FR

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

De janvier 2019 à avril 2020

Les rançongiciels

Paysage des menaces de l'ENISA

Aperçu

Le rançongiciel (*ransomware*) est désormais une arme populaire entre les mains d'acteurs malveillants qui tentent quotidiennement de nuire aux gouvernements, aux entreprises et aux particuliers. Dans ce cas, la victime du rançongiciel est susceptible de subir des pertes économiques, soit en payant la rançon demandée, soit en payant les frais de recouvrement de la perte si celle-ci ne respecte pas les exigences de l'attaquant. Lors d'un incident survenu en 2019, la ville de Baltimore (Maryland) a subi un blocage dont le rétablissement devrait coûter 18,2 millions de dollars (env. 15,4 millions d'euros), bien que la ville ait refusé de payer la rançon.[1] Au vu du nombre croissant d'incidents, il est évident que l'hypothèse ne repose pas sur le fait de savoir «si» on en sera victime mais plutôt «quand» cela se produira. Cependant, dans la majorité des pays qui luttent contre les rançongiciels, plusieurs problématiques doivent encore être abordées, comme le manque de coordination et de collaboration entre les agences et les autorités, ainsi que l'absence de législation permettant clairement de faire des attaques par rançongiciel un délit.

Bien que des polices de cyberassurance existent depuis le début des années 2000[2], les attaques par rançongiciel sont l'une des principales raisons qui expliquent l'intérêt accru porté à ce type d'assurance ces cinq dernières années. Dans certains incidents survenus en 2019[7], des contrats de la sorte ont permis de couvrir la rançon ou les frais de recouvrement. Malheureusement, en sachant que les cibles potentielles des rançongiciels sont couvertes par une assurance, les attaquants partent du principe qu'ils seront très probablement payés. L'autre revers de la médaille pour la victime, c'est que les compagnies d'assurance garantissent le versement de la rançon par anticipation afin de limiter les dégâts et de préserver l'intégrité de sa réputation, mais ce paiement escompté des rançons encourage la communauté des pirates informatiques, sans pour autant garantir la reprise de l'activité de la victime ni même sa réputation.[3]

Conclusions

10,1_milliards d'euros, c'est le montant estimé des rançons payées en 2019

Le montant des rançons payées a été supérieur de 3,3 milliards d'euros par rapport à 2018.

365 %_de détections en plus dans les entreprises en 2019

La détection des rançongiciels dans les ordinateurs en milieu professionnel a augmenté par rapport au premier semestre 2018.[22]

66 %_des organismes de santé ont subi une attaque

Plus de 66 % des organismes de santé ont été victimes d'une attaque par rançongiciel en 2019.[23]

45 %_des organisations attaquées ont payé la rançon

Ce pourcentage correspond aux organisations attaquées en 2019 qui ont payé la rançon et dont la moitié d'entre elles n'ont toujours pas récupéré leurs données.[37]

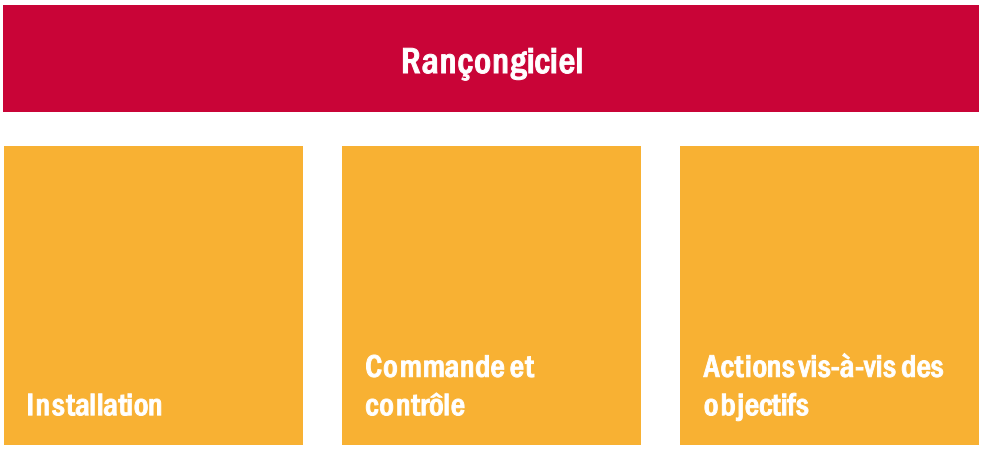
28 %_des incidents de sécurité ont été attribués à des logiciels malveillants

Le rançongiciel a été la deuxième fonctionnalité la plus fréquente après le logiciel malveillant C&C, représentant un tiers (28 %) des incidents de sécurité.[32]

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

Description

_Les rançongiciels visent plus haut

Au premier et au deuxième trimestres 2019, les attaques par rançongiciel ont été moins nombreuses que celles enregistrées pendant la même période au cours des trois années précédentes. Cependant, ces attaques par rançongiciel se sont concentrées sur des cibles de choix. Pendant toute l'année 2018, on a assisté au déploiement de chevaux de Troie d'accès à distance (RAT - *Remote Access Trojan*), de téléchargeurs (*downloaders*) et de portes dérobées (*backdoors*); cependant, en 2019, ces logiciels malveillants sont restés inactifs.[9,10] On en arrive maintenant à la conclusion que ces logiciels ont fourni aux attaquants les renseignements nécessaires pour identifier des cibles vulnérables de haut rang, prêtes à payer des rançons plus élevées. Dans la même veine, au cours de l'année considérée, les rançongiciels se sont étendus à des secteurs autres que celui de la santé, en ciblant des entreprises du secteur de l'industrie et de la fabrication. Dernièrement, la famille de rançongiciels LockerGoga a été utilisée pour endommager des systèmes assurant le contrôle du matériel dans des usines de production.[11]

