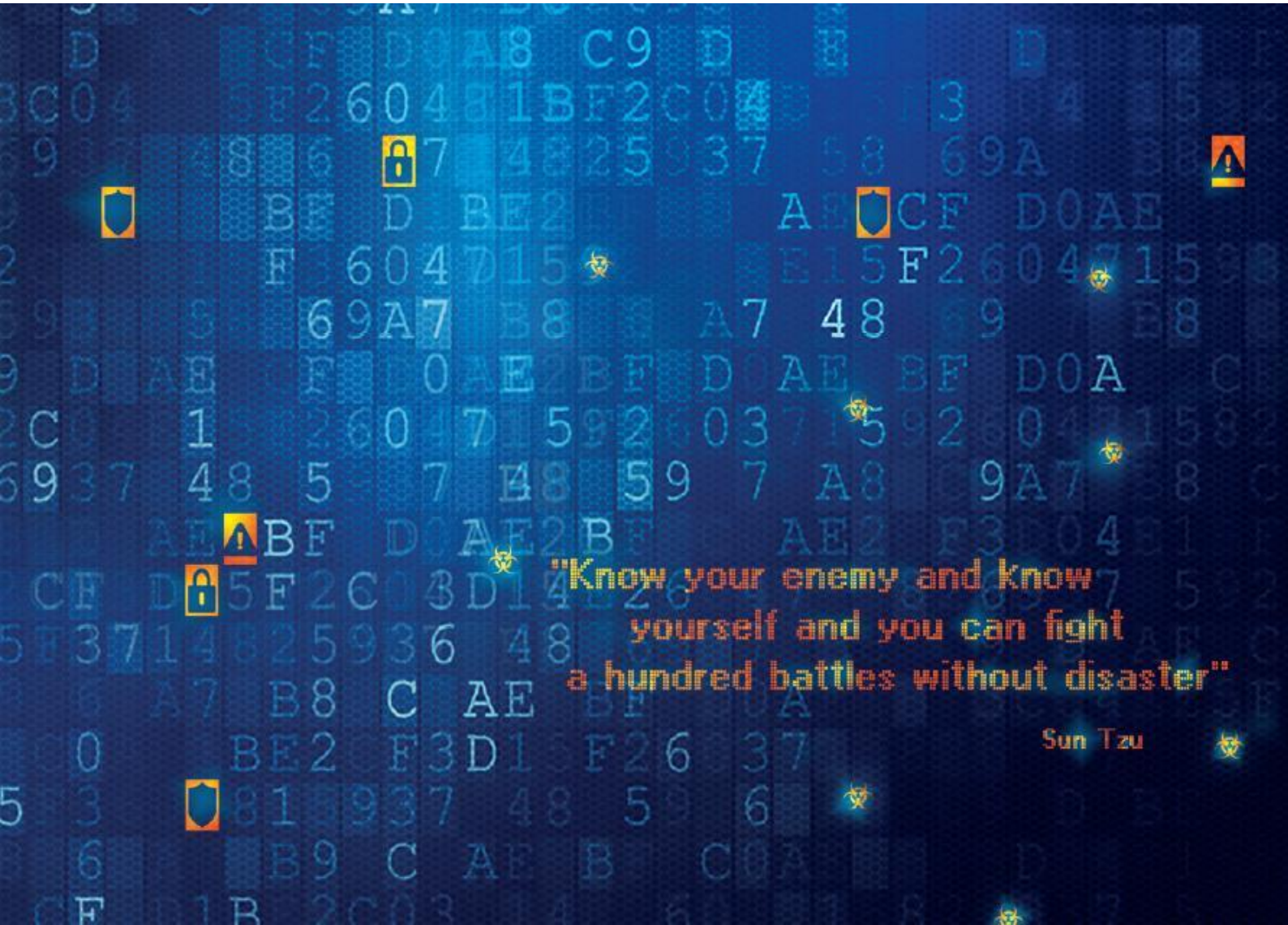
THALES

# Dossier de presse

## *The CyberThreat Handbook*

## Thales - Verint

*Le “Who’s who” des cyberattaquants*



# 1. A propos de Thales

Thales (Euronext Paris : HO) est un **leader mondial de hautes technologies** qui façonne aujourd'hui le monde de demain. Le Groupe propose des solutions, services et produits à ses clients dans les domaines de l'aéronautique, de l'espace, du transport, de l'identité et sécurité numériques, et de la défense. Avec **80 000 collaborateurs dans 68 pays**, Thales a réalisé un chiffre d'affaires de 19 milliards d'euros en 2018 (sur une base pro forma intégrant Gemalto).

Thales investit notamment dans les innovations numériques - **connectivité, *big data*, intelligence artificielle et cybersécurité** – technologies au cœur des moments décisifs des entreprises, des organisations et des Etats.


Dans un monde en constante mutation et de plus en plus connecté, Thales est aux côtés de ceux qui ont de grandes ambitions : mettre le numérique au service d'un monde meilleur et plus sûr. Afin que nous puissions bénéficier des nouvelles technologies en toute confiance, **Thales accompagne et sécurise la transformation des systèmes d'information les plus critiques et protège tout le cycle de vie de la donnée, de sa création à son exploitation.**

Nos 5000 spécialistes en informatique critique et en cybersécurité conçoivent un éventail unique de solutions technologiques d'exception qui répondent aux exigences les plus poussées de nos clients - Etats, administrations, grandes entreprises, opérateurs d'importance vitale. Plus de 50 pays et de nombreuses grandes entreprises traitant de processus métier critiques et de données sensibles font confiance à Thales, leader européen de la cybersécurité et leader mondial de la protection des données, pour assurer leur transformation digitale.

# 2. Le service d'analyse technique des cyber-menaces de Thales

**« Connaissez votre ennemi et connaissez-vous vous-même et vous pourrez mener cent batailles »**, selon Sun Tzu's, dont la couverture figure en couverture du rapport. On ne peut pas combattre efficacement son ennemi si on ne connaît pas ses motivations, ses moyens financiers et techniques, ses techniques d'attaque, etc.

Or dans le domaine des cybermenaces, connaître son ennemi peut s'avérer extrêmement complexe :

- Par nature, nombre de cyberattaquants ont **une volonté claire de dissimulation** ;
- Les cyberattaques sont extrêmement **diversifiées**, certaines visant des secteurs, des zones géographiques ou des organisations de manière plus ou moins précises, avec des motivations très différentes et une « performance » variable en fonction des groupes d'attaquants.

## - *L'analyse technique des cybermenaces : de quoi s'agit-il ?*

Le service de renseignements sur les cyberattaques de Thales collecte, analyse, trie et met en corrélation les données relatives à chaque type de cyberattaque, à l'attaquant et à son mode de fonctionnement.

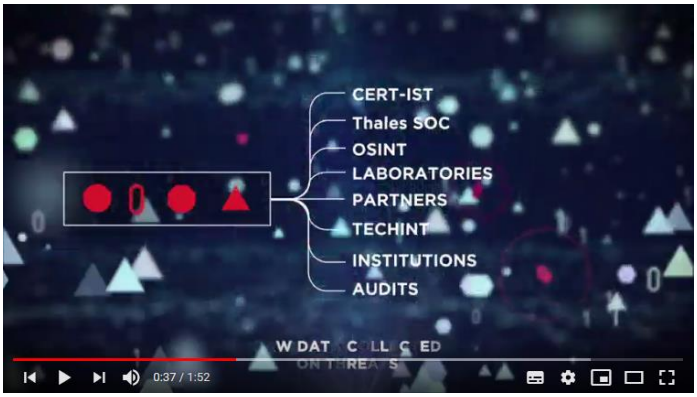
C'est l'ambition de l'analyse technique des cybermenaces : **analyser et comprendre les cybermenaces pour mieux s'en protéger et mieux les détecter**. LA finalité de cette analyse de la menace est l'interconnexion avec les outils de détection des cyberattaques (comme la sonde et le SOC). Il s'agit d'analyse les menaces afin d'adapter en permanence la pertinence des règles de détection.

Le service d'analyse technique des cybermenaces est basé sur des données qui sont récoltées grâce à un **large nombre de sources** qu'elles soient humaines, publique, privées, techniques ou non. Cette approche multi-source repose également sur des **coopérations internationales** (avec des sociétés comme Verint ou ESET par exemple), qui permettent d'élargir le nombre de sources, et d'apporter une réponse globale à des cybermenaces par nature internationales.

