EUROPEAN UNION AGENCY
FOR CYBERSECURITY


# RAPPORT DE L'ENISA SUR LE PAYSAGE DES MENACES 2021

Avril 2020 à mi-juillet 2021

OCTOBRE 2021

# À PROPOS DE L'ENISA

L'Agence européenne pour la cybersécurité (ENISA) est l'agence de l'Union européenne qui vise à garantir un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'Union européenne sur la cybersécurité, l'ENISA contribue à la politique de l'Union en matière de cybersécurité, améliore la fiabilité des produits, services et processus TIC à l'aide de schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'Union, et aide l'Europe à se préparer aux défis informatiques de demain. Par le partage des connaissances, le renforcement des capacités et des initiatives de sensibilisation, l'Agence œuvre de concert avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, améliorer la résilience des infrastructures de l'Union et maintenir la sécurité numérique de la société européenne et de ses citoyens. Pour plus d'informations sur l'ENISA et ses travaux, consultez le site: www.enisa.europa.eu.

## CONTACT

Pour contacter les auteurs, veuillez utiliser l'adresse etl@enisa.europa.eu.
Pour les demandes de renseignements des médias concernant le présent document, veuillez utiliser l'adresse press@enisa.europa.eu.

## ÉDITEURS

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras — Agence de l'Union européenne pour la cybersécurité

## CONTRIBUTEURS

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

## REMERCIEMENTS

Nous tenons à remercier les membres et les observateurs du groupe de travail ad hoc de l'ENISA sur les paysages des cybermenaces (Working Group on Cyber Threat Landscapes) pour leurs précieux commentaires et retours dans le cadre de la validation de ce rapport. Nous tenons également à remercier le groupe consultatif de l'ENISA et le réseau des agents de liaison nationaux pour leurs remarques utiles.
Nous souhaitons en outre remercier les équipes de l'ENISA chargées de l'appréciation de la situation (Situational Awareness) et de la notification des incidents (Incident Notification) pour leur contribution active et leur soutien dans le cadre de la consolidation de différents éléments d'information dans le paysage des menaces.

## MENTION LÉGALE



## DÉCLARATION CONCERNANT LES DROITS D'AUTEUR

ISBN: 978-92-9204-536-4 — DOI: 10.2824/324797 — ISSN: 2363-3050

# TABLE DES MATIÈRES

# RÉSUMÉ

Voici la neuvième édition du rapport de l'ENISA sur le paysage des menaces (ci-après «rapport ETL»). Il s'agit d'un rapport annuel sur l'état des menaces en matière de cybersécurité, qui identifie les principales menaces, les grandes tendances observées en ce qui concerne les menaces, les acteurs des menaces et les techniques d'attaque, et qui décrit également les mesures d'atténuation pertinentes. Dans le cadre de l'amélioration constante de notre méthodologie pour le développement des paysages des menaces, les travaux de cette année ont été soutenus par un groupe de travail ad hoc de l'ENISA sur les paysages des menaces pour la cybersécurité mis sur pied récemment.

La période couverte par le rapport ETL 2021 s'étend d'avril 2020 à juillet 2021 et est appelée «période de référence» tout au long du rapport. Les principales menaces identifiées au cours de la période de référence sont les suivantes:

- **Rançongiciels**
- **Logiciels malveillants**
- **Cryptominage**
- **Menaces liées au courrier électronique**
- **Menaces visant les données**
- **Menaces visant la disponibilité et l'intégrité**
- **Désinformation — mésinformation**
- **Menaces non malveillantes**
- **Attaques de la chaîne d'approvisionnement**

Dans le présent rapport, nous abordons les 8 premières catégories de menaces pour la cybersécurité. Les menaces visant la chaîne d'approvisionnement, la 9e catégorie, ont été analysées en détail, en raison de leur importance particulière, dans un rapport de l'ENISA dédié intitulé «ENISA Threat landscape for Supply Chain Attacks» (Rapport de l'ENISA sur le paysage des menaces pour les attaques de la chaîne d'approvisionnement)[1].

Pour chacune des menaces identifiées, les techniques d'attaque, les incidents et les tendances notables sont examinés, de même que les mesures d'atténuation proposées. En ce qui concerne les tendances, pour la période de référence, il convient de noter que:

- Les **rançongiciels** ont été évalués comme la **principale menace pour 2020-2021.**
- **Les organisations gouvernementales ont renforcé leur action** tant au niveau national qu'international.
- **Les cyberdélinquants sont de plus en plus motivés par la monétisation** de leurs activités, par exemple les rançongiciels. La **cryptomonnaie** reste la méthode de paiement la plus courante pour les acteurs des menaces.
- Le **déclin des logiciels malveillants** observé en 2020 se poursuit en 2021. En 2021, nous avons assisté à une augmentation du nombre d'acteurs des menaces qui recourent à des langages de programmation relativement nouveaux ou peu courants pour transmettre leur code.
- Le volume d'**infections par cryptominage** a atteint un **niveau record** au premier trimestre 2021 par rapport aux dernières années. Le **gain financier** associé au cryptominage a incité les acteurs des menaces à commettre ces attaques.
- **La COVID-19 reste le leurre principal dans les campagnes** d'attaques par courrier électronique.
- **Les violations de données liées au secteur des soins de santé se sont multipliées**.
- **Les campagnes traditionnelles de déni de service distribué (DDoS)** en 2021 sont plus ciblées, plus persistantes et de plus en plus multivectorielles. **L'internet des objets (IdO)** associé aux **réseaux mobiles** donne lieu à une nouvelle vague d'attaques DDoS.

