enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

FR

De janvier 2019 à avril 2020

# Principaux incidents dans l'UE et dans le monde

Paysage des menaces de l'ENISA

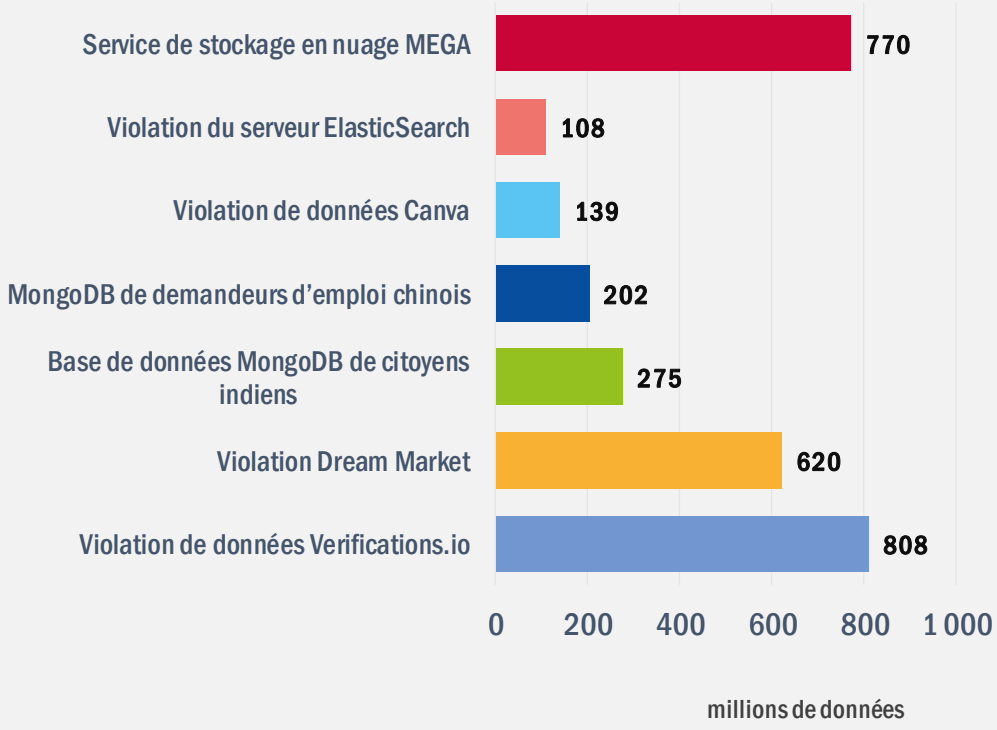
# Aperçu

**La sophistication des capacités de menace s'est accrue en 2019; de nombreux adversaires ont désormais recours aux codes d'exploitation, au vol d'identifiants et aux attaques en plusieurs étapes.** Le nombre de violations de données est encore très élevé et la quantité d'informations financières et d'identifiants d'utilisateur volés augmente. Dans certains cas, le fait de ne pas corriger une vulnérabilité connue susceptible d'affecter les logiciels ou les bibliothèques en cours d'utilisation (dans un délai raisonnable) peut avoir de graves répercussions.

Depuis ces dix dernières années, **les logiciels malveillants (*malware*) font partie de la liste des 15 principales menaces répertoriées par l'ENISA et, pourtant, de nombreux systèmes de sécurité ne sont toujours pas en mesure de détecter cette menace.** Si, pendant de nombreuses années, les logiciels malveillants se sont principalement répandus par le biais de pourriels malveillants, désormais, ils se propagent grâce à des messages d'hameçonnage bien ficelés. Les entreprises spécialisées dans la technologie tout comme les fournisseurs de messagerie électronique ont investi dans des filtres antipourriels, améliorant ainsi la détection des pièces jointes malveillantes. Cependant, **les adversaires misent désormais sur l'innovation pour augmenter leurs chances d'atteindre des victimes potentielles.** Au cours de la période considérée, bon nombre de ces innovations ont été payantes pour les acteurs malveillants.

Partout dans le monde, les organismes et professionnels de la santé ont été mis sous pression en raison de la pandémie de COVID-19; la santé est donc devenue l'un des secteurs les plus importants à protéger contre les cyberattaques. Le nombre d'incidents visant le secteur de la santé et impliquant des rançongiciels (*ransomware*), déjà élevé, a encore augmenté pendant la pandémie.

