enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

FR

De janvier 2019 à avril 2020

Les logiciels malveillants (*malware*)

Paysage des menaces de l'ENISA

Aperçu

Le logiciel malveillant (*malware*) est une cyberattaque couramment utilisée. Dans les familles de logiciels malveillants figurent des cryptomineurs, des virus, des rançongiciels (*ransomware*), des vers et des espiogiciels (*spyware*). Ils ont pour objectifs communs de voler des informations ou d'usurper des identités, de faire de l'espionnage et de provoquer l'interruption des services.[1]

En 2019, les cryptomineurs ont été l'une des familles de logiciels malveillants les plus répandues dans le paysage des menaces[2]; ils ont engendré des coûts informatiques élevés, une augmentation de la consommation d'électricité et une baisse de la productivité des employés.[3] Les rançongiciels ont connu une légère augmentation en 2019 par rapport à 2018, mais ils restent tout de même en bas de la liste des différents types de logiciels malveillants.[2]

Les protocoles web et de messagerie ont été les premiers vecteurs d'attaque les plus souvent utilisés pour diffuser des logiciels malveillants. Cependant, en utilisant des techniques par force brute ou en exploitant les vulnérabilités du système, certaines familles de logiciels malveillants ont réussi à se propager plus profondément à l'intérieur d'un réseau. Bien que le nombre d'attaques détectées dans le monde soit resté au même niveau que l'année précédente, on a pu constater un changement de cibles, passant des consommateurs aux entreprises.[4]

Conclusions

400 000_ **détections d'espiogiciels et de publiciels (*adware*) préinstallés sur des appareils mobiles[4]**

13 %_ **de logiciels malveillants Windows détectés en plus sur les terminaux d'entreprise à travers le monde[4]**

71 %_ **des organisations ont déjà fait l'expérience de la propagation d'un logiciel malveillant d'un employé à un autre[47]**

46,5 %_ **de tous les logiciels malveillants contenus dans des courriels se trouvaient dans un type de fichier «.docx»[24]**

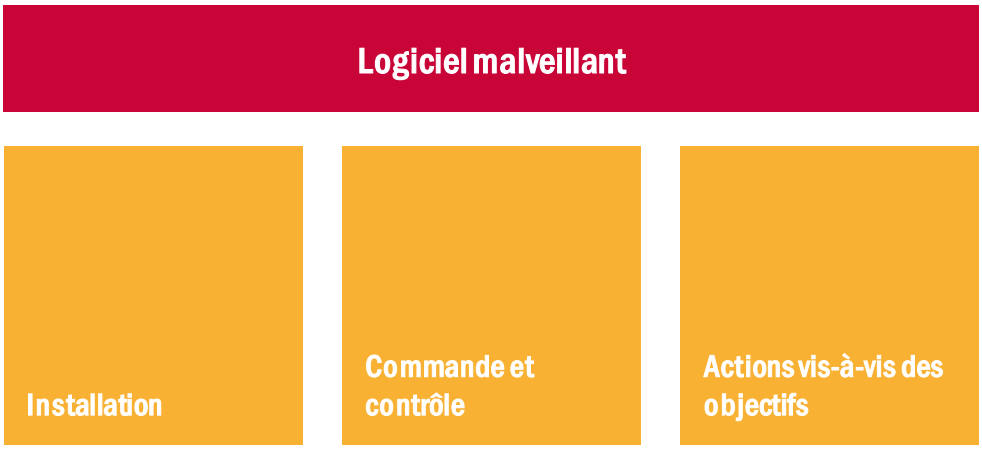
50 %_ **d'augmentation des logiciels malveillants conçus pour voler des données personnelles, autrement appelés logiciels de traque (*stalkerware*)[15]**

67 %_ **des logiciels malveillants ont été transmis par des connexions HTTPS chiffrées[48]**

Chaîne de frappe

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 types de logiciels malveillants les plus courants

Emotet était la souche de logiciels malveillants la plus courante en 2019, mais il évolue en 2020. Apparu pour la première fois en 2014, ce logiciel malveillant était alors considéré comme un cheval de Troie bancaire. Depuis lors, il s'est amélioré en intégrant une fonctionnalité de commande et de contrôle (C&C), des mécanismes d'évasion supplémentaires qui lui permettent notamment de détecter s'il fonctionne dans un environnement de bac à sable (*sandbox*) et de distribuer de dangereuses charges utiles, telles que Trickbot et Ryuk.[7] La figure ci-après présente le classement des logiciels malveillants bancaires détectés en 2019.

