enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

FR

De janvier 2019 à avril 2020

L'hameçonnage

Paysage des menaces de l'ENISA

Aperçu

L'hameçonnage (*phishing*) est une technique frauduleuse qui consiste à voler des données d'utilisateur comme des identifiants de connexion, des informations de carte bancaire, voire de l'argent, en utilisant des méthodes d'ingénierie sociale (*social engineering*). **Ce type d'attaque est généralement lancé par messages électroniques, semblant provenir d'une source fiable, dont le but est de persuader l'utilisateur d'ouvrir une pièce jointe malveillante ou de cliquer sur une URL frauduleuse.** Une forme ciblée d'hameçonnage appelée *spearphishing* s'appuie sur des recherches préalables concernant les victimes afin que l'arnaque semble plus authentique; c'est pourquoi ce type d'attaque est l'une des plus efficaces sur les réseaux d'entreprises.[1]

De nombreux individus victimes d'hameçonnage justifient leur acte par une réaction émotionnelle et c'est exactement ce que recherchent les pirates informatiques. Toute simulation d'hameçonnage réalisée dans le cadre d'une formation devra essayer de reproduire cet aspect. La formation des utilisateurs de messagerie électronique est l'une des mesures souvent utilisées pour prévenir l'hameçonnage, mais les résultats ne sont pas convaincants car les auteurs de menace changent constamment de mode opératoire. La norme DMARC (*Domain-based Message Authentication, Reporting and Conformance*) garantit le blocage de tout courriel provenant de domaines frauduleux, permettant ainsi de réduire le taux de réussite des attaques d'hameçonnage, d'usurpation (*spoofing*) et de pourriels (*spams*).

Dans les années à venir, le courriel restera le moyen privilégié pour l'hameçonnage, mais plus pour longtemps. Nous constatons déjà une augmentation de l'utilisation des messageries de médias sociaux, de WhatsApp et autres pour mener des attaques. Le changement le plus important portera sur les méthodes utilisées pour envoyer les messages; celles-ci seront de plus en plus sophistiquées avec l'adoption de l'intelligence artificielle (IA) hostile pour préparer et envoyer les messages. L'hameçonnage (*phishing*) et l'hameçonnage ciblé (*spearphishing*) sont des vecteurs d'attaque majeurs pour d'autres menaces, par exemple les menaces internes involontaires.

Conclusions

26,2_ **milliards de dollars de pertes en 2019 occasionnées par des attaques par compromission de la messagerie d'entreprise (BEC - *Business E-mail Compromise*)[20]**

42,8 %_ **de toutes les pièces jointes malveillantes se présentaient sous forme de documents Microsoft Office[25]**

667 %_ **d'augmentation des escroqueries par hameçonnage en seulement 1 mois pendant la pandémie de COVID-19[6]**

30 %_ **des messages d'hameçonnage ont été distribués un lundi[29]**

32,5 %_ **de l'ensemble des courriels comprenaient le mot clé «paiement» dans l'objet du message[28]**

Chaîne de frappe

Hameçonnage

Reconnaissance

Armement

Livraison

Exploitation

Étape du processus d'attaque

Ampleur de l'objectif

Installation

Commande et contrôle

Actions vis-à-vis des objectifs

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

EN SAVOIR PLUS

Tendances

_Messagerie web et SaaS: types de services les plus ciblés

Selon certaines projections et pour la première fois au premier trimestre 2019, les attaques par hameçonnage visant les services de type SaaS (*Software-as-a-Service*) et de messagerie web ont dépassé celles contre les services de paiement; il s'agit donc des services les plus touchés avec 36 % de toutes les attaques d'hameçonnage.[2] Cette nouvelle tendance suit celle de 2018, année au cours de laquelle les services SaaS et de messagerie web avaient tout juste dépassé le secteur financier[3]. Bien que ce chiffre soit tombé à 30,8 % fin 2019, les services susmentionnés sont restés en tête de liste[2,3], **les services de Microsoft 365 représentant la principale cible des hameçonneurs**.[4]

_Les attaques de type BEC (compromission de la messagerie en entreprise) restent un problème

