enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

FR

De janvier 2019 à avril 2020

L'usurpation d'identité

Paysage des menaces de l'ENISA

Aperçu

L'usurpation d'identité ou la fraude à l'identité est l'utilisation illicite des données d'identification d'une victime par un imposteur pour se faire passer pour cette personne afin d'obtenir un avantage financier et d'autres bénéfices.

Selon un rapport annuel sur la sécurité, au moins 900 cas internationaux d'usurpation d'identité ou de délits liés à l'identité ont été détectés en 2019[1]. Les incidents les plus importants signalés ont été les suivants:

- l'exposition des données à caractère personnel de près de 106 millions de clients américains et canadiens suite à l'incident de violation de données qui a frappé la banque Capital One en mars 2019[2];
- l'exposition de 170 millions de noms d'utilisateurs et de mots de passe utilisés par le développeur de jeux vidéo Zynga en septembre 2019;
- le vol de 20 millions de comptes du service britannique de diffusion audio en continu Mixcloud[3];
- la compromission des données à caractère personnel de 600 000 conducteurs et de 57 millions d'utilisateurs suite à l'incident de violation de données d'Uber en novembre 2019;[3]
- et le vol de 9 millions de dossiers personnels de clients d'EasyJet, comprenant des données de cartes d'identité et de cartes bancaires.

La tendance à l'usurpation d'identité se retrouve en grande partie dans les violations de données qui, par rapport à 2018, ont enregistré un nombre record de 3 800 cas rendus publics, 4,1 milliards de données exposées et une augmentation de 54 % du nombre de violations signalées.[4]

Conclusions

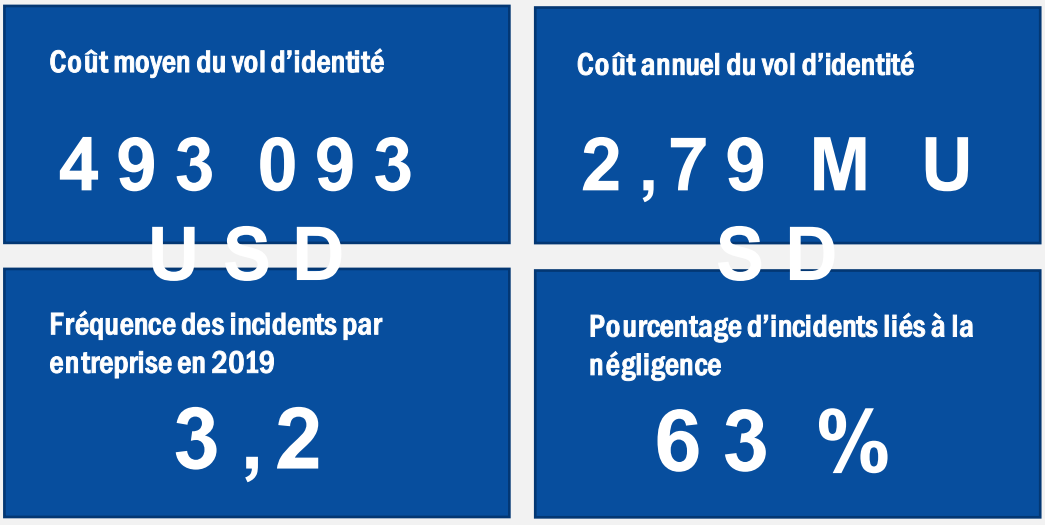


Figure 1: Source: Étude d'IBM Security – Cost of Insider Threats: Global Report[13]

