**La cyberattaque contre OKTA, Inc. en 2022.**

Sous la direction du Professeur Michel Séjean.



*Présenté par Sarah BENATALLAH et Rolande Sangale.*

# TABLE DES MATIÈRES

[**INTRODUCTION 3**](#_gcidkn8xb42r)

[**I. Les faits 4**](#_s5ql2xz6qusf)

[**A) L’attaque 4**](#_z5w5ihusnosj)

[**B) Une attaque par rebond. 7**](#_cq9nqd4jpz73)

[**II. La réponse 9**](#_r01tscuswc2)

[**A) La réponse d’Okta 9**](#_87acaw43edts)

[**B) La réaction des parties prenantes 10**](#_xbys4gxxiryr)

[**C) L'interprétation des experts 11**](#_fhltkus2lwd2)

[**III. Les conséquences de la cyberattaque. 11**](#_6eb83ts1tc02)

# INTRODUCTION

L'ingénierie sociale est le thème retenu par le mois de la cybersécurité en 2023. Ce rendez-vous annuel, introduit en 2012 par l’Agence de l'Union européenne pour la cybersécurité (ENISA), est un dispositif de sensibilisation sous forme d’événements et conférences, qui vise à promouvoir le sujet de la cybersécurité à travers les pays de l’Union européenne. Son but : mieux comprendre les menaces liées à la cybersécurité et mieux les appréhender. En France, l’institution responsable de ce dispositif est le site CyberMalveillance.gouv.fr[[1]](#footnote-1).

Par définition, la cyberattaque est un « ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité »[[2]](#footnote-2).

En droit, la cybercriminalité englobe deux types de délits : celles ciblant directement ce que la loi Godfrain[[3]](#footnote-3), relative à la fraude numérique, appelle « les systèmes de traitement automatisés de données», mais aussi celles « ayant “ juste” le numérique pour vecteur»[[4]](#footnote-4). Or, « si les cybercriminels sont des maîtres de la manipulation, cela ne signifie pas qu’ils sont tous des manipulateurs de la technologie »[[5]](#footnote-5). Pour mettre en œuvre leur attaque, il arrive qu’ils privilégient un mode opératoire plus simple : établir un lien avec une personne dans le but de récupérer des informations confidentielles à des fins frauduleuses. Pour les cybercriminels, c'est une forme de manipulation. Cette pratique, appelée l'ingénierie sociale, repose sur les interactions sociales plutôt que sur des compétences techniques, et est largement exploitée pour des attaques ciblées et d'envergure, visant à voler des données, ou encore de l’argent. Cette approche vise donc à induire l’Homme en erreur, afin d’obtenir de son manque de vigilance, des données confidentielles ou un accès non autorisé. Il est donc crucial de sensibiliser et de former les individus comme remparts essentiels contre de telles attaques. Parmi les méthodes les plus fréquentes d'ingénierie sociale, on compte le *phishing[[6]](#footnote-6)*, ou hameçonnage, le *hacking*, ou le *ransomware* aussi appelé́ rançongiciel[[7]](#footnote-7).

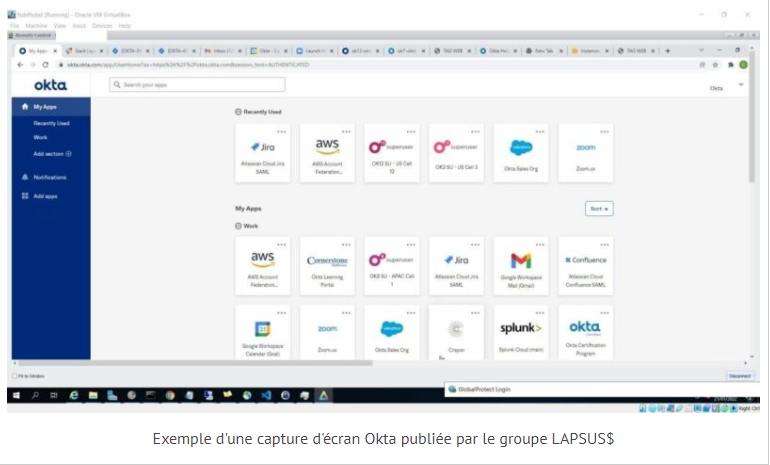
Dans l’affaire OKTA Entreprise *versus* le groupe de pirates LAPSUS$, le mode opératoire de ces derniers s’inscrit dans cette méthode de manipulation, qui semble connaître « un emballement tel depuis quelques années seulement, que le nombre de ces infractions dépasse désormais celles des infractions constatées dans le monde physique »[[8]](#footnote-8).

# Les faits

# L’attaque

« Fin janvier 2022, Okta a détecté une tentative de compromettre le compte d'un ingénieur de support client tiers travaillant pour l'un de nos sous-traitants. L'affaire a fait l'objet d'une enquête et a été maîtrisée par le sous-traitant. Nous pensons que les captures d'écran partagées en ligne sont liées à cet événement de janvier. Sur la base de notre enquête à ce jour, il n'y a aucune preuve d'activité malveillante en cours au-delà de l'activité détectée en janvier »[[9]](#footnote-9). Ce communiqué, posté par la société Okta, « spécialiste de l’authentification »[[10]](#footnote-10) le 22 mars 2022, donne quelques éléments sur le déroulé de l’attaque.