Une étude récente a révélé que 88 % des organisations mondiales avaient subi des attaques par hameçonnage ciblé et 86 % d'entre elles des attaques de type BEC.[16] En 2019, Microsoft 365 a été l'un des services les plus ciblés avec pour objectif principal de collecter des identifiants.[17] Une fois ces identifiants obtenus, l'attaquant était alors capable de recueillir beaucoup plus de données sur l'organisation, un processus qui pouvait durer des semaines, voire des mois[18], pour ensuite donner lieu à des attaques d'hameçonnage ciblé. Se faisant passer pour un employé, un président-directeur général (PDG), voire un fournisseur de confiance, l'attaquant parvenait à détourner des fonds ou à réacheminer des paiements sur des comptes tiers.[14] Au premier trimestre 2019, les entreprises ont été visées par des attaques de type BEC 120 % plus souvent qu'un an auparavant[19], ce qui a provoqué des pertes à hauteur de 26,2 milliards de dollars (env. 22,2 milliards d'euros).[20]

_Adoption du HTTPS pour plus des deux tiers des sites d'hameçonnage

Ces dernières années, le nombre de sites d'hameçonnage ayant adopté le HTTPS a fortement augmenté[13]. Au dernier trimestre 2019, 74 % des sites d'hameçonnage utilisaient le HTTPS[32], une hausse significative par rapport aux 32 % seulement deux ans auparavant. Bien que des technologies, telles que HTTPS et SSL, soient conçues pour sécuriser les communications entre un client et un serveur, la présence d'une icône en forme de cadenas dans la barre d'adresse du navigateur peut donner l'illusion que le site web consulté est fiable.

Les auteurs de menace peuvent également utiliser des sites légitimes qu'ils ont piratés pour héberger du contenu d'hameçonnage; il devient alors difficile pour l'utilisateur final d'identifier un site comme dangereux[14]. D'autres facteurs contribuent à la forte augmentation de l'utilisation du HTTPS, en particulier la multitude de services de certificats gratuits comme Let's Encrypt[15] et le fait que les navigateurs modernes indiquent chaque site HTTPS comme sécurisé, sans aucune vérification supplémentaire.

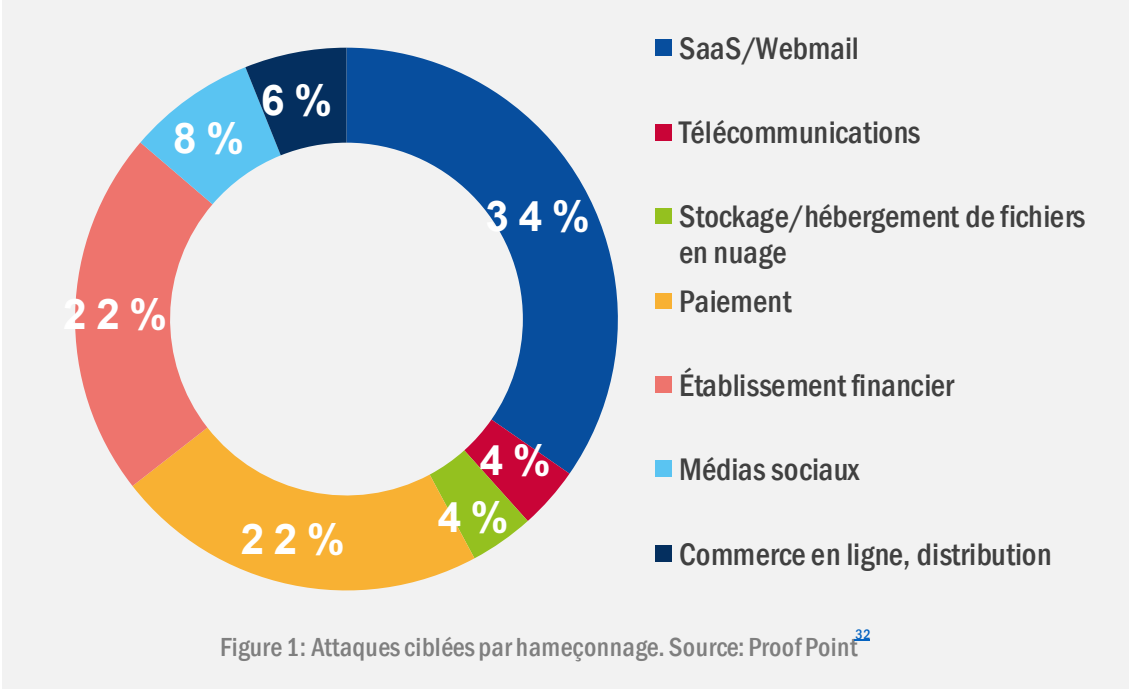


Figure 1: Attaques ciblées par hameçonnage. Source: Proof Point[32]

