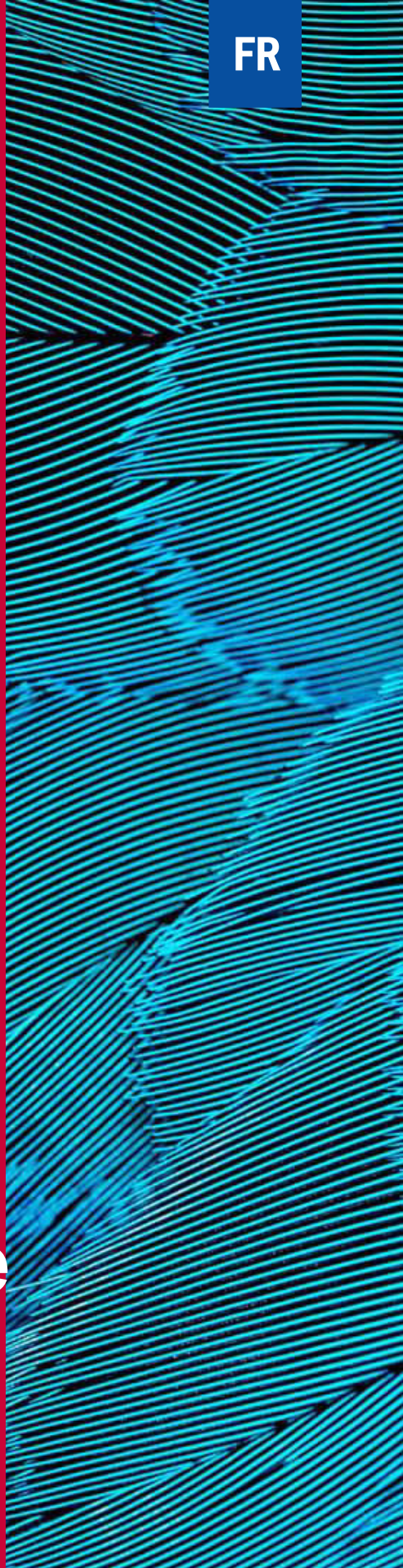
FR

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



De janvier 2019 à avril 2020

Le déni de service distribué

Paysage des menaces de l'ENISA

Aperçu

Les attaques par déni de service distribué (DDoS - *Distributed Denial of Service*) se produisent lorsque les utilisateurs d'un système ou d'un service ne sont pas en mesure d'accéder aux informations, services ou autres ressources concernés. Cette étape peut être franchie en épuisant le service ou en surchargeant un élément de l'infrastructure réseau.[1] Les acteurs malveillants ont augmenté le nombre d'attaques en ciblant davantage de secteurs avec des motifs différents. Alors que les mécanismes et les stratégies de défense sont de plus en plus solides, les compétences techniques des acteurs malveillants sont également en progression. Les rapports[3,4,5] indiquent que l'utilisation de techniques d'attaque par réflexion et amplification favorisant de nouveaux vecteurs, différents des plus connus (amplification UDP, etc.), est en augmentation.[6] En outre, les acteurs malveillants améliorent leurs tactiques commerciales en se lançant dans la promotion de leurs services sur le web. Par le passé, la promotion des services DDoS se faisait sur les forums du *dark web*, alors qu'aujourd'hui, elle s'effectue sur les chaînes de médias sociaux courantes, telles que YouTube et Reddit.[2]

En 2019, de nouvelles entrées ont fait leur apparition dans le top 10 des principaux pays générant du trafic DDoS (Hong Kong, Afrique du Sud, etc.).[7] L'année 2019 a également été marquée par une augmentation de l'activité DDoS par l'intermédiaire de réseaux de machines zombies (*botnets*). L'internet des objets (IoT - *Internet of Things*) constitue un «foyer» pour les *botnets* DDoS; d'ailleurs, la Chine (24 %), le Brésil (9 %) et l'Iran (6 %) sont considérés comme les pays les plus infectés par les agents de *botnets*.[3] Selon les prédictions d'un chercheur en sécurité, la mise en œuvre et la distribution de réseaux 5G augmenteront de façon exponentielle le nombre d'objets connectés, ce qui provoquera l'expansion des réseaux de machines zombies.[3]