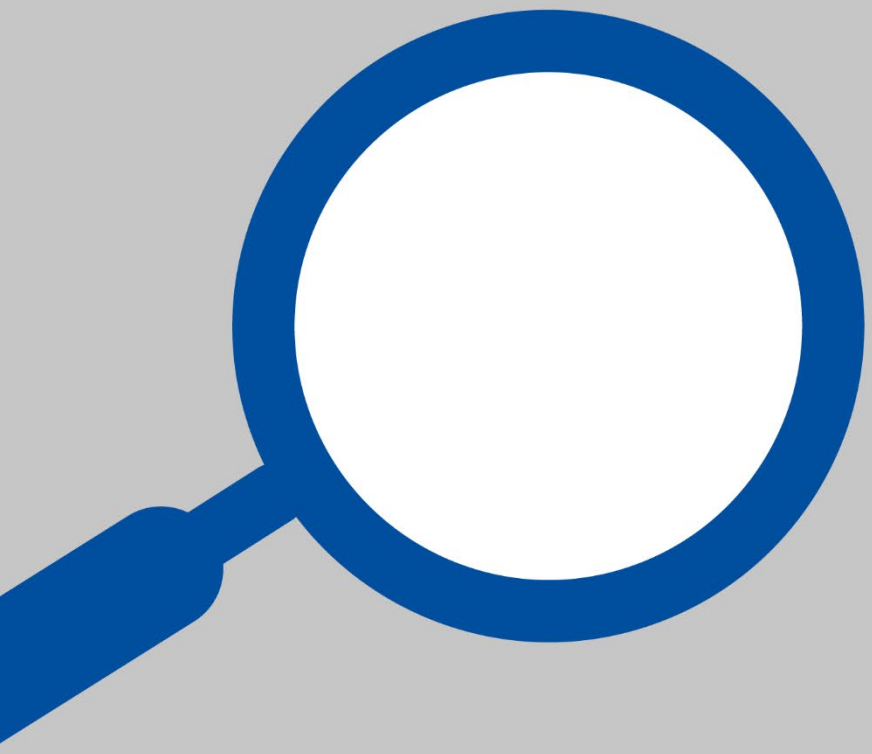
[1] *ENISA Threat Landscape for Supply Chain Attacks*, juillet 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

- En 2020 et 2021, nous observons un **pic d'incidents non malveillants**, étant donné que la pandémie de COVID-19 a favorisé la multiplication des **erreurs humaines** et des **configurations système incorrectes**, à tel point que la plupart des violations en 2020 ont été causées par des erreurs.

Comprendre les tendances concernant les acteurs des menaces, leurs motivations et leurs cibles aide grandement à planifier les défenses de la cybersécurité et les stratégies d'atténuation. Cela fait partie intégrante de notre évaluation globale des menaces, dans la mesure où cela permet de définir les priorités des contrôles de sécurité et d'élaborer une stratégie dédiée en fonction de l'influence potentielle et de la probabilité de matérialisation des menaces. Dans cette perspective, aux fins du rapport ETL 2021, les quatre catégories suivantes d'acteurs des menaces pour la cybersécurité sont prises en considération:

- **Acteurs parrainés par des États**
- **Acteurs de la cybercriminalité**
- **Acteurs de services de piratage pour le compte d'autrui**
- **Hacktivistes**

Grâce à une analyse continue, l'ENISA a dégagé des tendances et des points d'intérêt pour chacune des menaces majeures présentées dans le rapport ETL 2021. Les conclusions et jugements clés de la présente évaluation reposent sur des ressources multiples et accessibles au public qui sont mentionnées dans les références utilisées pour l'élaboration du présent document. Le rapport s'adresse principalement aux décideurs et aux responsables politiques stratégiques, mais il est également intéressant pour la communauté de techniciens en cybersécurité.



# VUE D'ENSEMBLE DU PAYSAGE DES MENACES

Dans sa neuvième édition, le rapport de l'ENISA sur le paysage des menaces (ci-après «rapport ETL ») dresse une vue d'ensemble du paysage des menaces pour la cybersécurité. Le rapport ETL est en partie stratégique et en partie technique, avec des informations pertinentes pour les lecteurs spécialisés ou non. Les travaux de cette année ont été soutenus par un nouveau groupe de travail ad hoc de l'ENISA sur les paysages des menaces pour la cybersécurité (Working Group on Cybersecurity Threat Landscapes)[2].

Les attaques contre la cybersécurité ont continué d'augmenter au cours des années 2020 et 2021, non seulement en termes de vecteurs et de nombre, mais aussi en termes de conséquences. La pandémie de COVID-19 a également, comme prévu, eu une incidence sur le paysage des menaces pour la cybersécurité. L'un des développements les plus tenaces qui ont résulté de la pandémie de COVID-19 est le passage durable à un modèle de bureau hybride. Par conséquent, les menaces pour la cybersécurité liées à la pandémie et à l'exploitation de la «nouvelle norme» deviennent courantes. Cette tendance a élargi la surface d'attaque, de sorte que nous avons assisté à une augmentation du nombre de cyberattaques visant des organisations et des entreprises par l'intermédiaire des bureaux au domicile privé[3].

D'une manière générale, les menaces pour la cybersécurité sont en augmentation. Sous l'impulsion d'une présence en ligne toujours croissante, de la transition des infrastructures traditionnelles vers des solutions en ligne et dans le nuage, d'une interconnectivité avancée et de l'exploitation de nouvelles caractéristiques des technologies émergentes telles que l'intelligence artificielle (IA)[4][5], le paysage de la cybersécurité s'est développé en termes de sophistication des attaques, de leur complexité et de leur incidence. En particulier, la menace pesant sur les chaînes d'approvisionnement et leur importance en raison de leurs effets en cascade potentiellement catastrophiques occupe désormais la première place parmi les menaces majeures, si bien que l'ENISA a élaboré un paysage des menaces dédié à cette catégorie de menaces[6].

Il convient de noter que dans cette version du rapport ETL, une attention particulière a été accordée à l'incidence des cybermenaces dans différents secteurs, y compris ceux énumérés dans la directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI). Des informations intéressantes peuvent être tirées des particularités de chaque secteur en ce qui concerne le paysage des menaces, ainsi que les interdépendances potentielles et les domaines importants. Par conséquent, les paysages de menaces sectorielles méritent une attention accrue.

Des avancées notables ont également été réalisées par les défenseurs de la cybercommunauté cette année, ainsi que par les décideurs politiques. La communauté internationale a commencé à prendre conscience de l'importance de la communication et de la coopération dans l'examen et le suivi des cyberdélinquants, les rançongiciels (la menace la plus importante pour la période de référence du rapport ETL 2021) étant en particulier devenus un point prioritaire à l'ordre du jour des réunions sur la stratégie entre les dirigeants au niveau mondial.