Tendances

_Le *Phishing-as-a-Service* (PhaaS) en hausse

Ces types de services sont généralement proposés sur abonnement ou sous forme de kit, téléchargeable contre paiement. En supprimant les barrières technologiques à l'entrée, ils permettent donc à toute personne moins compétente sur le plan technique de mener des attaques ciblées. Le rapport d'un chercheur en sécurité[21] a permis d'identifier 5 334 kits d'hameçonnage uniques disponibles en juin 2019. Plus inquiétant encore, c'est le coût relativement faible de ces solutions, à savoir un tarif compris entre 50 et 80 USD pour un abonnement mensuel. Selon le même rapport, 87 % des kits intégraient des mécanismes d'évasion tels que l'encodage des caractères HTML et le chiffrement de contenu. Fait intéressant, certains de ces services étaient hébergés sur des services en nuage légitimes avec des noms de domaine (DNS) et des certificats appropriés. Les statistiques provenant d'une seule de ces places de marché sur le *darknet* révèlent le succès de ces attaques qui permettent à l'attaquant ou au groupe de voler aux alentours de 65 000 comptes par mois.[22]

_Évolution des incidents

- L'efficacité des attaques par hameçonnage a changé grâce au stockage en ligne, à DocuSign et aux services Microsoft en nuage.
- Les imposteurs utilisent des stratagèmes pour attaquer, comme la compromission de messagerie en entreprise (BEC) et les techniques d'usurpation d'identité basées sur l'ingénierie sociale, pour que les campagnes d'hameçonnage soient plus efficaces.
- Le stratagème privilégié a été l'hameçonnage des services Microsoft 365, mais la collecte d'identifiants reste l'objectif principal.
- Pour être efficaces, plus de 99 % des courriels diffusant des logiciels malveillants ont nécessité une intervention humaine (liens à suivre, ouverture de documents, acceptation d'avertissements de sécurité, etc.).[44]

Principales méthodes d'hameçonnage en 2019

- Collecte d'identifiants de courriels génériques
- Hameçonnage de comptes Office 365
- Hameçonnage des établissements financiers
- Hameçonnage Microsoft OWA
- Hameçonnage OneDrive
- Hameçonnage American Express
- Hameçonnage générique Chalbhai
- Hameçonnage de comptes Adobe
- Hameçonnage DocuSign
- Hameçonnage Netflix
- Hameçonnage de comptes Dropbox
- Hameçonnage de comptes LinkedIn
- Hameçonnage de comptes Apple
- Hameçonnage de services d'envoi/livraison
- Hameçonnage de documents en ligne Microsoft (Excel et Word)
- Hameçonnage des paramètres Windows
- Hameçonnage Google Drive
- Hameçonnage PayPal

Source: Proof Point[32]

Tendances

_COVID-19: un leurre d'hameçonnage

Apparue pour la première fois fin 2019, la pandémie de COVID-19 suscite la peur collective et les cybercriminels en profitent. Selon certaines informations, les attaques par hameçonnage impliquant le virus ont augmenté de 667 % en un mois (entre fin février 2020 et fin mars 2020); de plus, ce type de stratagème a représenté à lui seul 2 % de l'ensemble des escroqueries par hameçonnage.[5]

De nouvelles escroqueries ont été recensées, par exemple l'envoi de courriels d'hameçonnage conçus pour donner l'impression de provenir du Centre américain de contrôle et de prévention des maladies (CDC - *Centre of Disease Control*)[6], de l'Organisation mondiale de la santé[7] ou encore d'équipes médicales universitaires[8]. Ces messages pouvaient prétendre à tort la survenue de cas d'infection dans l'entourage de la victime ou partager des avis d'experts médicaux pour inciter la victime à cliquer sur un lien malveillant. Pour ces raisons, le FBI et l'OMS ont lancé des alertes.[8,9] En confinement, de nombreuses personnes ont télétravaillé et utilisé des systèmes de sécurité bien souvent obsolètes[11], les cybercriminels ont donc cherché à exploiter de nouvelles opportunités et vulnérabilités[12].

