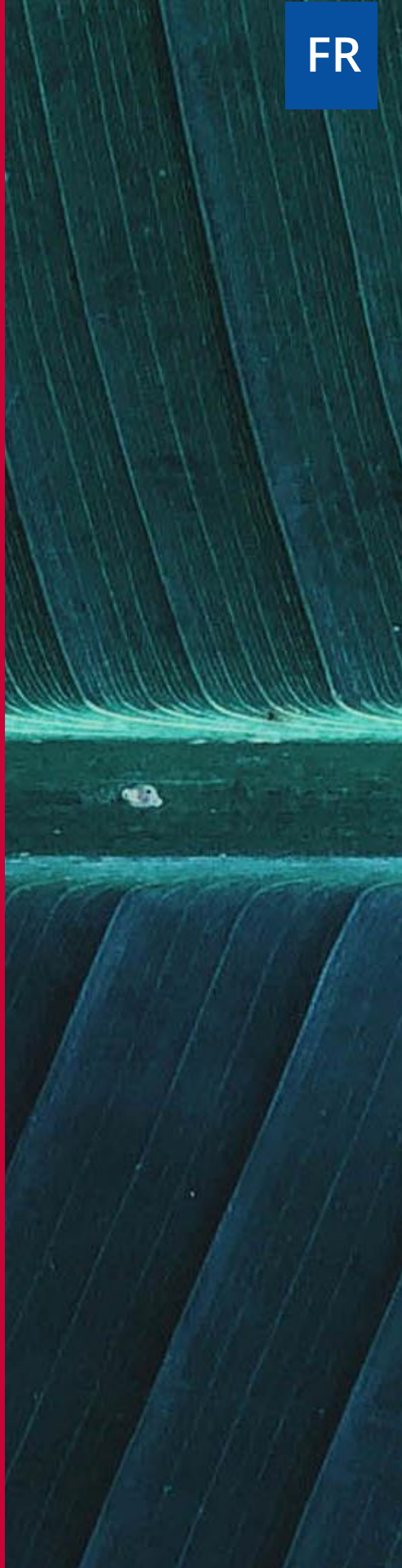
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

FR



De janvier 2019 à avril 2020

Les pourriels

Paysage des menaces de l'ENISA

Aperçu

Le premier pourriel (*spam*) a été envoyé en 1978 par un responsable marketing à 393 personnes via ARPANET. Il s'agissait d'une campagne publicitaire pour un nouveau produit de la société pour laquelle il travaillait: la Digital Equipment Corporation. Pour ces 393 premiers destinataires et malgré la nouveauté de l'idée, ce pourriel reçu s'est révélé aussi agaçant qu'il le serait de nos jours.[1] Il est désagréable de recevoir des pourriels, mais ces envois peuvent également offrir la possibilité aux acteurs malveillants de voler des informations à caractère personnel ou d'installer un logiciel malveillant (*malware*).[2] Le pollupostage consiste à envoyer des messages indésirables en très grande quantité. Il est considéré comme une menace pour la cybersécurité lorsqu'il est utilisé comme vecteur d'attaque pour distribuer ou favoriser d'autres menaces.

Autre aspect intéressant, la confusion qui peut parfois être faite entre pollupostage et campagne d'hameçonnage (*phishing*), le pourriel étant alors classé à tort dans cette dernière catégorie. La principale différence entre les deux réside dans le fait que l'hameçonnage est une action ciblée qui utilise des tactiques d'ingénierie sociale destinées à voler activement des données d'utilisateurs. En revanche, le pollupostage est une tactique qui consiste à envoyer en masse des courriers électroniques non sollicités à une liste d'envoi. Les campagnes d'hameçonnage peuvent utiliser des tactiques de pollupostage pour distribuer des messages tandis que le pourriel peut connecter l'utilisateur à un site web compromis afin d'installer un logiciel malveillant et de voler des données à caractère personnel.