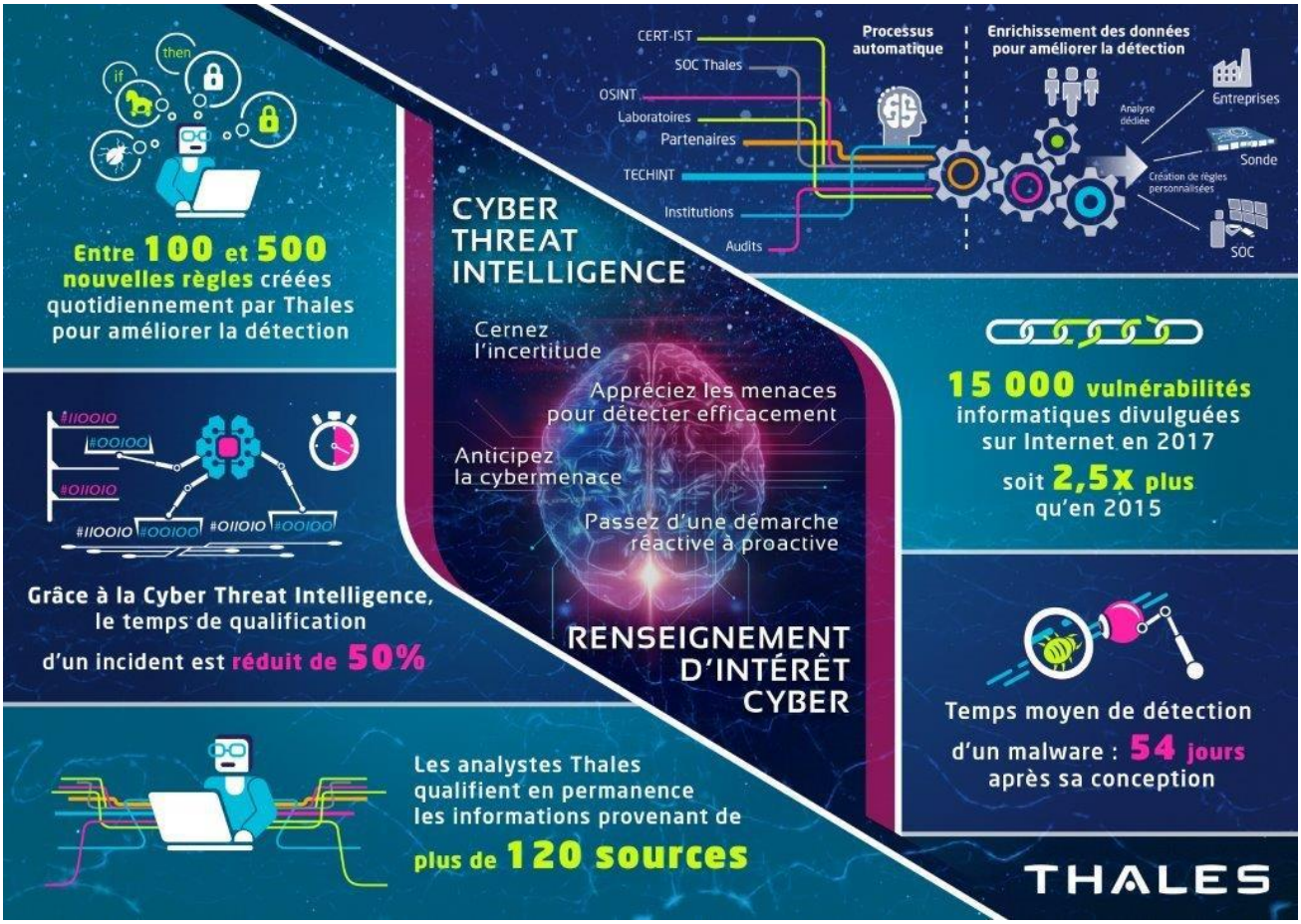
À cet effet, les analystes travaillent continuellement à **la collecte, au traitement et à l'analyse de données**. Ils analysent également les logiciels malveillants afin de **développer des rapports sur le comportement des hackers et de fournir des informations pertinentes aux clients attaqués**. Le service possède une base de données qui répertorie les attaques, les méthodes et techniques utilisées par les cyberattaquants pour infiltrer un système. Le service se concentre donc sur les questions suivantes: qui attaque qui ? Quand et avec quelle technique ? Quelles sont les motivations des attaquants ?

En partageant leurs analyses des comportements des cyber-criminels et de leurs modes opératoires, les équipes de Thales améliorent leurs connaissances des cybermenaces, ce qui

permet de renforcer les capacités de détection, d'anticiper les nouveaux risques et de mieux lutter, collectivement, contre les cyberattaques.




Découvrez comment fonctionne le service d'analyse des cybermenaces dans la video suivante:
https://www.youtube.com/watch?v=AALLwKz1GyU&list=PLypm7oU4utZVyK3tWuEhEYLjBfQ5Fck9w&index=31




- ***Le quotidien des analystes de Thales***

Le service d'analyse technique des cybermenaces est divisé en trois bureaux : le Bureau des analyses techniques, le Bureau du contexte stratégique et le Bureau Automatisation & Delivery. Le bureau d'analyse technique mène des enquêtes sur les campagnes de cyberattaques, en examinant les événements rapportés par diverses sources et par les équipes du centre de

cybersécurité. Le rôle du Bureau du contexte stratégique est de fournir des informations sur une attaque afin de la rendre compréhensible pour le client concerné, en établissant des liens entre les attaques et les événements qui peuvent les avoir déclenchées (événements financiers, politiques, sociaux, etc.). Enfin, le Bureau Automatisation et Delivery met à la disposition du client des ressources de type Big Data.


Vous désirez en savoir davantage? Découvrez le quotidien de nos experts, Quentin, Nicolas and Romain :

> ***Episode 1***: Quentin, à propos du bureau des analyses techniques

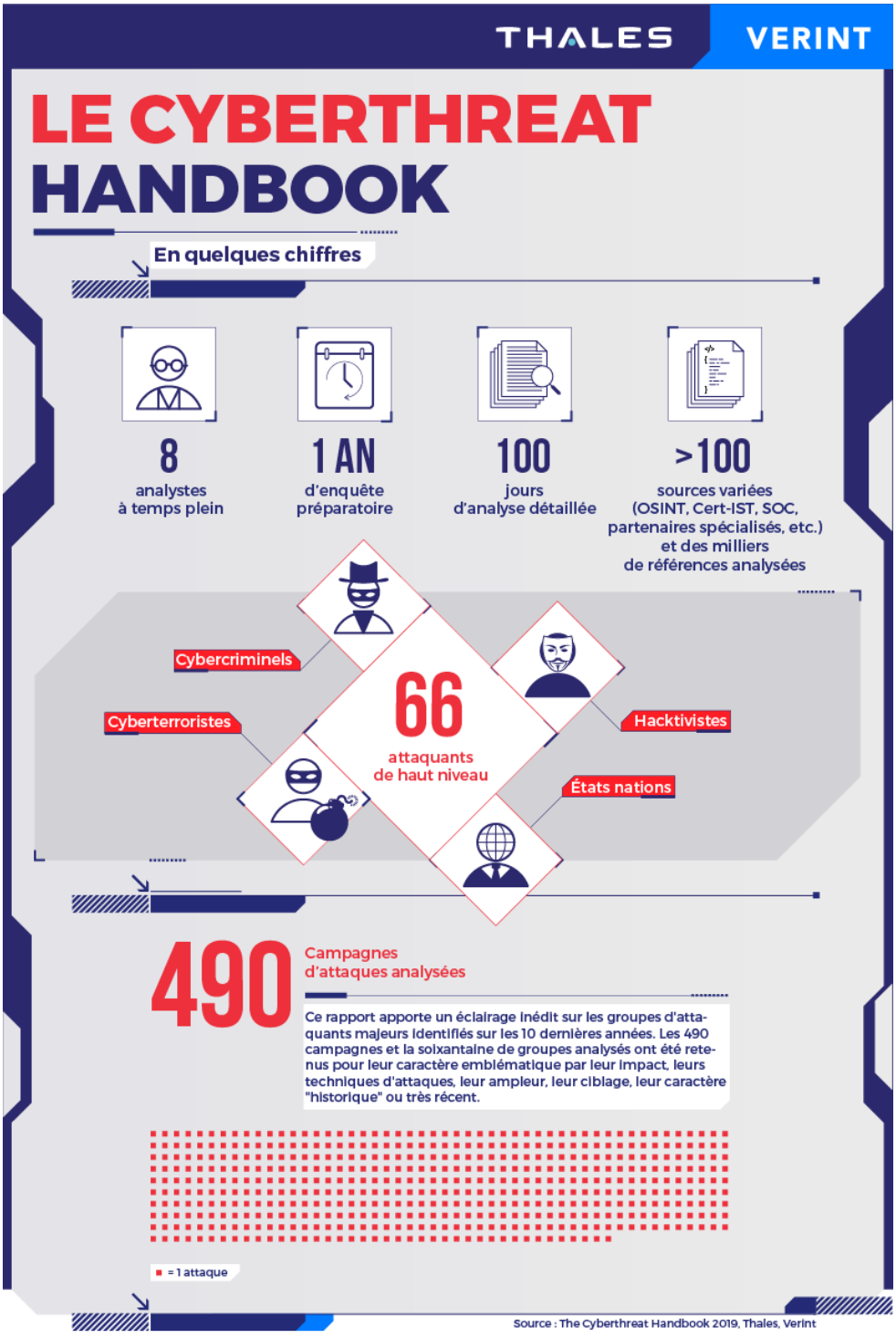
> ***Episode 2***: Nicolas, à propos du bureau du contexte stratégique

> ***Episode 3***: Romain, à propos du bureau Automatisation et Delivery

# 3. Le Cyberthreat Handbook de Thales et Verint

## - *Un rapport à l'ampleur inégalée*

Le Cyberthreat Handbook est le premier rapport de ce genre dans le monde au regard de la qualité de son contenu. Il s'appuie sur des informations collectées, recoupées et analysées pendant plusieurs milliers d'heures par nos équipes d'experts, qui ont étudié en profondeur les motivations et les techniques des attaquants sur une longue durée.