En l’espèce, tout débute le 16 janvier 2022. La société américaine Okta, spécialiste de la gestion des identités, est piratée via un accès au VPN de Sykes, une filiale acquise en 2021 par Sitel, une entreprise sous-traitante d'Okta, qui fournit un service client pour Okta. Les attaquants ont usurpé les accès d’un utilisateur et les ont employés pour s’authentifier auprès de la passerelle. Une fois à l’intérieur du réseau, ils ont utilisé des méthodes d’exploitation et de rebond classiques pour créer un compte administrateur et persister au sein du système d’information.. Dans le cadre de cette compromission, les pirates ont pu accéder à un tableur contenant des mots de passe de comptes administrateur de domaines compilés par un salarié depuis le gestionnaire de mots de passe LastPass dans un fichier dénommé *“DomAdmins-LastPass.xls*”. »[[11]](#footnote-11). De ce fait, ayant possession de ces comptes administrateurs, les pirates ont pu obtenir, à distance, « des captures d'écran et contrôler l’ordinateur via la session RDP[[12]](#footnote-12) »[[13]](#footnote-13). Une fois l’accès au système informatique effectif, l’attaquant, « a été en mesure de créer un nouveau compte utilisateur Sykes et l’ajouter à un groupe d’admin ayant un accès élargi au réseau Sitel de façon à y injecter un backdoor[[14]](#footnote-14) »[[15]](#footnote-15). Dès lors, le lien avec la société OKTA a rapidement pu être établi : le 20 janvier 2022, Okta a constaté une tentative d'accès au service, d’un compte Okta, appartenant à un employé de Sitel dont la localisation était anormale[[16]](#footnote-16) . Cette activité a été détectée et bloquée par Okta, qui en a rapidement informé Sitel[[17]](#footnote-17). Plus tard dans la journée, *Okta Security* commence à enquêter sur cet événement et l'élève au rang d’incident de sécurité. Puis, pour favoriser les chances de contenir le compte de l’utilisateur, le Service Desk Okta est sollicité, tout comme le service d'assistance Okta, qui a mis fin aux sessions de l'utilisateur et a suspendu le compte jusqu'à ce que la cause première de l'activité suspecte puisse être identifiée et corrigée[[18]](#footnote-18). Le 17 mars 2022, Okta reçoit un premier rapport sommaire de Sitel sur l’incident, que celle-ci avait commandé à Mendiant, une entreprise spécialisée dans la cybersécurité[[19]](#footnote-19). Cinq jours plus tard, dans la nuit, des captures d'écran sont partagées en ligne par un groupe connu de pirates, Lapsus$, permettant alors à Okta de déterminer que les captures d'écran étaient liées à l’incident de janvier chez Sitel, et ainsi, mettre un nom sur les auteurs de l’attaque.

[](https://www.it-connect.fr/okta-confirme-le-piratage-voici-les-dernieres-infos/?utm_content=cmp-true)

Pour terminer, Okta reçoit le rapport d'enquête final complet de Sitel, le 22 mars 2022, dans la journée[[20]](#footnote-20). Ce n’est que le 25 janvier 2022, que Sitel effectue officiellement « une communication auprès de ses clients - dont Okta - sur cet incident » [[21]](#footnote-21).

Même si les spécificités sur l'installation du logiciel malveillant dans le réseau de Sitel, puis de Sykes et son cheminement jusqu'à Okta n'ont pas été officiellement divulguées au public, le mode opératoire habituel du groupe de pirate Lapsus$, retrouvé en l’espèce, confirme que l'intrusion d’origine a été le résultat d’une ingénierie sociale : pour intégrer un poste de travail, son propriétaire a probablement donné son autorisation, cédant alors à la manipulation des *hackers*. De plus, s’agissant des captures d'écran publiées par Lapsus$, « des experts en cybersécurité ont confirmé leur vraisemblance à Reuters»[[22]](#footnote-22), une agence de presse anglaise. D’autres expertises permettent d’affirmer que « pour l’attaque d’Okta, ses membres se sont rapprochés d’un tiers, agent de support technique, qui avait des droit d’accès privilégiés à certains systèmes Okta (...) Mais l’une des tactiques privilégiées du groupe consiste à corrompre des salariés de grands groupes, payés pour faire tourner des outils d’accès à distance ou révéler des identifiants.»[[23]](#footnote-23)

Le peu d’informations fournies par Okta et son silence au moment de la survenance des faits, ne permettent pas d’affirmer l’une ou l’autre de ces hypothèses. Pour autant, il est indéniable que ce procédé s’inscrit dans l’une des tactiques favorites du groupe de pirates, à savoir, « l'accès aux comptes personnels des employés des organisations cibles» [[24]](#footnote-24).

En effet, ce *modus operand*i[[25]](#footnote-25) s’avère donc très dangereux et intrusif : « ces tactiques comprennent l'ingénierie sociale par téléphone, l'échange de cartes SIM pour faciliter la prise de contrôle des comptes, l'accès aux comptes de messagerie personnels des employés des organisations cibles, le paiement d'employés, de fournisseurs ou de partenaires commerciaux des organisations cibles pour l'accès aux informations d'identification et l'approbation de l'authentification multifactorielle (MFA[[26]](#footnote-26)), et l'intrusion dans les appels de communication de crise en cours de leurs cibles »[[27]](#footnote-27). Les « 18.000 clients »[[28]](#footnote-28) revendiqués par Okta, devront donc, probablement renforcer leur vigilance en attendant des clarifications sur les éventuelles données auxquelles les cybercriminels auraient pu accéder[[29]](#footnote-29).