# Principaux incidents de violation de données



# Chronologie

## 2019

### _ Janvier

Le service de stockage en nuage MEGA (Nouvelle-Zélande) a subi une violation de données exposant 770 millions de courriels et 21 millions de mots de passe.[1]

### _ Février

Près de 800 millions de données ont été exposées par Verification.io (États-Unis).[2]

### _ Mars

Norsk Hydro (Norvège) a été victime d'une attaque par rançongiciel.[3]

### _ Août

En Bulgarie, l'administration fiscale a subi une violation de données exposant les données personnelles de l'ensemble de ses citoyens majeurs.[8]

### _ Septembre

Mastercard (Belgique) a subi une violation de données qui a touché environ 90 000 clients en Europe.[9]

### _ Octobre

En Géorgie, des sites web et la télévision nationale ont fait l'objet d'une cyberattaque coordonnée.[30]

### _ Novembre

UniCredit (Italie) a été victime d'une violation de données ayant entraîné la fuite de 3 millions de dossiers.[10]

### _ Décembre

Prosegur (Espagne) a subi une attaque par rançongiciel qui a perturbé son fonctionnement.[11]

## 2020

### _ Janvier

Le ministère autrichien des affaires étrangères a été la cible d'une cyberattaque.[12]

## _ Avril

Facebook (États-Unis) a signalé une violation de données divulguant 540 millions de dossiers d'utilisateurs sur des serveurs exposés.[4]

## _ Mai

Thyssen-Krupp et Bayer (Allemagne) ont été visés par un logiciel espion.[5]

## _ Juillet

City Power (Afrique du Sud) a été victime d'une attaque par rançongiciel qui a perturbé l'approvisionnement en énergie de Johannesbourg.[7]

## _ Juin

Cinq hôpitaux en Roumanie ont été frappés par le rançongiciel BadRabbit.[6]

## _ Février

Le groupe INA (Croatie) a été victime d'une attaque par rançongiciel.[13]

## _ Mars

Le réseau ENTSO-E (Belgique) a été compromis, victime d'une intrusion.[14]

## _ Avril

Découverte de plus de 500 000 comptes Zoom (États-Unis) en vente sur le *dark web*.[31]

# Secteurs les plus ciblés

## Dans la ligne de mire

Au cours de la période considérée, les secteurs les plus visés ont été les services numériques, l'administration publique et le secteur des technologies. Les attaques contre les fournisseurs de services numériques servent souvent de passerelles pour atteindre d'autres cibles plus attrayantes. En revanche, les attaques contre le secteur des technologies ont permis aux acteurs malveillants de compromettre la chaîne d'approvisionnement ou de rechercher des vulnérabilités à exploiter.

La plateforme de courriels **Verifications.io**[18] a subi une importante violation de données en raison d'une base de données MongoDB non protégée. Plus de 800 millions de courriels contenant des informations sensibles, notamment des données à caractère personnel, ont été exposés.

Plus de 770 millions d'adresses électroniques et 21 millions de mots de passe uniques ont été exposés sur un célèbre forum de piratage hébergé par **MEGA**, service de stockage en nuage[1]. Nommée «Collection #1», il s'agit de la plus importante violation de données à caractère personnel de l'histoire.

**Citrix**, fournisseur de services en nuage et de virtualisation, a été victime d'une cyberattaque ciblée. Pour accéder aux systèmes de Citrix, les attaquants ont exploité plusieurs vulnérabilités logicielles critiques, comme la CVE-2019-19781, et ont utilisé une technique appelée la «pulvérisation de mots de passe» (*password spraying*).

**iNSYNQ**[19], fournisseur d'hébergement en nuage, a subi une attaque par rançongiciel qui a empêché les clients d'accéder à leurs données pendant plus d'une semaine, les obligeant à avoir recours à leurs sauvegardes locales.

# Secteurs les plus ciblés

**Services numériques_** Les services tels que messageries, plateformes sociales et collaboratives ainsi que les fournisseurs de services en nuage ont fait l'objet d'attaques en 2019. Ils ont également été utilisés comme passerelles pour mener d'autres attaques.

**Administration publique_** La rentabilité financière des rançons versées fait du secteur public l'une des cibles les plus attrayantes pour les attaques par rançongiciel.

**Secteur des technologies_** En 2019, le secteur des technologies a principalement subi des attaques de la chaîne d'approvisionnement qui essayaient de compromettre le développement de logiciels via des codes d'exploitation de type «0-Day» et des portes dérobées (*backdoors*).

**Finances_** Le nombre d'incidents dans des organismes financiers, et pas nécessairement des banques, a considérablement augmenté au cours de la période de référence.

