|  |  |  |  |
| --- | --- | --- | --- |
| Virus informatiques | Logiciels malveillants | Phishing | Piratage informatique |
| Les virus informatiques sont des programmes malveillants qui peuvent se propager à d'autres ordinateurs et causer des dommages aux fichiers et aux données. Les virus peuvent se propager via des e-mails, des pièces jointes, des sites web malveillants ou des supports de stockage infectés. | les logiciels malveillants, tels que les chevaux de Troie, les vers, les spywares, les rootkits, les ransomwares, etc., sont conçus pour infecter les systèmes informatiques et causer des dommages aux données et aux fichiers. | le phishing est une technique d'ingénierie sociale qui vise à tromper les utilisateurs en les incitant à divulguer des informations personnelles ou confidentielles telles que des mots de passe, des numéros de carte de crédit ou des informations bancaires. | le piratage informatique est une activité malveillante visant à infiltrer un système informatique ou un réseau en utilisant des techniques telles que l'exploitation de failles de sécurité, la force brute ou le vol de mots de passe. |

|  |  |  |  |
| --- | --- | --- | --- |
| Espionnage industriel | Cyberterrorisme | Cyber-espionnage | Réseaux de robots ou botnets |
| l'espionnage industriel est une activité visant à voler des informations confidentielles telles que des plans de produits, des données de recherche et développement ou des secrets commerciaux. | le cyberterrorisme est une forme de terrorisme qui utilise des techniques informatiques pour causer des dommages à des systèmes informatiques, des réseaux ou des infrastructures critiques. | le cyber-espionnage est une activité visant à recueillir des informations confidentielles sur les gouvernements, les entreprises ou les individus à des fins d'espionnage. | Un réseau de robots est un ensemble d’ordinateurs compromis supervisés via un canal de commande et contrôle. La personne qui exploite l’infrastructure de commande et contrôle, à savoir le maître des robots ou botmaster, utilise ces ordinateurs compromis, ou robots, pour lancer des attaques destinées à faire tomber le réseau d’une cible, à injecter des logiciels malveillants, à collecter des identifiants ou à exécuter des tâches gourmandes en puissance de calcul. |