_La cyberassurance gagne en popularité

En 2019, les polices de cyberassurance ont représenté un marché de 8 milliards de dollars (env. 6,7 milliards d'euros) rien qu'aux États-Unis. Bien que ces produits existent depuis le bug de l'an 2000 (ou bug du millénaire), ces dernières années, ils sont devenus beaucoup plus attrayants pour les organisations gouvernementales, les villes, les organismes de santé et plusieurs autres cibles potentielles de rançongiciel à haut risque. L'attaque SamSam à Atlanta (Géorgie) et l'incident de Lake City (Floride) ont été couverts par ce genre de polices d'assurance.[16] Avec l'augmentation des demandes de rançon, les polices de cyberassurance deviennent de plus en plus nécessaires pour les organisations et les entreprises. Cependant, le bon sens voudrait que les victimes évitent, si possible, de céder aux demandes. Lorsque les demandes de rançon sont honorées, cela encourage non seulement l'attaquant à réitérer son acte, mais la victime est également susceptible de ne pas s'en remettre car, dans bien des cas, l'attaquant ne respecte pas sa part du marché.

_Le protocole RDP (*Remote Desktop Protocol*): un risque élevé

Plusieurs familles de rançongiciels efficaces, tels que SamSam, BitPaymer et CrySiS, prennent pour cible des serveurs RDP pour lancer une attaque.[20] Malheureusement, de nombreuses organisations utilisent encore le protocole RDP au lieu du réseau privé virtuel (VPN - *Virtual Private Network*), plus sûr, pour l'accès à distance. Le problème avec le protocole RDP est qu'il présente des vulnérabilités susceptibles d'être exploitées et que le service RDP peut dépendre de serveurs internet facilement accessibles. Plus de 800 000 systèmes dotés de services RDP ont été signalés comme étant non corrigés et vulnérables; parmi eux, des systèmes dans la plage IP du centre de données Microsoft Azure.[51] Bien que Microsoft ait assuré au public que ces systèmes appartenaient à un tiers, un problème se pose concernant la sécurité des fournisseurs de services en nuage.

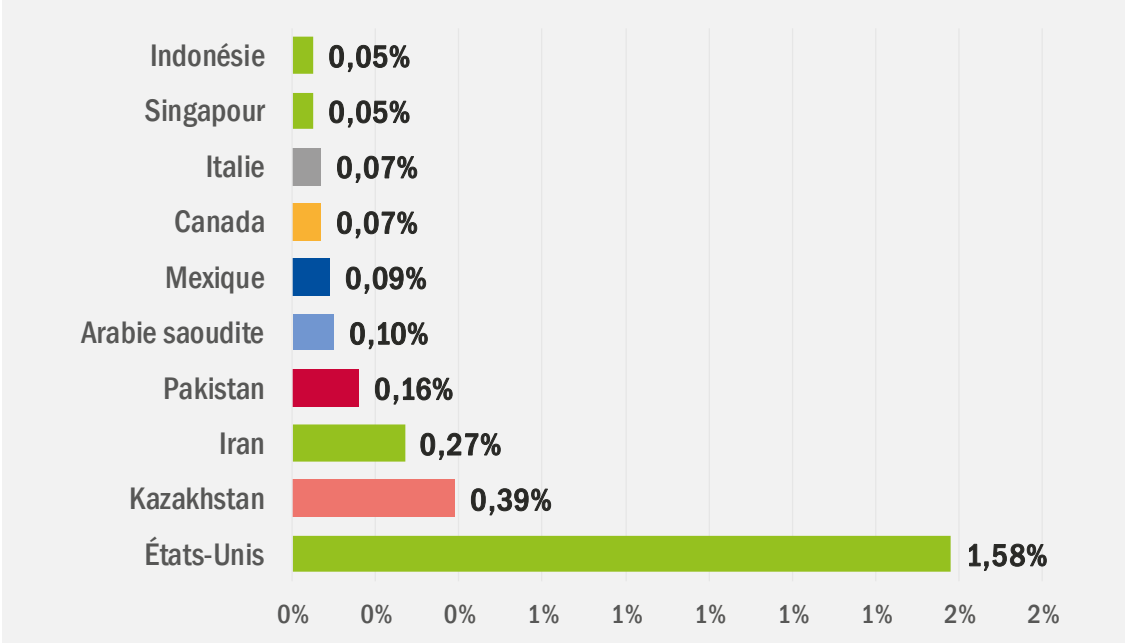


Figure 1: Top 10 des pays attaqués par des chevaux de Troie de type rançongiciel mobile (classement en fonction du pourcentage des utilisateurs attaqués) au deuxième trimestre 2019. Source: Kapersky[34]

