enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

FR

De janvier 2019 à avril 2020

Le cyberespionnage

Paysage des menaces de l'ENISA

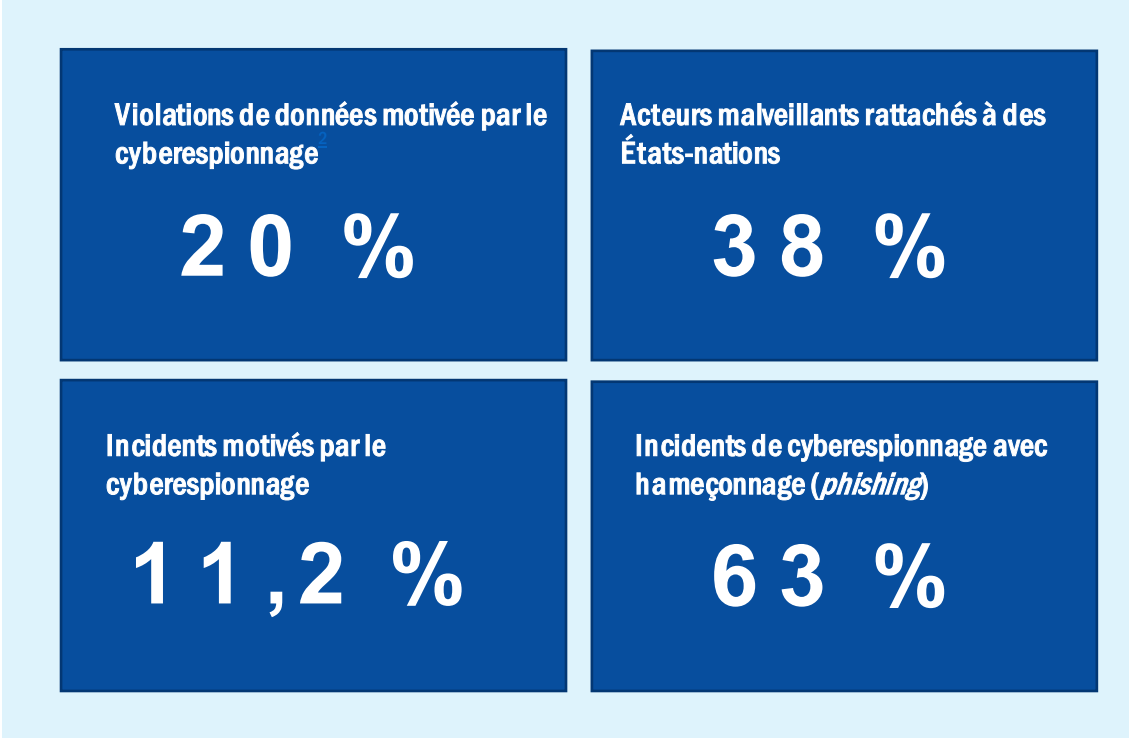
Aperçu

Considéré à la fois comme une menace et un mobile dans la stratégie de cybersécurité, le cyberespionnage se définit comme «l'utilisation des réseaux informatiques pour obtenir l'accès illicite à des informations confidentielles, généralement détenues par un gouvernement ou une autre organisation».[1]

En 2019, de nombreux rapports ont révélé que les organisations mondiales considéraient le cyberespionnage. (ou espionnage parrainé par un État-nation) comme une menace croissante touchant les secteurs industriels ainsi que les infrastructures critiques et stratégiques du monde entier, notamment les ministères, les compagnies ferroviaires, les opérateurs de télécommunications, les sociétés d'approvisionnement en énergie, les hôpitaux et les banques. Le cyberespionnage se concentre sur des enjeux géopolitiques et sur le vol de secrets d'État, de secrets d'affaires, de droits de propriété intellectuelle et de renseignements exclusifs dans des domaines stratégiques. Il mobilise également des acteurs de l'économie, de l'industrie et des services de renseignement extérieur, ainsi que des acteurs travaillant en leur nom. Dans un récent rapport, les analystes du renseignement sur la menace n'ont pas été étonnés d'apprendre que 71 % des organisations traitaient le cyberespionnage, ainsi que d'autres menaces, comme une «boîte noire» et qu'elles en apprenaient encore tous les jours sur le sujet.