**Santé_** Le nombre d'attaques contre le secteur de la santé ne cesse de croître.

# Tendances

## _Une tendance généralisée

- En 2019, on a pu observer une forte **activité des chevaux de Troie** dans le monde entier. Emotet et Agent Tesla ont été les logiciels malveillants les plus fréquents et les plus dangereux[↗].
- L'**hameçonnage (*phishing*)**[↗] demeure l'une des techniques les plus efficaces pour diffuser des outils malveillants. Les arnaques téléphoniques, les fausses factures, ainsi que les paiements, devis et bons de commande frauduleux constituent de puissants leurres d'hameçonnage.
- Le **rançongiciel (*ransomware*)**[↗] continue de générer de juteuses récompenses financières pour les acteurs malveillants. Une étude récente a permis d'identifier des campagnes de rançongiciels contrôlées par l'homme[17], dans lesquelles les adversaires se servent de méthodes de vol d'identifiants et de déplacement latéral, habituellement associées aux attaques ciblées comme celles menées par des acteurs parrainés par des États-nations.
- Les systèmes de **clonage de cartes** (*card-skimming*) sont devenus une menace importante en 2019 et 2020 en raison du nombre croissant d'acheteurs en ligne.
- La **compromission de la messagerie en entreprise** (BEC - *Business E-mail Compromise*) est une menace croissante suite au grand nombre d'identifiants et d'informations personnelles volés ces dix dernières années.
- Chaque mois, les entreprises subissent en moyenne 12 attaques par bourrage d'identifiants (***credential stuffing***), au cours desquelles l'attaquant parvient à trouver des identifiants valides.

# Conclusions

**84 %_** des cyberattaques reposent sur l'ingénierie sociale

**67 %_** des logiciels malveillants ont été transmis par des connexions HTTPS chiffrées[34]

**230 000_** nouvelles souches de logiciels malveillants chaque jour

**6_** mois correspond au temps moyen nécessaire pour détecter une violation de données

**71 %_** des organisations ont déjà fait l'expérience de la propagation d'un logiciel malveillant d'un employé à un autre[35]

# Acteurs

## _Qui

Lorsqu'un incident de cybersécurité se produit, trouver le responsable ou attribuer la responsabilité à un individu ou à un groupe d'individus reste une tâche très fastidieuse et un exercice bien souvent inutile. Pourtant, du point de vue de l'analyse de la menace, il est essentiel de classer les comportements, de comprendre la dynamique ainsi que le mode opératoire utilisé par certains adversaires. Cette analyse aide souvent les défenseurs à rechercher des pistes spécifiques et à essayer d'anticiper la prochaine action de l'adversaire.

À titre d'exemple, **Lazarus Group**, un groupe responsable d'attaques ciblées avancées (APT - *Advanced Persistent Threat*) prétendument parrainé par l'État, aurait été plus actif au cours de la période considérée dans le cadre d'attaques motivées aussi bien par l'argent que par l'espionnage. Le groupe a été associé à plusieurs incidents, dont la **campagne AppleJeus** qui visait non seulement les utilisateurs mais aussi les systèmes des plateformes d'échange de cryptomonnaies.[22] Parmi les incidents majeurs attribués à ce groupe, on peut citer:

- le piratage d'une centrale nucléaire et de l'agence spatiale indiennes en novembre 2019;
- la compromission d'une application d'échange de cryptomonnaies visant les administrateurs d'échange en octobre 2019;
- des attaques de guichets automatiques et de banques en Inde, identifiées en septembre 2019;
- une attaque dirigée contre les utilisateurs d'Android en Corée du Sud par le biais d'applications infectées par un cheval de Troie dans Google Play Store, identifiée en août 2019.

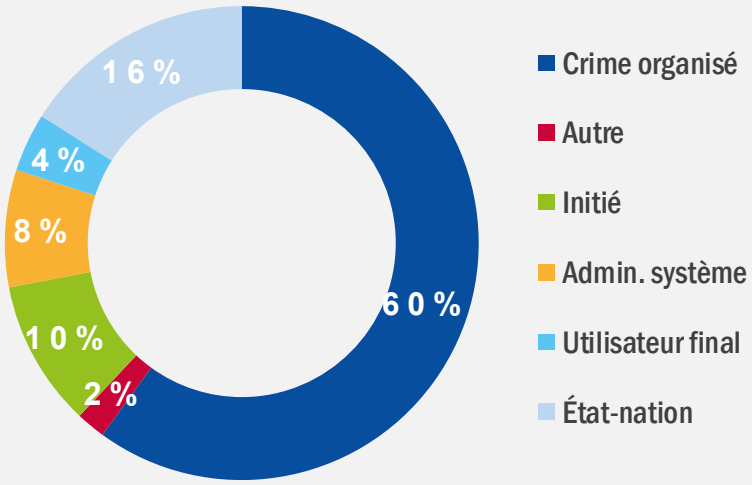
# Acteurs les plus actifs

**TURLA_** Ce groupe aurait ciblé les serveurs de messagerie Microsoft Exchange dans les secteurs de l'éducation, du gouvernement, de l'armée, de la recherche et de la pharmacie dans plus de 40 pays en 2019.[23]

**APT27_** Ce groupe aurait compromis les serveurs SharePoint d'organisations gouvernementales dans deux pays différents du Moyen-Orient.