Description

_ Les plus recherchés

LOCKERGOGA_ a été signalé pour la première fois en janvier 2019 lors d'une attaque contre Altran Technologies, société française de conseil en ingénierie.[40] Ses réseaux informatiques et toutes ses applications sont tombés en panne, ce qui a affecté ses activités dans plusieurs pays. LockerGoga est émis et exécuté par l'outil PsExec, qui est un substitut léger à Telnet, capable de passer certains contrôles de sécurité en tant que logiciel plus ou moins valide.[11] Une fois installé, les comptes utilisateurs dans le système ciblé sont modifiés et le système est déconnecté de force. En outre, les fichiers de l'outil sont automatiquement renommés et déplacés, ce qui les rend presque impossibles à localiser. Dans les dernières versions de LockerGoga, le verrouillage est si strict que les victimes ne sont même pas en mesure de visualiser la note d'extorsion ou les instructions de restauration, et ce même si les exigences sont satisfaites. Seuls quelques produits antimaliciels et antivirus sont capables de détecter et de défendre les systèmes contre LockerGoga, mais aucun déchiffreur spécifique n'existe.[10] Outre Altran Technologies, NorskHydro et deux entreprises chimiques basées aux États-Unis, à savoir Hexion et Momentive, ont été la cible de LockerGoga en 2019.[41] Pour la seule attaque de NorskHydro, le coût des dommages a été estimé à 50 millions de dollars (env. 42 millions d'euros).[21]

KATYUSHA_ est un cheval de Troie de type rançongiciel utilisé pour la première fois en octobre 2018. Il chiffre les fichiers de la victime, supprime les clichés instantanés (*shadow copies*) et envoie des pièces jointes par courriel. Katyusha utilise les codes d'exploitation EternalBlue et DoublePulsar pour se propager.[45] Malheureusement, aucun outil ni déchiffreur n'est encore disponible comme moyen de défense.

JIGSAW_ ne se contente pas de chiffrer les fichiers de la victime; il les supprime également si les exigences ne sont pas satisfaites dans le délai imparti, qui est généralement de 24 heures. De plus, si la victime tente, par exemple, d'éteindre son ordinateur, la vitesse de suppression augmente. Ce n'est pas un hasard si le nom de ce rançongiciel est tiré d'un personnage de film d'horreur.[45] Cependant, les sociétés de sécurité ne cessent de publier des mises à jour pour garantir l'efficacité du déchiffreur de Jigsaw.[46]

PEWCRYPT_ a été créé début 2019 et, contrairement à la plupart des rançongiciels, son seul but est d'obliger les personnes à s'abonner à la chaîne du youtubeur PewDiePie. PewDiePie était en concurrence avec T-Series, une chaîne indienne Bollywood, pour savoir laquelle était la plus populaire. Ses fans ont donc décidé d'utiliser PewCrypt pour augmenter ses chances de gagner. PewCrypt est un cas typique de rançongiciel qui se propage à l'aide de courriels indésirables et de publicités malveillantes en ligne. Il a été créé dans le langage de programmation Java. En mars 2019, l'auteur lui-même a publié un outil de déchiffrement.[47]

RYUK_ est apparu pour la première fois en août 2018; on a supposé qu'il était associé à des groupes de piratage nord-coréens. Très rapidement, il s'est avéré que les auteurs de Ryuk étaient en fait le même groupe qui s'était fait connaître pour avoir utilisé le rançongiciel Hermès tout en volant son code. Ryuk se caractérise principalement par son utilisation d'algorithmes militaires et ses attaques ciblées sur de grandes entreprises. De plus, il est demandé à la plupart de ses victimes de payer la rançon en bitcoins.[45]

DHARMA_ est un cryptovirus qui est apparu pour la première fois en 2016, mais de nouvelles versions sont toujours en cours de publication. Dharma ne se contente pas de chiffrer les fichiers de la victime, il supprime également tout cliché instantané (*shadow copy*). En 2019, il s'est propagé par l'intermédiaire de fichiers contaminés aux extensions populaires, nuisibles ou légitimes, telles que «.gif», «.AUF», «.USA», «.xwx», «.best» et «.heets». En septembre 2019, un chercheur en sécurité a publié le Rakhnidecryptor[42] pour aider les victimes de Dharma à déchiffrer leurs fichiers.

GANDCRAB_, utilisé pour la première fois en janvier 2018, a infecté plus de 50 000 systèmes en moins d'un mois, devenant ainsi l'un des rançongiciels les plus répandus de 2018.[43] Il exploite les macros Microsoft Office, VBScript et PowerShell pour attaquer sans être détecté.[45] GandCrab est similaire à Cerber, il s'appuie sur le modèle du rançongiciel à la demande (RaaS - *Ransomware-as-a-Service*) et permet aux développeurs ainsi qu'aux criminels de partager les bénéfices. Une équipe créée par Europol, la police roumaine, le bureau du Procureur général de Roumanie et Bitdefender ont réussi à mettre au point un outil de déchiffrement[44] après avoir piraté les serveurs de GandCrab. Les opérateurs de GandCrab ont annoncé leur retraite au deuxième trimestre 2019 après avoir récolté plus de 2 milliards de dollars en versement de rançons. Toutefois, le rançongiciel Sodinokibi, observé dans de petites campagnes, serait le successeur de GandCrab.[10]