Au cours de la période considérée, Emotet s'est transformé en réseau de machines zombies (*botnet*)[2], a renforcé son activité[8] et a lancé de nouvelles campagnes de pourriels (*spam*) localisées en se servant d'une fonctionnalité d'hameçonnage ciblé (*spearphishing*) pour installer des rançongiciels ou voler des informations.[5] En 2019, les détections d'Emotet ont augmenté de 73 % par rapport à l'année précédente, ciblant principalement les terminaux d'entreprise situés aux États-Unis et au Royaume-Uni, comme l'illustre le graphique ci-dessous.[4]

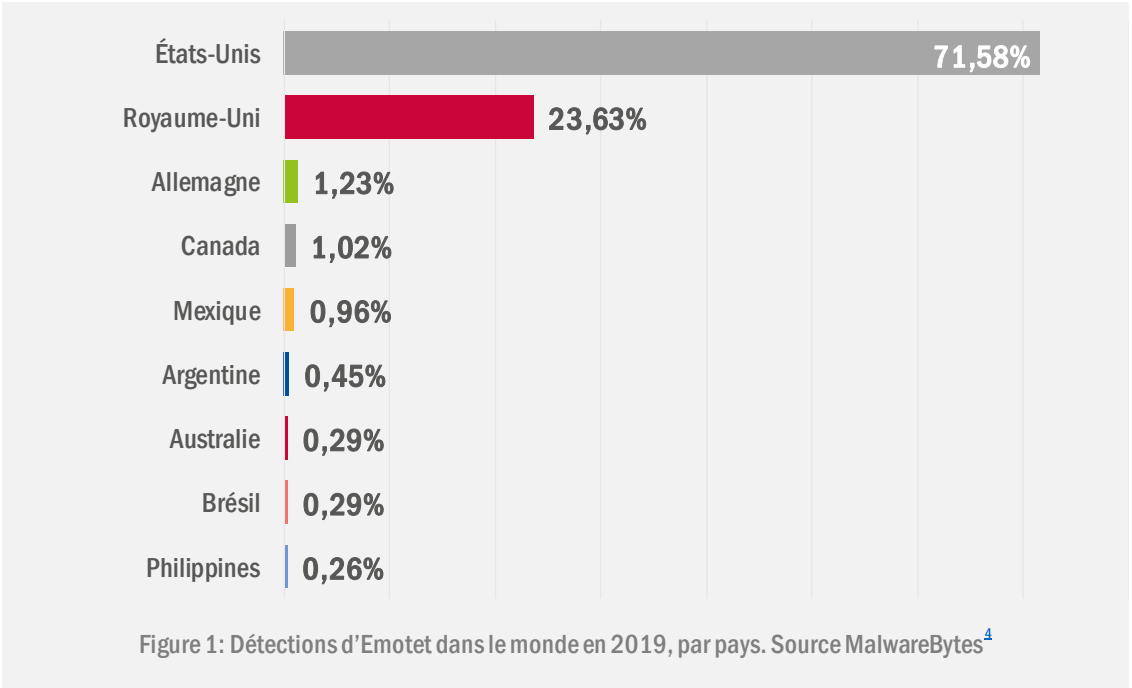


Figure 1: Détections d'Emotet dans le monde en 2019, par pays. Source MalwareBytes[4]

_Une transition vers des cibles en entreprise

Bien que les détections de logiciels malveillants soient restées globalement au même niveau qu'en 2018[4,9], on a pu observer une augmentation de 13 % des logiciels malveillants prenant pour cible des entreprises liées aux services, à l'éducation et à la distribution, qui font partie des secteurs les plus touchés.[4] On estime que plus d'un tiers des attaques de logiciels malveillants bancaires en 2019 visaient des utilisateurs en entreprise, avec pour objectif de compromettre les ressources financières de l'entreprise.[10] Les cinq principales souches de logiciels malveillants[4] ciblant les entreprises ont été Trojan.Emotet, Adware.InstallCore, HackTool.WinActivator, Riskware.BitCoinMiner et Virus.Renamer. En 2019, les attaques par rançongiciel visant le secteur public ont augmenté en raison de sa capacité à payer des rançons plus élevées.[11] Les cybercriminels cherchent à atteindre des cibles de grande valeur, c'est pourquoi ils ont conçu de nouveaux types de logiciels malveillants capables de se propager latéralement au sein d'un réseau d'entreprise plutôt que par l'internet.[12]