Une chose est sûre, l’attaquant visait spécifiquement les clients d’Okta, puisque « LAPSUS$ a diffusé les captures d'écran (messagerie Slack et ticketing interne) sur son canal Telegram. Un message accompagnant les captures d'écran mentionne que les pirates s'intéressent UNIQUEMENT (aux) clients d'Okta»[[30]](#footnote-30), mais pour autant, l'attaque s’est faite initialement par le poste de travail d’un employé Sitel, et non Okta.

# Une attaque par rebond.

Les entreprises sont de plus en plus préoccupées par les cybermenaces au sein ou à travers de leur chaîne d'approvisionnement. En 2021, les experts en sécurité informatique ont constaté une augmentation de 15,1 % des cyberattaques et des violations de données par rapport à 2020[[31]](#footnote-31). Cette évolution devrait perdurer, « en raison des tendances florissantes telles que l’industrie 4.0 ou la numérisation des processus, adoptées par les entreprises à l’échelle globale» [[32]](#footnote-32). Par conséquent, les industries et les gouvernements du monde entier doivent aborder ce risque avec prudence, en veillant à mettre en place des solutions et des stratégies pour renforcer la sécurité et la résilience de l'ensemble de leur chaîne d'approvisionnement[[33]](#footnote-33).

L’affaire d’Okta, pousse à un questionnement intéressant sur les conséquences d’une attaque passant d’abord par un sous-traitant, qui a souvent la qualité de fournisseur d’identité. Pour rappel, les cybercriminels, en l’espèce, ont intégré le système de la société, via un accès au VPN de Sykes, société détenue par Sitel[[34]](#footnote-34), mais ont spécifié leur intérêt exclusif pour les clients d’Okta, confirmant ainsi une « attaque par rebond »[[35]](#footnote-35). Il est donc évident, que « les fournisseurs et les vendeurs ont souvent des privilèges d’accès étendus aux réseaux, aux données et aux applications des clients. Cela en fait une première étape attrayante pour les pirates pour infiltrer les organisations cibles. Une fois à l’intérieur des systèmes d’un fournisseur ou d’un vendeur, les attaquants peuvent utiliser des voies d’accès de confiance pour se déplacer latéralement et compromettre discrètement les clients en aval. Comme cet accès provient d’un tiers légitime, il peut plus facilement échapper aux contrôles de sécurité »[[36]](#footnote-36). Le risque est donc d'autant plus accru lorsque la cible initiale est un utilisateur légitime, et « la méthode par défaut pour les connecter a souvent été les réseaux privés virtuels (VPN). Le VPN repose sur des contrôles de sécurité de base : mots de passe et MFA. Mais ce n’est pas parce qu’une personne a saisi le bon nom d’utilisateur et peut produire un token[[37]](#footnote-37) MFA qu’elle est légitime. Sans télémétrie supplémentaire, telle que l’analyse du comportement de l’utilisateur, les organisations n’ont aucun moyen de savoir si un compte a été compromis. Étant donné que les hackers n’ont qu’à passer le processus de connexion pour compromettre une infrastructure, l’ingénierie sociale est devenue très efficace » [[38]](#footnote-38).

Les clients d’Okta, ont naturellement voulu savoir qui était ce fournisseur de service tiers, intermédiaire de la cyberattaque. Sur son site officiel, Okta répond simplement que «Sykes Enterprises, Inc. (qui a été acquis par Sitel en septembre 2021) est le fournisseur de services tiers qui fournit l'ingénierie du support client au nom d'Okta »[[39]](#footnote-39).

Ce manque de précision dans la réponse d’Okta éclaire sur l'attitude de l'entreprise à l'égard des légitimes préoccupations des clients quant à la sécurité de leurs données et à la portée de l'attaque. Les parties prenantes ne risquent pas de se contenter d’une telle réponse.

# II. La réponse

# La réponse d’Okta

Okta s’est tout d’abord montrée très rassurante, notamment en publiant un rapport[[40]](#footnote-40) rendu le 19 avril 2022 par David Bradbury, responsable de la sécurité des systèmes d'information (ci-après “RSSI”) d'Okta. Cette communication se divise en plusieurs parties : l’investigation de l’attaque y est reportée dans une première section. À la suite, on retrouve une seconde section intitulée « Collaboration avec nos clients », puis une troisième dénommée « Enseignements tirés », et pour finir, une dernière partie nommée « Les prochaines étapes ». Bien que ce rapport ait été rendu deux mois après l’attaque, Okta semble contrôler la situation, rassurant sa clientèle grâce à un écrit exhaustif, décrivant les mesures prises par la société, manifestant ainsi une gestion proactive de cette crise.

En effet, le RSSI de la société avance, au nom et pour le compte d’Okta : « Nous avons réagi en toute transparence en transmettant les informations en notre possession à ce moment-là»[[41]](#footnote-41), et ajoute que « maintenant que nous sommes arrivés à l’issue de notre investigation, nous avons transmis les deux documents suivants aux clients d’Okta dont nous pensions initialement qu’ils pourraient être impactés : le rapport d’expertise final, préparé pour Okta par une société de cybersécurité de renommée mondiale » et « le plan d’action de sécurité d’Okta, qui détaille les mesures à court et à long terme permettant de renforcer la sécurité de nos sous-traitants tiers ayant accès aux systèmes de support client »[[42]](#footnote-42).

Conscient « qu’il est vital d’agir pour rétablir la confiance » des « clients » et de leur « écosystème», Okta s’engage « à agir sur d’autres fronts : gestion des risques chez les tiers, accès aux systèmes de support client» et « communication avec les clients » [[43]](#footnote-43).