En 2019, **le nombre de cyberattaques parrainées par des États-nations et ayant pour cible l'économie s'est accru; il est d'ailleurs probable que cette tendance à la hausse se poursuive**. Pour être plus précis, les attaques parrainées par des États-nations et autres attaques menées par des adversaires contre l'Internet industriel des objets (IIoT - *Industrial Internet of Things*) se multiplient dans les secteurs des services publics, du pétrole et du gaz naturel et de la fabrication. En outre, les cyberattaques menées par des groupes de menaces ciblées avancées (APT - *Advanced Persistant Threat*) indiquent que les attaques financières sont souvent motivées par l'espionnage. À l'aide de tactiques, techniques et procédures (TTP) semblables à celles de leurs homologues en matière d'espionnage, des groupes comme Cobalt, Carbanak et FIN7 auraient réussi à prendre pour cible de grands établissements financiers et des chaînes de restaurants.

- La commission des affaires étrangères du Parlement européen a appelé les États membres à créer un centre de cyberdéfense et à travailler de concert sur leur défense commune. Elle a déclaré que «l'environnement stratégique de l'Union se détériore [...] afin de relever la multitude de défis qui affectent directement ou indirectement la sécurité de ses États membres et de ses citoyens: que les questions qui concernent la sécurité des citoyens de l'UE comprennent: les conflits armés aux frontières orientales et méridionales du continent européen, et les États fragiles; le terrorisme - et en particulier le djihadisme -, les cyberattaques et les campagnes de désinformation; l'ingérence étrangère dans les processus politiques et électoraux européens».[42]
- Motivés par des gains financiers, politiques ou idéologiques, les auteurs de menace concentreront de plus en plus leurs attaques sur des réseaux de fournisseurs dont les programmes de cybersécurité sont faibles. Les cyberespions ont lentement modifié leurs modèles d'attaque pour exploiter des partenaires logistiques de tierce et quatrième parties.[1]



Incidents

- Le ministère sud-coréen de la défense nationale a annoncé que des pirates inconnus avaient mis en péril les systèmes informatiques du bureau du ministère chargé des marchés publics.[3]
- Le département de la justice des États-Unis a annoncé le déploiement d'une opération parrainée par un État étranger, par l'intermédiaire d'un réseau de machines zombies (*botnet*), dans le but de perturber des entreprises cibles dans les secteurs des médias, de l'aérospatiale, de la finance et des infrastructures critiques.[16]
- La société norvégienne Visma, spécialisée dans les logiciels, a révélé qu'elle avait été prise pour cible par des pirates informatiques qui avaient essayé de voler des secrets d'affaires à ses clients.[4]
- Des individus ont été arrêtés alors qu'ils s'apprêtaient à accéder aux systèmes informatiques de plusieurs partis politiques et du parlement fédéral australien.[17]
- L'entreprise aérospatiale européenne Airbus a révélé qu'elle avait été la cible de pirates informatiques apparemment parrainés par un État-nation, ces derniers ont fait main basse sur des informations personnelles et des identifiants appartenant à de nombreux employés.[19]
- Suite à une attaque contre les forces militaires indiennes au Cachemire, des pirates informatiques pakistanais ont pris pour cible près de 100 sites web et systèmes critiques du gouvernement indien.[5]
- La commission électorale nationale d'Indonésie a indiqué que des individus chinois et russes avaient consulté la base de données des électeurs avant les élections présidentielles et législatives prévues dans le pays.[20]
- À l'approche des élections européennes du mois de mai, plusieurs instances gouvernementales européennes ont été prises pour cible par des pirates informatiques étrangers.[21]
- L'*Australian Signal Directorate* a révélé avoir mené des cyberattaques contre l'EIIL au Moyen-Orient.[22]
- La police finlandaise a enquêté sur une attaque par déni de service dirigée contre le service web utilisé pour publier les résultats du scrutin des élections en Finlande.[6]
- Le bureau d'*Amnesty International* à Hong Kong a annoncé qu'il avait été victime d'une cyberattaque.[23]
- Les forces de défense israéliennes ont lancé une attaque aérienne sur le Hamas suite à leur tentative de piratage ratée de cibles israéliennes.[7]

