The world is how we shape it

sopra steria

ÉTAT DE LA CYBERSÉCURITÉ EN 2025

Sommaire

Synthèse 03

Introduction 05

Insight: Les directives sur la défense numérique 06

01. Cybercriminalité et méthodes 08

Étapes de compromission 09

Outils et techniques 10

Infrastructure 12

Insight: Surveillance et gestion à distance 13

02. Compromission initiale 15

Phishing 15

Tendances du phising observées en 2024 15

Médias sociaux 19

Dans la boîte de réception 19

Vulnérabilités 23

Focus sur les réseaux privés virtuels 25

L'armement des vulnérabilités 26

Cibler l'interface 27

Insight: La cybersécurité OT en 2024 28

03. Après la compromission 30

Logiciels malveillants et voleurs 31

A l'intérieur des systèmes 32

Observés et bloqués 33

Insight: Empoisonnement du référentiel 36

L'écosystème des ransomwares 38

04. Paysage des menaces 39

Volatilité des groupes de ransomware 40

Principales observations 41

Insight: L'intelligence artificielle 42

05. Recommandations pour les défenseurs 44

Phising 45

Vulnérabilités 46

Logiciels malveillants 46

Le point de vue du Pentester 47

Perspectives 2025 49

Comment Sopra Steria peut vous aider 51

Synthèse

Le rapport « Etat de la Cybersécurité en 2025 » fournit une analyse complète du paysage actuel de la cybersécurité et met en évidence les principales tendances, menaces et évolutions réglementaires. L'objectif de ce rapport est d'informer les décideurs sur l'évolution de l'environnement de la cybersécurité et de fournir des recommandations concrètes pour renforcer la sécurité des organisations.

La Norvège s'apprête à mettre en place son premier cadre réglementaire intersectoriel pour la sécurité numérique, en s'inspirant de la directive NIS1 de l'UE et de certains éléments de la directive NIS2. La loi sur la sécurité numérique et la loi sur la résilience opérationnelle numérique (DORA) sont essentielles pour façonner le paysage de la cybersécurité. La réglementation DORA se concentre spécifiquement sur la résilience du secteur financier face aux menaces liées aux technologies avancées de l'information et de la communication (TIC). Ces cadres visent à obliger les entreprises à prendre la cybersécurité au sérieux et à intégrer la résilience dans leurs activités de base.

En 2024, les cybercriminels ont employé diverses tactiques, notamment l'utilisation d'outils de surveillance et de gestion à distance (RMM) et de logiciels légitimes à des fins malveillantes. La spécialisation des groupes cybercriminels et l'exploitation d'environnements hybrides ont constitué des tendances notables. Les cybercriminels ont utilisé des méthodes telles que le phishing, l'exploitation de comptes valides et l'exploitation de vulnérabilités publiques pour obtenir un accès initial.

Les techniques de collecte de données et les objectifs destructeurs tels que le chiffrement des données et l'inhibition de la restauration du système ont prévalu.

L'utilisation croissante par les cybercriminels d'outils d'administration légitimes, de logiciels malveillants, d'outils de vol de données et d'outils d'évasion de réseau complique considérablement la détection et l'atténuation de ces menaces. Le rapport souligne la sophistication de ces outils et la nécessité de mettre en place des stratégies de détection et de réponse avancées.

D'importantes vulnérabilités ont été identifiées dans les réseaux privés virtuels (VPN), les interfaces de programmation d'applications (API) et d'autres composants d'infrastructures critiques. La militarisation des vulnérabilités et l'exploitation des services de tunnellisation pour l'exfiltration de données constituent des préoccupations majeures. Le délai d'exploitation, qui mesure le temps moyen nécessaire à l'exploitation d'une vulnérabilité après sa divulgation, a considérablement diminué ces dernières années pour n'être plus que de cinq jours. Pour atténuer ces risques, les organisations doivent donner la priorité à l'application régulière de correctifs et de mises à jour.

Le phishing demeure l'un des principaux vecteurs d'attaque, avec les attaques de phishing multicanal, les attaques Adversary-in-the-middle (AiTM) et la montée en puissance des plateformes de Phishing-as-a-Service (PhaaS) qui constituent des tendances significatives. Le rapport fournit des observations détaillées sur les tactiques de phishing et les stratégies d'atténuation, en soulignant l'importance de l'authentification multifactorielle (MFA) et de la sensibilisation des utilisateurs.

La résurgence des logiciels malveillants, en particulier des voleurs d'informations comme Lumma Stealer, met en évidence le rôle des logiciels malveillants dans les opérations d'accès initial et les défis posés aux défenseurs par les attaquants utilisant des techniques de persistance. Ce rapport souligne la nécessité de disposer de solutions robustes de détection et d'intervention sur les points finaux (EDR) pour lutter contre ces menaces.

L'évolution du modèle RaaS (Ransomware-as-a-Service) et la volatilité des groupes de ransomware sont examinées, soulignant l'augmentation significative des attaques de ransomware et l'utilisation de techniques avancées par les opérateurs. Le rapport recommande des mesures proactives, telles que la segmentation du réseau et la détection des menaces en temps réel, pour atténuer les risques liés aux ransomwares.

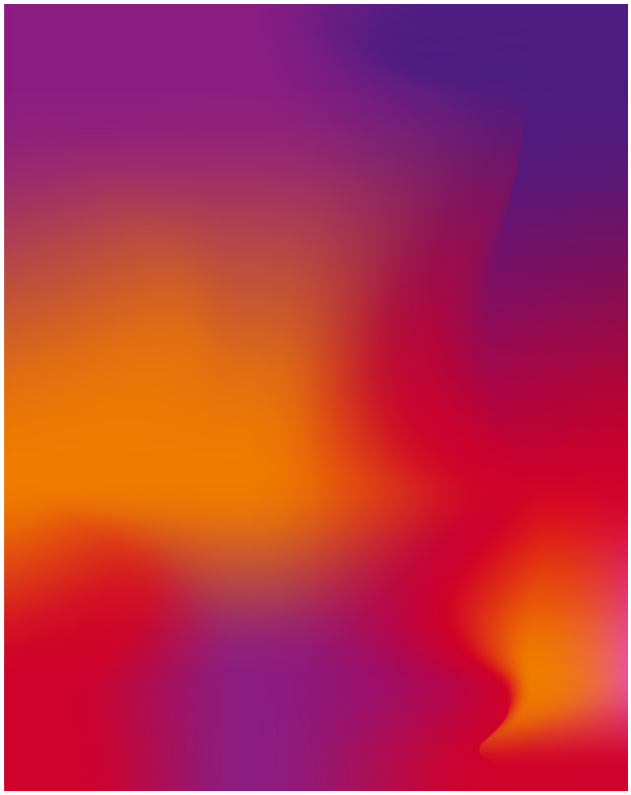
L'impact de l'IA générative sur la cybersécurité comprend la génération de faux contenus, l'ingénierie sociale et le développement de logiciels malveillants. Les risques associés à l'IA fantôme et à l'utilisation d'agents virtuels pour des attaques automatisées sont également abordés. Les organisations doivent mettre en place des mesures de protection pour prévenir l'utilisation malveillante des technologies d'IA.

Introduction

Ce rapport s'adresse à un large public : responsables de la sécurité, praticiens, ainsi qu'à tous ceux qui s'intéressent à la cybersécurité.

À une époque où les acteurs de menaces étatiques et les vulnérabilités émergentes font quotidiennement la une, identifier les menaces prioritaires devient de plus en plus complexe. Ce rapport compile les données de terrain de Sopra Steria provenant d'un large éventail d'organisations de divers secteurs. Les lecteurs peuvent explorer les analyses des méthodologies d'attaque, les actions post-intrusion des cybercriminels, ainsi que les recommandations pratiques des experts en réponse aux incidents afin de se protéger contre de telles violations. La cybersécurité peut apparaître comme une lutte sans fin, mais ce rapport reflète la conviction qu'avec intelligence, perspicacité et préparation, les défenseurs peuvent conserver un avantage stratégique.

L'objectif de ce rapport est d'informer et d'éclairer les parties prenantes sur un paysage de menaces en constante évolution. Et de fournir une connaissance stratégique permettant aux lecteurs de mieux naviguer dans l'environnement de la cybersécurité.



— L'objectif de ce rapport est d'informer et d'éclairer les parties prenantes sur un paysage de menaces en constante évolution.

Les directives sur la défense numérique

Selon la stratégie nationale pour la sécurité de l'information en 2003,

« Il est nécessaire d'entamer des travaux sur le cadre réglementaire afin de garantir que les règles existantes soient mieux appliquées dans la pratique et de fournir une base solide pour leur renouvellement et leur développement (...) »

Depuis plus de vingt ans, les autorités norvégiennes s'attachent à identifier les infrastructures informatiques critiques. Plus de vingt ans après cette première stratégie pour la sécurité de l'information, la Norvège s'apprête à introduire son premier cadre réglementaire intersectoriel pour la sécurité numérique. L'adoption de la loi sur la sécurité numérique, qui transpose d'abord la directive NIS1 puis la directive NIS2, s'inscrit toutefois dans une démarche pilotée par l'UE. Globalement, nous observons une multiplication des réglementations qui régissent la cybersécurité, tant au niveau national qu'à l'échelle régionale via les directives européennes. L'objectif de ces réglementations, qu'elles émanent des autorités nationales ou de l'UE, est de contraindre les entreprises à prendre la cybersécurité au sérieux, les recommandations et mesures volontaires ayant montré leurs limites.

Les cadres réglementaires reflètent souvent une compréhension évolutive du paysage des menaces et la loi sur la sécurité numérique/NIS2 ne fait pas exception. L'interconnexion croissante des infrastructures critiques et la dépendance aux systèmes numériques ont amplifié les vulnérabilités. Il devient donc essentiel d'adopter des cadres qui non seulement traitent les risques existants, mais préparent également aux défis futurs. L'approche intersectorielle de cette loi reconnaît que les menaces de cybersécurité ne respectent pas les frontières sectorielles et qu'une approche unifiée s'impose pour protéger l'infrastructure nationale.

L'année 2024 marque un tournant : le cadre réglementaire fait l'objet d'une attention accrue et son impact devient tangible. La loi DORA, applicable au secteur financier et qui entrera en vigueur en 2025, constitue le premier cadre réglementaire norvégien à véritablement s'attaquer au paysage complexe des menaces auxquelles fait face le secteur financier. DORA introduit notamment des tests basés sur les menaces et renforce les exigences en matière de réponse aux incidents. Ces éléments témoignent d'une évolution vers des mécanismes plus robustes d'identification et d'atténuation des risques dans les secteurs fortement exposés aux menaces avancées.

Contrairement à la loi sur la sécurité numérique, qui s'appliquera à une grande partie des organisations norvégiennes tous secteurs confondus, DORA est bien plus complète en termes de résilience opérationnelle numérique. Le secteur financier, compte tenu de son importance systémique et de sa vulnérabilité

aux cyberattaques, nécessite des réglementations plus strictes qui mettent l'accent non seulement sur la prévention, mais aussi sur la continuité et la récupération. Les exigences détaillées de DORA visent à garantir que les institutions financières restent fonctionnelles même en conditions dégradées, réduisant ainsi le risque de perturbation généralisée.

La loi sur la sécurité numérique, qui n'est pas encore entrée en vigueur, réglemente principalement les exigences fondamentales de sécurité. Elle impose une approche de la sécurité fondée sur les risques au sein des organisations. Bien que ce cadre n'impose pas explicitement une approche fondée sur les menaces, plusieurs éléments suggèrent que les organisations doivent tenir compte de l'évolution constante du paysage des menaces dans leurs efforts de sécurité. Premièrement, le niveau de sécurité des organisations doit s'établir sur une compréhension de la sécurité numérique comme fondement de leur activité.

Deuxièmement, le risque organisationnel est étroitement lié aux acteurs de menaces auxquels l'organisation fait face. Troisièmement, la gestion des risques n'est pas un processus statique mais une approche dynamique qui doit s'adapter aux évolutions du paysage des menaces et aux nouveaux vecteurs d'attaque.

D'ici 2025, NIS2 devrait être transposée dans la législation norvégienne. Toutefois, son entrée en vigueur effective reste incertaine. Ce cadre, encore en cours d'élaboration, mettra davantage l'accent sur la continuité des activités et la gestion des incidents. La portée exacte et les détails de ces exigences restent à déterminer. Néanmoins, cette progression vers des réglementations plus détaillées et concrètes indique une tendance plus large à l'intégration de la cybersécurité dans les stratégies et cadres nationaux.

L'essentiel est que les organisations norvégiennes doivent adopter une approche holistique du travail de sécurité, dont le non-respect peut entraîner des sanctions sous forme d'amendes administratives. L'introduction de ces cadres souligne une évolution générale vers l'intégration de la résilience dans les structures opérationnelles fondamentales des organisations, leur permettant d'être mieux équipées pour affronter les défis d'un paysage numérique en évolution rapide.

— Les cadres réglementaires reflètent souvent une compréhension évolutive du paysage des menaces, et la loi sur la sécurité numérique/NIS2 ne fait pas exception. —

01

Cybercriminalité et méthodes

En 2024, les cybercriminels ont déployé un large éventail de tactiques, techniques et procédures (TTP) couvrant plusieurs étapes de la Kill Chain. Ils ont exploité de nombreux outils, logiciels malveillants et méthodes pour faire progresser leurs attaques, illustrant des tendances significatives dans l'évolution des cybermenaces. Ces tendances mettent en évidence les efforts des attaquants pour contourner les systèmes de détection traditionnels et tirer parti de la complexité des environnements hybrides.

On observe notamment une utilisation accrue des outils de surveillance et de gestion à distance (RMM) qui, en raison de leurs capacités étendues et de leur intégration dans certains environnements d'entreprise, permettent aux attaquants de déployer diverses techniques tout en se dissimulant dans le trafic légitime.

L'analyse des outils et logiciels malveillants prédominants révèle une diversification des méthodes et une exploitation renforcée des logiciels légitimes à des fins malveillantes.

En 2024, les groupes cybercriminels se sont spécialisés, avec davantage de groupes se concentrant sur une étape de la chaîne d'attaque plutôt que sur l'attaque complète : par exemple, des attaquants spécialisés dans l'accès initial, l'exploitation de vulnérabilités ou le développement de logiciels malveillants.

Les acteurs criminels innovent avec des techniques d'évasion et un chiffrement renforcé pour contourner les solutions de sécurité. La persistance de ces acteurs démontre l'intérêt lucratif que représente cette méthode d'extorsion pour les cybercriminels, particulièrement à travers les attaques de double extorsion.

Les cybercriminels, de plus en plus adaptatifs, se concentrent sur les infrastructures réseau et les plateformes SaaS, ciblant les fondements des environnements cloud et du travail à distance. Cette transition illustre non seulement leur capacité à exploiter les faiblesses organisationnelles, comme la gestion des correctifs, mais aussi leur stratégie visant à maximiser l'impact dans un monde interconnecté.

Étapes de compromission

Accès initial

Les observations de Sopra Steria révèlent que les cybercriminels ont principalement exploité les techniques suivantes du référentiel MITRE ATT&CK[1] pour accéder aux systèmes tout au long de 2024 :

• Phishing (T1566): les cybermenaces continuent de faire preuve d'innovation dans les campagnes de phishing.

• Comptes Valides (T1078) : la prévalence des voleurs d'informations en 2024 a considérablement influencé la façon dont les acteurs malveillants ont obtenu leur accès initial aux systèmes cibles.