Enfin, pour clôturer ce rapport, le RSSI n’omet pas de préciser que « la technologie d’Okta a fait ses preuves pendant l’incident », mais formule tout de même des regrets sur le fait que leurs « efforts pour communiquer sur les événements survenus chez Sitel n’ont pas été à la hauteur » de leurs « attentes » ou de celles de leurs « clients»[[44]](#footnote-44). Des promesses futures sont avancées par le groupe Okta, qui est « plus déterminé que jamais à - se - montrer à la hauteur de - nos - attentes », tout en rappelant encore une fois, « l’importance cruciale d'Okta pour de nombreuses organisations et pour toutes les personnes qui s’appuient sur elles »[[45]](#footnote-45).

# La réaction des parties prenantes

Toutefois, un silence de deux mois suivant une cyberattaque, ne peut être ignoré, et pourrait même constituer une sorte de réponse assez claire de la part de la société. D’ailleurs, dans le cadre d’une « foire aux questions »[[46]](#footnote-46) (ci-après “FAQ”), disponible sur le site officiel d’Okta, les internautes ont voulu savoir « pourquoi Okta n'a-t-il pas prévenu ses clients en janvier ? ». La société s’est défendue en avançant : « Nous voulons reconnaître que nous avons fait une erreur. Sitel est notre fournisseur de services et nous en sommes responsables en dernier ressort. En janvier, nous ne connaissions pas l'étendue du problème de Sitel - nous savions seulement que nous avions détecté et empêché une tentative de prise de contrôle de compte et que Sitel avait retenu les services d'une société d'expertise judiciaire tierce pour enquêter. À ce moment-là, nous n'avons pas reconnu qu'il y avait un risque pour Okta et nos clients » [[47]](#footnote-47). Sans expliquer pourquoi elle n'a pas ouvert la communication dès la survenance de l’attaque, la société se contente de rejeter la faute sur son sous-traitant, en indiquant « Nous aurions dû exiger plus activement et plus énergiquement des informations de la part de Sitel. À la lumière des preuves que nous avons recueillies au cours de la semaine écoulée, il est clair que nous aurions pris une décision différente si nous avions été en possession de tous les éléments dont nous disposons aujourd'hui »[[48]](#footnote-48).

S’agissant du nombre de clients affectés suite à cette attaque, la question suivante a été posée : « Comment Okta a-t-il déterminé le nombre de clients potentiellement concernés ?»[[49]](#footnote-49), Okta avance qu’ « en essayant de déterminer le rayon d'action de cet incident, notre équipe a supposé le pire des scénarios et a examiné tous les accès effectués par tous les employés de Sitel à l'application SuperUser pendant la période de cinq jours au cours de laquelle Sitel a été compromise. Nous avons déterminé que l'impact potentiel maximal est de 366 (environ 2,5% des) clients, ce qui reflète le nombre total de clients Okta dont le serveur Okta a été accédé par Sitel pendant cette période. Ce chiffre est trop élevé car il inclut tous les accès légitimes à l'assistance clientèle de Sitel au cours de cette période »[[50]](#footnote-50).

# L'interprétation des experts

Okta semble sereine face à la situation, et rassure tant bien que mal ses clients. Néanmoins, si la déclaration de leur RSSI ne semble pas revêtir une ampleur importante, certains experts en cybersécurité ne sont pas de cet avis.

En effet, dans son analyse de l’attaque postée sur son compte twitter, le chercheur indépendant Bill Demirkapi considère qu’« il semble qu'ils essaient de minimiser l'attaque autant que possible, allant jusqu'à se contredire directement dans leurs propres déclarations»[[51]](#footnote-51). En ce sens, « la nature de cet impact n'était pas claire et Okta n'a pas immédiatement répondu à un courriel demandant combien d'organisations étaient potentiellement affectées ou comment cela cadrait avec l'avis d'Okta selon lequel les clients n'avaient pas besoin de prendre des mesures correctives »[[52]](#footnote-52). En effet, il explique que « La chronologie de l'attaque est extrêmement inquiétante pour le groupe Sitel. Les attaquants n'ont pas du tout tenté de maintenir une sécurité opérationnelle. Ils ont littéralement fait des recherches sur Internet sur des outils malveillants connus depuis les machines compromises et les ont téléchargées à partir de sources officielles»[[53]](#footnote-53).

Une réactivité trop lente de la part d’Okta, qui plus est un géant de la sécurisation des données, mais aussi responsable de plus de 18.000 clients divers, est essentiellement reprochée, et engendre des conséquences dévastatrices.

# III. Les conséquences de la cyberattaque.

La conséquence première de l’attaque est certainement l’atteinte à la réputation de la société victime. En l’espèce, il est pertinent de relever dans un premier temps, une communication désastreuse de la part de Sitel[[54]](#footnote-54), mais également d’Okta, qui semble tenter de minimiser la situation. En effet, le rapport[[55]](#footnote-55) de leur RSSI, indique que leur priorité principale réside dans la restauration de la confiance de leurs clients ainsi que dans la consolidation de leur système[[56]](#footnote-56). Comme mentionné précédemment, Okta a tenté de rassurer le public, en indiquant que seule 2,5% de sa cliente pourrait être touchée par l’attaque. En interne, Okta a revu ses programmes de sécurité et s'est engagée à trouver de nouvelles méthodes pour accélérer la transmission d'informations, concernant « tous les problèmes potentiels, grands ou petits, à la fois en interne et avec des tiers »[[57]](#footnote-57). L'objectif est d'améliorer la fluidité de la communication en cas d'incident de cybersécurité[[58]](#footnote-58). La société a également renforcé ses procédures d'audit pour les futurs sous-traitants, en exigeant qu'ils adoptent un système d'authentification plus robuste via la solution IDAM d'Okta. De plus, Okta a choisi de superviser directement tous les terminaux tiers accédant à leurs outils de support, afin d'assurer une meilleure visibilité et de réagir efficacement aux incidents de sécurité[[59]](#footnote-59).