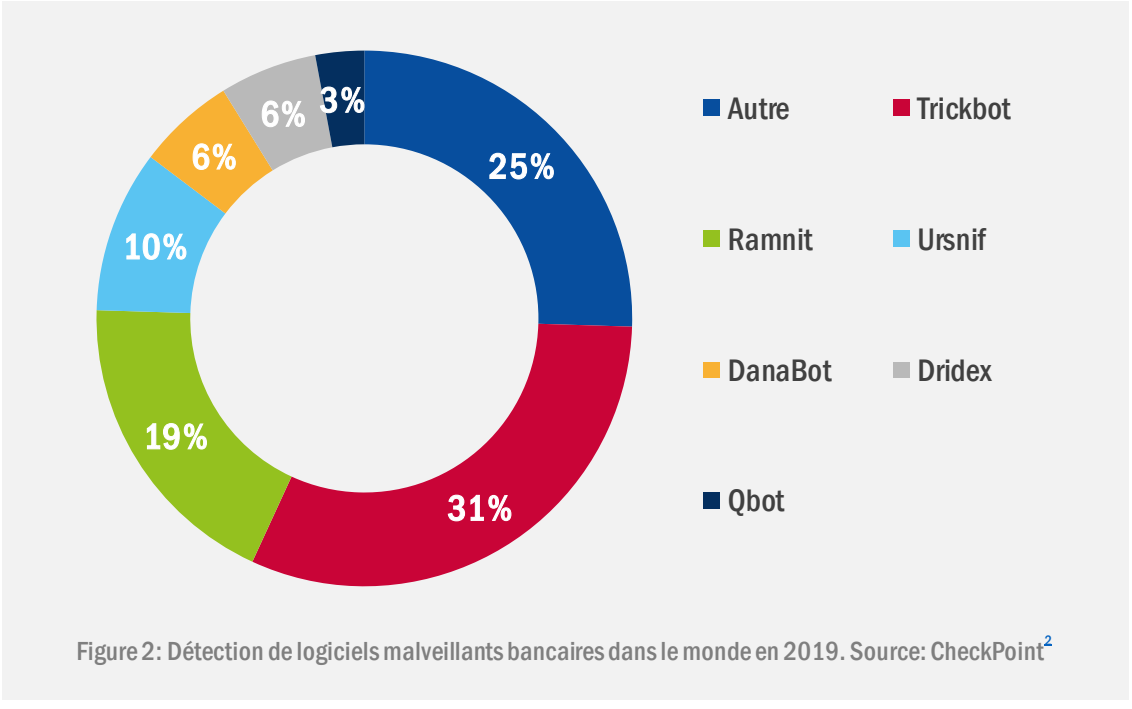


Figure 2: Détection de logiciels malveillants bancaires dans le monde en 2019. Source: CheckPoint[2]

Tendances

_ Le MaaS ou logiciel malveillant à la demande

Le «*malware-as-a-service*» (MaaS) désigne un logiciel malveillant spécifique vendu sur des forums clandestins qui fournit à ses clients (cybercriminels) les outils et l'infrastructure nécessaires pour mener des attaques ciblées. Le propriétaire du MaaS fournit ce service en livrant un kit qui comprend un programme de chargement initial (*initial loader*), un serveur de commande et contrôle (C&C) et une porte dérobée (*backdoor*), le tout permettant de prendre le contrôle total de l'ordinateur infecté.

Un chercheur en sécurité[13] a récemment identifié quatre types d'attaque utilisant divers outils du portefeuille MaaS de Golden Chickens (GC), ce qui confirme la sortie de variantes améliorées avec des codes mis à jour pour trois de ces outils.

- **TerraLoader**. Chargeur polyvalent écrit en PureBasic. TerraLoader est un produit phare du portefeuille de services Maas GC.
- **more_eggs**. Logiciel malveillant de type porte dérobée capable de repérer un serveur C&C fixe et d'exécuter des charges utiles supplémentaires téléchargées à partir d'une ressource web externe. La porte dérobée est écrite en JavaScript.
- **VenomLNK**. Fichier de raccourci Windows vraisemblablement généré par une version plus récente du kit de base VenomKit.

L'essor des logiciels malveillants bancaires sur les appareils mobiles

Les applications mobiles conçues pour dérober les données de paiement, les identifiants et les fonds des comptes bancaires des victimes ont augmenté de 50 % au cours du premier semestre 2019.[14] Habituellement, les acteurs malveillants utilisent des techniques d'hameçonnage (*phishing*) pour obtenir des références bancaires, soit par l'affichage d'une fausse page imitant la page de connexion de la banque, soit par l'introduction de fausses applications mobiles ressemblant aux applications bancaires originales. Cependant, en 2019, les cybercriminels sont devenus plus créatifs, comme dans le cas du Trojan-Banker.AndroidOS.Gustuff.a, capable de contrôler une application bancaire légitime grâce à l'utilisation abusive des fonctions d'accessibilité du système d'exploitation et ainsi d'automatiser les transactions frauduleuses.[15] On a fréquemment découvert de nouvelles versions de logiciels malveillants bancaires mobiles en vente sur des forums clandestins[15] et de nouvelles techniques d'évasion ne cessent de se développer. Parmi les nouveautés découvertes en 2019, on a remarqué que les logiciels malveillants pouvaient se servir de capteurs de mouvement leur permettant de se déclencher qu'en cas de déplacement du smartphone, à l'image du cheval de Troie bancaire mobile Anubis capable de détecter un environnement de bac à sable.[16] Les logiciels malveillants bancaires les plus répandus en 2019[11] ont été Asacub (44,4 %), Svpeng (22,4 %), Agent (19,1 %), Faketoken (12 %) et Hqwar (3,8 %).

