RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Date : 19 février 2025
Version : 1.0
Nombre de pages : 46

CLOUD COMPUTING

ÉTAT DE LA MENACE INFORMATIQUE

TLP:CLEAR

Table des matières

1 SYNTHÈSE

Le *cloud computing* est une technologie particulièrement structurante pour nos usages numériques, à laquelle les secteurs privés et publics ont de plus en plus recours. Ce constat s'explique notamment par les opportunités et l'effet levier apportés par cette technologie dans la transformation numérique. Le *cloud* offre cependant de nouvelles opportunités d'attaques et problématiques de sécurité pour les organisations qui l'utilisent, qu'elles disposent de leurs propres environnements *Cloud*, ou fassent appel à des fournisseurs de services (*Cloud service provider*, CSP). Ces derniers représentent à la fois une cible d'intérêt pour les données qu'ils traitent au quotidien, mais aussi et surtout pour les accès qu'ils peuvent offrir vers leur client.

Les attaquants poursuivant des finalités lucratives, d'espionnage et de déstabilisation ont intégré le ciblage et la compromission des environnement *cloud* dans leur mode opératoire. Certains ont notamment développé des compétences spécifiques à la compromission de ces environnements. Par exemple, les modes opératoires d'attaque (MOA) Mango Sandstorm, Scattered Spider, Nobelium, Storm-0558 ou encore Storm-0501, sont employés à des fins lucratives, d'espionnage ou de déstabilisation, pour compromettre ce type d'environnements.

La maîtrise des environnements *cloud*, par certains opérateurs de MOA se traduit notamment par la multiplication des tentatives de latéralisation depuis des environnements *on-premise* compromis, vers le *cloud* et parfois même réciproquement. Un savoir-faire également utilisé pour exploiter les mauvaises configurations ou défauts de sécurisation (permissions excessives, applications obsolètes, API mal sécurisée, espace de stockage exposés etc.).

L'exploitation de vulnérabilités dans des équipements de bordure (tels que des équipements VPN) constitue un point d'entrée privilégié par une vaste gamme d'acteurs malveillants. Dans une moindre mesure, les attaquants réputés liés à des États et disposant de ressources plus importantes utilisent également des vulnérabilités jour-0 (*0-day*) pour compromettre les environnements ciblés.

Enfin, une des tendances grandissantes identifiée par l'ANSSI est l'utilisation des services de *cloud* comme infrastructures d'attaques, qu'il s'agisse de louer de l'infrastructure d'attaque chez des opérateurs de *cloud*, ou d'utiliser des plateformes grand public comme lieu de stockage, d'accès à des codes malveillants ou d'exfiltration de données volées. Ces nouvelles pratiques complexifient la détection en dissimulant les activités malveillantes au sein du trafic légitime des utilisateurs de ces plateformes.

Afin d'assurer la sécurité des environnements *cloud*, il est important de souligner que, selon les principes de la responsabilité partagée, les clients de services *cloud* sont en partie dépendants du fournisseur pour leur sécurité mais disposent également de responsabilités importantes concernant la gestion des données et des identités. Ainsi, des compromissions facilitées par un faible cloisonnement entre systèmes d'information dû à l'hybridation générée par l'usage du *cloud* ou les manquements dans la supervision des systèmes d'informations (SI) sont fréquemment constatées.

A ce titre, cet état de la menace sur le *cloud Computing* comprend un volet dédié aux recommandations de l'ANSSI adressées aux clients de fournisseurs de services *cloud*, ainsi qu'aux fournisseurs de services *cloud* eux-mêmes. Ces recommandations sont des bonnes pratiques de cybersécurité à adopter afin de se prémunir contre les menaces abordées. Elles ne sont pas exhaustives et doivent être adaptées et complétées dans le cadre du contexte opérationnel et fonctionnel des systèmes d'information considérés.

2 INTRODUCTION

2.1 Qu'est-ce que le *cloud Computing* ?

Le *cloud* (ou *cloud computing*) désigne une pratique consistant à héberger certaines ressources informatiques (équipements, applications, infrastructures ou services) dans un centre de données accessibles à distance à travers Internet, plutôt que dans un système d'information local (*on-premise*).

Il existe plusieurs types de *cloud* : le *cloud* public, offre mutualisée pour l'ensemble des clients d'un offreur de solutions *cloud*, le *cloud* privé, offre dont les ressources (processeur, réseau et stockage) sont physiquement dédiées à l'entité souscrivant à l'offre, et le *cloud* hybride ou communautaire, offre qui est physiquement dédiée à un ensemble d'entités d'intérêt commun, qu'elles soient étatiques ou privées [1].