• Exploitation de Vulnérabilités Publiques (T1190) : l'exploitation de vulnérabilités dans les systèmes exposés sur Internet demeure une méthode marginalement utilisée par la sphère cybercriminelle.

Les méthodes utilisées par les cybercriminels pour obtenir l'accès initial aux systèmes compromis impliquent de plus en plus l'utilisation de comptes valides préalablement acquis par les acteurs malveillants. À travers une compromission initiale par un voleur d'informations, RDP, SSH ou autre, les identifiants sont achetés sur le darknet puis réutilisés à d'autres fins.

Collecte de données

Les attaquants ont diversifié et intensifié leur recherche d'informations sensibles sur les systèmes compromis. Cela explique la présence des techniques suivantes dans le top des techniques de 2024 :

• Extraction des Identifiants du Système d'Exploitation (T1003)

• Données du Système Local (T1005)

• Exfiltration par Canal C2 (T1041)

Impact et objectifs Destructeurs

• Chiffrement des Données (T1486) : principalement utilisé dans les attaques de ransomware pour rendre les données inaccessibles aux victimes.

• Inhibition de la Récupération Système (T1490) : empêche les victimes de restaurer les systèmes à partir de sauvegardes, aggravant l'impact de l'attaque.

Ces méthodes indiquent un objectif destructeur final accompagné d'impacts significatifs sur les systèmes cibles.

[1] https://attack.mitre.org/techniques/enterprise/

Outils et Techniques

L'utilisation croissante de services et de plateformes légitimes par les cybercriminels marque un changement majeur dans leurs tactiques. Ne se limitant plus aux outils malveillants traditionnels, ils adoptent désormais une approche de type « Living off the Land », exploitant des outils déjà présents sur le système cible.

Cette évolution témoigne de leur expertise avancée et de leur connaissance approfondie des environnements qu'ils ciblent, reflétant un nouveau niveau de maturité technologique.

Utilisation accrue d'outils d'administration légitimes :

Des outils comme ADExplorer, AnyDesk, Advanced IP Scanner et PsExec sont fréquemment détournés pour des intrusions dans les systèmes d'entreprise. Ces outils permettent aux attaquants d'explorer l'infrastructure, de maintenir un accès constant et d'étendre leurs attaques tout en réduisant le risque de détection en faisant passer leurs actions pour des opérations légitimes.

Par exemple, AnyDesk et TeamViewer facilitent le contrôle à distance, tandis qu'ADExplorer et les commandes PowerShell permettent la cartographie de l'Active Directory.

Prolifération des logiciels malveillants et des outils de vol de données

Des outils de vol de données tels que Mimikatz, LaZagne et d'autres, ainsi que des logiciels malveillants spécialisés comme Lumma Stealer, Redline et Raccoon Stealer, ont été largement déployés pour extraire des informations d'identification.

Ces outils permettent aux attaquants d'exfiltrer des mots de passe et des informations sensibles, facilitant ainsi l'accès non autorisé et les mouvements latéraux au sein des réseaux d'entreprise.

Les cybercriminels actualisent fréquemment leurs outils pour échapper à la détection. Par exemple, Lumma Stealer bénéficie de mises à jour hebdomadaires de son code et de ses serveurs, ce qui le rend plus difficile à détecter et plus attractif pour les criminels. Ce cycle de mise à jour rapide lui permet de devancer les fonctions de sécurité des navigateurs web. De même, Latrodectus, le successeur d'IcedID, supprime certaines fonctions dans ses mises à jour pour échapper à la détection.

Exploitation des services de tunnellisation et des outils d'évasion réseau

Les cybercriminels exploitent des services de tunneling tels que Ngrok et Cloudflare Tunnel pour contourner les mesures de sécurité. Ces outils compliquent la détection et l'interruption des connexions malveillantes, et illustrent la sophistication croissante des attaquants pour échapper aux défenses réseau.

Utilisation d'outils d'exploitation des vulnérabilités

Des outils et techniques tels que Metasploit, Nmap et Kerberoasting sont déployés pour identifier et exploiter les vulnérabilités des systèmes réseau et des services d'authentification. En révélant les mauvaises configurations de sécurité, ces approches permettent aux attaquants d'infiltrer et de compromettre potentiellement des infrastructures entières.

Outils d'évasion et de persistance

Les attaquants exploitent des outils comme SystemBC et SocGholish pour dissimuler leur présence et maintenir l'accès aux systèmes infectés. Ils utilisent également BITSAdmin et PowerShell pour automatiser les tâches malveillantes. Cette combinaison d'outils légitimes et de logiciels malveillants avancés rend leurs actions plus difficiles à détecter et plus efficaces.

Utilisation de services légitimes pour l'exfiltration de données

Les cybercriminels exploitent des plateformes de partage de fichiers comme Dropbox et MEGA pour exfiltrer discrètement des données volées. En s'appuyant sur des services de confiance, ils compliquent la détection pour les équipes de sécurité, démontrant leur habileté à contourner les défenses traditionnelles et à exploiter les vulnérabilités des services externes.

Canaux C2 multiples pour éviter la détection

Les attaquants exploitent des canaux tels que Discord, Telegram, IRC et SMTP pour communiquer avec les machines infectées. Cette diversité témoigne de leur capcité technique à maintenir des systèmes de commandement et de contrôle (C2) flexibles et résilients. En utilisant plusieurs services, ils réduisent le risque de perturbation si un canal est bloqué, démontrant leur capacité d'adaptation.

Infrastructure

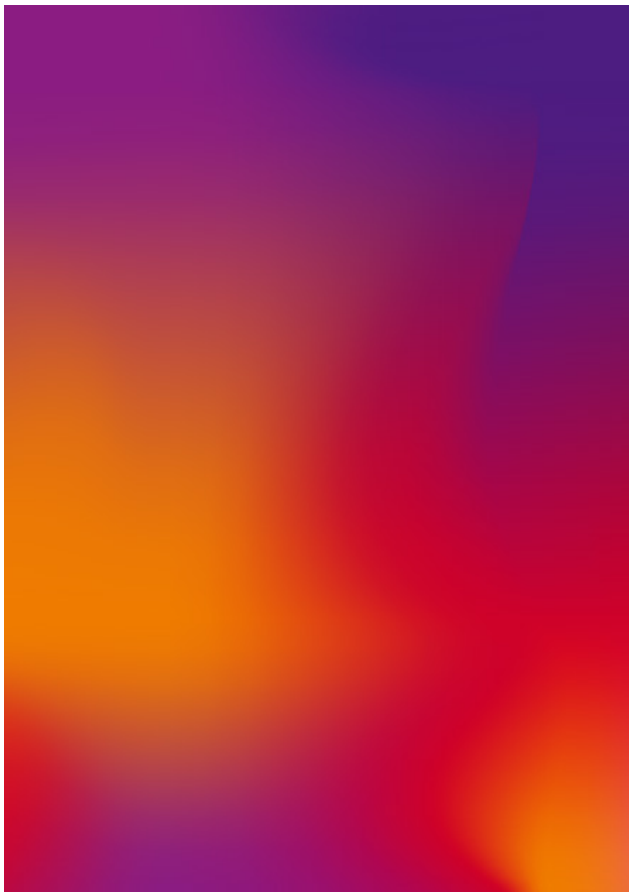
Exploitation des API et des technologies de streaming

Les attaquants exploitent les API de services tels que GitHub, GitLab, GoFile et Vimeo pour intégrer ces plateformes dans leurs processus C2. Cette automatisation renforce la résilience et l'efficacité de leurs opérations.

L'utilisation de technologies comme WebSockets et WatsonTCP témoigne de leur maîtrise des protocoles de communication avancée.

Obfuscation via des algorithmes de destination générés aléatoirement

En utilisant des algorithmes qui génèrent des destinations aléatoires pour le transfert de données, les cybercriminels compliquent la détection des flux d'exfiltration. Cette technique d'obfuscation révèle une compréhension approfondie des méthodes d'analyse du trafic réseau et des moyens de contourner les mesures de détection basées sur les patterns comportementaux.



Utilisation des services cloud

Les attaquants exploitent des services tels que CloudFlare, Amazon Web Services et Firebase pour dissimuler leurs activités derrière une infrastructure cloud légitime. Cela complique, pour les analystes de sécurité, la distinction entre trafic normal et trafic malveillant, démontrant la maturité des attaquants et leur connaissance des pratiques de sécurité cloud.

Surveillance et gestion à distance

Un outil de surveillance et de gestion à distance (RMM) est un type de logiciel conçu pour aider les fournisseurs de services gérés (MSP) et les professionnels informatiques à surveiller et gérer à distance les terminaux, réseaux et ordinateurs clients lorsque l'accès physique est limité. Ces outils offrent généralement une gamme de fonctionnalités, telles que l'accès à distance, la surveillance, l'automatisation, les alertes, la génération de rapports et la gestion de la sécurité.

Bien que conçus à des fins légitimes, ils sont de plus en plus exploités par les cybercriminels pour leurs capacités étendues. Les cybercriminels utilisent les outils RMM pour contrôler à distance les ordinateurs des victimes, mener des opérations de reconnaissance, déployer des logiciels malveillants et maintenir un accès persistant, contournant souvent les mesures de sécurité traditionnelles grâce à leur nature légitime. Cela a été observé lors d'une campagne menée en août 2024, où les attaquants ont utilisé l'ingénierie sociale, notamment le phishing et les appels téléphoniques, pour inciter les victimes à installer le logiciel RMM AnyDesk. Les acteurs étatiques et les groupes de ransomware exploitent les outils RMM pour l'accès non autorisé, la persistance, l'exécution de commandes et l'exfiltration de données. Notamment, les attaques de ransomware menées entre juillet et août 2024 impliquaient AnyDesk et modifiaient les paramètres RDP pour déployer des ransomwares et exfiltrer des données.

Les adversaires recourent fréquemment à l'ingénierie sociale, comme les fenêtres pop-up alarmistes, le phishing ou les appels ciblés, pour inciter les victimes à installer un logiciel RMM.

À titre d'exemple, deux campagnes d'août 2024 ont convaincu les victimes d'installer AnyDesk, un RMM légitime :

Accès initial :

- E-mails piégés et appels téléphoniques persuasifs.
- Usurpation d'identité de banques britanniques, utilisant des sites web falsifiés et des méthodes de phishing.

Après l'installation :

- Diffusion de diverses charges utiles, telles que des logiciels malveillants System BC et des tunnels SSH inversés, pour élever les privilèges et exécuter des activités malveillantes sur les systèmes compromis.
- Accès aux comptes bancaires des victimes et exfiltration de données.

Les outils RMM sont fréquemment utilisés par les groupes de ransomware car ils permettent d'établir une persistance et un contrôle à distance, mais ils facilitent également le déploiement de ransomware et l'exfiltration de données. Par exemple, des attaques de ransomware menées entre juillet et août 2024 ont exploité AnyDesk ou modifié les paramètres du protocole de bureau à distance (RDP) :

Accès initial :

• Play a exploité des systèmes exposés sur Internet et des identifiants compromis pour accéder à des systèmes RDP et serveurs Exchange exposés.

• Ransomware INC a utilisé les infections Gootloader pour une campagne ciblant les hôpitaux américains.

• Mad Liberator a ciblé les victimes utilisant déjà AnyDesk, en envoyant des demandes de connexion non sollicitées pour obtenir un accès non autorisé.

• Akira a exploité un serveur de sauvegarde Veeam non corrigé via CVE-2023-27532.

Après l'installation :

• Les outils RMM sont utilisés pour maintenir la persistance, exfiltrer les données et finalement déployer le ransomware.

• Désactivation de la saisie utilisateur.

Protégez votre organisation contre les menaces liées à la surveillance et à la gestion à distance.

La détection des activités malveillantes RMM nécessite une combinaison de mesures techniques et d'analyses, telles que :

• Détection et réponse sur les terminaux (EDR) : déployer des solutions EDR qui surveillent les activités des terminaux et détectent les comportements suspects. Les outils EDR peuvent identifier les outils RMM non autorisés sur la base de leur comportement et de leurs modèles de communication.

• Audits réguliers : effectuer régulièrement des audits de sécurité et des évaluations de vulnérabilités pour identifier et atténuer les risques potentiels. Les audits peuvent aider à découvrir des installations et configurations logicielles non autorisées.

• Liste blanche d'applications : mettre en place une liste blanche d'applications pour s'assurer que seuls les logiciels approuvés peuvent s'exécuter sur votre réseau. Cela peut empêcher l'installation et l'exécution d'outils RMM non autorisés.

02

Compromission initiale

Pendant la phase de compromission initiale, les adversaires tentent de prendre pied dans un réseau. En 2024, Sopra Steria a observé que les cybercriminels s'appuyaient principalement sur trois techniques pour infiltrer les systèmes : le phishing, l'utilisation de comptes valides et l'exploitation de vulnérabilités publiques.

Cette section propose une analyse des tendances du phishing en 2024, ainsi que des vulnérabilités observées la même année.

Phishing

Le phishing est passé du statut de simple nuisance à celui de pierre angulaire de la cybercriminalité moderne, exploitant les vulnérabilités humaines et techniques. Il constitue le principal vecteur d'attaque initiale, la fréquence des attaques et la sophistication des tactiques augmentant chaque année. En 2024, Sopra Steria a observé que 59,9 % de tous les incidents survenus sur les réseaux de ses clients étaient liés au phishing.

L'augmentation des incidents de phishing constatée par Sopra Steria en 2023 s'est poursuivie tout au long de 2024.

Tendances du phishing observées en 2024

Les tendances du phishing en 2024 présentent des similitudes avec les années précédentes mais ont évolué, de nouvelles techniques apparaissant pour s'adapter aux environnements changeants. Cette section fournit une analyse des tactiques de phishing les plus répandues observées par Sopra Steria tout au long de 2024.

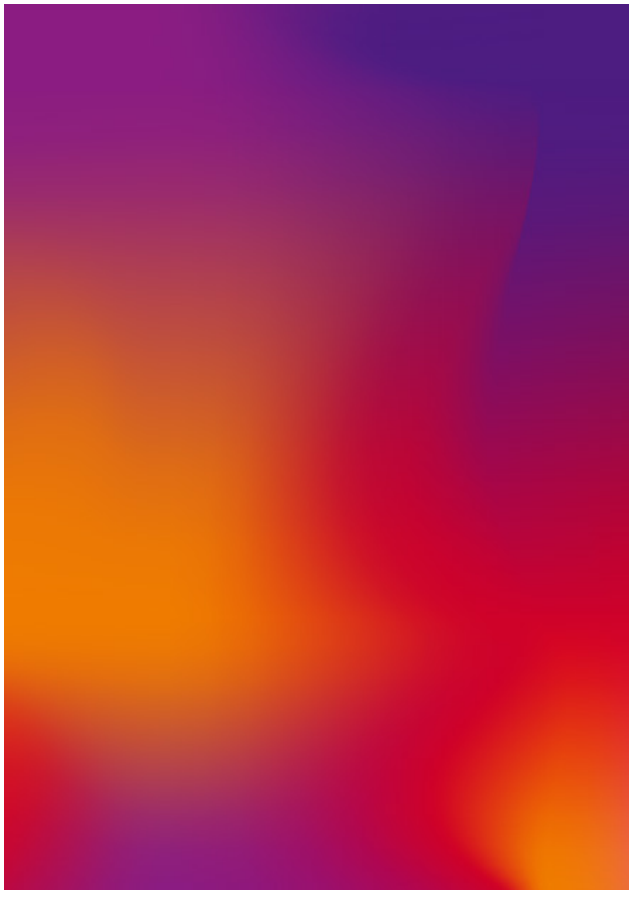
Collecte d'identifiants

L'une des tendances les plus significatives et en constante augmentation est la collecte d'informations d'identification. Au-delà de l'exploitation immédiate, ces identifiants sont souvent vendus ou échangés pour être utilisés dans des attaques ultérieures telles que la prise de contrôle de comptes, la fraude financière et l'usurpation d'identité.