Tendances

_Les logiciels malveillants sans fichier

Les logiciels malveillants sans fichier ne contiennent pas de fichier exécutable, ce qui leur permet d'échapper aux filtres de sécurité habituels et aux techniques de liste blanche. Par conséquent, cette famille de logiciels malveillants peut avoir jusqu'à dix fois plus de chances de réussir que les autres.[18] Au lieu d'un fichier exécutable, ce type de logiciel malveillant demande à l'attaquant d'injecter un code malveillant dans un logiciel de confiance déjà installé, soit à distance (par ex., dans le cas du système de gestion *Windows Management Instrumentation* ou WMI et PowerShell), soit en téléchargeant activement des documents (par ex., des documents Office) contenant des macros malveillantes.[19] Après une attaque réussie, le logiciel malveillant peut gagner en persistance grâce au registre, au planificateur de tâches intégré ou au WMI. Les attaques de logiciels malveillants sans fichier ont augmenté de 265 % au cours du premier semestre 2019.[20] La majorité d'entre elles reposaient sur des scripts (38 %), tandis que les autres exécutaient une attaque en mémoire (24 %) ou utilisaient abusivement les outils système intégrés (20 %).[21]

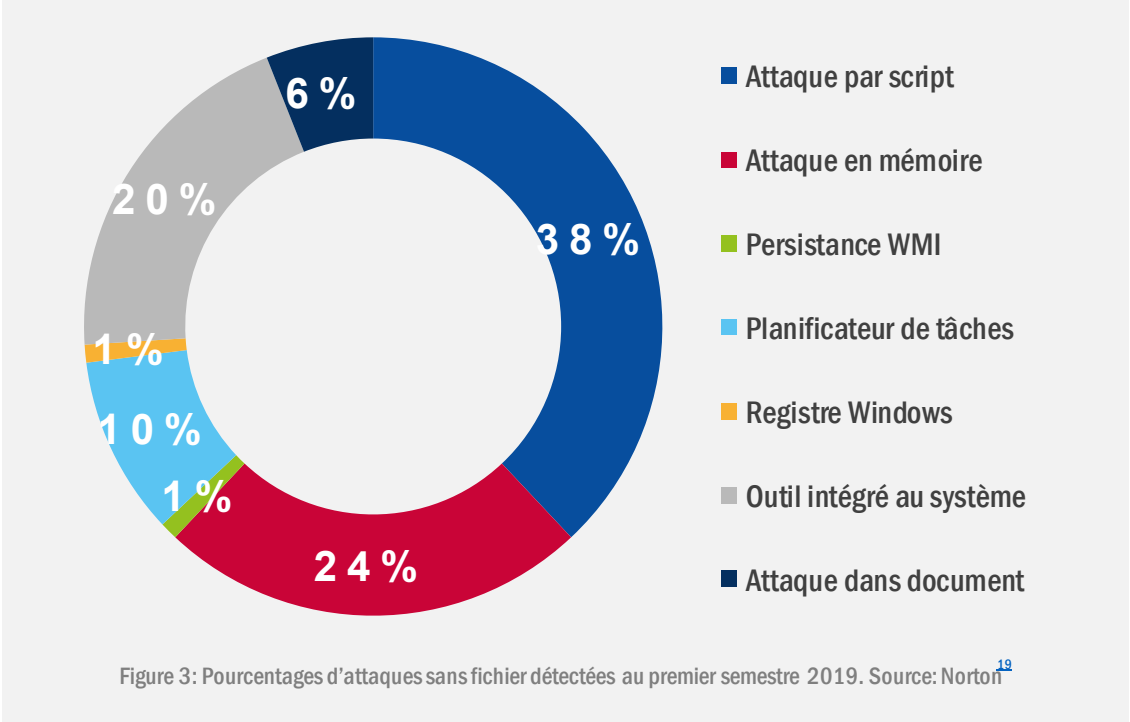


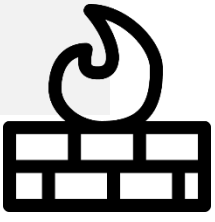
Figure 3: Pourcentages d'attaques sans fichier détectées au premier semestre 2019. Source: Norton[19]

Comment éviter une attaque sans fichier et s'en défendre?

Pour les organisations, le meilleur moyen de se défendre contre les attaques sans fichier est de maintenir les logiciels à jour. Comme la plupart des infections sans fichier se produisent sur des applications Microsoft et surtout sur des fichiers «.docx», il est particulièrement important de toujours mettre à jour la dernière version de ce logiciel. Microsoft a également mis à jour son progiciel Windows Defender pour détecter toute activité irrégulière à l'aide de l'application PowerShell.

Selon un chercheur en sécurité[18], la clé pour contrer efficacement une campagne d'attaques sans fichier consiste à traiter chacune des phases du cycle de vie de la menace à l'aide d'une approche de défense intégrée et sur plusieurs niveaux. Dans cette approche, il est important d'étudier les différentes étapes de l'attaque et d'entreprendre les opérations suivantes:

- analyser et évaluer les actions effectuées par l'attaquant;
- identifier les techniques utilisées;
- surveiller les activités dans PowerShell ou autres moteurs de script;
- accéder aux données agrégées sur les menaces;
- contrôler l'état du système ciblé;
- stopper les processus arbitraires;
- corriger les processus faisant partie de l'attaque;
- isoler les appareils infectés.