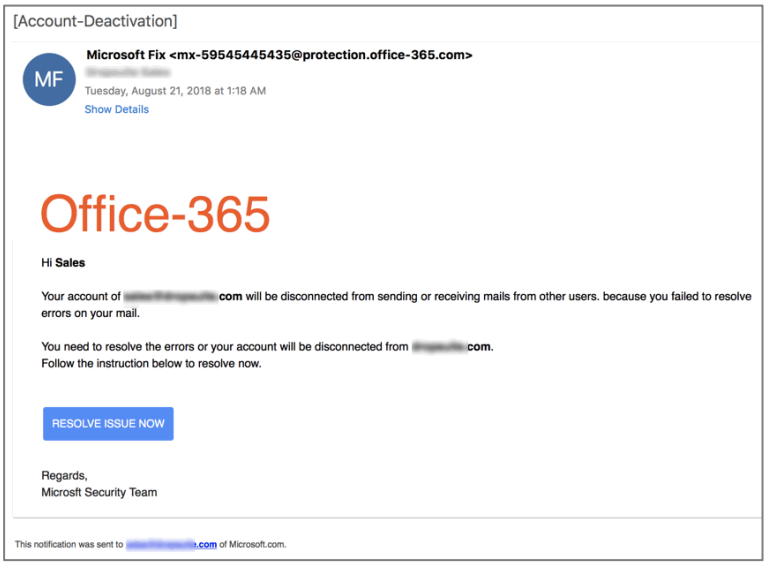


Figure 2: Courriel d'hameçonnage Office 365. Source: Dropsuite[45]

_Réaction de l'ENISA face à la pandémie de COVID-19

L'épidémie de COVID-19 a engendré d'immenses changements dans la façon de mener nos vies. Dans ce monde de plus en plus connecté, il nous est heureusement possible de poursuivre virtuellement notre vie professionnelle et notre vie privée. Au cours de cette période sans précédent, l'Agence de l'Union européenne pour la cybersécurité (ENISA) a fait part de ses recommandations en matière de cybersécurité[46] sur différents sujets, notamment le travail à distance, les achats en ligne et la cybersanté; elle a également fait le point sur les principaux conseils de sécurité adaptés aux secteurs concernés. L'ENISA examine le paysage des menaces pendant la pandémie et fournit des conseils sur la façon d'atténuer les risques liés aux menaces les plus critiques. Une attention particulière est accordée à l'hameçonnage en raison de l'intensification du nombre d'attaques.

Figure 3: Vidéo YouTube de l'ENISA sur la COVID-19. Source: ENISA

Incidents

_Les secteurs cibles

Le secteur de la santé a été fortement pris pour cible lors des attaques d'hameçonnage (ou d'hameçonnage ciblé) perpétrées en 2019. Selon un chercheur en sécurité[42], l'hameçonnage a constitué le principal vecteur d'attaque de l'année grâce à l'utilisation de tactiques d'ingénierie sociale dans le but de transmettre des courriels infectés par des logiciels malveillants[↗] ou contenant des liens dirigeant vers des sites web infectés. D'autres secteurs ont également été la cible d'attaques d'hameçonnage, comme les gouvernements et autres entités de l'administration publique. Ainsi, en novembre et en décembre 2019, plusieurs diplomates et fonctionnaires du gouvernement ukrainien ont reçu des courriels d'hameçonnage ciblé qui les ont ensuite dirigés vers des sites web compromis.[43]

_Vecteurs d'attaque

L'hameçonnage ciblé (*spearphishing*) reste une technique d'accès initial extrêmement répandue chez les acteurs malveillants. Ces derniers utilisent différentes tactiques d'ingénierie sociale pour inciter les destinataires à ouvrir des pièces jointes ou à naviguer sur un site web infecté. Les messages d'hameçonnage ciblé contiennent généralement des documents Microsoft Office exécutant des macros malveillantes ou un lien vers ces documents. Lorsque l'utilisateur sélectionne «Activer le contenu», la macro intégrée commence généralement l'exécution d'une chaîne de scripts obfusqués qui aboutit au téléchargement de la première étape du logiciel malveillant ou de l'injecteur (*dropper*). À cette fin, JavaScript et PowerShell semblent rester les langages de script les plus courants.