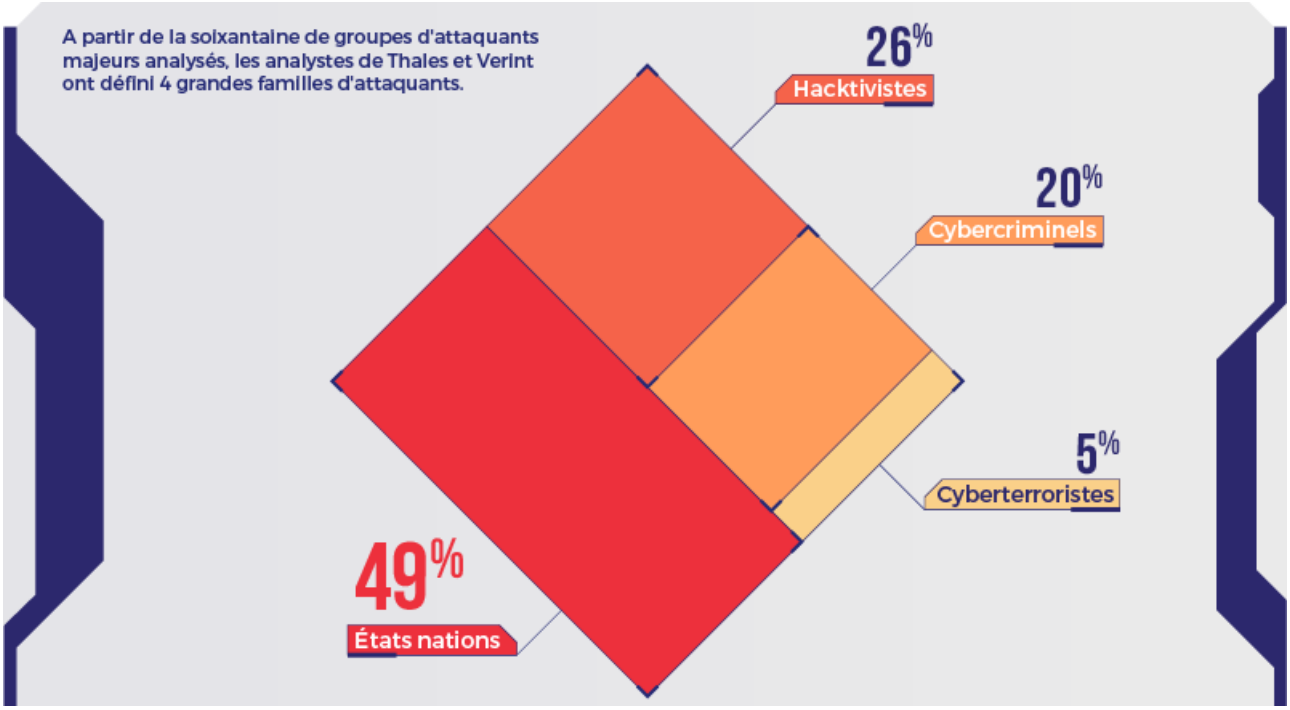
## - *Principales conclusions: Les 4 grandes familles de cyberattaquants*

Les analystes de Thales et Verint ont défini quatre grandes familles d'attaquants à partir de leurs motivations et de leur objectif final. Sur la soixantaine de groupes d'attaquants majeurs analysés :

- 49% des groupes d'attaquants sont parrainés par des Etats, qui se concentrent souvent sur du vol de données sensibles de cibles géopolitiques. Cette proportion importante s'explique en grande partie par les importantes ressources financières et humaines dont disposent ces attaquants, qui rendent leur action particulièrement significative
  .
- Les cyberactivistes (26%) poursuivent, quant à eux, des motivations idéologiques et dénoncent des faits qu'ils jugent inacceptables en portant atteinte à l'image de leurs cibles.

- Ils sont suivis de près par les cybercriminels (20%) dont l'appât du gain les pousse à cibler principalement le secteur de la finance et du commerce.

- Enfin, les cyberterroristes, qui représentent 5% des groupes analysés mènent le plus souvent des actions de propagande pour recruter de nouveaux adeptes soit pour détruire les données de leurs victimes.



## Quatre profils distincts

### ÉTATS NATIONS

Moyens financiers

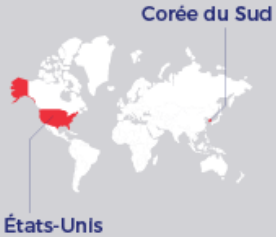

**Motivations**

- Cyberespionnage
- Déstabilisation politique
- Sabotage

**Secteurs les plus impactés**

- Défense
- Gouvernement

**Zones géographiques les plus touchées**




**Principales méthodes d'attaques**

- « Backdoors » (portes dérobées)

### HACKTIVISTES

Moyens financiers


**Motivations**

- Idéologiques (communautaires, religieuses, politiques, etc.)
- Dénonciation de faits jugés inacceptables
- Atteinte à l'image