Description

_ Les plus recherchés

REVIL ou SODINOKIBI ou SODIN_ est apparu pour la première fois lors d'une attaque web contre l'outil italien WinRAR en juin 2019. Il est également soupçonné d'être impliqué dans trois attaques de prestataires d'infogérance et dans une quatrième contre la société américaine PerCSoft, dont la clientèle est principalement issue du secteur de la santé.[48] Sodinokibi semble être un produit du célèbre groupe de cyberespionnage FruityArmor, actif depuis 2016. Sodinokibi a touché plusieurs pays dans le monde. Taïwan a subi 17,56 % de toutes les attaques de Sodinokibi enregistrées jusqu'à présent, ce qui en fait le pays le plus ciblé par celui-ci. En Europe, les pays les plus visés sont l'Allemagne (8,05 %), l'Italie (5,12 %) et l'Espagne (4,88 %). La distribution de Sodinokibi s'effectue selon un modèle RaaS; il chiffre les fichiers nécessaires pour que l'attaque puisse se dérouler système par système. Les attaquants intègrent une «clé passe-partout» dans leur code, leur permettant ainsi de déchiffrer les fichiers à distance, quel que soit le chiffrement d'origine.[49] Cependant, si l'ordinateur possède un clavier russe, arménien, syrien ou autre, il n'est alors pas possible pour Sodinokibi de le chiffrer, un indice probable quant à l'origine des auteurs.[50]

SAMSAM_ continue de cibler les infrastructures critiques, à l'échelle mondiale, pour la cinquième année consécutive. Les attaques SamSam visent principalement les hôpitaux, les entreprises de santé et les organisations gouvernementales pour garantir le paiement rapide de rançons importantes. Il exploite les vulnérabilités du protocole RDP (*Remote Desktop Protocol*). À ce jour, le groupe responsable de la distribution du rançongiciel SamSam a récolté plus de 6 millions de dollars (env. 5 millions d'euros) sous forme de rançons et il a coûté plus de 30 millions de dollars (env. 25,4 millions d'euros) aux victimes.[45] Pour la seule attaque de 2018 contre la ville d'Atlanta, les dommages et les coûts de recouvrement ont atteint 17 millions de dollars (env. 14,4 millions d'euros).[43]

«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

Description

_ Les secteurs cibles

LES ÉTATS-NATIONS SONT TOUJOURS SOUS LE FEU DES PROJECTEURS_ En 2018, les rançongiciels ont servi à prendre pour cible les organisations des États-nations afin de faire de l'argent. Cette tendance s'est poursuivie en 2019, année au cours de laquelle des nations ou des groupes de nations ont masqué leur identité en utilisant les mêmes outils que ceux créés par d'autres groupes ou acteurs d'États-nations. Cette manipulation d'outils permet à l'attaquant de dissimuler son origine et sa nation afin d'éviter toute conséquence diplomatique, en particulier lorsque la cible est une organisation du gouvernement ou de l'État.

En 2019, plusieurs attaques contre des organisations gouvernementales ou étatiques ont eu lieu, comme celle où il a été demandé à la ville californienne de Lodi[4] de payer une rançon de 400 000 dollars (env. 340 000 euros) pour être libérée du blocage des lignes téléphoniques du département de police, de la ligne d'urgence des travaux publics, des numéros de l'hôtel de ville et des systèmes de paiement et financiers de la ville. Refusant d'obtempérer, la ville s'est remise de l'attaque grâce à des sauvegardes. En août 2019, le département des Ressources d'information du Texas (DIR - *Department of Information Resources*) a fait état d'une attaque coordonnée par rançongiciel contre 23 petites organisations gouvernementales.[5] Le coût pour le comté du Texas a été estimé à 3,25 millions de dollars (env. 2,75 millions d'euros). Baltimore a subi une attaque avec le rançongiciel RobbinHood qui a causé des dommages d'un montant de 18,2 millions de dollars (env. 15,4 millions d'euros); tandis que la ville de Lake City (Floride) a été attaquée par le rançongiciel Ryuk qui a occasionné une perte de 460 000 dollars (env. 389 768 euros). En juillet 2019, une attaque par rançongiciel a également frappé la ville de New Bedford (Massachusetts)[6]; le montant de la rançon exigée pour celle-ci s'élevait à 5,3 millions de dollars (env. 4,4 millions d'euros). La ville a refusé de payer la rançon et a préféré débourser un million de dollars pour se remettre de l'attaque.[7]

LES ÉTABLISSEMENTS D'ENSEIGNEMENT SONT DÉSORMAIS DE LA PARTIE_ En 2019, nous avons observé un changement dans les attaques puisqu'elles s'orientent désormais vers les établissements d'enseignement. Selon un rapport publié par la société de sécurité Emsisoft, 1 051 écoles et universités ont été victimes de 62 incidents par rançongiciel. En 2018, les incidents touchant les établissements d'enseignement n'étaient que de 11. Selon le rapport, les écoles américaines ont été les deuxièmes victimes les plus fréquentes après les municipalités locales.[8]