La menace liée à l'usurpation d'identité

En 2019, certains acteurs malveillants à l'origine d'incidents majeurs survenus au cours des années précédentes ont été remis à la justice. En juin, le service de police de la ville de New York, en collaboration avec le FBI, a traduit en justice les membres du groupe «Fraud Ring». Opérant à la fois à l'intérieur et à l'extérieur des États-Unis, ils avaient réussi à voler, en 2012, des identifiants d'iPhones d'une valeur d'un million de dollars (env. 846 000 euros) dans le cadre d'une vaste opération d'usurpation d'identité. Jusqu'à l'arrestation de ce groupe, le montant total des vols a atteint 19 millions de dollars (env. 16 millions d'euros)[4]. Un mois plus tard, l'«accord Equifax» a été annoncé publiquement[5]. La société Equifax a dû accepter d'indemniser la Commission fédérale du commerce des États-Unis (FTC - *Federal Trade Commission*), le Bureau de protection financière des consommateurs (CFPB - *Consumer Financial Protection Bureau*), 48 États, ainsi que les districts de Columbia et de Puerto Rico pour le préjudice lié à sa violation de données survenue en 2017, indemnisation qui s'élèvera au moins à 575 millions de dollars (env. 487 millions d'euros). En raison de cette violation de données, jugée «tout à fait évitable», près de 148 millions d'adresses et de numéros de sécurité sociale d'Américains avaient été divulgués. En fin d'année, le Brésil a infligé à Facebook une amende de 1,6 million de dollars (env. 1,35 million d'euros) au nom de citoyens brésiliens pour la fuite de données en faveur de Cambridge Analytica.[3]

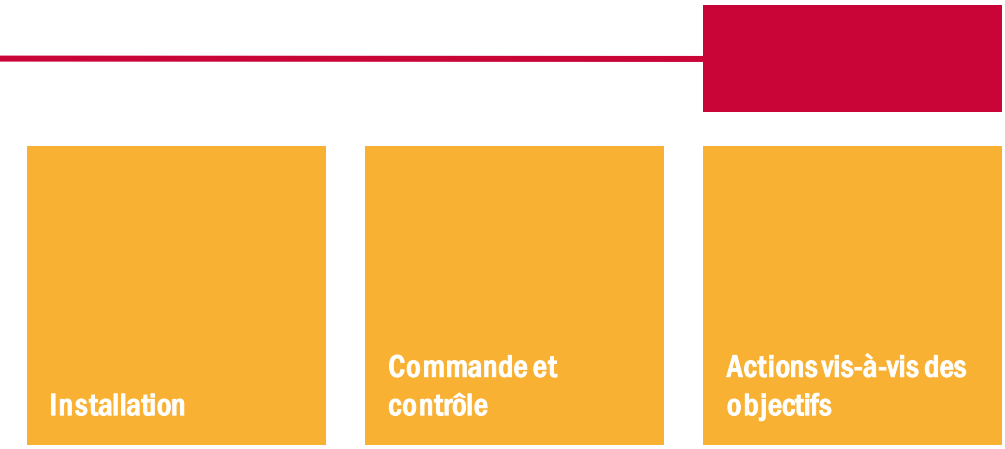
Chaîne de frappe

Usurpation d'identité

Reconnaissance	Armement	Livraison	Exploitation

Étape du processus d'attaque

Ampleur de l'objectif



Mis au point par Lockheed Martin, le modèle de Cyber Kill Chain® s'inspire d'un concept militaire lié à la structure d'une attaque. Pour étudier un vecteur d'attaque en particulier, utilisez cette chaîne de frappe schématisée pour représenter chaque étape du processus puis référencer les outils, les techniques et les procédures utilisés par l'attaquant.

EN SAVOIR PLUS

Tendances

_Les attaques d'usurpation de marque

Conformément à la tendance observée en 2018, certaines marques sont privilégiées dans les attaques d'usurpation en raison de leur forte réputation. Même si ces marques favorites, à l'image de Microsoft (44 %) et d'Amazon (17 %), restent en tête du classement pour les attaques d'usurpation de marque en 2019, on remarque de nouvelles entrées dans le classement comme l'administration fiscale américaine (IRS - *Internal Revenue Service*).[7] Les informations sensibles figurant dans le formulaire W-2 (*Wage and Tax Statement*) ont toujours attiré les imposteurs qui, au cours de l'année considérée, se sont fait passer pour l'IRS dans 10 % des courriels d'usurpation d'identité. En conséquence, des formulaires W-2 valides et des formulaires standard de déclaration de revenus pour les particuliers (1040 - *US Individual Tax Return*) sont disponibles sur les réseaux clandestins en ligne (*dark web*) à un tarif compris entre 1 et 52 USD.