Exemples

_Une attaque par hameçonnage visant les étudiants de l'université de Lancaster a abouti à la perte de données à caractère personnel[37]

_Des hackers ont piraté les identifiants de connexion de 2 500 utilisateurs de Discord[38]

_Un fournisseur de services de remise en forme a été victime d'une attaque par hameçonnage[39]

_Des patients ont été touchés par l'attaque par hameçonnage d'UConn Health[41]

_Une filiale d'un constructeur automobile a perdu 37 millions de dollars (env. 31 millions d'euros) en raison d'une escroquerie de type BEC[33]

Atténuation

Actions proposées

- Former le personnel à reconnaître les courriels falsifiés et frauduleux, ainsi qu'à rester vigilant. Lancer de fausses campagnes d'hameçonnage pour tester l'infrastructure de l'organisation, de même que la réactivité du personnel.
- Envisager l'utilisation d'une passerelle de messagerie sécurisée associée à une maintenance régulière (éventuellement automatisée) des filtres (antipourriel, antivirus, filtrage basé sur des règles).
- Envisager d'appliquer des solutions de sécurité qui utilisent des techniques d'apprentissage automatique afin d'identifier les sites d'hameçonnage en temps réel.
- Désactiver l'exécution automatique de codes, de macros, de rendu des graphiques et de préchargement des liens envoyés sur les clients de messagerie et les mettre à jour fréquemment.
- Mettre en œuvre l'une des normes suivantes pour réduire les courriers indésirables: SPF (*Sender Policy Framework*)[34], DMARC (*Domain-based Message Authentication, Reporting & Conformance*)[35] et DKIM (*Domain Keys Identified Mail*).[36]
- Dans l'idéal, utiliser des communications électroniques sécurisées par signatures numériques ou chiffrement pour les opérations financières critiques ou lors d'échanges d'informations sensibles.
- Implémenter la détection des fraudes et des anomalies au niveau du réseau pour les courriels entrants et sortants.
- Éviter de cliquer sur des liens aléatoires, en particulier des liens courts rencontrés dans les médias sociaux.
- Ne pas cliquer sur des liens ou télécharger des pièces jointes si vous n'êtes pas absolument sûr de la source du courriel.

- Éviter le partage excessif de renseignements personnels sur les médias sociaux, par ex. la durée de votre absence au bureau ou à domicile, vos informations de vol, etc., car les auteurs de menace les utilisent activement pour recueillir des informations sur leurs cibles.
- Vérifier que le nom de domaine des sites web consultés ne contient pas de coquilles, en particulier pour les sites web sensibles, ceux des banques par exemple. Les acteurs malveillants enregistrent généralement de faux domaines qui ressemblent à des domaines légitimes et qu'ils utilisent ensuite pour «hameçonner» leurs cibles. Chercher uniquement une connexion HTTPS n'est pas suffisant.
- Activer l'authentification à deux facteurs dès que possible pour empêcher les piratages de comptes.
- Utiliser un mot de passe robuste et unique pour chaque service en ligne. La réutilisation d'un même mot de passe pour différents services constitue un grave problème de sécurité et doit être absolument évitée. L'utilisation d'identifiants robustes et uniques pour chaque service en ligne limite le risque d'un éventuel piratage de compte au seul service concerné. L'utilisation d'un logiciel gestionnaire de mots de passe permettra de faciliter la gestion de l'ensemble des mots de passe.
- Au moment de transférer de l'argent sur un compte, revérifier les informations de la banque bénéficiaire par le biais d'un autre moyen. Il ne faut pas faire confiance aux courriels non chiffrés et non signés, surtout dans des cas d'utilisation sensibles comme celui-ci.
- Vérifier le fonctionnement des formulaires de contact, d'inscription, d'abonnement et de retour d'expérience sur votre site web et ajouter, si nécessaire, des règles de vérification afin de les rendre inexploitables par des attaquants.