Les lecteurs spécialisés des éditions précédentes du rapport ETL 2021 remarqueront une différence dans la cartographie des principales menaces. Cette année, l'ENISA a pris du recul et a consolidé les catégories de menaces afin d'intégrer et de mieux représenter les menaces similaires. Cette démarche s'inscrit dans le cadre des

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM — *Cost of a Data Breach Report 2020* — https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] *ENISA AI Threat Landscape:* https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
[6] *ENISA Threat Landscape for Supply Chain Attacks*, juillet 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

efforts permanents déployés en vue d'une révision de la taxinomie des menaces, et contribuera à établir des tendances de façon méthodologique au cours des prochaines années.

Le rapport ETL 2021 repose sur diverses sources de renseignements de sources ouvertes et sur la cybermenace. Il identifie les menaces, tendances et conclusions majeures, et fournit des stratégies d'atténuation de haut niveau pertinentes. L'ENISA œuvre actuellement à la consolidation de la méthodologie pour l'établissement de rapports sur le paysage des menaces afin de promouvoir la transparence et la cohérence des travaux.

## 1.1. PRINCIPALES MENACES

Plusieurs cybermenaces sont apparues et se sont concrétisées au cours des années 2020 et 2021. Sur la base de l'analyse présentée dans le présent rapport, le rapport de l'ENISA sur le paysage des menaces 2021 identifie et met l'accent sur les 8 principaux groupes de menaces suivants (voir Figure 1). Ces 8 groupes de menaces sont mis en évidence en raison de leur importance au cours de la période de référence, de leur popularité et de l'incidence de la matérialisation de ces menaces.

- **Rançongiciels**
  Le rançongiciel est un type d'attaque malveillante par laquelle les attaquants chiffrent les données d'une organisation et exigent un paiement pour rétablir l'accès. Les rançongiciels ont constitué la principale menace au cours de la période de référence, avec plusieurs incidents majeurs très médiatisés. L'importance et l'incidence de la menace des rançongiciels sont également mises en évidence par une série d'initiatives politiques connexes dans l'Union européenne (UE) et dans le monde entier.

- **Logiciels malveillants**
  Les logiciels malveillants sont des logiciels ou micrologiciels destinés à effectuer un processus non autorisé qui aura une incidence négative sur la confidentialité, l'intégrité ou la disponibilité d'un système. La menace des logiciels malveillants a toujours occupé une place importante depuis de nombreuses années, mais dans une moindre mesure au cours de la période de référence du rapport ETL 2021. L'utilisation de nouvelles techniques d'attaque et certaines victoires majeures de la communauté répressive ont eu des répercussions sur les opérations des acteurs des menaces concernés.

- **Cryptominage**
  Le cryptominage, ou minage clandestin, est un type de cybercriminalité dans lequel un criminel utilise secrètement la puissance de calcul d'une victime pour générer de la cryptomonnaie. Avec la prolifération des cryptomonnaies et leur adoption de plus en plus large par le grand public, une augmentation des incidents de cybersécurité correspondants a été observée.

- **Menaces liées au courrier électronique**
  Les attaques liées au courrier électronique englobent un ensemble de menaces qui exploitent les faiblesses de la psychologie humaine et des habitudes quotidiennes, plutôt que des vulnérabilités techniques dans les systèmes d'information. Il est intéressant de noter que, malgré les nombreuses campagnes de sensibilisation et d'éducation contre ces types d'attaques, la menace persiste dans une mesure notable. En particulier, la compromission de courriers électroniques professionnels et les techniques sophistiquées avancées permettant d'obtenir des gains financiers sont en hausse.

- **Menaces visant les données**
  Cette catégorie englobe les violations/fuites de données. Une violation ou une fuite de données désigne la divulgation de données sensibles, confidentielles ou protégées dans un environnement non sécurisé. Les violations de données peuvent résulter d'une cyberattaque, de l'intervention d'un initié, d'une perte involontaire ou d'une exposition des données. La menace reste élevée, car l'accès aux données est une cible privilégiée pour les attaquants pour de nombreuses raisons, telles que l'extorsion, la rançon, la diffamation, la mésinformation, etc.

- **Menaces visant la disponibilité et l'intégrité**
  La disponibilité et l'intégrité sont la cible d'une multitude de menaces et d'attaques, en particulier celles par déni de service (DoS) et les attaques web. Strictement lié aux attaques basées sur le web, le déni de service distribué (DDoS) est l'une des menaces les plus graves pour les systèmes informatiques: il cible leur disponibilité en épuisant les ressources, provoquant une baisse des performances, une perte de données et des interruptions de service. Cette menace occupe constamment une place élevée dans le rapport ETL, en raison à la fois de sa manifestation dans des incidents réels et de son incidence potentiellement élevée.

- **Désinformation — mésinformation**
  Les campagnes de désinformation et de mésinformation sont de plus en plus nombreuses, favorisées par l'utilisation accrue des plateformes de médias sociaux et des médias en ligne, ainsi que par l'augmentation de la présence en ligne des citoyens en raison de la pandémie de COVID-19. C'est la première fois que ce groupe de menaces est cité dans le rapport ETL, mais son importance dans le cyberespace est grande. Les campagnes de désinformation et de mésinformation sont fréquemment utilisées dans des attaques hybrides pour réduire la perception globale de confiance, un des principaux défenseurs de la cybersécurité.

- **Menaces non malveillantes**
  Les menaces sont généralement considérées comme des activités volontaires et malveillantes provoquées par des adversaires qui présentent un certain intérêt à attaquer une cible spécifique. Avec cette catégorie, nous couvrons les menaces pour lesquelles l'intention malveillante n'est pas évidente. Il s'agit principalement de menaces fondées sur des erreurs humaines et des configurations système incorrectes, mais elles peuvent également faire référence à des catastrophes naturelles qui ciblent les infrastructures informatiques. En raison également de leur nature, ces menaces sont constamment présentes dans le paysage annuel des menaces et constituent une préoccupation majeure pour l'évaluation des risques.