Ces documents, associés aux numéros de sécurité sociale et aux dates de naissance, également disponibles, permettent à tout *hacker* inexpérimenté prêt à investir un montant de 1 000 dollars (env. 846 euros) d'accéder légalement à un compte bancaire basé aux États-Unis, de remplir une fausse déclaration de revenus, de demander un remboursement et d'encaisser un investissement qui a doublé voire triplé. Selon le Bureau d'enquêtes criminelles de l'IRS (*IRS Criminal Investigation*), plus de 10 000 déclarations de revenus des particuliers accompagnées de demandes de remboursement supérieures à 83 millions de dollars (env. 70 millions d'euros) étaient potentiellement frauduleuses.[9]

Le cycle des étapes de la fraude fiscale «Dirty Dozen»

Figure 2 - Source: BDO[19]

Tendances

_Le *SIM-Swapping*: usurpation d'identité par carte SIM

Utilisée depuis 2016, cette technique visait initialement les détenteurs de cryptomonnaies. Cependant, en 2019, la même technique a été utilisée contre des personnes ou des comptes très en vue dans l'intention d'usurper l'identité de la victime. Un certain nombre de victimes de fraude à la carte SIM (*SIM-Swapping*) ont été enregistrées, comme Jack Dorsey (PDG de Twitter), Jessica Alba (actrice), Shane Dawson (acteur), Amanda Cerny (actrice, victime à deux reprises), Matthew Smith (acteur, victime à quatre reprises) et King Bach (artiste).[10] La technique du *SIM-Swapping* a également été utilisée de façon massive dans deux affaires: dans la plus grande banque du Mozambique, où près de 50 000 dollars (env. 42 300 euros) ont été volés sur des comptes d'entreprises de renom, et au Brésil, où 5 000 victimes, principalement des hommes politiques, des ministres et des gouverneurs, ont vu leurs comptes piratés par un gang organisé.[11]

_Les cartes cadeaux utilisées comme cheval de Troie pour compromettre la messagerie d'entreprise

En 2019, les attaques par compromission de la messagerie en entreprise (BEC - *Business Email Compromise*) ont causé des pertes de plusieurs milliards d'euros. Dans de tels incidents, les attaquants se font passer pour une personne de confiance, appartenant généralement à l'entreprise, pour inciter la victime par la ruse à effectuer une transaction financière ou à divulguer des informations sensibles, personnelles ou professionnelles. Dans plus de la moitié des attaques BEC, la victime a été incitée à acheter une carte cadeau. Au cours de la procédure d'achat, des informations sensibles, telles que des références de compte bancaire, ont été interceptées. La victime a également été contrainte d'envoyer la carte cadeau à l'attaquant, comme option d'encaissement anonyme, irréversible et directe. Le montant moyen dérobé par carte cadeau a atteint 1 500 dollars (env. 1 269 euros).[12]

Conclusions

20 %_ **des attaques d'usurpation d'identité ont utilisé des comptes compromis**[7]

30 %_ **des comptes de cadres supérieurs ciblés par des attaques ont été compromis par tromperie du nom affiché**[7]

65 %_ **des attaques BEC ont incité les victimes à acheter des cartes cadeaux**[12]

3,32_ **millions d'euros, c'est le coût moyen d'une violation de données**

95 %_ **des personnes ayant répondu à une enquête Eurobaromètre considèrent l'usurpation d'identité comme un délit grave**

Tendances

Les doubles numériques

La technique antifraude des «masques numériques» a été dévoilée lorsque plus de 60 000 identités numériques volées ont été découvertes en vente, en avril 2019, sur Genesis, un marché du darknet. Ces doubles numériques étaient facilement disponibles à l'achat, pour une valeur allant de 5 à 200 USD chacun. Il est plus facile pour le propriétaire d'un double d'imiter un utilisateur réel dans une boutique en ligne ou sur un système de paiement, surtout si ce double est associé à des identifiants et des mots de passe volés. Outre l'achat de doubles numériques, de nouveaux outils sont apparus pour aider l'usurpateur potentiel, à l'image du navigateurTenebris qui intègre un générateur capable de développer des empreintes digitales et des masques numériques uniques.[11]