**VICIOUS PANDA_** En avril 2020, l'administration publique mongole aurait été prise pour cible par ce groupe.[24]

**GAMAREDON_** Ce groupe aurait pris pour cible le ministère de la défense ukrainien dans une campagne d'hameçonnage ciblé à partir de décembre 2019.[25]



# Motivations

## _Pourquoi

Bien qu'il soit difficile de déterminer la motivation première d'une cyberattaque, il nous est toutefois possible de réaliser un classement en fonction du résultat de l'incident.

**Financier:** Le nombre d'incidents ayant entraîné le vol d'informations, de données et d'identifiants d'utilisateur est le plus élevé observé durant la période de référence. La plupart du temps, l'objectif consiste à voler des données/informations puis de les vendre sur le *dark web*. On peut également identifier d'autres utilisations de ces informations/données qui serviront notamment à lancer d'autres types d'attaques avec un tout autre résultat, comme l'espionnage ou la fraude financière. Plus de 620 millions de coordonnées de comptes ont été volées sur 16 sites web piratés puis mises en vente sur le célèbre marché parallèle Dream Market.

**Espionnage:** Ce mobile est à l'origine d'un nombre croissant d'attaques signalées, principalement en raison des tensions géopolitiques et commerciales actuelles. Le nombre d'incidents d'espionnage n'est pas important, mais leur taille et leur ampleur les placent en deuxième position dans la liste de l'ENISA répertoriant les cinq principales motivations. Parmi les incidents notables, citons celui rapporté en avril 2019, au cours duquel un employé de General Electric et un homme d'affaires chinois ont été accusés par le département de la Justice des États-Unis d'espionnage économique et du vol de secrets commerciaux de General Electric.[20] En outre, l'Agence France-Presse (AFP) a rapporté qu'Airbus avait été victime d'une campagne de cyberespionnage sophistiquée. Les attaquants auraient violé les systèmes informatiques de plusieurs fournisseurs d'Airbus avant de s'introduire dans les systèmes informatiques de l'entreprise.[21]

**Les cinq principales motivations sont: le gain financier, l'espionnage, les perturbations, la politique et les représailles.**

# Les principales motivations

La figure ci-dessous montre que l'aspect **financier** reste le principal mobile pour la plupart des cyberattaques. Dans certains cas, plusieurs motivations sont identifiables au sein d'une même attaque. Ainsi, l'espionnage, l'aspect politique, le gain financier et les perturbations sont souvent des mobiles combinés. De nombreux incidents proviennent de systèmes automatisés et sont transmis «à la demande», payés en cryptomonnaie. Parmi les services fournis figurent la distribution de rançongiciels (*ransomware*), la commande et le contrôle (C&C), le déni de service distribué (DDoS - *Distributed Denial of Service*), le pourriel et d'autres activités illicites.

# Vecteurs d'attaque

## _Comment

Les cyberattaques nécessitent en moyenne trois étapes pour atteindre les actifs de valeur d'une victime. En examinant les vecteurs d'attaque les plus fréquemment utilisés, il faut considérer en priorité le point d'entrée, le plan d'action et l'action sur les actifs. Il s'agit là des étapes les plus critiques auxquelles doivent correspondre des approches distinctes dans une stratégie de défense.

**Point d'entrée:** En 2019, les techniques les plus fréquemment utilisées pour lancer une cyberattaque ont été la force brute avec vol d'identifiants, l'ingénierie sociale, les erreurs de configuration et l'exploitation d'applications web. L'exploitation d'applications web, par exemple, a souvent été utilisée comme point d'entrée en raison du recours croissant à ce type d'applications pour transférer des données dans le nuage. Les erreurs de configuration du nuage et la mauvaise utilisation des systèmes ont été les principaux points d'entrée dans un grand nombre d'incidents. L'utilisation de l'ingénierie sociale pour planifier une attaque s'appuie sur des outils tels que l'hameçonnage et la compromission de la messagerie en entreprise (BEC)[16]. Parmi d'autres techniques moins fréquentes mais tout aussi importantes, on trouve l'exploitation des vulnérabilités (de systèmes non corrigés et «0-Day») et les portes dérobées des logiciels, souvent utilisées dans des attaques plus complexes et plus sophistiquées.

**Plan d'action**: L'installation d'un logiciel malveillant est la technique la plus largement utilisée pendant la phase «plan d'action». Une fois installé, il permet à l'adversaire de faire de la reconnaissance, de se déplacer dans les systèmes et réseaux de la victime, d'installer des outils supplémentaires comme un rançongiciel, de voler des données et de communiquer avec un serveur C&C.

# Les *cinq* actifs les plus recherchés par les cybercriminels

## 01_Propriété industrielle et secrets d'affaires

La propriété industrielle et les secrets d'affaires sont les actifs les plus prisés en raison de leur grande valeur pour leurs propriétaires, le marché et, dans certains cas, le monde criminel.

