



De janvier 2019 à avril 2020

Bilan de l'année

Paysage des menaces de l'ENISA

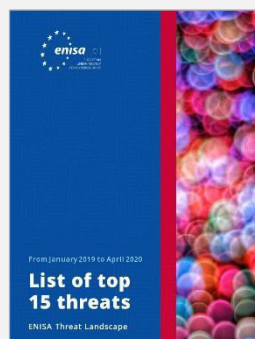
Avant de commencer

— Huit années d'étude du paysage des menaces

Cette année, l'Agence de l'Union européenne pour la cybersécurité (ENISA) célèbre le premier anniversaire du nouveau règlement sur la cybersécurité et la huitième édition du rapport sur le Paysage des menaces (ETL - *ENISA Threat Landscape*). Le règlement sur la cybersécurité¹ redéfinit et renforce le rôle de l'ENISA en lui attribuant un mandat permanent, des ressources supplémentaires et de nouvelles missions. En outre, un nouveau chapitre s'ouvre pour l'Agence avec l'arrivée d'un nouveau directeur exécutif, d'une nouvelle stratégie et d'une nouvelle structure organisationnelle. Avec tous ces changements, il était temps pour l'ETL de se transformer également et d'adopter une nouvelle structure assortie d'une présentation moderne et conviviale, en s'éloignant ainsi du rapport long et statique. Grâce à sa nouvelle identité visuelle et à son nouveau format, le rapport ETL est désormais un rapport numérique polyvalent, dynamique et simple d'utilisation, qui s'efforce de répondre aux attentes d'un public de plus en plus nombreux et exigeant.



ETL 2012



ETL 2020

Évolution du Paysage des menaces de l'ENISA de 2012 à 2020

Format de l'ETL

La présente édition analyse le paysage des menaces pour la période comprise entre janvier 2019 et avril 2020 et se structure comme suit:

BILAN DE L'ANNÉE. Ce rapport donne un aperçu général du paysage des menaces et expose les thèmes les plus importants abordés dans tous les autres rapports. Il fournit également la liste des 15 principales menaces recensées par l'ENISA, ainsi que ses conclusions et ses recommandations.

APERÇU DU RENSEIGNEMENT SUR LA CYBERMENACE. [↗](#) Ce rapport résume les principaux thèmes relatifs à la communauté du renseignement sur la cybermenace (CTI - *Cyber Threat Intelligence*) ainsi que ceux abordés dans différents forums.

ANALYSE SECTORIELLE ET THÉMATIQUE DE LA MENACE. [↗](#) Ce rapport résume les derniers travaux effectués par l'ENISA pour décrire le paysage des menaces relatif à des secteurs et technologies spécifiques. Cette année, nous présentons les résultats des travaux réalisés pour la 5G, l'Internet des objets (IoT - *Internet of Things*) et les voitures intelligentes.

PRINCIPAUX INCIDENTS DANS L'UE ET DANS LE MONDE. [↗](#) Ce rapport donne un aperçu des principaux incidents de cybersécurité qui se sont produits dans l'UE et dans le monde, en mettant en évidence les enseignements à en tirer.

THÈMES DE RECHERCHE. [↗](#) Ce rapport présente les principaux aspects liés à la recherche et à l'innovation en matière de cybersécurité.

TENDANCES ÉMERGENTES. [↗](#) Ce rapport identifie les tendances émergentes et se concentre sur les problématiques et les opportunités à venir dans le domaine de la cybersécurité.

LISTE DES 15 PRINCIPALES MENACES. [↗](#) Un rapport est rédigé pour chaque menace. Il comporte un aperçu général, les conclusions, les incidents majeurs, les statistiques, les vecteurs d'attaque et les mesures d'atténuation correspondantes.



Avant de commencer

— Méthodologie

Le contenu obtenu pour la rédaction du rapport ETL repose sur des informations de sources publiques, principalement de nature stratégique, et couvre plusieurs secteurs, technologies et contextes. Ce rapport se veut agnostique à l'égard de l'industrie et des fournisseurs; il fait référence ou cite les travaux de diverses recherches en matière de sécurité, des blogs et des articles de presse relatifs à la sécurité, tous clairement identifiés tout au long du texte par de nombreuses notes de fin de document.