- Un réseau iranien de sites et comptes internet aurait été utilisé pour diffuser de fausses informations sur les États-Unis, Israël et l'Arabie saoudite.[24]
- Des agences gouvernementales croates ont été visées par une série d'attaques menées par des pirates informatiques non identifiés parrainés par un État. Les logiciels malveillants en cause, Empire Backdoor et SilentTrinity, n'avaient jusqu'alors jamais été rencontrés.[26]
- La Libye a arrêté deux hommes accusés de collaborer avec une «usine à trolls» russe pour influencer les élections dans plusieurs pays d'Afrique.[27]
- Plusieurs grands groupes industriels allemands, dont BASF, Siemens et Henkel, ont annoncé qu'ils avaient été victimes d'une campagne de piratage parrainée par un État.[28]
- Un groupe parrainé par un État aurait mené une série de cyberattaques contre des journalistes, des universitaires, des avocats, des militants des droits de l'homme et des hommes politiques égyptiens.[8]
- Des diplomates et des utilisateurs russophones très en vue en Europe de l'Est ont été pris pour cible par un groupe de pirates informatiques parrainé par un État à l'aide d'un logiciel malveillant appelé Attor.[29]
- On a découvert qu'une société israélienne de cybersécurité avait vendu un espiogiciel (*spyware*) et que celui-ci avait été utilisé pour cibler de hauts responsables gouvernementaux et militaires dans au moins 20 pays grâce à l'exploitation d'une vulnérabilité dans WhatsApp.[32]
- On a appris qu'une campagne menée pendant sept ans par un groupe d'espions hispanophones non identifiés avait abouti au vol de fichiers cartographiques sensibles de hauts responsables de l'armée vénézuélienne.[10]
- Un groupe de cyberespionnage parrainé par un État aurait mené une campagne d'hameçonnage visant des agences gouvernementales et des entreprises publiques chinoises pour obtenir des informations ayant trait aux échanges économiques, aux questions de défense et aux relations internationales.[33]
- Le ministère tchèque des affaires étrangères a fait l'objet d'une cyberattaque lancée par un État étranger indéterminé.[34]
- Un acteur non-étatique a pris pour cible le parti travailliste britannique (*Labour Party*) en lançant une importante attaque par déni de service distribué qui a temporairement mis hors ligne les systèmes informatiques du parti à l'approche des élections nationales.[36]

Incidents

L'affaire General Electric

Xiaoqing Zheng, citoyen américain d'origine chinoise, a été accusé d'espionnage contre General Electric (GE). M. Zheng aurait volé des secrets technologiques portant sur les turbines de GE puis les aurait fournis à un homme d'affaires chinois qui, à son tour, les aurait transmis à un fonctionnaire chinois. M. Zheng a travaillé pour GE de 2008 à 2018.[15]

Le département de la justice des États-Unis a accusé les deux hommes d'avoir volé des informations pour servir leurs propres intérêts commerciaux dans deux sociétés de recherche et développement de turbines (Liaoning Tianyi Aviation Technology Co Ltd et Nanjing Tianyi AVI Tech Co Ltd).[47]

Le mode opératoire de cet auteur de menace interne consistait à:

- copier les secrets sur une clé USB jusqu'à ce que GE bloque l'utilisation de ces périphériques;
- chiffrer les secrets et utiliser la stéganographie pour dissimuler les fichiers de données dans le code binaire de fichiers photos numériques;
- brancher un iPhone à l'ordinateur professionnel pour copier les images;
- envoyer les fichiers vers son adresse électronique personnelle.

