FR

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De janvier 2019 à avril 2020

Le cryptominage

Paysage des menaces de l'ENISA

Aperçu

Le cryptominage (également connu sous le nom de *cryptojacking*) est l'utilisation non autorisée des ressources d'un appareil pour miner des cryptomonnaies. Les cibles sont généralement des appareils connectés, tels que des ordinateurs et des téléphones portables; cependant, les cybercriminels visent désormais de plus en plus les infrastructures en nuage.[1] Ce type d'attaque n'attire pas beaucoup l'attention des services de répression et sa pratique abusive est rarement signalée[2], principalement du fait que les retombées négatives sont assez peu nombreuses. Néanmoins, il peut arriver que les organisations constatent une hausse de leurs coûts informatiques, une dégradation de leurs composants informatiques, une augmentation de leur consommation d'électricité et une diminution de la productivité de leurs employés engendrée par le ralentissement des postes de travail.[3]

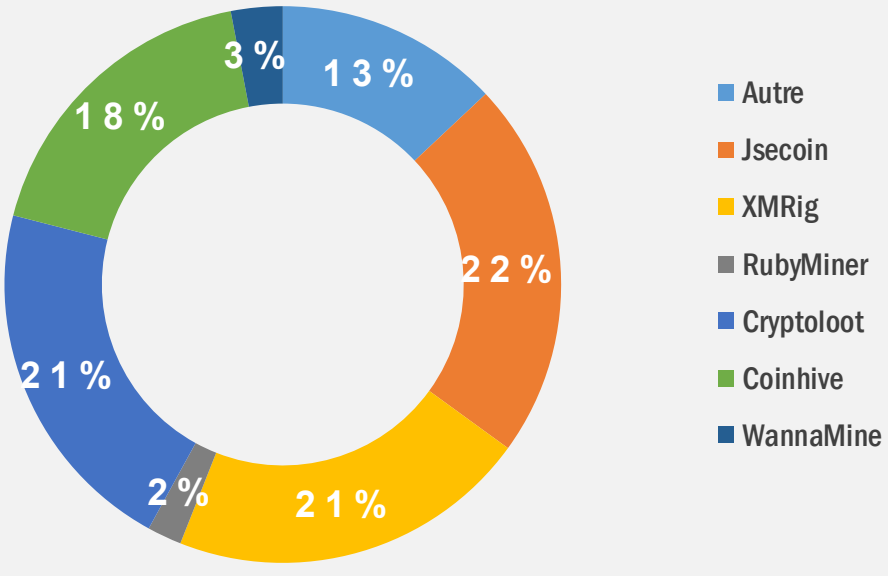


Figure 1: Principaux cryptomineurs dans le monde. Source: Check Point[9]

Conclusions

64,1_millions d'opérations de cryptominage enregistrées fin 2019

78 %_d'activités de cryptominage en moins au second semestre 2019 par rapport au premier semestre

Les activités avaient augmenté de 9 % au premier semestre 2019 par rapport aux six mois précédents en 2018.[4,5]

65 %_des 120 plateformes d'échange les plus prisées au troisième trimestre 2019 s'appuyaient sur des processus de connaissance du client (KYC - *Know Your Customer*) faibles ou poreux

32 % des plateformes d'échange effectuaient des transactions de cryptomonnaies anonymes intraçables (*privacy coins*).[6]

39,3 %_des infections par cryptominage en 2019 visaient le Japon.

20,8 % des infections par cryptominage visaient l'Inde et 14,2 % Taïwan; la figure 2 illustre les cinq pays dans lesquels les tentatives d'infection par des mineurs de cryptomonnaies ont été les plus détectées en 2018 et 2019.[7]

13 %_des incidents de cryptominage sont attribués au Trojan.Win32.Miner.bbb

De novembre 2018 à octobre 2019, parmi les mineurs les plus actifs figuraient ensuite le Trojan.Win32.Miner.ays (11,35 %) et le Trojan.JS.Miner.m (11,12 %).[6]