Ainsi, le vol d'identifiants alimente un vaste marché souterrain florissant pour les informations d'identification volées.

Attaques de phishing multicanal

En 2024, les attaques de phishing multicanal ont augmenté, les acteurs de menaces utilisant les SMS, les appels téléphoniques et les applications de messagerie en plus du courrier électronique. Les acteurs se font souvent passer pour du personnel de support informatique afin de tromper les utilisateurs cibles et de les inciter à télécharger des logiciels malveillants ou à accorder un accès. Selon les fournisseurs de télécommunications norvégiens [2] , des filtres anti-usurpation ont été introduits et sont plus efficaces pour bloquer les faux appels. Les acteurs de menaces utilisent donc de plus en plus souvent des numéros danois et suédois pour contourner ces défenses.



[2] https://www.telenor.no/bedrift/aktuelt/sikkerhet/spoofing-filter/

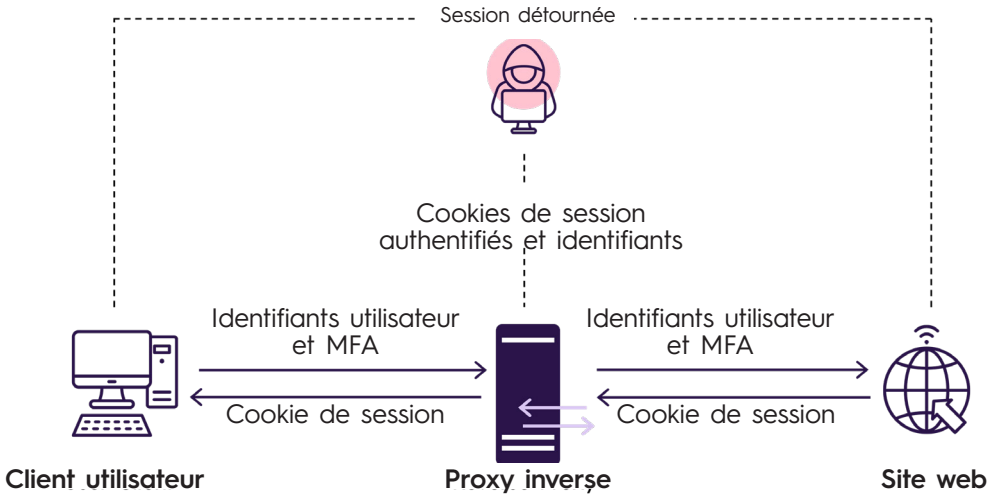
Adversaire au milieu (AiTM)

Sopra Steria a observé une forte prévalence d'attaques AiTM dans sa base de clients tout au long de 2024.

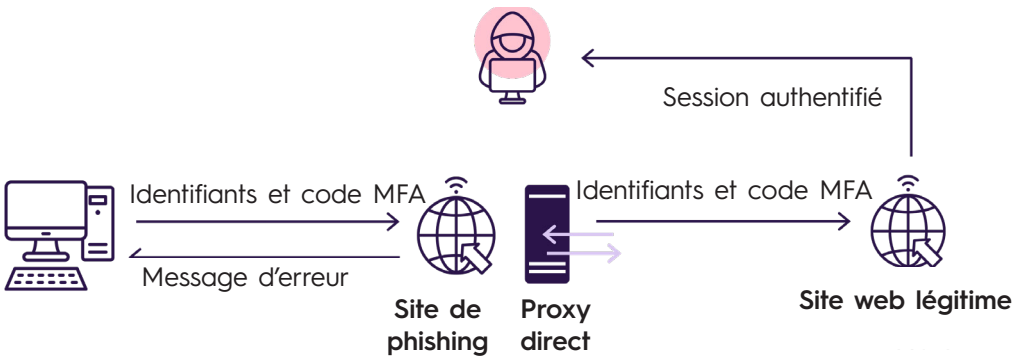
La disponibilité de plateformes PhaaS telles que Tycoon et Evilginx a contribué à la popularité croissante des attaques AiTM, les rendant facilement accessibles aux acteurs de menaces, quelles que soient leurs compétences techniques. Ces attaques utilisent des proxys pour intercepter les communications entre les utilisateurs et les sites web légitimes, capturant les identifiants et les cookies de session pour contourner l'authentification multifactorielle (MFA).

Les techniques observées comprennent les attaques AiTM par proxy inverse, qui ciblent des comptes spécifiques en interceptant le trafic vers des sites légitimes et les attaques AiTM par proxy direct, qui imitent les pages de connexion pour voler les identifiants et les jetons MFA sans passer directement par le proxy.

AiTM par proxy inverse



AiTM par proxy direct



Exemple

Le 18 avril 2024, la police métropolitaine du Royaume-Uni, en collaboration avec les forces de l'ordre internationales et des partenaires du secteur privé, a réussi à démanteler LabHost, un fournisseur de PhaaS. LabHost, également connu sous le nom de LabRat, est apparu fin 2021 et proposait divers services de phishing ciblant des banques et d'autres organisations, principalement au Canada, aux États-Unis et au Royaume-Uni.

Au moment du démantèlement, LabHost comptait plus de 2000 utilisateurs criminels qui avaient déployé plus de 40000 sites frauduleux, affectant des centaines de milliers de victimes dans le monde entier. La plateforme fournissait des outils permettant d'obtenir des codes d'authentification à deux facteurs, des modèles de phishing personnalisables et un composant de phishing par SMS très prisé.

Exemple

Sopra Steria a observé plusieurs incidents impliquant l'utilisation de Tycoon et Evilginx. Après la compromission initiale, ces incidents impliquent souvent l'ajout de dispositifs d'authentification supplémentaires au compte utilisateur pour la persistance, l'interrogation de documents sensibles et l'ajout de règles de boîte de réception dans les messageries.

Le phishing en tant que service

Le PhaaS est devenu une force significative dans le paysage mondial du phishing en offrant des solutions clés en main qui simplifient et rationalisent les opérations de phishing. En 2024, la majorité des courriels de phishing provenait de ces plateformes. En fournissant des kits de phishing prêts à l'emploi, des domaines contrefaits et des services de support complets, le PhaaS abaisse la barrière à l'entrée pour les cybercriminels, permettant des attaques de phishing plus répandues et plus sophistiquées.

Des plateformes comme « Darcula », « Tycoon » et « Caffeine » (aujourd'hui « ONNX ») permettent même à des attaquants peu qualifiés de lancer des campagnes sophistiquées, ciblant souvent des comptes protégés par MFA grâce à des capacités AiTM intégrées. L'adaptabilité des plateformes PhaaS, qui inclut des tactiques telles que l'intégration d'URL de phishing dans des fichiers HTML, PDF ou ZIP pour contourner la détection, a conduit à une augmentation notable de la collecte d'identifiants en 2024. Cette année-là, les principaux fournisseurs de PhaaS ont envoyé des millions d'e-mails de phishing chaque mois, amplifiant considérablement leur impact.

Médias sociaux

L'utilisation des médias sociaux et des faux profils dans les attaques de phishing a considérablement augmenté en 2024. Les acteurs de menaces surveillent des plateformes comme LinkedIn en temps réel, exploitant des mises à jour telles que les changements de postes pour lancer des attaques d'ingénierie sociale peu après que ces modifications aient été apportées. Sopra Steria a observé des cas où cette tactique a été utilisée pour obtenir un accès initial aux systèmes des victimes.

En outre, des acteurs étatiques ont été observés menant des campagnes de phishing dans lesquelles ils se font passer pour des recruteurs ou des demandeurs d'emploi.

À l'aide d'outils d'IA, ils créent des profils et des CV convaincants pour attirer les cibles dans de fausses réunions, les diriger vers des portails chargés de logiciels malveillants ou compromettre les identifiants par le biais de fausses évaluations de compétences. Dans certains cas, les attaquants obtiennent des postes de travail à distance pour abuser de l'accès légitime, voler des données, de la propriété intellectuelle et des fonds.

Dans la boîte de réception

En 2024, Sopra Steria a enregistré un total de 824 millions d'événements de courrier électronique sur l'ensemble de sa base de clients, chaque courrier entrant comportant en moyenne 4,6 URL et 1,7 pièce jointe. Cette prévalence de liens et de fichiers intégrés souligne la difficulté de distinguer les courriels légitimes des menaces potentielles, augmentant le risque d'attaques de phishing. Cette section traite spécifiquement des observations sur les courriels mis en quarantaine, les pièces jointes et les menaces liées aux domaines au sein de la base de clients de Sopra Steria.

Courriels en quarantaine

Une analyse des données clients de Sopra Steria de 2024 a révélé que plus de 29 millions d'e-mails, soit environ 3,6 % de l'ensemble des e-mails, ont été mis en quarantaine ou marqués comme courriers indésirables. Bien que tous les courriels mis en quarantaine ou marqués comme indésirables ne soient pas des tentatives de phishing, ils révèlent souvent des patterns suspects, ce qui les rend précieux pour l'analyse des menaces.

Pièces jointes

L'analyse des données clients de Sopra Steria révèle que les types de fichiers les plus courants dans les dossiers de quarantaine, à l'exception des images et des fichiers texte, sont RAR, HTML, ZIP, PDF et DOCX. Cela correspond aux tendances mondiales des types de fichiers couramment utilisés dans le phishing et d'autres cyberattaques. À l'échelle mondiale, nous avons observé des techniques de phishing intéressantes, notamment des fichiers SVG, des documents OneNote contenant des URL malveillantes et des fichiers RDP en pièces jointes. Ces cas sont relativement rares dans les données de nos clients, probablement en raison de nos mesures proactives de blocage de ces pièces jointes et du fait que ces méthodes sont souvent employées par de petits groupes spécialisés ayant des cibles spécifiques.

Les cinq principaux types de fichiers trouvés dans les dossiers en quarantaine

8,2 % RAR

Les fichiers RAR sont fréquemment exploités dans les campagnes de phishing en raison de leur capacité à regrouper plusieurs composants malveillants. Les fichiers RAR chiffrés ou protégés par mot de passe peuvent contourner les filtres de messagerie, dissimuler leur contenu aux analyses automatiques et transmettre des logiciels malveillants tels que des ransomwares ou des chevaux de Troie.

6,1 % HTML

Les fichiers HTML sont couramment utilisés dans les attaques de phishing en raison de leur polyvalence. Ils contiennent souvent des URL qui mènent à des sites de phishing ou se connectent à des serveurs contrôlés par les attaquants pour déployer du contenu de phishing. Pour échapper à la détection, les fichiers HTML sont souvent intégrés dans des archives ZIP, des documents Microsoft Office ou d'autres types de fichiers. Des techniques telles que la contrebande HTML, où le code malveillant est caché dans le HTML, permettent aux attaquants de contourner les filtres de sécurité et de diffuser des logiciels malveillants ou des schémas de phishing d'identifiants.

6,1 % ZIP

Les fichiers ZIP sont un outil de phishing courant en raison de leur capacité à compresser et dissimuler des charges utiles malveillantes. Les attaquants les utilisent pour regrouper des composants nuisibles et contourner les filtres de sécurité, en particulier lorsqu'ils sont chiffrés ou protégés par mot de passe. Les fichiers RAR sont cependant souvent préférés aux fichiers ZIP car ils peuvent regrouper des structures plus complexes, ce qui les rend plus efficaces dans les campagnes de phishing sophistiquées.

6,0 % PDF

Les fichiers PDF restent un vecteur de phishing populaire, contenant souvent des URL qui mènent à des sites de phishing par le biais de redirections en plusieurs étapes. Il peut s'agir de services légitimes, de défis CAPTCHA ou de liens directs vers des domaines de phishing. Les attaquants cachent souvent les PDF dans des couches d'autres types de fichiers, comme les fichiers ZIP, ou les hébergent sur des plateformes légitimes pour éviter la détection. Cette approche reflète les tactiques de phishing HTML et souligne la capacité d'adaptation des attaquants à utiliser des formats fiables à des fins malveillantes.

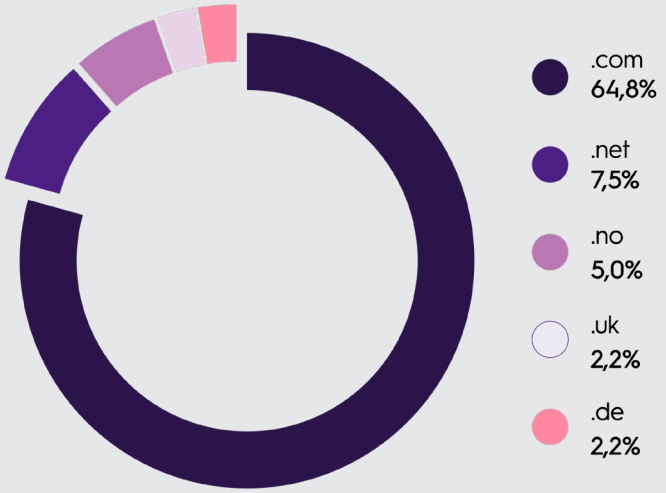
3,4 % DOCX

Les fichiers DOCX, malgré un faible taux de quarantaine, constituent toujours une menace. Bien que les macros soient bloquées par défaut dans les installations modernes d'Office, les attaquants utilisent d'autres méthodes d'exploitation telles que l'injection de modèles. En 2024, une tendance notable consiste à utiliser des fichiers DOCX corrompus dans les campagnes de phishing. Ces fichiers endommagés peuvent contourner les filtres de sécurité et, lorsque les destinataires les ouvrent, la fonction de récupération de Word restaure le document, entraînant une interaction avec le contenu malveillant intégré.

Domaines

Les domaines de premier niveau (TLD) les plus fréquemment identifiés dans les dossiers de quarantaine de la base de clients de Sopra Steria en 2024 sont .com, .net, .no, .uk et .de. Notamment, une partie de tous les TLD dans ces dossiers provient de .ru (Russie) et .cn (Chine). Ces TLD sont rarement associés à des communications électroniques légitimes pour nos clients, ce qui rend leur présence particulièrement suspecte.

Les cinq premiers TLD trouvés dans les courriels mis en quarantaine



Les cinq principaux domaines de premier niveau trouvés dans les courriels mis en quarantaine reflètent un mélange de domaines mondiaux et régionaux de confiance. Bien qu'ils soient attendus dans les réseaux de Sopra Steria, leur utilisation répandue et leur crédibilité en font des cibles de choix pour les abus. Les campagnes de phishing exploitent souvent les TLD populaires tels que .com, .net, et les domaines régionaux spécifiques tels que .no, .uk et .de pour paraître légitimes. Ces domaines sont souvent associés à des services d'hébergement robustes qui résistent aux démantèlements et aux actions en justice, offrant ainsi aux attaquants une infrastructure stable pour leurs activités malveillantes.

Les attaquants intègrent de plus en plus ces TLD à des plateformes cloud comme AWS et Google Cloud pour héberger des pages de phishing, mêlant ainsi le trafic malveillant à l'utilisation légitime. Des services de confiance tels que Dropbox et OneDrive sont également utilisés pour héberger des charges utiles, tandis que des certificats gratuits (par exemple Let's Encrypt) permettent de créer des sites de phishing convaincants, sécurisés par HTTPS.