## 02_Informations classifiées de l'État/l'armée

Cet actif comprend toutes les informations qu'un État juge sensibles. En 2019, les tensions commerciales et diplomatiques entre les pays ont rendu ce type d'informations encore plus attrayantes.

## 03_Infrastructure des serveurs

L'infrastructure des serveurs est le premier actif sensible autre que des données. Dans de nombreuses attaques, l'objectif principal consiste à prendre le contrôle de l'infrastructure des serveurs de la victime.

## 04_Données d'authentification

Les données d'authentification sont de précieux actifs pour générer des profits, mais également dans le but de soutenir une attaque.

## 05_Données financières

Les données financières, comme les informations relatives aux cartes de crédit, aux opérations bancaires et aux paiements,
ont toujours de la valeur pour les cybercriminels.

# Veille stratégique

## _Quels sont les changements apportés dans le paysage depuis la pandémie de COVID-19?

En 2019, l'ENISA a continué à cartographier le paysage des menaces, aidant ainsi les décideurs et les responsables politiques à définir des stratégies pour défendre les citoyens, les organisations et le cyberespace. Ce travail s'inscrit dans le cadre de sa stratégie visant à fournir une veille stratégique à ses parties prenantes. Suite à une demande de la Commission européenne et des États membres, la nouvelle génération de télécommunications mobiles, ou 5G, a constitué le thème central de l'année 2019. **L'Agence continuera à couvrir ces thématiques du paysage des menaces et, en 2020**, l'accent sera placé sur l'intelligence artificielle.

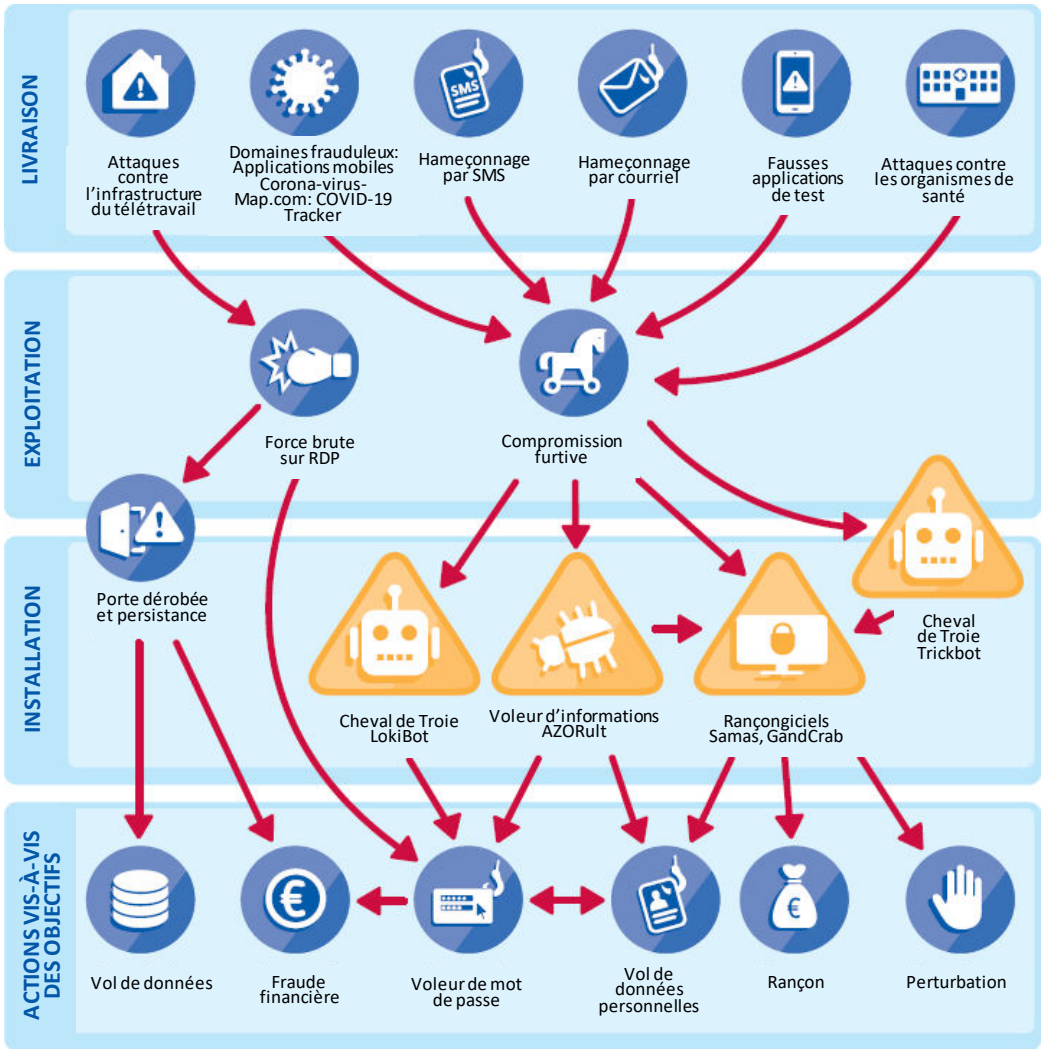
La pandémie de COVID-19 a été une période prolifique pour les acteurs malveillants qui ont mené des attaques prenant pour cible des domaines sensibles tels que des prestataires de services de santé et des télétravailleurs. L'ENISA dresse le paysage des menaces rencontrées pendant la pandémie et donne des conseils sur les mesures d'atténuation qui aideront à réduire l'exposition aux menaces.