Chaîne de frappe

Cryptominage

Reconnaissance	Armement	Livraison	Exploitation

Étape du processus d'attaque

Ampleur de l'objectif

Cryptominage

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

Tendances

_Fermeture du célèbre service de cryptominage Coinhive

À ses débuts en septembre 2017, Coinhive s'était présenté comme une source de revenus alternative pour les développeurs web à la place des bannières publicitaires.[24] Il utilisait des bibliothèques JavaScript, qui pouvaient être installées sur les sites web, ainsi que la puissance de calcul de l'internaute pour miner légitimement la cryptomonnaie. Jusqu'à sa fermeture, en mars 2019, ce service s'était retrouvé fortement malmené par des acteurs malveillants qui injectaient du code dans des sites web piratés dans le but de miner la cryptomonnaie Monero et de détourner des fonds dans leurs propres poches. Après sa fermeture, le volume des opérations de cryptominage sur le web a chuté de 78 % au cours du second semestre 2019.[4] Suite à cette baisse, les cybercriminels ont alors commencé à se concentrer sur des cibles plus intéressantes, en particulier des serveurs puissants[9] et des infrastructures en nuage.[1] Coinhive a depuis été détrôné[9] par Jsecoin (22 %), XMRig (21 %) et Cryptoloot (21 %). La répartition mondiale des principaux cryptomineurs est représentée dans la figure 1.

_Accroissement des attaques sur les infrastructures en nuage

Une tendance à la hausse est apparue au premier semestre 2019 concernant les incidents d'attaques de cryptominage en nuage.[15,25] Les environnements en nuage utilisent généralement des mécanismes qui adaptent les ressources à la demande et sont donc des cibles lucratives pour l'exécution de logiciels de minage. Cependant, cela se fait au détriment des propriétaires de site web qui, pour leur part, doivent payer des factures plus élevées pour le dépassement des quotas.[15] Au cours du premier semestre 2019, les vulnérabilités des conteneurs en nuage ont augmenté de 46 % par rapport à la même période de 2018.[26] Les attaquants ont réussi à exploiter les interfaces de programmation (API - *Application Programming Interfaces*) et les plateformes de gestion des conteneurs afin d'installer des images malveillantes (par ex., Docker et Kubernetes) et de miner des cryptomonnaies.[25]

Incidents

*Avril 2019*_Campagne de cryptominage baptisée Beapy, exploitant la faille EternalBlue et affectant les entreprises en Chine[3]

*Mai 2019*_PCASTLE, mineur de Monero, avait pour cible principale les systèmes basés en Chine et utilisait des techniques d'attaque sans fichiers[19]

Plus de 50 000 serveurs appartenant à des entreprises des secteurs de la santé, des télécommunications, des médias et des technologies de l'information ont été infectés par un logiciel malveillant qui minait la cryptomonnaie TurtleCoin (TRTL).[20] Une nouvelle famille de logiciels malveillants, nommée BlackSquid, a eu recours à huit codes d'exploitation connus, dont EternalBlue et DoublePulsar, avant de s'étendre sur des serveurs web situés en Thaïlande et aux États-Unis dans le but de fournir des scripts pour le minage de Monero.[17,21]

*Août 2019*_Découverte d'un cryptomineur dans 11 référentiels de langage RubyGem, exposant des milliers d'utilisateurs à un code de cryptominage[22]

Tendances

_Passage au cryptominage sur fichiers

Une baisse du cryptominage par navigateur en faveur du cryptominage sur fichiers a été constatée en 2019. Les attaques de cryptominage sur fichiers[27] se propagent par le biais de logiciels malveillants et utilisent des codes d'exploitation préexistants sur des systèmes d'exploitation non corrigés, tels qu'EternalBlue, ainsi que d'autres vulnérabilités à haut risque. Plusieurs facteurs ont contribué à ce changement, en particulier la fermeture de Coinhive, célèbre service de minage sur le web[1], et la baisse de valeur des cryptomonnaies.[10] Un autre facteur permet de l'expliquer: le cryptominage sur fichiers a toujours été plus efficace que le minage sur le web, puisque 25 fois plus rentable.[3] Les auteurs de menace ont adapté leurs logiciels malveillants en intégrant des outils supplémentaires afin d'extraire des informations sensibles de l'ordinateur des victimes.

_Baisse mondiale des attaques de cryptominage

En 2019, une tendance à la baisse[5] des attaques de cryptominage a été constatée, principalement en raison de la fermeture de Coinhive[6], des efforts coordonnés des services de répression et de la dépréciation de la cryptomonnaie Monero. Cependant, comme l'on sait que les attaques de cryptominage suivent la valeur des cryptomonnaies, il est possible qu'un service similaire à Coinhive émerge et alimente un nouveau pic. Les premières statistiques de 2020 révèlent une augmentation de 30 % par rapport à l'année précédente en mars.

