# Connaissances et anticipation sur les groupes APT

*Par le Chef d'escadron Maxime SERRES, stagiaires EMSST 2024-2025,*

*Mastère spécialisé cybersécurité attaque et défense des systèmes informatiques,*
*École nationale supérieure des Mines de Nancy*

Derrière chaque organisation se trouvent des Hommes ; les groupes APT (*Advanced Persistent Threats*) n'échappent pas à cette règle. D'un point de vue sécuritaire, il est donc légitime, afin de s'en protéger, de mieux connaître ces organisations malveillantes

## ➢ Concepts entourant les APT

Dans le paysage des cybermenaces, les groupes APT (que nous appellerons plus facilement les APT) agissent principalement dans le champ de conflictualité qu'est le cyberespace. La connaissance de leurs procédés d'exécution relève du renseignement sur la menace cyber plus fréquemment appelée CTI pour *Cyber Threat Intelligence*.

Aucun consensus ne se dégage clairement quant à la définition de la menace APT. La menace est-elle prégnante car elle est sophistiquée ou bien parce qu'elle est de nature pénétrante vis-à-vis des systèmes informatiques ? En l'appliquant à un groupe d'individus, nous retiendrons la définition que donne l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) d'une cyberattaque.

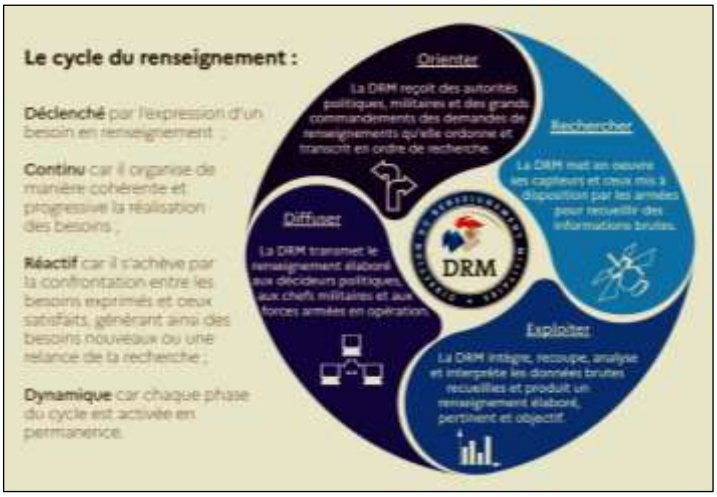
Définition : une cyberattaque est un ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité. Une cyberattaque peut être ponctuelle ou s'inscrire dans la durée.

Nous nuancerons cette définition en y apportant les caractéristiques d'une opération qui s'inscrit dans le temps long et qui a trait au cyber-espionnage, au sabotage ou à des activités de subversion voire d'ingérence.

À l'heure du *Big data*, la cible principale de ces groupes demeure l'information. Les APT représentent une menace qui ne se cantonne pas à cibler le monde occidental. Militaires ou civils, à vocation idéologique ou à but lucratif, éventuellement soutenus par des gouvernements à travers le monde, ces groupes sont de toutes origines. La MITRE Corporation en recense 152 au moment de la rédaction de ces lignes.

## ➢ L'organisation des APT

La structure des groupes APT demeure en grande partie opaque. La collecte de renseignements sur leur organisation peut être réalisée avec l'emploi controversé de méthodes dîtes de sécurité offensive : attaquer les attaquants soulève des problèmes éthiques et légaux.




Parmi les APT, outre l'aspect technicien des hackers et autres développeurs de malware, voire d'administrateurs systèmes, deux types de profils plus spécialisés existent : l'analyste *threat intelligence* et l'analyste *competitive intelligence* :

- le premier agit dans le montage de l'infrastructure attaquante notamment via l'enregistrement de noms de domaines DNS dynamiques à la typologie variée et dépendants de la cible.