**Secteurs les plus impactés**

- Gouvernement
- Éducation

**Zones géographiques les plus touchées**


**Principales méthodes d'attaques**

- Défiguration de sites web
- Attaque en déni de service

### CYBERCRIMINELS

Moyens financiers

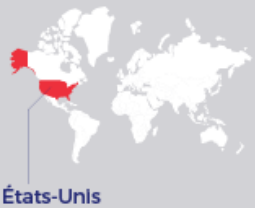

**Motivations**

- Gain financier

**Secteurs les plus impactés**

- Finance
- Commerce et distribution

**Zones géographiques les plus touchées**




**Principales méthodes d'attaques**

- Rançongiciel
- Cheval de Troie bancaire

### TERRORISTES

Moyens financiers


**Motivations**

- Prosélytisme
- Destruction de données

**Secteurs les plus impactés**

- Défense
- Gouvernement
- Médias

**Zones géographiques les plus touchées**


**Principales méthodes d'attaques**

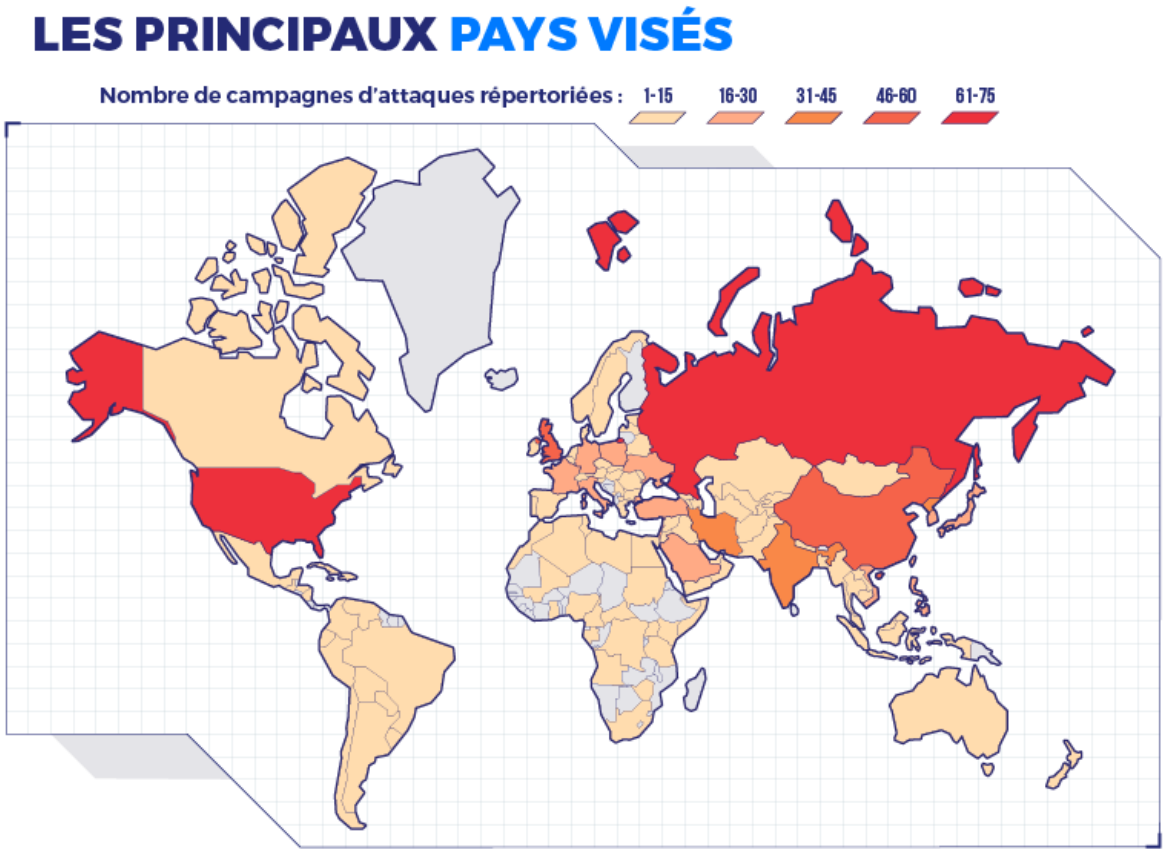
- Défiguration de site web
- Destruction numérique (wiper)

## - *Les pays et zones géographiques les plus visées*

Ces cybermenaces sont globales et la quasi-totalité des pays du monde sont visés, néanmoins à des degrés divers. Si certaines attaques peuvent cibler très précisément un Etat en particulier, il n'est pas toujours possible d'identifier avec précision le ciblage de certaines attaques, qui vont concerner des zones géographiques entières, ce qui explique les deux cartes ci-dessous.

Deux tendances se dégagent :

- Toutes les grandes puissances économiques, politiques et militaires mondiales sont particulièrement visées par des attaques. Ainsi, les 12 pays au PIB le plus élevés figurent tous parmi les Etats les plus visés, au premiers rang desquels les Etats-Unis, la Russie, l'Union Européenne (en particulier le Royaume-Uni, la France et l'Allemagne), la Chine, puis l'Inde, la Corée du Sud et le Japon, qui sont les zones géographiques mondiales les plus ciblées par les cyberattaquants. A l'inverse, les pays d'Afrique sont relativement peu touchés par des cyberattaques de grande ampleur.
- Au-delà du rayonnement mondial des Etats, le classement des pays les plus attaqués est également le reflet de tensions géopolitiques ou économiques régionales, en particulier sur 4 zones spécifiques :
    - La Corée du Nord et la Corée du Sud,
    - L'Europe de l'Est (Ukraine, Pologne) et la Turquie
    - L'Asie du Sud-Est
    - Le Proche-Orient et le Moyen-Orient, avec par exemple l'Iran, Israël ou l'Arabie Saoudite



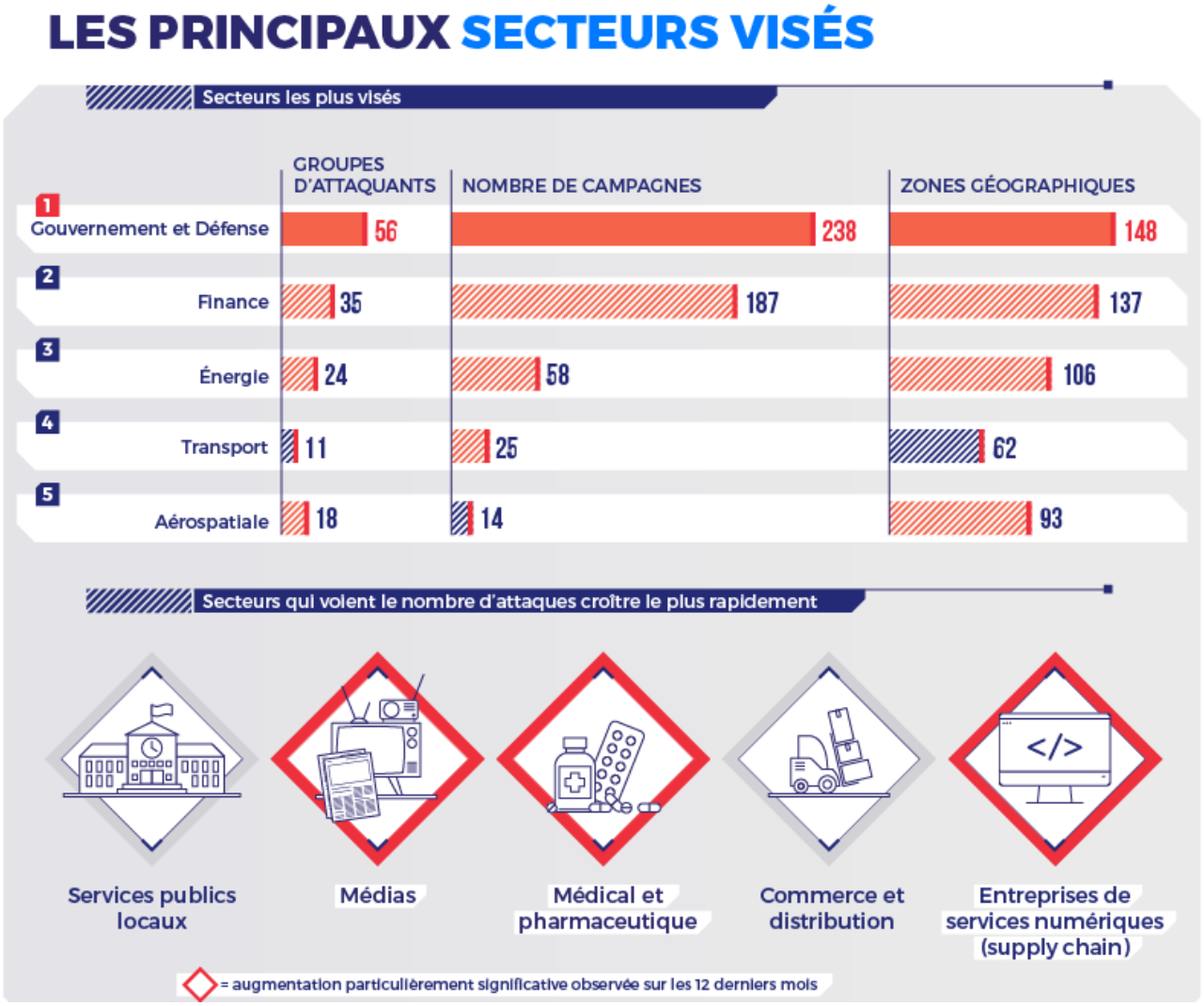

La quasi-totalité des pays du monde sont visés par des campagnes de cyberattaques majeures, à des degrés divers. Si les cyberattaquants peuvent viser très précisément un Etat en particulier, il n'est pas toujours possible d'identifier le ciblage de certaines attaques, qui vont concerner des zones géographiques entières, au premiers rangs desquelles l'Amérique du Nord (les Etats-Unis en particulier), le Moyen-Orient, l'Europe, l'Asie de l'Est et du Sud-est.

## - *Les secteurs les plus visés*

Il n'est pas étonnant de constater que les adversaires qui disposent du plus de moyens, techniques, financiers ou humains, ont pour cible principale les Etats, leurs capacités de défense et l'ensemble des grands acteurs intervenants dans ce secteur. Ces attaquants, pour la plupart eux-mêmes sponsorisés par des Etats, mènent des attaques ciblées, visant très précisément un Etat ou une entreprise importante à sa souveraineté.

La finance est le deuxième domaine le plus touché par les cyberattaquants, essentiellement attirés par l'appât du gain. Par conséquent, leurs offensives sont globales et visent l'ensemble des acteurs du système financier à l'échelle mondiale : 137 zones géographiques différentes ont ainsi été ciblées par les groupes d'attaquants intervenus dans ce secteur.

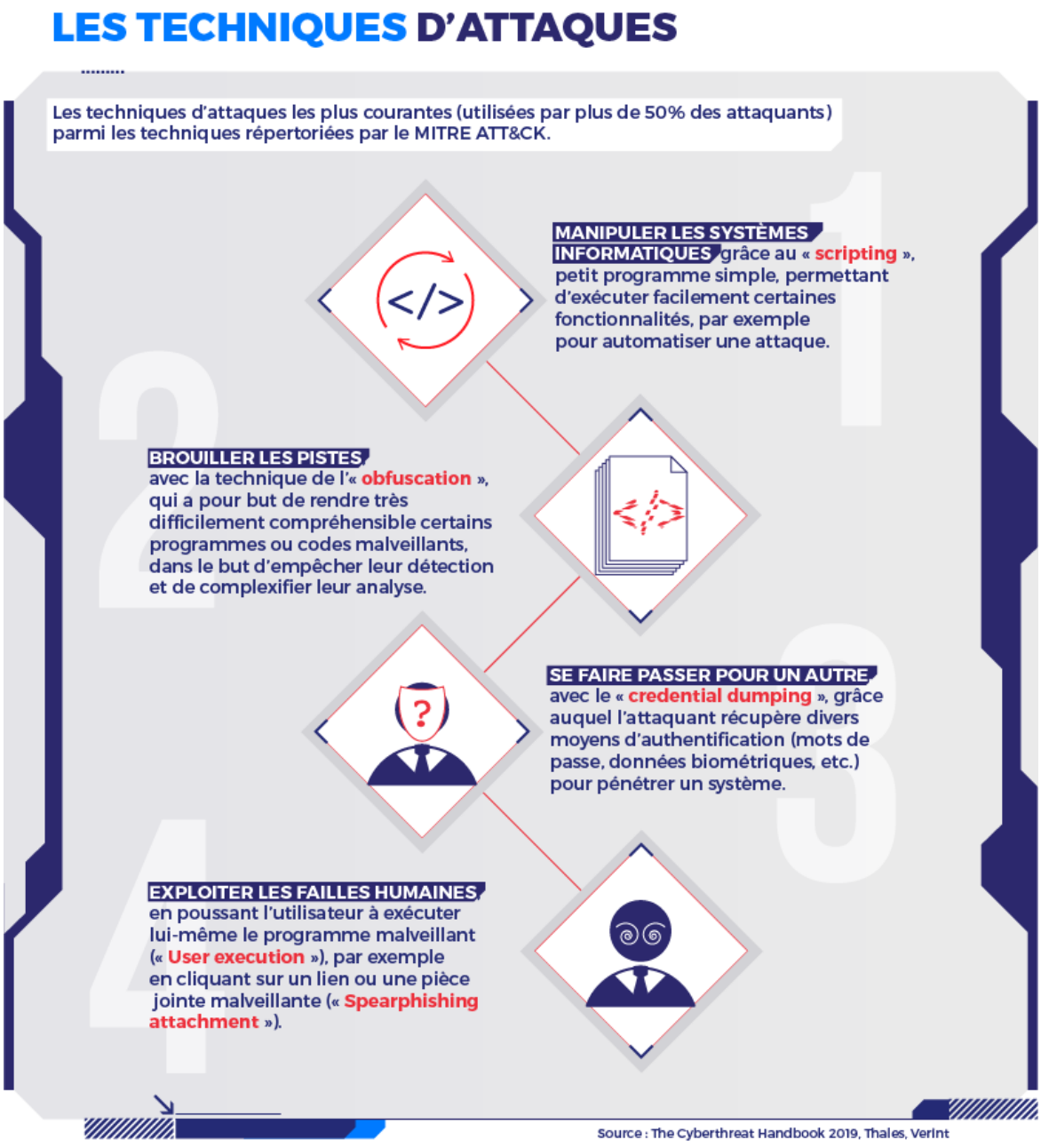
L'énergie fait également l'objet de nombreuses attaques – 24 attaquants ont touché 106 pays – qui sont également très diversifiées – plus de 230 familles de malwares ont été répertoriées pour ce seul secteur.



## - *Les techniques et modes opératoires des hackers*

Malgré de nombreuses campagnes de sensibilisation, la technique du phishing (le hameçonnage) reste encore largement employée par les cyberattaquants, en particulier dans des versions sophistiquées (spear phishing), via des mails qui visent spécifiquement des personnes ciblées. Ces attaques revêtent un haut caractère de personnalisation – l'attaquant s'étant préalablement renseigné sur la personne visée pour tirer la maximum d'informations personnelles la concernant, afin qu'elle n'identifie pas le message reçu comme un spam.

On peut également mentionner parmi les techniques d'attaques les plus utilisées, celle de « l'obfuscation », qui a pour but de rendre très difficilement compréhensible certains programmes ou codes malveillants, que les pirates utilisent comme méthode de dissimulation, en encore le « credential dumping », grâce auquel l'attaquant récupère divers moyens d'authentification (mots de passe, données biométriques, etc.) pour pénétrer un système.



On constate par ailleurs un changement dans les types de malwares utilisés :

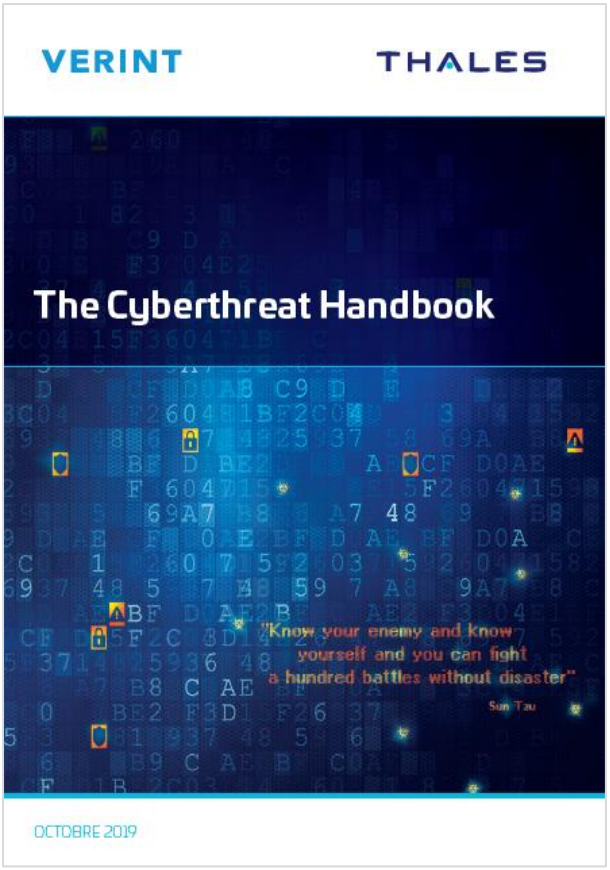
- Les attaquants se concentrent sur l'utilisation de certains types de malware, comme les malwares visant les objets connectés, les ransomwares ou rançongiciels qui cryptent les données en échange d'une rançon ;

- L'apparition d'un « supermarché du malware » (malwares as a service). qui permet aux cyberpirates d'acheter et d'utiliser des logiciels malveillants développés par d'autres groupes d'attaquants, qui s'en font une spécialité. De plus en plus utilisée, cette pratique permet un gain de temps considérable pour les groupes qui n'ont plus à développer leur malwares. Cela rend par ailleurs la tâche des analystes plus complexe puisque les groupes d'attaquants ne se caractérisent plus nécessairement par le malware utilisé.

## - *Le point de vigilance de Thales pour l'avenir : la supply chain*

La caractéristique principale commune à l'ensemble des groupes d'attaquants est leur ingéniosité, ils cherchent à se renouveler constamment et tentent de contourner les solutions de cyberprotection mises en place par les entreprises, les organisations et les administrations. De plus en plus de groupes d'attaquants se concentrent désormais sur les failles des prestataires, partenaires et fournisseurs, souvent de plus petite taille, qui n'ont pas accès à toutes les ressources humaines et financières pour investir significativement dans la protection de leurs cyberespaces. Utilisés comme de véritables Chevaux de Troie, ils constituent aujourd'hui une véritable cible pour les hackers, qui les utilisent comme porte d'entrée vers de plus gros fournisseurs.

## - *Executive summary et méthodologie*




Réalisé par Thales et Verint, le *Cyberthreat Handbook* est un document original qui propose une analyse environnementale du paysage des cybermenaces. Ce répertoire dynamique vise, dans sa première édition, à fournir une analyse rigoureuse et synthétique de 66 groupes d'attaquants d'envergure mondiale. Nulle prétention d'exhaustivité. Il s'agit plutôt de présenter les cybermenaces en s'appuyant sur des sources libres que Thales et Verint estiment fiables.

Ensemble de cartes d'évaluation spécifiques, le rapport familiarise le lecteur avec des groupes aux profils différents. Y figurent des auteurs de cyberattaques soutenus par des États-nations, des groupes cybercriminels de haut vol, des groupes d'hacktivistes et des cyberterroristes. Ce panorama montre la grande diversité de la menace, tant sur le plan technique, au vu des multiples *modus operandi*, qu'en termes de performance, certains faisant preuve d'une sophistication extrême, comme le groupe ATK91 (Xenotime, Triton, TEMP.Veles), capable d'infiltrer et de manipuler, avec son logiciel

malveillant, Triton des infrastructures critiques et des systèmes de sécurité et de contrôle dans l'industrie.