Ces dernières années, les copieurs de carte (*skimmers*), les fouilleurs de poubelles (*dumpster divers*), les pirates informatiques (*hackers*), les usurpateurs de droits d'administrateur (*administrator impersonators*) et les hameçonneurs (*phishers*) ont été identifiés comme les principaux groupes à l'origine des attaques d'usurpation d'identité. Cette liste s'est élargie en 2019 avec l'arrivée des hameçonneurs vocaux (*vishers*) et des hameçonneurs par SMS (*smishers*). Les *vishers* opèrent par téléphone. Contrairement aux imposteurs téléphoniques, les *vishers* prétendent représenter une organisation bien connue et proposent d'aider la victime en lui rendant un service lié, par exemple, à la gestion d'un logiciel informatique, à une question financière ou à un remboursement d'impôts. Les *smishers* envoient de faux SMS qui, en cas de réponse du destinataire, détournent ou redirigent directement l'appareil vers un site d'hameçonnage.

La figure ci-après montre les principaux types de données perdues en 2019, les informations de messagerie représentant le plus grand nombre de données perdues ou volées. Ces chiffres révèlent la gravité de la situation puisque les courriels peuvent contenir des informations sensibles à caractère personnel, professionnel et officiel.

Principaux types de données perdues en 2019

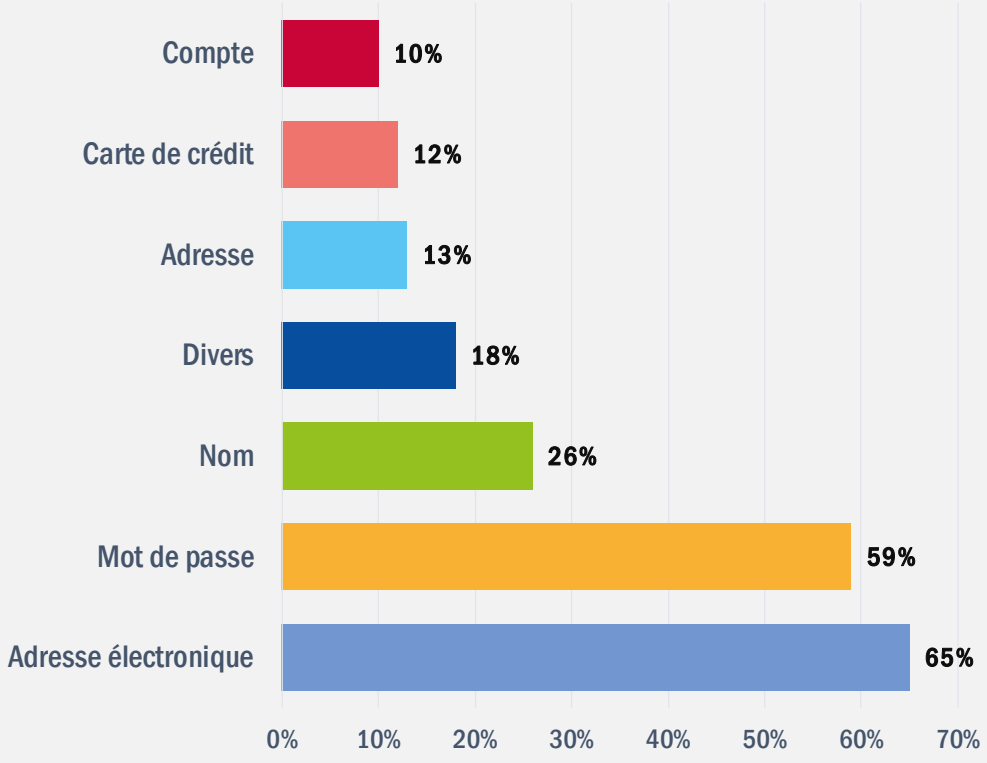


Figure 3 - Source: RiskBased SECURITY[8]

