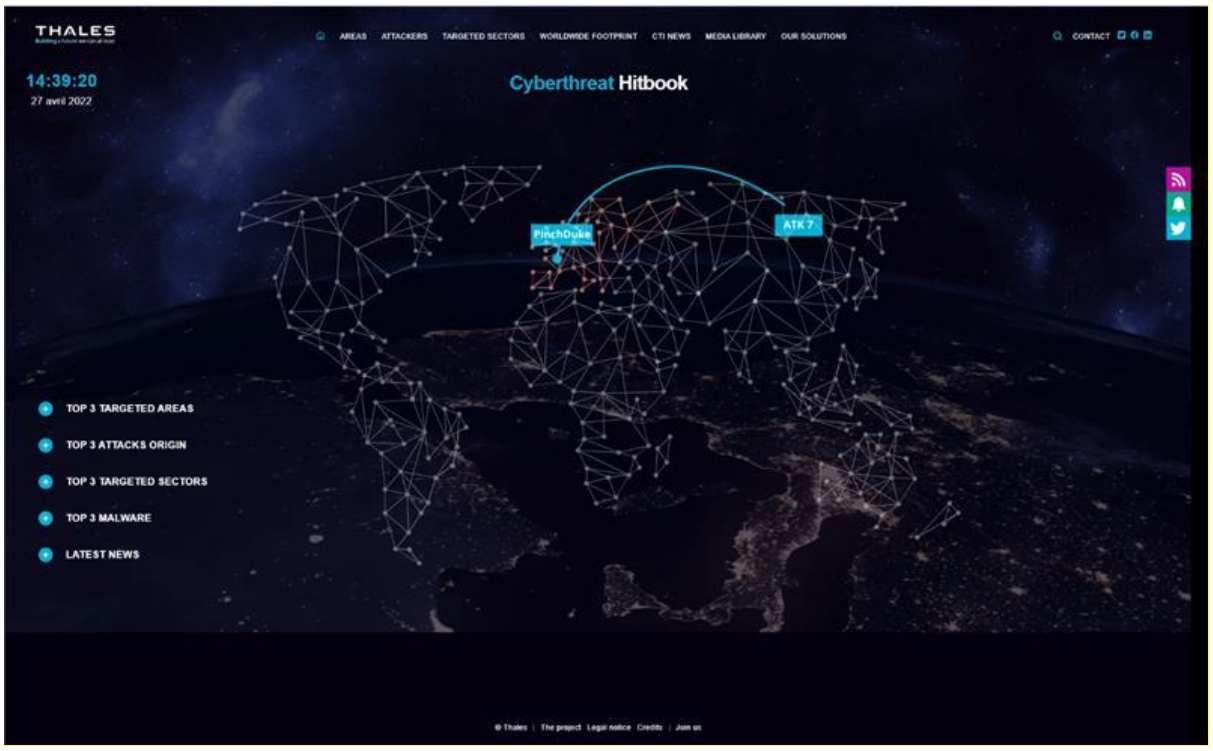
**COMMUNIQUÉ DE PRESSE**
31 Mai 2022
Paris La Défense

# Thales présente son Atlas des cyberattaquants 2022

## *Pour tout savoir de la nouvelle vague de menaces invisibles*

- La crise sanitaire a généré l'apparition de nouveaux vecteurs de cybermenaces, comme le recours accru au télétravail, l'augmentation des échanges à distance et la digitalisation de la majorité des secteurs d'activité. Les conséquences sont inédites : **une augmentation de 37,7% des attaques entre 2020 et 2021**, sur la zone Europe, selon l'ANSSI.
- Face à ce constat et pour lutter efficacement et collectivement contre cette menace, il est indispensable d'avoir **une bonne « hygiène cyber »** et d'**améliorer notre connaissance et compréhension des cyberattaques.**
- C'est l'ambition du centre d'analyse technique de la menace (CTI) de Thales. Il collecte, analyse, trie et met en corrélation les données relatives à chaque type de cyberattaque, à l'attaquant et à son mode opératoire, dans le but de détecter et lutter contre ces attaques.
- Dans le prolongement de ses missions, le CTI de Thales vient de lancer **sur Internet son Atlas des cyberattaquants 2022**, qui témoigne de l'importance des attaques et de l'organisation des groupes attaquants.




Thales publie aujourd'hui son **Atlas des cyberattaquants 2022 accessible sur Internet et mis constamment à jour, en direct.** Ces 5 dernières années, plus de 20 000 cyberattaques ont été analysées par les experts du CTI de Thales, sur 9 zones géographiques et dans 16 secteurs d'activité. Ces cyberattaques révèlent l'impressionnante capacité d'organisation des attaquants, des formes inédites de menaces installées sur le long terme et de nouveaux jeux de pouvoirs hybrides, entre les secteurs publics et privés.

- **Une professionnalisation des cyberattaquants de plus en plus importante**

Afin de faire face aux enjeux de développement et de rentabilité qu'ils rencontrent, **les groupes d'attaquants se sont progressivement organisés et structurés sur le même modèle que nos petites et moyennes entreprises**. Leurs nouvelles organisations regroupent notamment un département R&D, chargé de renforcer l'efficacité des cyberattaques et d'en développer de nouvelles toujours plus innovantes ; un département Ressources Humaines, qui gère le recrutement de nouveaux profils ou encore un département juridique, qui négocie avec les victimes les contreparties financières de « l'après-attaque ».

