THALES
Building a future we can all trust

Dossier de presse

Thales Cyber Threat Handbook 2020 :
La cybercriminalité organisée

1. A propos de Thales……..3

2. Le service d'analyse technique des cybermenaces de Thales……4

3. Le *Cyberthreat Handbook*…….……....7

4. Quelques exemples de cybercriminels……..……11

5. Autres rapports d'analyse technique des cybermenaces…...12

6. Des questions ?.....13

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 **83 000 collaborateurs dans 68 pays**, Thales a réalisé un chiffre d'affaires de 19 milliards d'euros en 2019 (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 6 000 ingénieurs 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

« Le plus grand supplice est de craindre ce que l'on peut éviter », disait Thalès de Milet, dont la citation figure dans le rapport. Les cybermenaces ne sont pas une fatalité : nous pouvons apprendre à combattre les cyberattaquants en en connaissant leurs motivations, leurs moyens financiers et techniques, leurs techniques d'attaque, etc.

Néanmoins, 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. Ces informations techniques sont ensuite contextualisées au regard de l'environnement stratégique (géopolitique, social, économique, etc.) dans lequel elles s'incluent.

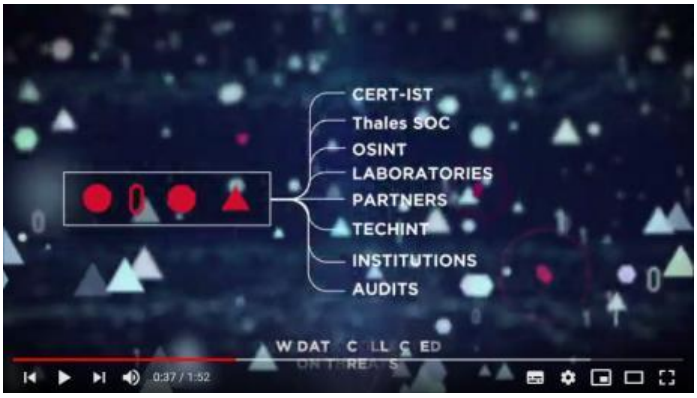
C'est l'ambition de l'analyse technique des cybermenaces : **analyser et comprendre les cybermenaces pour mieux s'en protéger et mieux les détecter**. La finalité de cette analyse de la menace est l'interconnexion avec les outils de détection des cyberattaques (comme la sonde et le SOC). Il s'agit d'analyse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