Pour l'élaboration du rapport sur le Paysage des menaces de l'ENISA, nous avons suivi une double approche. Tout d'abord, nous avons procédé à une recherche documentaire approfondie de la littérature disponible provenant de sources publiques, comme des articles de presse, des avis d'experts, des rapports de renseignements, des analyses d'incidents et des rapports de recherche en matière de sécurité. Ensuite, nous avons interrogé des membres du groupe des parties prenantes de l'ETL, experts en la matière, ainsi que des membres appartenant à la communauté du renseignement sur la cybermenace de l'Union européenne. Ces derniers nous ont aidés à définir la liste des 15 principales menaces et à valider les hypothèses sur les tendances et les problématiques futures en matière de cybersécurité.

Nous tenons également à remercier les membres du groupe des parties prenantes de la CTI pour tout le soutien qu'ils nous ont apporté pour l'élaboration des rapports au cours de ces huit éditions. Les membres de ce groupe examinent et valident les analyses réalisées pour chaque rapport ETL et se prononcent sur la liste annuelle des 15 principales cybermenaces.



Nous aimerions avoir votre avis sur ce rapport!

Merci de prendre un moment pour remplir le questionnaire. Pour accéder au formulaire, veuillez cliquer [ici](#).

— Qui doit lire quoi

Le rapport ETL est en partie stratégique et en partie technique, avec des informations pertinentes pour les lecteurs spécialisés ou non. Il cible différents publics et adopte différents niveaux de langage technique, et ce en fonction du domaine et de l'importance du sujet pour des lecteurs non spécialisés. Le tableau ci-dessous décrit le type de public et de contenu pour chaque rapport ETL.

RAPPORT ETL	TYPE DE CONTENU	PUBLIC CIBLE
BILAN DE L'ANNÉE	Générique	Tous
APERÇU DU RENSEIGNEMENT SUR LA CYBERMENACE ↗	Spécifique	Membres et praticiens de la communauté de la CTI.
ANALYSE SECTORIELLE ET THÉMATIQUE DE LA MENACE ↗	Stratégique	Experts en gestion stratégique, responsables et décideurs politiques, analystes de risques, directeurs et responsables de la cybersécurité.
PRINCIPAUX INCIDENTS DANS L'UE ET DANS LE MONDE ↗	Stratégique	Experts en gestion stratégique, responsables et décideurs politiques, analystes de risques, gestionnaires et responsables des risques.
THÈMES DE RECHERCHE ↗	Stratégique	Experts en gestion stratégique, responsables et décideurs politiques, analystes de risques, gestionnaires et responsables des risques.
TENDANCES ÉMERGENTES ↗	Stratégique	Experts en gestion stratégique, responsables et décideurs politiques, analystes de risques, gestionnaires et responsables des risques.
LISTE DES 15 PRINCIPALES MENACES ↗	Technique	Responsables de la sécurité de l'information, responsables de la sécurité des systèmes d'information (RSSI), spécialistes en cybersécurité et analystes CTI.

Les 15 principales menaces

Principales menaces 2018		Évaluation des tendances
1	Logiciels malveillants (<i>malware</i>)	---
2	Attaques sur le web	↗
3	Attaques d'applications web	---
4	Hameçonnage (<i>phishing</i>)	↗
5	Déni de service	↗
6	Pourriels (<i>spam</i>)	---
7	Réseaux de machines zombies (<i>botnets</i>)	↗
8	Violations de données	↗
9	Menaces internes	↘
10	Manipulation physique, dommages, vol et perte	---
11	Fuites d'informations	↗
12	Usurpation d'identité	↗
13	Cryptominage (<i>cryptojacking</i>)	↗
14	Rançongiciels (<i>ransomware</i>)	↘
15	Cyberespionnage	↘





Principales menaces 2019-2020		Évaluation des tendances	Changement dans le classement
1	Logiciels malveillants (<i>malware</i>) ↗	---	---
2	Attaques sur le web ↗	---	↗
3	Hameçonnage (<i>phishing</i>) ↗	↗	↗
4	Attaques d'applications web ↗	---	↘
5	Pourriels (<i>spam</i>) ↗	↘	↗
6	Déni de service ↗	↘	↘
7	Usurpation d'identité ↗	↗	↗
8	Violations de données ↗	---	---
9	Menaces internes ↗	↗	---
10	Réseaux de machines zombies (<i>botnets</i>) ↗	↘	↘
11	Manipulation physique, dommages, vol et perte ↗	---	↘
12	Fuites d'informations ↗	↗	↘
13	Rançongiciels (<i>ransomware</i>) ↗	↗	↗
14	Cyberespionnage ↗	↘	↗
15	Cryptominage (<i>cryptojacking</i>) ↗	↘	↘