Mesures d'atténuation

Cette menace ayant un caractère global, plusieurs mesures d'atténuation recommandées pour d'autres menaces dans le présent rapport peuvent être utilisées dans le cadre des contrôles d'atténuation de base suivants[2]:

- Identifier les rôles critiques au sein de l'organisation et estimer leur exposition aux risques d'espionnage. Évaluer ces risques en fonction des informations professionnelles (c.-à-d. la veille économique).
- Élaborer des politiques de sécurité qui s'adaptent aux contrôles de sécurité des ressources humaines, de l'entreprise et des opérations afin d'atténuer les risques. Celles-ci doivent inclure des règles et des pratiques en matière de sensibilisation, de gouvernance d'entreprise et d'opérations de sécurité.
- Établir des pratiques d'entreprise pour communiquer les règles élaborées au personnel et le former à celles-ci.
- Élaborer des critères d'évaluation (ICP) pour évaluer le fonctionnement et les adapter aux changements ultérieurs.
- Créer une liste blanche pour les services applicatifs critiques en fonction du niveau de risque évalué.
- Évaluer les vulnérabilités et appliquer régulièrement des correctifs aux logiciels, en particulier pour les systèmes se trouvant sur le périmètre.
- Mettre en œuvre le principe du «besoin d'en connaître» pour définir des droits d'accès et établir des contrôles pour surveiller l'utilisation abusive de profils privilégiés.
- Mettre en place un filtrage de contenu pour tous les canaux d'entrée et de sortie (par ex., messagerie électronique, web, trafic réseau).

Références

1. «Cyber Threatscape Report. 2019.» IDefense - Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

2. «Data Breach Investigations Report 2020» DBR & Verizon. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf

3. Catalin Cimpanu. «Hackers breach and steal data from South Korea's Defense Ministry» 16 janvier 2019. ZDNet. https://www.zdnet.com/article/hackers-breach-and-steal-data-from-south-koreas-defense-ministry/

4. Jack Stubbs. «China hacked Norway's Visma to steal client secrets: investigators» 6 février 2019. Reuters. https://www.reuters.com/article/us-china-cyber-norway-visma/china-hacked-norways-visma-to-steal-client-secrets-investigators-idUSKCN1PV141

5. Kate Fazzini. «In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides». 28 février 2019. CNBC. https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html

6. Kati Pohjanpalo. «Finland Detects Cyber Attack on Online Election-Results Service». 10 avril 2019. Bloomberg.

https://www.bloomberg.com/news/articles/2019-04-10/finland-detects-cyber-attack-on-online-election-results-service

7. Lily Hay Newman «What Israel's Strike on Hamas Hackers Means For Cyberwar» 5 juin 2019. Wired. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

8. «Egypt Is Using Apps to Track and Target Its Citizens, Report Says» 3 octobre 2019. The New York Times. https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html

9. Colin Lencher. «Huawei accuses the US of "launching cyber attacks" against the company» 4 septembre 2019. The Verge. https://www.theverge.com/2019/9/4/20849092/huawei-cyberattacks-us-government-netowrks-employee-harassment

10. Catalin Cimpanu «A cyber-espionage group has been stealing files from the Venezuelan military» 5 août 2019. ZDNet. https://www.zdnet.com/article/a-cyber-espionage-group-has-been-stealing-files-from-the-venezuelan-military/

11. Catalin Cimpanu. «Croatian government targeted by mysterious hackers» 5 juillet 2019. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

12. Michael McGowan. «China behind massive Australian National University hack, intelligence officials say» 6 juin 2019. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

13. «General election 2019: Labour Party hit by second cyber-attack» 12 novembre 2019. BBC. https://www.bbc.com/news/election-2019-50388879