LE SECTEUR DE LA SANTÉ CONTINUE À SOUFFRIR_ Au cours des années précédentes, les organismes de santé étaient la cible favorite des attaquants par rançongiciel, tendance qui s'est une nouvelle fois confirmée en 2019. Wood Ranch Medical, prestataire de soins californien, a été frappé par une attaque pendant la période estivale. Suite à son refus de payer la rançon, les dossiers médicaux électroniques de la société ont été complètement détruits (y compris les sauvegardes). Cet incident a forcé la société Wood Ranch Medical à annoncer la fermeture de son activité en fin d'année.[12] En avril 2019, un autre prestataire de soins médicaux, Michigan Brookside ENT and Hearing Centre, a connu des événements exactement similaires[13] qui l'ont également obligé à mettre la clé sous la porte. En outre, en Australie, deux groupes hospitaliers ont été attaqués: GippslandHealth Alliance et South West Alliance of Rural Health. Par conséquent, les hôpitaux de plusieurs villes, dont Warrnambool, Colac, Geelong, Warragul, Sale et Bairnsdale, n'ont pas pu accomplir d'actes médicaux normaux car leurs systèmes avaient été mis hors ligne pour limiter l'exposition.[14] Dans ce secteur, la perte de données est tout aussi dommageable que la perte financière. Par exemple, les informations médicales protégées de plus de 300 000 patients ont été divulguées à la suite d'une attaque par rançongiciel lancée en juin 2019 contre le groupe Premier Family Medical dans l'Utah.[15]

L'INFOGÉRANCE EN BAISSE_ De nombreuses industries dépendent de prestataires de services d'infogérance et de fournisseurs de services en nuage pour héberger des informations sensibles, essentielles à leurs activités. Elles comptent également sur eux pour assurer l'intégrité de leurs données et empêcher tout accès non autorisé à celles-ci.[17] Or, les rançongiciels GandCrab et Sodin ciblent les vulnérabilités des services d'infogérance et exposent donc leur infrastructure et les données qu'elles hébergent, permettant ainsi à l'attaque par rançongiciel de se propager à l'ensemble de la clientèle des services d'infogérance. Webroot2FA, outil d'infogérance courant, présente ce genre de vulnérabilités et a été utilisé dans plusieurs affaires en 2019.[18] Cette année, plusieurs services d'infogérance ont été attaqués sur une période de trois mois seulement, comme PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. et IT By Design.[19]

Vecteurs d'attaque

_ Comment

Un nouveau rançongiciel appelé Sodinokibi exploite la vulnérabilité récemment révélée d'Oracle WebLogic Server (CVE-2019-2725) pour permettre l'exécution de codes à distance. La victime est infectée sans qu'aucune mesure ne soit prise. En outre, des correctifs officiels ont été publiés pour Oracle WebLogic Server versions 10.3.6.0 et 12.1.3.0.[51] La même attaque exploite la vulnérabilité CVE-2018-8453 pour obtenir davantage de privilèges d'utilisateur (élévation), mettre fin à la liste noire des processus, supprimer les fichiers sur liste noire et exfiltrer les informations d'hôte.[48]

Une autre vulnérabilité, la CVE-2019-0708, est également utilisée pour l'implantation de rançongiciels. Elle permet une connexion non autorisée via le protocole RDP (*Remote Desktop Protocol*) de Microsoft. En mai 2019, Microsoft a publié des correctifs pour les versions actuelles du système d'exploitation (OS) ainsi que pour les versions qui ne sont plus prises en charge.[51]

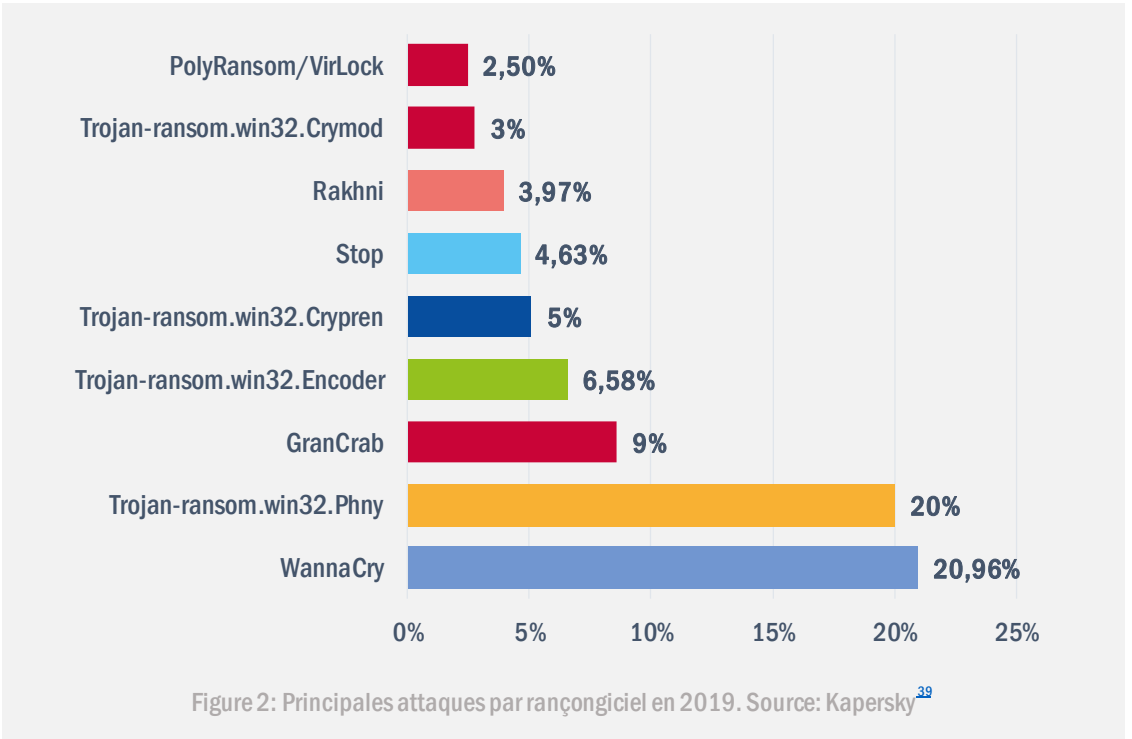


Figure 2: Principales attaques par rançongiciel en 2019. Source: Kapersky[39]