L'Agence partage ses recommandations en matière de cybersécurité en rapport avec la pandémie de COVID-19 sur une variété de sujets, y compris le travail à distance, les achats en ligne et la cybersanté; en outre, elle fournit de précieux conseils de sécurité mis à jour pour les secteurs concernés.[32]

En pleine pandémie de COVID-19, l'**hôpital universitaire de Brno** (République tchèque) a été victime d'une cyberattaque[33] qui l'a obligé à transférer ses patients et à reporter les interventions chirurgicales. Cet incident est jugé critique car cet hôpital est l'un des plus grands laboratoires de dépistage de la COVID-19 en République tchèque.

# _Le paysage des menaces liées à la COVID-19

L'ENISA a préparé de nombreuses ressources en vue de la mise en place d'une campagne de sensibilisation. Elle a également partagé d'autres ressources internes et externes, dédiées aux experts de la cybersécurité, portant sur les questions de sécurité associées aux problématiques rencontrées au cours de la pandémie de COVID-19. Parmi ces ressources figurait une analyse sur les menaces les plus critiques au cours de cette période.



# Références


**1.** «MEGA Data Breach Exposed 773 Million Email Addresses and Passwords.» 19 janvier 2019. Latest Hacking News. https://latesthackingnews.com/2019/01/19/mega-data-breach-exposed-773-million-email-addresses-and-passwords/

**2.** «Largest Leak in History: Email Data Breach Exposes Over Two Billion Personal Records.» 8 avril 2019. CPO Magazine. https://www.cpomagazine.com/cyber-security/largest-leak-in-history-email-data-breach-exposes-over-two-billion-personal-records/

**3.** «LockerGoga Ransomware Disrupts Operations at Norwegian Aluminum Company.» 20 mars 2019. Recorded Future. https://www.recordedfuture.com/lockergoga-ransomware-insight/

**4.** «Researchers find 540 million Facebook user records on exposed servers.» 3 avril 2019. Tech Crunch. https://techcrunch.com/2019/04/03/facebook-records-exposed-server/

**5.** «Winnti: Attacking the Heart of the German Industry» 24 juillet 2019. Web.br. https://web.br.de/interaktiv/winnti/english/

**6.** «Cyber-attacks against 5 hospitals in Romania. CCR's website, also hacked» 20 juin 2019. Romanian Journal. https://www.romaniajournal.ro/society-people/cyber-attacks-five-hospitals-romania-ccr-website-hacked/

**7.** «Here's how ransomware attacks like the one on CityPower work – and why some victims end up paying criminals millions» 25 juillet 2019. Business Insider South Africa. https://www.businessinsider.co.za/ransomware-attack-on-citypower-johannesburg-why-victims-pay-criminals-2019-7

**8.** «Breach Saga: Bulgarian Tax Agency Fined; Pen Testers Charged.» 30 août 2019. Bank Info Security. https://www.bankinfosecurity.com/bulgaria-fines-tax-office-penetration-testers-charged-a-13000

**9.** «Breach Of Mastercard Loyalty Program Affected 90K Germans' Data» 23 août 2019. PYMNTS.com. https://www.pymnts.com/news/security-and-risk/2019/mastercard-loyalty-program-data-breach-germany/

**10.** «UniCredit confirms data breach» 28 octobre 2019. PrivSec Report. https://gdpr.report/news/2019/10/28/privacy-unicredit-confirms-data-breach/

**11.** «Prosegur Hacked: Spanish SOC Provider Hit by Ryuk Ransomware» 28 novembre 2019. Computer Business Review. https://www.cbronline.com/news/prosegur-hacked-ransomware

**12.** «Serious cyber-attack' on Austria's foreign ministry» 5 janvier 2020. BBC. https://www.bbc.com/news/world-europe-50997773

**13.** «Croatia's largest petrol station chain impacted by cyber-attack» 20 février 2020. ZDNet. https://www.zdnet.com/article/croatias-largest-petrol-station-chain-impacted-by-cyber-attack/