Légende: Tendances: ↘ En baisse, --- Stable, ↗ En hausse **Classement:** ↗ En hausse, --- Identique, ↘ En baisse ↘

— L'évolution du paysage

Les années 2019 et 2020 ont apporté d'importants changements dans le paysage des cybermenaces dont la description figure dans ces rapports. Deux faits distincts ont largement contribué à ces changements: les soudaines forces de transformation, uniques dans l'histoire, libérées par la **pandémie de maladie à coronavirus 2019 (COVID-19)**; et la tendance croissante continue des **capacités adverses avancées des auteurs de menaces**. Il est intéressant de noter que ces dernières sont venues amplifier l'impact de la pandémie de COVID-19 dans le cyberspace.

La pandémie de COVID-19 a forcé l'adoption à grande échelle de technologies visant à maîtriser différents aspects critiques de la crise, tels que la coordination des services de santé, la réponse internationale à la propagation de la COVID-19, l'adoption de régimes de télétravail, l'apprentissage à distance, les communications interpersonnelles, le contrôle des mesures de confinement, les téléconférences et bien d'autres encore. Face à cette situation, les chefs d'entreprise ont évalué les risques émergents liés à l'adoption (technologique) brutale, qui s'est matérialisée suite à la transformation imposée par la pandémie de COVID-19². Quant à la **cybersécurité, elle a été confrontée à un paradoxe puisqu'elle a été à la fois la problématique et l'opportunité de cette transformation**. Les changements imposés dans le paysage des technologies de l'information (TI) ont affaibli les mesures de cybersécurité existantes, faisant de leur adaptation rapide un défi. Parallèlement, la **cybersécurité constitue un vecteur de confiance dans les nouveaux cas d'utilisation des services numériques et elle a donc la possibilité de faciliter la transformation**.



En télétravail, **les spécialistes de la cybersécurité ont dû adapter les dispositifs de défense existants** à un nouveau modèle d'infrastructures, tout en essayant de minimiser l'exposition à un grand nombre d'attaques inédites dont les points d'entrée sont désormais les domiciles et autres appareils intelligents connectés à l'internet des employés. En même temps et sous forte pression, ils ont dû mettre en œuvre des solutions basées sur des composants auparavant moins fiables, comme l'accès à distance via l'internet public, les services en nuage, les services de diffusion vidéo en flux continu non sécurisés ainsi que les appareils et applications mobiles. Face à la pandémie de COVID-19, les mesures nécessaires pour garantir la sécurité tout en réduisant l'impact sur les entreprises ont poussé les organisations aux limites de leur capacité à répondre aux changements. En outre, si de nombreux modes opératoires se sont rapidement adaptés à l'évolution des modes de travail, **les professionnels de la cybersécurité se sont retrouvés à agir à la limite de leurs propres capacités.**

En peu de temps, les professionnels de la sécurité informatique ont dû répondre rapidement aux problématiques posées par le télétravail, comme les transferts de données d'entreprise dès lors que les employés utilisent leur connexion internet à domicile pour accéder à des applications basées sur le nuage, à des logiciels d'entreprise, à des visioconférences et au partage de fichiers.

Puisque la pandémie de COVID-19 n'est encore pas entièrement sous contrôle, et face à l'incertitude qui règne quant à sa propagation future, on s'attend à ce qu'elle continue de représenter un défi pour les professionnels de la cybersécurité. En outre, compte tenu du temps qui s'écoule avant que les incidents ne soient détectés et analysés, elle laissera son empreinte dans le paysage des cybermenaces pendant encore un long moment. La pandémie de COVID-19 a révélé que les personnes malveillantes avaient un niveau de capacité qui leur permettait de s'adapter rapidement à ces transformations. En 2019-2020, le *modus operandi* des adversaires s'est focalisé sur la personnalisation des vecteurs d'attaque. Au cours de la période considérée, parmi les principaux accomplissements des adversaires figurent des méthodes avancées de vol d'identifiants, le bourrage d'identifiants (*credential stuffing*), des attaques par hameçonnage très ciblé, des attaques d'ingénierie sociale avancées, des techniques avancées d'obfuscation des logiciels malveillants et l'intrusion plus importante des plateformes mobiles. Si les cybercriminels se mettent à combiner ces avancées avec l'intelligence artificielle et l'apprentissage automatique, nous assisterons à l'avenir à une augmentation des attaques réussies et des campagnes indétectables.