**Figure 1:** Rapport de l'ENISA sur le paysage des menaces 2021 — Principales menaces


Il convient de noter que les menaces susmentionnées impliquent des catégories et la collecte de menaces, regroupées dans les huit domaines indiqués ci-dessus. Chacun des groupes de menaces est analysé plus en détail dans un chapitre spécifique du présent rapport, qui développe ses particularités et fournit des informations, des conclusions, des tendances, des techniques d'attaque et des vecteurs d'atténuation plus spécifiques.

## 1.2. PRINCIPALES TENDANCES

La liste ci-dessous récapitule les principales tendances observées dans le paysage des cybermenaces au cours de la période de référence. Celles-ci sont également examinées en détail dans les différents chapitres composant le rapport de l'ENISA sur le paysage des menaces de 2021.

- Les **compromissions de la chaîne d'approvisionnement très sophistiquées et lourdes de conséquences** se sont multipliées, comme l'a souligné le rapport de l'ENISA sur le paysage des menaces dédié à la chaîne d'approvisionnement. Les **fournisseurs de services gérés** sont des cibles de grande valeur pour les cyberdélinquants.
- **La COVID-19 a favorisé les activités de cyberespionnage** et créé des **opportunités pour les cyberdélinquants**.
- **Les organisations gouvernementales ont renforcé leur action** tant au niveau national qu'international. Des efforts accrus ont été observés de la part des gouvernements pour démanteler les acteurs de menaces parrainés par des États et intenter des actions en justice à leur encontre.
- **Les cyberdélinquants sont de plus en plus motivés par la monétisation** de leurs activités, par exemple les rançongiciels. La **cryptomonnaie** reste la méthode de paiement la plus courante pour les acteurs des menaces.
- Les attaques de cybercriminalité **ciblent et affectent de plus en plus des infrastructures critiques**.
- **Les compromissions par courrier électronique d'hameçonnage et les attaques par force brute sur les services de bureau à distance** restent les deux **vecteurs d'infection par rançongiciels** les plus courants.
- L'accent mis sur les **modèles commerciaux** de type **RaaS (Ransomware as a Service, Rançongiciel en tant que service)** a augmenté au cours de l'année 2021, de sorte qu'il devient difficile d'imputer correctement la responsabilité aux différents acteurs des menaces.
- La fréquence des schémas de **rançongiciels à triple extorsion** a fortement augmenté au cours de l'année 2021.
- Le **déclin des logiciels malveillants** observé en 2020 se poursuit en 2021. En 2021, nous avons assisté à une augmentation du nombre d'acteurs des menaces qui recourent à des langages de programmation relativement nouveaux ou peu courants pour transmettre leur code.
- Les **logiciels malveillants ciblant des environnements de conteneurs** sont devenus beaucoup plus fréquents, avec des évolutions nouvelles telles que des logiciels malveillants sans fichier exécutés à partir de la mémoire.
- Les développeurs de logiciels malveillants continuent de trouver des moyens de **compliquer l'ingénierie inverse et l'analyse dynamique**.
- Le volume d'**infections par cryptominage** a atteint un **niveau record** au premier trimestre 2021 par rapport aux dernières années. Le **gain financier** associé au cryptominage a incité les acteurs des menaces à commettre ces attaques.
- **Le volume de minage pirate en 2021 et les activités de cryptominage sont à un niveau record**.
- Nous constatons une **transition des techniques de cryptominage des navigateurs vers une approche basée sur des fichiers**.
- **La COVID-19 reste le leurre principal dans les campagnes** d'attaques par courrier électronique.
- La **compromission de la messagerie en entreprise, mieux connue sous le terme anglais «Business E-mail Compromise» (BEC),** s'est **accrue**, a gagné en **sophistication** et est devenue plus **ciblée**.
- Le modèle commercial de type **PhaaS (Phishing-as-a-Service, hameçonnage en tant que service)** prend de l'importance.
- Les acteurs des menaces ont déplacé leur attention vers les **informations relatives aux vaccins** dans le contexte des menaces visant les données et les informations.
- **Les violations de données liées au secteur des soins de santé se sont multipliées**.
- Les attaques traditionnelles par déni de service distribué (DDoS) s'orientent vers les **réseaux mobiles et l'internet des objets (IdO)**.
- Le **déni de service de rançon (Ransom Denial of Service, RDoS)** est la nouvelle frontière des attaques par déni de service.
- Le **partage des ressources dans des environnements virtualisés** fait office d'amplificateur des attaques par DDoS.

- Les **campagnes DDoS** en 2021 sont devenues plus ciblées, beaucoup plus persistantes et de plus en plus multivectorielles.
- La **désinformation facilitée par l'intelligence artificielle (IA)** aide les attaquants à commettre leurs méfaits.
- **L'hameçonnage est au cœur des attaques de désinformation** et exploite fortement les croyances de la population.
- **La désinformation et la mésinformation** sont au cœur des activités de cybercriminalité et augmentent à un rythme sans précédent.
- **Le modèle commercial de type DaaS (Disinformation-as-a-Service, désinformation en tant que service)** s'est considérablement développé sous l'effet de la pandémie de COVID-19 et de la nécessité de disposer de davantage d'informations.
- En 2020 et 2021, nous avons observé un **pic d'incidents non malveillants**, étant donné que la pandémie de COVID-19 a favorisé la multiplication des **erreurs humaines** et des **configurations système incorrectes**, à tel point que la plupart des violations en 2020 ont été causées par des erreurs.
- Nous avons assisté à un **pic d'incidents non malveillants dans le domaine de la sécurité informatique dans le nuage**.

## 1.3. PROXIMITÉ DES PRINCIPALES MENACES DANS L'UE

Un aspect important à prendre en considération dans le contexte du rapport de l'ENISA sur le paysage des menaces est la proximité d'une cybermenace par rapport à l'Union européenne (UE). Cela est particulièrement important pour aider les analystes à évaluer le poids des cybermenaces, pour les associer avec des acteurs et des vecteurs potentiels des menaces, et même pour guider la sélection de vecteurs d'atténuation ciblés appropriés. Conformément à la classification proposée pour la politique européenne de sécurité et de défense commune (PESD)[7], nous classons les cybermenaces en quatre catégories, comme illustré dans le Tableau 1.