_Le Monero reste la cryptomonnaie de prédilection

À l'image des tendances précédentes, le Monero (XMR) est resté la cryptomonnaie de prédilection en 2019 pour les activités de cryptominage. Deux raisons à cela: tout d'abord, le Monero met l'accent sur la confidentialité et l'anonymat et, par conséquent, les transactions sont intraçables. Deuxièmement, l'algorithme de preuve de travail (*Proof-of-Work*) est conçu pour garantir la viabilité du minage avec un processeur standard plutôt qu'avec du matériel spécialisé. Au troisième trimestre 2019, 32 % des plateformes d'échange effectuaient des transactions avec des cryptomonnaies anonymes et intraçables (*privacy coins*), comme le Monero. Toutefois, en prévision de la nouvelle réglementation contre le blanchiment d'argent, de nombreuses plateformes d'échange ont choisi de radier ces *privacy coins.*

_Pays les plus visés

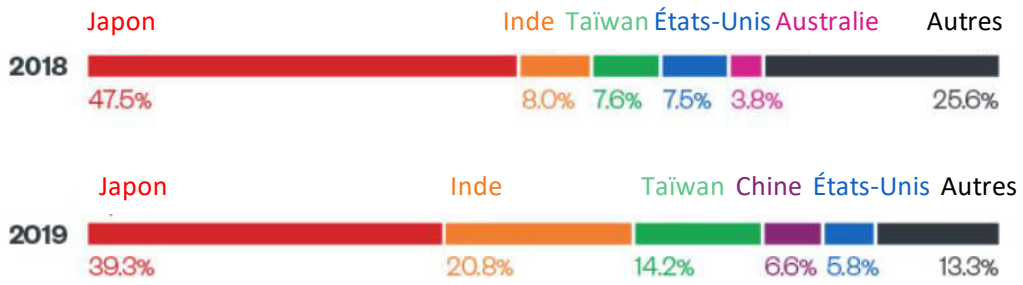


Figure 2: Pays les plus visés par le cryptominage. Source: Trend Micro[7]

Vecteurs d'attaque

_Techniques

Pour exécuter ou diffuser des cryptomineurs, les cybercriminels ont eu recours aux techniques suivantes:

- intégration de capacités de cryptominage dans des logiciels malveillants existants;[10]
- compromission de sites web;[11]
- attaques persistantes de type «drive-by» (c.-à-d. par téléchargement furtif);[12]
- utilisation des réseaux sociaux;[13]
- utilisation des applications mobiles et des app stores;[14]
- utilisation de kits d'exploitation;[15]
- utilisation de réseaux publicitaires et de publicités malveillantes;[16]
- utilisation de supports amovibles;[17]
- utilisation de cryptomineurs capables de se propager d'une machine à une autre.[18]

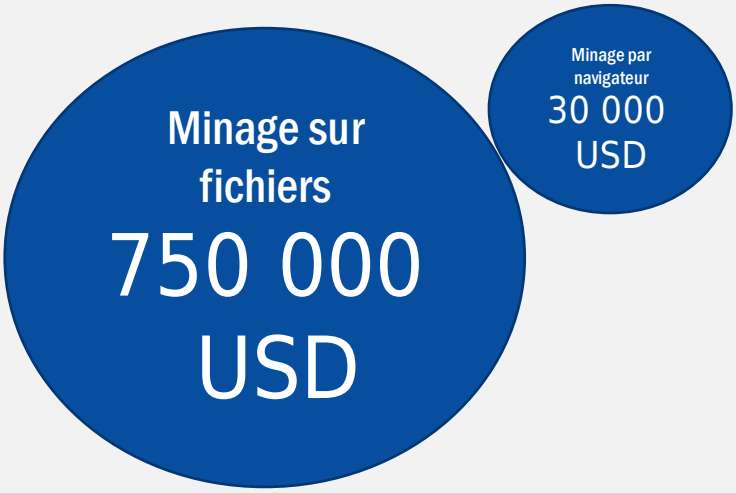


Figure 3: Combien peut rapporter un botnet de minage de monnaies en 30 jours? Source: Broadcom[3]

