Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Secrétariat général

Centre national pour la cybersécurité NCSC
www.ncsc.admin.ch

NCSC

Types de menaces, auteurs et outils

Table des matières

1 Préambule

Le présent document fournit un aperçu des menaces courantes et de leur classification, ainsi qu'une typologie des auteurs dont celles-ci émanent.

2 Menaces

Internet fait peser toutes sortes de menaces sur les particuliers ainsi que sur les organisations privées ou publiques. Un schéma pyramidal aide à en distinguer les grandes catégories.

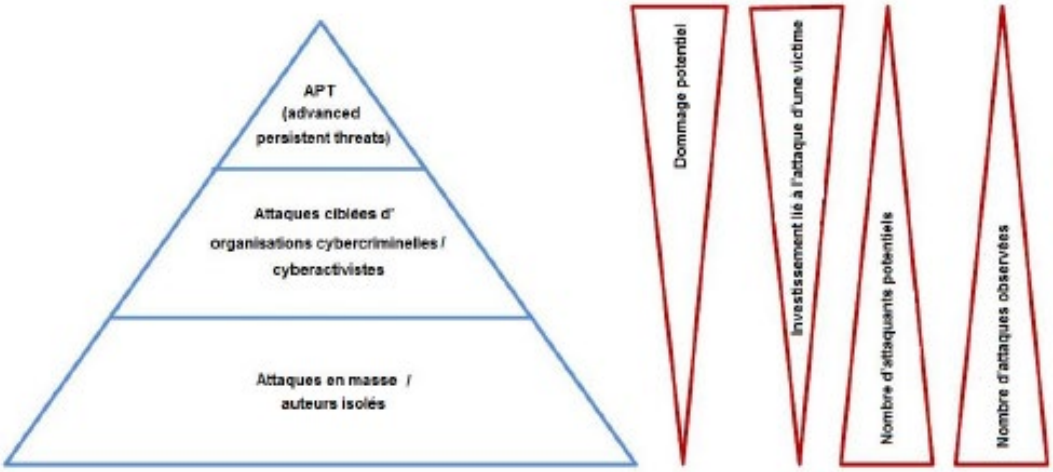

Illustration 1: représentation simplifiée de la pyramide des menaces selon SANS[1], RecordedFuture[2]

La menace dite *advanced persistent threat* (APT) forme le sommet de la pyramide. Elle peut occasionner des dommages très élevés à une organisation spécifique ou, dans un contexte politique, nuire gravement à la sécurité de pays entiers. L'agresseur est prêt à investir énormément de temps, d'argent et de savoir-faire dans son attaque, et il dispose généralement de ressources considérables. Soucieux de passer inaperçu le plus longtemps possible, il vise à s'installer dans le réseau de sa victime pour y dérober en continu les informations qui l'intéressent. Dans de rares cas, il commet des sabotages (ou tente d'en commettre). Compte tenu des ressources et des compétences élevées que ce genre d'attaque requiert, le nombre d'agresseurs classés dans cette catégorie est limité. Il augmente néanmoins de manière constante.

Le milieu de la pyramide est occupé par les cybercriminels et les cyberactivistes. Bien que ceux-ci ne disposent en temps normal que de faibles ressources, il ne faut pas sous-estimer ce type de menace. En règle générale, ces agresseurs ont un éventail de cibles plus réduit et sont aussi moins tenaces que les auteurs d'APT, encore que la frontière entre cybercriminalité organisée et APT soit perméable. Des acteurs étatiques peuvent également utiliser l'offre proposée sur le marché de la cybercriminalité pour atteindre leurs objectifs. Ils confient aussi des missions à des organisations cybercriminelles pour être en mesure de nier toute implication en cas de découverte.

Les attaques opportunistes perpétrées à large échelle ou par des auteurs isolés constituent le socle de la pyramide. En dépit des ressources limitées qui leur sont consacrées, ces menaces doivent être prises au sérieux, ne serait-ce qu'en raison de leur nombre élevé. Là encore, la frontière avec l'étage supérieur de la pyramide est perméable, car les cyberattaques de masse

[1] www.sans.org

[2] https://www.recordedfuture.com/assets/prioritizing-cyber-threats-1.png

sont souvent menées, ou du moins commanditées, par des organisations cybercriminelles. Cette perméabilité témoigne également du fait que l'organisation du marché noir est fondée sur la division du travail selon le modèle classique de l'offre et de la demande.

3 Agresseurs

Les tableaux ci-après classent les agresseurs en fonction de leurs possibilités et de leurs mobiles. Ce classement permet de déterminer les objectifs, les ressources et la ténacité potentielle des auteurs. Il ne prétend pas être exhaustif.