Incidents

- Incident du comté de Baltimore[1]
- Attaque des hôpitaux en Alabama[7]
- Incident de la ville californienne de Lodi[4]
- Incident au Texas (département des Ressources d'information)[5]
- Attaque Ryuk à Lake City (Floride)[7]
- Incident de New Belford (Massachusetts)[6]
- Attaques par rançongiciel contre plus de 500 écoles et universités[8]
- Affaire Wood Ranch Medical (Californie)[12]
- Incident de Michigan Brookside ENT and Hearing Center[13]
- Incidents de Gippsland Health Alliance et South West Alliance of Rural Health (Australie)[14]
- Incident du groupe Premier Family Medical (Utah)[15]
- Incidents d'infogérance de PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. et IT By Design[19]
- Incident du centre de données Microsoft Azure[51]
- Attaque LockerGoga d'Altran Technologies[40]
- Attaque LockerGoga de Norsk Hydro[7]
- Attaques LockerGoga de Hexion et Momentive[41]
- Incident informatique à Albany[60]
- Incident du comté de Jackson (Géorgie)[61]
- Incident de Riviera Beach (Floride)[62]
- Incident de la Nouvelle-Orléans[63]
- Attaque de Demant, fabricant danois d'appareils auditifs[64]

Atténuation

_Actions proposées

- Conserver des sauvegardes fiables respectant la règle du 3-2-1 (c.-à-d. conserver au moins trois copies, sur deux supports différents, en gardant une de ces copies hors site).[5]
- Investir dans une police de cyberassurance qui couvre les dommages en cas d'attaque par rançongiciel.[21]
- Utiliser la segmentation du réseau, le chiffrement des données, le contrôle d'accès et la mise en œuvre d'une politique pour garantir l'exposition minimale des données.
- Utiliser des méthodes telles que la surveillance pour identifier rapidement toute infection.
- Surveiller l'accès à l'infrastructure publique utilisée et son état.
- Créer un service de supervision de la sécurité (SOC - *Security Operation Centre*) doté d'un personnel de sécurité qualifié au sein de chaque organisation ou entreprise.
- Utiliser des outils appropriés et mis à jour pour la prévention des rançongiciels.
- Définir avec précision et mettre en œuvre un minimum de droits d'accès aux données des utilisateurs afin de minimiser l'impact des attaques (c.-à-d. moins de droits, moins de données chiffrées).
- Implémenter une gestion solide des vulnérabilités et des correctifs.
- Mettre en œuvre un filtrage de contenu pour éliminer les pièces jointes indésirables, les courriels au contenu malveillant, les pourriels et le trafic réseau indésirable.
- Protéger les terminaux au moyen de logiciels antivirus tout en bloquant l'exécution de fichiers (par ex., bloquer l'exécution dans le dossier temporaire).
- Instaurer des politiques pour contrôler les périphériques externes et l'accessibilité des ports.
- Établir une liste blanche pour empêcher le lancement d'exécutables inconnus sur les terminaux.
- Investir dans la sensibilisation des utilisateurs aux rançongiciels, notamment concernant les bonnes pratiques de navigation sécurisée.

_Déchiffreurs

Des progrès significatifs ont été réalisés par EUROPOL[7] et 163 partenaires dans le cadre du projet «No more ransom»[7]. En 2019, le portail compte 28 outils supplémentaires et peut désormais déchiffrer 140 types d'infections par rançongiciel.[65] Une poignée de déchiffreurs de rançongiciel ont été développés et de nombreux autres ont été mis à jour. Quelques exemples sont énumérés ci-dessous.

RANÇONGICIELS (*ransomware*)	DÉCHIFFREUR
Aurora[52], **Muhstik**[53], **Ryuk**[54]	Emsisoft
Rakhni, Aura, Autoit, Pletor, Rotor, Lamer, Lortok, Democry, TeslaCrypt, Chimera, Crysis, Jaff, Dharma, Cryakl, Yatron, FortuneCrypt,[55,56]	Kaspersky Lab
GandCrab[44]	Europol, police roumaine et bureau du Procureur général de Roumanie, Bitdefender
Jigsaw[46]	Avast
Mira[57]	F-Secure
Nemty[58]	Tesorion
PewCrypt[47]	Auteur de PewCrypt

Références

1. «Washington idle as ransomware ravages cities big and small» 28 septembre 2019. Politico. https://www.politico.com/news/2019/09/28/ransomware-cities-washington-007376

2. «What you — and your company — should know about cyber insurance», 20 août 2019. Talos. https://blog.talosintelligence.com/2019/08/cyber-insurance-FAQs.html

3. «The State of Ransomware in 2019» 17 juin 2019. IT Pro Today. https://www.itprotoday.com/threat-management/state-ransomware-2019