Tendances

_Paysage des *botnets* et des serveurs de commande et contrôle (C&C)

Le trafic mondial des réseaux de machines zombies (*botnets*) a augmenté de 71,5 % depuis 2018[2]. Les *botnets* les plus souvent observés ont été Emotet (41 %), Trickbot (25 %) et DanaBot (5 %)[2]. On a remarqué une augmentation sensible du trafic de *botnets* en Russie (143 %), principalement attribuée à l'assouplissement des procédures d'enregistrement et à la baisse d'intérêt de la part des services de répression.[14] En 2019, la Russie hébergeait la plupart des C&C de *botnets*, suivie par les États-Unis, les Pays-Bas, la Chine et la France. Les cybercriminels ont utilisé des algorithmes de génération de noms de domaine (DGA - *Domain Generation Algorithms*) pour prendre en charge de nombreuses communications C&C. 50 % de ces enregistrements ont été effectués dans des domaines de premier niveau (TLD - *Top-Level Domain*) «.com» et «.net».[15] Au cours de la période considérée, ces enregistrements de noms de domaine ont chuté de 71 % au profit d'autres protocoles de communication comme le poste-à-poste (P2P - *Peer-to-Peer*).[13]

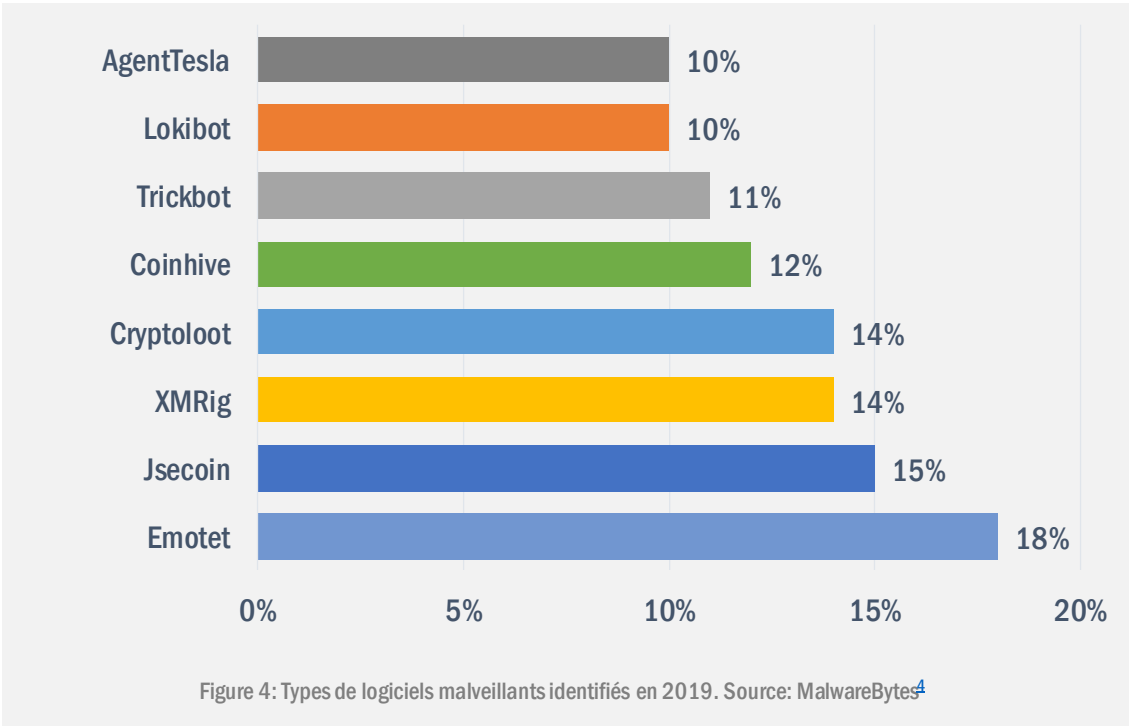


Figure 4: Types de logiciels malveillants identifiés en 2019. Source: MalwareBytes[4]

_Comment

Selon une étude datant de 2019, 94 % de l'ensemble des logiciels malveillants ont été distribués par courriel.[24] Bien que ce vecteur soit comptabilisé comme point d'entrée, il est intéressant de noter qu'en cas d'attaque réussie, le logiciel malveillant peut télécharger une charge utile supplémentaire qui, tel le comportement d'un ver, permet sa propagation latérale au sein du réseau (Emotet et Trickbot). En outre, après la distribution initiale du logiciel malveillant, dans la plupart des cas (71 %), c'est l'activité des employés qui permettait de le diffuser. Une fois de plus, de nouvelles vulnérabilités dans le protocole RDP (*Remote Desktop Protocol*) ont attiré l'attention, car celles-ci permettent l'exécution de code à distance (RCE - *Remote Code Execution*) et sont donc *wormable*.[30] Bien que ces vulnérabilités récemment découvertes n'aient pas encore été exploitées à grande échelle, on s'attend à ce qu'un nouveau ver puisse cibler des systèmes non corrigés dans un avenir proche.[31]