Références

1. «What Is Phishing?». Cisco. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

2. «Phishing Activity Trends Report Q1». 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf

3. «2018 Phishing Trends & Intelligence Report» 2018. Phishlabs.

https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf

4. «Microsoft remains phishers' #1 target for the fifth straight quarter» 22 août 2019. Vade Secure.
https://www.vadesecure.com/en/phishers-favorites-q2-2019/

5. «Threat Spotlight: Coronavirus-Related Phishing». 26 mars 2020. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

6. «Coronavirus phishing emails: How to protect against COVID-19 scams» 2020. https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

7. «Covid-19 Drug Advice From The WHO Spoofed to Distribute Agent Tesla Info-Stealer». 2020. IBM.
https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From-The-WHO-Disguised-As-HawkEye-Info-Stealer-2f9a23ad901ad94a8668731932ab5826

8. «Abnormal Attack Stories #6: Coronavirus Credential Theft» 13 mars 2020.
https://abnormalsecurity.com/blog/abnormal-attack-stories-6-coronavirus-credential-theft/

9. «FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic». 20 mars 2020. FBI.
https://www.ic3.gov/media/2020/200320.aspx

10. «Beware of criminals pretending to be WHO». 2020. OMS. https://www.who.int/about/communications/cyber-security

11. «Global police agencies issue alerts on Covid-related cyber-crime». 6 avril 2020. SC Magazine.
https://www.scmagazineuk.com/global-police-agencies-issue-alerts-covid-related-cyber-crime/article/1679473

12. «Catching the virus cybercrime, disinformation and the COVID-19 pandemic». 3 avril 2020. EUROPOL.
https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic

13. «New FireEye Email Threat Report Reveals Increase in Social Engineering Attacks». 25 juin 2019. FireEye.
https://www.fireeye.com/company/press-releases/2019/new-fireeye-email-threat-report-reveals-increase-in-social-engin.html

14. «HTTPS Protocol Now Used in 58% of Phishing Websites». 24 juin 2019. Trend Micro.
https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/https-protocol-now-used-in-58-of-phishing-websites

15. Let's Encrypt. https://letsencrypt.org/

16. «2020 "State of the Phish": Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike». 23 janvier 2020. Proof Point. https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical

17. «Human factor report». 2019. Proof Point. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

18. «Phishing Activity Trends Report Q3». 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf

19. «Business Email Compromise Results in $26B in Losses Over the Last Three Years». 12 septembre 2019. Proof Point. https://www.proofpoint.com/us/corporate-blog/post/business-email-compromise-results-26b-losses-over-last-three-years

20. «Business Email Compromise The $26 Billion Scam» 10 septembre 2019. FBI. https://www.ic3.gov/media/2019/190910.aspx

21. «Evasive Phishing Driven by Phishing-as-a-Service». 1er juillet 2019. Cyren.

https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service

22. «Phishing made easy: Time to rethink your prevention strategy?». 2016. Imperva. https://www.imperva.com/docs/Imperva-HII-phishing-made-easy.pdf

23. «Q3 2019: Email Fraud and Identity Deception Trends». 2019. Agari. https://www.agari.com/insights/ebooks/2019-q3-report/

24. «FBI: BEC Losses Soared to $1.8 Billion in 2019». 12 février 2020. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/fbi-bec-losses-soared-to-18/

25. «Email: Click with Caution». Juin 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

26. «Experts report a rampant growth in the number of malicious, lookalike domains». 18 novembre 2019. https://securityaffairs.co/wordpress/94021/hacking/lookalike-domains-tls-certificate.html

27. «Proofpoint Q3 2019 Threat Report — Emotet's return, RATs reign supreme, and more». 7 novembre 2019. Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

28. «Human Factor Report.» 2019. Proof Point. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

29. «2019 Phishing and fraud report» 2019. F5 Labs. https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5Labs_2019_Phishing_and_Fraud_Report.pdf

30. «Report: Microsoft, PayPal, and Netflix Most Impersonated Brands in Phishing Attacks in Q1 2019» 8 mai 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/report-microsoft-paypal-and-netflix-most-impersonated-brands-in-phishing-attacks-in-q1-2019