Plusieurs critères ont été retenus pour définir ce qui fait selon nous l'importance des menaces. Certains groupes nous ont paru pertinents en raison des résultats ou du caractère récent de leurs actions. Ainsi, ayant découvert ATK120 (Lyceum/Hexane) fin août 2019 après son entrée sensationnelle dans le paysage des cybermenaces, nous l'avons intégré à nos travaux. D'autres sont inactifs depuis plusieurs années, mais leur statut d'APT (Advanced Persistent Threats), qui caractérise les groupes soutenus par des États-nations et leurs campagnes passées, nous incite à les considérer comme faisant toujours partie intégrante du paysage. De même, impossible d'ignorer le groupe ATK2 (APT17) par exemple, dont les campagnes ont perdu en intensité depuis 2014, dans la mesure où la dernière avait compromis les sites Internet du Groupement des industries françaises aéronautiques et spatiales (GIFAS) ainsi que les systèmes de certains de ses membres. Plus généralement, nous avons sélectionné les groupes en fonction de leurs capacités de nuisance et/ou de destruction, de la difficulté à les détecter, de leur agilité et de leurs motivations (ou de motivations supérieures). Il serait illusoire d'espérer cartographier tous les groupes d'attaquants connus. D'abord parce qu'ils sont très nombreux, ensuite parce que les modes d'attaque sont parfois reproduits presque à l'identique d'un groupe à l'autre. Citons notamment la backdoor IceFog du groupe chinois du même nom, largement diffusée et utilisée par d'autres groupes d'origine chinoise. Aussi efficace que soit ce programme, sa simple utilisation passée ne suffit pas à justifier d'inclure ici tous les groupes susceptibles d'y recourir à nouveau. Par sa nature même, le paysage des cybermenaces est très complexe à étudier : de nombreux pirates informatiques opèrent dans l'ombre, avec la volonté très nette de se dissimuler.

Les groupes décrits dans ce rapport ont en commun d'être des attaquants d'envergure, que ce soit par le nombre de campagnes menées, par leurs compétences technologiques, par l'agilité de leurs modes opératoires et par leur détermination. En somme, tous sont des adversaires résolus, capables d'attaques majeures. Comme l'indique notre système de notation, spécialement créé aux fins de ce rapport, leur niveau de « performance » est variable. Nous décrivons brièvement chacun de ces attaquants. Nous donnons leurs noms à partir de plusieurs sources et précisons leur nature (soutenu par un État, criminel, hacktiviste ou terroriste), leurs cibles connues (secteurs d'activité et zones géographiques), le langage utilisé, et leurs origines, motivations et objectifs supposés. Nous replaçons également en contexte l'activité de certains groupes à la lumière d'évènements internationaux intervenus durant leurs campagnes. Ces mêmes campagnes sont en outre détaillées, illustrations à l'appui, sur la chronologie qui accompagne chaque carte d'évaluation pour retracer les activités connues. Chaque carte indique le logiciel malveillant utilisé, qu'il soit spécifique au groupe d'attaquants en question ou utilisé par d'autres, les outils légitimes utilisés et les vulnérabilités exploitées. Enfin, nous avons disséqué le *modus operandi* habituel de l'attaquant, en expliquant ses tactiques, techniques et procédures à partir de la matrice élaborée par MITRE ATT&CK. Dans le même ordre d'idées, l'objectif est de savoir identifier formellement un groupe dès l'attaque, grâce à une connaissance aiguë de ses habitudes.

**L**e *Cyberthreat Handbook* rassemble ainsi des analyses sur près de 490 campagnes offensives menées dans une quarantaine de secteurs d'activité et 39 pays par 66 attaquants de nature diverse (49 % soutenus par un État, 26 % d'hacktivistes, 20 % de cybercriminels et 5 % de terroristes). Le plus souvent, les groupes soutenus par un État cherchent à voler des données sensibles auprès de cibles géopolitiques et/ou de fournisseurs d'infrastructures critiques, en général en déployant des techniques backdoor. Animés par des motivations idéologiques (communautaires, religieuses, politiques, etc.), les hacktivistes dénoncent des faits qu'ils jugent inacceptables en organisant des attaques DDoS, ou bien en faisant du prosélytisme ou de la désinformation par dégradation. Les cybercriminels sont des groupes en quête de profits financiers colossaux, par exemple avec des rançongiciels. Enfin, les cyberterroristes adoptent une approche prosélyte – pour trouver de nouveaux adeptes –, ou détruisent soit des données – en utilisant entre autres des *wipers* – soit des infrastructures, par dégradation et tentative d'intrusion avec des outils du commerce.

Analyser les attaquants dans leur diversité aide à reconstituer les particularités de certains types de groupes. Ainsi, les groupes d'attaquants les plus virulents et les mieux formés ne développent pas nécessairement leur propre logiciel malveillant, par exemple. La plupart utilisent des *malwares* développés par d'autres, qui en ont fait leur spécialité. Certains conçoivent des armes digitales, d'autres les utilisent dans le cadre d'une stratégie offensive bien structurée. Les groupes d'origine chinoise notamment ont pris l'habitude de partager avec d'autres groupes leurs logiciels malveillants les plus efficaces. Une autre tendance croissante consiste à acheter sur le dark web un botnet malveillant auprès du plus offrant pour diffuser, dans un second temps, un *malware* plus évolué.

La particularité de ces groupes est parfois d'ordre géographique. Selon leur origine géographique, tous les groupes d'attaquants n'utilisent pas les mêmes techniques. Par exemple, très peu de groupes cybercriminels chinois utilisent des *ransomwares*, préférant le minage de cryptomonnaies, ou *cryptomining,* pour l'essentiel de leurs attaques. Au Moyen-Orient, les pirates informatiques privilégient l'utilisation frauduleuse des réseaux sociaux et des messageries cryptées (WhatsApp, Telegram, etc.) ou développent des *malwares* ciblant des applications mobiles (surtout sur Android). Les groupes nord-coréens, qui se spécialisent chacun sur un thème spécifique (espionnage du secteur de la défense aux États-Unis et en Europe, espionnage de la Corée du Sud, crime financier), mettent actuellement en commun leurs infrastructures d'attaque. Avec cette stratégie, il devient très difficile d'attribuer certaines attaques à un groupe particulier. Cela a conduit la plupart des observateurs à les amalgamer sous le nom générique de Lazarus. Ces spécificités géographiques s'expliquent, comme en Corée du Nord ou en Chine, par le fait que ces groupes d'attaquants communiquent entre eux et partagent des techniques d'attaque, souvent parce qu'ils sont soutenus par les mêmes institutions d'État. Elles relèvent parfois de limitations techniques (par exemple, l'indisponibilité relative de Play Store au Moyen-Orient), qui amène les attaquants à adopter tel *modus operandi* plutôt que tel autre. Quoi qu'il en soit, cette corrélation entre l'origine géographique des attaquants et les outils qu'ils emploient n'est pas systématique. Les attaquants russes, dont les motivations sont variées, mettent à profit tout l'arsenal informatique à leur disposition, par exemple.

Cette vaste analyse permet aussi d'identifier les tendances en matière de comportement technique. En ce qui concerne les attaques de chaîne d'approvisionnement notamment, le renforcement des systèmes de défense mondiaux oblige les attaquants à adopter des tactiques plus élaborées. Ces attaques restent donc très efficaces et on observe une forte progression des attaques indirectes, qui passent par les fournisseurs des diverses organisations. Ces derniers servent alors de cheval de Troie. Ce sont par exemple les prestataires de services habituels d'une entreprise qui servent à cibler les composants informatiques intégrés aux systèmes (applications mobiles, lignes de code, logiciels, etc.) ou aux objets connectés, comme les caméras de surveillance. Autre tendance émergente : le recours grandissant aux signatures de *malware* avec certificat de sécurité. Les hackers signent alors leurs logiciels malveillants avec des certificats volés, ce qui trompe maints programmes antivirus.

Nous constatons aussi que certaines techniques restent très usitées en raison de leur efficacité considérable. Le plus souvent, leur succès repose sur l'exploitation de la négligence et de l'erreur humaines. Le harponnage, pourtant aussi vieux que les cyberattaques, est ainsi encore efficace et très répandu.