Les URL de phishing combinent ces éléments avec des tactiques telles que le typosquatting, les chaînes de redirection et les paramètres encodés, masquant leur intention tout en imitant des marques de confiance.

Le Business Email Compromise (BEC) est une forme sophistiquée de cybercriminalité dans laquelle les attaquants utilisent le courrier électronique pour tromper les entreprises et leur faire transférer de l'argent ou des informations sensibles. Ces attaquants se font souvent passer pour des dirigeants ou des partenaires de confiance et utilisent des tactiques telles que de fausses factures ou des demandes urgentes pour manipuler leurs cibles. L'objectif est d'exploiter la confiance et l'autorité associées aux comptes de messagerie usurpés pour mener des activités frauduleuses.

Le Business Email Compromise (BEC) a évolué avec l'intégration d'outils d'IA générative, conduisant à des attaques plus sophistiquées et plus difficiles à détecter. Les mesures de cybersécurité traditionnelles peinent à suivre le rythme, nécessitant des stratégies de défense multicouches.

Les escroqueries BEC peuvent impliquer l'usurpation de comptes de messagerie, le spear phishing et l'utilisation de logiciels malveillants pour infiltrer les réseaux et faire passer des requêtes frauduleuses dans le temps. Les attaquants manipulent souvent les règles de boîte de réception pour dissimuler leurs activités, se déplacent latéralement au sein des organisations, détournent les conversations et altèrent l'authentification multifactorielle pour conserver l'accès. Ils exploitent également des applications légitimes pour exfiltrer des messageries et mènent des attaques discrètes pour échapper à la détection.

En 2024, Sopra Steria a géré plusieurs cas importants de Business Email Compromise (BEC). L'une des tactiques observées consistait à utiliser des comptes compromis au sein d'organisations externes du même secteur. Ces comptes étaient utilisés pour envoyer des courriels de phishing, qui réussissaient à contourner les filtres de messagerie de l'entreprise cible parce qu'ils provenaient de fournisseurs externes connus ou d'organisations partenaires.

Cette stratégie exploite également la confiance inhérente des destinataires cibles. Dans certains incidents observés par Sopra Steria, les attaquants utilisent les comptes compromis pour envoyer d'autres courriels de phishing, propageant ainsi l'attaque au sein de l'organisation. Après l'accès initial aux comptes d'utilisateurs, les attaquants recherchent généralement des documents sensibles tels que des données financières, établissent des règles pour les boîtes de réception et utilisent les comptes compromis pour envoyer des courriels de phishing en interne et à des organisations externes.

— Le Business Email Compromise (BEC) a évolué avec l'intégration d'outils d'IA générative, conduisant à des attaques plus sophistiquées et plus difficiles à détecter.

Vulnérabilités

L'année 2024 a connu des développements significatifs dans le paysage des vulnérabilités de cybersécurité. Diverses sources[3] [4] ont rapporté une augmentation notable du nombre total de vulnérabilités découvertes par rapport à 2023. De plus, le nombre de vulnérabilités exploitées a augmenté d'environ 20 % [5].

Parmi les catégories de vulnérabilités les plus notables figuraient les Cross-Site Scripting (XSS), classées comme la vulnérabilité logicielle la plus critique de 2024 par MITRE et la Cybersecurity and Infrastructure Security Agency (CISA), dépassant 2023 de 10,2 %.

Les vulnérabilités Out-of-Bounds Write et SQL Injection ont également continué à dominer le paysage des menaces. Ces catégories, identifiées dans la liste MITRE 2024 CWE Top 25, ont mis en évidence des faiblesses persistantes dans les systèmes logiciels que les adversaires exploitent fréquemment pour compromettre des données et perturber des services.

[3] https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/

[4] https://www.secpod.com/blog/the-cybersecurity-landscape-of-2024-key-insights-from-the-annual-vulnerability-report/

[5] https://vulncheck.com/blog/2024-exploitation-trends

Nombre d'alertes de vulnérabilités créées par le SOC de Sopra Steria

Janvier
GitLabEE/CE
Cisco Unified Communications
Ivanti
Citrix Netscaler
Jenkins

Février
Ivanti
Fortnet

Mars
Cisco Secure Client

Avril
xz/liblzma
Palo Alto
GlobalProtect
Oracle
Cisco
ArcaneDoor

Mai
Check Point Security Gateway

Juin
MOVEit Gateway/Transfer
GitLab pipeline

Juillet
Cisco Smart software
Oracle
Cisco Email Gateway
OpenSSH
Clonage de dépôts Git
Cisco Nexus Switch
Citrix Netscaler
GitLab

Août
Windows TCP IP
Apache HTTP Server

Septembre
GitLab CEÆE
VMware Vcenter
SolarWinds
GitLab
Cisco Smart Licensing
Veeam
Linux CUPS

Octobre
Firefox
WhatsUp Gold
WatchGuard
GitLab
Junos
Cisco ASA, FMC & FTD

Novembre
Palo Alto
FortiOS SSLVPN
Citrix Virtual Apps & Desktops
Ivanti

Décembre
Apache Struts
Cisco ASA
Application Ivanti Cloud Services
Produits d'accès privilégié à distance (PRA) et de support à distance (RS)
Palo Alto PAN-OS
Framework Apache MINA

Traiter régulièrement les vulnérabilités Windows par le biais des versions Patch Tuesday de Microsoft est bénéfique, car cela raccourcit la durée de vie de ces vulnérabilités. Par conséquent, les entreprises qui planifient leurs mises à jour de systèmes Windows en fonction de ces versions sont moins affectées par les vulnérabilités des produits Microsoft. Cependant, les vulnérabilités dans les plateformes en dehors du calendrier de publication de Microsoft, comme Fortinet, Cisco, Citrix et VMware, sont devenues des cibles attractives pour les entités malveillantes, plusieurs groupes étatiques et criminels de haut niveau utilisant ces exploits pour des attaques de ransomware et des opérations d'espionnage.

Focus sur les réseaux privés virtuels

Les opérateurs de ransomware ont maintenu leur attention sur les solutions VPN tout au long de 2024, à la fois pour l'exploitation et comme point d'accès pour l'utilisation d'identifiants compromis. Les attaques de ransomware se sont orientées vers l'exploitation des vulnérabilités des technologies de périmètre réseau, telles que les VPN et l'infrastructure de bureau virtuel, souvent en raison d'une authentification multifactorielle manquante ou non appliquée. Les solutions VPN qui utilisent Secure Socket Layer/Transport Layer Security (SSL/TLS), souvent connues sous le nom de SSLVPN, WebVPN ou VPN sans client, ont été fortement ciblées.

Ces solutions sont fréquemment ciblées par les acteurs de menaces en raison de leur forte exposition sur Internet, ce qui les rend visibles et accessibles aux attaquants.

Le recours à des pratiques et algorithmes de sécurité obsolètes a encore aggravé la situation, rendant ces solutions vulnérables aux attaques par force brute et à d'autres formes d'attaques. En outre, les implémentations génériques de ces solutions manquent souvent d'authentification robuste, s'appuyant fréquemment sur une authentification à facteur unique qui peut être facilement compromise.

Cela a amené les autorités de sécurité de nombreux pays, dont le NCSC en Norvège, à recommander de remplacer les solutions d'accès à distance utilisant SSL/TLS par des solutions plus sûres.

Exemple

Des vulnérabilités notables, comme celles qui exploitent Windows SmartScreen, ont fait l'objet d'une attention particulière en raison de leur exploitation récurrente par des acteurs de menaces visant à contourner les mesures de sécurité intégrées à Windows Defender. En particulier, la vulnérabilité CVE-2023-36025 a été exploitée par des groupes cybercriminels tels que TA544 pour déployer le cheval de Troie d'accès à distance Remcos dans des attaques sophistiquées visant principalement des institutions européennes.

La vulnérabilité de contournement de la fonction de sécurité Windows SmartScreen (CVE-2024-21351) a été activement exploitée par de nombreux groupes de cybercriminels qui l'ont utilisée pour infiltrer des institutions financières et déployer des logiciels malveillants tels que DarkGate et Phemedrone Stealer.

Exemple

Les produits Connect Secure et Policy Secure d'Ivanti ont fait l'objet d'une attention particulière en raison de la détection de plusieurs vulnérabilités critiques, qui ont été exploitées par divers acteurs de cybermenaces, y compris des groupes sophistiqués parrainés par des États.

« Les attaques de ransomware se sont orientées vers l'exploitation des vulnérabilités des technologies de périmètre réseau, telles que les VPN et l'infrastructure de bureau virtuel, souvent en raison d'une authentification multifactorielle manquante ou non appliquée. »

L'armement des vulnérabilités

Tout au long de l'année, les groupes de ransomware ont continué à se concentrer sur l'exploitation des vulnérabilités système, une tendance observée régulièrement ces dernières années. Un changement notable s'est produit avec la perturbation d'acteurs établis comme LockBit, conduisant à l'émergence de nouvelles souches de ransomware telles que RansomHub, Fog et 3AM. Contrairement à leurs prédécesseurs, ces nouvelles souches exploitent les vulnérabilités au niveau de l'exécution, plutôt qu'au niveau réseau ou applicatif. Cette évolution s'est accompagnée de mesures anti-détection avancées, notamment l'utilisation de mots de passe pour bloquer l'accès aux configurations intégrées, qui protègent leurs charges utiles et compliquent les efforts de rétro-ingénierie. Par conséquent, ces mesures ont considérablement entravé les efforts de détection et d'atténuation.

L'évolution des techniques d'évasion utilisées par les voleurs d'informations, les chevaux de Troie et les chargeurs constitue un domaine important d'exploitation des vulnérabilités. Des logiciels malveillants comme Raspberry Robin ont exploité les vulnérabilités d'émulateur et de sandbox en utilisant des bibliothèques dynamiques virtuelles (VDLL).

En identifiant les vulnérabilités de l'environnement sandbox et en y répondant, ces logiciels malveillants ont échappé à la détection. De même, RedLine a tiré parti de vulnérabilités liées à l'analyse de langages de programmation moins courants, tels que Lua, échappant ainsi aux systèmes traditionnels de détection de logiciels malveillants qui ne sont pas équipés pour analyser ces langages.

Une autre tendance observée au cours de 2024 est l'exploitation de vulnérabilités plus simples et plus accessibles. Les problèmes

liés à l'injection de commandes et à l'authentification incorrecte ont été fréquemment ciblés, reflétant la tendance plus générale des acteurs de menaces à favoriser les exploits à faible complexité et à fort impact.

La vulnérabilité de contournement d'authentification dans l'interface web de gestion PAN-OS de Palo Alto Networks (CVE-2024-0012) en est un exemple. Cette évolution s'est également manifestée par une exploitation accrue des vulnérabilités liées à l'injection de commandes (CWE-77), telles que la vulnérabilité du logiciel Cisco NX-OS (CVE-2024-20399), dont le score CVSS est de 6,7. Cela a conduit à une augmentation des attaques réussies et à un risque plus élevé de violations de données et d'interruptions de systèmes.

Cibler l'interface de programmation d'applications

L'adoption des interfaces de programmation d'applications (API) a explosé, ce qui est essentiel pour les microservices, la prolifération de l'IA et les architectures orientées conteneurs, les rendant attractives pour l'innovation. Cette adoption rapide a également élargi la surface d'attaque pour les acteurs malveillants, comme en témoigne l'augmentation notable de 80 % des violations de données liées aux API au cours de l'année écoulée. Ces violations ont exposé plus de 1,6 milliard d'enregistrements, soulignant l'urgence de renforcer la sécurité des API[6].

Les API sont vulnérables à un large éventail de menaces, souvent aggravées par leur ouverture. Ces risques comprennent les violations de données et les accès non autorisés dus à des mauvaises configurations ou à une validation insuffisante des paramètres. Il devient de plus en plus facile d'exploiter les API, notamment grâce aux progrès des capacités d'appel d'API de l'IA, qui démocratisent l'accès et permettent aux attaquants, quelle que soit leur expertise, de sonder les API de manière approfondie et efficace.

Exemple

Les chargeurs de logiciels malveillants et les ransomwares ont exploité les vulnérabilités des systèmes de défense. Les opérations impliquant GuLoader et Remcos ont exploité des vulnérabilités à partir de vecteurs de courrier électronique de phishing.

GuLoader a utilisé des techniques d'évasion complexes pour manipuler et contourner les défenses système, tandis que Remcos a exploité les vulnérabilités système pour maintenir le contrôle à distance, permettant ainsi le déploiement ultérieur de ransomware.

Exemple

La fuite de 13 millions de secrets d'API du dépôt GitHub montre que les attaquants accordent une grande valeur aux secrets d'API pour les utiliser dans d'autres compromissions. Cela reflète les mêmes tendances observées avec les identifiants d'utilisateurs ordinaires.

[6] https://www.firetail.io/reports/the-state-of-api-security-2024

La cybersécurité OT en 2024

En 2024, nous avons constaté une augmentation significative de l'intérêt pour la cybersécurité OT dans les pays nordiques, sous l'effet d'une multiplication des incidents internationaux et d'un renforcement des exigences réglementaires. Les ransomwares continuent de dominer en tant que menace la plus répandue, ciblant les industries dans tous les secteurs, de l'énergie et de la fabrication aux services publics. Par ailleurs, la fréquence croissante des exploitations zero-day et la découverte antérieure d'outils avancés tels que PipeDream soulignent la vulnérabilité grandissante des systèmes de contrôle industriel (ICS), essentiels à l'infrastructure moderne.

Les développements internationaux, tels que les retombées de l'attaque de la chaîne d'approvisionnement SolarWinds et les décisions de la SEC en matière de responsabilité, ont encore amplifié l'attention portée à la sécurité de la chaîne d'approvisionnement. Les organisations adoptent de plus en plus de mesures telles que les contrôles de nomenclature logicielle (SBOM) et les systèmes d'inventaire pour faire face à ces risques et garantir la conformité.

Les pressions réglementaires se sont également intensifiées. Les mises à jour de la loi norvégienne sur la sécurité numérique, de la directive NIS2, de la loi sur la résilience cybernétique (CRA) et de diverses réglementations sectorielles ont conduit à des exigences de conformité plus strictes. Les opérateurs d'infrastructures critiques sont désormais soumis à une surveillance accrue pour mettre en œuvre des cadres de sécurité robustes tels que la norme IEC 62443, identifier et gérer les risques de cybersécurité pour leur environnement OT et développer une résilience renforcée dans leurs opérations.

Face à ces défis, on observe un mouvement croissant vers des stratégies de cybersécurité proactives. Les organisations adoptent des mesures telles que la segmentation réseau, la détection de menaces en temps réel, des services SOC adaptés aux environnements OT et des programmes complets de formation des employés. L'intégration de ces efforts à la conformité réglementaire permet non seulement de faire face aux menaces immédiates, mais pose également les bases d'une approche plus solide et résiliente de la sécurisation des infrastructures critiques face à un paysage de menaces de plus en plus sophistiqué.

Cela dit, le chemin est encore long pour atteindre une protection et une résilience appropriées des infrastructures critiques, proportionnelles aux conséquences potentielles des incidents. De nombreuses organisations en sont encore aux premières étapes de la mise en œuvre des mesures de sécurité nécessaires et la route à parcourir nécessitera une attention soutenue, des investissements et de l'innovation. Il est encourageant de constater que certains de nos clients établissent une référence mondiale en matière de cybersécurité OT, prouvant ainsi qu'il est possible d'atteindre un niveau de sécurité de classe mondiale. Ces pionniers donnent un aperçu de ce qui est possible, même si le paysage général continue d'évoluer et de s'adapter aux nouvelles menaces.