**14.** «European power grid organization says its IT network was hacked» 9 mars 2020. Cyberscoop. https://www.cyberscoop.com/european-entso-breach-fingrid/

**15.** «FullzHouse hackers pivot from phishing to Magecart card skimming attacks» 26 novembre 2019. ZDNet. https://www.zdnet.com/article/fullz-house-threat-group-pivots-from-phishing-to-magecart-card-skimming-attacks/

**16.** «FBI warns of cloud based BEC attacks.» 8 avril 2020. Info Security. https://www.infosecurity-magazine.com/news/fbi-warns-of-cloudbased-bec-attacks/

**17** «Microsoft Alerts Healthcare to Human-Operated Ransomware» 1er avril 2020. Dark Reading. https://www.darkreading.com/vulnerabilities---threats/microsoft-alerts-healthcare-to-human-operated-ransomware/d/d-id/1337463

**18.** «Verification.io suffers major data breach.» 15 mars 2019. PrivSec Report. https://gdpr.report/news/2019/03/15/verification-io-suffers-major-data-breach/

**19.** «Inside the Insynq attack: "We had to assume they were listening"» 8 août 2019. Accounting Today. https://www.accountingtoday.com/news/inside-the-insynq-ransomware-attack-we-had-to-assume-they-were-listening

**20.** «Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets». 23 avril 2019. USA DoJ. https://www.justice.gov/opa/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s-trade

**21.** «Airbus supply chain hacked in a cyberespionage campaign» 27 septembre 2019. CERT-UE. https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-190927-2.pdf

**22.** «Lazarus group's "AppleJeus" sequel targets cryptocurrency traders» 10 janvier 2020. The Cyber-Security Source. https://www.scmagazineuk.com/lazarus-groups-applejeus-sequel-targets-cryptocurrency-traders/article/1670446

**23** «Russian Nation-State Group Employs Custom Backdoor for Microsoft Exchange Server» 7 juillet 2019. Dark Reading. https://www.darkreading.com/application-security/russian-nation-state-group-employs-custom-backdoor-for-microsoft-exchange-server/d/d-id/1334628

**24.** «Vicious Panda: The COVID Campaign» 12 mars 2020. Check Point Research. https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/

**25.** «Gamaredon APT Improves Toolset to Target Ukraine Government, Military» 5 février 2020. Threat Post. https://threatpost.com/gamaredon-apt-toolset-ukraine/152568/

**26.** «Virus attacks Spain's defense intranet, foreign state suspected: paper» 26 mars 2019. Reuters. https://www.reuters.com/article/us-spain-security-cyberattack/virus-attacks-spains-defense-intranet-foreign-state-suspected-paper-idUSKCN1R7115

**27** «115 Million Pakistani Mobile Users Data Go on Sale on Dark Web» 10 avril 2020. Rewterz. https://www.rewterz.com/articles/115-million-pakistani-mobile-users-data-go-on-sale-on-dark-web

**28.** «Your business hit by a data breach? Expect a bill of $3.92 million» 23 juillet 2019. ZDNet. https://www.zdnet.com/article/your-business-hit-by-a-data-breach-expect-a-bill-of-3-92-million/

**29.** «Cyber Security Statistics for 2019» 21 mars 2019. Cyber Defense. https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019/

**30.** «Georgia "I'll Be Back" Cyber Attack Terminates TV, Takes Down 15,000 Websites.» 29 octobre 2019. Forbes. https://www.forbes.com/sites/daveywinder/2019/10/29/georgia-ill-be-back-cyber-attack-terminates-tv-takes-down-15000-websites/#1a5746347a48

**31.** «Half a million Zoom accounts for sale on the dark web.» 16 avril 2020. We Live Security by ESET. https://www.welivesecurity.com/2020/04/16/half-million-zoom-accounts-sale-dark-web/

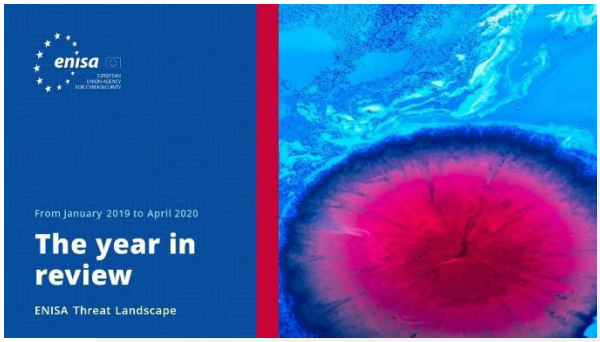
**32.** «ENISA COVID-19 Resources». ENISA. https://www.enisa.europa.eu/topics/wfh-covid19

**33.** «Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak» 17 mars 2020. Security Magazine. https://www.securitymagazine.com/articles/91921-brno-university-hospital-in-czech-republic-suffers-cyberattack-during-covid-19-outbreak

**34.** «Most malware in Q1 2020 was delivered via encrypted HTTPS connections». 25 juin 2020. Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

**35.** «Malware statistics and facts for 2020» 29 juillet 2020. Comparitech. https://www.comparitech.com/antivirus/malware-statistics-facts/

# Documents connexes




Rapport sur le Paysage des menaces de l'ENISA **Bilan de l'année**

Résumé des tendances en matière de cybersécurité observées entre janvier 2019 et avril 2020.