Par conséquent, ils ont décidé de mettre fin à leur contrat avec les sociétés Sykes et Sitel.

Il est important de rappeler qu’il n'existe pas de solution infaillible contre les cyberattaques par ingénierie sociale, mais les bonnes mesures, l'éducation et la sensibilisation à leurs effets nuisibles pourraient mener à des solutions plus satisfaisantes pour toutes les parties prenantes. Malheureusement, toutes les mesures prises ne peuvent pas être qualifiées de réussies. L’impact financier négatif engendré par l’attaque, s’est traduit par une baisse significative en bourse des actions d’Okta. La confiance autrefois accordée à cette société, a probablement été brisée de manière irréversible : si une société d’authentification des données est elle-même est sujette à des attaques en cybersécurité, comment peut-elle garantir cette sécurité à d’autres ?[[60]](#footnote-60).

Surtout, Okta a été victime d'une nouvelle attaque en septembre 2023[[61]](#footnote-61), démontrant encore une fois, que leur réaction face à cette cyberattaque, les mesures prises et leur gestion de la crise, n’a peut-être pas été la plus efficace.

**Sécuriser les connexions RDP en limitant les accès RDP**

On peut utiliser le pare-feu Windows pour limiter l'accès au port RDP (par défaut le port 3389) uniquement aux adresses IP autorisées. Pour cela, il faut configurer des règles de pare-feu pour permettre l'accès uniquement aux adresses IP spécifiques ou aux plages d'adresses IP autorisées. : pour aller plus loin, v. Karner, K.,”[Restreindre l'accès RDP par adresse IP](https://www.hostwinds.fr/tutorials/restrict-rdp-access-by-ip-address)”, *site Hostwinds.com*,  15 nov. 2019, [dernière consultation 04 mars 2024].

1. « Dispositif Cyber Malveillance » v. le site cybermalveillance.gouv.fr, « À propos », *[site internet de Cybermalveillance](https://www.cybermalveillance.gouv.fr/a-propos),* article non daté, [09/03/2024] [↑](#footnote-ref-1)
2. « Vocabulaire de la défense », v. le site legifrance.gouv.fr, « Vocabulaire de la défense : cyberdéfense (liste de termes, expressions et définitions adoptés) », *[site internet de Legifrance](https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035583357),* article non daté, [09/03/2024] [↑](#footnote-ref-2)
3. « Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique . NOR : JUSX8700198L . », v. le site legifrance.gouv.fr, « Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique », *[site internet de Legifrance](https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000875419),*

   Article non daté, [09/03/2024]. [↑](#footnote-ref-3)
4. Dalloz actualité [PODCAST] *«* Cyberarnaques » : quand l'internaute mord à l'hameçon – Sophie Sontag Koenig– *(web radio Amicus Radio)* – 21 avril 2023. Disponible : [https://www-dalloz-fr.ezpaarse.univ-paris1.fr](https://www-dalloz-fr.ezpaarse.univ-paris1.fr/documentation/Document?id=ACTU0217863)

   [10 décembre 2023] [↑](#footnote-ref-4)
5. Antoine, L. 2022. Ingénierie sociale: quelles sont les 4 principales menaces et comment s’en prémunir ? *CyberUniversity.* 14 février. Disponible : [https://www.cyberuniversity.com/](https://www.cyberuniversity.com/post/ingenierie-sociale-quelles-sont-les-4-principales-menaces-et-comment-sen-premunir) [10 décembre 2023] [↑](#footnote-ref-5)
6. « Le phishing est une forme d'escroquerie sur internet », v. le site CNIL, « [Le phishing, c'est quoi ?](https://www.cnil.fr/fr/cnil-direct/question/le-phishing-cest-quoi)», *site internet de la CNIL*, article non daté , [dernière consultation 04 mars 2024]. [↑](#footnote-ref-6)
7. « L'ingénierie sociale consiste à entrer en relation avec un individu dans le but de lui soutirer des informations confidentielles à des fins frauduleuses. », v. le site Nomios.fr, « Qu'est-ce que l'ingénierie sociale ? », *[site internet de Nomios](https://www.nomios.fr/ressources/ingenierie-sociale/),* article non daté, [09/03/2024]. [↑](#footnote-ref-7)
8. Loveday, B. 2016. The Shape of Things to Come. Reflections on the potential implications of the 2016 Office of National Statistics Crime Survey for the Police Service of England and Wales, *Policing: A Journal of Policy and Practice*, vol. 12, p. 398-409. [↑](#footnote-ref-8)
9. Okta. 2022. Okta Official Statement on LAPSUS$ Claims*. Blog.* 22 mars. Disponible : [https://www.okta.com/blog](https://www.okta.com/blog/2022/03/okta-official-statement-on-lapsus-claims/) [10 décembre 2023] [↑](#footnote-ref-9)
10. Cheminat, J. *[«](https://www.lemondeinformatique.fr/actualites/lire-pirate-par-lapsus$-okta-avance-une-piste-86202.html)*[Piraté par Lapsus$, Okta avance une piste](https://www.lemondeinformatique.fr/actualites/lire-pirate-par-lapsus$-okta-avance-une-piste-86202.html)»,v. le site lemondeinformatique.fr*[, site internet Le Monde Informatique](https://www.lemondeinformatique.fr/actualites/).* 22 mars 2022, [04 mars 2024]