3.1 Advanced persistent threats (APT)

Nom	Acteurs étatiques / APT
Description	Des États ou des acteurs entretenant pour la plupart des liens avec des États exécutent eux-mêmes ou commanditent l'attaque. En règle générale, ils visent à obtenir des informations dans un contexte d'espionnage classique ou industriel. Lors de tensions politiques accrues ou de crises, les attaques peuvent porter sur des infrastructures critiques ou consister en des opérations de désinformation ciblées.
Mobiles	Obtention d'informations, perturbation d'infrastructures critiques, opérations d'influence
Ressources techniques	Les États ou les acteurs entretenant des liens avec des États disposent en principe de toutes les compétences techniques nécessaires. Il faut donc considérer qu'ils ont des ressources considérables. En parallèle, ils peuvent avoir recours à des spécialistes de diverses disciplines ou en recruter rapidement.
Ressources financières	Très importantes, tant que l'agresseur considère que le résultat attendu justifie les ressources financières engagées.
Rationalité	Élevée
Ténacité	Élevée
Méthodes de défense	• Investissements (y c. en personnel) dans la détection • Accroissement de la visibilité sur les terminaux • Segmentation et surveillance des réseaux et de tous les systèmes • Protection des services d'annuaire (Active Directories) • Recours à des outils comme AppLocker, n'exécuter que des macros signées numériquement • Installation de passerelles de sécurité (*security gateways*) centralisées par lesquelles tout le trafic doit transiter • Blocage de formats de fichiers dangereux sur les passerelles • Séparation des tâches sensibles et de la navigation sur Internet / de la correspondance électronique • Généralisation de l'authentification à deux facteurs • Gestion des patchs en temps utile et sous surveillance

	• Programme efficace de sauvegarde et de récupération des données avec sauvegardes hors ligne et hors site sur plusieurs générations
Leviers pour des poursuites pénales	Procéder à une analyse détaillée des attaques afin d'identifier les auteurs. Des enquêtes coordonnées à l'échelle internationale sont nécessaires. Elles peuvent être mues par des intérêts politiques.
Résistance aux poursuites pénales	Très élevée
Cibles probables	• Systèmes contenant des informations sensibles • Informations stratégiques • Systèmes de personnes clés ou de décideurs • Systèmes peu exposés (installation de portes dérobées, difficiles à découvrir) • Confidentialité et intégrité des systèmes • Disponibilité des systèmes critiques en cas de tensions politiques accrues ou de crises • Infrastructures critiques

3.2 Organisations cybercriminelles (attaques ciblées)

Nom	Organisations cybercriminelles (attaques ciblées)
Description	Des organisations cybercriminelles peuvent lancer des attaques ciblées comparables à une APT. Elles s'en prennent à des organisations étatiques ou privées afin d'accéder à des informations qu'elles vont revendre ou utiliser à leur avantage. Les systèmes de transactions financières ou les systèmes de gestion des distributeurs de billets de banque (ATM cash-out) sont très souvent pris pour cible. Les attaques incluant le déploiement de rançongiciels s'avèrent très lucratives pour leurs auteurs, raison pour laquelle elles se multiplient ces derniers temps. Les agresseurs copient les données avant de les chiffrer, puis menacent de les revendre si la rançon n'est pas payée.
Mobiles	Chantage, obtention et revente d'informations (espionnage industriel), utilisation de systèmes de transactions financières à des fins propres
Ressources techniques	Moyennes à élevées selon l'organisation
Ressources financières	Moyennes à élevées selon l'organisation
Rationalité	Élevée
Ténacité	Moyenne
Méthodes de défense	• Investissements (y c. en personnel) dans la détection • Accroissement de la visibilité sur les terminaux • Segmentation et surveillance des réseaux et de tous les systèmes • Protection des services d'annuaire (Active Directories) • Recours à des outils comme AppLocker, n'exécuter que des macros signées numériquement • Installation de passerelles de sécurité (*security gateways*) centralisées par lesquelles tout le trafic doit transiter • Blocage de formats de fichiers dangereux sur les passerelles

	• Séparation des tâches sensibles et de la navigation sur Internet / de la correspondance électronique • Généralisation de l'authentification à deux facteurs • Gestion des patchs en temps utile et sous surveillance • Programme efficace de sauvegarde et de récupération des données avec sauvegardes hors ligne et hors site sur plusieurs générations
Leviers pour des poursuites pénales	Analyse des outils et de l'infrastructure utilisés pour l'attaque, étroite collaboration avec les services de police et de renseignement compétents. Surveillance des organisations cybercriminelles en activité.
Résistance aux poursuites pénales	Moyenne à élevée. Les poursuites pénales dérangent toutefois les activités des agresseurs, qui cherchent à ne pas se faire repérer par les autorités.
Cibles probables	• Systèmes présentant des exigences élevées en matière de disponibilité • Systèmes contenant des informations confidentielles à haute valeur de revente • Systèmes contenant des informations financières

