



De janvier 2019 à avril 2020

# Attaques sur le web

Paysage des menaces de l'ENISA



# Aperçu

Les attaques sur le web constituent une méthode attrayante par laquelle les auteurs de menace peuvent tromper leurs victimes en utilisant les systèmes et services du web comme vecteur d'attaque. Elles couvrent une vaste surface d'attaque, notamment en facilitant les URL ou les scripts malveillants pour diriger l'utilisateur ou la victime vers le site web souhaité ou en téléchargeant du contenu malveillant (attaques par point d'eau<sup>1</sup>, attaques de type «drive-by»<sup>2</sup>) et en injectant du code malveillant dans un site web légitime mais compromis dans le but de voler des informations (par ex., le *formjacking* ou vol de formulaire<sup>3</sup>), de gagner de l'argent, voire d'extorquer des fonds par le biais d'un rançongiciel (*ransomware*).<sup>4</sup> En plus de ces exemples, les failles d'exploitation des navigateurs internet et les compromissions de système de gestion de contenu sont d'importants vecteurs observés par différentes équipes de recherche et utilisés par des acteurs malveillants.

Les attaques par force brute, par exemple, visent un système d'exploitation en submergeant une application web de tentatives de connexion par nom d'utilisateur et mot de passe. Les attaques sur le web peuvent avoir une incidence sur la disponibilité des sites web, des applications et des interfaces de programmation (API - *Application Programming Interfaces*), portant ainsi atteinte à la confidentialité et à l'intégrité des données.



**«L'augmentation de la complexité des applications web et la généralisation de leurs services créent des difficultés pour les protéger contre des menaces aux motivations diverses, allant du préjudice financier à l'atteinte à la réputation, en passant par le vol d'informations critiques ou personnelles.»**

*ETL 2020*

# Chaîne de frappe


## Attaques sur le web

Reconnaissance

Armement

Livraison

Exploitation

 *Étape du processus d'attaque*

 *Ampleur de l'objectif*



Installation

Commande et  
contrôle

Actions vis-à-vis  
des objectifs

Mis au point par Lockheed Martin, le modèle de Cyber Kill Chain® s'inspire d'un concept militaire lié à la structure d'une attaque. Pour étudier un vecteur d'attaque en particulier, utilisez cette chaîne de frappe schématisée pour représenter chaque étape du processus puis référencer les outils, les techniques et les procédures utilisés par l'attaquant.

[EN SAVOIR PLUS](#)

## Une tendance généralisée

- **VOL DE DONNÉES D'UTILISATEURS VIA DES LOGICIELS MALVEILLANTS DE FORMJACKING.** L'injection de code malveillant dans les sites web est une technique bien connue employée par les cybercriminels. Des cas de *formjacking* (ou vol de formulaire) ont déjà été signalés, principalement dans le cadre d'activités de cryptominage. Cependant, selon un chercheur en sécurité<sup>4</sup>, les acteurs malveillants utilisent désormais cette technique pour s'attaquer aux données et coordonnées bancaires des utilisateurs. Les sites web visés sont restés infectés pendant 45 jours en moyenne. En mai 2019, ce même chercheur en sécurité a signalé le blocage de près de 63 millions de requêtes web malveillantes liées au *formjacking*.
- **«MAGECART» VA PLUS LOIN EN CIBLANT LA CHAÎNE D'APPROVISIONNEMENT.** Selon un chercheur en sécurité, l'une des sociétés françaises de médias numériques a été prise pour cible par l'acteur malveillant «Group12», qui a d'abord infecté l'inventaire publicitaire du site, en diffusant un code malveillant (*skimmer*), avant d'infecter les milliers de sites web qui hébergeaient les publicités.<sup>5</sup> Selon les observations, le fonctionnement de ce groupe a gagné en efficacité grâce à la mise en place de son infrastructure de *skimming* quelques mois seulement avant le début de la campagne. Par conséquent, tout utilisateur final risquait d'être infecté par la simple consultation d'un site web hébergeant l'une de ces publicités.<sup>6</sup>
- **PLATEFORMES DE COLLABORATION ET DE MESSAGERIE WEB.** Celles-ci deviennent des passerelles entre les acteurs malveillants et les victimes sur ce que l'on appelle la porte dérobée SLUB. En mars 2019, un chercheur en sécurité est tombé sur une campagne qui utilisait des attaques par point d'eau (*watering hole*) pour infecter les victimes en exploitant la vulnérabilité CVE-2018-81747. Cette attaque impliquait des procédés d'infection en plusieurs étapes. Le téléchargement d'un fichier DLL, exécuté via PowerShell, qui déclenche le téléchargement du logiciel malveillant et l'exécution de la porte dérobée principale, est un exemple du fonctionnement de ces procédés. À noter que le logiciel malveillant se connectait au service de messagerie d'un espace de travail Slack pour envoyer le résultat des commandes, qui étaient transmises via un morceau de code GitHub dans lequel l'attaquant ajoutait potentiellement les commandes.<sup>7,8</sup>