Les entreprises spécialisées en fourniture de services sur le *cloud* (*Cloud Service Provider*, CSP) déclinent leurs services selon trois principaux modèles [2, 3] :

- *Infrastructure as a Service* (IaaS), qui fournit des ressources de base comme des serveurs et du stockage (par exemple : AWS, Bleu, Cegedim.cloud, Cloud Temple, DS Outscale, Google Cloud, Microsoft Azure, NumSpot, Orange Business, Oracle, OVHCloud, S3ns, Scaleway, Scalingo, etc.).
- *Platform as a Service* (PaaS), qui offre des plateformes pour développer et déployer des applications. Par exemple : la plupart des fournisseurs de IaaS susmentionnés ont des offres PaaS, ou encore Clever Cloud, Google App Engine, Heroku, Microsoft Azure App Services, Platform.sh, etc.
- *Software as a Service* (SaaS), qui permet d'utiliser des applications logicielles en ligne sans avoir à en gérer l'infrastructure (par exemple : la plus part des fournisseurs de PaaS susmentionnés offrent aussi des services SaaS, ou encore Brevo, Citadel, Google Workspace, Microsoft 365, Nameshield Salesforce, Tixeo, Whaller, etc.).

D'autres modèles d'offres sur le *cloud* existent, tels que les *Containers-as-a-Service* (CaaS) qui visent à déployer et gérer des applications conteneurisées sur une infrastructure *cloud* en se libérant de la gestion des serveurs sous-jacents [1].

La responsabilité partagée

La responsabilité partagée sur le *cloud* désigne la répartition des tâches de sécurité et de gestion entre le fournisseur de services *cloud* et le client.

Les différents modèles de services *cloud* présentent des niveaux de menace variés en fonction de leur nature et des responsabilités partagées entre le fournisseur de services *cloud* et l'utilisateur. Dans le cas d'une offre de service IaaS, le fournisseur gère l'infrastructure (serveurs, réseaux, stockage), tandis que l'utilisateur est responsable des systèmes d'exploitation, des applications et des données. Pour une offre de service PaaS, le fournisseur gère la plateforme et l'infrastructure sous-jacente, l'utilisateur est responsable des applications développées et des données. Enfin, un fournisseur de SaaS prend en charge l'ensemble de l'infrastructure, de la plateforme et des applications, tandis que l'utilisateur est responsable de la gestion de ses données et des utilisateurs. Le fournisseur met néanmoins à disposition les outils et mécanismes nécessaires pour gérer ces accès de manière sécurisée.

Du fait de la diversité des services *cloud* proposés, ce cadre théorique est en pratique souvent complexifié. En effet, il est possible depuis plusieurs années de bâtir un système d'information ou une application en « kit », reposant sur l'empilement et l'assemblage de briques disponibles sur étagère, où chacunes d'entre elles fournissent un service spécialisé « clé en main » en fonction du niveau de délégation recherché (par ex. base de données, *front-end*, *back-end*, *pipeline* de traitements, stockage, lacs de données, tableaux de bords, gestion des identités, etc). Selon les besoins, ces briques peuvent être fournies par un même CSP ou issues de la combinaison de services proposés par plusieurs CSP. Un défaut de configuration unitaire ou une mauvaise sécurisation de leur interfaçage sont susceptibles de créer de nouvelles opportunités pour les attaquants.

