’un autre côté, les entreprises se professionnalisent pour faire face aux attaques et recrutent des hackers éthiques, éprouvent leurs systèmes et restent en veille permanente.