- **EXTENSION DE NAVIGATEUR, FRAUDE ET PUBLICITÉ MALVEILLANTE.** Un chercheur en sécurité a découvert une vaste campagne de publicité malveillante (*malvertising*) qui utilisait les extensions Google Chrome; celle-ci a touché environ 1,7 millions d'utilisateurs. Ces extensions Chrome cachaient la fonctionnalité publicitaire sous-jacente aux utilisateurs finaux pour finalement permettre au navigateur infecté de rester connecté à l'infrastructure de commande et de contrôle (C&C). Selon les conclusions de ce chercheur, cette campagne a connu une accélération entre mars et juin 2019, mais il est probable qu'elle existait bien longtemps avant cela.<sup>9</sup> Les observations d'un autre chercheur en sécurité ont démontré que l'activité du publiciel (*adware*) NewTab, qui facilite les extensions de navigateur, s'est accrue fin 2019.<sup>11</sup>
- **UTILISATION DE GOOGLE SITES POUR L'HÉBERGEMENT DE CHARGES UTILES FURTIVES.** Le logiciel malveillant (*malware*) connu sous le nom de «LoadPCBanker» (Win32.LoadPCBanker.Gen) a été découvert dans le modèle Classeurs de Google Sites (version classique de Google Sites). Selon un chercheur en sécurité, l'auteur a d'abord utilisé la version classique de Google Sites pour créer une page web et a ensuite facilité le modèle Classeurs pour héberger les charges utiles. Puis, il a utilisé le service SQL comme canal d'exfiltration pour envoyer et stocker les données des victimes.<sup>12,13</sup>
- **RANÇONGICIEL UTILISANT UN CONVERTISSEUR VIDÉO EN LIGNE COMME MOYEN DE TÉLÉCHARGEMENT FURTIF.** Selon un chercheur en sécurité, ShadowGate, autrement appelé la campagne WordJS, est actif depuis 2015 et prend pour cible les logiciels publicitaires ainsi que les sites web. En 2016, le kit d'exploitation Greenflash Sundown a été développé pour renforcer l'activité de cette campagne, et ce en injectant le kit dans des services publicitaires compromis et en diffusant un rançongiciel. En 2018, ShadowGate a été repéré; il délivrait depuis peu des cryptomineurs sur des serveurs en Extrême-Orient. La répartition de ShadowGate par pays est présentée à la figure 1 du présent rapport. Son activité a également été signalée par un autre chercheur en sécurité qui l'avait détectée sur [onlinevideoconverter\[.com\]](http://onlinevideoconverter.com), l'un des principaux sites web servant à la diffusion du kit d'exploitation.<sup>14,15,16,17,18</sup>