31. «Spam and phishing in Q3 2019». 26 novembre 2019. Kaspersky. https://securelist.com/spam-report-q3-2019/95177/

32. «Phishing Activity Trends Report». 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

33. «Toyota Subsidiary Loses $37 Million Due to BEC Scam» 20 septembre 2019. CPO Magazine. https://www.cpomagazine.com/cyber-security/toyota-subsidiary-loses-37-million-due-to-bec-scam/

34. Open SPF. http://www.openspf.org/

35. «Domain-based Message Authentication, Reporting & Conformance». DMARC. https://dmarc.org/

Références

36. «DomainKeys Identified Mail (DKIM)». DKIM. http://www.dkim.org/

37. «Cyber incident». 22 juillet 2019. Lancaster University. https://www.lancaster.ac.uk/news/phishing-attack

38. «Hackers publish login credentials of 2500 Discord users» 22 juillet 2019. Cyware Social. https://cyware.com/news/hackers-publish-login-credentials-of-2500-discord-users-8d3ea2c7

39. «Bodybuilding.com Breach: Proof That An Organization's Biggest Cyber Risk Is Its People» 24 avril 2019. Forbes. https://www.forbes.com/sites/jameshadley/2019/04/24/bodybuilding-com-breach-proof-that-an-organizations-biggest-cyber-risk-is-its-people/#1ea113751bef

40. «Phishing Attack Exposes 600k Health Records» 19 juin 2019. Secure World. https://www.secureworldexpo.com/industry-news/healthcare-data-breach-example-2019

41. «326,000 Patients Impacted in UConn Health Phishing Attack». 25 février 2019. Health IT Security. https://healthitsecurity.com/news/326000-patients-impacted-in-uconn-health-phishing-attack

42. «Cybercrime Tactics and Techniques: the 2019 state of healthcare». 2019. Malwarebytes. https://resources.malwarebytes.com/resource/cybercrime-tactics-and-techniques-the-2019-state-of-healthcare/

43. «Significant Cyber Incidents». 2019. CSIS. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

44. «More Than 99% of Cyberattacks Need Victims' Help». 9 septembre 2019. Dark Reading. https://www.darkreading.com/cloud/more-than-99--of-cyberattacks-need-victims-help/d/d-id/1335769

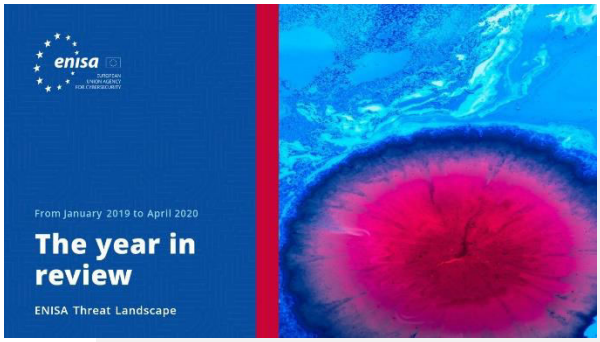
45. «office-365-phishing-attacks-deconstructed» https://dropsuite.com/office-365-phishing-attacks-deconstructed/

46. ENISA. https://www.enisa.europa.eu/topics/wfh-covid19

«De nombreux individus victimes d'hameçonnage justifient leur acte par une réaction émotionnelle et c'est exactement ce que cherchent les pirates informatiques.»

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

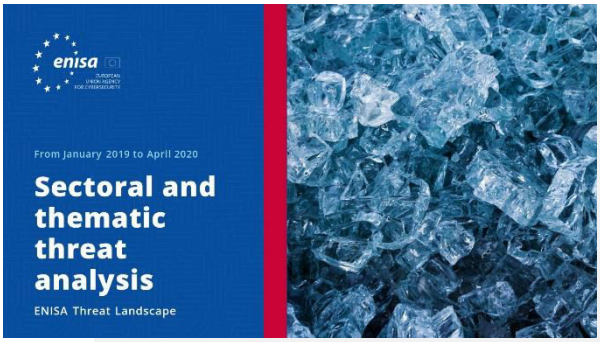
Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.

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