_ Résumé

La liste ci-dessous récapitule les principales tendances observées dans le paysage des cybermenaces au cours de la période considérée. Celles-ci sont également examinées en détail dans les différents rapports composant le paysage des menaces de 2020.

01_ La surface d'attaque en matière de cybersécurité continue de s'étendre alors que nous entrons dans une nouvelle phase de transformation numérique.

02_ Après la pandémie de COVID-19, il existera une nouvelle norme sociale et économique encore plus dépendante d'un cyberspace sécurisé et fiable.

03_ L'utilisation des plateformes de médias sociaux dans des attaques ciblées constitue une tendance sérieuse qui touche différents domaines et concerne différents types de menaces.

04_ Des attaques subtilement ciblées et persistantes sur des données de grande valeur (par ex., propriété intellectuelle et secrets d'État) sont méticuleusement planifiées et exécutées par des auteurs parrainés par des États.

05_ Des attaques lancées massivement, de courte durée et à large impact, sont utilisées pour atteindre de multiples objectifs, tels que le vol d'identifiants.



_ Résumé

06_ La motivation sous-tendant la majorité des cyberattaques reste financière.

07_ Les rançongiciels restent largement répandus avec des conséquences coûteuses pour de nombreuses organisations.

08_ De nombreux incidents de cybersécurité passent encore inaperçus ou prennent beaucoup de temps avant d'être détectés.

09_ Grâce à l'automatisation accrue de la sécurité, les organisations investiront davantage dans la préparation en utilisant le renseignement sur la cybermenace (*Cyber Threat Intelligence*) comme principale capacité.

10_ Le nombre de victimes d'hameçonnage ne cesse de croître car cette méthode exploite la dimension humaine, considérée comme le maillon le plus faible.

Avec tous les changements observés dans le paysage des cybermenaces et les problématiques créées par la pandémie de COVID-19, il reste encore beaucoup de chemin à parcourir avant que le cyberspace ne devienne un environnement fiable et sûr pour chacun.



_ Les citoyens de l'UE sont-ils davantage conscients des risques et des problématiques posés par le cyberspace?

La Commission européenne a préparé une enquête⁴ Eurobaromètre spéciale en 2019 dans le but de comprendre la sensibilisation, les expériences et les perceptions des citoyens de l'UE en matière de cybersécurité.



EUROBAROMÈTRE

Les résultats de cette enquête montrent que l'utilisation de l'internet en Europe continue de croître, en particulier par l'intermédiaire des smartphones, et que les citoyens sont davantage conscients des dangers potentiels qu'ils courent en ligne.

Selon les résultats de l'enquête, les préoccupations concernant la confidentialité et la sécurité en ligne ont déjà conduit plus de 9 internautes sur 10 à modifier leur comportement en ligne, généralement en refusant d'ouvrir les courriels de personnes inconnues, en installant des logiciels antivirus, en ne consultant que des sites web connus et fiables et en n'utilisant que leur ordinateur personnel.

Bien que ces résultats soient plutôt encourageants, de nombreux internautes tombent toujours dans les mailles de la fraude en ligne et de l'hameçonnage par courriel. Il en ressort que les personnes malveillantes utilisent des attaques sophistiquées qui sont de plus en plus difficiles à détecter et à éviter. Par conséquent, les stratégies d'atténuation doivent être régulièrement mises à jour pour tenir compte des derniers renseignements (CTI) disponibles sur les techniques d'attaque.





«Le paysage des menaces devient extrêmement difficile à cartographier. Non seulement les attaquants développent de nouvelles techniques pour échapper aux systèmes de sécurité, mais les menaces augmentent en complexité et en précision dans des attaques ciblées.»