    [↑](#footnote-ref-10)
11. [↑](#footnote-ref-11)
12. « Le protocole RDP (Remote Desktop Protocol) permet aux collaborateurs en télétravail de se connecter à l'ordinateur qu'ils utilisent au bureau » : v. le site CLOUDFLARE[, « Qu'est-ce que le RDP (Remote Desktop Protocol) ? »,](https://www.cloudflare.com/fr-fr/learning/access-management/what-is-the-remote-desktop-protocol/)*site internet de CLOUDFLARE*, article non daté, [dernière consultation le 1er mars 2024]. [↑](#footnote-ref-12)
13. Corot, L. 2022. 366 clients d'Okta potentiellement affectés par le piratage mené par Lapsus$. *Usine Digitale*. 22 mars. Disponible : <https://www.usine-digitale.fr/article/> [10 décembre 2023] [↑](#footnote-ref-13)
14. «Un backdoor (ou porte dérobée) est un programme informatique malveillant utilisé pour donner aux pirates un accès à distance non autorisé à un ordinateur infecté en exploitant les vulnérabilités du système » : v. le site OCI,  «  [Qu'est-ce qu'un programme backdoor ?](https://www.oracle.com/fr/security/qu-est-ce-qu-un-programme-backdoor/) *», site internet de OCI*, article non daté, [dernière consultation 04 mars 2024]. [↑](#footnote-ref-14)
15. Filippone, D. 2022.Un chercheur détaille le piratage d’Okta.*. Le Monde Informatique.* 30 mars. Disponible :

    [https://www.lemondeinformatique.fr/actualites/lire-un-chercheur-detaille](https://www.lemondeinformatique.fr/actualites/lire-un-chercheur-detaille-le-piratage-d-okta-86283.html) [10 décembre 2023] [↑](#footnote-ref-15)
16. Okta Help Center. 2022. *Frequently Asked Questions Regarding the January 2022 Compromise* . Disponible : <https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022-Compromise?language=en_US> [↑](#footnote-ref-16)
17. *Ibid.* [↑](#footnote-ref-17)
18. *Ibid.* [↑](#footnote-ref-18)
19. Kallenborn, G 2022. Le piratage d’Okta par Lapsus$ a été… une vraie promenade de santé. *01net*. 30 mars. Disponible : [https://www.01net.com/actualites/](https://www.01net.com/actualites/le-piratage-d-okta-par-lapsusdollar-a-ete-une-vraie-promenade-de-sante-2055696.html) [10 décembre 2023] [↑](#footnote-ref-19)
20. Okta Help Center. 2022. *Frequently Asked Questions Regarding the January 2022 Compromise* . Disponible : <https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022-Compromise?language=en_US> [10 décembre 2023] [↑](#footnote-ref-20)
21. Cheminat, J. 2022.Piraté par Lapsus$, Okta avance une piste*. Le Monde Informatique.* 22 mars. Disponible :

    [https://www.lemondeinformatique.fr/actualites/](https://www.lemondeinformatique.fr/actualites/lire-pirate-par-lapsus$-okta-avance-une-piste-86202.html) [10 décembre 2023] [↑](#footnote-ref-21)
22. *Reuters,* Disponible :[*https://www.reuters.com/*](https://www.reuters.com/) [10 décembre 2023] [↑](#footnote-ref-22)
23. Jouzel, M. 2022. Les prouesses des hackers de Lapsus$ révèlent les faiblesses des services de support et le risque de corruption des employés. *BeyondTrust*. 5 mars. Disponible : [https://www.beyondtrust.com/fr/blog/entry/](https://www.beyondtrust.com/fr/blog/entry/les-prouesses-des-hackers-de-lapsus-revelent-les-faiblesses-des-services-de-support-et-le-risque-de-corruption-des-employes) [10 décembre 2023] [↑](#footnote-ref-23)
24. *It Info*. 2022. Microsoft et Okta répondent aux cyberattaques Lapsus$. 24 mars. Disponible : [https://br.atsit.in/fr/](https://br.atsit.in/fr/?p=213290) [10 décembre 2023] [↑](#footnote-ref-24)
25. Centre national des ressources textuelles et lexicales, Étymol. et Hist. 1892 (Guérin). Loc. lat. signifiant «manière d'opérer», comp. de modus (mode) et de operandi, génitif du gérondif de operari (opérer). Disponible : <https://www.cnrtl.fr/etymologie/MODUS%20OPERANDI> [10 décembre 2023] [↑](#footnote-ref-25)
26. « Le MFA est une méthode d’authentification dans laquelle l’utilisateur doit fournir au minimum deux facteurs de vérification pour accéder à une ressource de type application, compte en ligne ou VPN. », v. le site Onelogin, « [Qu’est-ce que l’authentification multifacteur (MFA) et comment fonctionne-t-elle ?](https://www.onelogin.com/fr-fr/learn/what-is-mfa)», *[site internet de Onelogin](https://www.onelogin.com/fr-fr/learn/what-is-mfa)*, article non daté, [dernière consultation 04 mars 2024]. [↑](#footnote-ref-26)
27. O’Donnell-Welch, L. 2022. L.lapsus$ group uses ‘unique blend’ of social engineering, identity-centric tactics. *Decipher.* 23 mars. Disponible : [https://duo.com/decipher/lapsususd](https://duo.com/decipher/lapsususd-group-uses-unique-blend-of-social-engineering-identity-centric-tactics) [10 décembre 2023] [↑](#footnote-ref-27)
28. *Okt*a. Disponible : [https://www.okta.com/fr](https://www.okta.com/fr/?utm_source=google&utm_campaign=emea_france_fra_all_all_dg-ao_emea_search_google_text_kw_it-brand-OktaExact_utm2&utm_medium=cpc&utm_id=aNK4z0000004DopGAE&gad_source=1&gclid=CjwKCAiAg9urBhB_EiwAgw88mS-moLPZAnRNgI6Q7J5lZTNYJvPxA9TAlJbroLFE78R3c_JXV7oRRRoCFyMQAvD_BwE) [10 décembre 2023] [↑](#footnote-ref-28)
29. Corot, L. 2022. Le piratage d'Okta par Lapsus$ a finalement eu peu d'impact*. Usine Digitale*. 21 avril. Disponible : <https://www.usine-digitale.fr/article/l-effet-limite-du-piratage-de-lapsus-sur-okta.N1995697>