4. «California City Confirms Phone Line and Financial Data System Disruptions Caused by Ransomware». 2 août 2019. Trend Micro. https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/california-city-confirms-phone-line-and-financial-data-system-disruptions-caused-by-ransomware

5. «Coordinated Ransomware Attack Cripples Local Government Organizations in Texas», 19 août 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coordinated-ransomware-attack-cripples-local-government-organizations-in-texas

6. «The State of Ransomware in the US: Report and Statistics 2019». 12 décembre 2019. EMSISOFT blog. https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

7. «Alabama hospitals have been hit by a massive ransomware attack» 3 octobre 2019. https://www.foxnews.com/tech/alabama-hospitals-ransomware-attack

8. «500+ Schools Have Been Affected by Ransomware in 2019», 4 octobre 2019. Campus Safety, https://www.campussafetymagazine.com/safety/500-schools-ransomware-2019/

9. «Latest Quarterly Threat Report - Q1 2019» 2019. Proof Point. https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

10. «Proofpoint Q2 2019 Threat Report - Emotet's hiatus, mainstream impostor techniques, and more». 19 septembre 2019. Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q2-2019-threat-report-emotets-hiatus-mainstream-impostor-techniques

11. «6 of the Biggest Cybersecurity Crises of 2019 (So Far)» 24 septembre 2019. EC-Council Blog. https://blog.eccouncil.org/6-of-the-biggest-cybersecurity-crises-of-2019-so-far/

12. «Ransomware Attacks Double in 2019: Medical Providers Can't Recover and Shut Down» 3 octobre 2019. https://www.natlawreview.com/article/ransomware-attacks-double-2019-medical-providers-can-t-recover-and-shut-down

13. «Michigan's Brookside ENT and Hearing Center forced to close due to a Ransomware Attack» 23 avril 2019. SPAM Fighter. https://www.spamfighter.com/News-22154-Michigans-Brookside-ENT-and-Hearing-Center-forced-to-close-due-to-a-Ransomware-Attack.htm

14. «Victorian hospitals across Gippsland, Geelong and Warrnambool hit by ransomware attack». 1er octobre 2019. https://www.abc.net.au/news/2019-10-01/victorian-health-services-targeted-by-ransomware-attack/11562988?nw=0

15. «Ransomware Attack Affects 300,000 Patients in Utah». 12 septembre 2019. CISO Mag. https://www.cisomag.com/ransomware-attack-affects-300000-patients-in-utah/

16. «The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks». 27 août 2019. ProPublica. https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

17. «CYBER THREATSCAPE REPORT». 2019. Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

18. «Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread». 2019. Coveware. https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

19. «Armor Identifies 15 New Ransomware Victims in the Last 2 Weeks, All of them Educational Institutions – Threat Intelligence». 20 septembre 2019. Armor. https://www.armor.com/resources/armor-identifies-10-new-ransomware-victims-in-the-past-9-days/

20. «4 Ransomware Trends to Watch in 2019». 13 février 2019. https://www.recordedfuture.com/ransomware-trends-2019/

21. «BDO Cyber Threat Insights - 2019 2nd Quarter Report», juillet 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-2nd-quarter-report

22. «BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare». Octobre 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health

23. «Healthcare Cyber Heists in 2019» 3 octobre 2019. VMWare. https://www.carbonblack.com/resources/threat-research/healthcare-cyber-heists-in-2019/

24. «Australia | Global Threat Report | Defender Power On The Rise». 2019. VMWARE. https://www.carbonblack.com/land/australia-global-threat-report-defender-power-on-the-rise/

25. «France | Global Threat Report | Defender Power On The Rise». 2019. VMWARE. https://www.carbonblack.com/land/france-global-threat-report-defender-power-on-the-rise/

26. «Italy | Global Threat Report | Defender Power On The Rise». 2019. VMWARE. https://www.carbonblack.com/land/italy-global-threat-report-defender-power-on-the-rise/

27. «Japan | Global Threat Report | Defender Power On The Rise». 2019. VMWARE. https://www.carbonblack.com/land/japan-global-threat-report-defender-power-on-the-rise/

28. «Canada | Global Threat Report | Defender Power On The Rise». 2019. VMWARE. https://www.carbonblack.com/land/canada-global-threat-report-defender-power-on-the-rise/

29. «Singapore | Global Threat Report | Defender Power On The Rise». 2019. VMWARE. https://www.carbonblack.com/land/singapore-global-threat-report-defender-power-on-the-rise/

30. «UK | Global Threat Report | Defender Power On The Rise». 2019. VMWARE. https://www.carbonblack.com/land/uk-global-threat-report-defender-power-on-the-rise/

31. «Anticipating the Unknowns». Mars 2019. Cisco. https://ebooks.cisco.com/story/anticipating-unknowns/

32. «2020 Data Breach Investigations Report» 2020. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

33. «IBM Security Study: Taxpayers Oppose Local Governments Paying Hackers in Ransomware Attacks». 5 septembre 2019. IBM. https://newsroom.ibm.com/2019-09-05-IBM-Security-Study-Taxpayers-Oppose-Local-Governments-Paying-Hackers-in-Ransomware-Attacks

34. «IT threat evolution Q2 2019 statistics» 2019 Kaspersky, https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/

35. «IT threat evolution Q1 2019 statistics» 2019 Kaspersky, https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