Les principaux secteurs d'activité visés nous en disent également beaucoup sur les profils types qui ressortent de l'analyse. Plus de la moitié des groupes ciblent des institutions gouvernementales, souvent des organisations de défense, puis viennent la finance, les transports, l'énergie et l'aéronautique. Il n'est pas surprenant que les adversaires les plus compétents et les plus motivés visent en premier lieu des États, leurs capacités de défense et les grands acteurs majeurs du secteur. Ces attaquants, pour la plupart eux-mêmes soutenus par un État, mènent des attaques ciblées sur des rivaux géopolitiques ou sur leurs opérateurs stratégiques. La finance est le deuxième secteur le plus touché par les groupes d'attaquants. Ces derniers sont surtout des cybercriminels en quête de profits financiers colossaux. Leurs offensives, d'ampleur mondiale,

visent tous les acteurs du système financier mondial. À notre connaissance, 137 zones géographiques ont été la cible de groupes d'attaquants dans ce secteur. De même concernant les attaques contre des géants de l'énergie, essentiellement des multinationales, avec 24 attaquants actifs dans 106 pays. Le secteur de l'énergie fait aussi l'objet d'attaques très diverses, nos analystes ayant identifié plus de 230 familles de *malware* dans les cas d'usage. Cela s'explique probablement par le nombre croissant d'atteintes aux systèmes SCADA ou proto-IoT, que visent également des attaques toujours plus nombreuses dans les transports.

De manière générale, ce top 5 montre que les systèmes en place dans les secteurs critiques sont les plus ciblés, et que des scénarios de « cyber-Pearl Harbor » portant sur les villes intelligentes de demain et sur leurs infrastructures clés par exemple sont tout à fait possibles. Par ailleurs, les attaques se multiplient dans le secteur de la santé, à travers le vol de données personnelles ou d'informations sur des produits pharmaceutiques ultra-sensibles et présentant un intérêt particulier. Sur fond de crise de l'information, les médias deviennent eux aussi une cible privilégiée. Le plus souvent, il s'agit d'attaques de point d'eau, qui imitent un site Internet officiel pour disséminer de fausses informations ou d'attaques SWC (Strategic Web Compromise), plus sophistiquées, qui compromettent un site Internet officiel pour les mêmes raisons.

**L**e *Cyberthreat Handbook* brosse également un tableau précis, inédit, du paysage des cybermenaces en instaurant une notation par attaquant fondée sur la matrice MITRE ATT&CK. L'objectif est de montrer le niveau de menace que représente chaque groupe. C'est la deuxième grande finalité de ce rapport : fournir une estimation quantifiée de la menace que constituent les attaquants. En connaissant leurs tactiques habituelles, nous pouvons savoir si leur potentiel de nuisance et/ou de destruction est plus ou moins important au regard de leurs techniques (selon qu'elles sont faciles ou non à mettre en œuvre, qu'elles permettent à l'attaquant de contrôler tout ou partie d'un système, que les attaquants mobilisent un nombre limité de techniques ou un arsenal élaboré, selon qu'ils changent de techniques régulièrement et font preuve d'une grande agilité). Ces indications sont autant de paramètres objectifs qui nous autorisent à attribuer une note indicative pour chaque attaquant.

**L**a matrice MITRE ATT&CK définit 12 tactiques auxquelles un attaquant peut recourir pour mener ses campagnes. Chacune de ces 12 tactiques comprend entre 9 et 68 techniques identifiées par la matrice MITRE. Ce modèle forme la base du système de notation d'attaquants Thales-Verint. Pour certains, la note n'est pas indiquée parce que leurs techniques ne sont pas connues. Ainsi, si la note d'un attaquant est faible ou nulle, elle ne reflète pas forcément son véritable niveau technique. Ce dernier peut être important mais inconnu, ce qui renforce la menace potentielle. La note est obtenue par la formule suivante :

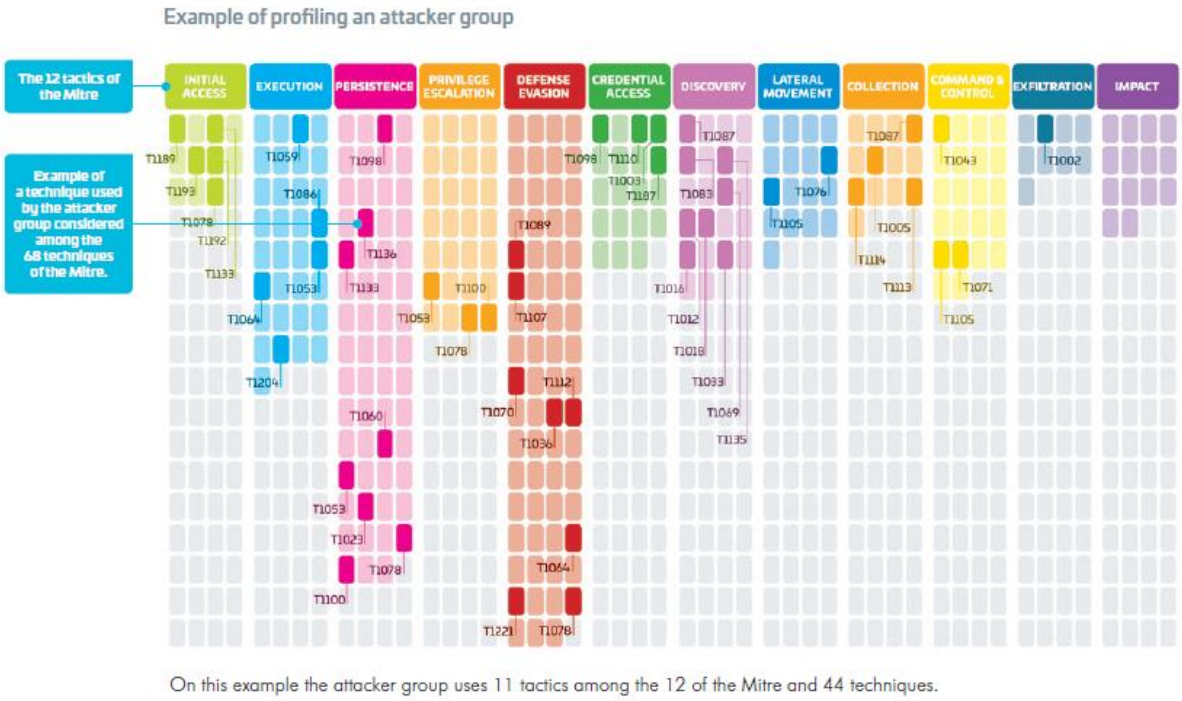
$$Score_{complexity} = \frac{Number\ of\ malware\ allowing\ this\ technique}{Number\ of\ attackers\ using\ this\ technique}$$

$$Score_{interest} = f(required\ permissions, impacted\ tactics, scarcity)$$

$$Score_{technique} = f(Score_{complexity}, Score_{interest})$$

$$Score_{tactic} = \sum Score_{technique}$$

$$Score_{attacker} = Average\left(\frac{Score_{tactic}}{Score_{maximum}}\right) \times 100$$




**L**'intérêt de ce rapport est que les utilisateurs peuvent se concentrer sur les menaces les plus pertinentes. La nature dynamique du répertoire et son système d'évaluation aident à fixer des priorités et à doser les efforts en fonction du domaine d'activité et/ou du pays où opère chaque organisation. En effet, ce rapport a pour objectif global d'aider à prioriser les actions en développant le renseignement à partir des informations disponibles.

- ***Téléchargez le rapport (en anglais)***

Pour plus d'information, téléchargez le rapport ici:
https://thalesgroup-myfeed.com/THECYBERTHREATHANDBOOK

# 4. Quelques exemples de groupes d'attaquants

## - FIN7, parmi les cybercriminels

FIN7 est un groupe financièrement motivé, actif depuis au moins 2013, qui cible principalement les secteurs du commerce de détail, de l'hôtellerie et de la restauration, principalement aux États-Unis. Des hypothèses évoquent qu'il s'agit du même groupe que Carbanak, mais il semble qu'il s'agisse de deux entités distinctes qui utilisent des outils similaires et qui font donc respectivement l'objet d'un suivi à l'heure actuelle. Son objectif principal est de voler les actifs financiers des entreprises, comme les cartes de débit, ou d'avoir accès aux données financières ou aux ordinateurs des employés du département des finances afin d'effectuer des virements sur des comptes offshore.

Le groupe utilise souvent l'hameçonnage comme principal vecteur d'attaque, y compris des campagnes de spear phishing conçues sur mesure. En outre, le groupe a utilisé une société écran surnommée « Combi Security », prétendument basée en Russie et en Israël, pour donner une apparence de légitimité et recruter des pirates pour rejoindre l'entreprise criminelle.