ETL 2020

À quoi s'attendre

— Les auteurs parrainés par des États-nations sont susceptibles de





TENDANCE	DESCRIPTION	MENACE
	Continuer à utiliser le cyberspace pour lancer des attaques contre les processus électoraux de pays étrangers en menaçant les systèmes démocratiques et les droits de l'homme. ⁵	Attaques contre les droits de l'homme et les systèmes démocratiques
	Continuer à harceler les opposants et à surveiller leurs citoyens par la manipulation d'informations sur les réseaux sociaux, associée à des campagnes d'espionnage (<i>spywares</i>).	Attaques contre les droits de l'homme et les systèmes démocratiques
	Lancer des campagnes de désinformation sophistiquées ⁶ destinées à influencer les perceptions ou à manipuler les opinions en faveur d'un certain programme politique ou d'objectifs de spéculation financière.	Campagnes de désinformation
	Augmenter la course aux cyberarmes ⁷ dans le but de développer des capacités cybernétiques. Le cyberspace étant considéré comme un domaine de guerre, les États-nations sont susceptibles de se lancer dans la recherche de cyberarmes par le biais d'agents sponsorisés en vue d'un cyberconflit.	Course aux cyberarmes incontrôlée
	Poursuivre des objectifs stratégiques tels que: obtenir des secrets industriels par espionnage, obtenir des moyens de pression sur les prises de décisions politiques, financer le régime par la fraude financière, mener des opérations d'informations cybernétiques et, enfin, affaiblir ou démoraliser l'adversaire par des activités perturbatrices ou destructrices.	Vol de données

Les cyberdélinquants sont susceptibles de

TENDANCE	DESCRIPTION	MENACE
	Continuer à cibler les adolescents et les jeunes adultes avec des attaques de sextorsion (chantage par webcam) affectant d'abord psychologiquement puis physiquement les victimes. ⁸	Sextorsion (chantage par webcam)
	Augmenter le nombre d'attaques de cyberharcèlement pendant et après la pandémie de COVID-19 auprès d'adolescents qui utilisent encore davantage les plateformes numériques à des fins personnelles ou éducatives. ⁹	Cyberharcèlement



Les cybercriminels sont susceptibles de

TENDANCE	DESCRIPTION	MENACE
	Augmenter l'utilisation d'outils basés sur l'IA pour créer des contrefaçons très crédibles (formats image, audio et vidéo), communément appelées «hypertrucages», afin d'escroquer les entreprises.	Hypertrucage
	Améliorer les tactiques qui compromettent les processus métier pour obtenir des avantages financiers.	Compromission de processus métiers (BPC - Business Process Compromise)
	Diminuer un niveau de l'organisation (sous la direction) pour compromettre la messagerie d'entreprise.	Compromission de messagerie d'entreprise (BEC - Business E-mail Compromise)
	Augmenter l'utilisation des fournisseurs de services d'infogérance pour distribuer des logiciels malveillants.	Logiciels malveillants (malware)

Conclusions/recommandations politiques

- Au cours des dernières décennies, les décideurs politiques et les technologues vivaient dans deux mondes distincts et ne parlaient pas le même langage. Pour relever les défis de la numérisation, ceux-ci doivent désormais **travailler ensemble**, de A à Z, en développant une approche commune. La plupart des technologies actuelles étant liées au cyberspace, la contribution des experts en cybersécurité revêt une importance capitale dans nombre de ces discussions.
- Compte tenu de l'innovation technologique croissante et de l'expansion rapide du cyberspace, l'élaboration de politiques européennes de cybersécurité, à la fois efficaces et globales, est absolument essentielle. L'établissement de **politiques de cybersécurité matures** fournira la capacité de sécurité nécessaire à tous les niveaux de la société: gouvernements, infrastructures critiques, entreprises, secteur tertiaire et particuliers. La capacité de sécurité doit être efficace et flexible pour pouvoir relever les nouveaux défis qui se présentent et ainsi faire face à l'évolution constante du cyberspace.
- Étant donné le nombre croissant de parties prenantes dans l'UE et dans les États membres impliqués dans les activités de CTI, **la coopération et la coordination** de ces activités à l'échelle de l'UE sont primordiales. L'ENISA encouragera la coopération avec les différentes parties prenantes et tentera en premier lieu d'identifier les exigences en matière de CTI auprès de divers groupes de parties prenantes, en particulier au sein de l'UE (c.-à-d. la Commission, les organes, les agences et les États membres de l'UE).
- Le renseignement sur la cybermenace doit être considéré comme le principal outil de **préparation à la cybersécurité** et de facilitation des approches fondées sur les risques. L'intégration de ce renseignement aux processus de gestion de la sécurité aidera celui-ci à proliférer dans des domaines connexes et donnera davantage de flexibilité à des processus habituellement longs, comme la certification et l'évaluation des risques. En outre, il sera vu comme l'instrument qui permettra l'adoption de décisions d'urgence nécessaires à la gestion des crises.
- La pertinence du renseignement sur la cybermenace pour les décisions stratégiques et politiques est largement acceptée et considérée comme essentielle pour faciliter **la connexion avec les informations géopolitiques** et les systèmes cyberphysiques, ce qui permettra de l'intégrer dans les processus décisionnels à l'échelle de l'UE, mais aussi d'élargir son cadre à l'identification des menaces hybrides.