    [10 décembre 2023] [↑](#footnote-ref-29)
30. Serries, G. 2022. Piratage d'Okta : l'entreprise admet enquêter, LAPSUS$ revendique. *ZDNet.* 22 mars. Disponible : [https://www.zdnet.fr/actualites/piratage-d-okta-l-entreprise-admet](https://www.zdnet.fr/actualites/piratage-d-okta-l-entreprise-admet-enqueter-lapsus-revendique-39939261.htm) [10 décembre 2023] [↑](#footnote-ref-30)
31. Boyens, Jon M. 2022. Cybersecurity Supply Chain Risk Management for Systems and Organizations. *NIST Special Publication. NIST SP 800-161r1.* Mai. Disponible : <https://doi.org/10.6028/nist.sp.800-161r1> [10 décembre 2023] [↑](#footnote-ref-31)
32. Urcioli, L. 2022. La cybersécurité dans la chaîne d'approvisionnement, une tendance croissante. *Mecalux*. 24 octobre. Disponible : [https://www.mecalux.fr/articles-de-logistique/luca-urciuoli](https://www.mecalux.fr/articles-de-logistique/luca-urciuoli-cybersecurite-chaine-approvisionnement) [10 décembre 2023] [↑](#footnote-ref-32)
33. Urcioli, L. 2022. La cybersécurité dans la chaîne d'approvisionnement, une tendance croissante. *Mecalux*. 24 octobre. Disponible : [https://www.mecalux.fr/articles-de-logistique/luca-urciuoli](https://www.mecalux.fr/articles-de-logistique/luca-urciuoli-cybersecurite-chaine-approvisionnement) [10 décembre 2023] [↑](#footnote-ref-33)
34. Ladet, G. 2023. 10 cyberattaques qui ont exploité le principe d’exposition. *Chimere*. 9 mai. Disponible : <https://chimere.eu/fr/blog/2023/05/09/10-cyberattaques-qui-ont-exploite-le-principe-dexposition/>

    [10 décembre 2023] [↑](#footnote-ref-34)
35. Lafont, C. 2022. Ces cyberattaques à l'encontre d'entreprises qui ont marqué 2022. *One Wave.* 9 décembre. Disponible : <https://onewave.io/le-blog/ces-cyberattaques-a-lencontre-dentreprises-qui-ont-marque-2022/>

    [10 décembre 2023] [↑](#footnote-ref-35)
36. Ertl, B. 2023. Comment le piratage du service client d’Okta a exposé des données sensibles et des informations d’accès. *Kiteworks*. 28 octobre. Disponible : [https://www.kiteworks.com/fr/gestion-des-risques](https://www.kiteworks.com/fr/gestion-des-risques-lies-a-la-cybersecurite/piratage-service-client-okta/) [10 décembre 2023] [↑](#footnote-ref-36)
37. « En informatique, cet anglicisme est utilisé : pour désigner un identificateur de session pour identifier une session lors d'une communication réseau », v. le site Wikipedia, « *[Token](https://fr.wikipedia.org/wiki/Token)* », site internet de Wikipedia, article non daté, [dernière consultation 04 mars 2024]. [↑](#footnote-ref-37)
38. Bobe, B. 2023.Ingénierie sociale et accès VPN : La fabrication d’une faille moderne. Global Security Mag. Novembre. Disponible : [https://www.globalsecuritymag.fr/Ingenierie-sociale-et-acces-VPN-La-fabrication](https://www.globalsecuritymag.fr/Ingenierie-sociale-et-acces-VPN-La-fabrication-d-une-faille-moderne.html)