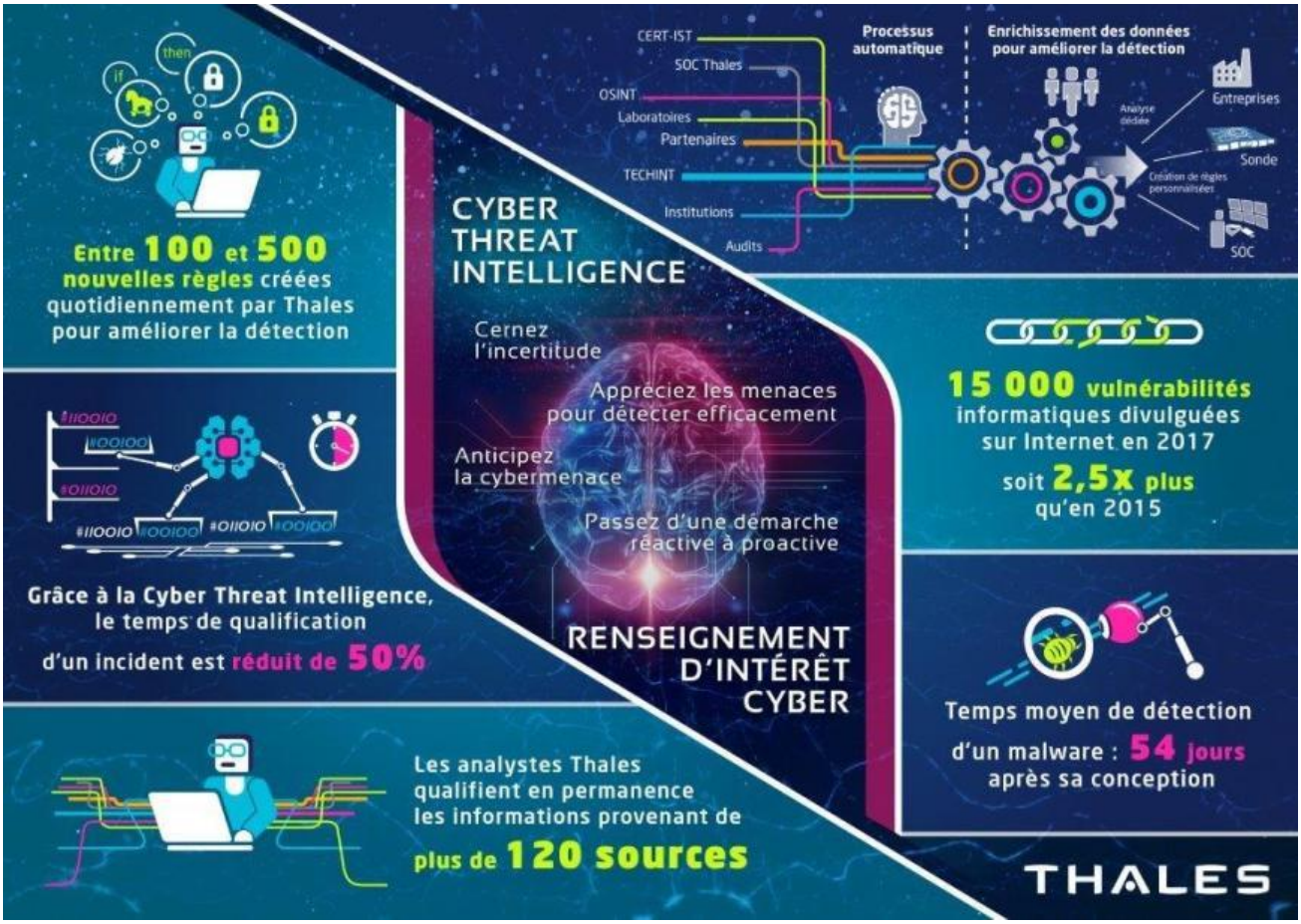
À cet effet, les analystes travaillent continuellement à **la collecte, au traitement et à l'analyse de données**. Ils analysent également les logiciels malveillants afin de **développer des rapports sur le comportement des hackers et de fournir des informations pertinentes aux clients attaqués**. Le 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 vidéo 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 contexte et stratégie et le Bureau *Automatation & 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 :

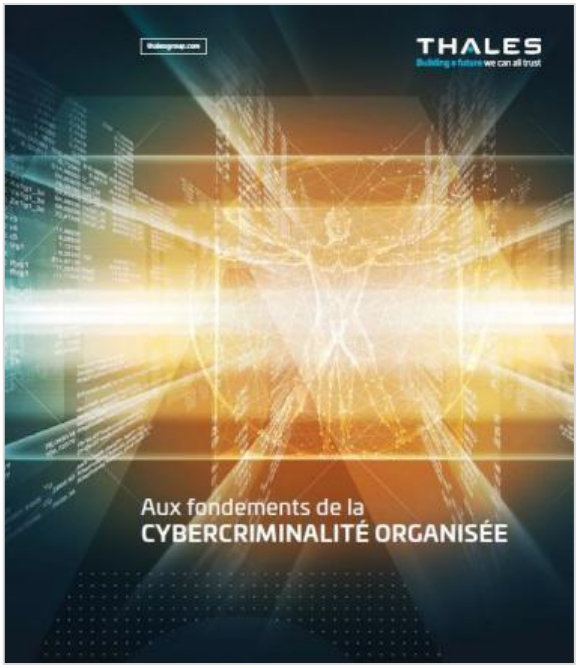
> ***Episode 1***: Quentin, à propos du bureau des analyses techniques

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

> ***Episode 3***: Romain, à propos du bureau *Automation & Delivery*

3. « Cyber Threat Handbook 2020, la cybercriminalité organisée » de Thales

- Introduction



Réalisée par Thales, cette édition du *Cyberthreat Handbook* consacrée à la cybercriminalité est un document original qui dévoile son analyse et ses conclusions face au risque que représente la cybercriminalité, un réseau très dangereux de différents groupes d'attaquants.