— Les opérateurs d'infrastructures critiques sont désormais soumis à une surveillance accrue pour mettre en œuvre des cadres de sécurité robustes tels que la norme IEC 62443.

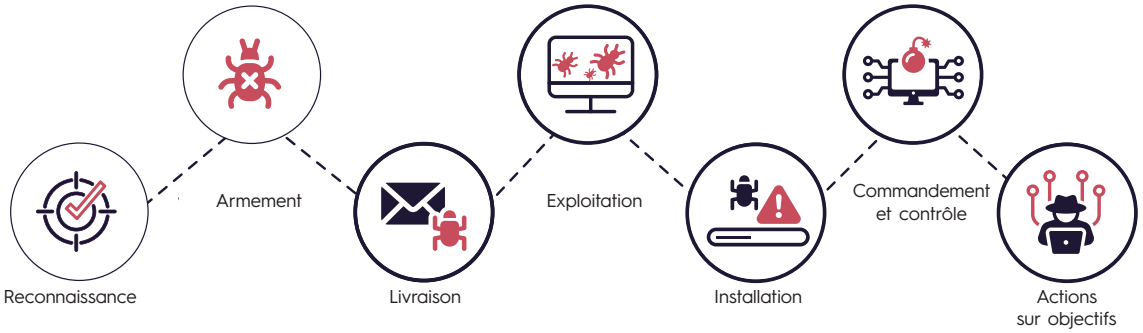
03

Après la Compromission

En 2024, les cybercriminels ont continué à utiliser un large éventail d'outils, de logiciels malveillants et de techniques pour mener à bien leurs attaques, révélant des tendances significatives dans l'évolution des cyber-menaces. On observe une diversification des méthodes et une exploitation accrue des logiciels légitimes à des fins malveillantes. Cette section couvre les tendances 2024 liées aux logiciels malveillants, aux voleurs d'informations et aux outils de piratage. Les observations de Sopra Steria montrent que les logiciels malveillants ont connu une résurgence, notamment par l'utilisation de voleurs d'informations.

D'autres services de sécurité comme l'ENISA (Agence de l'Union européenne pour la cybersécurité) confirment également cette tendance. Les exemples incluent Red-Line, Raccoon Stealer, Vidar, Agent Tesla, FormBook et Lumma Stealer. Lumma Stealer a notamment été largement observé dans la base de clients de Sopra Steria tout au long du second semestre 2024.

« Un autre défi pour les défenses de cybersécurité est l'utilisation accrue des techniques « living off the land », où les acteurs utilisent des outils et des fonctions légitimes de l'infrastructure qu'ils attaquent, détournant cette fonctionnalité pour répondre à leurs besoins malveillants. »



Logiciels malveillants et voleurs

Les logiciels malveillants, y compris les virus, les vers et les chevaux de Troie, sont des logiciels conçus pour endommager un ordinateur, un serveur, un client ou un réseau informatique. Ils peuvent permettre de prendre le contrôle de systèmes (par exemple, les botnets), de voler des données, de permettre un accès à distance (par exemple, les chevaux de Troie d'accès à distance) ou d'installer d'autres logiciels malveillants (par exemple, les téléchargeurs), en fonction de l'objectif de l'acteur de menace.

Les acteurs malveillants créent des logiciels malveillants ou y accèdent pour mener des cybercampagnes, échapper aux défenses et contrôler les actifs. Contrairement aux ransomwares, les logiciels malveillants constituent une menace distincte et persistante, dont les tactiques évoluent pour défier les défenses de cybersécurité.

Un autre défi pour les défenses de cybersécurité est l'utilisation accrue des techniques « Living off the Land », où les acteurs utilisent des outils et des fonctions légitimes de l'infrastructure qu'ils attaquent, détournant cette fonctionnalité pour répondre à leurs besoins malveillants. Bien qu'il ne s'agisse pas de logiciels malveillants, les attaquants peuvent utiliser ces outils à des fins malveillantes, telles que l'exécution de commandes non autorisées, le téléchargement de fichiers malveillants ou le contournement des mesures de sécurité [7].

Dans la cyber kill chain, les logiciels malveillants jouent généralement un rôle crucial aux stades de la livraison, de l'exploitation et de l'installation. Au cours de la phase de livraison, le logiciel malveillant est introduit dans le système cible, souvent par le biais de pièces jointes d'e-mails, de liens malveillants ou d'autres vecteurs. Lors de la phase d'exploitation, il exploite les vulnérabilités pour exécuter sa charge utile sur la cible.

Vient ensuite l'étape de l'installation, au cours de laquelle le logiciel malveillant s'installe sur le système afin d'établir un point d'ancrage pour d'autres activités malveillantes. En fonction de leurs capacités, les logiciels malveillants peuvent également être impliqués dans les étapes suivantes, telles que « commandement et contrôle » et « actions sur objectifs », permettant un contrôle continu et la réalisation des objectifs des acteurs de menaces.

[7] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

À l'intérieur des systèmes

Sopra Steria a détecté et bloqué plusieurs menaces importantes de logiciels malveillants ciblant les clients en 2024.

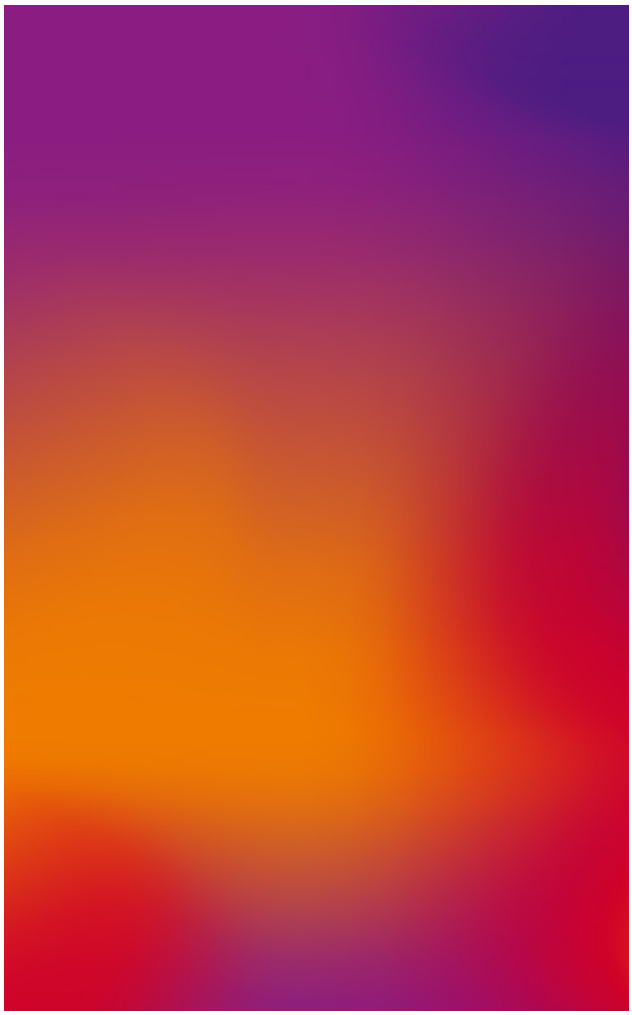
Les logiciels malveillants sont principalement associés à la phase d'installation de la cyber kill chain. Ils sont souvent conçus pour sécuriser un point d'accès initial, faciliter le téléchargement d'outils malveillants supplémentaires ou permettre aux acteurs de menaces d'accéder à d'autres points d'accès en vue d'intrusions ultérieures.

Les cas de logiciels malveillants représentent une part relativement faible de l'ensemble des cas vrais positifs traités par notre SOC. C'est au cours du premier semestre 2024 que cette proportion a été la plus élevée. En moyenne, 10,1 % de tous les cas TP traités par notre SOC étaient liés à des logiciels malveillants en 2024. Cela exclut les instances de logiciels malveillants qui ont été automatiquement bloquées par l'antivirus.

Malware-as-a-Service (MaaS) est un modèle commercial dans lequel les cybercriminels fournissent un accès à des logiciels malveillants et à l'infrastructure associée contre rémunération, tout comme le modèle de service légitime Software-as-a-Service (SaaS). Les MaaS, tels que les voleurs d'informations Vidar et Lumma Stealer, ont été particulièrement exploités par des groupes d'acteurs de menaces motivés par des raisons financières, qui déploient de la même manière d'autres variantes de voleurs d'informations.

Les voleurs d'informations constituent une menace majeure dans le paysage de la cybersécurité, car les acteurs de menaces les utilisent généralement pour récupérer les identifiants de connexion et les informations sensibles des systèmes compromis, ce qui peut conduire à d'autres violations, à des fraudes financières ou à des mouvements latéraux au sein d'une organisation. Les identifiants sont souvent vendus sur des marchés clandestins et jouent un rôle crucial dans les opérations d'accès initial, qui constituent souvent la première étape d'une intrusion en plusieurs phases.

L'augmentation de l'utilisation des voleurs d'informations est en corrélation avec l'accroissement des activités des courtiers d'accès initial (Initial Access Brokers - IAB), l'expansion des réseaux de distribution et la sophistication croissante des techniques d'évasion.



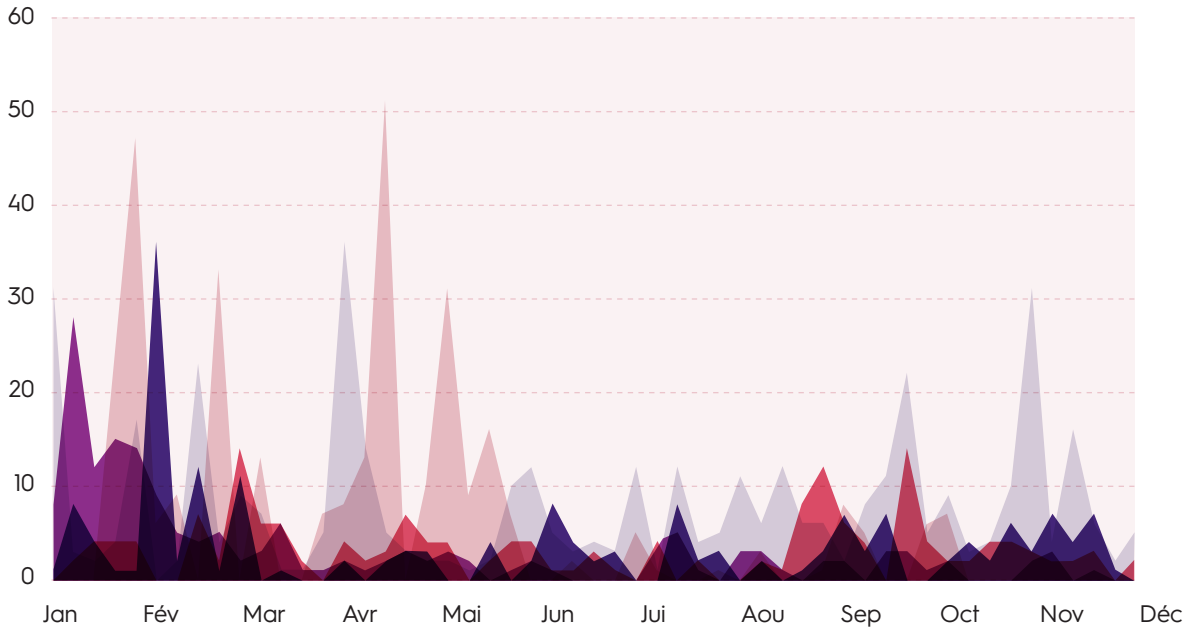
Observés et bloqués

Nous avons observé et bloqué des logiciels malveillants bien connus tout au long de l'année 2024, les types de logiciels malveillants Bearfoos, MediaArena, Phonzy, Plasti et Wacatac (appellation Microsoft) étant les plus importants. Il s'agit des cinq principales familles de logiciels malveillants observées l'année dernière :

Les 5 principales familles de logiciels malveillants

- Plasti
- Wacatac
- MediaArena
- Bearfoos
- Phonzy

Les familles de logiciels malveillants



Les logiciels malveillants les plus observés par Sopra Steria en 2024 sont tous des types de logiciels malveillants qui représentent des menaces importantes pour les systèmes informatiques et qui partagent largement les mêmes fonctionnalités. Ces familles de logiciels malveillants entrent dans la catégorie des « logiciels malveillants génériques » et partagent des méthodes de distribution très similaires.

L'infection se produit généralement par le biais de pièces jointes malveillantes, de sites web infectés, du téléchargement de logiciels piratés ou de l'utilisation de clés USB infectées.

Les logiciels malveillants génériques sont des logiciels malveillants que l'on peut facilement acheter ou télécharger sur le dark web ou d'autres plateformes illicites. Contrairement aux logiciels malveillants conçus sur mesure pour des cibles spécifiques, les logiciels malveillants génériques sont produits en masse et vendus à un large éventail de cybercriminels.

Ce type de logiciels malveillants est souvent utilisé dans le cadre de vastes attaques opportunistes plutôt que de campagnes ciblées.

Wacatac, également connu sous le nom de DeathRansom, a commencé comme un cheval de Troie et s'est transformé en ransomware, chiffrant les fichiers et exigeant une rançon. Il évite d'infecter les systèmes des pays d'Europe de l'Est et est lié au logiciel malveillant Vidar. De même, Bearfoos est un cheval de Troie ciblant Windows, qui exécute des commandes pour voler des données, installer des logiciels malveillants et fournir un accès à distance aux attaquants. Cela met en évidence la sophistication croissante des cybermenaces.

Outre les chevaux de Troie, MediaArena est un pirate de navigateur qui modifie la page d'accueil et le moteur de recherche, injecte des publicités et redirige les recherches. Il peut également ouvrir des onglets avec des publicités, diffuser de fausses mises à jour et promouvoir des escroqueries, compliquant ainsi le paysage des menaces numériques. Phonzy, connu sous le nom de Trojan : Script/Phonzy.A!ml, vole des données, installe des logiciels malveillants et permet aux attaquants de prendre le contrôle à distance. Cela souligne la nécessité de mettre en place des mesures de cybersécurité robustes. De même, Plasti, connu sous le nom de TROJ_PLASTI.A, effectue des actions nuisibles telles que le vol de données, l'installation de logiciels malveillants et la prise de contrôle à distance par les attaquants.