36. «The state of industrial cybersecurity». Juillet 2019. Kaspersky. https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf

37. «2019 Cyberthreat Defense Report» Cyber Edge Group. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

38. «Evasive Threats, Pervasive Effects». 27 août 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects

39. «IT threat evolution Q3 2019 statistics» 2019 Kaspersky, https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

40. «What You Need to Know About the LockerGoga Ransomware.» 20 mars 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/

41. «BDO Cyber Threat Insights - 2019 2nd Quarter Report», juillet 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-2nd-quarter-report

Références

42. Ransomware DecryptorTools, Kapersky https://noransom.kaspersky.com/

43. «ENISA Threat Landscape Report 2018». 28 janvier 2019. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

44. «New GandCrab v5.1 Decryptor Available Now», 19 février 2019. Bitdefender LABS. https://labs.bitdefender.com/2019/02/new-gandcrab-v5-1-decryptor-available-now/

45. «10 Ransomware Attacks You Should Know About in 2019» 28 avril 2019. Allot. https://www.allot.com/blog/10-ransomware-attacks-2019/

46. Ransomware DecryptorTools. Avast. https://www.avast.com/ransomware-decryption-tools

47. PewCrypt Ransomware Source. GitHub. https://github.com/000JustMe/PewCrypt

48. «Are the REvil, GranCrab Ransomware Families Related?» 25 septembre 2019. MSSP Alert. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/revil-gandcrab-related/

49. «Threat Landscape Report», Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2019.pdf

50. «Sodin Ransomware includes exploit for Windows CVE-2018-8453 bug». 4 juillet 2019. Security Affairs. https://securityaffairs.co/wordpress/87944/malware/sodin-ransomware-cve-2018-8453.html

51. «Threat Landscape Report» 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q2-2019.pdf

52. «Emsisoft Decryptor for Aurora» 2019. Emsisoft. https://www.emsisoft.com/ransomware-decryption-tools/aurora

53. «Emsisoft Decryptor for Muhstik» 2019. Emsisoft. https://www.emsisoft.com/ransomware-decryption-tools/muhstik

54. «Caution! Ryuk Ransomware decryptor damages larger files, even if you pay». 9 décembre 2019. Emsisoft. https://blog.emsisoft.com/en/35023/bug-in-latest-ryuk-decryptor-may-cause-data-loss/

55. «RakhniDecryptor tool for defending against Trojan-Ransom.Win32.Rakhni ransomware». Kaspersky. https://support.kaspersky.com/10556

56. «Another two bite the dust: Kaspersky updates decryption tool to fight ransomware pair». 27 septembre 2019. The Online Citizen. https://www.theonlinecitizen.com/2019/09/27/another-two-bite-the-dust-kaspersky-updates-decryption-tool-to-fight-ransomware-pair/

57. «Mira Ransomware Decryptor» 1er avril 2019. F-Secure. https://blog.f-secure.com/mira-ransomware-decryptor/

58. «Nemty update: decryptors for Nemty 1.5 and 1.6» Tesorion. https://www.tesorion.nl/nemty-update-decryptors-for-nemty-1-5-and-1-6/

59. «McAfee Labs Threats Report», Août 2019. McAfee, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

60. «The 10 biggest ransomware attacks of 2019» CRN. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/2

61. «The 10 biggest ransomware attacks of 2019» CRN. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/3

62. «The 10 biggest ransomware attacks of 2019» CRN. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/6

63. «The 10 biggest ransomware attacks of 2019» CRN. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/7

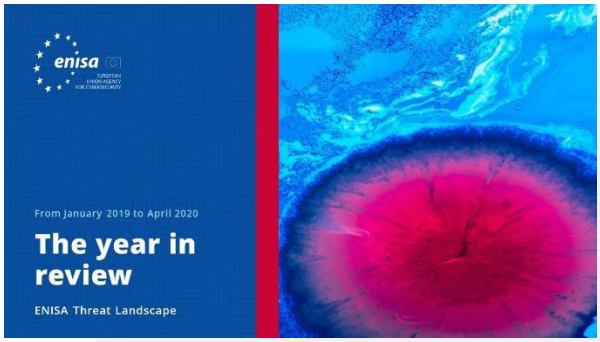
64. «The 10 biggest ransomware attacks of 2019» CRN. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/11

65. https://www.nomoreransom.org/

«Le renseignement sur la cybermenace (CTI) s'est imposé dans le domaine de la cybersécurité comme un instrument essentiel pour améliorer la flexibilité et l'efficacité de la défense contre les cyberattaques.»

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

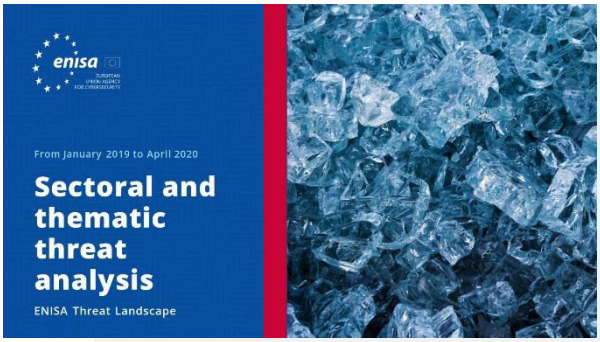
Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.

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

https://www.enisa.europa.eu