Vecteurs d'attaque

Comment

- **LE NUAGE: UNE INTERFACE POUR S'ATTAQUER AUX DONNÉES DES CLIENTS**. Au cours de l'année considérée, Amazon CloudFront, un réseau de diffusion de contenus (CDN - *Content Delivery Network*), a été compromis.[14] Les sites web hébergés ou liés à des bibliothèques sur l'infrastructure d'Amazon ont été exposés, révélant des contenus chargés en externe, y compris des données de cartes bancaires.
- **URL D'HAMEÇONNAGE**. Les techniques communes d'URL malveillantes[16], comme le cybersquattage (*domain squatting*), l'assombrissement de domaine (*domain shadowing*) et les raccourcisseurs d'URL (*URL shorteners*), ont de nouveau été utilisées en 2019. Au dernier trimestre 2019, on a constaté que 26 % des domaines malveillants utilisaient un certificat sécurisé et qu'un de ces certificats sur trois était de type SSL. Cette astuce a perturbé le jugement des visiteurs qui avaient jusqu'alors pour habitude de se fier à l'icône du cadenas dans leur navigateur comme signe de sécurité.[15]
- **ESCROQUERIE W2**. L'escroquerie W2 est une autre attaque qui vise les dossiers des entreprises et des organisations pour accéder à des informations sensibles. Cette escroquerie commence par l'usurpation d'identité d'un membre de la direction du service des finances ou des ressources humaines dans le but d'obtenir des données sur les employés. Ces données sont ensuite utilisées pour l'usurpation d'identité. Cette escroquerie porte le nom du formulaire fiscal américain W2 utilisé pour déclarer les salaires des employés. Bien qu'ancienne (puisque signalée pour la première fois en 2016 par l'IRS), cette arnaque d'ingénierie sociale n'a cessé de gagner en intensité, avec une augmentation de 10 % tous les ans depuis quelques années.[9,17]
- **NIMCY**. En 2019, un outil d'hameçonnage ciblé, appelé Nimcy, a été introduit par le groupe responsable de la famille de logiciels malveillants Zebrocy. Il a été développé au moyen du langage de programmation Nim (anciennement Nimrod), créé par le même groupe de pirates informatiques. Ce nouveau programme, à la fois téléchargeur (*downloader*) et porte dérobée (*backdoor*), a servi à voler des identifiants de connexion, des frappes, des communications et des fichiers auprès de diplomates, de fonctionnaires de la défense et de membres du personnel ministériel dans le secteur des affaires étrangères. Il semble que les attaquants se soient focalisés sur les gouvernements d'Asie centrale, avec une préférence pour le Pakistan et l'Inde.[14]

- **MENACES MOBILES.** Une augmentation des applications mobiles malveillantes a été constatée en 2019, tendance qui s'est poursuivie en 2020. Des plateformes parmi les plus utilisées et les plus fiables, telles que Google Play, ont, elles aussi, hébergé des applications visant à voler des identifiants (par ex., Acesse SantaMobile ou Modulo ID). Cependant, le nombre de téléchargements s'est révélé extrêmement faible, indiquant que les victimes potentielles n'étaient pas dupes.[20]
- **TROJAN-BANKER.ANDROIDOS.SVPENG.AK** Il s'agit du huitième cheval de Troie pour appareils mobiles le plus populaire qui est également le cheval de Troie bancaire mobile le plus répandu, respectivement responsable de 1,75 % et 16,85 % des attaques uniques, visant principalement les références bancaires et les codes d'authentification à deux facteurs de ses victimes. La majorité des victimes de ce cheval de Troie se trouvent en Russie, ce qui en fait le premier pays en termes de pourcentage d'utilisateurs attaqués par des chevaux de Troie bancaires mobiles.[21]
- **LE *FORMJACKING* OU LE VOL DE FORMULAIRE.** Le vol de formulaire (*formjacking)* était une pratique très courante en 2018, mais il semble que le nombre d'attaques ait considérablement diminué au cours du premier trimestre 2019. Cependant, à partir de mai, suite à l'attaque d'un professionnel de la santé américain au cours de laquelle des identifiants de connexion ont été volés, le nombre d'attaques a continué à grimper pendant le reste de l'année. Au cours de ce mois, un nombre record de 1,1 million de détections a été enregistré. Les cinq pays enregistrant le plus grand nombre d'attaques de *formjacking* en 2019 ont été les États-Unis (51,8 %), l'Australie (8,1 %), l'Inde (5,7 %), le Royaume-Uni (4,1 %) et le Brésil (3,5 %). Le groupe de pirates informatiques Magecart est fortement associé à la plupart des outils de *formjacking* mis au point, ainsi qu'aux attaques contre British Airways, Newegg, Feedify et Ticketmaster[22]