La cybercriminalité organisée a aujourd'hui atteint un niveau de prédation sans précédent à l'échelle mondiale. Ce phénomène d'une complexité incroyable est exigeant et nous interroge autant qu'il nous menace.

Le préjudice généré par la cybercriminalité organisée sur l'économie mondialisée a atteint depuis 2018 des niveaux sans précédents, se chiffrant en plusieurs centaines de milliards de dollars.

La cybercriminalité selon plusieurs observateurs, et notamment l'ANSSI, sera la plus grande menace des années à venir. Mais comment comprendre un phénomène si diffus, si mouvant et entrelacé ? Comment se prémunir contre un phénomène qu'on ne comprend pas définitivement, dont les contours sont flous, alors même que le niveau de menace qu'il génère aujourd'hui implique des risques stratégiques cruciaux pour les organisations et les sociétés ?

C'est cette question déterminante que l'équipe d'analyse technique de la menace cyber (CTI) de Thales, a souhaité explorer afin d'offrir à nos partenaires et au grand public des clés de compréhension du fonctionnement global de la cybercriminalité organisée.

Les demandes de rançons présentées se chiffrent, non plus en milliers, mais en millions voire en dizaines de millions d'euros et peuvent mettre en péril la survie d'une organisation stratégique. Ce phénomène a définitivement bouleversé le paysage de la menace cybercriminelle puisque les attaquants présentent des caractéristiques se rapprochant des plus grands groupes d'espionnage, tout en conservant une vocation financière.

Ce rapport inédit prend la forme d'une réflexion sur la nature de la cybercriminalité, sur ses modes de fonctionnement, sur les imaginaires qui l'animent, sur la place que les entreprises et les acteurs de la cybersécurité occupent en son sein.

Il s'agit d'un memento élémentaire sur les concepts à garder à l'esprit pour l'analyse du phénomène mais également d'un appel à la réflexion commune autour de la création de nouvelles méthodes d'analyse. Il n'est pas question ici de faire œuvre de morale ou de critiquer de manière sentencieuse mais de chercher les leviers de compréhension les plus adaptés pour assurer notre sécurité collective et lui donner une teinte proactive. L'idée est de présenter un regard différent, un angle d'approche innovant et de proposer une méthodologie à nos partenaires et au grand public pour comprendre cette incroyable complexité qui les concerne pour construire des stratégies saines.

- *Un rapport consacré à l'une des menaces les plus inquiétantes de notre société*

À l'échelle mondiale ce phénomène prend une forme d'autant plus préoccupante. L'Organisation des Nations-Unies et Accenture estiment que le coût de la cybercriminalité organisée devrait représenter 5 200 milliards de dollars pour l'économie mondiale entre 2020 et 2025. Cybersecurity Ventures avance le chiffre de 6 000 milliards par an. Ainsi, c'est quasiment la moitié du PIB de la Chine qui disparaitrait chaque année du fait des conséquences de cette cybercriminalité devenue organisée. L'ampleur du phénomène devient stratégique.

Avec des revenus estimés à 1 500 milliards de dollars par an par la société Bromium et le Dr Mike McGuire, chercheur en criminologie de l'Université de Surrey – soit environ 1,5 fois les revenus de la contrefaçon et 2,8 fois ceux du trafic de drogue – la cybercriminalité est considérée comme la menace la plus importante pour les entreprises, les organisations et les institutions.

