Catégories de sources de risque (SR)

Tableau issu des pages 20 et 21 du supplément guide EBIOS RM.

Profils d'attaquants	Exemples et modes opératoires habituels
Étatique	États, agences de renseignement. *Attaques généralement conduites par des professionnels, respectant un calendrier et un mode opératoire prédéfinis. Ce profil d'attaquant se caractérise par sa capacité à réaliser une opération offensive sur un temps long (ressources stables, procédures) et à adapter ses outils et méthodes à la topologie de la cible. Par extension, ces acteurs ont les moyens d'acheter ou de découvrir des vulnérabilités jour zéro (0-Day) et certains sont capables d'infiltrer des réseaux isolés et de réaliser des attaques successives pour atteindre une ou des cibles (par exemple au moyen d'une attaque visant la chaîne d'approvisionnement).*
Crime organisé	Organisations cybercriminelles (mafias, gangs, officines). *Arnaque en ligne ou au président, demande de rançon ou attaque par rançongiciel, exploitation de réseaux de « machines robots » (botnet), etc. En raison notamment de la prolifération de kits d'attaques facilement accessibles en ligne, les cybercriminels mènent des opérations de plus en plus sophistiquées et organisées à des fins lucratives ou de fraude. Certains ont les moyens d'acheter ou de découvrir des vulnérabilités jour zéro (0-Day).*
Terroriste	Cyberterroristes, cybermilices. *Attaques habituellement peu sophistiquées mais menées avec détermination à des fins de déstabilisation et de destruction : déni de service (visant par exemple à rendre indisponibles les services d'urgence d'un centre hospitalier, arrêts intempestifs d'un système industriel de production d'énergie), exploitation de vulnérabilités de sites Internet et défigurations.*
Activiste idéologique	Cyber-hacktivistes, groupements d'intérêt, sectes. *Modes opératoires et sophistication des attaques relativement similaires à ceux des cyberterroristes mais motivés par des intentions moins destructrices. Certains acteurs vont mener ces attaques pour véhiculer une idéologie, un message*

	(exemple: utilisation massive des réseaux sociaux comme caisse de résonance).
Officine spécialisée	Profil de « cybermercenaire » doté de capacités informatiques généralement élevées sur le plan technique. Il est de ce fait à distinguer des script-kiddies avec qui il partage toutefois l'esprit de défi et la quête de reconnaissance mais avec un objectif lucratif. De tels groupes peuvent s'organiser en officines spécialisées proposant de véritables services de piratage. *Ce type de hacker chevronné est souvent à l'origine de la conception et de la création d'outils et kits d'attaques 3 accessibles en ligne (éventuellement monnayés) qui sont ensuite utilisables « clés en main » par d'autres groupes d'attaquants. Il n'a pas de motivations particulières autres que le gain financier.*
Amateur	Profil du hacker « script-kiddies » ou doté de bonnes connaissances informatiques, et motivé par une quête de reconnaissance sociale, d'amusement, de défi. *Attaques basiques mais capacité à utiliser les kits d'attaques accessibles en ligne.*
Vengeur	Les motivations de ce profil d'attaquant sont guidées par un esprit de vengeance aiguë ou un sentiment d'injustice (exemples : salarié licencié pour faute grave, prestataire mécontent suite au non-renouvellement d'un marché, etc.). *Ce profil d'attaquant se caractérise par sa détermination et sa connaissance interne des systèmes et processus organisationnels. Cela peut le rendre redoutable et lui conférer un pouvoir de nuisance important.*
Malveillant pathologique	Les motivations de ce profil d'attaquant sont d'ordre pathologique ou opportuniste et parfois guidées par l'appât du gain (exemples : concurrent déloyal, client malhonnête, escroc, fraudeur). *Ici, soit l'attaquant dispose d'un socle de connaissances en informatique qui l'amène à tenter de compromettre le SI de sa cible, soit il exploite par lui-même des kits d'attaques disponibles en ligne, soit il décide de sous-traiter l'attaque informatique en faisant appel à une officine spécialisée. Dans certains cas, l'attaquant peut porter son attention sur une source interne (salarié mécontent, prestataire peu scrupuleux) et tenter de la corrompre.*