- le second est, quant à lui, davantage lié au commanditaire de l'opération. Il s'agit d'un spécialiste de la filière d'appartenance de l'entreprise ciblée qui aurait un œil critique sur les informations dénichées par les hackers du groupe et serait apte à juger de la pertinence d'exfiltrer ou pas les données auxquelles ils ont accès. Cet expert – éventuellement intérimaire du groupe APT – apporte vraisemblablement sa valeur à la masse d'informations traitée. En se référant au cycle du renseignement militaire, il pourrait être responsable des phases d'orientation et d'exploitation.

Un critère de caractérisation de ces groupes de hackers est souvent leur nationalité. Russie, Chine, Corée du Nord et Iran mettent sur pied ces capacités d'attaques dans le cyberespace. Cependant, ces pays ne sont pas exempts des menaces ciblant leurs propres réseaux parce que , par exemple, 10 millions de cyberattaques quotidiennes auraient ciblé la Russie en 2020.

Côté occidental, les 5-EYES ne sont pas en reste avec notamment les agences de renseignement américaines. La CIA disposerait de 5.000 agents dédiés aux activités de cyber-espionnage tandis que la NSA *« tire parti de ses avantages en matière de technologie et de cybersécurité, conformément aux pouvoirs qui lui sont conférés, pour renforcer la défense nationale et sécuriser les systèmes de sécurité nationale. »* Ainsi, les actions de l'APT dénommé *Equation Group* ont été attribuées aux États-Unis (NSA) par la société Kaspersky en 2015 au même titre que la menace APT1 l'a été à la Chine par la société Mandiant en 2013.

La délicate question de l'attribution – ou le fait de désigner un groupe ou un État responsable derrière une cyberattaque de type APT – requiert d'être appuyé par des preuves irréfutables. Dans ce cadre, le *threat hunter* joue un rôle primordial en disposant d'une base de CTI la plus exhaustive possible.


Exemple : le groupe connu sous le code APT1 et sous l'alias Comment Crew aurait conduit l'opération Aurora entre 2009 et 2010 visant des entreprises du secteur financier, des médias et plusieurs autres firmes technologiques. Derrière cette structure, l'Armée Populaire de Libération (Chine) dissimulerait une unité cyber de premier plan. Cette unité militaire parmi les plus connues intégrerait l'ensemble du spectre des capacités d'un APT.

Qualifié de tentaculaire, le groupe APT1 a ainsi fait l'objet d'une attribution directe de la firme internationale de cybersécurité Mandiant dès février 2013. Les APT disposent de ressources financières et humaines parfois considérables estimées à l'aune de la persistance et de la patience qu'ils savent mettre en œuvre pour atteindre leurs objectifs.

Une analogie peut être faite avec un procédé entrepreneurial de sécurité offensive appelé le *red teaming*.

Définition : le red teaming est la pratique qui consiste à tester la sécurité de systèmes d'une organisation en essayant de les pirater. Une *Red Team* (« équipe rouge ») peut être un groupe externe de pentesters (testeurs d'intrusion) ou une équipe propre à l'organisation. Dans les deux cas, le rôle est le même : émuler un acteur réellement malveillant et tenter de pénétrer dans les systèmes.

Par essence, le *red teaming* se veut réaliste pour préparer une organisation à faire face aux menaces cyber. La mise en œuvre d'une *Red Team* sert à mettre en lumière des vulnérabilités mais sert aussi au maintien et à l'acquisition de compétences pour les équipes de défenseurs (équipe bleue ou *Blue Team*). Les scenarii d'attaques et les outils employés se calquent sur des opérations réellement conduites par les APT. Les *Red Teams* ciblent les infrastructures essentielles et de haute-valeur pour l'entreprise puis sont capables de proposer une remédiation aux problèmes de cybersécurité rencontrés.

Au sens large, une autre catégorie de *Red Team* composée de spécialistes hors domaine cybersécurité peut être sollicitée pour réaliser un travail de prospective vis-à-vis de la menace.
Exemple : l'initiative *Red Team* décidée à l'été 2019 par l'Agence de l'innovation de Défense (AID) avec l'État-major des armées (EMA), la Direction générale de l'armement (DGA) et la Direction générale des relations internationales et de la stratégie (DGRIS) dans le cadre du Document d'orientation de l'innovation de Défense.