Atténuation

_Actions proposées

- Éviter d'utiliser le gestionnaire de mots de passe fourni par le navigateur. En cas de besoin, utiliser un gestionnaire de mots de passe protégé hors ligne.[23]
- Authentifier tout expéditeur d'une demande de transfert d'argent par téléphone ou en personne.[19]
- Ne pas partager d'informations sensibles, comme des renseignements médicaux, sur des notes manuscrites afin d'éviter toute perte ou égarement. Les fichiers numériques conviennent mieux aux données dont la durée de vie est courte, ils devraient ensuite être complètement détruits.
- Utiliser la «chasse aux menaces» au sein de votre entreprise pour renforcer les plans de sécurité. La chasse aux menaces est effectuée par des membres compétents de l'équipe du service de supervision de la sécurité (SOC - *Security Operation Centre*) afin d'identifier de manière préventive les vulnérabilités et d'empêcher les menaces de les exploiter.
- Appliquer des politiques, telles que des règles basées sur la vitesse, pour atténuer la fraude à l'identité, en particulier pour les transactions par carte de paiement. Les données machine des transactions valides peuvent fournir suffisamment d'informations pour la définition d'une politique optimale.
- Utiliser la méthode d'authentification unique (SSO - *Single Sign-On*), le cas échéant, permettant à un utilisateur d'accéder à plusieurs applications avec le même ensemble d'identifiants numériques. Son utilisation est fortement recommandée pour minimiser le nombre de comptes utilisateurs et d'identifiants stockés.
- Protéger les terminaux au moyen de logiciels antivirus tout en bloquant de manière appropriée l'exécution de fichiers (par ex., bloquer l'exécution dans le dossier temporaire).
- L'authentification multifacteur est une mesure de sécurité permettant de surmonter le piratage ou la perte de mots de passe et de garantir la réussite du processus d'authentification avec de multiples clés. L'introduction de l'authentification multifacteur adaptative permet d'optimiser le processus d'authentification en fonction du comportement de l'utilisateur et du contexte associé.

- Vérifier les URL envoyées par courriel ou consultées de façon aléatoire en fonction de leur adresse IP, de l'ASN associé à l'IP, du propriétaire du domaine et de la relation entre ce domaine et d'autres, avant de prendre d'autres mesures.
- Les organisations utilisant des services en nuage doivent disposer de mesures de sécurité strictes pour leurs opérations dans le nuage et, de préférence, utiliser simultanément une architecture de stockage sur site, de stockage en nuage privé et de stockage en nuage public pour protéger les données à caractère personnel de leurs clients.
- Imposer l'utilisation de méthodes de chiffrement solides et actualisées, telles que TLS 1.3 (utilisant des clés éphémères), pour les données sensibles afin de prévenir le piratage.
- Protéger de façon adéquate tous les documents d'identité et leurs copies (physiques ou numériques) contre tout accès non autorisé.
- Ne pas divulguer d'informations d'identification à des destinataires non sollicités et ne pas répondre aux demandes faites par téléphone, par courriel ou en personne.
- Imposer l'utilisation d'appareils protégés par mot de passe, en veillant à la bonne qualité des identifiants, et sécuriser leurs méthodes de stockage.
- Veiller à la bonne qualité des identifiants et sécuriser leurs méthodes de stockage sur tous les supports utilisés.
- Faire particulièrement attention en cas d'utilisation de réseaux Wi-Fi publics, car les fraudeurs les piratent ou les imitent. En cas d'utilisation d'un de ces réseaux, éviter d'accéder à des applications et données sensibles. Utiliser un réseau privé virtuel (VPN - *Virtual Private Network*) de confiance pour vous connecter aux réseaux Wi-Fi publics.
- Vérifier régulièrement les opérations faisant l'objet de relevés bancaires ou de reçus afin de détecter toute irrégularité.
- Installer un filtrage de contenu pour éliminer les pièces jointes indésirables, les courriels au contenu malveillant, les pourriels et le trafic réseau indésirable.
- Imposer l'application de solutions de prévention contre la perte de données (DLP - *Data Loss Prevention*).