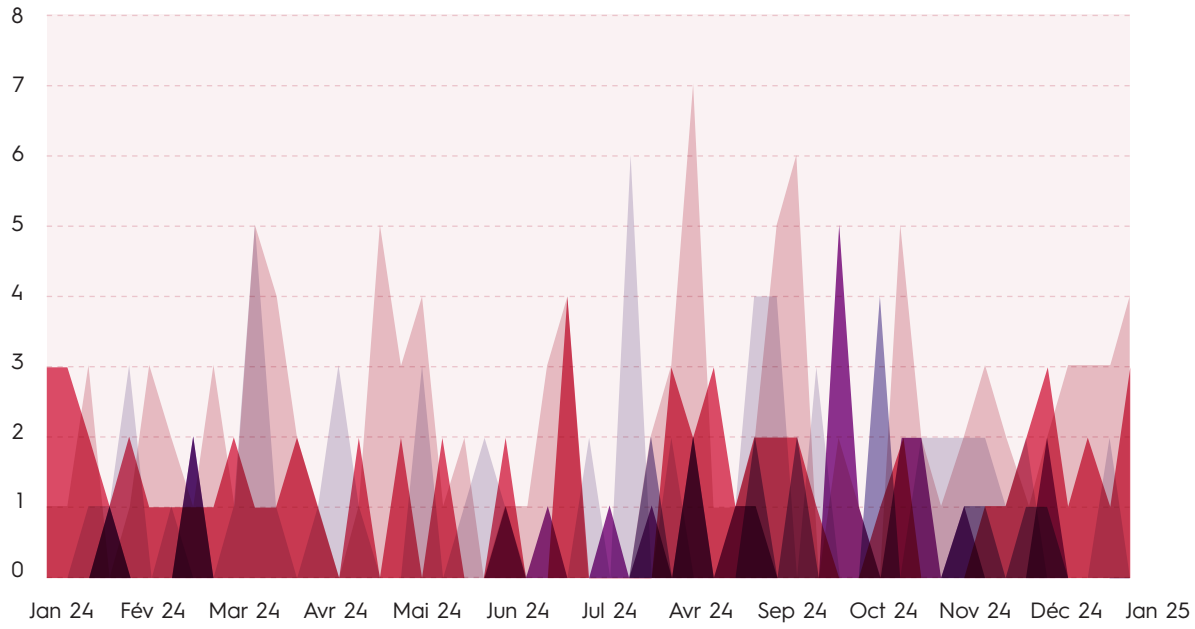
Un autre type de logiciel malveillant que Sopra Steria observe et bloque sont les hacktools, c'est-à-dire des programmes ou utilitaires conçus pour aider les attaquants à pirater. Ces outils sont disponibles dans une grande variété d'applications et sont généralement utilisés pour obtenir un accès non autorisé à un PC afin d'y insérer des vers, virus et chevaux de Troie.

Cette section s'appuie sur la définition des hacktools donnée par Microsoft. Microsoft classe de nombreux logiciels de piratage et de contournement de licence dans la catégorie des hacktools, qui sont plus répandus que les outils de piratage traditionnels tels que Metasploit, Cobalt Strike, Brute Ratel et Bloodhound. Bien que nous rencontrions des cas de ces outils au sein de la clientèle de Sopra Steria, ils ne sont pas aussi courants que les différents types de logiciels de piratage et de contournement de licence.

Top 5 des familles de Hacktools

- AutoKMS
- Crack
- Keygen
- Patcher
- RemoteAdmin

Les familles de Hacktools



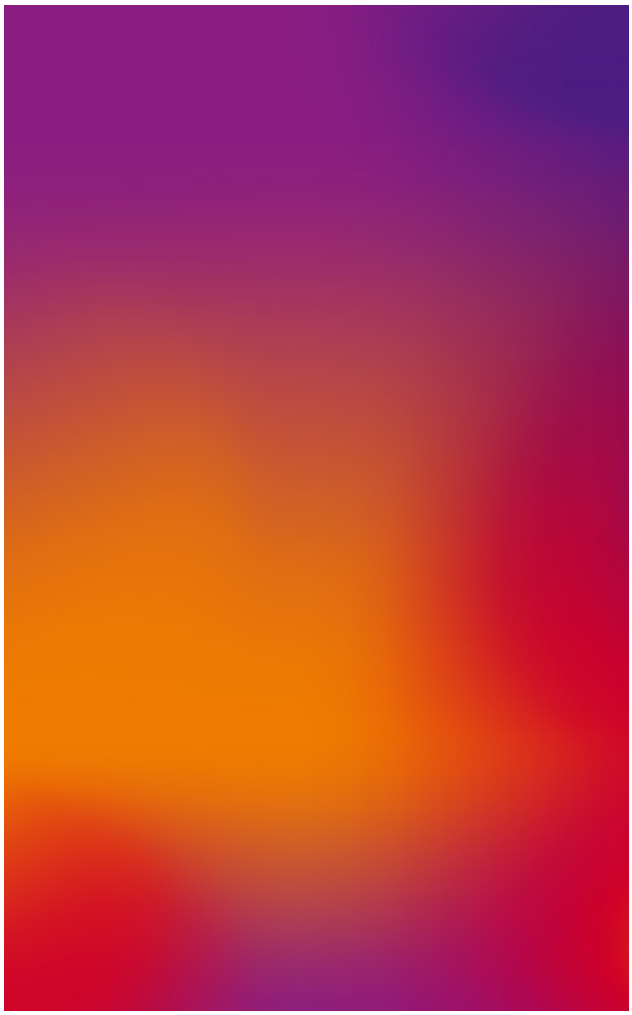
Les plus proéminents observés par Sopra Steria sont les hacktools AutoKMS, Crack, Keygen, Patcher et RemoteAdmin. La plupart de ces outils sont conçus pour contourner les mécanismes de licence logicielle, posant des risques tant pour la sécurité système que pour la légalité.

AutoKMS, Crack et Keygen sont des hacktools utilisés pour activer illégalement des logiciels non enregistrés ou piratés en contournant les mécanismes de licence. Bien qu'ils ne soient pas intrinsèquement malveillants, ils sont souvent fournis avec des logiciels malveillants, créant des vulnérabilités de sécurité. Patcher modifie de manière similaire les logiciels pour contourner les restrictions de licence, posant des risques tels que l'association avec des logiciels malveillants et des vulnérabilités de sécurité. L'utilisation de ces outils viole les accords de licence logicielle et les lois sur le droit d'auteur.

RemoteAdmin, d'autre part, est conçu pour fournir un accès à distance à un ordinateur, permettant à un utilisateur de contrôler le système depuis un emplacement différent. Bien que les outils d'administration à distance puissent être utilisés à des fins légitimes, telles que le support et la gestion informatique, ils peuvent également être exploités par des acteurs malveillants pour obtenir un accès

non autorisé aux systèmes. RemoteAdmin permet aux attaquants de contrôler un ordinateur comme s'ils étaient physiquement présents, incluant l'accès aux fichiers, l'exécution de programmes et la gestion des paramètres système.

— Dans la cyber kill chain, les logiciels malveillants jouent généralement un rôle crucial aux stades de la livraison, de l'exploitation et de l'installation.



Empoisonnement du référentiel

En 2024, le paysage des logiciels malveillants open-source s'est développé à un rythme alarmant, posant des défis à l'intégrité des chaînes d'approvisionnement logiciel. L'année a vu une augmentation de l'identification des paquets malveillants selon les rapports OSINT. Contrairement aux erreurs de codage accidentelles qui entraînent des vulnérabilités, les logiciels malveillants open-source sont délibérément conçus pour infiltrer et exploiter les chaînes d'approvisionnement en se faisant passer pour des composants légitimes.

Au cours de l'année 2024, les téléchargements fantômes sont également devenus une préoccupation majeure. Ces téléchargements se produisent lorsque des paquets malveillants contournent les gestionnaires de dépôts et pénètrent directement dans la machine d'un développeur ou dans l'infrastructure de build partagée.

Ce processus introduit des dépendances non contrôlées dans les projets, sapant les contrôles de sécurité établis et augmentant le risque d'introduction de logiciels malveillants.

Le risque s'en trouve considérablement accru, car les contrôles de sécurité sont souvent contournés, rendant les systèmes vulnérables à des logiciels non validés. Le volume même de ces téléchargements fantômes a explosé, atteignant des milliards par mois, ce qui met en évidence une profonde lacune de gouvernance dans les chaînes d'approvisionnement logiciel.

La nature furtive des logiciels malveillants open-source et leur capacité à s'infiltrer par le biais de dépôts apparemment inoffensifs les rendent particulièrement difficiles à détecter. Les écosystèmes qui hébergent ces dépôts, comme npm, GitHub et PyPI, sont devenus des points névralgiques en raison de leurs faibles barrières à l'entrée et de l'absence de vérifications rigoureuses de l'identité des auteurs.

Cela a permis aux attaquants d'introduire facilement divers composants malveillants, en exploitant les lacunes dans la gestion des dépendances et en construisant des pipelines pour diffuser leur code malveillant.

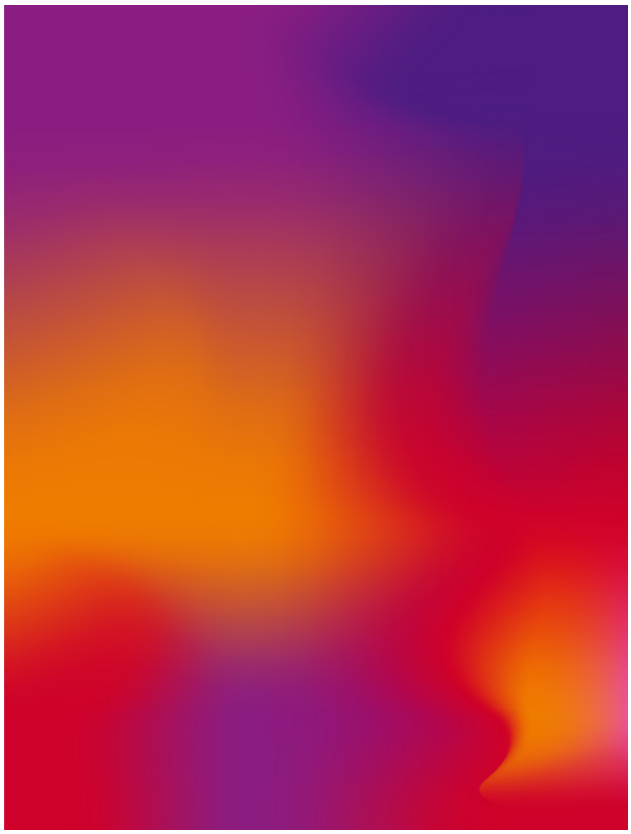
Les organisations doivent mettre en œuvre des mesures de sécurité strictes pour protéger leurs chaînes d'approvisionnement logiciel. Il s'agit notamment de procéder à un examen approfondi de la sécurité des composants open-source, d'utiliser des outils automatisés pour détecter les paquets malveillants et de maintenir un plan de réponse aux incidents robuste pour faire face aux menaces potentielles.

Exemple

Des acteurs étatiques ont été observés utilisant des dépôts de code pour cibler principalement les développeurs afin d'obtenir un accès, comme l'acteur nord-coréen Moonstone Sleet distribuant des logiciels malveillants par le biais de dépôts npm pour exfiltrer des données sensibles des portefeuilles de cryptomonnaies.

Exemple

En mars 2024, une porte dérobée a été découverte dans xz-utils, une suite logicielle qui offre aux développeurs une compression sans perte. Un code malveillant ajouté aux versions 5.6.0 et 5.6.1 de xz-utils a modifié le fonctionnement du logiciel. La porte dérobée manipule sshd, le fichier exécutable utilisé pour établir des connexions SSH à distance. Toute personne en possession d'une clé de chiffrement prédéterminée pouvait dissimuler le code de son choix dans un certificat de connexion SSH, le télécharger et l'exécuter sur l'appareil compromis. L'incident de la porte dérobée XZ Utils a suscité des discussions approfondies au sein de la communauté de sécurité. L'une des principales préoccupations était de savoir comment le développeur de la porte dérobée avait pu passer inaperçu pendant si longtemps, ce qui mettait en évidence les faiblesses potentielles des processus de sécurité actuels.



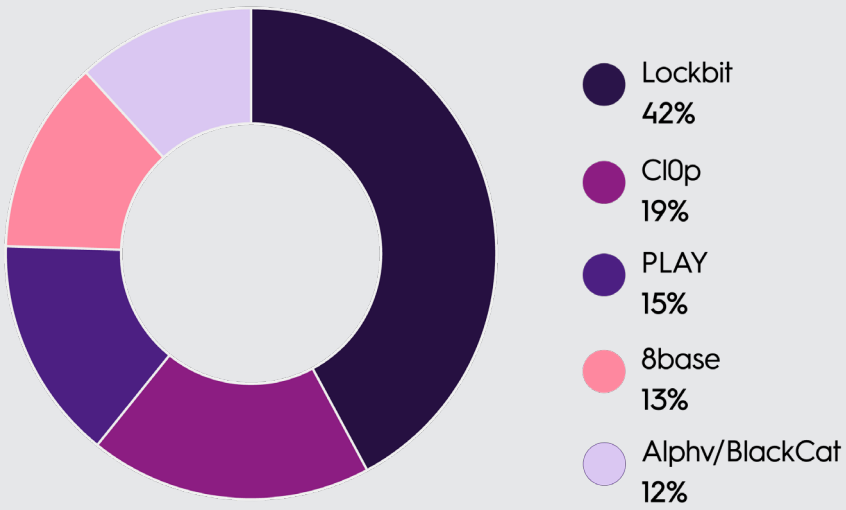
L'écosystème des ransomwares

Le modèle RaaS a continué à se développer en 2024, permettant aux cybercriminels de déléguer les opérations d'extorsion aux opérateurs de ransomwares en échange d'une part des bénéfices ou d'un paiement. Cette approche a démocratisé les attaques de ransomware en fournissant des outils prêts à l'emploi à des affiliés inexpérimentés.

Les opérateurs RaaS développent et maintiennent l'infrastructure tandis que les affiliés mènent les attaques. Ce modèle complique l'attribution des attaques et permet une résilience accrue : l'arrestation des affiliés n'affecte pas les opérateurs et les affiliés peuvent changer de kit si nécessaire.

Les groupes d'acteurs de menaces qui exploitent ce modèle comprennent Lockbit, DarkSide, REvil, Dharma et Akira. Les attaquants utilisent une combinaison d'outils natifs et téléchargés pour atteindre leurs objectifs, et se concentrent sur le vol et l'exfiltration de données. L'affilié d'un groupe de ransomware, Cactus, a été observé utilisant un outil qui exfiltre automatiquement des fichiers vers le cloud lors d'une compromission, qui a ensuite été affiché sur son site de fuite. wlls ont ensuite menacé de divulguer d'autres informations pour faire pression sur leur victime.

Les cinq groupes de ransomware les plus actifs en 2024



Source : ENISA

04

Paysage des menaces

En 2024, les objectifs des acteurs de cybermenaces, qu'il s'agisse de cybercriminels ou de groupes parrainés par des États, évoluent rapidement et leurs tactiques, techniques et procédures (TTP) connaissent des changements notables, comme nous l'avons vu précédemment dans ce rapport.

L'évolution du paysage des menaces pose des défis considérables, car les cybercriminels deviennent plus sophistiqués et plus efficaces, en grande partie en raison de la réduction des barrières à l'entrée. Leur principal objectif est d'accéder sans autorisation à des informations et systèmes sensibles, souvent à des fins financières, et ils utilisent diverses techniques d'attaque avancées pour y parvenir.

Avec la transformation numérique en cours, les cybercriminels se sont adaptés en ciblant de plus en plus les infrastructures réseau, les services de stockage cloud et les plateformes SaaS (Software as a Service). Ils exploitent diverses vulnérabilités, notamment une gestion inadéquate des correctifs, des configurations erronées, des API non sécurisées et des logiciels obsolètes. Les logiciels malveillants conçus pour infiltrer et exploiter les chaînes d'approvisionnement en se faisant passer pour des composants légitimes sont de plus en plus nombreux.

En outre, la scène de l'hacktivisme est fortement influencée par les conflits géopolitiques, en particulier ceux liés à Gaza, à Israël et à l'Iran, ainsi qu'à l'Ukraine. Les acteurs parrainés par des États jouent un rôle clé dans le paysage des menaces, en utilisant des ressources considérables pour l'espionnage et le vol de propriété intellectuelle.

