ARCSI
Association des Réservistes du Chiffre et de la Sécurité de l'Information

Université Paris Cité

Compte-rendu du « Lundi de la cybersécurité »
Lundi 19 Mai 2025

APT (Advanced Persistent Threats)
Les menaces persistantes avancées

Organisé par Pr. Ahmed Mehaoua, Béatrice Laurent et Gérard Peliks

Rédigé par Clarisse Veron, étudiante en Master 2 Cybersécurité et E-santé

SOMMAIRE

Introduction *3*

I. Les APT : une menace invisible mais redoutablement efficace *4*

Une menace d'un nouveau genre **4**

Des attaques à visée géopolitique ou économique **4**

Une attaque mise en scène en direct **4**

Une menace qui échappe aux outils classiques **5**

II. Le déroulé d'une attaque APT : étapes clés *6*

Reconnaissance et ingénierie sociale **6**

Intrusion initiale (attaque) **6**

Établissement d'un canal de communication **6**

Élévation de privilèges **7**

Expansion latérale **7**

Exfiltration des données **7**

Effacement des traces **7**

III. Contre-mesures : sensibiliser et surveiller *9*

Sensibiliser tous les collaborateurs, sans exception **9**

Maîtriser les privilèges : le principe du moindre accès **9**

Surveiller activement les signaux faibles **10**

Réagir vite et signaler **10**

IV. Géopolitique des APT : acteurs étatiques et groupes connus *11*

Des cyberattaques devenues instruments de puissance **11**

APT28 (Fancy Bear) : une menace bien identifiée **11**

Une cartographie mondiale des groupes APT **12**

Et la France ? **12**

V. Claire Alberio : être réserviste en gendarmerie *13*

Deux types de réserve, une même ambition **13**

Un engagement au croisement de l'expertise civile et des besoins institutionnels **13**

Un appel à contribution **13**

VI. Questions / Réponses *14*

Introduction

Le Lundi de la cybersécurité du 18 mai 2025 a permis d'aborder deux thématiques complémentaires autour de la résilience et de la sensibilisation face aux menaces persistantes et aux enjeux de défense numérique. Deux intervenants ont rythmé la soirée :

- **Gérard Peliks**, expert en cybersécurité, qui a proposé une plongée pédagogique et illustrée dans l'univers des **APT (Advanced Persistent Threats)**, ou menaces persistantes avancées. À travers une mise en scène réaliste d'une attaque ciblée, il a exposé les différentes phases d'une compromission de grande ampleur.
- **Claire Alberio**, réserviste citoyenne en gendarmerie et fidèle intervenante du cycle, a ensuite présenté le rôle des réserves citoyennes et opérationnelles dans le soutien à la cybersécurité nationale.

Comme à l'accoutumée, la séance s'est conclue par un échange nourri entre les participants, illustrant l'intérêt croissant pour les mécanismes d'attaque et de défense numérique dans un contexte international tendu.

I. Les APT : une menace invisible mais redoutablement efficace

Dans son intervention très vivante et souvent théâtralisée, Gérard Peliks a souhaité rendre accessible la compréhension des **APT (Advanced Persistent Threats)**, en français « menaces persistantes avancées ». Selon lui, il s'agit aujourd'hui du type d'attaque le plus redouté dans le monde cyber, tant par sa **discrétion**, sa **durée**, que par les **objectifs stratégiques** qu'elle vise.

Une menace d'un nouveau genre

Contrairement aux cyberattaques classiques (type rançongiciel diffusé massivement), les APT sont **des attaques ciblées**, **sophistiquées** et **durables**. Elles ne visent pas l'effet immédiat, mais l'infiltration silencieuse d'un système d'information pour **en extraire les données les plus sensibles**, parfois durant des mois, voire des années, sans jamais être détectées. Gérard insiste :

« Vous ne voyez pas l'attaque arriver, vous ne la voyez pas se dérouler, vous ne la verrez jamais repartir. Mais entre-temps, elle vous a volé tout ce qui comptait. »

Il rappelle qu'il existe une légende urbaine souvent entendue :

- Lorsqu'une petite entreprise est attaquée, c'est à cause d'un manque de maturité en cybersécurité.
- Lorsqu'une grande entreprise est attaquée… c'est qu'elle a été la cible d'une APT.