14. Nicole Perlroth, Matthew Rosenberg. «Russians Hacked Ukrainian Gas Company at Center of Impeachment» 13 janvier 2020. The New York Times. https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html

15. Danny Bradbury. «GE Engineer Charged for Novel Data Theft» 24 avril 2019. Info Security. https://www.infosecurity-magazine.com/infosec/ge-engineer-charged-data-theft-1/

16. «U.S. announces disruption of "Joanap" botnet linked with North Korea». 30 janvier 2019. CyberScoop. https://www.cyberscoop.com/joanap-botnet-north-korea-department-of-justice/

17. «The cyber attack on Parliament was done by a "state actor" — here's how experts figure that out». 20 février 2019. ABC News. https://www.abc.net.au/news/2019-02-20/cyber-activists-or-state-actor-attack-how-experts-tell/10825466

18. «While Trump was meeting with Kim Jong Un in Vietnam, North Korean hackers reportedly attacked targets in the US». 5 mars 2019. Business Insider. https://www.businessinsider.com/north-korean-hackers-trump-kim-meeting-mcafee-2019-3

19. «Airbus hit by series of cyber attacks on suppliers». 26 septembre 2019. France 24. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

20. «Indonesia Says Election Under Attack From Chinese, Russian Hackers». 12 mars 2019. Bloomberg. https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers

21. «Cyber-espionage warning: Russian hacking groups step up attacks ahead of European elections». 21 mars 2019. ZDNet. https://www.zdnet.com/article/cyber-espionage-warning-russian-hacking-groups-step-up-attacks-ahead-of-european-elections/

22. «Australian cyber soldiers hacked Islamic State and crippled its propaganda unit – here's what we know». 18 décembre 2019. ABC News. https://www.abc.net.au/news/2019-12-18/inside-the-secret-hack-on-islamic-state-propaganda-network/11809426

23. «State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack». 25 avril 2019. Amnesty International https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/

24. «New Report Shows How a Pro-Iran Group Spread Fake News Online». 14 mai 2019. The New York Times. https://www.nytimes.com/2019/05/14/world/middleeast/iran-fake-news-report.html

25. «China behind massive Australian National University hack, intelligence officials say». 6 juin 2019. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

26. «Croatian government targeted by mysterious hackers». 5 juillet 2019. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

27. «Two Russians accused of election interference arrested in Libya». 8 juillet 2019. Cyber Scout. https://cyberscout.com/en/blog/two-russians-accused-of-election-interference-arrested-in-libya

28. «BASF, Siemens, Henkel, Roche target of cyber attacks». 24 juillet 2019. Reuters. https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147

29. «New espionage malware found targeting Russian-speaking users in Eastern Europe» 10 octobre 2019. ZDNet. https://www.zdnet.com/article/new-espionage-malware-found-targeting-russian-speaking-users-in-eastern-europe/

30. «Advanced Israeli spyware is targeting Moroccan human rights activists». Novembre 2019. The Next Web. https://thenextweb.com/security/2019/10/14/advanced-israeli-spyware-is-targeting-moroccan-human-rights-activists/

31. «Hacking the hackers: Russian group hijacked Iranian spying operation, officials say». 21 octobre 2019. Reuters. https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK

32. «Israeli spyware allegedly used to target Pakistani officials' phones». 19 décembre 2019. The Guardian. https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones

33. «A phishing campaign with nation-state hallmarks is targeting Chinese government agencies». 8 août 2019. Cyber Scoop. https://www.cyberscoop.com/china-phishing-anomali-nation-state-apt/

34. «Foreign power was behind cyber attack on Czech ministry: Senate». 13 août 2019. Reuters. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

35. «Huawei technicians helped government officials in two African countries track political rivals and access encrypted communications.» 15 août 2019. The Wall Street Journal. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

36. «Labour suffers second cyber-attack in two days" 12 novembre 2019. The Guardian. https://www.theguardian.com/politics/2019/nov/12/labour-reveals-large-scale-cyber-attack-on-digital-platforms

37. «Extensive hacking operation discovered in Kazakhstan». 23 novembre 2019. ZDNet. https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/

Références

38. «A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems». 20 novembre 2019. Wired. https://www.wired.com/story/iran-apt33-industrial-control-systems/

39. «Russian "Gamaredon" Hackers Back at Targeting Ukraine Officials». 6 décembre 2019. Security Week. https://www.securityweek.com/russian-gamaredon-hackers-back-targeting-ukraine-officials

40. «Iran announced it foiled "really massive" foreign cyber attack». 11 décembre 2019. Security Affairs. https://securityaffairs.co/wordpress/94981/cyber-warfare-2/iran-foreign-cyber-attack.html

41. «Croatian government targeted by mysterious hackers». 5 juillet 2019. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

42. «Rapport sur la mise en œuvre de la politique étrangère et de sécurité commune – rapport annuel» 18 décembre 2019. Parlement européen. https://www.europarl.europa.eu/doceo/document/A-9-2019-0054_FR.html

43. «Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent». 26 septembre 2012. Krebs on Security. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information

44. «Energy Manufacturer Also Victimized by IE Zero Day in Watering Hole Attack». 2 janvier 2013. The Threat Post. https://threatpost.com/energy-manufacturer-also-victimized-ie-zero-day-watering-hole-attack-010213/77359/

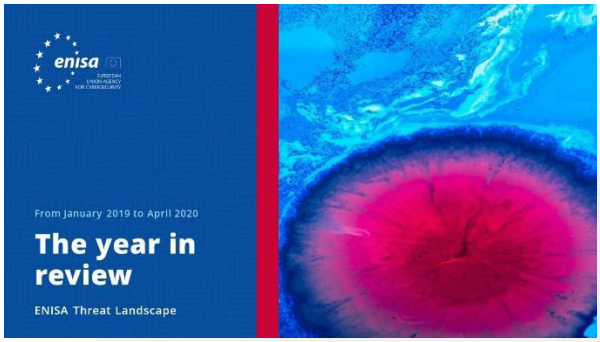
45. «The French Connection: French Aerospace-Focused CVE-2014-0322 Attack Shares Similarities with 2012 Capstone Turbine Activity». 25 février 2014. CrowdStrike Blog. https://www.crowdstrike.com/blog/french-connection-french-aerospace-focused-cve-2014-0322-attack-shares-similarities-2012/

46. «Advanced Persistent Threat Groups». Fireeye. https://www.fireeye.com/current-threats/apt-groups.html

47. «U.S. accuses pair of stealing secrets, spying on GE to aid China». 23 avril 2019. Reuters. https://www.reuters.com/article/us-usa-justice-ge/us-accuses-pair-of-stealing-secrets-spying-on-ge-to-aid-china-idUSKCN1RZ24O


«Le nombre de cyberattaques parrainées par des États-nations et ayant pour cible l'économie s'est accru en 2019.»
ETL 2020

Documents connexes



LIRE LE RAPPORT

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

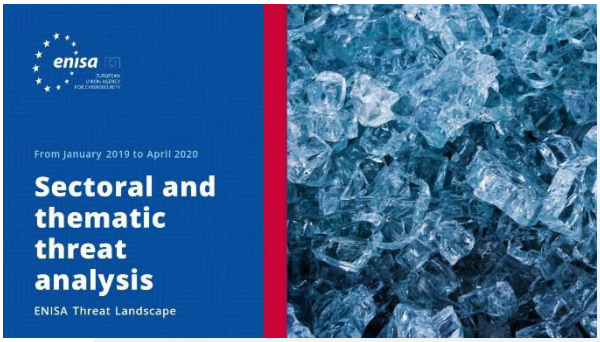
Rapport sur le Paysage des menaces de l'ENISA
Liste des 15 principales menaces

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

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.

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