Ils se livrent à une reconnaissance approfondie pour se préparer à perturber les infrastructures critiques, ce qui souligne la complexité et la gravité de ces menaces. Des acteurs notables comme le groupe Volt Typhoon, soutenu par l'État chinois, ont infiltré des réseaux informatiques aux États-Unis, avec l'intention potentielle de perturber des infrastructures essentielles. De même, Salt Typhoon a pénétré dans des entreprises de télécommunications de plusieurs pays. L'objectif était probablement d'obtenir un accès à grande échelle aux données relatives au trafic téléphonique sous la forme d'enregistrements détaillés des appels et, éventuellement, au contenu du trafic d'un ensemble plus large d'appels téléphoniques. Ces deux types d'informations peuvent, pour l'attaquant, avoir une grande valeur en vue d'une exploitation ultérieure.

Leurs méthodes non conventionnelles soulignent l'aggravation des menaces et mettent en évidence des environnements compromis dans des secteurs clés tels que les télécommunications et l'énergie.

Volatilité des groupes de ransomware

En 2024, plusieurs groupes de ransomware ont été à la fois créés et dissous. Ce n'est peut-être pas spécifique à l'année 2024, mais nous avons observé des changements significatifs provoqués par des actions judiciaires impliquant plusieurs pays, comme l'opération menée en février contre le groupe LockBit, grâce à une vulnérabilité PHP non corrigée sur leur site. Bien que cette opération n'ait pas éliminé LockBit, elle a considérablement réduit son niveau de menace. À l'issue de l'opération, des clés de déchiffrement ont été récupérées et fournies aux victimes, ce qui montre à quel point les efforts et la coordination au niveau international peuvent faire la différence.

Toutefois, la disparition d'un groupe de ransomware n'implique pas nécessairement une diminution de l'activité globale des ransomwares. En effet, les groupes peuvent changer de nom au fil du temps, mais la plupart des acteurs impliqués restent souvent les mêmes. Par exemple, l'opération RansomHub, active depuis le début de 2024, a attiré un afflux d'affiliés qui ont abandonné les opérations LockBit (et BlackCat).

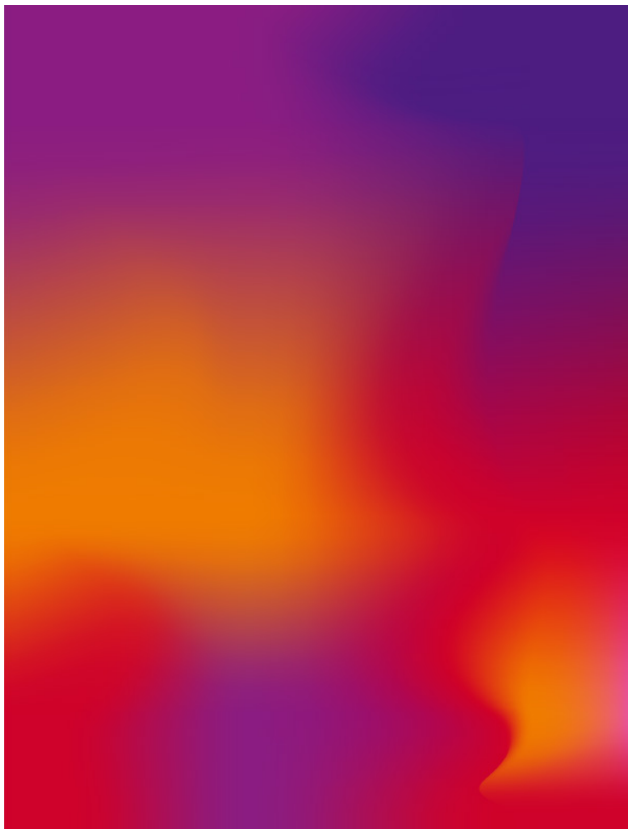
Principales observations

« La prolifération des voleurs d'informations a entraîné une augmentation des fuites de données, souvent facilitées par l'utilisation d'identifiants volés. »

Les cybercriminels utilisent fréquemment des infrastructures malveillantes et des services cloud publics pour héberger des logiciels malveillants et exfiltrer des données. Entretemps, les ransomwares et les campagnes destructrices restent dominants, les opérateurs utilisant des modèles de Ransomware-as-a-Service (RaaS) pour étendre leurs capacités d'attaque et cibler un plus grand nombre de victimes. Ces acteurs ne se contentent pas de chiffrer et de voler des données, ils utilisent également la menace d'une exposition publique pour extorquer des paiements, en exploitant souvent le stockage cloud pour les transferts de données. En outre, des groupes de ransomwares sophistiqués sont de plus en plus utilisés par des acteurs étatiques pour obtenir des informations sur les données, les infrastructures critiques ou d'autres informations précieuses d'autres pays.

Les observations montrent que les méthodes d'exfiltration visant à contourner les mesures de sécurité sont de plus en plus sophistiquées. En réponse à l'industrie de la cybersécurité qui développe des méthodes de détection spécifiquement pour se défendre contre la menace latente posée par les voleurs d'informations, les cybercriminels tentent d'échapper à la détection en innovant avec des outils d'archivage ou d'autres protocoles d'exfiltration. On observe également une augmentation de l'utilisation des techniques d'exfiltration, telles que l'exfiltration vers le stockage cloud et l'utilisation de canaux chiffrés. Cela reflète l'adaptation des attaquants à l'utilisation croissante de solutions cloud pour l'exfiltration de données, tout en sécurisant leurs communications.

En outre, cette méthode d'exfiltration basée sur le cloud vise à « se fondre dans le bruit » du trafic de données, étant donné que de nombreuses entreprises stockent leurs données dans des clouds tiers. Des outils tels que Cobalt Strike, Mimikatz, PsExec, RClone et PowerShell restent très utilisés par les attaquants, ce qui souligne à la fois leur efficacité et leur polyvalence dans les attaques, qu'il s'agisse de mouvements latéraux, d'exfiltration ou de collecte de données sensibles. Cela souligne le besoin critique de règles de détection spécifiques pour identifier à la fois les outils de piratage largement répandus et l'utilisation malveillante d'outils légitimes.



L'intelligence artificielle

En 2024, nous avons constaté des progrès remarquables dans l'IA, en particulier dans le domaine de l'IA générative, avec de nouveaux modèles plus puissants mis à disposition presque chaque semaine, montrant des améliorations significatives en termes de qualité, de précision et de quantité d'informations qu'ils peuvent traiter. De nombreux modèles ont également introduit la multimodalité complète, les entrées et sorties n'étant plus limitées au texte mais également aux images/audio/vidéo, ce qui donne aux modèles la capacité de voir et d'écouter. Bien que le marché soit encore largement dominé par OpenAI, Microsoft, Google, Meta et Amazon, on assiste également à une montée en puissance des modèles open-source et des modèles tiers de plus petites entreprises qui rivalisent également avec les plus grands modèles. De nouvelles capacités ont également été mises à disposition pour nous permettre d'exécuter les modèles sur notre propre matériel local, ce qui nous donne la possibilité d'exécuter le traitement de l'image, de la vidéo, de l'audio et du texte dans notre propre infrastructure ou en périphérie.

Cette année, de nombreuses organisations ont commencé à utiliser l'IA générative pour le développement d'applications (GitHub Copilot) et la collaboration (Microsoft 365 Copilot); d'autres en sont aux premières phases d'évaluation de l'utilisation de la GenAI pour l'automatisation des activités. Un risque auquel de nombreuses entreprises ont été confrontées cette année est la Shadow GenAI, où les employés ont commencé à utiliser l'un des nombreux milliers d'outils et de services GenAI sur le marché avec les données de l'entreprise, sans savoir comment les différents services traitent les données.

Ce manque de visibilité et de contrôle crée des vulnérabilités potentielles en matière de sécurité, des problèmes de conformité et la possibilité de fuites de données sensibles.

On constate également une augmentation du nombre de cybercriminels et même d'acteurs de menaces étatiques qui utilisent l'IA générative à des fins malveillantes pour :

- Générer des contenus «deepfake» dans le but de mener des attaques d'ingénierie sociale ou de manipuler l'opinion publique au moyen de fausses informations, en particulier en relation avec des questions politiques ou des conflits internationaux en cours.

- De nouvelles méthodes d'ingénierie sociale utilisant l'IA générative pour reproduire la voix ou le visage d'une personne. Grâce aux améliorations apportées aux modèles et au matériel, il est désormais possible de générer de fausses vidéos en temps réel, même lors d'appels Microsoft Teams.

- Générer de nouveaux codes malveillants tels que de nouveaux logiciels malveillants, virus ou chevaux de Troie. Bien que la qualité des logiciels malveillants générés par GenAI soit actuellement assez faible, nous pensons qu'avec toutes les améliorations apportées aux modèles, ce risque deviendra plus important dans les années à venir.

« Un risque auquel de nombreuses entreprises ont été confrontées cette année est la Shadow GenAI, où les employés ont commencé à utiliser l'un des nombreux milliers d'outils et de services GenAI sur le marché avec les données de l'entreprise, sans savoir comment les différents services traitent les données. »

Heureusement, de nombreux fournisseurs d'IA ont ajouté des mesures de protection supplémentaires à leurs modèles pour interdire ce type d'abus et nous constatons aujourd'hui que les cybercriminels trouvent de nouvelles méthodes pour contourner ces protections à l'aide d'une technique appelée « prompt injection ».

Une autre tendance qui a émergé est l'utilisation d'agents virtuels, où l'on peut combiner l'IA générative avec un agent virtuel qui présente un ensemble d'intégrations prédéfinies et un ensemble d'instructions. Ces agents peuvent assumer diverses tâches, comme la collecte d'informations ou la reconnaissance à l'aide d'outils tels que AutoGPT, Autogen ou MetaGPT.

Ils peuvent également effectuer des tests de sécurité automatisés à l'aide de frameworks tels que PentestGPT. Ces frameworks d'agents deviennent aujourd'hui si puissants qu'ils peuvent être utilisés pour mener des attaques automatisées et même interagir localement avec des ordinateurs à l'aide de fonctions telles que les API Anthropic Computer Use ou fonctionner dans un environnement virtualisé.

Même si nous ne pensons pas que les cyberattaques par IA deviendront la norme de sitôt, nous remarquons que les cybercriminels utilisent la GenAI pour les assister. L'IA devrait contribuer au développement de logiciels malveillants et d'exploits, à la recherche de vulnérabilités et aux mouvements latéraux en rendant les techniques existantes plus efficaces. Toutefois, à court terme, ces domaines continueront à dépendre de l'expertise humaine.

L'IA permettra également aux cybercriminels novices et aux hacktivistes de mener des opérations d'accès et de collecte d'informations plus facilement.

L'IA générative deviendra un sujet encore plus important dans les années à venir, de plus en plus d'entreprises cherchant à tirer parti de la technologie dans de multiples domaines au sein de l'entreprise.

05

Recommandation pour les défenseurs

Les organisations devraient adopter une approche globale de la sécurité, en intégrant la résilience dans leurs opérations de base afin de mieux gérer l'évolution rapide du paysage numérique. Il est important d'adopter des tests basés sur les menaces et d'améliorer la réponse aux incidents. Les efforts de sécurité doivent être dynamiques et s'adapter à l'évolution du paysage des menaces.

De nombreuses tendances de la cybercriminalité rapportées au niveau mondial en 2024 reflètent les observations et les incidents de Sopra Steria. Le phishing, avec ses nouvelles méthodes, constitue la plus grande catégorie d'incidents de sécurité traités par notre Security Operations Center en 2024. La couverture des outils EDR est cruciale pour détecter et répondre aux activités malveillantes. Nous recommandons à toutes les organisations d'adhérer aux principes fondamentaux du NSM en matière de sécurité des TIC. Les organisations qui ont atteint un niveau élevé de maturité en matière de sécurité, ce qui inclut une bonne politique de correctifs, un inventaire des actifs et un contrôle des points d'accès exposés, protègent plus facilement leur infrastructure et réduisent le nombre d'incidents de sécurité.

Phishing

La défense contre le phishing nécessite une approche multicouche pour se protéger efficacement contre ces attaques trompeuses.

L'authentification multifactorielle (MFA) pour tous les comptes d'utilisateurs est une nécessité. Avec l'augmentation du phishing AiTM, il convient d'opter pour une MFA résistante au phishing.

Formez régulièrement les employés à reconnaître et à signaler les tentatives de phishing, car la vigilance humaine est une ligne de défense cruciale. Utilisez des outils et des services anti-phishing avancés qui peuvent surveiller, bloquer et filtrer les tentatives de phishing en temps réel, réduisant ainsi les risques que des courriels malveillants n'atteignent les boîtes de réception.

• Activez l'authentification multifactorielle forte (MFA) : mettez en œuvre l'authentification multifactorielle pour tous les comptes d'utilisateurs afin de les protéger contre les techniques avancées de phishing. L'idéal est d'utiliser un système d'authentification multifactorielle résistant au phishing.

• Sensibilisation des utilisateurs : sensibilisez régulièrement les employés à l'identification et au signalement des tentatives de phishing.

• Outils et services anti-phishing : utilisez des outils qui surveillent, bloquent et filtrent les tentatives de phishing en temps réel.

Méthodes d'authentification

Méthode	Protection AiTM
Connexion sans mot de passe par téléphone	X
Numéro de téléphone + SMS	X
Nom d'utilisateur et mot de passe	X
Application Microsoft Authenticator + Correspondance de numéros	X
FiDO2	V
Authentification basée sur certificat	V
Accès conditionnel (Appareil conforme)	V
Accès conditionnel Emplacements de confiance	V
Exiger que l'appareil soit marqué comme appareil joint Azure AD hybride	V

Vulnérabilités

Les organisations devraient donner la priorité à la sécurisation de leurs API en mettant en œuvre des mécanismes d'authentification et d'autorisation robustes, des tests de sécurité réguliers et une surveillance continue, tout en assurant une configuration et une validation correctes pour atténuer les risques associés.

De plus, la mise à niveau des solutions VPN vers des solutions plus sûres et l'application d'une authentification multifactorielle sont essentielles pour contrôler et sécuriser tous les points d'accès exposés, en veillant à ce que seul l'accès autorisé soit possible. La mise à jour régulière et l'application de correctifs aux logiciels VPN, associées à des mécanismes d'authentification forts, peuvent réduire les risques de manière significative. En outre, les organisations doivent donner la priorité à l'application régulière de correctifs et de mises à jour dans tous les aspects de leur infrastructure, y compris les dispositifs réseau, les systèmes de virtualisation et les applications autonomes. Compte tenu de la diminution du délai d'exploitation [8], les adversaires étant désormais capables d'exploiter les vulnérabilités dans un délai moyen de cinq jours seulement, il est plus que jamais essentiel d'appliquer les correctifs en temps voulu.

• Correctifs et mises à jour réguliers : donnez la priorité à l'application régulière de correctifs et de mises à jour afin d'atténuer les risques liés aux vulnérabilités.

• Sécurisez les API et les technologies de streaming : mettez en œuvre des mécanismes d'authentification et d'autorisation robustes, des tests de sécurité réguliers et une surveillance continue.

Logiciels malveillants

La défense contre les logiciels malveillants nécessite une combinaison de mesures préventives et de surveillance. Veillez à ce qu'un logiciel antivirus soit installé sur tous les appareils et maintenu à jour pour détecter et supprimer les logiciels malveillants. Mettez en place des outils de surveillance réseau pour détecter toute activité inhabituelle susceptible d'indiquer la présence de logiciels malveillants.