Bien que les attaques par déni de service ne constituent rien de nouveau pour les défenseurs de la cybersécurité et des réseaux, leur niveau de sophistication ne cesse de s'accroître; quant aux acteurs malveillants, on remarque qu'ils sont plus actifs que par le passé pour mener des opérations de reconnaissance.[3,8]

Conclusions

241 %_ **d'augmentation du nombre total d'attaques au cours du troisième trimestre 2019 par rapport à la même période de 2018**[3]

79,7 %_ **de l'ensemble des attaques DDoS ont été des attaques SYN Flood**[7]

86 %_ **des attaques contrées au cours du troisième trimestre 2019 utilisaient plus de deux vecteurs**[9]

84 %_ **des attaques DDoS ont duré moins de 10 minutes**[10,11]

509_ **heures, c'est la durée de la plus longue attaque DDoS au cours du deuxième trimestre 2019**[3]

Chaîne de frappe

Déni de service

Reconnaissance	Armement	Livraison	Exploitation

Étape du processus d'attaque

Ampleur de l'objectif

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

Les cinq principales attaques DDoS

SYN FLOOD: 500-580 MILLIONS DE PAQUETS PAR SECONDE. Parmi toutes les techniques utilisées par les acteurs malveillants, SYN Flood est toujours considérée comme une attaque difficile à contrer en raison de ses caractéristiques, de l'infrastructure visée et du matériel supplémentaire dont elle a besoin pour traiter un volume élevé de paquets. En janvier 2019, un chercheur en sécurité a relevé une activité record pour SYN Flood qui avait pris pour cible un de ses clients et distribuait 500 millions de paquets par seconde (mpps); en avril 2019, ce volume est alors passé à 580 mpps.[12]

WS-DISCOVERY. *Web services dynamic discovery*[13] (WS-Discovery) est un protocole de découverte multidiffusion. On a pu constater qu'il était principalement utilisé par les dispositifs IoT pour permettre la détection automatique de chaque nœud sur les réseaux locaux (LAN - *Local Area Network*) mais, comme d'autres protocoles, il peut être utilisé à d'autres fins que celles prévues, en particulier dans le domaine de l'IoT.[5] Les acteurs malveillants y ont trouvé un bon repaire pour leurs attaques par amplification. Un chercheur en sécurité a relevé[3] un facteur d'amplification de 95 tandis qu'un autre chercheur a repéré une augmentation de 15 000 % par rapport à la taille de ses octets d'origine.[14]

ATTAQUES PAR RÉFLEXION ET AMPLIFICATION. Ces attaques sont largement et historiquement connues pour générer une petite requête dans le but de diffuser une charge utile plus importante. En résumé, l'acteur malveillant usurpe l'adresse IP de l'expéditeur (victime), puis l'hôte de destination envoie toutes les réponses correspondantes à la victime.[9] Cette méthode est surtout efficace sur les protocoles UDP en raison de leur mode sans connexion et de leur facteur d'amplification (par ex., le CLDAP a un facteur d'amplification allant de 50 à 70). En revanche, le protocole TCP n'est pas sujet à ce type d'attaque.[15]

Les attaques d'inondation par réflexion et amplification SYN-ACK en constituent un bon exemple. Ce type d'inondation n'a pas nécessairement besoin d'une large bande passante pour avoir de l'impact. En revanche, grâce à un nombre élevé de paquets par seconde, l'attaque peut passer inaperçue, permettant ainsi d'accroître son efficacité.[3]

DDoS DE TYPE «TAPIS DE BOMBES» (*CARPET BOMBING*). On sait que ce type d'attaque par déni de service distribué et réfléchi (DRDoS - *Distributed Reflection Denial of Service*) vise principalement les secteurs des télécommunications et des prestations de services.[17] Par exemple, lors d'une de ces attaques[18], les adresses IP d'un fournisseur d'accès à l'internet, sélectionnées de manière aléatoire, ont été prises pour cible dans le but de faire rebondir le trafic vers les routeurs de bordure du fournisseur. Par conséquent, la victime n'a pu identifier le DDoS qu'une fois son service submergé par la sélection de sa propre plage d'adresses IP.[19]