Une manière de souligner à quel point ces attaques sont **professionnelles, structurées, et souvent pilotées par des États ou des mafias organisées**, avec des moyens financiers et techniques considérables.

Des attaques à visée géopolitique ou économique

Gérard Peliks cite plusieurs exemples de groupes APT connus, notamment :

- **APT28 (Fancy Bear)**, lié au renseignement militaire russe (GRU),
- **APT41** (Chine), impliqué dans le vol de code source stratégique,
- **APT38** (Corée du Nord), dont les actions financent les programmes militaires via le cyber-braquage bancaire.

Ces groupes visent des entités stratégiques : ministères, industriels de la défense, universités, hôpitaux ou ONG, notamment en France. En 2024, les attaques de type APT ont connu une **hausse de 58 %** selon certains indicateurs.

« Ce n'est pas du phishing en masse, c'est de la pêche à l'hameçon. On ne cherche pas n'importe qui, on cible uniquement ceux qui détiennent une information convoitée. »

Une attaque mise en scène en direct

Pour illustrer les mécanismes d'une APT, Gérard a raconté une attaque fictive, mais plausible, dans laquelle un faux mail, envoyé en apparence par les organisateurs des Lundis de la

cybersécurité, propage un document PDF malveillant.
Ce **scénario de spear phishing** piégeait l'une des animatrices, Béatrice Laurent, qui, croyant à une communication interne, clique sur le lien… et déclenche ainsi une infection.

Ce simple **clic de trop**, rappelle Gérard, suffit à permettre :

- la **mise en place d'un canal de communication discret** (avec un serveur C2),
- l'**installation furtive d'un maliciel** (qui peut résider uniquement en mémoire),
- une **élévation de privilèges** en compromettant l'Active Directory,
- puis une **exfiltration progressive de données**.

Cette démonstration vise à marquer les esprits sur **la facilité avec laquelle une erreur humaine peut compromettre tout un système d'information**, même avec des dispositifs de sécurité déjà en place.

« Un clic trop rapide, une curiosité mal placée, et c'est tout un réseau qui peut être infiltré. »

Une menace qui échappe aux outils classiques

Gérard Péliks souligne enfin que les APT échappent souvent aux antivirus traditionnels. Ils utilisent des techniques avancées telles que :

- **le Fast Flux DNS**, pour faire changer constamment l'IP d'un domaine malveillant,
- des **RATs (Remote Access Trojans)** pour prendre le contrôle à distance des postes infectés,
- la **stéganographie**, pour dissimuler des données qui sont volées dans des images,
- ou encore l'usage de **ports standards chiffrés (443, 990)** pour exfiltrer les données en toute discrétion.

« Les cyberattaquants n'ont pas besoin d'aller vite. Ils prennent leur temps. Ils infiltrent, écoutent, extraient. Et quand on s'en aperçoit… il est souvent trop tard. »

Enfin, Gérard rappelle que le véritable enjeu réside moins dans la technologie que dans la **vigilance humaine**, et il conclut cette partie sur une phrase forte :

« La meilleure défense, c'est la lucidité collective. Pas seulement celle du RSSI, mais de chaque salarié. »

II. Le déroulé d’une attaque APT : étapes clés

L’un des apports les plus pédagogiques de l’intervention de Gérard Peliks fut sa présentation des **phases successives d’une attaque APT**, sous la forme d’un **scénario réaliste et structuré**, largement illustré par ses diapositives.

Il insiste sur le fait qu'une attaque APT n'est **ni improvisée ni brutale**, mais **progressive**, souvent **invisible** et **ciblée** avec précision. L’attaque suit un **cycle bien défini**, que l’on retrouve dans la plupart des campagnes orchestrées par des groupes structurés.

Reconnaissance et ingénierie sociale

Avant même de lancer une attaque, le groupe malveillant commence par **collecter des informations** sur la cible. Cette phase de reconnaissance se divise en deux formes :

- **Passive**, via les réseaux sociaux, les sites internet, les CVs en ligne, les publications, etc. Un simple profil LinkedIn mal configuré peut déjà indiquer qui travaille sur quoi, avec qui, et dans quel secteur.
- **Active**, en interagissant directement avec l’environnement de la cible (visites physiques, appels à l’accueil, faux entretiens téléphoniques).

Cette étape permet de repérer **les profils clés** (collaborateurs sensibles, administrateurs système, membres de direction…) et d’élaborer un plan d’attaque sur mesure.

« Vous en dites trop en ligne. Et les prédateurs, eux, savent écouter. »

Intrusion initiale (attaque)

La deuxième étape consiste à **pénétrer le système**, souvent par le biais d’un **mail de spear phishing**. C’est ici que la **cible humaine** est exploitée : le mail frauduleux semble crédible, urgent ou personnalisé. Une fois ouvert, il incite à cliquer sur une pièce jointe ou un lien.

Dans la démonstration, un faux mail co-signé par Béatrice Laurent et Gérard Peliks lui-même — annonçant un changement de jour pour les Lundis de la cybersécurité — contenait un fichier PDF infecté. Ce simple clic suffit à **exécuter un morceau de code malveillant**.

« Un petit clic, une grosse claque. »

Établissement d’un canal de communication

Une fois l'infection initiale réussie, le maliciel s’installe **furtivement**, sans alerter l'utilisateur. Il établit une **connexion vers un serveur distant de commande et de contrôle (C2)**, appartenant au groupe attaquant.

Grâce à cette communication, le maliciel peut :

- Télécharger ses composants supplémentaires,
- Recevoir des instructions,

- Envoyer des données collectées.

Cette communication utilise souvent **le protocole HTTPS (port 443)**, difficile à bloquer car il est utilisé pour la majorité du trafic web sécurisé. De plus, les groupes APT utilisent des techniques comme le **Fast Flux DNS** ou le **double Fast Flux**, pour changer constamment les adresses IP et domaines utilisés, rendant toute traçabilité quasiment impossible.

Élévation de privilèges

À ce stade, le maliciel n'a que les droits de l'utilisateur piégé. Il lui faut donc **monter en privilèges** pour accéder à l'Active Directory ou à d'autres ressources critiques.

C'est ici qu'entrent en jeu des outils comme **Mimikatz**, initialement développé comme preuve de concept par un chercheur français, mais largement repris par des groupes malveillants. Mimikatz permet de :

- Récupérer les identifiants stockés en mémoire,
- Détourner des jetons d'authentification,
- Accéder à des comptes avec des privilèges élevés.

Une fois administrateur du poste, puis du réseau, le groupe attaquant **prend le contrôle du système d'information** de manière silencieuse.

Expansion latérale

Avec les droits d'administration, les assaillants peuvent maintenant **se déplacer latéralement** dans le système d'information : de poste en poste, de serveur en serveur, pour **repérer les ressources stratégiques**, les documents confidentiels, les bases de données sensibles.

Ils étendent progressivement leur contrôle, tout en maintenant une **présence discrète**, évitant toute détection par les outils de sécurité classiques.

Exfiltration des données

Lorsque l'objectif est atteint, les données identifiées sont **exfiltrées** vers l'extérieur. Cela se fait généralement de manière :

- **Chiffrée**, pour échapper aux inspections réseau,
- **Segmentée**, pour ne pas éveiller de soupçons (petites quantités, à intervalles réguliers),
- **Stéganographiée**, parfois, pour dissimuler les données dans des images ou autres supports inoffensifs.

Les ports utilisés sont souvent **443 (HTTPS)** ou **990 (FTPS)**.

Effacement des traces

Enfin, pour **effacer toute trace de leur passage**, les groupes APT peuvent :

- Supprimer les journaux système,

- Désinstaller les outils utilisés,
- Détruire le maliciel.

À l’issue du processus, la victime ne se rend compte de l’attaque que bien plus tard — parfois plusieurs mois après — lors d’un audit, d’une fuite avérée ou d’une alerte externe.

III. Contre-mesures : sensibiliser et surveiller

Après avoir exposé en détail le fonctionnement des attaques APT, Gérard Peliks a consacré une partie importante de son intervention à la **prévention**, en insistant sur un message central : **la technologie ne suffit pas**. Si les attaques APT sont redoutables, c'est parce qu'elles exploitent autant des **failles humaines** que des **failles techniques**. Et face à ces menaces furtives, il faut adopter une **hygiène cyber rigoureuse** à tous les niveaux de l'organisation.