Références

1. «2019 identity theft report released» 31 juillet 2019. ITIJ. https://www.itij.com/latest/news/2019-identity-theft-report-released

2. «Capital One data breach: What you can do now following bank hack» 12 août 2019. C | Net. https://www.cnet.com/how-to/capital-one-data-breach-what-you-can-do-now-following-bank-hack/

3. «Cybercrime Diary, Vol. 4, No. 4: Who's Hacked? Latest Data Breaches And Cyberattacks». 8 janvier 2020. Cyber crime Magazine. https://cybersecurityventures.com/cybercrime-diary-q1-2020-whos-hacked-latest-data-breaches-and-cyberattacks/

4. «$19 million worth of iPhones stolen in massive identity theft scam» 15 juin 2019. 9To5Mac. https://9to5mac.com/2019/06/05/19-million-worth-of-iphones/

5. «Equifax to pay at least $575 million as part of FTC settlement» 22 juillet 2019. C | Net. https://www.cnet.com/news/equifax-to-pay-at-least-575m-as-part-of-ftc-settlement/

6. «2019 data breaches: 4 billion records breached so far» Norton. https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html

7. «Q1 2019: Email Fraud and Identity Deception Trends» Agari. https://www.agari.com/insights/ebooks/2019-q1-report/

8. «Data Breach QuickView Report, 2019 Q3 trends.» Novembre 2019. RiskBased SECURITY. https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf

9. «IRS issues 2019 annual report; highlights program areas across the agency» 6 janvier 2020. IRS. https://www.irs.gov/newsroom/irs-issues-2019-annual-report-highlights-program-areas-across-the-agency

10. «Hackers Hit Twitter C.E.O. Jack Dorsey in a "SIM Swap." You're at Risk, Too» 5 septembre 2019. The New York Times. https://www.nytimes.com/2019/09/05/technology/sim-swap-jack-dorsey-hack.html

11. «IT threat evolution Q2 2019» 19 août 2019. Kaspersky. https://securelist.com/it-threat-evolution-q2-2019/91994/

12. «Phishing Activity Trends Report» 12 septembre 2019. Anti-phishing Working Group. https://docs.apwg.org/reports/apwg_trends_report_q2_2019.pdf

13. «The Cost of Insider Threats» IBM. https://www.ibm.com/downloads/cas/LQZ4RONE

14. «APT trends report Q2 2019» 1er août 2019. Kaspersky. https://securelist.com/apt-trends-report-q2-2019/91897/

15. «Proof Point Q3 2019 threat report: Emotets return, rats reign supreme and more» Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

16. ENISA Threat Landscape Report 2018. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

17. «Q2 2019 Cryptocurrency Anti-Money Laundering Report» Cipher Trace. https://ciphertrace.com/q2-2019-cryptocurrency-anti-money-laundering-report/

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

19. «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

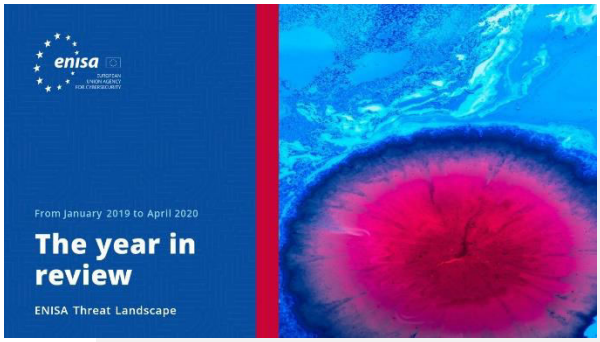
20. «IT threat evolution Q1 2019. Statistics» 23 mai 2019. Kaspersky. https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