ATTAQUES DDOS MULTIVECTORIELLES. Souvent, les acteurs malveillants utilisent plusieurs vecteurs d'attaques par déni de service pour complexifier et diversifier leur opération, ce qui signifie qu'en automatisant simplement différents types d'attaque de la couche application (HTTP Flood, DNS Flood, etc.) et de la couche réseau (réflexion/amplification UDP/TCP, etc.), ils essaient de maximiser leur impact en saturant la bande passante ainsi que les ressources ou les services dans l'environnement cible.[16]

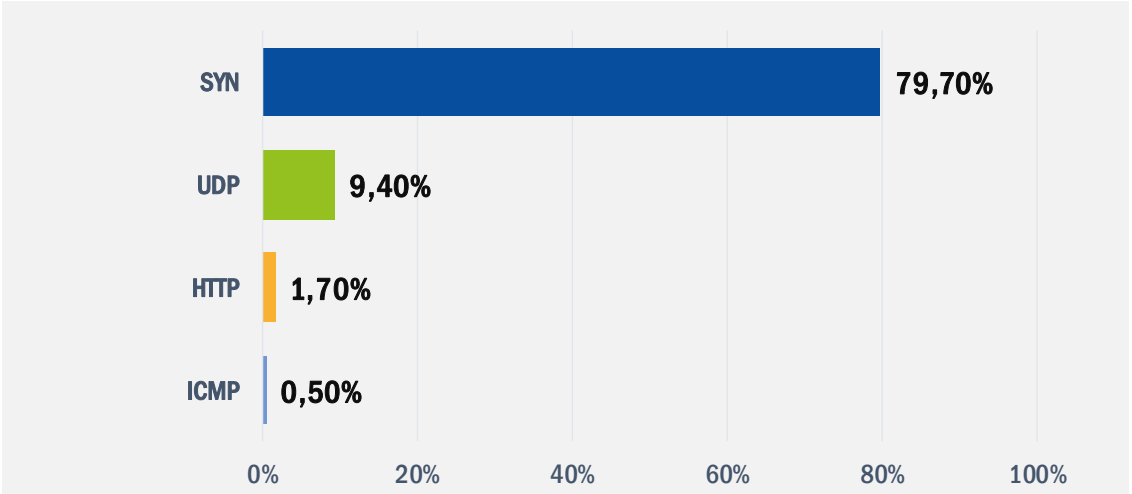


Figure 1: Répartition par type d'attaques par déni de service distribué. Source: Kapersky[16]

Vecteurs d'attaque

_ Comment

À l'instar des années précédentes, 2019 n'a pas fait exception en termes d'attaques UDP Flood. Selon un chercheur en sécurité, UDP Flood avait été le vecteur d'attaque le plus populaire et, selon son équipe, cela pourrait être lié au choix prépondérant de ce protocole UDP dans les industries à haut risque comme celle du jeu. Dans la liste des principaux vecteurs d'attaque figurent, après UDP Flood, les attaques SYN Flood, par réponse DNS et celles basées sur TCP.

Au cours de cette période, des attaques multivectorielles ont également été observées. Toutefois, selon un chercheur en sécurité, certaines d'entre elles ne sont que la dérive accidentelle d'une tentative de déni de service.[11]

Un rapport sur la cybersécurité[17] indique que les attaques par amplification DNS ont, selon l'équipe de recherche, représenté le vecteur d'attaque DDoS le plus important, suivi des attaques HTTP Flood et TCP SYN. Les vecteurs d'attaque observés au troisième trimestre 2019 se sont révélés similaires avec, en vecteur principal, SYN Flood, suivi des attaques UDP, TCP et HTTP.

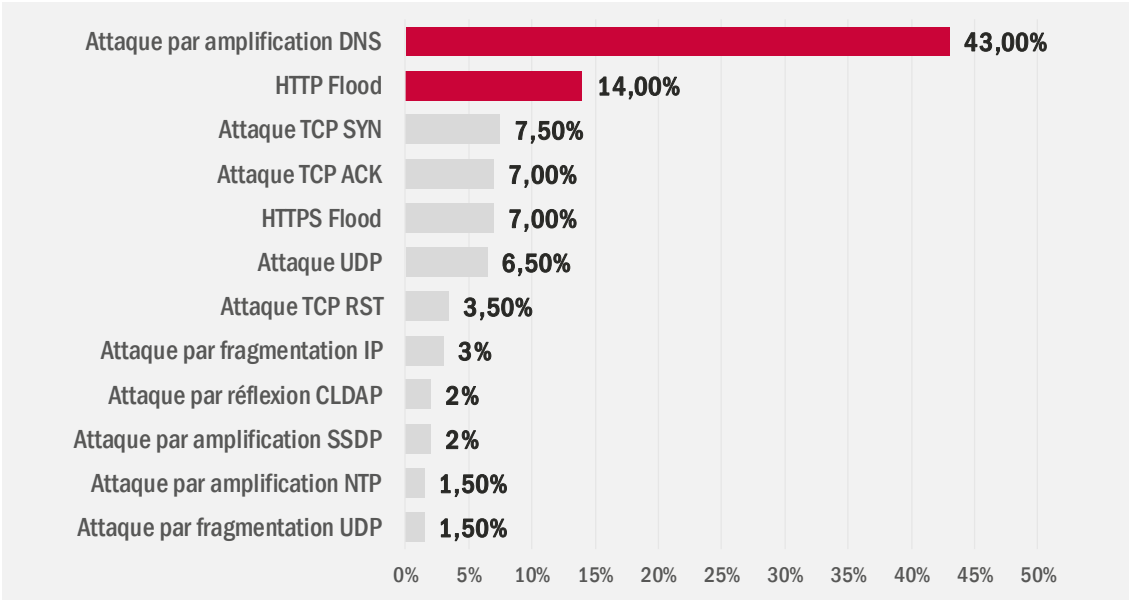


Figure 2: Répartition des vecteurs d'attaque par déni de service distribué. Source: NexusGuard[17]

Durée d'attaque

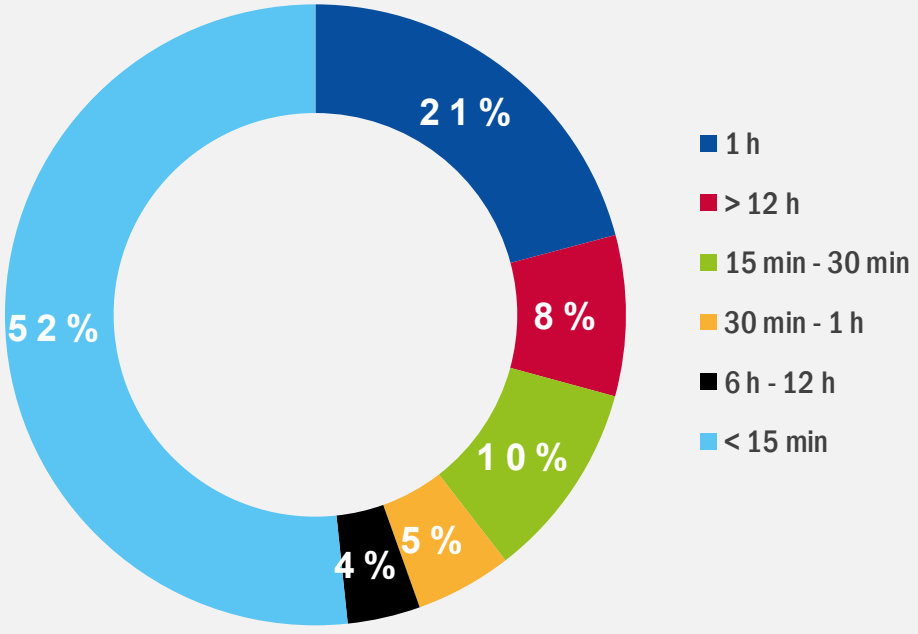


Figure 3 - Source: Imperva[11]

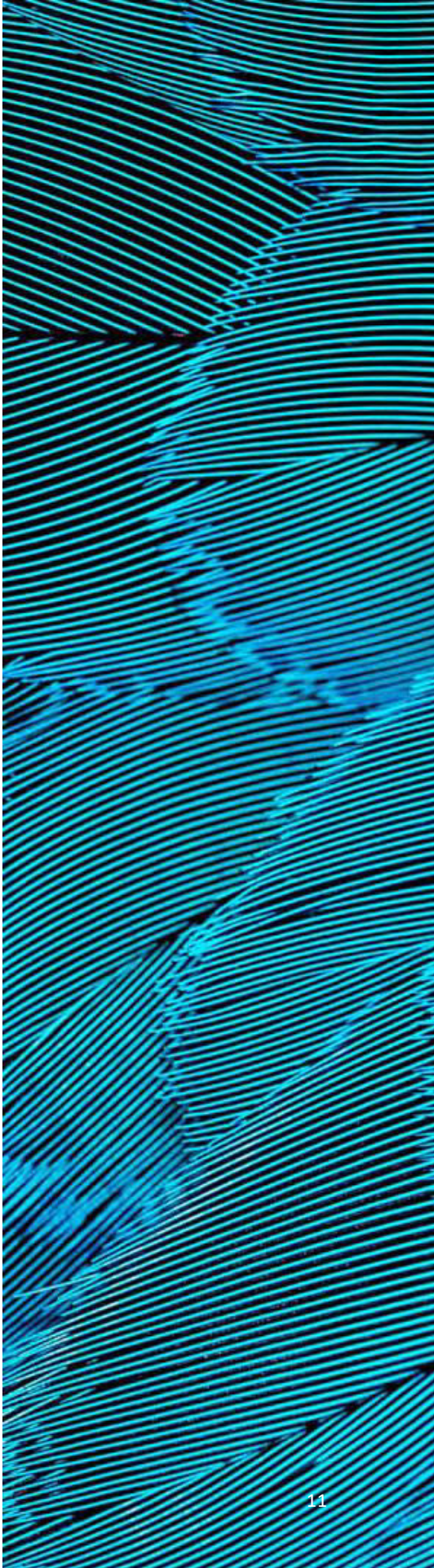
Atténuation

Actions proposées

- Connaître les services et les ressources critiques et privilégier la défense en cas de surcharge éventuelle. Veiller à ce qu'un plan d'intervention soit en place pour faire face à de tels scénarios.[20]
- Selon les exigences, envisager un service de protection DDoS ou un prestataire d'infogérance DDoS. Utiliser des méthodes telles que la surveillance pour identifier rapidement les infections.[1]
- Comme pour le point précédent, la publication de services par le biais de réseaux de diffusion de contenu peut être un moyen efficace d'absorber des attaques volumétriques (d'autres techniques sont à mettre en place pour des attaques plus sophistiquées).[21]
- Les fournisseurs d'accès à l'internet et de services en nuage jouent un rôle essentiel dans la défense contre les attaques DDoS. Mettre à leur disposition un plan et une voie de communication clairs est la clé du succès pour réagir à une attaque par déni de service.
- Adopter une attitude proactive et fortement défensive avant qu'une défaillance critique ne se produise, dans le cadre de laquelle l'équipe et les fournisseurs concernés configureront et affineront les contrôles en fonction des exigences de fonctionnement spécifiques.[22] La facilitation des serveurs cache ou la suppression à la source des demandes/requêtes inappropriées dans la couche application ainsi que la mise en œuvre d'un PCA[23] pour les fournisseurs de services sont de bons exemples de mesures proactives.
- Veiller à tester et à réévaluer vos techniques, technologies et fournisseurs de défense.
- Créer un registre des risques en analysant les moindres détails de votre environnement, en commençant par vos actifs critiques en interne jusqu'à votre empreinte numérique et votre présence sur l'internet.[24]

«Bien que les attaques par déni de service ne constituent rien de nouveau pour les défenseurs de la cybersécurité et des réseaux, leur niveau de sophistication ne cesse de s'accroître; quant aux acteurs malveillants, on remarque qu'ils sont plus actifs que par le passé pour mener des opérations de reconnaissance»

ETL 2020



Références

1. «Understanding Denial-of-Service Attacks» 20 novembre 2019. CISA. https://www.us-cert.gov/ncas/tips/ST04-015

2. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. «DDoS attacks in Q1 2019» 21 mai 2019. Kaspersky. https://securelist.com/ddos-report-q1-2019/90792/

3. «Q4 2019 - The State of DDoS Weapons Report.» 2019. A10 Networks. https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/

4. Chad Seaman. «Anatomy of a SYN-ACK Attack.» 2 juillet 2019. Akamai. https://blogs.akamai.com/sitr/2019/07/anatomy-of-a-syn-ack-attack.html

5. Brandon Vigliarolo. «A new type of DDoS attack can amplify attack strength by more than 15,300%.» 18 septembre 2019. TechRepublic. https://www.techrepublic.com/article/a-new-type-of-ddos-attack-can-amplify-attack-strength-by-more-than-15300/

6. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. «DDoS attacks in Q4 2018» 7 février 2019. Kaspersky. https://securelist.com/ddos-attacks-in-q4-2018/89565/

7. Oleg Kupreev, Ekaterina Badovskaya, Alexander Gutnikov. «DDoS attacks in Q3 2019» 11 novembre 2019. Kaspersky. https://securelist.com/ddos-report-q3-2019/94958/

8. «2019 Website Threat Research Report.» 2019. sucuri

9. «DDoS attacks up 241% in Q3 2019 compared to same period last year.» 19 novembre 2019. Neustar. https://www.home.neustar/about-us/news-room/press-releases/2019/ddos-attacks-up-241--in-q3-2019-compared-to-same-period-last-year#

10. «2019 Half-Year DDoS Trends Report.» 2019. Corero Security. https://www.corero.com/blog/infographic-2019-mid-year-ddos-trends-report/

11. Nadav Avital, Avishay Zawoznik, Johnathan Azaria, Kim Lambert. «2019 Global DDoS Threat Landscape Report.» 2019. Imperva. https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/

12. Tomer Shani. «Updated: This DDoS Attack Unleashed the Most Packets Per Second Ever. Here's Why That's Important.» 30 avril 2019. Imperva. https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/

13. «Web Services Dynamic Discovery (WS-Discovery) Version 1.1» 1er juillet 2009. OASIS. http://docs.oasis-open.org/ws-dd/discovery/1.1/wsdd-discovery-1.1-spec.html

14. Jonathan Respeto. «New DDoS Vector Observed in the Wild: WSD attacks hitting 35/Gbps.» 18 septembre 2019. Akamai. https://blogs.akamai.com/sitr/2019/09/new-ddos-vector-observed-in-the-wild-wsd-attacks-hitting-35gbps.html

15. «Threat Alert: TCP Amplification Attacks.» 9 novembre 2019. Radware. https://blog.radware.com/security/2019/11/threat-alert-tcp-reflection-attacks/

16. «Kaspersky report finds over half of Q3 DDoS attacks occurred in September.» 11 novembre 2019. Kaspersky. https://usa.kaspersky.com/about/press-releases/2019_kaspersky-report-finds-over-half-of-q3-ddos-attacks-occurred-in-september

17. «DDoS Threat Report 2019 Q1.» 2019. NexusGuard. https://blog.nexusguard.com/threat-report/ddos-threat-report-2019-q1

18. «International traffic – DDoS.» 22 septembre 2019. Cool Ideas. https://coolzone.cisp.co.za/announcements.php?announcement=2038-international-traffic-ddos-cool-ideas

19. Catalin Cimpanu. «Carpet-bombing' DDoS attack takes down South African ISP for an entire day.» 24 septembre 2019. ZDNet. https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/

20. «Guidance following recent DoS attacks in the run up to the 2019 General Election.» 13 novembre 2019. NCSC. https://www.ncsc.gov.uk/guidance/guidance-following-recent-dos-attacks-2019-general-election

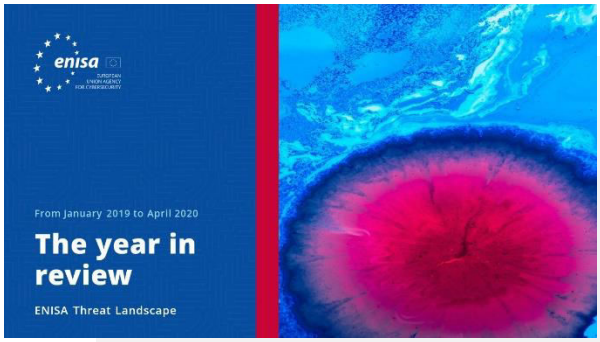
21. V. Revuelto, S. Meintanis, K. Socha. «DDoS Overview and Response Guide.» 10 mars 2017. CERT-UE. https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf

22. «State of the Internet/Security DDoS and Application Attacks, Volume 5, Issue 1.» 2019. Akamai. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/state-of-the-internet-security-ddos-and-application-attacks-2019.pdf

23. P. Fergusson, D. Senie. «Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.» Mai 2000. IETF Tools. https://tools.ietf.org/html/bcp38

24. Pierluigi Paganini. «Cyber Defense Magazine Sept Edition 2019.» 4 septembre 2019. SecurityAffairs. https://securityaffairs.co/wordpress/90795/breaking-news/cyber-defense-magazine-september-2019.html

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

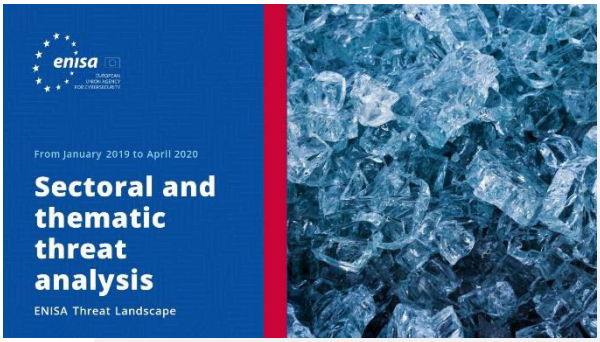
Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.

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.

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

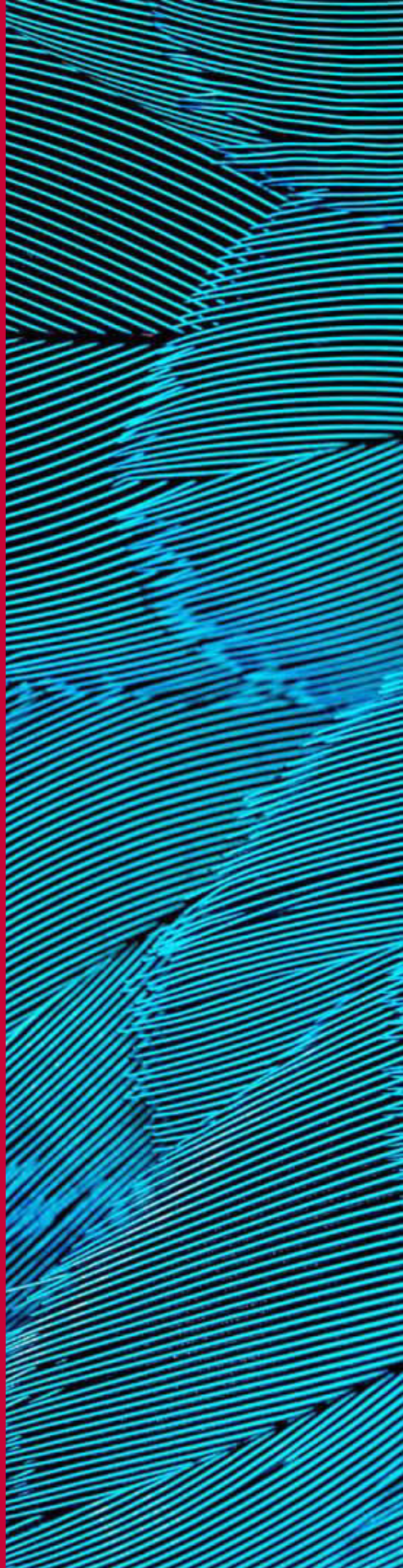
Il convient de noter que, sauf mention contraire, la présente publication représente les points de vue et les interprétations de l'ENISA. Elle ne doit pas être interprétée comme une action légale de l'ENISA ou des organes de l'ENISA à moins d'être adoptée conformément au règlement (UE) nº 526/2013. Elle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