## Une tendance généralisée

- **LES SYSTÈMES DE GESTION DE CONTENU RESTENT UNE CIBLE IDÉALE.** Compte tenu de la popularité des systèmes de gestion de contenu auprès des internautes, ces systèmes constituent une cible attrayante pour les acteurs malveillants. Un chercheur en sécurité a relevé une augmentation de l'exploitation d'une vulnérabilité identifiée en 2018 (Drupalgeddon2 ) et visant la plateforme Drupal. De manière similaire, un autre chercheur en sécurité a remarqué une tendance aux exploitations de WordPress visant des vulnérabilités et des plugins tiers obsolètes. <sup>19,20</sup>
- **ATTAQUES PAR POINT D'EAU: UTILISATION DES FAILLES D'EXPLOITATION DES NAVIGATEURS INTERNET.** Un auteur de menace a été pris en train de commettre une attaque par point d'eau à l'aide d'un portail d'informations en langue coréenne. Lors de cette attaque, l'injection automatique d'un script malveillant (JavaScript) dans la page d'accueil du site web (en s'appuyant sur un second script) permettait de vérifier le navigateur de la victime puis d'exploiter une vulnérabilité de Google Chrome (CVE-2019-13720). En outre, en juillet 2019, on a découvert une nouvelle version du logiciel malveillant SLUB, qui est une porte dérobée, en train d'infecter le navigateur de la victime (vulnérabilité CVE-2019-0752 d'Internet Explorer) à l'aide d'un site web «point d'eau» spécifique. Dans le cadre d'une autre enquête, l'équipe de sécurité d'un développeur de logiciels a identifié un ensemble de sites web compromis qui avaient été utilisés dans des attaques par point d'eau pour exploiter les vulnérabilités de l'iPhone. <sup>21,22</sup>



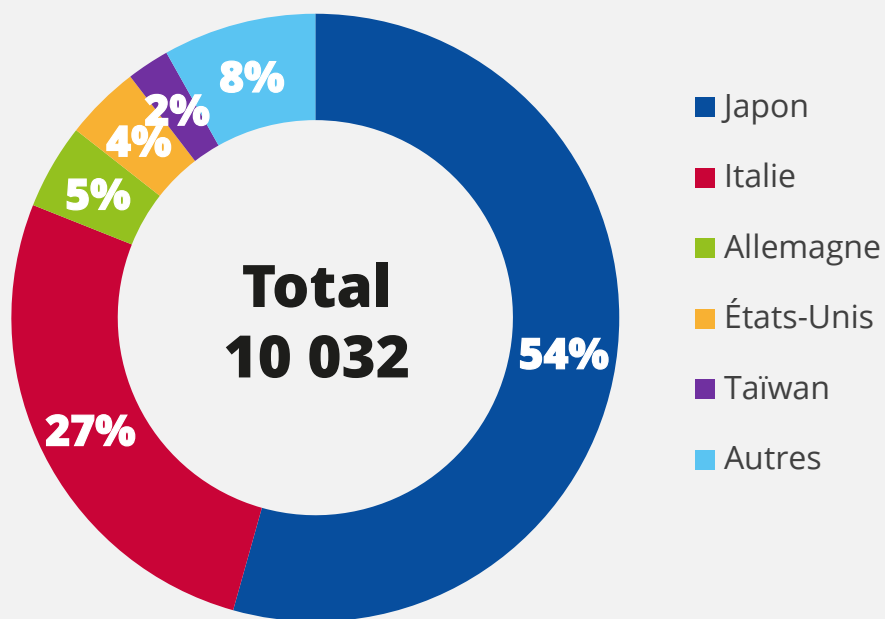


Figure 1: Répartition en pourcentage de ShadowGate par pays

# Vecteurs d'attaque

## Comment

- **DRIVE-BY DOWNLOADS OU TÉLÉCHARGEMENTS FURTIFS.** Ce vecteur d'attaque permet de télécharger des contenus malveillants sur l'appareil de la victime. Dans ce type d'attaque, il faut que l'utilisateur final consulte le site web légitime qui a été compromis. Pour ce faire, il suffit d'utiliser des scripts malveillants injectés dans le site web légitime, d'exploiter des failles du navigateur ou de rediriger officieusement l'utilisateur vers un site web compromis.<sup>25,26</sup>
- **ATTAQUES PAR POINT D'EAU.** Cette technique est utilisée pour des attaques ciblées à l'aide de kits d'exploitation dotés de fonctionnalités de furtivité. En d'autres termes, il s'agit du type d'attaque utilisée par un acteur malveillant souhaitant compromettre un groupe d'utilisateurs spécifiques par l'utilisation d'exploits ou d'autres contenus malveillants (par ex., des scripts ou des publicités) injectés dans le site web.<sup>27</sup>
- **FORMJACKING.** Avec cette technique, les pirates injectent du code malveillant dans les formulaires de paiement de sites web légitimes. Cette attaque sert principalement à s'emparer de données bancaires et autres informations à caractère personnel. Dans ce contexte, l'utilisateur saisit ses coordonnées bancaires ou les données de sa carte dans le portail de paiement du site d'e-commerce. Une fois les informations collectées et soumises, le script malveillant transmet simultanément les données au portail et à l'acteur malveillant. Ces informations sont ensuite utilisées à diverses fins criminelles: gain financier, extorsion et mise en vente sur les marchés parallèles.<sup>3,4</sup>
- **URL MALVEILLANTE.** Il s'agit d'un lien créé dans l'intention de distribuer un logiciel malveillant ou de mettre en œuvre une escroquerie. Ce processus implique de manipuler psychologiquement la victime par ingénierie sociale pour la persuader de cliquer sur l'URL malveillante qui sert ensuite à diffuser le *malware* ou le contenu malveillant pour ainsi compromettre sa machine.<sup>28</sup>



## Opération WizardOpium


Une vulnérabilité «0-Day» dans Google Chrome a été découverte en circulation lors d'attaques ciblées sur le web. Cette faille, enregistrée sous la référence CVE-2019-13720, concerne les versions antérieures à la version 78.0.3904.87 des systèmes Microsoft Windows, Mac et Linux. Le défaut se trouve dans le composant audio du navigateur web et la réussite de son exploitation est susceptible de provoquer l'exécution de code arbitraire.

Découverte par un chercheur en sécurité et référencée CVE-2019-13720, cette vulnérabilité «0-Day» n'a été attribuée à aucun auteur de menace particulier, mais on considère qu'elle fait partie de la campagne suivie sous le nom d'«Opération WizardOpium». En attendant, Google a publié une mise à jour pour la version 78.0.3904.87 de Chrome. Selon le chercheur, l'attaque profite d'une injection de type par point d'eau sur un portail d'informations en langue coréenne. Un code JavaScript malveillant inséré dans la page d'accueil permet de charger le script de profilage à partir d'un site à distance.<sup>23,24</sup>

Un exploit de navigateur est une forme d'exploitation utilisant un code malveillant qui tire parti des failles et des vulnérabilités du logiciel (système d'exploitation et navigateur) ou des plugins associés pour finalement accéder à l'appareil de la victime.

## Actions proposées

- Suivre un bon processus et un bon programme de gestion des correctifs.
- Mettre à jour le navigateur internet et les plugins associés pour les actualiser et corriger les vulnérabilités connues.
- Appliquer les correctifs aux pages basées sur le système de gestion de contenu et au portail pour éviter les plugins et modules complémentaires non vérifiés.
- S'assurer que les terminaux et les logiciels installés sont mis à jour, corrigés et protégés.
- Isoler les applications (liste blanche des applications) et créer un bac à sable (*sandbox*) pour réduire le risque d'attaques par compromission de type «drive-by». Par exemple, la technique d'isolation du navigateur peut permettre de protéger les terminaux contre l'exploitation du navigateur et les attaques par compromission de type «drive-by». [29,30,31](#)
- Pour les propriétaires de sites web, le durcissement des serveurs et des services est une approche proactive visant à atténuer les attaques sur le web. Il s'agit notamment de contrôler la version des scripts de contenu ainsi que d'analyser les fichiers et les scripts hébergés localement pour le serveur ou le service web. [32](#)
- La restriction du contenu web est une autre technique de protection contre les attaques sur le web. L'utilisation d'outils de facilitation, tels que bloqueurs de publicités (*adblockers*) ou bloqueurs de JavaScript, permettra également de limiter l'exécution possible de codes malveillants lors de la consultation de certains sites web. [29,30](#)
- Surveiller la messagerie web et filtrer le contenu pour détecter et empêcher la diffusion d'URL et de fichiers/charges utiles malveillants.