— Conclusions/recommandations économiques

- En 2019, un nombre croissant de **laboratoires d'essai et de cyber ranges**¹⁰ ont été mis à disposition sur site et dans des offres en nuage. Il s'agit de ressources importantes pour former le personnel, simuler des attaques et tester des stratégies de défense multiples. Le tout basé sur un environnement virtuel polyvalent.
- Bien que certains critères et exigences en matière de CTI aient été développés pour différents profils d'utilisateurs de CTI, **des exigences similaires** seront nécessaires pour d'autres produits, services et outils de CTI. Les fournisseurs de CTI devront prendre davantage en compte les exigences des utilisateurs pour faciliter l'adoption des produits et services de CTI.
- L'investissement dans certains concepts de base du renseignement sur la cybermenace, en particulier **la maturité de ce renseignement et la hiérarchie des menaces**, s'avère très utile pour l'utilisation de ce type de renseignement. Les fournisseurs devront orienter leurs offres en fonction de différents niveaux de maturité de CTI afin de faciliter l'utilisation efficace du CTI au sein d'organisations de différentes tailles et aux budgets variés.
- À long terme, il semble qu'**OpenCTI**¹¹ soit une bonne solution à la fragmentation des offres de CTI, étant donné sa capacité inhérente à intégrer des sources CTI de différents types dans un environnement d'outils unique. Les fournisseurs de CTI devront fournir les « passerelles » nécessaires à partir de leurs produits pour permettre leur intégration à OpenCTI. Le concept de *cyber range* a été défini pour la première fois en 2013 par l'Agence européenne de défense (AED), dans le rapport intitulé « *Common staff target for military cooperation on cyber ranges in the European Union* », comme un environnement polyvalent à l'appui de trois processus primaires: le développement, la garantie et la diffusion des connaissances.

— Conclusions et recommandations en matière de recherche et d'enseignement

- Il faudra que l'UE poursuive son investissement dans **la recherche et le développement en cybersécurité**, en mettant l'accent sur les initiatives de recherche à long terme et à haut risque. La recherche et l'innovation à long terme sont des pratiques coûteuses qui restent hors de portée de la plupart des organisations du secteur privé.
- Le développement des connaissances et des compétences en matière de cybersécurité est essentiel pour améliorer la préparation et la résilience. Il convient que l'UE continue à **renforcer ses capacités** en investissant dans des programmes de formation en matière de cybersécurité, dans la certification professionnelle ainsi que dans des exercices et des campagnes de sensibilisation.
- La recherche en cybersécurité doit inclure l'expertise de disciplines sociale, comportementale et économique. **La recherche pluridisciplinaire** en matière de cybersécurité doit être encouragée et incitée dans toute l'UE.
- Les résultats des projets de recherche dans le domaine de la cybersécurité, et en particulier du renseignement sur la cybermenace, doivent être évalués et cartographiés dans un contexte plus large afin d'identifier **les chevauchements et les lacunes**, puis de les comparer aux pratiques, services et produits commerciaux existants. La diffusion de ces résultats à la communauté d'utilisateurs sera ainsi facilitée.
- Il convient de développer des approches novatrices pour l'assimilation des connaissances en matière de CTI par domaines pouvant en bénéficier. **Les cyberranges, les menaces hybrides et les évaluations géopolitiques en sont des exemples**. Les synergies obtenues peuvent stimuler les cas d'utilisation et la qualité du contenu de manière multidirectionnelle.
- L'utilisation de l'**intelligence artificielle (IA)** et de l'apprentissage automatique dans le cadre du CTI devra faire l'objet d'une étude plus approfondie. Le nombre d'étapes manuelles dans l'analyse du CTI se verra ainsi réduit et la valeur des fonctions d'apprentissage automatique au sein des activités de CTI améliorée.
- La fourniture et l'utilisation de matériel de CTI en open source doivent être encouragées. **Le transfert de connaissances** sera ainsi facilité tout en réduisant le seuil des compétences requises en matière de CTI.