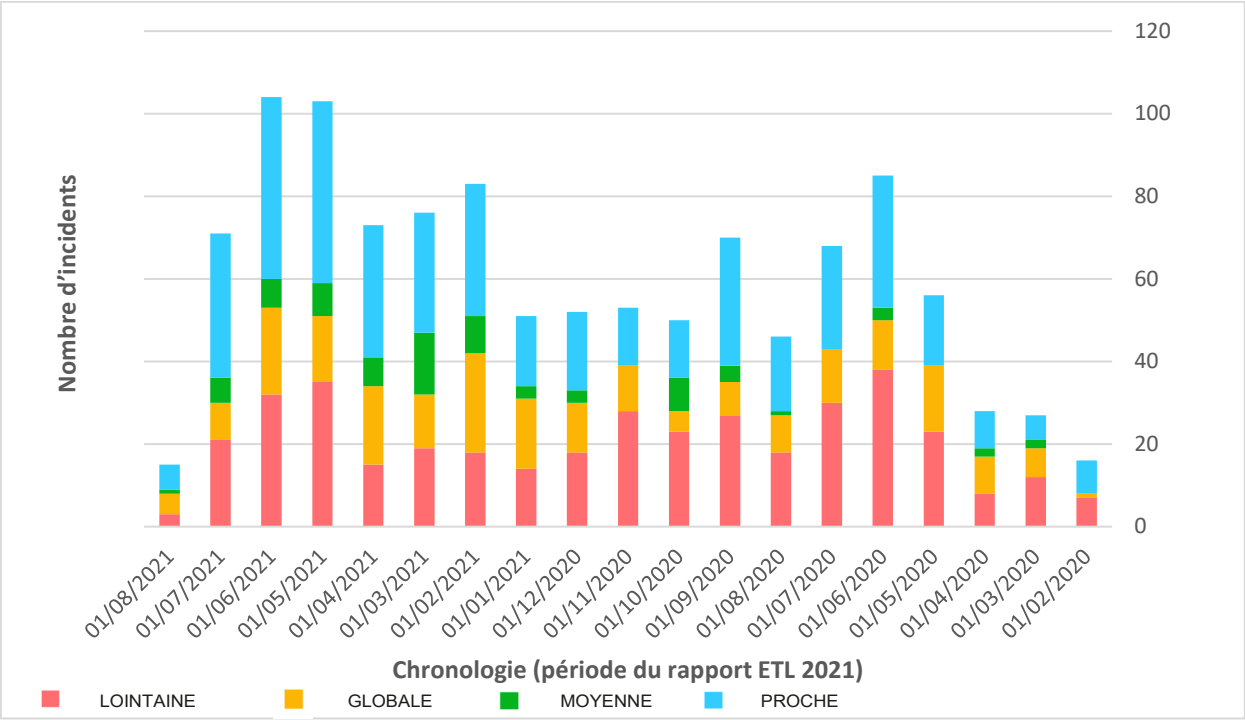
**Tableau 1:** Classification de la proximité des cybermenaces

| Proximité | Préoccupations |
|---|---|
| **PROCHE** | Réseaux et systèmes affectés, contrôlés et assurés à l'intérieur des frontières de l'UE. Population touchée à l'intérieur des frontières de l'UE. |
| **MOYENNE** | Réseaux et systèmes jugés essentiels pour les objectifs opérationnels dans le cadre du marché unique numérique de l'UE et des secteurs de la directive SRI, mais ils sont contrôlés et assurés par des autorités institutionnelles autres que l'UE ou des autorités publiques ou privées d'États membres. Population touchée dans des zones géographiques proches des frontières de l'UE. |
| **LOINTAINE** | Réseaux et systèmes qui, s'ils sont influencés, auront une incidence critique sur les objectifs opérationnels dans le cadre du marché unique numérique de l'UE et des secteurs de la directive SRI. Ils ne sont pas contrôlés ni assurés par des autorités institutionnelles de l'UE ni par des autorités publiques ou privées d'États membres. Population touchée dans des zones géographiques éloignées de l'UE. |
| **GLOBALE** | Tous les domaines susmentionnés |

La Figure 2 représente une chronologie des incidents liés aux principales catégories de menaces signalées dans le rapport ETL 2021. Il convient de noter que les informations figurant dans le graphique sont basées sur des renseignements d'origine sources ouvertes (ROSO) et résultent de travaux réalisés par l'ENISA dans le domaine de l'appréciation de la situation[8].

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
[8] Conformément à l'article 7, paragraphe 6, du règlement sur la cybersécurité de l'UE: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

**Figure 2:** Chronologie des incidents observés liés aux menaces majeures du rapport ETL (appréciation de la situation fondée sur les ROSO) du point de vue de leur proximité.




Comme le montre la figure ci-dessus, le nombre d'incidents a augmenté en 2021 par rapport à 2020. En particulier, la catégorie PROCHE («NEAR» en anglais) enregistre un nombre sans cesse croissant d'incidents liés à des menaces majeures, ce qui implique leur importance dans le contexte de l'UE. Sans surprise, les tendances mensuelles (non présentées dans la figure par souci de concision) sont assez similaires dans les différentes classifications, étant donné que la cybersécurité ne connaît aucune frontière et que, dans la plupart des cas, les menaces se matérialisent à tous les niveaux de proximité. Il convient de noter que, au cours des derniers mois couverts par le rapport ETL 2021, une plus grande proximité de type PROCHE de l'UE a été observée, une tendance que l'ENISA continuera à surveiller pour vérifier comment elle évolue et quelle est sa relation avec les activités des acteurs des menaces et des vecteurs de menaces actuels.