## - Anonymous Italia, parmi les Hacktivistes

Apparu en 2012, Anonymous Italia est l'un des plus anciens groupes hacktivistes du paysage italien de la cybermenace. Le groupe est caractérisé par une idéologie anarchiste, avec un sens aigu de la justice sociale et des questions environnementales. Cette empreinte hautement idéologique se traduit par une nette aversion pour les institutions politiques et les forces de sécurité italiennes. Dans ce contexte, nous identifions des tendances récurrentes dans la sélection des cibles des hacktivistes. En réalité, la police, les partis politiques et les institutions gouvernementales ont toujours été parmi leurs cibles privilégiées. Il convient de noter que de nombreuses attaques ont apparemment été menées en coopération avec deux autres groupes hacktivistes italiens, à savoir LulzSec ITA et AntiSecurity ITA, qui se caractérisent par une même idéologie.

Tout au long de sa longue activité, le groupe a exécuté des centaines de fuites de données, de défigurations de sites et d'attaques DDoS. Son attaque de 2015 contre le ministère de la Défense (avec des milliers de fuites) a également conduit à l'arrestation de deux membres éminents du collectif, connus sous les pseudos Aken et Otherwise. Fait intéressant, ce dernier a contribué au développement d'un portail « sans serveur » pour la coordination des opérations du groupe, dénommé Osiris, démontrant des capacités techniques importantes. Il est à noter que le groupe participe aussi activement à la promotion d'opérations réelles, telles que #OpGreenRights, #OpPaperStorm et la Million Mask March.

## - *Turla, parmi les Etats-nations*

ATK13 (Turla, Uroburos, Waterbug, Venomous Bear) est un acteur malveillant de cyberespionnage actif depuis au moins 2008, date à laquelle il s'est introduit dans le système du Département de la Défense américain. ATK13 est un groupe russophone perçu comme étant une organisation soutenue par l'État russe.

En 2015, Kaspersky a décrit ATK13 comme l'un des « plusieurs groupes d'élite APT ayant utilisé - et abusé - de liaisons par satellite pour gérer leurs opérations - le plus souvent, leur infrastructure C&C ».

En 2018 et 2019, ATK13 continue de cibler les gouvernements et les organisations internationales dans de multiples vagues d'attaques et continue à améliorer ses outils. L'attaque la plus récente visait un groupe iranien APT appelé OilRig. L'attaque de Turla contre l'un des groupes iraniens les plus prospères combine opportunisme et intérêts internationaux. Rappelons que depuis 2014 et l'annexion de la Crimée, les pressions occidentales et la chute du prix du pétrole ont plongé la Russie dans la récession. Pour cette raison, la Russie s'est rapprochée de l'Arabie saoudite, dont l'alliance avec les États-Unis s'était affaiblie sous l'ère Obama dans le cadre de l'accord nucléaire iranien, soutenu par l'ancien président américain. Il semble que le changement de ligne diplomatique américaine depuis l'élection de Donald Trump n'ait pas détourné l'Arabie saoudite de cette alliance. Ce rapprochement d'intérêts a été dénoncé par l'Iran, lors de la dernière réunion de l'OPEP à Vienne en juillet 2019. La raison de cette tension est également d'ordre économique, puisque les deux pays se préparent à s'attaquer au marché européen du gaz.

## - *Lazarus, parmi les Etats-nations*

Lazarus n'est pas un simple groupe de menaces. Il représente le Bureau 121 qui est l'un des huit Bureaux associés au Bureau général de reconnaissance (RGB) de Corée du Nord. Le Bureau 121 est le principal bureau chargé des cyber-opérations. Il a été réorganisé en septembre 2016 et il est maintenant composé de :

- Laboratoire 110 : Il s'agit de la principale unité cybernétique du RGB ; il applique des techniques de cyberattaque pour mener des opérations de renseignement
    - Bureau 98 : recueille principalement des informations sur les transfuges nord-coréens, les organisations qui les soutiennent, les instituts de recherche étrangers liés à la Corée du Nord et les professeurs d'université en Corée du Sud.
    - Bureau 414 : recueille des informations sur les organismes gouvernementaux, les organismes publics et les entreprises privées à l'étranger.
    - Bureau 35 : Le Bureau s'est concentré sur le développement de logiciels malveillants, la recherche et l'analyse des vulnérabilités, les exploits et les outils de piratage.
- Unité 180 : Unité spécialisée dans la conduite de cyber-opérations visant à voler de l'argent étranger en dehors de la Corée du Nord.
- Unité 91 :
    - elle se concentre sur les cyberattaques ciblant des réseaux isolés, en particulier les infrastructures nationales critiques de la Corée du Sud telles que le KHNP et le ministère de la Défense nationale de la République de Corée.
    - vole des informations et des technologies confidentielles pour mettre au point des armes de destruction massive.

- Bureau de liaison 128 et 413 : Responsable du piratage de sites Web de renseignements étrangers et de la formation d'experts en informatique.

## - *United Cyber Caliphate, parmi les cyberterroristes*

United Cyber Caliphate (UCC) ou Division de piratage de l'État islamique est le nom d'un regroupement de plusieurs groupes de pirates informatiques travaillant pour l'organisation terroriste de l'État islamique d'Irak et du Levant (EI). L'organisation a vu le jour en avril 2016. Il est surtout connu pour sa campagne contre le personnel militaire et gouvernemental américain. Le 4 avril 2016, la Cyber Caliphate Army (CCA), la principale unité de piratage de l'EI, et d'autres groupes pro-EI comme la Sons Caliphate Army (SCA) et Kalacnikov.TN (KTN) ont fusionné et formé The United Cyber Caliphate (UCC). Les groupes de l'UCC comprennent : - Cyber Caliphate, ou Cyber Caliphate Army (CCA) a été créé peu après la création de l'État islamique. La personne clé derrière le groupe était Junaid Hussain (Abu Hussain al Britani), ou TriCK. L'attaque cyberterroriste la plus importante de la CCA s'est produite en janvier 2015 lorsque les comptes Twitter et YouTube du U.S. Central Command et plus tard les comptes Twitter du magazine Newsweek ont été piratés. - La Sons Caliphate Army (SCA) a été créée en 2016, en tant que sous-groupe du Cyber Caliphate. Principalement connu pour perturber le trafic des réseaux sociaux sur Facebook et Twitter. SCA a déclaré avoir piraté 10 000 comptes Facebook, plus de 150 groupes Facebook et plus de 5 000 profils Twitter. - Kalachnikov E-Security Team a été créé en 2016. Ce groupe se concentre sur les conseils en matière de sécurité technique pour les djihadistes de l'EI. Il a également téléchargé de la documentation sur le jihadisme lié à l'EI, partagé des messages de groupes de cyberdjihadistes, signalé des attaques réussies sur des sites Web et des pages Facebook et publié diverses techniques de piratage sur le Web. Peu à peu, les pirates ont commencé à mener ou à aider des actions de défiguration.

# 5. Autres rapports d'analyse technique des cybermenaces

### Thales – Verint 2018 : Panorama des cybermenaces

L'analyse technique des cybermenaces est à la cybersécurité ce que le renseignement est à la sécurité : le recueil et la corrélation d'un maximum d'informations relatives à la menace afin de s'en protéger avant que ne survienne un incident. Il s'agit de caractériser les organisations, les stratégies, les tactiques voire les identités des cyber-attaquants potentiels. A l'heure où la cyber-menace devient globale, l'échange d'information entre les acteurs mondiaux majeurs de la cybersécurité doit permettre à chacun d'enrichir sa vision donc la pertinence de ses analyses.
Dans ce contexte, Thales et Verint publient un rapport sur le panorama des menaces et renforcent leur coopération dans le domaine du renseignement sur la menace.

**Téléchargez le rapport**: http://www.thalesgroup-events.com/ThalesVerint

### THALES - SEKOIA 2019 – Rapport sur les cybermenaces financières

Le secteur financier est l'une des cibles privilégiées des cyberattaquants. Distributeurs de billets, transactions financières, vols de données bancaires etc, la cybercriminalité occasionne des pertes en milliards de dollars pour l'industrie financière mondiale, un risque que les parties prenantes du secteur ne peuvent plus prendre. Dans leur rapport, fruit de leur récente association, Thales et SEKOIA apporte un éclairage détaillé sur les cybermenaces dans le secteur financier.

**Téléchargez le rapport**: http://www.thalesgroup-events.com/ReportTHALESSEKOIA

**Principales conclusions :** https://www.thalesgroup.com/fr/marches-specifiques/systemes-dinformation-critiques-et-cybersecurite/news/thales-et-sekoia

# 6. Des questions?


**CONTACT PRESS**

**Thales, media relations**
Constance Arnoux
+33 (0)6 44 12 16 35
constance.arnoux@thalesgroup.com


**FIND OUT MORE**

Thales Group
Télécharger les photos

@Thalesgroup