C'est dans ce contexte que les spécialistes de Thales ont décrypté, dans cette édition du CyberThreat Handbook consacrée à la cybercriminalité, le phénomène de cybercriminalité organisée, un système qui permet aux cybercriminels de mettre en pratique un mode opératoire performant et très innovant, allant jusqu'à l'hybridation avec d'autres pans de la cybermenace.

- *Un réseau organisé*

La cybercriminalité fonctionne comme un réseau très puissant de différents groupes d'attaquants. Elle ne doit plus être appréhendée aujourd'hui sous la forme d'un 'phénomène' observable mais d'une logique 'organisée' compréhensible. L'enjeu de la compréhension de la cybercriminalité mondiale et de son impact sur les sociétés réside dans ce processus croissant d'organisation.

Cette logique organisée représente la menace la plus importante et la plus évolutive pour les entreprises, les OIV et les institutions. Ce n'est pas le nombre colossal de groupes d'attaquants qui donne corps à la cybercriminalité organisée mais la tendance que ces groupes ont à l'interaction. Les interactions, les mouvements permanents solidarisent la cybercriminalité organisée et lui donne vie.

Au sein de cette organisation, on retrouve, sur le haut du panier, un ensemble de groupes d'attaquants particulièrement performants techniquement, avec des stratégies de compromission très élaborées et des moyens financiers importants : ce sont les Big Game Hunters (« Big Game Hunting » = la chasse aux gros gibiers).

Ces groupes se rapprochent dans leurs modes opératoires et leurs infrastructures techniques, de certains groupes d'espionnage sponsorisés. Ils visent des cibles très précises, des institutions politiques ou de grandes entreprises, par ransomware, avec des demandes de rançon souvent importantes. Nous avons observé des demandes de rançon unitaire de 2 millions d'euros et des gains cumulés allant jusqu'à 15 millions de dollars lors de campagnes de l'opérateur MAZE qui avait pris pour cible Bouygues Construction en début d'année 2020.

- *Le modèle de la spécialisation*

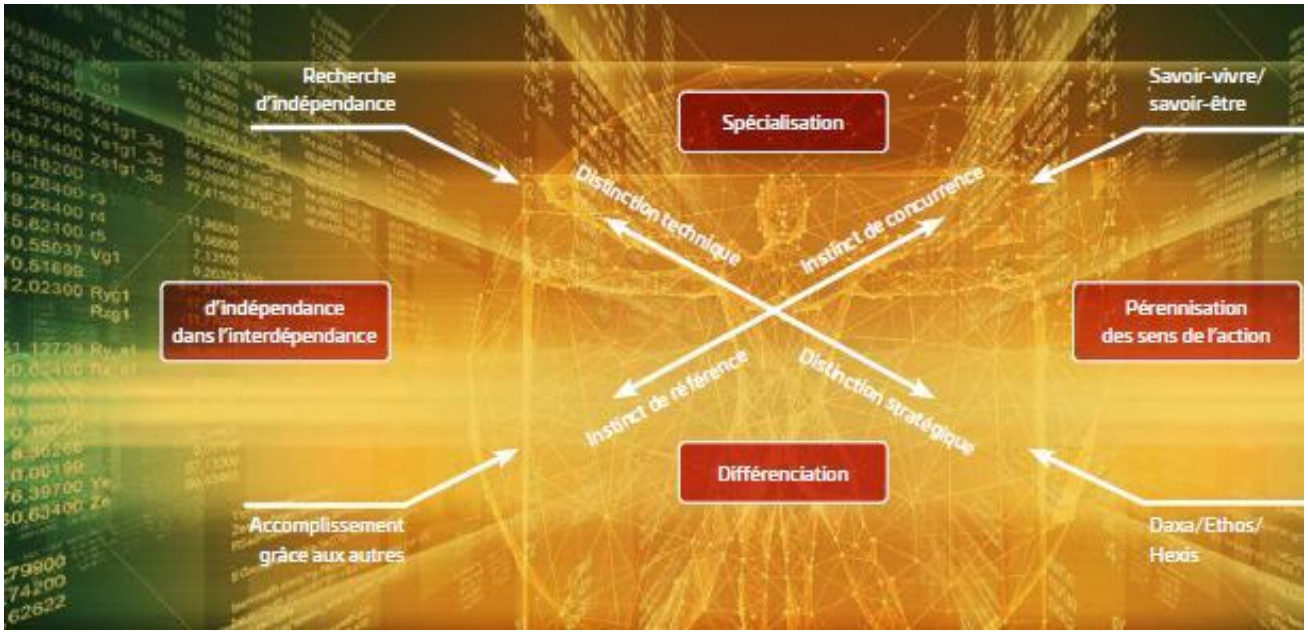
Les attaquants, recherchent inconsciemment et en permanence à se différencier. Ce caractère inconscient est lié à deux formes d'instincts que l'on retrouve dans d'autres espaces sociaux : l'instinct de référence et l'instinct de concurrence. Ces instincts sont par exemple très visibles dans le cadre du Big Game Hunting (BGH).