## 1.4. PRINCIPALES MENACES PAR SECTEUR

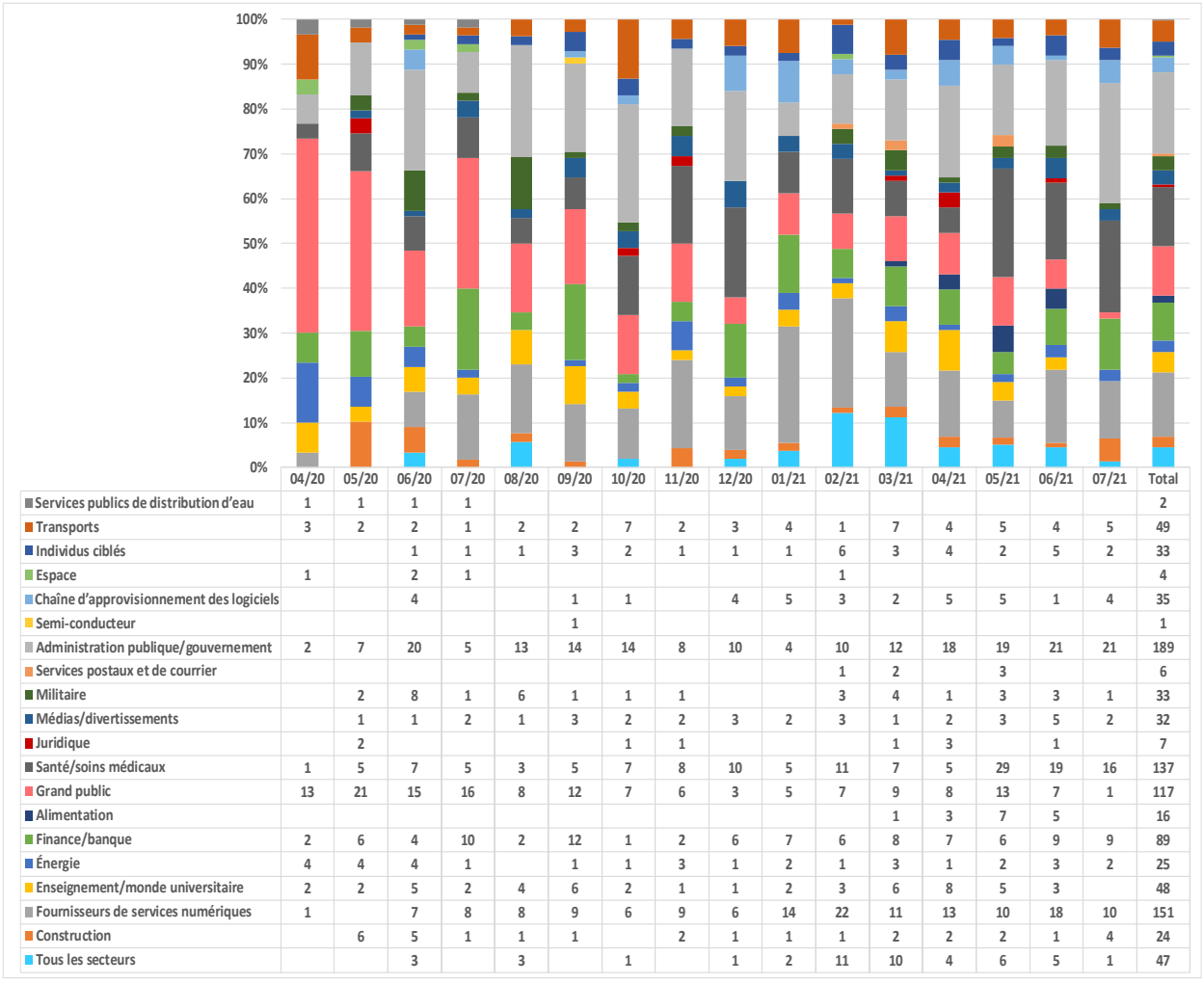
Les cybermenaces ne se limitent généralement pas à un secteur particulier et, dans la plupart des cas, en touchent plusieurs. Cela s'explique en effet par le fait que, dans de nombreux cas, les menaces se manifestent par l'exploitation de vulnérabilités des systèmes TIC sous-jacents qui sont utilisés dans divers secteurs. Toutefois, les attaques ciblées ainsi que les attaques exploitant les différences de maturité en matière de cybersécurité entre les secteurs et la popularité/l'importance de certains secteurs, sont autant de facteurs à prendre en considération. Ces facteurs favorisent la manifestation des menaces sous forme d'incidents dans des secteurs spécifiques, raison pour laquelle il faut examiner en profondeur les aspects sectoriels des incidents et menaces observés. En outre, les tendances constatées dans chaque secteur et les dépendances intersectorielles sont des observations qui peuvent être tirées d'une telle analyse.

Les figures 3 et 4 mettent en évidence les secteurs touchés concernant les incidents observés sur la base des renseignements d'origine sources ouvertes (ROSO) et résultent de travaux réalisés par l'ENISA dans le domaine de l'appréciation de la situation[9]. Elles font référence à des incidents liés aux principales menaces du rapport ETL 2021. Il s'agit de la première tentative de l'ENISA visant à cartographier l'incidence des menaces sur des secteurs spécifiques. Dans les années à venir et dans les futures versions du paysage des menaces, des

[9] Conformément à l'article 7, paragraphe 6, du règlement sur la cybersécurité de l'UE (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