Actions proposées

- Surveiller l'utilisation de la batterie sur les appareils des utilisateurs et, en cas de pics suspects dans l'utilisation du processeur, rechercher la présence de mineurs sur fichiers.
- Implémenter un filtrage de contenu pour éliminer les pièces jointes indésirables, les courriels au contenu malveillant et les pourriels.
- Implémenter le filtrage du protocole de minage Stratum ainsi que la liste noire des adresses IP et des domaines des groupes de minage fréquentés.
- Protéger les terminaux au moyen d'antivirus ou d'extensions de navigateur bloquant les cryptomineurs.
- Effectuer régulièrement des audits de sécurité pour détecter toute anomalie du réseau.
- Implémenter une gestion solide des vulnérabilités et des correctifs.
- Établir une liste blanche pour empêcher le lancement d'exécutables inconnus sur les terminaux.
- Investir dans la sensibilisation des utilisateurs au cryptominage, notamment au regard des bonnes pratiques de navigation sécurisée.
- Implémenter des correctifs et des réparations contre des codes d'exploitation bien connus (par ex. Eternal Blue) sur des cibles moins évidentes, comme les systèmes de gestion de file d'attente, les terminaux de point de vente, voire les distributeurs automatiques.
- Surveiller et mettre sur liste noire les exécutables courants de cryptominage.

Références

1. Sergiu Gatlan. «Cryptominers Still Top Threat In March Despite Coinhive Demise.» 9 avril 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/cryptominers-still-top-threat-in-march-despite-coinhive-demise/

2. «Internet Organised Crime Threat Assessment (IOCTA).» 2019. EUROPOL https://www.europol.europa.eu/iocta-report

3. «Beapy: Cryptojacking Worm Hits Enterprises in China.» 24 avril 2019. BROADCOM. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china

4. Bill Conner. «SONICWALL Cyber Threat Report.» 2020. SONICWALL https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/

5. Yessi Bello Perez. «Unsuspecting victims were cryptojacked 52.7 million times in the first half of 2019.» 24 juillet 2019. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/07/24/cryptojacking-cryptocurrency-million-hits-first-half-2019/

6. Ben Noble. «A Third of Cryptocurrency Exchanges Still Host Privacy Coins Despite Fears of Impending FATF Travel Rule.» 27 novembre 2019. CIPHERTRACE https://ciphertrace.com/ciphertrace-q3-2019-caml-press-release/

7. «Defending Systems Against Cryptocurrency Miner Malware.» 28 octobre 2019. Trend Micro. https://www.trendmicro.com/vinfo/be/security/news/cybercrime-and-digital-threats/defending-systems-against-cryptocurrency-miner-malware

8. «Kaspersky Security Bulletin '19 Statistics.» 2009. Kaspersky. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_2019_Statistics_EN.pdf

9. «CYBER SECURITY REPORT.» 2020. Check Point Research cp<r>. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf

10. Ionut Ilascu. «EternalBlue Exploit Serves Beapy Cryptojacking Campaign.» 25 avril 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/eternalblue-exploit-serves-beapy-cryptojacking-campaign/

11. «New mining worm PsMiner uses multiple high-risk vulnerabilities to spread.» 12 mars 2019. 360 Total Security. https://blog.360totalsecurity.com/en/new-mining-worm-psminer-uses-multiple-high-risk-vulnerabilities-to-spread/

12. Dan Thorp-Lancaster. «New drive-by cryptocurrency mining scheme persists after you exit your browser window.» 9 novembre 2017. Windows Central. https://www.windowscentral.com/new-drive-cryptocurrency-mining-scheme-persists-even-after-you-exit-your-browser-window

13. Dr. Michaeal McGuire. «Social Media Platforms and the Cybercrime Economy.» 2019. Bromium. https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf

14. Axelle Apvrille. «Abusing cryptocurrencies on Android smartphones.» 2019. Fortinet. https://fortinetweb.s3.amazonaws.com/fortiguard/research/currency-insomnihack19.pdf

15. «2019 Midyear Security Roundup Evasive Treats Pervasive Effects.» 2019. Trend Micro https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf

16. Margi Murphy. «YouTube shuts down hidden cryptojacking adverts.» 29 janvier 2018. The Telegraph https://www.telegraph.co.uk/technology/2018/01/29/youtube-shuts-hidden-crypto-jacking-adverts/