Sensibilisez les employés aux risques liés au téléchargement et à l'ouverture de fichiers suspects ou au fait de cliquer sur des liens inconnus, car il s'agit de méthodes courantes de diffusion de logiciels malveillants. En outre, utilisez des solutions de détection et de réponse sur les terminaux (EDR) pour surveiller les activités des terminaux et réagir rapidement aux menaces potentielles.

• Informations sur les appareils et renseignements sur les menaces en temps réel : surveillez le trafic réseau à l'aide d'analyses avancées et restez informé des menaces émergentes.

• Installez et mettez à jour un logiciel antivirus : veillez à ce qu'un logiciel antivirus soit installé et régulièrement mis à jour.

• Renforcez la détection de l'exfiltration de données : mettez en œuvre des règles de détection spécifiques pour les outils de piratage largement répandus et l'utilisation malveillante d'outils légitimes.

[8] https://socradar.io/top-10-exploited-vulnerabilities-of-2024/

Le point de vue du Pentester

Au cours de l'année écoulée, l'équipe chargée des tests de pénétration a identifié plusieurs vulnérabilités et faiblesses récurrentes chez les clients. Nombre d'entre elles reflètent des problèmes fondamentaux qui ont persisté au fil des ans et restent plus que jamais d'actualité.

Ces vulnérabilités continuent d'offrir aux attaquants la possibilité d'élever leurs privilèges et d'avoir un impact significatif, ce qui souligne l'importance de les traiter efficacement.

Principales conclusions des tests de pénétration :

Mauvaise hygiène des mots de passe : une mauvaise hygiène des mots de passe reste une faille que nous exploitons fréquemment pour obtenir un accès au domaine. Grâce à des attaques par pulvérisation de mots de passe utilisant des mots de passe simples et prévisibles, nous obtenons souvent un accès non autorisé aux comptes d'utilisateur, de service et d'administration.

Modèles de certificats vulnérables : les modèles de certificats mal configurés sont un problème récurrent, permettant une escalade de privilèges. Dans certains cas, des utilisateurs ordinaires du domaine ont pu obtenir des droits d'administrateur de domaine en raison de paramètres inappropriés dans les modèles de certificat.

Fichiers sensibles dans les partages de fichiers : nous découvrons souvent des fichiers de configuration contenant des chaînes de connexion et des jetons en clair, ainsi que des mots de passe et d'autres données sensibles dans des partages de fichiers. Cela offre aux attaquants des possibilités directes d'escalade horizontale et d'exposition d'informations critiques. L'absence de contrôles d'accès et de journalisation appropriés ne fait qu'exacerber ce problème.

Mauvaises configurations : les erreurs de configuration restent un problème courant, dont voici quelques exemples :

- Des configurations faibles dans les plateformes cloud, entraînant un accès involontaire à des données ou ressources sensibles.
- Une segmentation réseau mal mise en œuvre, ce qui facilite les mouvements latéraux des attaquants au sein d'un environnement.

Problèmes d'autorisation et de scripts inter-sites dans les applications web : nous rencontrons fréquemment des implémentations d'autorisation manquantes ou faibles dans les API et les applications web. Ces vulnérabilités ont entraîné un accès non autorisé à des données et systèmes sensibles, ainsi que la possibilité d'effectuer des actions non autorisées. Dans certains cas, cela nous a permis d'escalader les privilèges verticalement (obtention d'autorisations de niveau supérieur) ou horizontalement (accès aux données d'autres utilisateurs).

En outre, nous identifions souvent des vulnérabilités de type cross-site scripting (XSS) dans les applications web. Ces failles nous permettent d'injecter des scripts malveillants, ce qui peut compromettre les sessions des utilisateurs, défigurer les sites web ou conduire au vol de données sensibles.

— Une mauvaise hygiène des mots de passe reste une faille que nous exploitons fréquemment pour obtenir un accès au domaine.

Recommandations pour améliorer la sécurité

Renforcez les pratiques en matière de mots de passe :

Appliquez des politiques robustes en matière de mots de passe et rendez obligatoire la MFA pour tous les systèmes critiques. Empêchez l'utilisation de mots de passe simples et couramment utilisés.

Examinez les autorisations d'accès :

Vérifiez régulièrement les zones de fichiers partagés et assurez-vous que les informations sensibles ne sont pas stockées sans protection adéquate.

Renforcez les configurations :

Examinez et mettez à jour les configurations, y compris les modèles de certificats, afin de les aligner sur les meilleures pratiques.

Testez les mécanismes d'autorisation :

Testez régulièrement les applications web afin de vous assurer que les autorisations sont correctement mises en œuvre et qu'aucune donnée sensible n'est accessible sans autorisation appropriée.

Perspectives 2025

En 2025, il est fort probable que l'utilisation de l'IA dans les cyberattaques devienne encore plus sophistiquée et répandue.

Les cybercriminels exploiteront de plus en plus l'IA pour créer des courriels de phishing et des attaques d'ingénierie sociale très convaincants, imitant le comportement humain et les modèles de langage avec une plus grande précision, ce qui les rendra plus difficiles à détecter. La technologie Deepfake sera également utilisée par de nombreux acteurs de menaces pour créer des vidéos et des enregistrements audio réalistes à des fins d'usurpation d'identité, de fraude et de contournement des mesures de sécurité, ce qui permettra aux attaquants de se faire passer pour des personnes et d'obtenir un accès non autorisé à des informations sensibles.

De plus, dans le cadre des opérations d'information, l'IA sera exploitée pour amplifier la création de contenu et produire des personnages fictifs plus convaincants et plus réalistes.. Cela renforcera la capacité des acteurs de menaces à influencer l'opinion publique et à mener des campagnes de désinformation. Dans l'ensemble, l'intégration de l'IA dans les cyberattaques les rendra plus évolutives, plus sophistiquées et plus difficiles à combattre. Les organisations devront investir dans des mesures de sécurité avancées et dans une surveillance continue pour garder une longueur d'avance sur ces menaces en constante évolution.

Parallèlement, la valeur accordée aux identifiants volés par les acteurs de menaces restera élevée, sous l'effet de plusieurs tendances clés observées en 2024. Tout au long de l'année 2024, on a constaté une augmentation significative de l'utilisation d'identifiants légitimes pour l'accès initial dans les cyberattaques. Le marché des identifiants compromis, souvent acquis par le biais de logiciels malveillants voleurs d'informations, a continué de prospérer. Les attaquants ont compris que même un simple identifiant d'employé, qui peut être obtenu pour seulement 10 dollars, peut conduire à des compromissions très médiatisées. Il est fort probable que cette tendance se poursuive en 2025, car la demande pour ce type d'identifiants reste forte en raison de leur efficacité pour obtenir un accès non autorisé aux systèmes. Les organisations devront donner la priorité à la sécurité des identifiants, y compris à des méthodes d'authentification robustes et à une surveillance continue, afin d'atténuer les risques associés au vol d'identifiants.

Les groupes de cybercriminels continuant à se spécialiser, cette tendance devrait persister, voire s'intensifier en 2025, afin de répondre à l'évolution des exigences du marché de la cybercriminalité. Nous verrons probablement des groupes se consacrer exclusivement à un domaine étroitement spécialisé, comme l'exfiltration ou l'exploitation d'infrastructures cloud. En outre, les collaborations entre ces groupes pourraient devenir plus fréquentes, avec des alliances temporaires formées pour des campagnes spécifiques ou le partage de ressources, telles que les vulnérabilités et les infrastructures.

Les groupes de menaces persistantes avancées (APT) alignés sur les États collaborent de plus en plus avec les cybercriminels, en particulier dans l'utilisation de ransomwares, de courtiers d'accès initial et d'attaques destructrices. Cette collaboration brouille la frontière entre la cybercriminalité et les attaques soutenues par des États, ce qui a un impact significatif sur l'attribution des attaques et la gestion de la sécurité en général.

En outre, la directive NIS2 récemment approuvée par l'UE vise à renforcer considérablement la collaboration entre les États membres de l'UE dans la lutte contre la cybercriminalité. Outre le fait qu'elle contribuera à une meilleure protection des systèmes, cette directive aura probablement un impact sur les efforts préventifs et opérationnels des forces de l'ordre, des agences de renseignement et des équipes de réponse aux incidents de sécurité informatique (Computer Security Incident Response Teams - CSIRT) dans les différents pays. La directive encourage l'augmentation et la normalisation des rapports, l'amélioration du partage des informations, le renforcement des mécanismes de coopération et l'harmonisation du cadre juridique.

Matrice de probabilité

Très improbable <10 %	**Peu probable** 10–40 %	**Même chance** 40–60 %
Probable 60–90 %	**Très probable** >90 %	

— Les groupes de menaces persistantes avancées (APT) alignés sur les États collaborent de plus en plus avec les cybercriminels, en particulier dans l'utilisation de ransomwares, de courtiers d'accès initial et d'attaques destructrices.

Comment Sopra Steria peut vous aider

D'après nos observations pour l'année 2024, il y a beaucoup à faire pour obtenir un niveau de sécurité acceptable. La menace dans le domaine cyber s'accroît et le rythme s'accélère.

Chez Sopra Steria, nous avons plus de 3000 experts qui peuvent aider votre entreprise à réduire la probabilité d'une cyberattaque réussie en réduisant systématiquement les risques et en augmentant de façon mesurable la maturité de la sécurité.

Si vous devez vous « concentrer sur trois choses seulement » en 2025 pour optimiser votre sécurité, privilégiez les domaines suivants :

Meilleure gestion du phishing

- Formez et sensibilisez vos employés au phishing par le biais du courrier électronique, du chat et du téléphone.
- Mettez en place des outils anti-phishing qui aident instantanément vos employés à évaluer le risque des courriels.
- Établissez des procédures de signalement et d'alerte afin que vos employés puissent signaler les risques ou les comportements potentiels en matière de sécurité.

Compréhension du paysage des menaces

- Veillez à ce que l'entreprise dispose d'une connaissance actualisée du paysage des menaces qui pèsent sur elle.
- Sachez quels sont les actifs et les informations critiques de votre entreprise qui ont de la valeur aux yeux d'un attaquant.
- Comprenez comment l'intelligence artificielle et les nouvelles réglementations affectent le paysage.

Réduction de la surface d'attaque

• Corrigez les vulnérabilités, en vous concentrant sur les vulnérabilités exploitées connues ou celles qui sont exposées sur Internet.

• Mesurez la qualité des systèmes informatiques par rapport à des frameworks connus et fixez des exigences claires en matière de conformité.

• Utilisez une authentificatiton multifactorielle (MFA) résistante au phishing.

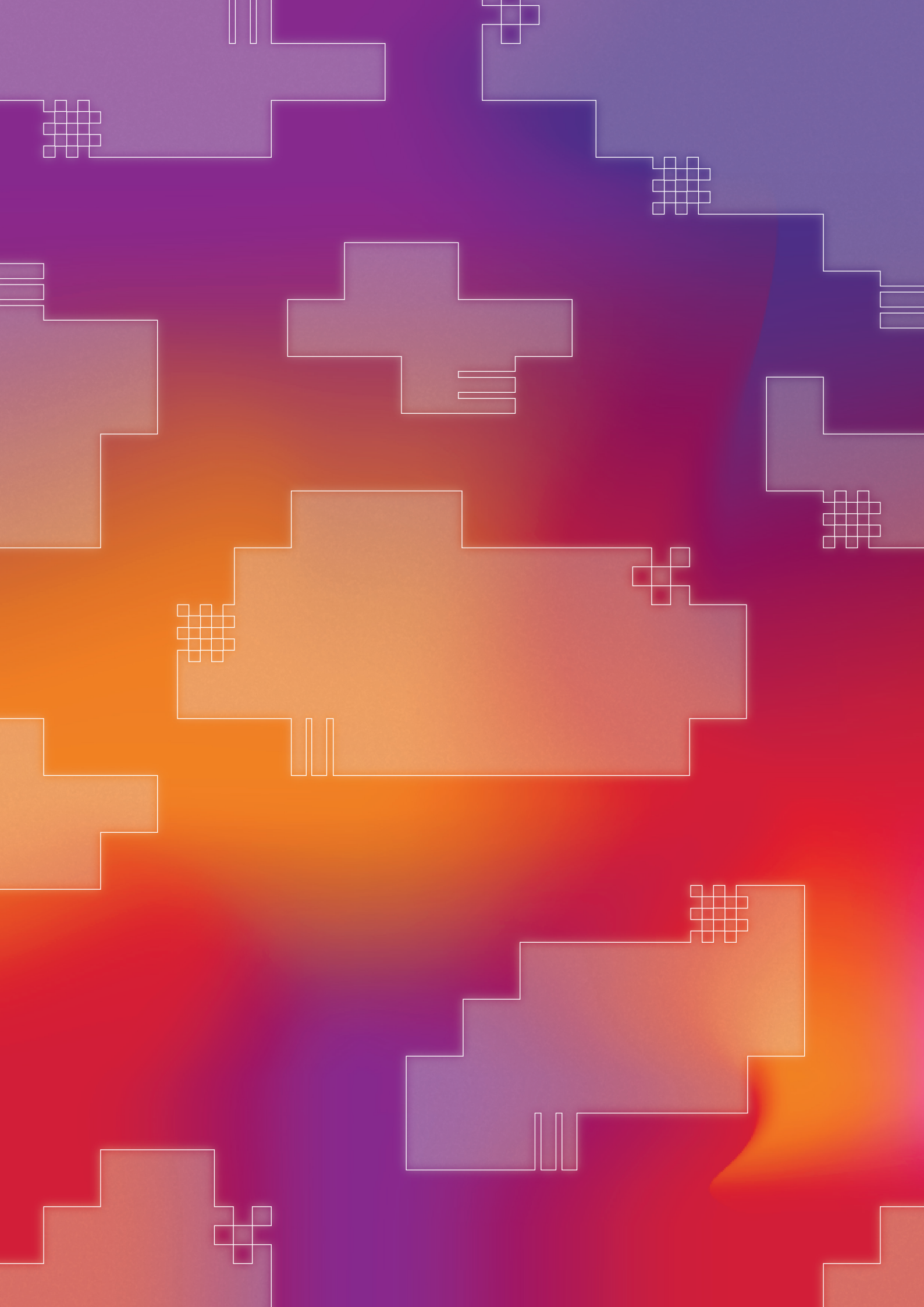
Dans le domaine de la sécurité, les acteurs de menaces exploitent constamment et de manière opportuniste un espace numérique qui offre de plus en plus d'opportunités. Il peut être difficile de s'y retrouver et de savoir où concentrer ses efforts en matière de sécurité.

• Comment mettre en place un projet qui nous protège mieux contre le phishing?

• Comment réduire systématiquement la surface d'attaque?

Ces questions se posent souvent alors que nous sommes quotidiennement submergés par les cybermenaces et nouvelles technologies. Chez Sopra Steria, nous pouvons aider votre entreprise à évaluer son niveau de maturité, à réaliser des tests de sécurité, à améliorer sa sécurité, à surveiller sa sécurité, à renforcer sa capacité de réponse, à élaborer une stratégie, à définir une image cible, à se mettre en conformité et bien plus encore. Nos clients fournissent des services essentiels à la société et nous travaillons 24 heures sur 24, 7 jours sur 7 pour les aider à sécuriser ces services et leurs fonctions sociétales critiques. Nous voulons aider, et nous pouvons aider.

Fabien Lecoq

Directeur Cybersécurité chez Sopra Steria

fabien.lecoq1@soprasteria.com