**«Les attaques sur le web comprennent généralement des techniques parmi lesquelles figurent l'injection SQL, la modification des paramètres, l'injection de code indirect (*cross-site scripting*), la traversée de répertoires (*path traversal*) et la force brute, dont le but consiste à compromettre un système ou une application.»**

ETL2020



# Références

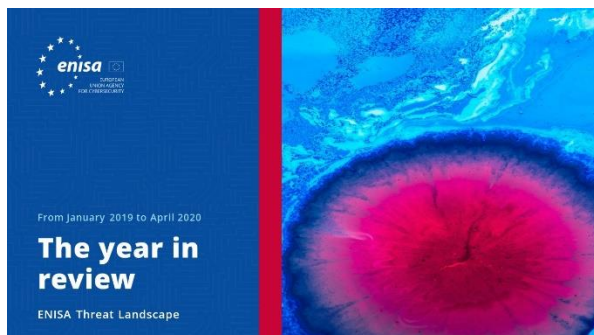
1. «Watering Hole» Proofpoint. <https://www.proofpoint.com/uk/threat-reference/watering-hole>
2. «What Is a Drive-By Download?» Kaspersky. <https://www.kaspersky.com/resource-center/definitions/drive-by-download>
3. «Formjacking: Major Increase in Attacks on Online Retailers», Broadcom. <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/formjacking-attacks-retailers>
4. «What is Formjacking and How Does it Work?», Norton. <https://us.norton.com/internetsecurity-emerging-threats-what-is-formjacking.html>
5. «Magecart's 7 Groups: Hackers Dropping Counter-Intelligence Code in JavaScript Skimmers». 14 novembre 2018. CBR. <https://www.cbronline.com/in-depth/magecart-analysis-riskiq>
6. «How Magecart's Web-Based Supply Chain Attacks are Taking Over the Web». 10 mars 2019. CBR. <https://www.cbronline.com/analysis/riskiq-magecart-supply-chain-attacks>
7. «CVE-2018-8174 Detail» 5 septembre 2019. NIST. <https://nvd.nist.gov/vuln/detail/CVE-2018-8174>
8. «Join a Slack workspace». Slack. <https://slack.com/intl/en-gb/help/articles/212675257-Join-a-Slack-workspace>
9. «New SLUB Backdoor Uses GitHub, Communicates via Slack» 7 mars 2019. Trend Micros. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/>
10. «Security Researchers Partner With Chrome To Take Down Browser Extension Fraud Network Affecting Millions of Users» 13 février 2020. Cisco Duo Security. <https://duo.com/labs/research/crxcavator-malvertising-2020>
11. «Mac threat detections on the rise in 2019» 16 décembre 2019. Malware Bytes. <https://blog.malwarebytes.com/mac/2019/12/mac-threat-detections-on-the-rise-in-2019/>
12. «File Cabinet», Google. <https://sites.google.com/site/tiesitestutorial/create-a-page/file-cabinet>
13. Google Sites. <https://sites.google.com/site/>
14. «Talos ShadowGate Take Down: Global Malvertising Campaign Thwarted» 1<sup>er</sup> septembre 2016. <https://blog.talosintelligence.com/2016/09/shadowgate-takedown.html>
15. «New Bizarro Sundown Exploit Kit Spreads Locky» Trend Micro. <https://blog.trendmicro.com/trendlabs-security-intelligence/new-bizarro-sundown-exploit-kit-spreads-locky/>
16. «Incoming! Multiple Popular Websites Attacked for Cryptocurrency Mining via GreenFlash Sundown Exploit Kit» 360 Blog. <https://blog.360totalsecurity.com/en/incoming-multiple-popular-websites-attacked-cryptocurrency-mining-via-greenflash-sundown-exploit-kit/>
17. «ShadowGate Returns to Worldwide Operations With Evolved Greenflash Sundown Exploit Kit» 27 juin 2019. Trend Micro. <https://blog.trendmicro.com/trendlabs-security-intelligence/shadowgate-returns-to-worldwide-operations-with-evolved-greenflash-sundown-exploit-kit/>