Sensibiliser tous les collaborateurs, sans exception

Pour Gérard, le facteur humain reste le **maillon le plus fragile** du dispositif de cybersécurité. La compromission ne commence pas forcément par une faille technique : **un clic malheureux, une curiosité mal placée, ou une routine non remise en question suffisent à déclencher une attaque.**

C'est pourquoi il prône une **sensibilisation globale**, qui doit impliquer :

- Le personnel de direction,
- Les ingénieurs et techniciens,
- Les fonctions support (RH, finances, communication…),
- Mais aussi les **personnels d'accueil, de maintenance ou les stagiaires**.

« Une attaque APT ne distingue pas les fonctions : elle exploite les comportements. »

Il rappelle avec humour (et sévérité) le cas de Béatrice Laurent, co-organisatrice des Lundis de la cybersécurité, qui dans la mise en scène a cliqué sur un faux mail... malgré ses connaissances. Cela souligne que **personne n'est à l'abri**, et que la vigilance ne doit pas reposer sur un seul individu, mais sur une **culture commune de la sécurité.**

Maîtriser les privilèges : le principe du moindre accès

Un autre pilier de la défense contre les APT repose sur la **gestion fine des privilèges**. Gérard insiste : **plus les droits sont larges et mal contrôlés, plus le terrain est favorable à une expansion silencieuse de l'attaque.**

Il recommande :

- De **restreindre au strict nécessaire** les accès aux fichiers, bases de données, et outils sensibles.
- D'**auditer régulièrement l'Active Directory** pour détecter les anomalies ou comptes inactifs encore actifs.
- D'**interdire les droits administrateurs** sur les postes utilisateurs (hors exception justifiée).
- D'**isoler les environnements critiques** par des cloisonnements réseau (micro-segmentation).

« C'est comme une maison avec des alarmes partout… mais où tout le monde a la clé. »

Surveiller activement les signaux faibles

Les attaques APT ne laissent souvent que des **traces très faibles**, difficilement détectables par un antivirus traditionnel. D'où l'importance croissante des outils de **détection comportementale et réseau**, comme :

- **EDR (Endpoint Detection and Response)** : pour surveiller les postes clients.
- **NDR (Network Detection and Response)** : pour analyser les flux réseau en profondeur.
- **SIEM** ou solutions d'agrégation de logs : pour corréler des événements suspects.

Gérard Peliks cite également des éditeurs ou outils spécialisés (sans faire de publicité directe), tels que **Balabit, Interdata, Pink Castle, Wallix** (entreprise française), qui peuvent aider à identifier une élévation de privilèges ou un comportement anormal à temps.

« Si vous n'avez rien vu au moment où l'APT prend les droits d'administrateur, il est déjà trop tard. »

Réagir vite et signaler

Enfin, Gérard a rappelé l'importance d'une **réaction rapide** lorsqu'une attaque est suspectée :

- **Isoler le poste infecté** sans délai,
- **Prévenir les autorités compétentes**, comme **cybermalveillance.gouv.fr** ou **l'ANSSI**,
- **Conserver les traces** pour les investigations ultérieures,
- **Notifier la CNIL** sous 72 heures en cas de fuite de données personnelles (RGPD).

Il recommande notamment la lecture du **rapport du CERT-FR sur les actions du groupe APT28**, publié le 29 avril 2025, comme ressource actualisée et instructive.

Au terme de cette partie, Gérard rappelle que, malgré la complexité apparente des APT, **la prévention repose sur des gestes simples**, répétés et ancrés dans les habitudes. La meilleure défense reste une combinaison de **bon sens numérique**, **réduction de la surface d'attaque** et **surveillance continue.**

« Le clic de trop est toujours possible. Ce qui compte, c'est que l'attaque ne devienne pas systémique. »

IV. Géopolitique des APT : acteurs étatiques et groupes connus

Dans la dernière partie de son intervention, Gérard Peliks a élargi son propos en situant les APT dans un **contexte géopolitique mondial**, rappelant que les attaques informatiques ne relèvent pas uniquement de la cybercriminalité opportuniste, mais aussi — et de plus en plus — **d'opérations commanditées ou tolérées par des États**. Les groupes APT ne sont pas des hackers isolés : ce sont des **structures organisées, financées, entraînées**, parfois intégrées aux services de renseignement de grandes puissances.