_Incidents

- **Airbus** a subi une violation de données qui a touché des employés en Europe.[34,35]
- Un logiciel malveillant de clonage de cartes (*card-skimming*) installé sur le site web de l'**American Medical Collection Agency** a entraîné le vol des données personnelles de 12 millions de patients.[36]
- **LifeLabs**, important fournisseur de diagnostics de laboratoire, a été victime d'une attaque par rançongiciel qui a entraîné le vol de 15 millions de comptes dans lesquels figuraient des résultats de tests et des numéros des cartes de santé.[37,38]
- Une attaque par rançongiciel contre la **ville de Pensacola, en Floride**, a conduit à la mise en ligne de 2 Go de données susceptibles de contenir des informations à caractère personnel.[39]
- Les données personnelles de 2 400 **membres des forces armées de Singapour** pourraient avoir fait l'objet d'une fuite par hameçonnage de courriels au moyen d'un logiciel malveillant.[40]

Atténuation

_Actions proposées

- Mettre en œuvre la détection des logiciels malveillants pour tous les canaux d'entrée/sortie, y compris la messagerie, le réseau, le web et les systèmes d'application sur toutes les plateformes applicables (c.-à-d. les serveurs, l'infrastructure réseau, les ordinateurs personnels et les appareils mobiles).
- Inspecter le trafic SSL/TLS permettant au pare-feu de décrypter ce qui est transmis vers et depuis les sites web, les communications par courriel et les applications mobiles.
- Établir des interfaces entre les fonctions de détection des logiciels malveillants (chasse aux menaces fondée sur l'analyse) et la gestion des incidents de sécurité pour mettre en place des moyens de réponse efficaces.
- Utiliser les outils disponibles pour analyser les logiciels malveillants afin de partager des informations sur ces logiciels et sur leur atténuation (c.-à-d. la MISP - *Malware Information Sharing Platform*).[32]
- Élaborer des politiques de sécurité précisant les processus à suivre en cas d'infection.
- Connaître les capacités des différents outils de sécurité et développer de nouvelles solutions de sécurité. Identifier les lacunes et appliquer le principe de la défense en profondeur.
- Utiliser le filtrage des courriels (ou filtrage antipourriel) pour détecter les courriers électroniques malveillants et supprimer les pièces jointes exécutables.
- Contrôler régulièrement les résultats des tests antivirus.[30,42]
- Surveiller les journaux à l'aide d'une solution de gestion des informations et des événements de sécurité (SIEM - *Security Information and Event Management*). Parmi les sources de journaux indicatives figurent les alertes antivirus, les solutions de détection et de réponse sur les terminaux (EDR - *Endpoint Detection and Response*), les journaux des serveurs proxy, les journaux d'événements Windows et Sysmon[43], les journaux des systèmes de détection d'intrusion (IDS - *Intrusion Detection System*)[44], etc.
- Désactiver ou réduire l'accès aux fonctions PowerShell.[45]

«La sophistication des capacités de menace s'est accrue en 2019; de nombreux adversaires ont désormais recours aux codes d'exploitation, au vol d'identifiants et aux attaques en plusieurs étapes.»

ETL 2020

Références

1. «What is Malware». Veracode. https://www.veracode.com/security/malware
2. «Cyber Security Report». 2019. Checkpoint. https://www.checkpoint.com/downloads/resources/cyber-security-report-2020.pdf
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. «2020 State of Malware Report». Février 2020. Malware Bytes. https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf
5. «Evasive Threats, Pervasive Effects» 2019. Trend Micro, Research. https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf
6. «SonicWall Cyber Threat Report». 2020. SonicWall. https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/
7. «Emotet is back: botnet springs back to life with new spam campaign». 16 septembre 2019. Malwarebytes Labs. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/
8. «Increased Emotet Malware Activity» 22 janvier 2020. US CERT. https://www.us-cert.gov/ncas/current-activity/2020/01/22/increased-emotet-malware-activity
9. «SonicWall Security Metrics» SonicWall. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics
10. «Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection». 16 avril 2019. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection
11. «Internet organised crime threat assessment» 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf
12. «Narrowed Sights, Bigger Payoffs: Ransomware in 2019» 6 juin 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019
13. «GOLDEN CHICKENS: Evolution of the MaaS». 20 juillet 2020. QuoIntelligence. https://quointelligence.eu/2020/07/golden-chickens-evolution-of-the-maas/
14. «From Supply Chain to Email, Mobile and the Cloud» 25 juillet 2019. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/
15. «Mobile malware evolution 2019». 25 février 2020. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/
16. «Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics». 17 janvier 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/
17. «Spamhaus Botnet Threat Report 2019». 28 janvier 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019
18. «What Is Fileless Malware?». McAfee. https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html
19. «What is fileless malware and how does it work?» . Norton. https://us.norton.com/internetsecurity-malware-what-is-fileless-malware.html
20. «Trend Micro Report Reveals 265% Growth In Fileless Events». 28 août 2019. Trend Micro. https://www.trendmicro.com/en_hk/about/newsroom/press-releases/2019/2019-08-28.html
21. «Understanding Fileless Threats» 29 juillet 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats

22. «SonicWall Sees Dramatic Jump In IoT Malware, Encrypted Threats, Web App Attacks Through Third Quarter». 22 octobre 2019. SonicWall. https://www.sonicwall.com/news/dramatic-jump-in-iot-malware-encrypted-threats-web-app-attacks-third-quarter/

23. «2020 Vulnerability and Threat Trends». 2020. SKYBOX. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/2020_VT_Trends-Report-reduced.pdf

24. «Over a third of banking malware attacks in 2019 targeted corporate users – demonstrating the need for protection». 16 avril 2019. Kaspersky. https://www.kaspersky.com/about/press-releases/2020_over-a-third-of-banking-malware-attacks-in-2019-targeted-corporate-users-demonstrating-the-need-for-protection

25. «Internet organised crime threat assessment» 2019. EUROPOL (EC3). https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

26. «Narrowed Sights, Bigger Payoffs: Ransomware in 2019» 6 juin 2019. Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

27. «From Supply Chain to Email, Mobile and the Cloud» 25 juillet 2019. CheckPoint. https://www.checkpoint.com/press/2019/check-point-research-from-supply-chain-to-email-mobile-and-the-cloud-no-environment-is-immune-to-cyber-attacks/

28. «Mobile malware evolution 2019». 25 février 2020. Kaspersky. https://securelist.com/mobile-malware-evolution-2019/96280/

29. «Mobile banking malware surges in 2019». 25 juillet 2019. Computer Weekly. https://www.computerweekly.com/news/252467340/Mobile-banking-malware-surges-in-2019

30. «Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics». 17 janvier 2019. Trend Micro. https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/

31. «BlueKeep attacks are happening, but it's not a worm». 3 novembre 2019. ZDNet. https://www.zdnet.com/article/bluekeep-attacks-are-happening-but-its-not-a-worm/

32. MISP Projects. http://www.misp-project.org/

33. «PowerShell, fileless malware's great attack vector». 25 février 2019. Panda. https://www.pandasecurity.com/mediacenter/malware/powershell-fileless-malware-attack-vector/

34. «Airbus Statement on Cyber Incident». 30 janvier 2019. Airbus. https://www.airbus.com/newsroom/press-releases/en/2019/01/airbus-statement-on-cyber-incident.html

35. «Airbus data breach impacts employees in Europe» 30 janvier 2019. ZDNet. https://www.zdnet.com/article/airbus-data-breach-impacts-employees-in-europe/

36. «Massive Quest Diagnostics data breach impacts 12 million patients». 4 juin 2019. ZDNet. https://www.zdnet.com/article/massive-quest-diagnostics-data-breach-impacts-12-million-patients/

37. «Hackers crack 15M LifeLabs accounts, obtain lab results and health card numbers». 17 décembre 2019. Daily Hive. https://dailyhive.com/calgary/lifelabs-hacked-cyber-attack

38. «Why the LifeLabs Hack Likely Is Worse than Most». 18 décembre 2019. The Tyee. https://thetyee.ca/Analysis/2019/12/18/LifeLabs-Data-Hack/

39. «Personal Information in City of Pensacola Cyberattack». 17 janvier 2020. City of Pensacola. https://www.cityofpensacola.com/CivicSend/ViewMessage/Message/100944

40. «Personal data of 2,400 Mindef, SAF staff may have been leaked» 22 décembre 2019. The Straits Times - Singapore. https://www.straitstimes.com/singapore/personal-data-of-2400-mindef-saf-staff-may-have-been-leaked

Références

41. AVTEST – The Independent IT-Security Institute. https://www.av-test.org/en/

42. «Real world protection tests.» AV Comparatives. https://www.av-comparatives.org/dynamic-tests/