18. «GreenFlash Sundown exploit kit expands via large malvertising campaign» 26 juin 2019. Malware Bytes. <https://blog.malwarebytes.com/threat-analysis/2019/06/greenflash-sundown-exploit-kit-expands-via-large-malvertising-campaign/>
19. «FAQ about SA-CORE-2018-002» 28 mars 2018. Drupal. <https://groups.drupal.org/security/faq-2018-002>
20. «Drupalgeddon2 still used in attack campaigns» 7 octobre 2019. Akamai. <https://blogs.akamai.com/sitr/2019/10/drupalgeddon2-still-used-in-attack-campaigns.html>
21. «Trustwave Global Security Report 2019», 2019. Trustwave.
22. «Stable Channel Update for Desktop» 31 octobre 2019. [https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop\\_31.html](https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html)
23. «Chrome 0-day exploit CVE-2019-13720 used in Operation WizardOpium». 1<sup>er</sup> novembre 2019. Kaspersky. <https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium/94866/>
24. «CVE-2019-13720 flaw in Chrome exploited in Operation WizardOpium attacks» 1<sup>er</sup> novembre 2019. Security Affairs. <https://securityaffairs.co/wordpress/93278/hacking/cve-2019-13720-lazarus-attacks.html>
25. «Web Browser-Based Attacks». Morphisec. <https://www.morphisec.com/hubfs/1111/briefs/BrowserAttacksBrief-190327.pdf>
26. «The 5 most common cyber attacks in 2019». 9 mai 2019. IT Governance. <https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks>
27. «Exploit Kits: Their Evolution, Trends and Impact». 7 novembre 2019. Cynet. <https://www.cynet.com/blog/exploit-kits-their-evolution-trends-and-impact/>
28. «Web-Based Threats: First Half 2019». 1<sup>er</sup> novembre 2019. Palo Alto. <https://unit42.paloaltonetworks.com/web-based-threats-first-half-2019/>
29. «Mitigating Drive-by Downloads» Avril 2020. ACSC. <https://www.cyber.gov.au/publications/mitigating-drive-by-downloads>
30. «MITRE ATT&CK: Drive-by compromise» 5 décembre 2019. MITRE. <https://resources.infosecinstitute.com/mitre-attck-drive-by-compromise/#gref>
31. «Protecting users from web-based attacks with browser isolation» 26 septembre 2019. Shi Blog – Security Solutions. <https://blog.shi.com/solutions/protecting-users-from-web-based-attacks-with-browser-isolation/>
32. «[https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es\\_p=9346257](https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es_p=9346257)». 11 avril 2019. Broadcom. [https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es\\_p=9346257](https://symantec-enterprise-blogs.security.com/blogs/feature-stories/istr-2019-cyber-skimming-payment-card-data-hits-big-time?es_p=9346257)

# 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

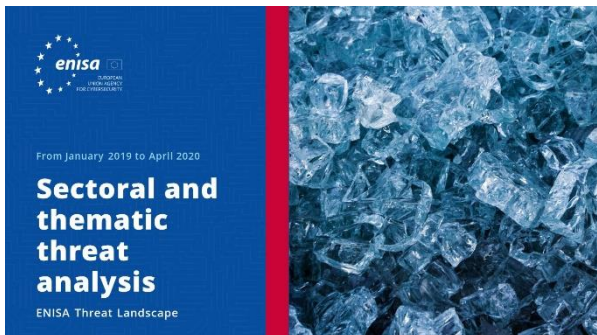


## Rapport sur le Paysage des menaces de l'ENISA **Thèmes de recherche**

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.

# 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](mailto: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](mailto: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) 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](mailto:info@enisa.europa.eu)  
[www.enisa.europa.eu](http://www.enisa.europa.eu)



Tous droits réservés. Copyright ENISA 2020.

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