L'instinct de référence pousse les attaquants à s'observer en permanence pour ne pas être dépassés et pour améliorer continuellement leur mode opératoire. L'instinct de concurrence en est

le pendant. Sans s'affronter directement, la proximité dans l'espace qu'ils occupent, la proximité des modes opératoires et des arsenaux qu'ils mobilisent attise une concurrence. Ces deux instincts animent un processus de différenciation, une recherche de performance, d'innovation et parfois même de reconnaissance.

Cette recherche compulsive de différenciation est intrinsèquement liée à une autre forme de pulsion, prenant la forme d'une tendance à la spécialisation. Exister en tant qu'acteur crédible de la cybercriminalité exige de se spécialiser par une distinction stratégique ou une distinction technique.

Les techniques des cybercriminels évoluent sans cesse grâce à ce réseau et aux interactions au sein de ce réseau : chaque groupe se spécialise puis s'entraide pour bénéficier de l'expertise des autres. La spécialisation fait leur force et leur performance ; les criminels peuvent se concentrer sur un type d'attaque et bénéficier de l'expertise des autres pour pouvoir être plus performants et avoir davantage d'impact.



- *Les techniques et modes opératoires des groupes d'attaquants*

Nous assistons depuis mi-2018 à une évolution importante de ce dernier impliquant une nouvelle forme de prédation notamment dans le domaine des attaques par logiciels de rançon en France et à l'étranger. Des attaques par logiciels de rançon se sont notamment multipliées et sont liées à phénomène contextuel plus large de Malware-as-a-Service (MaaS) et de renforcement des interactions entre les grands cybercriminels.

Un phénomène de haut niveau de Malware as a Service est en train d'émerger pour venir renforcer une pratique de Big Game Hunting (BGH), expliquée dans ce rapport. Elle constitue une menace importante pour les organisations.

Il y a ensuite plusieurs services de Ransomware-as-a-Service qui se sont également fait connaître en 2019 du fait de leur efficacité. L'un des plus connus GandCrab (développé par ATK168 - Pinchy Spider), a annoncé son retrait la même année après avoir engrangé 150 millions de dollars de gains en un an et d'être remplacé par d'autres services comme Sodinokibi (sans doute développé par le même groupe).

De façon étonnante, 60% de ces revenus colossaux proviennent des marchés illégaux en ligne, 30% du vol de propriété intellectuelle et des secrets commerciaux et seulement 0,07% des recettes de ransomware, qui sont pourtant les attaques qui font le plus dégâts.

Bien que des secteurs soient plus sensibles que d'autres, tels que les médias, la santé ou les collectivités territoriales, les cybercriminels n'ont pas de cibles prédéfinies mais agissent davantage par opportunité lorsqu'une entreprise est vulnérable. Les cybercriminels scannent l'ensemble de leur réseau pour trouver les vulnérabilités et s'y infiltrer. De plus, ils font preuve d'une importante capacité à observer le monde qui les entourent, à analyser ce qu'il se dit dans les médias, dans des rapports notamment, afin de trouver de nouvelles manières d'attaquer.