17. Matthew Beedham. «New cryptocurrency mining malware is spreading across Thailand and the US.» 4 juin 2019. TheNextWeb – HARD FORK. https://thenextweb.com/hardfork/2019/06/04/security-crypto-jacking-mining-malware/

18. Sean Lyngaas. «BlueKeep is back. For now, attackers are just using it for cryptomining.» 4 novembre 2019. CyberScoop. https://www.cyberscoop.com/bluekeep-exploited-cryptomining/

19. Janus Agcaoili. «Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques.» 5 juin 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-malware-pcastle-zeroes-back-in-on-china-now-uses-multilayered-fileless-arrival-techniques/

20. Marie Huillet. «Researchers Say 50,000 Servers Worldwide Infected With Privacy Coin Cryptojacking Malware.» 29 mai 2019. Cointelegraph. https://cointelegraph.com/news/researchers-say-50-000-servers-worldwide-infected-with-privacy-coin-cryptojacking-malware

21. Johnlery Triunfante, Mark Vicente. «BlackSquid Slithers Into Servers and Drives With 8 Notorious Exploits to Drop XMRig Miner.» 27 août 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/blacksquid-slithers-into-servers-and-drives-with-8-notorious-exploits-to-drop-xmrig-miner/

22. «Malicious cryptojacking code found in 11 Ruby libraries.» 2 août 2019, Decrypt. https://decrypt.co/8602/malicious-cryptjacking-code-found-in-11-ruby-libraries

23. Brook Chelmo. «Cryptojacking in 2019: Cryptocurrency Value Keeping Attack Vector in Play.» 6 août 2019. SonicWall. https://blog.sonicwall.com/en-us/2019/08/cryptojacking-in-2019-cryptocurrency-value-keeping-attack-vector-in-play/

24. Catalin Cimpanu. «Coinhive cryptojacking service to shut down in March 2019». 27 février 2019. ZD Net. https://www.zdnet.com/article/coinhive-cryptojacking-service-to-shut-down-in-march-2019/

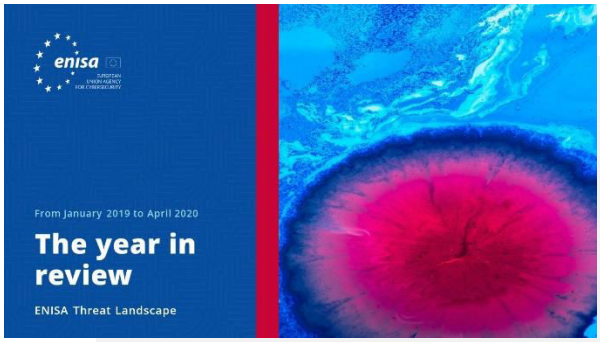
25. Tom Hegel. «Making it Rain - Cryptocurrency Mining Attacks in the Cloud». 14 mars 2019. AT&T Business. https://cybersecurity.att.com/blogs/labs-research/making-it-rain-cryptocurrency-mining-attacks-in-the-cloud/

26. «How a Prominent Cryptomining Botnet is Paving the Way for a Lucrative and Illicit Revenue Model». Août 2019. Carbon Black. https://www.carbonblack.com/resources/access-mining/

27. «Cryptojacking Attacks: Who's Mining on Your Coin?». 5 avril 2019. Security Intelligence. https://securityintelligence.com/cryptojacking-attacks-whos-mining-on-your-coin/

28. «Malware Creates Cryptominer Botnet Using EternalBlue and Mimikatz». 12 avril 2019. Bleeping Computer. https://www.bleepingcomputer.com/news/security/malware-creates-cryptominer-botnet-using-eternalblue-and-mimikatz/

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

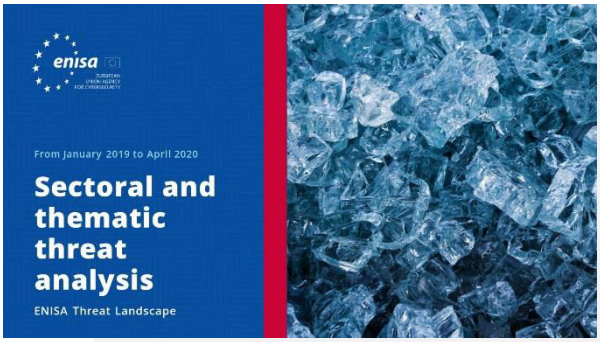
Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.

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