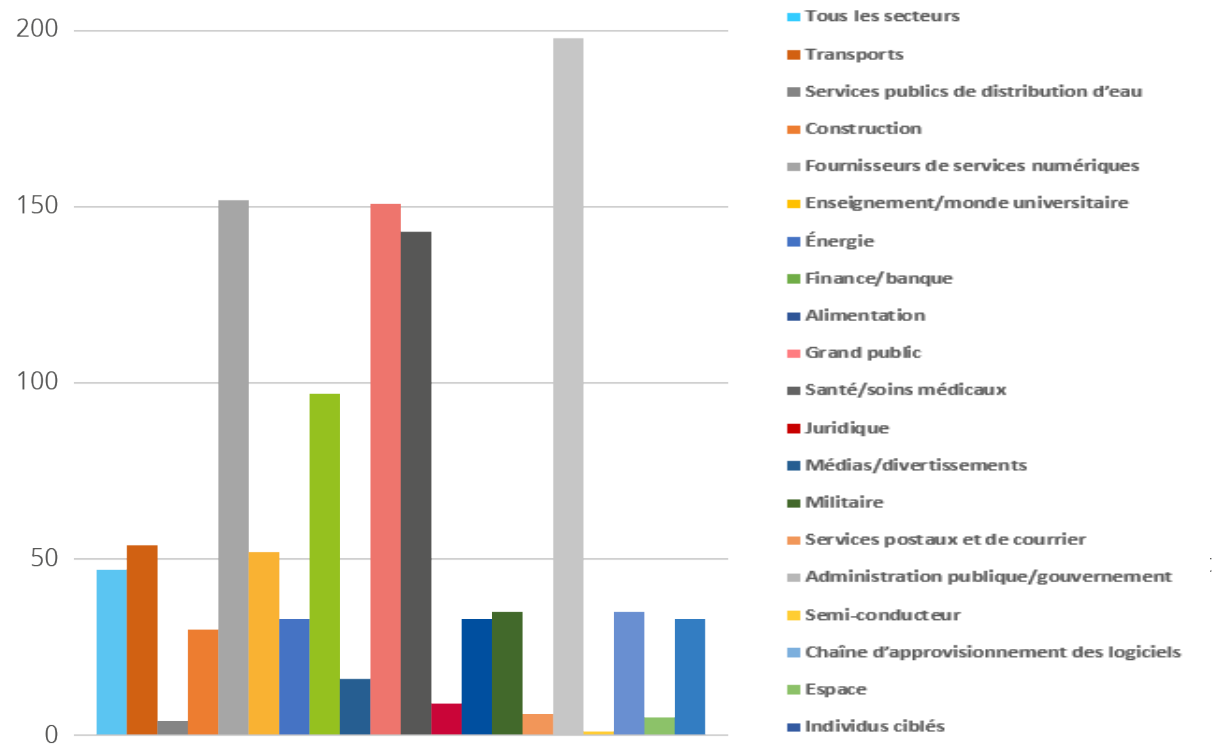
efforts seront déployés pour aligner les secteurs sur ceux énumérés dans la directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI) et dans la proposition de révision de cette dernière (directive SRI 2.0).

**Figure 3:** Chronologie des incidents observés liés aux principales menaces du rapport ETL du point de vue du secteur touché.




| | 04/20 | 05/20 | 06/20 | 07/20 | 08/20 | 09/20 | 10/20 | 11/20 | 12/20 | 01/21 | 02/21 | 03/21 | 04/21 | 05/21 | 06/21 | 07/21 | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Services publics de distribution d'eau | 1 | 1 | 1 | 1 | | | | | | | | | | | | | 2 |
| Transports | 3 | 2 | 2 | 1 | 2 | 2 | 7 | 2 | 3 | 4 | 1 | 7 | 4 | 5 | 4 | 5 | 49 |
| Individus ciblés | | | 1 | 1 | 1 | 3 | 2 | 1 | 1 | 1 | 6 | 3 | 4 | 2 | 5 | 2 | 33 |
| Espace | 1 | | 2 | 1 | | | | | | | 1 | | | | | | 4 |
| Chaîne d'approvisionnement des logiciels | | | 4 | | | 1 | 1 | | 4 | 5 | 3 | 2 | 5 | 5 | 1 | 4 | 35 |
| Semi-conducteur | | | | | | 1 | | | | | | | | | | | 1 |
| Administration publique/gouvernement | 2 | 7 | 20 | 5 | 13 | 14 | 14 | 8 | 10 | 4 | 10 | 12 | 18 | 19 | 21 | 21 | 189 |
| Services postaux et de courrier | | | | | | | | | | | 1 | 2 | | 3 | | | 6 |
| Militaire | | 2 | 8 | 1 | 6 | 1 | 1 | 1 | | | 3 | 4 | 1 | 3 | 3 | 1 | 33 |
| Médias/divertissements | | 1 | 1 | 2 | 1 | 3 | 2 | 2 | 3 | 2 | 3 | 1 | 2 | 3 | 5 | 2 | 32 |
| Juridique | | 2 | | | | | 1 | 1 | | | | 1 | 3 | | 1 | | 7 |
| Santé/soins médicaux | 1 | 5 | 7 | 5 | 3 | 5 | 7 | 8 | 10 | 5 | 11 | 7 | 5 | 29 | 19 | 16 | 137 |
| Grand public | 13 | 21 | 15 | 16 | 8 | 12 | 7 | 6 | 3 | 5 | 7 | 9 | 8 | 13 | 7 | 1 | 117 |
| Alimentation | | | | | | | | | | | | 1 | 3 | 7 | 5 | | 16 |
| Finance/banque | 2 | 6 | 4 | 10 | 2 | 12 | 1 | 2 | 6 | 7 | 6 | 8 | 7 | 6 | 9 | 9 | 89 |
| Énergie | 4 | 4 | 4 | 1 | | 1 | 1 | 3 | 1 | 2 | 1 | 3 | 1 | 2 | 3 | 2 | 25 |
| Enseignement/monde universitaire | 2 | 2 | 5 | 2 | 4 | 6 | 2 | 1 | 1 | 2 | 3 | 6 | 8 | 5 | 3 | | 48 |
| Fournisseurs de services numériques | 1 | | 7 | 8 | 8 | 9 | 6 | 9 | 6 | 14 | 22 | 11 | 13 | 10 | 18 | 10 | 151 |
| Construction | | 6 | 5 | 1 | 1 | 1 | | 2 | 1 | 1 | 1 | 2 | 2 | 2 | 1 | 4 | 24 |
| Tous les secteurs | | | 3 | | 3 | | 1 | | 1 | 2 | 11 | 10 | 4 | 6 | 5 | 1 | 47 |

**Figure 4:** Secteurs ciblés par nombre d'incidents (avril 2020 — juillet 2021)




Au cours de cette période de référence, un grand nombre d'incidents ont visé des administrations publiques et des gouvernements, ainsi que des fournisseurs de services numériques. Ce dernier secteur n'est pas surprenant compte tenu de sa fourniture horizontale des services et donc de son incidence sur de nombreux autres secteurs. Nous avons également observé un nombre significatif d'incidents visant des utilisateurs finaux et pas nécessairement un secteur particulier. Le secteur de la santé a également été ciblé de manière importante, et cette activité montre des signes d'augmentation au cours des derniers mois de la période de référence (mai — juillet 2021). Il est intéressant de noter que le secteur de la finance est confronté à un nombre constant d'incidents tout au long de l'année. La chaîne d'approvisionnement des logiciels montre également une augmentation du nombre d'incidents en 2021, observation figurant également dans le rapport de l'ENISA sur le paysage des menaces liées à la chaîne d'approvisionnement[10].