Ces 41 dernières années, les campagnes de pourriels ont tiré profit de nombreux événements sociaux et sportifs très appréciés à l'échelle mondiale, notamment la finale de l'UEFA Europa League et l'US Open. Pourtant, cela n'est rien comparé à l'activité de pollupostage observée cette année en lien avec la pandémie de COVID-19.[8]

Conclusions

85 %_ de tous les courriels échangés en avril 2019 étaient des pourriels, un chiffre record en 15 mois[1]

14_ millions de pourriels liés à des actes d'extorsion sexuelle ont été détectés en 2019[2,3]

58,3 %_ des comptes de messagerie dans l'industrie minière ont fait l'objet de pollupostage[17]

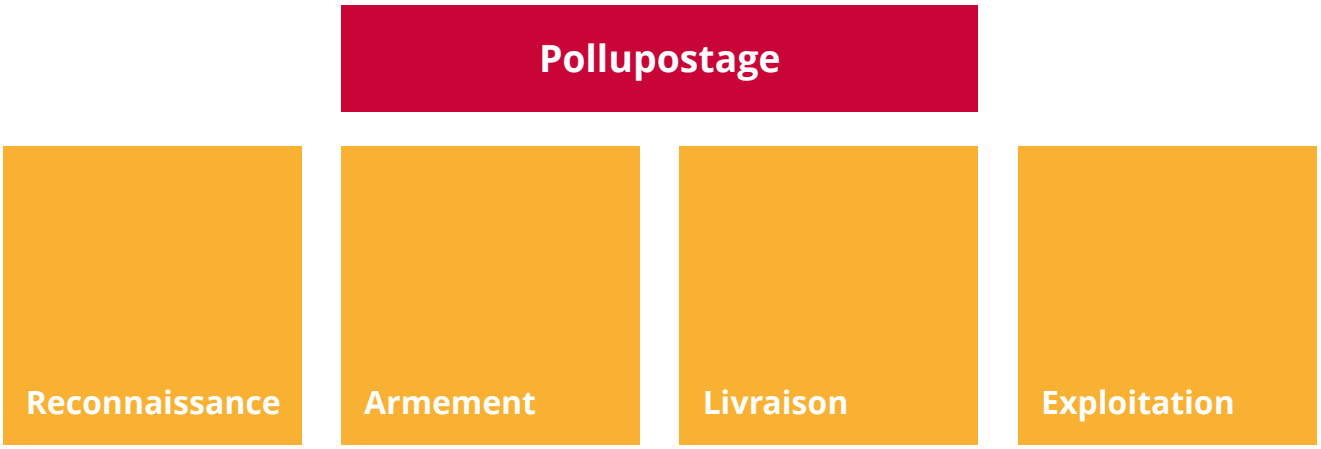
10 %_ des détections totales de pourriels visaient des comptes de messagerie allemands[2,3]

13 %_ des violations de données ont été occasionnées par des pourriels malveillants[16]

83 %_ des entreprises n'étaient pas protégées contre l'usurpation de marque par courriel[20]

42 %_ des responsables de la sécurité des systèmes d'information (RSSI) ont traité au moins un incident de sécurité résultant d'un pourriel[1]

Chaîne de frappe



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

Description

Des novices expérimentés

Après 41 ans d'existence, le pourriel reste une menace notable pour la sécurité, et ce malgré toutes les autres menaces existantes beaucoup plus efficaces. Cependant, une fois encore au cours de la période considérée, les campagnes de pourriels ont laissé apparaître de nouveaux groupes cibles, de nouveaux moyens et de nouveaux profits. Par exemple, en août 2019, plusieurs comptes ont été pris pour cible par des courriers indésirables qui encourageaient leur propriétaire à partager non seulement une version scannée de leur pièce d'identité, mais également un selfie afin de leur permettre de «gagner» un smartphone gratuit. Dans une autre campagne de pollupostage, il a été demandé aux utilisateurs d'envoyer une photo personnelle. Le groupe cible des *spammeurs* s'est ensuite développé de manière à inclure l'adresse électronique utilisée par l'utilisateur afin d'activer des services de télévision payante ou de diffusion en direct. Ces comptes ont été *spammés* à l'aide de faux messages d'expiration ou de renouvellement de licence. Les utilisateurs étaient invités à répondre et à saisir leurs coordonnées bancaires et leurs informations personnelles pour renouveler leur inscription.[2]

Le pollupostage au service des logiciels malveillants, des rançongiciels et des chevaux de Troie d'accès à distance