Les groupes APT sont souvent organisés de manière hiérarchique et spécialisée, similaire à ce qui se fait en entreprise classique mais en se focalisant sur les opérations clandestines. Dans certains cas, un groupe APT peut reproduire la structure numérique d'une cible pour s'entraîner à l'attaquer avant de procéder réellement à l'intrusion. Les opérations stratégiques conduites par les APT nécessitent une indéniable part de créativité et de manœuvrabilité.

- **Le renseignement en cybersécurité**

Pour déjouer les vols de données et se prémunir contre l'intrusion des APT dans les systèmes informatiques, le premier rempart demeure la formation et la sensibilisation du personnel. Considérant que de nombreux groupes APT sont gouvernementaux ou sponsorisés par des gouvernements, les enjeux militaires et d'influences géostratégiques trouvent un écho dans le cyberespace.

En opération comme dans le monde de l'entreprise, le contexte est à prendre en compte. L'environnement tactique, opératif et stratégique, influe directement sur le déroulement et la collecte d'informations de toutes origines (ROHUM, ROEM et ROIM[1]). Il en est de même pour le Renseignement d'Origine Cyber (ROC) qui – dans le cadre de la lutte contre les APT – fait sens sous la forme du recueil d'indices de compromission (plus généralement énoncé en anglais en tant qu'IOC ou *Indicators of Compromise*).

Définition : un IoC (indicateur de compromission) en sécurité informatique est une donnée technique qualifiée qui permet de détecter des activités malveillantes sur un système d'information. Ces indicateurs peuvent s'appuyer sur des données de types variés comme, par exemple, un hash de fichiers, une signature, une adresse IP, une

[1] Renseignement d'Origine HUMaine, Électromagnétique, IMagerie

URL[2], un nom de domaine… mais dans tous les cas, la donnée technique seule ne suffit pas pour parler d'IoC.

Selon cette définition, la donnée brute n'est pas suffisante. Elle doit être raffinée et contextualisée pour devenir un renseignement, une empreinte numérique qui peut laisser présumer de la survenue d'un opérateur APT dans un système.

Sur le terrain, cela se traduit par la mise en place planifiée et coordonnée de moyens de détection sur les systèmes déployés en opérations mais également par la création d'un circuit de traitement des supports physiques. En effet, une stratification de l'analyse est requise ; de la primo-analyse sur le théâtre d'opération à l'analyse exhaustive réalisée par exemple au CRAC (Centre de Recherche Avancée Cyber) appartenant à la DRM (Direction du Renseignent Militaire), un cheminement clair et une traçabilité sans faille sont nécessaires.

Élever des remparts adaptés pour protéger les systèmes nécessite une analyse poussée de la menace. Exploiter les renseignements cyber collectés, c'est le domaine de la *Cyber Threat Intelligence* (CTI) qui utilise diverses plateformes pour mettre en forme et présenter la masse de données. La CTI suit une méthodologie similaire au cycle du renseignement.

Après exploitation, la mise à jour des TTPs (Techniques Tactiques et Procédures) des groupes APT découle de recoupements d'informations qui permettent de rendre opérationnel le renseignement cyber. La CTI peut elle-même être subdivisées en différents sous-domaines :

- ***tactical threat intelligence****,* qui comprend notamment la collecte des IOCs ;
- ***operational threat intelligence****,* afin de discerner l'objectif régionalisé d'une cyberattaque ou d'un opérateur APT ;
- ***strategic threat intelligence****,* pour obtenir une vision globale la menace.

Les différentes strates opérationnelles se retrouvent dans les procédés de collecte du renseignement et d'analyse des cybermenaces.Le renseignement conduit à l'action ; il en est de même en cybersécurité. Dans la lutte contre les menaces quiciblent les systèmes numériques, la connaissance est un maillon essentiel de la sécurité globale cyber-physique.


OpenCTI est une plateforme initialement développée par l'ANSSI pour contextualiser les menaces cyber

[2] Hash : fonction de conversion ; IP n° d'identification de chaque ordinateur connecté à Internet ;URL (Uniform Resource Locator) chaîne de caractères pour identifier une ressource sur Internet.