La performance de leur mode opératoire est renforcée par leurs capacités d'adaptations stratégiques importantes. Dès les débuts de la crise du COVID-19, les acteurs de la cybercriminalité organisée ont été les premiers à utiliser la thématique dans leurs leurres pour du phishing, les premiers à imiter des sites légitimes liés au COVID-19 (Imitation de la cartographie dynamique de suivi de l'épidémie de l'Université John Hopkins par les opérateurs du malware Azorult par exemple), les premiers à développer des applications téléphones compromises ou à compromettre des applications légitimes en lien avec le COVID-19.

- *Appréhender la menace : les recommandations établies*

Pour atteindre leurs objectifs, les cybercriminels misent sur leurs techniques mais également sur le vent de panique qu'ils créent dans les institutions ou entreprises. L'effet de la panique peut être dévastateur dans l'estimation des conséquences d'une attaque. Il est impératif de ne pas céder aux menaces ni au chantage, il faut accepter d'être une cible voire une victime.

Pour prévenir la menace il est recommandé d'anticiper et d'améliorer la stratégie de gestion de crise. Pour cela, les entreprises et les organisations doivent s'y préparer et anticiper les réactions nécessaires. Les solutions ne sont pas toujours techniques, il faut également se préparer à gérer une attaque en passant par la gestion de crise, les modalités d'assurance, la sensibilisation des collaborateurs, etc.

Dans le cas d'une attaque, au lieu de payer une rançon, les experts de Thales vous recommandent de ne pas payer de rançon mais de vous rapprocher immédiatement des autorités compétentes et vous invitent à suivre les conseils détaillés de l'ANSSI :

- Pour réduire le risque d'attaque par rançongiciels
  - Sauvegarder les données
  - Maintenir à jour les logiciels et systèmes
  - Utiliser et maintenir à jour les logiciels antivirus
  - Cloisonner le système d'information
  - Limiter les droits des utilisateurs et autorisations des applications
  - Maîtriser les accès Internet
  - Mettre en œuvre une supervision des journaux
  - Sensibiliser les collaborateurs
  - Évaluer l'opportunité de souscrire à une assurance cyber
  - Mettre en œuvre un plan de réponse aux cyberattaques
  - Penser sa stratégie de communication de crise cyber

- Pour bien réagir en cas d'attaque
  - Adopter les bons réflexes
  - Piloter la gestion de la crise cyber
  - Trouver de l'assistance technique
  - Communiquer au juste niveau
  - Ne pas payer la rançon
  - Déposer plainte
  - Restaurer les systèmes depuis des sources saines

- ***Téléchargez le rapport en français***

Pour plus d'information, téléchargez le rapport ici: https://thalesgroup-myfeed.com/WPTHALESCyberThreatHandbook2020FR

4. Quelques exemples de cybercriminels

- ***Maze***

Le groupe MAZE, un *Big Game Hunter*, en utilisant le chantage à la divulgation des données de ses cibles à partir de fin 2019 avec l'attaque contre l'américain Southwire, a changé les règles du jeu et a été imité par ses concurrents. Ces derniers ont commencé à intégrer cette tactique de manière systématique dans leur mode opératoire en se référant à Maze ce qui a accentué ce phénomène de différenciation. Le matin du 30 janvier 2020, Bouygues Construction a été attaqué par Maze. Le groupe a exigé une rançon de 10 millions d'euros contre la non-divulgation des 200 Go de données qui semblaient avoir été volés. Cette attaque a fait du chantage à la divulgation un élément récurrent du modus operandi de Maze.

- ***FIN6***

ATK88 (FIN6) a visé, en 2019, la société Eurofins avec son logiciel de rançon Ryuk. Dans ses résultats trimestriels, le groupe de bio-analyse a fait état d'une perte de 62 millions d'euros liée à l'attaque. Le même groupe, qui a visé trois hôpitaux en Alabama et la ville de la Nouvelle-Orléans, ainsi qu'Altran (20 millions d'euros de pertes) et Norsk Hydro (75 millions d'euros de pertes) avec son logiciel de rançon LockerGoga, est très proche d'un autre cybercriminel de très grande envergure, ATK103 (TA505), qui a attaqué cette année l'hôpital de Rouen avec son logiciel de rançon Cl0p.