En août 2019, des courriels indésirables contenant des fichiers d'image disque ISO malveillants ont été utilisés pour propager le logiciel malveillant LokiBot[↗] et déposer le cheval de Troie d'accès à distance (RAT - *Remote Access Trojan*) FlawedAmmyy. Le pollupostage a également été utilisé pour diffuser le cheval de Troie TrickBot, le cheval de Troie espion Negasteal (également connu sous le nom d'Agent Tesla), le RAT Ave Maria (également connu sous le nom de Warzone) et le logiciel malveillant de macros Pawload, désormais célèbre depuis 2018. Plusieurs familles de rançongiciels[↗] ont également été diffusées via des pourriels[↗], à l'instar de Dharma, Crysis et Ryuk; ces rançongiciels ont tous été signalés comme très actifs au cours de l'année de référence.[15,21]

Les SMS indésirables

Une opération de SMS indésirables a été menée cette année,[↗] qui a exposé les données personnelles de plus de 80 millions d'utilisateurs. Un grand nombre de numéros de téléphone ont reçu des messages dans lesquels figuraient certaines formules telles que «free money» (argent facile) ou «for real» (pour de vrai), ainsi que des liens vers des sites frauduleux. À partir de ce moment-là, il était demandé à toute personne cliquant sur le lien de s'inscrire et de fournir par là même des informations sensibles. Il a été prouvé que la base de données utilisée par les *spammeurs* appartenait à la société ApexSMSCompany, dont la légitimité reste à ce jour inconnue. Bien que des chercheurs en sécurité aient accédé à la base de données et essayé de récupérer autant d'informations que possible, craignant que l'opération ne s'arrête inopinément, on ignore toujours qui peut accéder à ces données et les utiliser, et pour quelle raison, car celles-ci sont toujours disponibles.[4]

Les formulaires comme moyens d'attaque

Les *spammeurs* ont procédé à la manipulation des formulaires de retour d'expérience sur les sites web des grandes entreprises, généralement utilisés pour poser des questions, exprimer des souhaits ou s'abonner à des lettres d'information. Cependant, au cours de l'année considérée, au lieu d'envoyer des pourriels dans les messageries de l'entreprise, les *spammeurs* ont exploité le faible niveau de sécurité des sites web, ont contourné tous les tests reCAPTCHA et ont enregistré de multiples comptes en renseignant des informations de messagerie valables. Les victimes recevaient donc une réponse légitime de l'entreprise qui renfermait également le message du *spammeur*.[2] Même Google Forms a été manipulé de cette façon pour récupérer les données des utilisateurs et envoyer des pourriels de nature commerciale. Un cas plus agressif a été relevé, celui de l'attaque par pourriels ciblant les comptes de l'entreprise et demandant que l'argent soit transféré à l'attaquant. Pour convaincre la victime, les *spammeurs* prétendaient être en mesure d'envoyer des messages abusifs avec le courriel de la victime à plus de 9 millions d'adresses électroniques, mettant ainsi l'adresse électronique de l'entreprise sur liste noire.[3]

Description

Le pourriel Chameleon

En 2019, plusieurs campagnes ont eu recours au même réseau de machines zombies (*botnet*) pour distribuer des messages indésirables, bien qu'elles aient utilisé des en-têtes et des modèles aléatoires pour formater le contenu. C'est pour cette raison que les chercheurs en sécurité, qui ont commencé à examiner ces campagnes, ont considéré qu'il ne s'agissait que d'un seul groupe et l'ont baptisé «Chameleon spam».[5]

Les pourriels de Chameleon provenaient de différents pays et contenaient des liens frauduleux vers de fausses offres d'emploi, de faux sites de réservation de billets d'avion, de fausses offres spéciales pour l'achat de produits, voire vers de simples services bien connus. Ces courriers indésirables s'appuyaient sur des modèles identiques à ceux utilisés par des sociétés légitimes, comme Google, Qatar Airways, FedEx, LinkedIn ou Microsoft, de sorte que le destinataire ne puisse remarquer la différence.[2]

Droits dans leurs *bots*

En octobre 2019, une vaste distribution de courriels utilisant des modèles en anglais, allemand, italien et polonais, a été observée, avec pour objet commun «*Payment Remittance Advice*» (en français, avis de paiement). Ces messages comprenaient un document en pièce jointe qui contenait une macro; il était alors demandé aux destinataires de l'activer à l'ouverture du document. Une fois activée, la macro permettait de lancer le processus d'infection en essayant de télécharger le cheval de Troie Emotet.[13]

En 2019, le *botnet* de pourriels Necurs s'est révélé très actif après une long période de faible activité. Le *botnet* Gamut a été le troisième réseau zombies de pourriels le plus actif en 2019. Les messages de Gamut sont principalement liés à des suggestions de rencontres, à des offres de produits pharmaceutiques et à des offres d'emploi.[1]

_Nombre de réseaux zombies C&C associés à des familles de logiciels malveillants

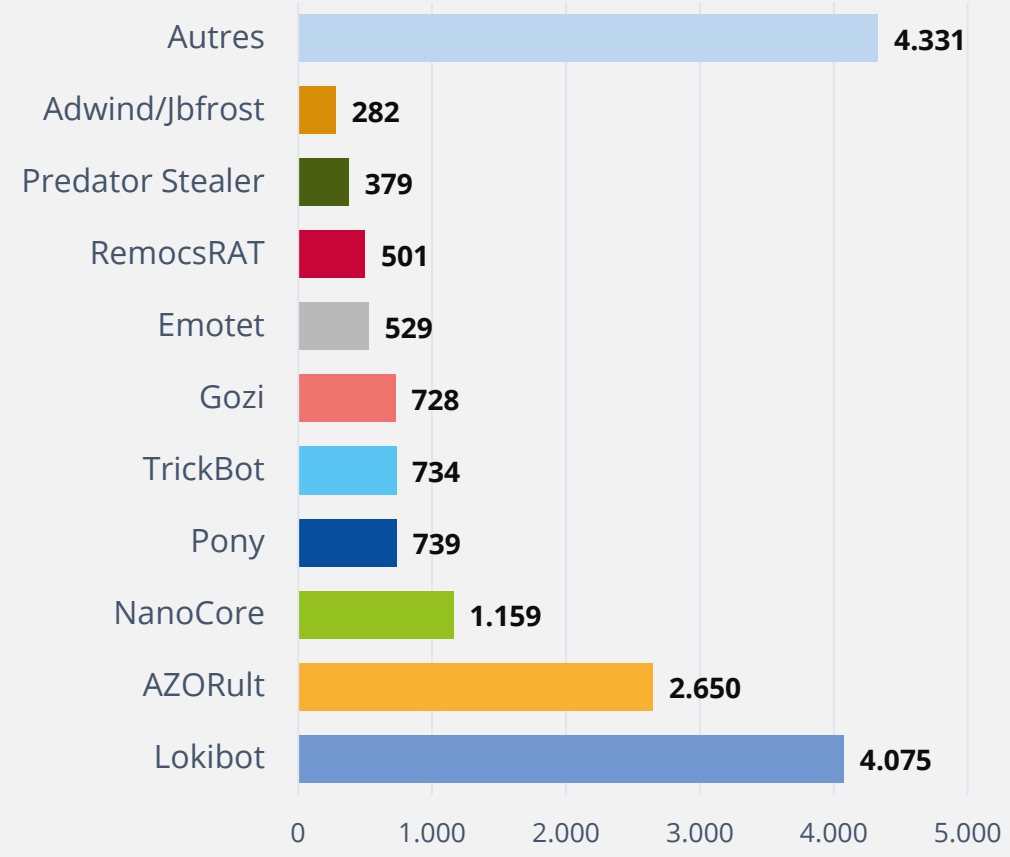


Figure 1 - Source: Spamhaus [14]

Description

La pandémie de COVID-19 a ouvert de nouvelles portes

Peu après le début de la pandémie de COVID-19, des sites web d'hameçonnage et des fichiers malveillants distribués par courriel sont apparus, dans lesquels figuraient les termes «coronavirus» ou «COVID-19». Une campagne de pollupostage COVID-19 aurait diffusé le fichier Eeskiri-COVID.chm19, un enregistreur de frappe déguisé. Le nom du fichier pourrait indiquer que la campagne a pris naissance en Estonie (*eeskiri* signifie «règle» en estonien).[11] À la mi-février 2020, on enregistrait seulement quelques centaines d'attaques COVID-19 par jour, mais en mars 2020, plus de 2 500 attaques se déroulaient chaque jour, ce qui annonçait une année difficile en matière de pollupostage.[12]

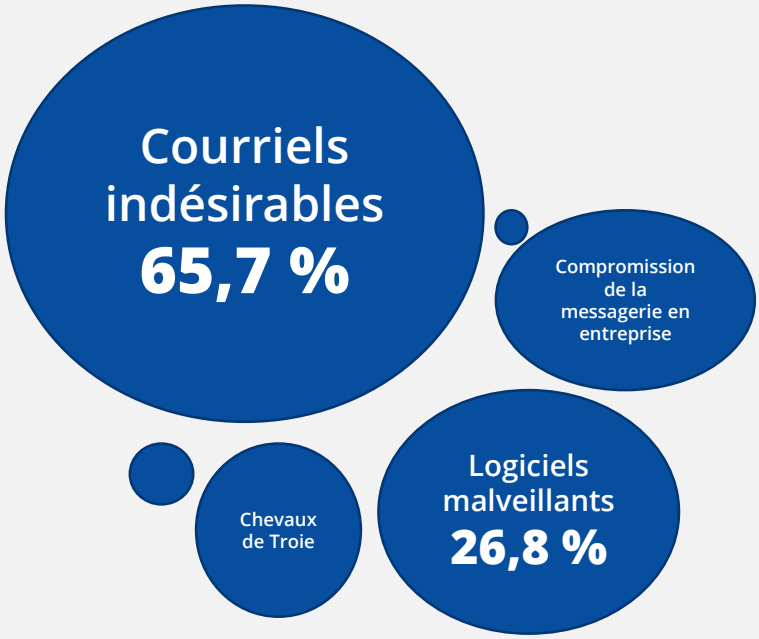


Figure 2: Menaces liées à la COVID-19. Source: Trend Micro[11]

_ Exemples

01_ L'opération de pollupostage d'ApexSMS

ApexSMS, société de SMS marketing, a subi une violation de données exposant les données de contact de plus de 80 millions de personnes.

02_ La campagne de pollupostage Chameleon

Cette campagne de pollupostage massive persistante émanait d'un réseau de machines zombies qui envoyait des messages aux en-têtes aléatoires en changeant fréquemment de modèle.

03_ Campagne de distribution de pourriels Emotet

Campagne de pollupostage permettant la distribution de logiciels malveillants Emotet.

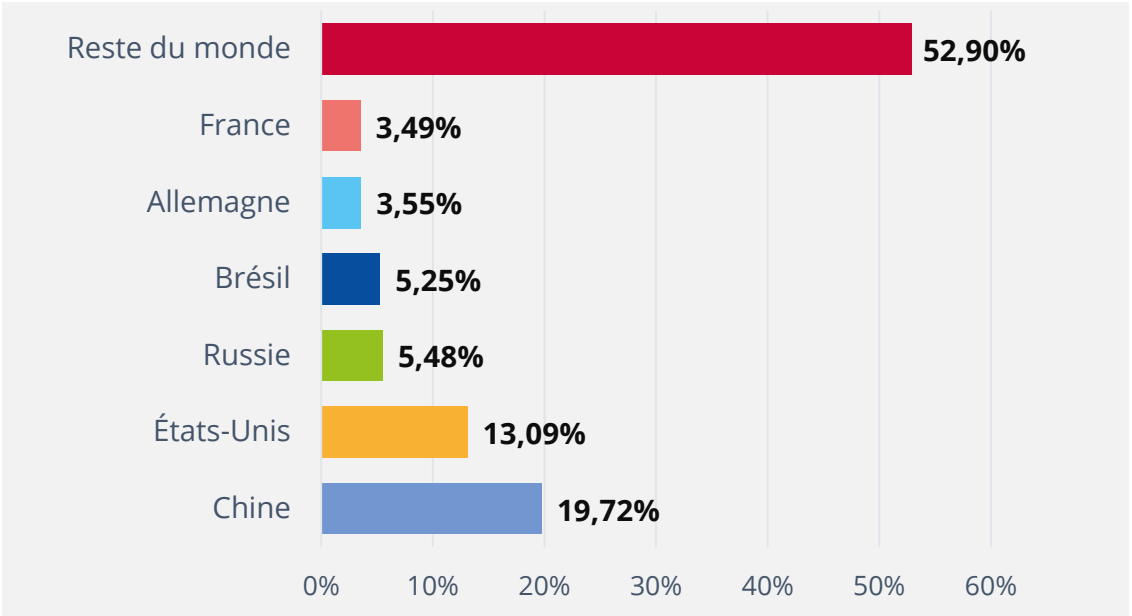
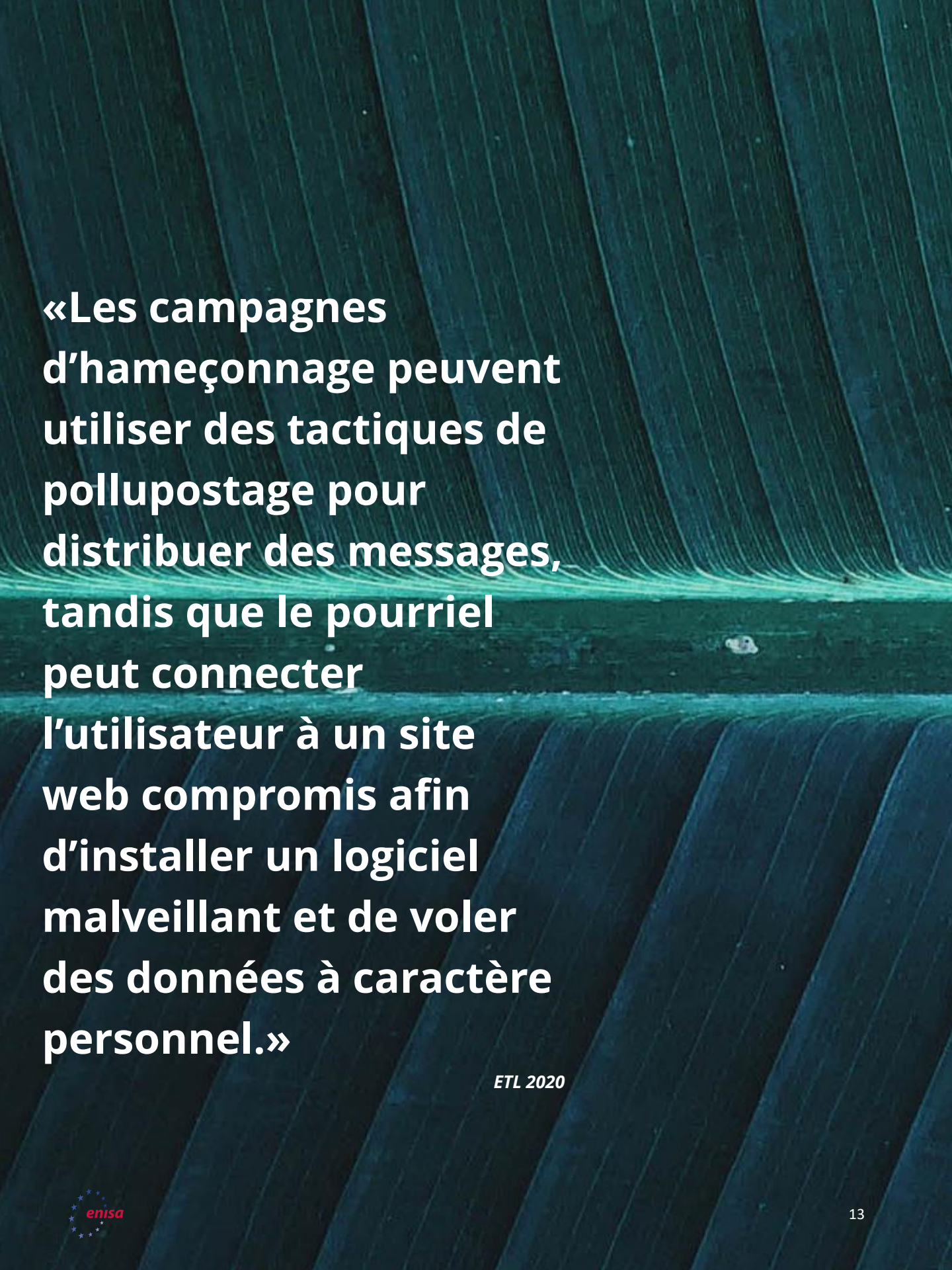


Figure 3: Pays d'origine des pourriels les plus fréquents. Sources multiples[17]

Atténuation

Actions proposées

- Mettre en œuvre un filtrage de contenu pour repérer les pièces jointes indésirables, les courriels au contenu malveillant, les pourriels et le trafic réseau indésirable.
- Mettre régulièrement à jour le matériel, le microprogramme, le système d'exploitation et tout pilote ou logiciel.
- Utiliser l'authentification multifacteur pour accéder aux comptes de messagerie.
- Éviter les transferts d'argent vers des comptes bancaires non vérifiés.
- Éviter de se connecter à de nouveaux liens reçus par courriel ou SMS.
- Élaborer des procédures opérationnelles standard et des politiques pour le traitement des données sensibles.
- Utiliser une passerelle de messagerie électronique sécurisée associée, si possible, à une maintenance régulière et automatisée des filtres (antipourriel, antivirus, filtrage basé sur des règles).
- Désactiver l'exécution automatique de codes, l'activation des macros et le préchargement des graphiques et des liens envoyés par courriel.
- Mettre en œuvre des techniques de sécurité telles que les protocoles SPF (*Sender Policy Framework*), DMARC (*domain-based message authentication, reporting and conformance*) et DKIM (*Domain Keys Identified Mail*).
- Mettre régulièrement à jour les listes blanches, les filtres de réputation et la liste noire en temps réel (RBL - *Real-time Blackhole List*).
- Utiliser l'intelligence artificielle et l'apprentissage automatique pour les contrôles de détection des anomalies.



«Les campagnes d'hameçonnage peuvent utiliser des tactiques de pollupostage pour distribuer des messages, tandis que le pourriel peut connecter l'utilisateur à un site web compromis afin d'installer un logiciel malveillant et de voler des données à caractère personnel.»

ETL 2020

Références

1. «Email: Click with Caution - How to protect against phishing, fraud, and other scams» Juin 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

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

3. «Spam and phishing in Q2 2019» 28 août 2019. Kaspersky. https://securelist.com/spam-and-phishing-in-q2-2019/92379/

4. «SMS Spammers Doxxed» 9 mai 2019. Tech Crunch. https://techcrunch.com/2019/05/09/sms-spammers-doxxed/

5. «Tracking the Chameleon Spam Campaign» 25 septembre 2019. Trustwave. https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/tracking-the-chameleon-spam-campaign/

6. «5 Biggest Cyberattacks of 2019 (So Far) and Lessons Learned» 7 juin 2019. Gordon Flesch. https://www.gflesch.com/blog/biggest-cyberattacks-2019

7. «The world worst spammers». 2019. Spamhaus. https://www.spamhaus.org/statistics/spammers/

8. «Appellation de la maladie à coronavirus 2019 (COVID-19) et du virus qui la cause». 2020. OMS. https://www.who.int/fr/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it

9. «WHO Director-General's opening remarks at the media briefing on 2019 novel coronavirus» 6 février 2020. OMS. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-2019-novel-coronavirus/

10. «COVID-19 situation update worldwide, as of 11 June 2020» 2020. ECDC. https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

11. «Developing Story: COVID-19 Used in Malicious Campaigns» 24 avril 2020. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

12. «2019 Novel Coronavirus and COVID-19 Themed Attacks Dominate Threat Landscape» 6 avril 2020. HIPAA Journal. https://www.hipaajournal.com/2019-novel-coronavirus-and-covid-19-themed-attacks-dominate-threat-landscape/

13. «Emotet is back: botnet springs back to life with new spam campaign» 16 septembre 2019. Malwarebytes Lab. https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/

14. «Spamhaus Botnet Threat Report 2019» 28 janvier 2020. Spamhaus. https://www.spamhaus.org/news/article/793/spamhaus-botnet-threat-report-2019

15. «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

16. «Anticipating the Unknowns: 2019 Cisco CISO Benchmark Study», 28 février 2019. Cisco. https://blogs.cisco.com/security/anticipating-the-unknowns-2019-cisco-ciso-benchmark-study

17. «Internet Security Threat Report» Volume 24, février 2019. Broadcom. https://docs.broadcom.com/doc/istr-24-2019-en

18. «Spam and phishing in Q1 2019» 5 mai 2019. Kaspersky. https://securelist.com/spam-and-phishing-in-q1-2019/90795/

19. «Total Global Email & Spam Volume for May 2020» Mai 2019. Talos. https://talosintelligence.com/reputation_center/email_rep#global-volume

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

21. «The World's Most Abused TLDs» Spamhaus. https://www.spamhaus.org/statistics/tlds/

22. «Trend Micro Cloud App Security Report 2019» 10 mars 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-report-2019

23. «The Sprawling Reach of Complex Threats». 2019. Trend Micro Research. https://documents.trendmicro.com/assets/rpt/rpt-the-sprawling-reach-of-complex-threats.pdf

24. «SONIC WALL Security Center Metrics». SONIC WALL. https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics

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

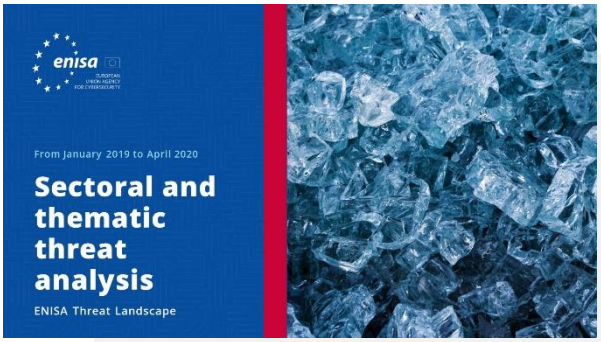
Rapport sur le Paysage des menaces de l'ENISA **Liste des 15 principales menaces**

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.

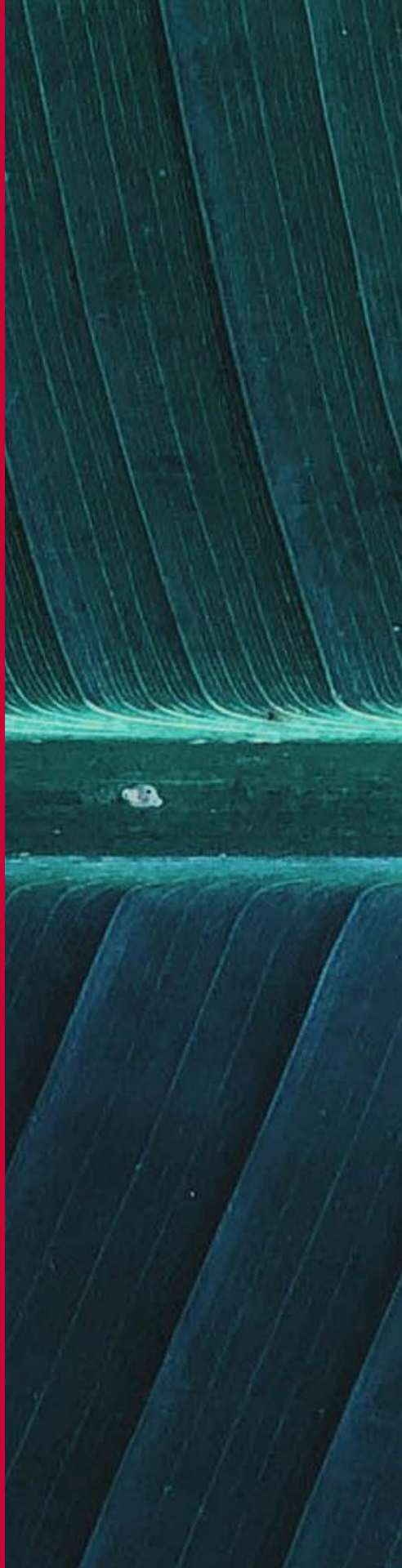
Les sources de tiers sont citées de façon adéquate. L'ENISA n'est pas responsable du contenu des sources externes, notamment des sites web externes, mentionnées dans la présente publication.

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