**«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

Références

1. «Règlement de l'UE sur la cybersécurité». Avril 2019. Parlement européen et Conseil de l'Union européenne <https://eur-lex.europa.eu/eli/reg/2019/881/oj>
2. «COVID-19 Risks Outlook: A Preliminary Mapping and its Implications». 19 mai 2020. WEF. <https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications>
3. «Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions. Lutter contre la désinformation concernant la COVID-19 – Démêler le vrai du faux». Juin 2020. Commission européenne. <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52020JC0008>
4. «Special Eurobarometer 499: Europeans' attitudes towards cybersecurity». 29 janvier 2020 https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG
5. «EUvsDosinfo» <https://euvsdosinfo.eu/european-elections-2019/>
6. «Manipulating Social Media to Undermine Democracy». 2017. Freedom House. <https://freedomhouse.org/report/freedom-net/2017/manipulating-social-media-undermine-democracy>
7. «Conceptualising Cyber Arms Races» 2016. NATO CCD COE. <https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf>
8. «How online "sextortion" drove one young man to suicide». 8 février 2018. Today. <https://www.today.com/parents/how-online-sextortion-drove-one-young-man-suicide-t122735>
9. «Cyberbullying may increase during COVID-19 pandemic, experts says». 30 mars 2020. Healio. <https://www.healio.com/news/pediatrics/20200330/cyberbullying-may-increase-during-covid19-pandemic-expert-says>
10. Le concept de *cyber range* a été défini pour la première fois en 2013 par l'Agence européenne de défense (AED), dans le rapport intitulé « *Common staff target for military cooperation on cyber ranges in the European Union* », comme un environnement polyvalent à l'appui de trois processus primaires: le développement, la garantie et la diffusion des connaissances.
11. Open CTI. <https://www.opentcti.io/en/>

«Le renseignement sur la cybermenace (CTI) s'est imposé dans le domaine de la cybersécurité comme un instrument essentiel pour améliorer la flexibilité et l'efficacité de la défense contre les cyberattaques.»

ETL 2020

Documents connexes



LIRE LE RAPPORT

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

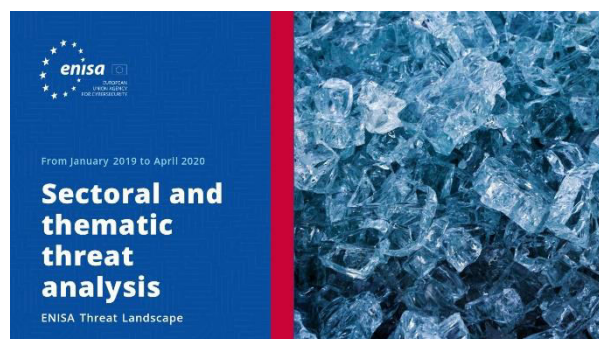
Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.



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

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.





Rapport sur le Paysage des menaces de l'ENISA Principaux incidents dans l'UE et dans le monde

Principaux incidents de cybersécurité survenus 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.

LIRE LE RAPPORT

— 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 rapport, veuillez utiliser l'adresse press@enisa.europa.eu.



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) n° 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.

Déclaration concernant les droits d'auteur

© Agence de l'Union européenne pour la cybersécurité (ENISA), 2020 Reproduction autorisée, moyennant mention de la source.

Droit d'auteur pour l'image de couverture: © Wedia. Pour toute utilisation ou reproduction de photos ou d'autres matériels non couverts par le droit d'auteur de l'ENISA, l'autorisation doit être obtenue directement auprès des titulaires du droit d'auteur.

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



Tous droits réservés. Copyright ENISA 2020.

<https://www.enisa.europa.eu>