21. «IT threat evolution Q3 2019. Statistics» 29 novembre 2019. Kaspersky. https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

22. «FORMJACKING: How Malicious JavaScript Code is Stealing User Data from Thousands of Websites Each Month» Août 2019. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-formjacking-deep-dive-en.pdf

23. «Tax Fraud & "Identity Theft On Demand" Continue to Take Shape on the Dark Web» VMWare. https://www.carbonblack.com/resources/threat-research/tax-fraud-identity-theft-dark-web/

Documents connexes



LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Bilan de l'année**

Résumé des tendances en matière de cybersécurité observées entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

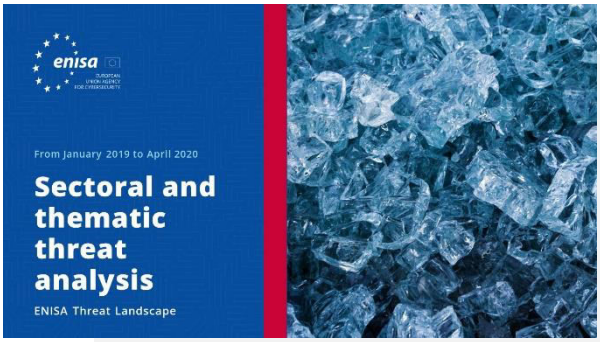
Rapport sur le Paysage des menaces de l'ENISA
Liste des 15 principales menaces

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

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA
Thèmes de recherche

Recommandations concernant les thèmes de recherche provenant de divers secteurs de la cybersécurité et du renseignement sur la cybermenace.



LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Analyse sectorielle et thématique de la menace**

Analyse contextualisée de la menace entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Tendances émergentes**

Principales tendances en matière de cybersécurité observées entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA
Aperçu du renseignement sur la cybermenace

L'état actuel du renseignement sur la cybermenace dans l'UE.

À propos

_ L'Agence

L'Agence de l'Union européenne pour la cybersécurité (ENISA) est l'agence de l'Union dont la mission consiste à garantir un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'Union européenne sur la cybersécurité, l'ENISA contribue à la politique de l'Union en matière de cybersécurité, améliore la fiabilité des produits, services et processus TIC à l'aide de schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'Union, et aide l'Europe à se préparer aux défis cybernétiques de demain. En partageant les connaissances, en renforçant les capacités et en organisant des initiatives de sensibilisation, l'Agence œuvre de concert avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, améliorer la résilience des infrastructures de l'Union et, au bout du compte, maintenir la sécurité numérique de la société européenne et de ses citoyens. Pour plus d'informations sur l'ENISA et ses travaux, consultez le site https://www.enisa.europa.eu/media/enisa-en-francais/.

Contributeurs

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) et *tous les membres du groupe des parties prenantes CTI de l'ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT-UE) et Thomas Hemker.

Éditeurs

Marco Barros Lourenço (ENISA) et Louis Marinos (ENISA).

Contact

Pour toute question sur ce document, veuillez utiliser l'adresse enisa.threat.information@enisa.europa.eu.

Pour les demandes de renseignements des médias concernant le présent document, veuillez utiliser l'adresse press@enisa.europa.eu.

Nous aimerions avoir votre avis sur ce rapport!
Merci de prendre un moment pour remplir le questionnaire. Pour accéder au formulaire, veuillez cliquer ici.

Avis juridique

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

Les sources de tiers sont citées de façon adéquate. L'ENISA n'est pas responsable du contenu des sources externes, notamment des sites web externes, mentionnées dans la présente publication.

La présente publication est uniquement destinée à des fins d'informations. Elle doit être accessible gratuitement. Ni l'ENISA ni aucune personne agissant en son nom n'est responsable de l'utilisation qui pourrait être faite des informations contenues dans la présente publication.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grèce
Tél.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu