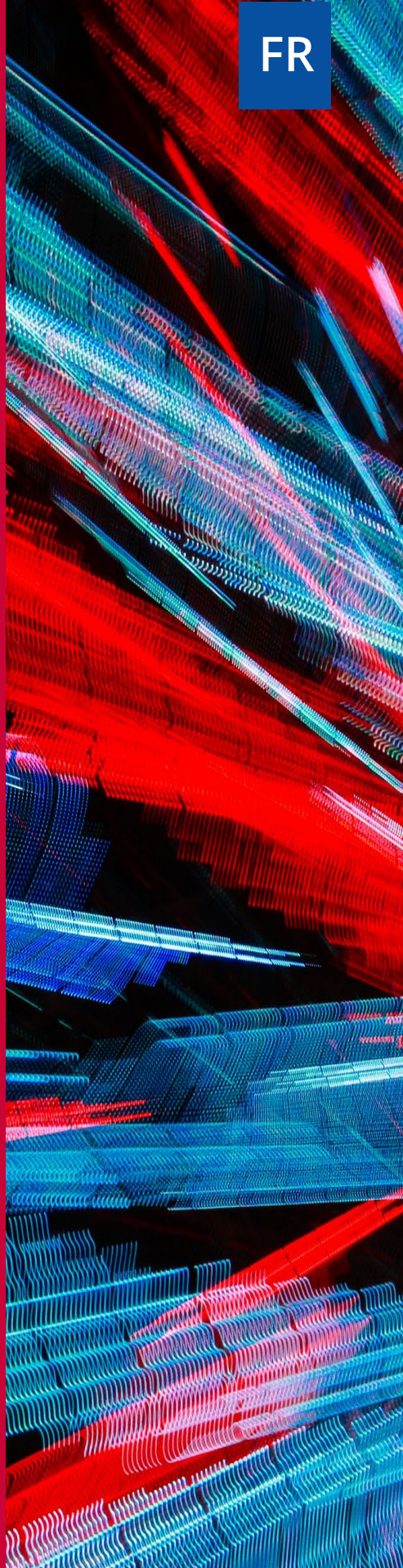
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

FR



De janvier 2019 à avril 2020

Tendances émergentes

Paysage des menaces de l'ENISA

Aperçu

À quoi s'attendre

Avec le début d'une nouvelle décennie, nous pouvons nous attendre à des changements importants quant à notre façon de percevoir et de comprendre la cybersécurité ou la sécurité du cyberespace. Tel que défini dans la norme **ISO/IEC 27032:2012**[1], le cyberespace est un *«environnement complexe résultant de l'interaction de personnes, de logiciels et de services sur l'internet au moyen de dispositifs technologiques et de réseaux connectés, qui n'existe sous aucune forme physique»*. La protection de cet environnement complexe deviendra d'autant plus difficile à mesure que nous connecterons davantage de personnes, d'appareils et de systèmes et que nous exécuterons davantage de processus et de services sur le réseau. Nous sommes également plus dépendants de sa fiabilité, de son intégrité, de sa disponibilité et de sa sûreté pour travailler, communiquer et mener nombre de nos activités quotidiennes. Du fait de cette dépendance croissante, les acteurs malveillants auront de plus en plus d'occasions d'utiliser le cyberespace pour manipuler, intimider, tromper, harceler et escroquer des personnes et des organisations. La protection des personnes, des entreprises et des organisations utilisant le cyberespace aura tendance à évoluer au cours de la prochaine décennie, passant de la sécurité traditionnelle des réseaux et des systèmes d'information à un concept plus large incluant le contenu et les services.

Au cours de la dernière décennie, la «quatrième révolution industrielle» a considérablement accéléré le rythme du changement, transformant l'activité des personnes, leur façon de faire, la nature des compétences requises, le lieu d'accomplissement du travail, la structuration des relations professionnelles, ainsi que l'organisation, la répartition et la rémunération du travail.

En raison de la pandémie actuelle de COVID-19, nous amorçons la décennie avec une nouvelle norme et de profonds changements dans le monde réel et le cyberespace. Avec la distanciation sociale ou le confinement, les personnes auront tendance à utiliser l'espace virtuel pour communiquer, créer des liens et avoir une vie sociale. Cette nouvelle norme apportera de nouveaux défis dans la chaîne de valeur numérique et, en particulier, dans le secteur de la cybersécurité.

Au cours de la prochaine décennie, les risques liés à la cybersécurité deviendront plus difficiles à évaluer et à interpréter en raison de la complexité croissante du paysage des menaces, de l'écosystème des adversaires et de l'expansion de la surface d'attaque.

Il y a trop de variables à prendre en compte pour garantir l'efficacité de la gestion des cyber-risques. La diversité technologique est un facteur important que la plupart des organisations connaissent bien aujourd'hui. Un autre aspect concerne la sophistication des outils, tactiques, techniques et procédures (TTP) utilisés par les adversaires pour mener leurs attaques. Les acteurs malveillants adaptent et ajustent si nécessaire leurs TTP à l'environnement de leur victime puis collaborent avec d'autres pour atteindre leurs objectifs.

La définition d'une posture de risque, la gestion des données, l'application de mesures pertinentes et la réponse au changement sont autant d'obstacles à la création d'une stratégie efficace de gouvernance des cyber-risques. **Au cours de la prochaine décennie, de nouvelles approches seront nécessaires pour s'éloigner des analyses en silo et se rapprocher d'un type matriciel d'interconnexion des facteurs, des variables et des conditions**. Il s'agit d'une problématique importante pour de nombreuses organisations qui tentent de protéger leur infrastructure, leurs opérations et leurs données contre des adversaires plus forts, dotés de meilleures ressources et mieux équipés.

Tendances émergentes

_Dix problématiques en matière de cybersécurité

01_Faire face aux risques systémiques et complexes. Le cyber-risque se caractérise par la vitesse et l'ampleur de sa propagation ainsi que par l'éventuelle intention des auteurs de menace. L'interconnexion des différents systèmes et réseaux permet aux cyberincidents de se propager rapidement et largement, rendant ainsi les cyber-risques plus difficiles à évaluer et à atténuer.

02_Détection généralisée de l'IA adverse.
La détection des menaces exploitant l'IA (intelligence artificielle) pour lancer une attaque ou éviter la détection constituera un défi majeur pour l'avenir des systèmes de cyberdéfense.[14]

03_Réduction des erreurs involontaires.
Compte tenu du nombre croissant de systèmes et de dispositifs connectés au réseau, l'erreur involontaire reste l'une des vulnérabilités les plus exploitées dans les incidents de cybersécurité. De nouvelles solutions visant à réduire ces erreurs contribueront largement à la réduction du nombre d'incidents.

04_Menaces sur la chaîne d'approvisionnement et les tiers.
La chaîne d'approvisionnement diversifiée qui caractérise aujourd'hui l'industrie des technologies offre de nouvelles possibilités aux auteurs de menace pour tirer profit de ces systèmes complexes et exploiter les multiples vulnérabilités introduites par un écosystème hétérogène de fournisseurs tiers.[16]

05_Orchestration et automatisation de la sécurité.
L'analyse de la cybermenace et l'analytique comportementale gagneront en importance avec l'automatisation des processus et de l'analyse. L'investissement dans l'automatisation et l'orchestration permettra aux professionnels de la cybersécurité d'investir dans l'élaboration de stratégies plus solides en matière de cybersécurité.

06_Réduction des faux positifs. Cette promesse tant attendue est essentielle pour assurer l'avenir du secteur de la cybersécurité et pour lutter contre la lassitude des fausses alertes.

07_Stratégies de sécurité à confiance zéro.
Face à la pression croissante sur les systèmes informatiques imposée par les nouveaux besoins fonctionnels, tels que le travail à distance, la numérisation du modèle économique et la prolifération des données, la confiance zéro est considérée par de nombreux décideurs comme la solution de facto pour sécuriser les actifs d'une entreprise.

08_Erreurs de migration vers le nuage d'entreprise. Dans la mesure où de nombreuses entreprises décident de migrer leurs données vers des solutions en nuage, le nombre d'erreurs de configuration augmentera nécessairement, exposant ainsi les données à de possibles violations. Les fournisseurs de services en nuage aborderont ce problème en mettant en place des systèmes permettant d'identifier automatiquement ce type d'erreurs.

09_Menaces hybrides. Les nouveaux modes opératoires adoptent les menaces du monde virtuel et celles du monde réel. La propagation de la désinformation ou la diffusion de fausses nouvelles, par exemple, sont des éléments clés du paysage des menaces hybrides. L'EUvsDisinfo[15] est un projet phare du groupe de travail East StratCom du Service européen pour l'action extérieure, créé pour faire face à la menace de désinformation.

10_L'attrait de l'infrastructure en nuage: une cible de plus en plus prisée. La dépendance croissante à l'égard de l'infrastructure en nuage public augmentera le risque de défaillances. La mauvaise configuration des ressources en nuage reste la principale cause des attaques dans le nuage, mais les attaques visant directement les fournisseurs de services en nuage gagnent en popularité parmi les pirates informatiques.

Tendances émergentes

Les dépenses en cybersécurité

Selon Gartner[17], nombreux seront les conseils d'administration à demander une amélioration des données et une meilleure compréhension des retours sur investissement après des années d'investissements intensifs dans la cybersécurité. Cette tendance est principalement due au fait que les dépenses en matière de cybersécurité augmentent proportionnellement aux investissements réalisés dans les nouvelles technologies. Selon un rapport de l'IDC[22], les dépenses liées à la cybersécurité ont atteint 103 milliards de dollars (env. 87,5 milliards d'euros) en 2019, soit 9,4 % de plus que l'année précédente. Après des années d'investissement, les résultats obtenus par les responsables en charge de la sécurité seront bientôt passés au crible et sont essentiels pour permettre l'amélioration des données.

Le renseignement sur la cybermenace permettra de définir des stratégies de cybersécurité

Le renseignement sur la cybermenace (CTI - *Cyber Threat Intelligence*) vise à aider les organisations à mieux se préparer en améliorant leurs connaissances sur le paysage des menaces. Au lieu de s'appuyer exclusivement sur des informations générées par des systèmes ou des sources internes (ce que l'on sait sur ce que l'on sait), l'efficacité du CTI sera déterminée par la connaissance du *pourquoi*, du *comment* et du *quoi*, éléments alors inconnus pour l'équipe de cybersécurité. La proposition de valeur de toute capacité ou de tout programme CTI est de mieux préparer l'organisation à protéger ses actifs critiques contre des menaces inconnues.

La connaissance du paysage des menaces

L'automatisation et l'orchestration de la cybersécurité étant considérées comme une tendance croissante, **les équipes de cybersécurité consacreront moins de temps aux activités de surveillance, mais davantage aux opérations de préparation**. Bien conçue, une capacité de CTI peut fournir des connaissances contextualisées et exploitables sur les menaces afin d'informer les parties prenantes stratégiques, opérationnelles et tactiques de toute l'organisation. Concrètement, une capacité de CTI doit pouvoir répondre aux questions ci-dessous, en tenant compte des exigences des parties prenantes ainsi que du contexte et de l'environnement de l'organisation:

- Quelle est la surface d'attaque?
- Quels sont les actifs les plus précieux et le cyberterrain?
- Quelles sont les vulnérabilités les plus critiques?
- Quels sont les vecteurs d'attaque les plus utilisés?
- Comment les adversaires se comportent-ils et opèrent-ils de manière générale?
- À quoi ressemble le paysage des menaces pour:
    - le secteur et le type d'activité que l'organisation exerce?
    - l'environnement technologique adopté par l'organisation?
- Que faut-il faire pour atténuer les risques liés à ces menaces et qui doit s'en charger?

La pénurie de compétences en cybersécurité

Le manque de professionnels hautement qualifiés dans le domaine des technologies pose déjà un problème pour l'ambition affichée par l'Europe en matière de numérisation. Selon une étude[23], plus de 70 % des entreprises européennes déclarent que le manque de compétences entrave leurs stratégies d'investissement, tandis que 46 % des entreprises font état de difficultés à pourvoir les postes vacants en raison de la pénurie de compétences dans des domaines clés tels que la cybersécurité.

Tendances émergentes

_*Cinq* tendances en matière de cybermenaces

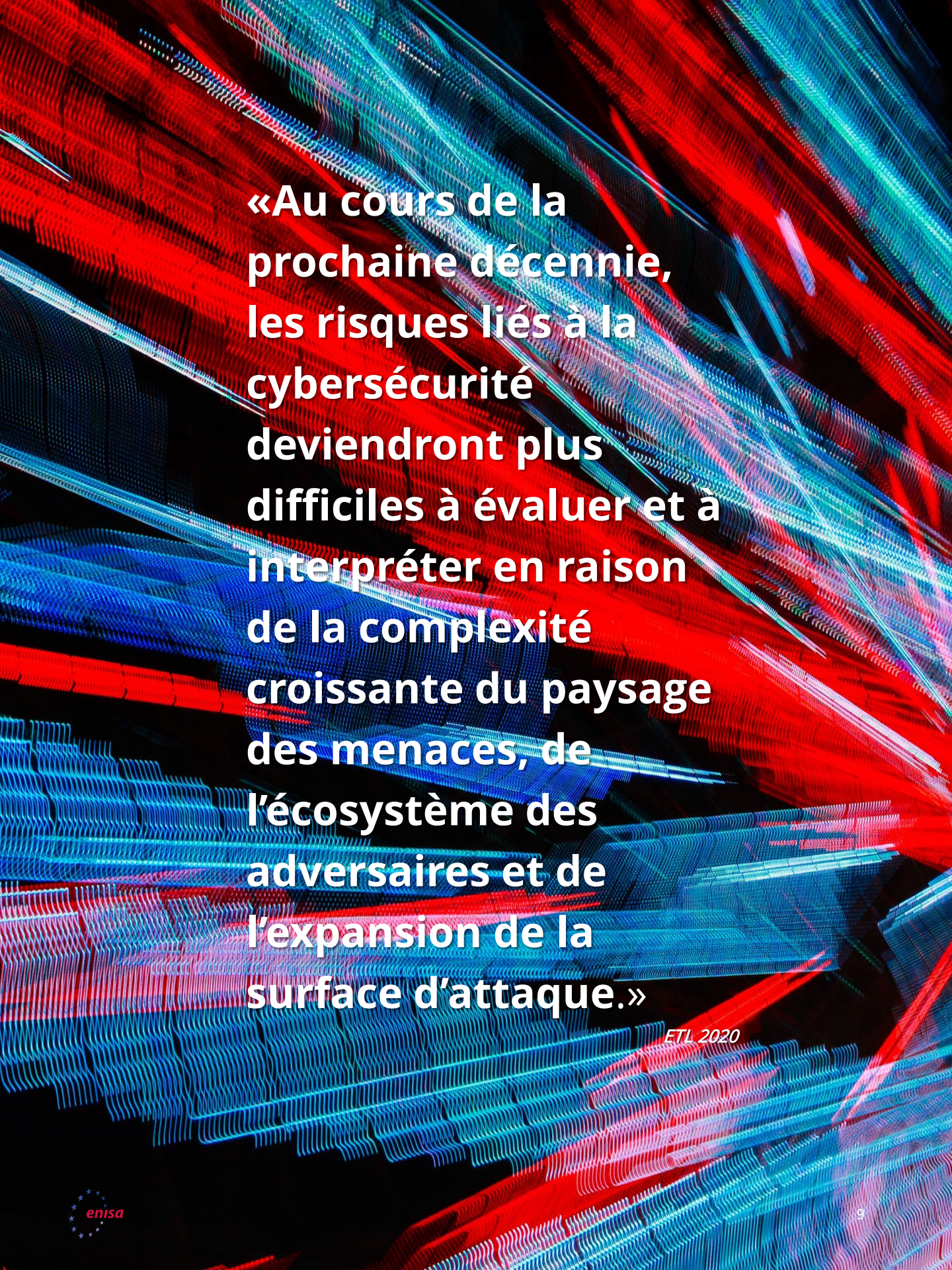
_01 Les logiciels malveillants font l'objet de mises à jour. Les souches des familles de logiciels malveillants sont mises à niveau vers de nouvelles versions présentant des fonctionnalités, des mécanismes de diffusion et de propagation supplémentaires. Emotet, par exemple, logiciel malveillant initialement conçu en 2014 comme cheval de Troie bancaire, est devenu l'un des distributeurs de logiciels malveillants les plus efficaces en 2019.[2]

_02 Les menaces deviendront totalement mobiles. Les utilisateurs sont de plus en plus dépendants des appareils mobiles pour sécuriser leurs comptes les plus sensibles. L'utilisation de l'authentification à deux facteurs liée à un mécanisme d'authentification dans une application ou via un message texte en est un exemple. Avec le nombre croissant de logiciels malveillants désormais entièrement mobiles, les applications frauduleuses, le piratage des cartes SIM (*SIMjacking*) et les attaques de systèmes d'exploitation, ces appareils mobiles constituent le maillon faible et sont donc extrêmement vulnérables aux attaques.

_03 Les attaquants utilisent de nouveaux types de fichiers, comme des fichiers image disque (ISO et IMG), pour diffuser des logiciels malveillants. Les fichiers DOC, PDF, ZIP et XLS restent les types de pièces jointes les plus utilisés pour diffuser des logiciels malveillants, mais d'autres types de fichiers sont désormais de plus en plus répandus. Quelques campagnes de diffusion d'AgentTesla InfoStealer et de NanoCore RAT utilisant le type de fichier image ont été découvertes en 2019.

_04 Augmentation des attaques par rançongiciel ciblées et coordonnées. En 2019, nous avons assisté à une escalade d'attaques malveillantes sophistiquées et ciblées au moyen de rançongiciels qui visaient principalement le secteur public, les organismes liés à la santé et des secteurs spécifiques. Les attaquants passent désormais de plus en plus de temps à recueillir des renseignements sur leurs victimes, pour savoir exactement ce qu'il faut chiffrer, créer un maximum de perturbations et obtenir des rançons plus élevées.

_05 Les attaques par bourrage d'identifiants (*credential stuffing*) vont se généraliser. Le *credential stuffing*, autrement dit l'injection automatisée de combinaisons nom d'utilisateur/mot de passe volées par le biais de demandes de connexion automatisées à grande échelle dirigées contre une application web, se multipliera suite aux violations de données anormalement nombreuses et au vol de milliards de données personnelles qui ont eu lieu ces dix dernières années.


«Au cours de la prochaine décennie, les risques liés à la cybersécurité deviendront plus difficiles à évaluer et à interpréter en raison de la complexité croissante du paysage des menaces, de l'écosystème des adversaires et de l'expansion de la surface d'attaque.»
ETL 2020

Tendances émergentes

_Dix tendances émergentes liées aux vecteurs d'attaque

01_Les attaques seront diffusées en masse sur une courte durée mais avec un impact plus large

Ces attaques ont pour but d'affecter le plus grand nombre d'appareils possibles pour voler des informations personnelles ou bloquer l'accès aux données en chiffrant les fichiers.

02_Des attaques précisément ciblées et persistantes seront méticuleusement planifiées avec des objectifs bien définis et à long terme

Les acteurs malveillants prévoient ce type d'attaques pour atteindre des données de grande valeur, telles que des informations financières, des droits de propriété intellectuelle et industrielle, des secrets d'affaires, des informations classifiées, etc.

03_Les acteurs malveillants utiliseront les plateformes numériques dans des attaques ciblées

Les acteurs malveillants exploreront le potentiel des plateformes numériques pour soutenir des attaques ciblées (par ex., les médias sociaux, les jeux, les messageries, les plateformes de diffusion en continu, etc.). Du vol de données à caractère personnel pour mener des attaques d'hameçonnage ciblé (*spearphishing*) à la vaste distribution de logiciels malveillants, les plateformes numériques dotées d'un grand nombre d'abonnés sont des vecteurs d'attaque efficaces de plus en plus prisés par les acteurs malveillants.

04_ L'exploitation des processus métier augmentera

Avec davantage d'automatisation et moins d'intervention humaine, les processus métier peuvent faire l'objet de modifications malveillantes afin de permettre à l'attaquant d'en retirer un bénéfice. Communément appelée «compromission de processus métier» (BPC - *Business Process Compromise*), cette technique est souvent sous-estimée par les spécialistes en génie des procédés en raison de l'absence d'une évaluation appropriée en matière de risques.

05_ La surface d'attaque continuera à s'étendre

Le courriel n'est plus le seul et unique outil ni le principal vecteur d'attaque pour l'hameçonnage (*phishing*). Les acteurs malveillants utilisent désormais d'autres plateformes pour communiquer et inciter les victimes à ouvrir des pages web compromises. Une nouvelle tendance est en train d'émerger avec l'utilisation des SMS, de WhatsApp, de Snapchat et des messageries de réseaux sociaux.

06_Le télétravail sera exploité par le biais d'appareils domestiques

Le risque d'ouvrir de nouveaux points d'entrée pour les attaquants augmentera du fait de l'augmentation du nombre de personnes en télétravail qui connectent leurs appareils à des réseaux d'entreprise. Avec la pandémie de COVID-19, cette tendance incitera les responsables informatiques à renforcer les politiques de sécurité et à apporter d'urgence des changements à l'infrastructure informatique.

07_Les attaquants seront mieux préparés

Les attaquants choisissent leurs cibles avec soin, effectuent des reconnaissances contre des employés spécifiques avant de les viser par des attaques d'hameçonnage ciblé afin d'obtenir des identifiants utilisables et de prendre l'organisation pour cible. Après avoir accédé à une première machine, les attaquants peuvent alors utiliser des outils servant aux tests d'intrusion, comme Mimikatz, pour collecter et exploiter des identifiants avec privilèges élevés.

08_Les techniques d'obfuscation se perfectionneront

Les auteurs de menace innovent en permanence pour rendre les menaces plus efficaces et moins sensibles aux détections. Anubis, à la fois cheval de Troie bancaire Android et bot, a été distribué en se faisant passer pour une application inoffensive, principalement via Google Play Store.[1]

09_L'exploitation automatisée de systèmes non corrigés et d'applications abandonnées augmentera

L'augmentation anormale du trafic Telnet vers le port 445 observée en 2019 a levé le voile sur l'expansion de vers et de codes d'exploitation comme Eternal Blue. Telnet, qui n'est plus utilisé, sauf dans le domaine de l'internet des objets (IoT - *Internet of Things*), a enregistré les plus gros volumes au cours de cette période.

10_Les cybermenaces se déplacent vers la périphérie

Les dispositifs de bord se déploient aux frontières entre les réseaux interconnectés. Nous avons constaté une tendance croissante aux attaques visant ces dispositifs (comme les routeurs, les commutateurs et les pare-feu) qui ont un impact important sur une entreprise et sur l'écosystème numérique connecté.

Références

1. «ISO/IEC 27032:2012». ISO. https://www.iso.org/standard/44375.html

2. «Triple Threat: Emotet Deploys TrickBot to Steal Data & Spread Ryuk.» 2 avril 2019. Cybereason. https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware

3. «Understanding the relationship between Emotet, Ryuk and TrickBot.» 14 avril 2019. Intel471. https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/

4. «Investigating WMI Attacks» 9 février 2019. SANS. https://www.sans.org/blog/investigating-wmi-attacks/

5. «RDP Abuse and Swiss Army Knife Tool Used to Pillage, Encrypt and Manipulate Data» 18 décembre 2019. Bitdefender. https://labs.bitdefender.com/2019/12/rdp-abuse-and-swiss-army-knife-tool-used-to-pillage-encrypt-and-manipulate-data/

6. «Europe's huge privacy fines against Marriott and British Airways are a warning for Google and Facebook» 10 juillet 2019. CNBC. https://www.cnbc.com/2019/07/10/gdpr-fines-vs-marriott-british-air-are-a-warning-for-google-facebook.html

7. «This is how we might finally replace passwords» 27 mai 2019. C|Net. https://www.cnet.com/news/this-is-how-we-might-finally-replace-passwords/

9. «Authentication standards to help reduce the world's over-reliance on passwords.» FIDO. https://fidoalliance.org/overview/

10. «How Much Cyber Sovereignty is Too Much Cyber Sovereignty?» 3 octobre 2019. Council on Foreign Relations. https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty

11. «Conceptualising Cyber Arms Races». 2016. OTAN. https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

12. «Journalism, "Fake News" and Disinformation: A Handbook for Journalism Education and Training» 2018. UNESCO. https://en.unesco.org/fightfakenews

13. «The Big Connect: How Data Science is Helping Cybersecurity». 12 juin 2019. Info Security Group. https://www.infosecurity-magazine.com/blogs/data-science-helping-cybersecurity-1/

14. «Are You Ready For The Age Of Adversarial AI? Attackers Can Leverage Artificial Intelligence Too». 9 janvier 2020. Forbes. https://www.forbes.com/sites/forbestechcouncil/2020/01/09/are-you-ready-for-the-age-of-adversarial-ai-attackers-can-leverage-artificial-intelligence-too/#2a76dee14703

15. https://euvsdisinfo.eu/

16. «FBI Alerts Companies of Cyber Attacks Aimed at Supply Chains». 21 février 2020. Bitsight. https://www.bitsight.com/blog/fbi-alerts-companies-of-cyber-attacks-supply-chains

17. «Gartner Identifies the Top Seven Security and Risk Management Trends for 2019». 5 mars 2019. Gartner. https://www.gartner.com/en/newsroom/press-releases/2019-03-05-gartner-identifies-the-top-seven-security-and-risk-ma

18. «Android banking trojan.» 3 octobre 2019. Cyare. https://cyware.com/news/exploring-the-nature-and-capabilities-of-anubis-android-banking-trojan-6ea7dec4

19. «5 Top Trends for Mobile Cyber Security in 2020». 9 janvier 2020. Corrata. https://corrata.com/5-top-trends-for-mobile-cyber-security-in-2020/

20. «Malicious Attachments Remain a Cybercriminal Threat Vector Favorite». 27 août 2020. Threat Post. https://threatpost.com/malicious-attachments-remain-a-cybercriminal-threat-vector-favorite/158631/

21. «10 trends shaping the future of work». Octobre 2019. EPSC. https://op.europa.eu/en/publication-detail/-/publication/e77a1580-0cf5-11ea-8c1f-01aa75ed71a1/language-en/format-PDF/source-121729338

22. «Global security spending to top $103 billion in 2019, says IDC», 20 mars 2019. ZDNet. https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-idc/

23. «Insights into skills shortages and skills mismatch. learning from Cedefop's European skills and jobs survey». 2018. CEDEFOP. https://www.cedefop.europa.eu/files/3075_en.pdf

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.

Autres publications

Advancing Software Security in the EU

Ce rapport présente les éléments clés de la sécurité logicielle et donne un bref aperçu des approches et des normes existantes les plus pertinentes dans le paysage du développement de logiciels sécurisés.

LIRE LE RAPPORT

ENISA good practices for security of Smart Cars

Bonnes pratiques pour la sécurité des voitures intelligentes, c'est-à-dire les véhicules connectés et (semi-)autonomes, afin d'améliorer l'expérience des utilisateurs et la sécurité des voitures.

LIRE LE RAPPORT

Good Practices for Security of IoT - Secure Software Development Lifecycle

Sécurité de l'internet des objets mettant l'accent sur les orientations en matière de développement logiciel.

LIRE LE RAPPORT

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

ETL 2020

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

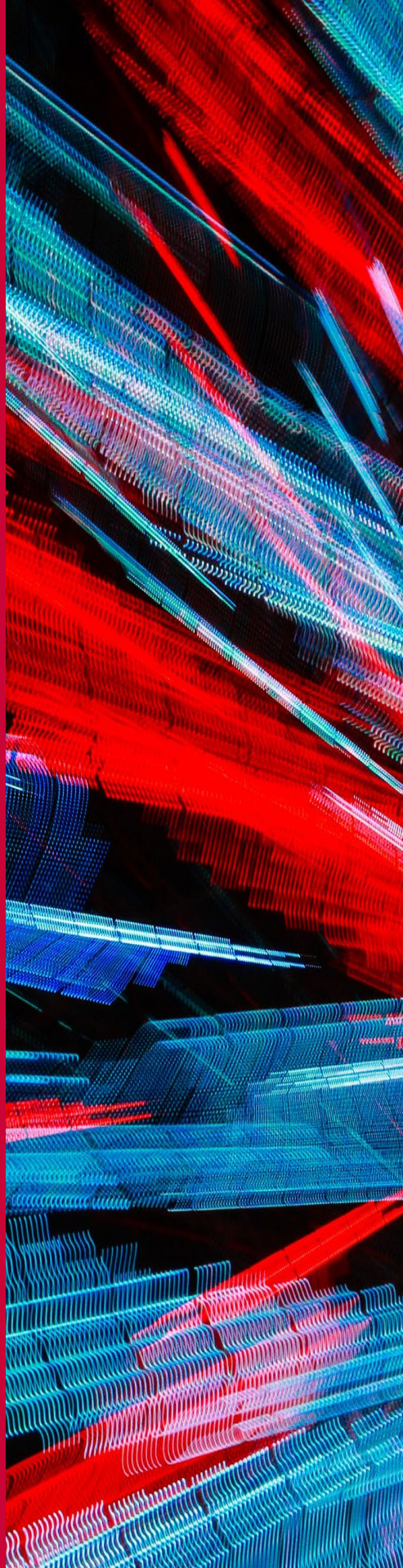
Il convient de noter que, sauf mention contraire, la présente publication représente les points de vue et les interprétations de l'ENISA. Elle ne doit pas être interprétée comme une action légale de l'ENISA ou des organes de l'ENISA à moins d'être adoptée conformément au règlement (UE) nº 526/2013. Elle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