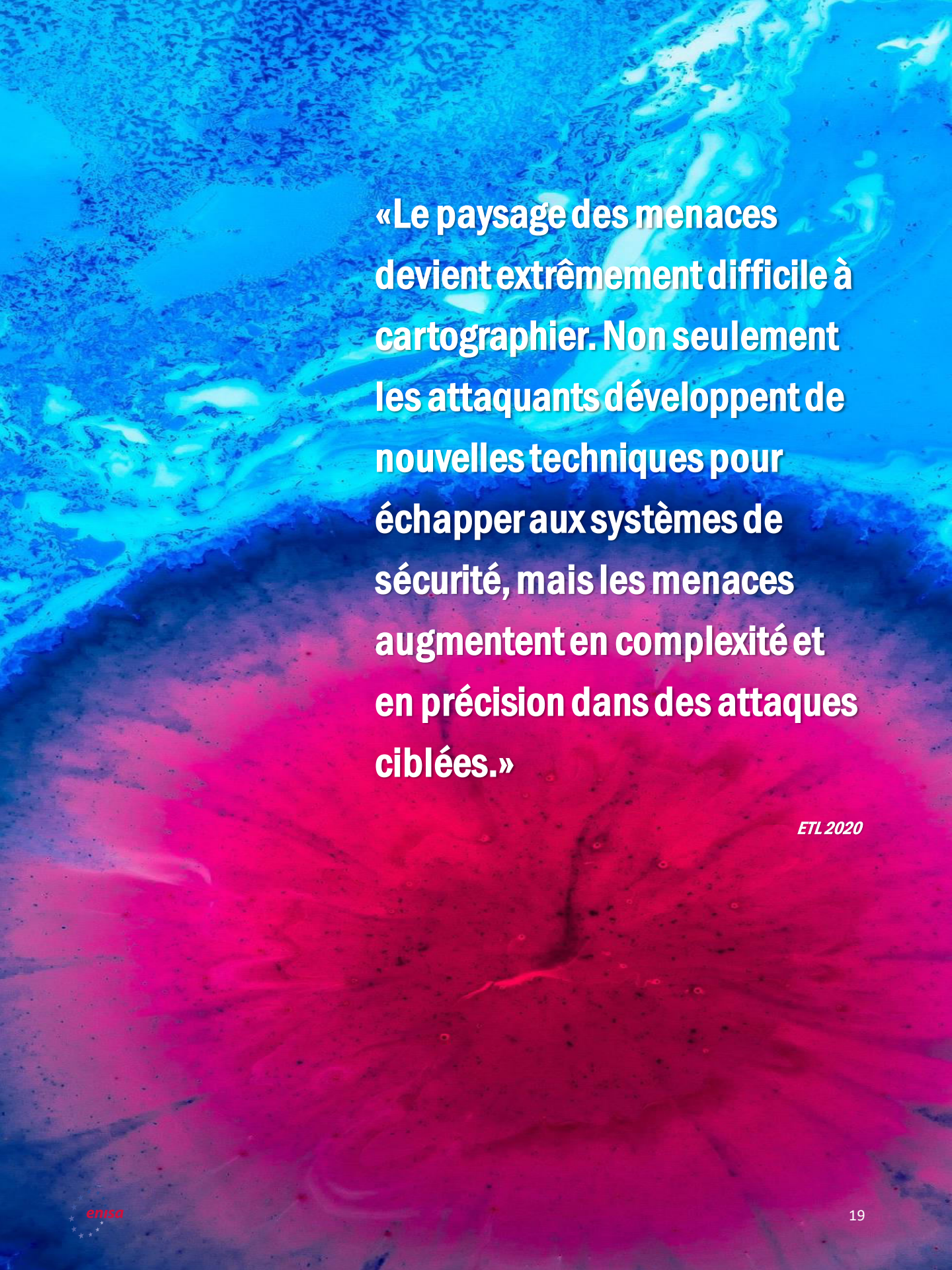
43. «The ThreatHunting Project.» https://www.threathunting.net/data-index

44. Mark Russinovich, Thomas Garnier. «Sysmon v11.10.» 24 juin 2020. Microsoft https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

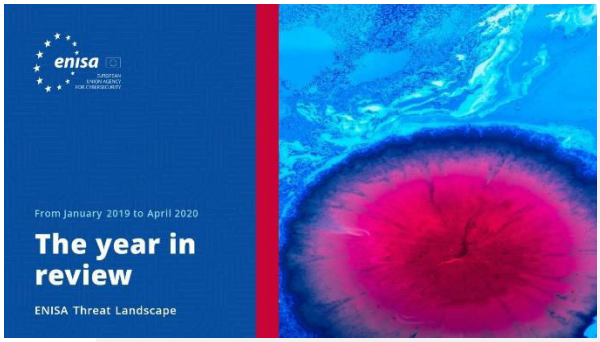
45. «Guide to Intrusion Detection and Prevention Systems (IDPS).» Février 2007. CSRC. https://csrc.nist.gov/publications/detail/sp/800-94/final

47. «Most malware in Q1 2020 was delivered via encrypted HTTPS connections». 25 juin 2020. Help Net Security. https://www.helpnetsecurity.com/2020/06/25/encrypted-malware/

48. «Malware statistics and facts for 2020» 29 juillet 2020. Comparitech. https://www.comparitech.com/antivirus/malware-statistics-facts/


«Le paysage des menaces devient extrêmement difficile à cartographier. Non seulement les attaquants développent de nouvelles techniques pour échapper aux systèmes de sécurité, mais les menaces augmentent en complexité et en précision dans des attaques ciblées.»
ETL 2020

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

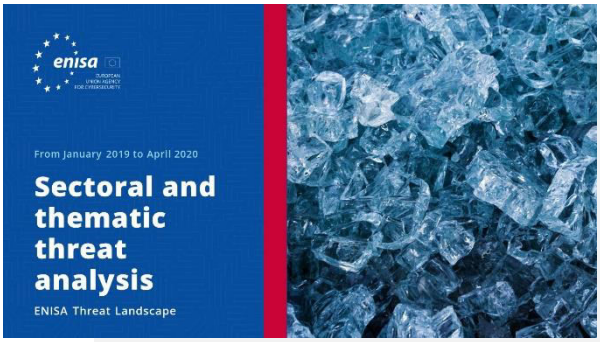
Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.

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