    [10 décembre 2023] [↑](#footnote-ref-38)
39. Okta Help Center. 2022. *Frequently Asked Questions Regarding the January 2022 Compromise* . Disponible : [https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022](https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022-Compromise?language=en_US) [10 décembre 2023] [↑](#footnote-ref-39)
40. Bradbury, D. *Blog Okta*. Disponible : <https://www.okta.com/fr/blog/author/david-bradbury/> [10 décembre 2023] [↑](#footnote-ref-40)
41. Bradbury, D. 2022. Okta conclut son investigation sur la compromission de janvier 2022. *Blog Okta .* 19 avril. Disponible : [https://www.okta.com/fr/blog/2022/04/okta-concludes-its-investigation](https://www.okta.com/fr/blog/2022/04/okta-concludes-its-investigation-into-the-january-2022-compromise/) [10 décembre 2023] [↑](#footnote-ref-41)
42. *Ibid.*  [↑](#footnote-ref-42)
43. *Ibid.*  [↑](#footnote-ref-43)
44. *Ibid.*  [↑](#footnote-ref-44)
45. *Ibid.*  [↑](#footnote-ref-45)
46. Okta Help Center. 2022. *Frequently Asked Questions Regarding the January 2022 Compromise* . Disponible : <https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022-Compromise?language=en_US> [10 décembre 2023] [↑](#footnote-ref-46)
47. *Ibid.*  [↑](#footnote-ref-47)
48. *Ibid.*  [↑](#footnote-ref-48)
49. *Ibid.*  [↑](#footnote-ref-49)
50. Okta Help Center. 2022. *Frequently Asked Questions Regarding the January 2022 Compromise* . Disponible : <https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022-Compromise?language=en_US> [10 décembre 2023] [↑](#footnote-ref-50)
51. Demirkapi, B. [@BillDemirkapi]. (2022, mars). New documents for the Okta breach: I have obtained copies of the Mandiant report detailing the embarrassing Sitel/SYKES breach timeline and the methodology of the LAPSUS$ group. [Tweet]. *Twitter.* Disponible : <https://x.com/BillDemirkapi/status/1508527487655067660?s=20> [10 décembre 2023] [↑](#footnote-ref-51)
52. Satter, R. 2022. Hackers hit authentication firm Okta, customers 'may have been impacted'. *Reuters*. 23 mars. Disponible : [https://www.reuters.com/technology/authentication-services-firm-okta](https://www.reuters.com/technology/authentication-services-firm-okta-says-it-is-investigating-report-breach-2022-03-22/) [10 décembre 2023] [↑](#footnote-ref-52)
53. Filippone, D. 2022.Un chercheur détaille le piratage d’Okta.*. Le Monde Informatique.* 30 mars. Disponible :

    [https://www.lemondeinformatique.fr/actualites/lire-un-chercheur-detaille](https://www.lemondeinformatique.fr/actualites/lire-un-chercheur-detaille-le-piratage-d-okta-86283.html) [10 décembre 2023] [↑](#footnote-ref-53)
54. Aspasch, K. 2023. Okta Could See Hit To Its Reputation After Second Major Breach In Two Years: Analysts*. The channelco CRN,* Octobre 23*.* Disponible:[https://www.crn.com/news/security](https://www.crn.com/news/security/okta-faces-potential-for-reputational-risk-after-second-major-breach-in-two-years-analysts) [11 décembre 2023] [↑](#footnote-ref-54)
55. Bradbury, D. 2022. Okta conclut son investigation sur la compromission de janvier 2022. *Blog Okta .* 19 avril. Disponible : [https://www.okta.com/fr/blog/2022/04/okta-concludes-its-investigation](https://www.okta.com/fr/blog/2022/04/okta-concludes-its-investigation-into-the-january-2022-compromise/) [10 décembre 2023] [↑](#footnote-ref-55)
56. Cheminat, J. 2022.Piraté par Lapsus$, Okta avance une piste*. Le Monde Informatique.toute l’actualité, intrusion pare-feu.* 22 mars. Disponible : [https://www.lemondeinformatique.fr/actualites/](https://www.lemondeinformatique.fr/actualites/lire-pirate-par-lapsus$-okta-avance-une-piste-86202.html) [10 décembre 2023] [↑](#footnote-ref-56)
57. Corot, L. 2022, Le piratage d'Okta par Lapsus$ a finalement eu peu d'impact, avril 2022. *l’Usine digitale, cybersécurité, cloud, gestion des données.*  Disponible : [https://www.usine-digitale.fr/](https://www.usine-digitale.fr/article/l-effet-limite-du-piratage-de-lapsus-sur-okta.N199569) [10 décembre 2023] [↑](#footnote-ref-57)
58. Bradbury, D. 2022. Okta conclut son investigation sur la compromission de janvier 2022. *Blog Okta .* 19 avril. Disponible : [https://www.okta.com/fr/blog/2022/04/okta-concludes-its-investigation](https://www.okta.com/fr/blog/2022/04/okta-concludes-its-investigation-into-the-january-2022-compromise/) [10 décembre 2023] [↑](#footnote-ref-58)
59. *Ibid.*  [↑](#footnote-ref-59)
60. Faife, C. 2022. Okta ends Lapsus$ hack investigation, says breach lasted just 25 minutes. *The verge, policy, tech, security*, Avril 2022. Disponible : [https://www.theverge.com/2022/4/20/23034360/okta-lapsus-hack-investigation](https://www.theverge.com/2022/4/20/23034360/okta-lapsus-hack-investigation-breach-25-minutes) [11 décembre 2023] [↑](#footnote-ref-60)
61. Sounack, L, 2023. Le service de support d’Okta compromis à l’aide d’un identifiant volé. *Channel News,* Cyberattaque, Octobre 2023. Disponible : [https://www.channelnews.fr/le-service-de-support-dokta](https://www.channelnews.fr/le-service-de-support-dokta-compromis-a-laide-dun-identifiant-vole-129293) [11 décembre 2023] [↑](#footnote-ref-61)