3.3 Organisations cybercriminelles (attaques opportunistes)

Nom	Organisations cybercriminelles (attaques opportunistes et non ciblées)
Description	Il s'agit de la forme classique de la cybercriminalité. Les agresseurs cherchent à tirer un profit financier de leurs attaques contre les appareils des utilisateurs finaux. Ils tentent notamment de se procurer des données d'accès, de faire chanter leurs victimes au moyen d'une attaque par déni de service (DDoS) ou d'envoyer des courriels indésirables par l'intermédiaire de systèmes infectés. Pour ce faire, ils recourent souvent à des prestations de type «Crimeware as a Service» négociées sur le marché noir.
Mobiles	Appât du gain
Ressources techniques	Moyennes. Des composants sont souvent achetés comme «Crimeware as a Service».
Ressources financières	Moyennes à élevées
Rationalité	Élevée
Ténacité	Faible face à une cible spécifique
Méthodes de défense	• Investissements (y c. en personnel) dans la sécurité • Installation de passerelles de sécurité (*security gateways*), blocage de formats de fichiers dangereux sur les passerelles • Séparation des tâches sensibles et de la navigation sur Internet / de la correspondance électronique • Authentification à deux facteurs pour toutes les ressources accessibles sur Internet • Gestion des patchs en temps utile et sous surveillance

	• Programme efficace de sauvegarde et de récupération des données avec sauvegardes hors ligne et hors site sur plusieurs générations
Leviers pour des poursuites pénales	Redirection des noms de domaine malveillants vers des serveurs que les organisations cybercriminelles ne maîtrisent pas (*sinkholing*). Étude des outils et de l'infrastructure utilisés pour l'attaque. Analyse et blocage des flux financiers correspondants.
Résistance aux poursuites pénales	Moyenne à élevée. Le caractère international de la plupart des incidents compromet l'efficacité des enquêtes.
Cibles probables	• Appareils d'utilisateurs finaux mal protégés • Applications de paiement bancaire

3.4 Hacktivistes

Nom	Hacktivistes, cyberactivistes
Description	Les cyberactivistes protestent à l'aide de moyens électroniques contre les décisions de gouvernements ou d'entreprises qui ne correspondent pas à leurs intérêts politiques ou sociétaux. Les groupes hacktivistes les plus connus sont «Anonymous» ou «LulzSec».
Mobiles	Diffusion de messages, lancement de débats, captation de l'attention et/ou dommages
Ressources techniques	Les ressources et compétences techniques sont très variables. Elles peuvent toutefois prendre des proportions considérables lors de grandes opérations spectaculaires.
Ressources financières	Limitées. La question des ressources financières ne revêt toutefois pas une grande importance pour l'agresseur, qui agit généralement sur une base volontaire.
Rationalité	Moyenne à élevée, en fonction de l'organisation du groupe
Endurance	Moyenne
Méthodes de défense	• Investissements (y c. en personnel) dans la sécurité • Installation de passerelles de sécurité (*security gateways*), blocage de formats de fichiers dangereux sur les passerelles • Séparation des tâches sensibles et de la navigation sur Internet / de la correspondance électronique • Authentification à deux facteurs pour toutes les ressources accessibles sur Internet • Gestion des patchs en temps utile et sous surveillance • Programme efficace de sauvegarde et de récupération des données avec sauvegardes hors ligne et hors site sur plusieurs générations
Leviers pour des poursuites pénales	Collaboration avec les services de police et de renseignement
Résistance aux poursuites pénales	Moyenne
Cibles probables	• Systèmes très exposés / retenant l'attention • Disponibilité des systèmes (DDoS), intégrité (dégradation de sites Internet)

3.5 Individus isolés

Nom	Individus isolés
Description	Un individu isolé agit de son propre chef, avec des moyens limités.
Mobiles	Selon l'agresseur
Ressources techniques	Faibles
Ressources financières	Faibles
Rationalité	Selon l'agresseur
Endurance	Faible à élevée, selon l'agresseur
Méthodes de défense	• Investissements (y c. en personnel) dans la sécurité • Installation de passerelles de sécurité (*security gateways*), blocage de formats de fichiers dangereux sur les passerelles • Séparation des tâches sensibles et de la navigation sur Internet / de la correspondance électronique • Authentification à deux facteurs pour toutes les ressources accessibles sur Internet • Gestion des patchs en temps utile et sous surveillance • Programme efficace de sauvegarde et de récupération des données avec sauvegardes hors ligne et hors site sur plusieurs générations
Leviers pour des poursuites pénales	Méthodes classiques, poursuites pénales
Résistance aux poursuites pénales	Faible
Cibles probables	• Systèmes faiblement protégés (cibles des attaques de néophytes [*script kiddies*]) • Cibles bien exposées, attirant un maximum d'attention (en cas d'actes de vengeance ou de dégradations)

4 Outils

Outre un grand nombre d'outils servant également à la poursuite de buts légaux (scanners de ports, outils de test d'intrusion, etc.), les agresseurs recourent à divers outils destinés spécialement à une utilisation malveillante. Tous ces outils ont en commun d'être employés à tous les niveaux de la pyramide (voir chapitre «Menaces»).

La banque de données «ATT&CK» de MITRE (https://attack.mitre.org/) fournit un aperçu des tactiques, techniques et procédures déployées lors de cyberattaques.

La mise en œuvre de ces tactiques, techniques et procédures repose sur des logiciels malveillants. MITRE dresse une longue liste des logiciels de ce type (https://attack.mitre.org/software/).