- ***Mummy Spider***

Le premier (ATK88-FIN6) utilise un malware du second (ATK103-TA505) appelé FlawedAmmyy. Ces liens d'intérêt préexistants devraient être renforcés à l'avenir avec l'apparition d'un autre groupe : ATK104 (Mummy Spider) et son logiciel malveillant de type loader Emotet qui télécharge d'autres logiciels malveillants sur les machines qu'il infecte et garde la main dessus. Cependant, le nombre de machines infectées par Emotet est colossal et touche tous les secteurs d'activité. Jusqu'à récemment, Emotet téléchargeait plusieurs logiciels malveillants différents. Il a surtout téléchargé le malware TrickBot, lui-même parfois utilisé par le malware Ryuk d'ATK88 (FIN6).

Si nous ne connaissons pas la nature exacte des liens entre les trois entités cybercriminelles ATK88 (FIN6), ATK103 (TA505) et ATK104 (Mummy Spider), qu'ils soient d'entraide ou commerciaux, il est certain que cette convergence d'intérêts va créer un réseau extrêmement puissant. Emotet, renforcé par ce lien avec ATK103 (TA505) et ATK88 (FIN6), peut droper des logiciels de rançon à haut degré de dévastation.

- ***Indrik Spider***

Le Groupe M6, l'un des plus grands groupes multimédias privé français, a lui été victime du logiciel de rançon BitPaymer en octobre 2019 créé par ATK180 (Indrik Spider). BitPaymer demande des rançons allant jusqu'à 216 Bitcoins (environ 2 millions d'euros d'équivalence suivant la valeur d'octobre 2019). De nombreuses attaques sur le réseau des municipalités ont également été constatées, car ces réseaux sont souvent critiques pour la vie locale mais très mal protégés.

- ***FIN7***

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. 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.

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

Thales – Verint 2019 : CyberThreat Handbook

Alimentées par leurs technologies et solutions de pointe en cybersécurité, Thales et Verint présentent leur « Cyberthreat Handbook », un rapport à l'envergure inédite, dans le but d'étudier et de catégoriser les groupes de cyberattaquants majeurs, allant des cybercriminels, des cyberterroristes et des cyberactivistes aux Etats nations. Dans le cadre d'un partenariat stratégique pour développer des technologies de pointe et complètes pour l'analyse technique de la menace, les équipes de Thales et Verint dévoilent un panorama inégalé des principales cybermenaces, en décrivant très précisément le mode opératoire, les motivations et les secteurs touchés par une soixantaine de groupes emblématiques, grâce à des analyses de multiples sources de renseignement telles que le web ou l'analyste technique de la menace.

Téléchargez le rapport : https://thalesgroup-myfeed.com/THECYBERTHREATHANDBOOK

Thales 2019 : Le télétravail en période de crise

Alors que nous vivons une crise sanitaire mondiale sans précédent, les hackers profitent de la situation pour mener des attaques qui ciblent les systèmes d'information des entreprises et des organisations mais également les particuliers. Il est donc essentiel de redoubler de vigilance et d'écarter autant que possible les risques de « pandémie cyber ». Pour aider les organisations à se prémunir contre ces risques dans cette période délicate, Thales donne accès gratuitement à l'étude réalisée par son Centre d'analyse technique des Cybermenaces.

Télécharger l'étude : https://www.thalesgroup.com/sites/default/files/database/document/2020-05/2020-04-03_COVID-19_MENACES_SUR_LE_TELETRAVAIL_%28FR%29%20%283%29.pdf

6. Des questions?

CONTACT PRESSE

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

PLUS DE RENSEIGNEMENTS

Thales Group
Cybersécurité
@Thalesgroup