Selon l'Atlas, ce dernier département semble indispensable pour faire de cette cyberactivité une activité lucrative, comme le démontre **l'augmentation du nombre d'organisations qui acceptent de payer une rançon pour récupérer leurs données**. En 2021, 32% des organisations cyberattaquées ont payé une rançon aux attaquants, tandis qu'en 2020 elles étaient 26%. L'un des groupes d'attaquants a même extorqué 180 millions d'euros en une seule cyberattaque[1].

Cette recherche constante de rentabilité conduit ces attaquants à **adopter une stratégie coûts/bénéfices, en prospectant sur les industries et les pays les plus ouverts à la numérisation de leur modèle économique**. L'Atlas révèle que sur les 20 000 attaques analysées, 72% des cyberattaquants ont pris pour cible le secteur de la défense et des administrations et 62% le secteur de la communication ; tandis que 72% d'entre eux ont perpétré leurs attaques en Amérique du Nord et 66% en Europe.

- **Une progression des cyberattaques « dormantes » d'origine étatique**

Ces 5 dernières années, l'Atlas dévoile un accroissement des cyberattaques d'origine étatique, en raison notamment de l'augmentation du nombre d'attaques dites « dormantes ». **Les cyberattaquants installent un virus dans le système informatique d'une entité afin d'accéder aux informations de son réseau sans se faire détecte**r, favorisant la mise en place d'un espionnage sur le long terme, donc plus dangereux.

Pouvant opérer entre 2 ans et plus d'une décennie, ces attaques dormantes s'expliquent par l'évolution des liens toujours étroits entre les entreprises privées et les Etats face aux cybermenaces et la professionnalisation des cyberattaquants. **Aujourd'hui, de plus en plus d'Etats tendent à externaliser leur activité cyber en ayant recours à des organisations de cyberattaquants**.

*« Le travail approfondi réalisé par Thales de connaissance du profil des attaquants, de leurs modes opératoires dans certaines régions et sur des secteurs spécifiques offre aujourd'hui la possibilité de se préparer à la menace. Cette cartographie est d'autant plus essentielle que dans certaines zones géographiques, telles que l'Afrique, les incidents dans leur grande majorité ne sont pas rapportés. Cette invisibilité du risque est une inquiétude majeure, alors*

[1] [Source: https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/?cmp=30726]

*même que la digitalisation croissante du continent a progressé au point de compter presque autant d'utilisateurs de services numériques qu'en Europe, soit 601 millions d'utilisateurs ! Des territoires entiers restent encore à explorer. L'ambition de l'Atlas des cyberattaquants 2022 est de rendre le maximum d'informations accessibles au plus grand nombre pour apporter une solution mondiale. »* précise **Ivan Fontarensky, Directeur technique cyberdéfense, Thales.**

- **Thales et la cybersécurité**

Thales sert 130 grands clients dans le monde, des gouvernements, opérateurs d'importance vitale et administrations. Le Groupe sécurise les systèmes critiques de 19 des 20 plus grandes banques mondiales, de 9 des 10 géants mondiaux de l'internet mais aussi plusieurs milliers d'entreprises.

Le Groupe dispose de trois grandes familles de produits :

- **Un portefeuille complet de services,** Cybels, adressant les besoins d'évaluation des risques, d'entraînement et de simulation, de détection et de réponse aux attaques ;
- **Des produits dits de souveraineté** comprenant le chiffrement et les sondes pour protéger les systèmes d'information critiques ;
- **Une plateforme de protection des données,** de sécurité du cloud et de gestion d'accès.

**Pour en savoir plus, une page internet dédiée au Thales Media Day est mise à jour régulièrement. A l'issue du Thales Media Day, les enregistrements de la plénière d'ouverture, des tables rondes et du discours de clôture seront accessibles.**

**L'Atlas des cyberattaquants est disponible sur ce lien.**

## À propos de Thales

Thales (Euronext Paris: HO) est un leader mondial des hautes technologies qui investit dans les innovations du numérique et de la « deep tech » – connectivité, big data, intelligence artificielle, cybersécurité et quantique – pour construire un avenir de confiance, essentiel au développement de nos sociétés. Le Groupe propose des solutions, services et produits qui aident ses clients – entreprises, organisations, Etats - dans les domaines de la défense, de l'aéronautique, de l'espace, du transport et de l'identité et sécurité numériques, à remplir leurs missions critiques en plaçant l'humain au cœur des décisions.

Thales compte 81 000 collaborateurs dans 68 pays. En 2021, le Groupe a réalisé un chiffre d'affaires de 16,2 milliards d'euros.

**CONTACTS PRESSE**

**Thales, Relations médias**
**Chrystelle Dugimont**

**EN SAVOIR PLUS**

Groupe Thales
Sécurité

**COMMUNIQUÉ DE PRESSE**
31 Mai 2022
Paris La Défense

Chystelle.dugimont@thalesgroup.com

**Anne-Sophie Malot**
Anne-sophie.malot@thalesgroup.com

**Marion Bonnet**
marion.bonnet@thalesgroup.com

@Thalesgroup