**LIRE LE RAPPORT**


Rapport sur le Paysage des menaces de l'ENISA
**Liste des 15 principales menaces**

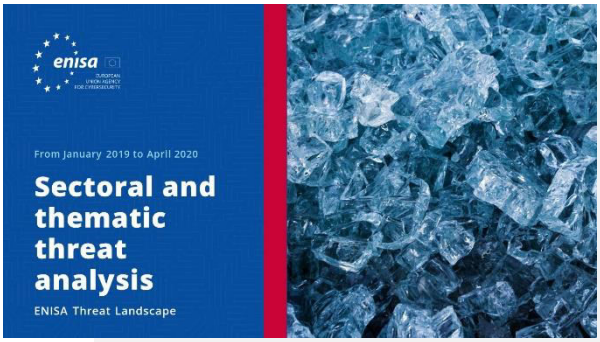
Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.

**LIRE LE RAPPORT**


Rapport sur le Paysage des menaces de l'ENISA
**Thèmes de recherche**

Recommandations concernant les thèmes de recherche provenant de divers secteurs de la cybersécurité et du renseignement sur la cybermenace.

**LIRE LE RAPPORT**




LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Analyse sectorielle et thématique de la menace**

Analyse contextualisée de la menace entre janvier 2019 et avril 2020.


LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Tendances émergentes**

Principales tendances en matière de cybersécurité observées entre janvier 2019 et avril 2020.


LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA
**Aperçu du renseignement sur la cybermenace**

L'état actuel du renseignement sur la cybermenace dans l'UE.

# Autres publications


## Roadmap on the Cooperation Between CSIRTS and LE

Feuille de route sur la coopération entre les CSIRT, en particulier avec les forces de l'ordre nationales et gouvernementales et le système judiciaire.

LIRE LE RAPPORT


## EU MS Incident Response Development Status Report

Étude visant à analyser le dispositif opérationnel actuel de réponse aux incidents dans les secteurs concernés par la directive NIS et à identifier les changements récents.

LIRE LE RAPPORT


## ENISA CSIRT maturity assessment model

Version actualisée du document «Challenges for National CSIRTs in Europe in 2016: Study on CSIRT Maturity» publiée par l'ENISA en 2017

LIRE LE RAPPORT

**«La sophistication des capacités de menace s'est accrue en 2019; de nombreux adversaires ont désormais recours aux codes d'exploitation, au vol d'identifiants et aux attaques en plusieurs étapes.»**

***ETL 2020***

# À propos

## L'Agence

L'Agence de l'Union européenne pour la cybersécurité (ENISA) est l'agence de l'Union dont la mission consiste 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 cybernétiques de demain. En partageant les connaissances, en renforçant les capacités et en organisant 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, au bout du compte, 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 https://www.enisa.europa.eu/media/enisa-en-francais/.


**Contributeurs**

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) et *tous les membres du groupe des parties prenantes CTI de l'ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT-UE) et Thomas Hemker.

**Éditeurs**

Marco Barros Lourenço (ENISA) et Louis Marinos (ENISA).

**Contact**

Pour toute question sur ce document, veuillez utiliser l'adresse enisa.threat.information@enisa.europa.eu.

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


**Nous aimerions avoir votre avis sur ce rapport!**
Merci de prendre un moment pour remplir le questionnaire. Pour accéder au formulaire, veuillez cliquer ici.

**Avis juridique**

Il convient de noter que, sauf mention contraire, la présente publication représente les points de vue et les interprétations de l'ENISA. Elle ne doit pas être interprétée comme une action légale de l'ENISA ou des organes de l'ENISA à moins d'être adoptée conformément au règlement (UE) nº 526/2013. Elle ne représente pas nécessairement l'état des connaissances et l'ENISA peut l'actualiser périodiquement.

Les sources de tiers sont citées de façon adéquate. L'ENISA n'est pas responsable du contenu des sources externes, notamment des sites web externes, mentionnées dans la présente publication.

La présente publication est uniquement destinée à des fins d'informations. Elle doit être accessible gratuitement. Ni l'ENISA ni aucune personne agissant en son nom n'est responsable de l'utilisation qui pourrait être faite des informations contenues dans la présente publication.



**ISBN:** 978-92-9204-354-4
**DOI:** 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grèce
Tél.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



https://www.enisa.europa.eu