## 1.5. MÉTHODOLOGIE

Le rapport de l'ENISA sur le paysage des menaces de 2021 (rapport ETL 2021) repose sur des informations provenant de sources ouvertes, principalement de nature stratégique, et sur les capacités propres à l'ENISA en matière de renseignements sur les cybermenaces; il couvre plusieurs secteurs, technologies et contextes. Ce rapport se veut agnostique à l'égard de l'industrie et des fournisseurs; il fait référence ou cite les travaux de divers chercheurs en matière de sécurité, des blogs et des articles de presse relatifs à la sécurité, tous identifiés tout au long du texte par de nombreuses notes de bas de page. La période couverte par le rapport ETL 2021 s'étend d'avril 2020 à juillet 2021 et est appelée «période de référence» tout au long du rapport.

Pour la production du rapport ETL 2021, l'approche suivante a été utilisée. Tout au long de la période concernée, l'ENISA a dressé, au moyen d'une appréciation de la situation, une liste des incidents majeurs apparaissant dans des sources ouvertes. Cette liste a servi de base à l'identification de la liste des principales menaces, ainsi qu'à l'établissement de plusieurs tendances et statistiques figurant dans le rapport.

[10] *ENISA Threat Landscape for Supply Chain Attacks*, juillet 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Ensuite, l'ENISA et des experts externes ont procédé à une recherche documentaire approfondie de la littérature disponible provenant de sources ouvertes, comme des articles de presse, des opinions d'experts, des rapports de renseignements, des analyses d'incidents et des rapports techniques en matière de sécurité. Grâce à une analyse continue, l'ENISA a dégagé des tendances et des points d'intérêt pour chacune des menaces majeures présentées dans le rapport ETL 2021. Les conclusions et jugements clés de la présente évaluation reposent sur des ressources multiples et accessibles au public qui sont mentionnées dans les références utilisées pour l'élaboration du présent document.

Dans le rapport, nous essayons d'établir une distinction entre ce qui a été signalé par nos sources et ce qui ressort de notre évaluation. (Pour ce faire, nous utilisons spécifiquement l'expression «dans notre évaluation»). Enfin, lors d'une évaluation, nous exprimons la notion de probabilité par des mots évoquant une graduation de la probabilité (par exemple, probable, très probable, certainement)[11].

Le cadre MITRE ATT&CK®[12] a été utilisé dans le présent rapport pour mettre en évidence les tactiques et techniques d'attaque pertinentes pour une menace donnée (voir annexe A). Pour chaque tactique ATT&CK®, les techniques utilisées par l'adversaire sont présentées. Cela peut donner lieu à une liste d'atténuations ATT&CK[13] pouvant être appliquées. MITRE ATT&CK® est une base de connaissances, un langage commun pour les tactiques et techniques des adversaires fondées sur des observations en situation réelle. La base de connaissances MITRE ATT&CK® est utilisée comme base pour l'élaboration de modèles et de méthodologies de menace spécifiques dans le secteur privé, dans les administrations publiques et dans la communauté des produits et services de cybersécurité.

Le rapport a été validé par le groupe de travail ad hoc de l'ENISA sur les paysages des cybermenaces[14], mis sur pied en avril 2021 et composé d'experts issus d'entités de secteurs publics et privés européens et internationaux.

Pour le développement futur des paysages des menaces, l'ENISA est en train de formaliser une nouvelle méthodologie, afin de promouvoir la transparence et de jeter les bases pour permettre des processus structurés et harmonisés. À cette fin, parallèlement à une taxinomie révisée des menaces, la méthodologie pour les paysages des menaces sera rendue publique à l'avenir.

## 1.6. STRUCTURE DU RAPPORT

Le rapport de l'ENISA sur le paysage des menaces (ETL) de 2021 a maintenu une structure similaire à celle des précédents rapports ETL pour mettre en évidence les principales cybermenaces en 2021. Les lecteurs des précédentes versions remarqueront que les catégories des menaces ont été consolidées en fonction de l'évolution vers une nouvelle taxinomie des menaces pour la cybersécurité à utiliser à l'avenir.

Le rapport est structuré comme suit:

Le **chapitre 2** examine les tendances liées aux acteurs des menaces (à savoir, acteurs parrainés par des États, acteurs de la cybercriminalité, acteurs de services de piratage pour le compte d'autrui et hacktivistes).
Le **chapitre 3** examine les principaux incidents, constatations et tendances concernant les rançongiciels.
Le **chapitre 4** présente les principaux incidents, constatations et tendances concernant les logiciels malveillants.
Le **chapitre 5** décrit les principaux incidents, constatations et tendances en matière de cryptominage.
Le **chapitre 6** met en évidence les principaux incidents, constatations et tendances concernant les menaces liées au courrier électronique.
Le **chapitre 7** examine les principaux incidents, constatations et tendances concernant les données.
Le **chapitre 8** présente les principaux incidents, constatations et tendances concernant les menaces qui visent la disponibilité et l'intégrité.
Le **chapitre 9** souligne l'importance des menaces hybrides et décrit les principaux incidents, constatations et tendances en matière de désinformation et de mésinformation.

[11] CIA - *Words of Estimative Probability* https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK®, https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

Le **chapitre 10** traite des principaux incidents, constatations et tendances concernant les menaces non malveillantes.
L'**annexe A** présente les techniques couramment utilisées pour chaque menace, sur la base du cadre MITRE ATT&CK®.
L'**annexe B** inclut les incidents notables par menace, observés au cours de la période de référence.