Des cyberattaques devenues instruments de puissance

Les APT sont aujourd'hui au cœur des **conflits hybrides** modernes. Elles permettent à un État de mener des actions offensives, de l'espionnage industriel à la désinformation, **sans déclaration de guerre**, tout en niant formellement toute implication. Gérard rappelle que la France, comme d'autres nations, est visée régulièrement par ce type d'opérations, dans un jeu d'influence global et feutré.

« Un État n'a pas d'amis. Il n'a que des intérêts », cite-t-il en reprenant une formule gaullienne.

Les attaques ne visent pas uniquement les institutions étatiques ou militaires : les **entreprises sensibles, les universités, les startups technologiques**, les **hôpitaux** ou encore les **collectivités territoriales** sont autant de cibles pour ces groupes.

APT28 (Fancy Bear) : une menace bien identifiée

Parmi les groupes évoqués, **APT28**, aussi connu sous le nom de **Fancy Bear**, a été au centre de la présentation. Rattaché au **GRU**, le service de renseignement militaire russe, APT28 est **responsable de multiples campagnes d'espionnage** visant notamment :

- Des ministères français,
- Des organisations de défense européenne,
- Des entreprises du secteur aéronautique ou de l'énergie.

Gérard a présenté un extrait du **rapport du CERT-FR** daté du 29 avril 2025, qui confirme l'implication d'APT28 dans des campagnes récentes visant une **dizaine d'entités françaises sensibles**.

La force d'APT28 réside dans :

- Une **connaissance fine des systèmes ciblés**,
- Une **utilisation intensive du spear phishing personnalisé**,
- Des malwares difficiles à détecter,
- Une **capacité de dissimulation grâce au Fast Flux DNS**.

« Quand APT28 vous cible, ce n'est jamais par hasard. Ils savent pourquoi ils viennent et ce qu'ils cherchent. »

Une cartographie mondiale des groupes APT

Au-delà du cas russe, Gérard Peliks a dressé un **panorama des principaux groupes APT connus**, classés par origine géopolitique :

- **Chine**
  - **APT41** : spécialisé dans le vol de **code source** de logiciels stratégiques, notamment américains.
  - **Deep Panda**, **Elder Wood**, etc. : axés sur l'espionnage industriel.
- **Corée du Nord**
  - **APT38 / Lazarus** : mène des attaques massives sur les systèmes bancaires pour **financer le régime**, notamment via le réseau SWIFT ou des ransomwares.
- **Iran**
  - **APT35 / APT39** : focalisés sur le Moyen-Orient, les dissidents politiques et les infrastructures critiques.
- **Russie**
  - **APT28 (Fancy Bear)** : renseignement militaire.
  - **APT29 (Cozy Bear)** : renseignement étranger (SVR).
  - **Gamaredon** : fortement actif contre l'Ukraine.

Il rappelle que ces noms techniques peuvent aussi être connus sous des **surnoms évocateurs** (Bears, Pandas, etc.) dans les rapports de cybersécurité. Ils traduisent une **guerre de l'ombre** qui oppose des puissances mondiales dans le cyberespace.

Et la France ?

Interrogé par le public en filigrane, Gérard n'élude pas la question : la France possède bien sûr des **capacités offensives** dans le domaine cyber, notamment via le **COMCYBER**. Mais sur les pratiques françaises en matière d'APT, il reste prudent :

« Je ne suis pas habilité à vous répondre. Ce serait probablement classé secret-défense. »

Cette mise en perspective globale a permis aux participants de mieux comprendre que **les attaques APT sont le prolongement numérique de stratégies étatiques**, et qu'elles imposent une vigilance accrue, bien au-delà de la seule sphère technique.

V. Claire Alberio : être réserviste en gendarmerie

En seconde partie de séance, **Claire Alberio**, fidèle intervenante des Lundis de la cybersécurité, a partagé son expérience en tant que **réserviste citoyenne puis opérationnelle de la gendarmerie nationale**. Elle a présenté de manière concrète ce qu'implique cet engagement, encore méconnu, mais essentiel dans la stratégie de cybersécurité nationale.

Deux types de réserve, une même ambition

Claire a rappelé qu'il existe **deux formes principales de réserve** dans la gendarmerie :

- La **réserve opérationnelle**, mobilisée sur le terrain pour des missions de sécurité ou d'appui.
- La **réserve citoyenne** composée de volontaires issus de la société civile, qui mettent **leurs compétences professionnelles au service de l'intérêt général**, notamment dans les domaines techniques comme le numérique.

Un engagement au croisement de l'expertise civile et des besoins institutionnels

Claire a mis en lumière **la complémentarité entre son métier civil dans le domaine cyber et son rôle de réserviste**. En tant que spécialiste, elle intervient dans des actions de :

- **Sensibilisation à la cybersécurité** auprès de publics variés,
- **Soutien aux enquêtes ou exercices** en lien avec les forces de l'ordre,
- **Veille et participation à des événements** collaboratifs sur la protection numérique.

Elle a souligné la **souplesse de l'engagement**, qui permet d'apporter son aide ponctuellement, en fonction de ses disponibilités, sans nécessairement s'engager à temps plein.

Un appel à contribution

Claire a conclu en incitant les personnes issues des secteurs de l'IT, de la cybersécurité, du droit ou de la pédagogie à **rejoindre la réserve citoyenne**, pour contribuer activement à la **cyberdéfense nationale**, même sans uniforme.

« Être réserviste, c'est une autre façon d'agir pour la sécurité du pays, en apportant son expertise là où elle peut vraiment faire la différence. »

VI. Questions / Réponses

Question : Peut-on considérer la NSA comme un groupe APT ?

Réponse : Gérard Peliks a rappelé que le terme « APT » désigne une méthode d'attaque persistante, souvent utilisée par des États. La NSA mène des opérations de surveillance et de renseignement numérique au niveau mondial. À ce titre, **elle dispose de capacités offensives comparables à celles des groupes APT** les plus avancés, même si elle opère dans un cadre étatique légal (américain).

Question : Où peut-on consulter un panorama global des attaques APT mondiales ?

Réponse : Plusieurs participants ont recommandé des ressources comme **le site ransomware.live**, **les rapports du CERT-FR**, ou encore des **cartes collaboratives sur uMap** répertoriant les attaques par secteur ou pays. Gérard a aussi mentionné les **lettres de veille de Lionel Guillet**, disponibles sur demande.

Question : Est-ce que Mimikatz permet une élévation de privilèges ?

Réponse : Un échange a eu lieu sur ce point. Gérard a précisé que **Mimikatz ne permet pas directement d'élever les privilèges**, mais permet de **récupérer les identifiants et hash en mémoire**, **à condition d'avoir déjà des droits administrateurs**. Il est donc utilisé dans **une phase post-compromission** pour renforcer le contrôle de l'attaquant sur le SI.

Question : Peut-on détecter une attaque APT dès les premières phases ?

Réponse : Oui, mais cela nécessite une **surveillance proactive** des signaux faibles : connexions réseau anormales, comportements inhabituels, élévation de privilèges injustifiée, etc. Des outils comme les **EDR**, **NDR**, ou des audits réguliers de l'Active Directory permettent d'agir avant que l'exfiltration de données ne survienne.

Question : Quels sont les critères pour devenir réserviste de la gendarmerie ?

Réponse : Claire Alberio a répondu qu'il faut :

- Être de nationalité française,
- Avoir plus de 17 ans,
- Être sans casier judiciaire,
- Et, pour la réserve citoyenne, **disposer d'une expertise utile à la gendarmerie** (cybersécurité, droit, communication, pédagogie, etc.).

L'engagement est basé sur le volontariat, avec une validation des candidatures par la gendarmerie.

Question : La France mène-t-elle aussi des attaques APT ?

Réponse : Gérard Peliks a répondu avec humour que **personne ne répondra officiellement à cette question**, car cela relève du **secret-défense**. Il rappelle toutefois que la France dispose d'un commandement cyber (COMCYBER) et de capacités offensives légales dans le cadre d'opérations militaires ou de renseignement.