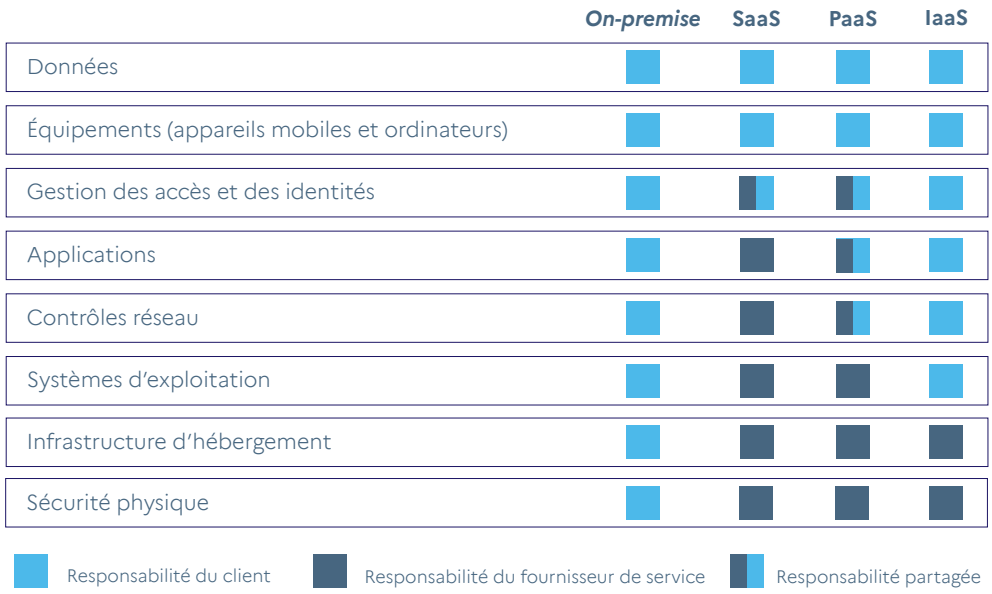

FIGURE 1 – Principes de la responsabilité partagée (production : ANSSI) [4, 5]

En s'appuyant sur les principes de la responsabilité partagée, cet état de la menace distingue la menace ciblant les opérateurs de services *cloud*, de la menace ciblant leurs clients.

2.2 Champ d'étude et surface d'attaque dans le *cloud*

Typologies des menaces contre le *cloud*

Le *cloud*, en tant que composante centrale de la transformation numérique, attire l'attention d'une variété d'acteurs malveillants. Les cybercriminels motivés par des objectifs lucratifs ciblent les environnements *cloud* à des fins de vol de données d'authentification, d'extorsion aux données volées, de déploiement de rançongiciel et de cryptominage. Des modes opératoires d'attaque réputés liés à des États sont utilisés pour cibler des environnements *cloud* à des fins d'espionnage, mais également de déstabilisation au travers d'attaques par déni de service distribué (DDoS) ou le sabotage des environnements *cloud* ciblés. Des groupes hacktivistes ciblent également les infrastructures *cloud* au moyen d'attaques par DDoS.

D'une manière générale, l'ANSSI constate un intérêt grandissant des attaquants pour la compromission des environnements *cloud*. En premier lieu, cette augmentation est le résultat de la multiplication des environnements hybrides, basés sur des infrastructures *on-premise* et *cloud*, offrant davantage d'opportunités de latéralisation aux attaquants. En second lieu, c'est également la conséquence d'un attrait grandissant des attaquants pour des environnements *cloud* avec lesquels ils semblent gagner en expertise, qui présenteraient davantage de failles de configurations et sur lesquels les défenseurs pourraient manquer de visibilité [6, 7]. La compromission des environnements *cloud* semble accessible à des MOA disposant de capacités variables. Au contraire des infrastructures *on-premise* qui diffèrent selon les organisations, la relative standardisation des environnements *cloud* faciliterait notamment les campagnes d'attaques des opérateurs de MOA disposant d'une bonne connaissance de la documentation publique sur le *cloud*, mise à disposition par les fournisseurs de services *cloud* eux-mêmes.

Quelle surface d'attaque sur le *cloud* ?

La surface d'attaque sur le *cloud* est vaste, notamment en raison des nombreux points d'entrées et de latéralisation exploitables par des attaquants :

- les interfaces de gestion, telles que les portails Web et les API utilisées pour administrer les ressources *cloud*, sont des cibles de choix ;
- les vulnérabilités logicielles dans les systèmes d'exploitation, les hyperviseurs, les conteneurs, les plateformes de gestion et les services *cloud* eux-mêmes peuvent être exploitées si elles ne sont pas corrigées ;
- les mauvaises pratiques de gestion des accès et des identités, comme l'utilisation de mots de passe faibles ou l'exposition d'interfaces d'authentification en l'absence d'authentification mutli-facteur (MFA), peuvent permettre à un attaquant de s'introduire dans le système et d'élever ses privilèges ;
- les erreurs de configuration dans les services *cloud*, telles que des permissions excessives sur les bases de données, le stockage ou les ressources réseau, peuvent également exposer des données sensibles à un accès non autorisé ;
- les dépendances avec des tiers, comme des fournisseurs de services ou des applications tierces intégrées au *cloud*, peuvent également être exploitées si ces fournisseurs sont compromis.

Malgré l'étendue et la diversité de ces vecteurs d'attaques, il apparaît que certaines techniques sont particulièrement récurrentes pour obtenir un accès initial sur des environnements *cloud*. Selon GOOGLE CLOUD, en 2023, 51,1% des accès initiaux sur le *cloud* ont été obtenus suite à l'exploitation d'interface *cloud* sans mots de passe ou dotés d'un mot de passe faible, tandis qu'une étude de la société THALES pointe les erreurs humaines et les problèmes de configuration comme premiers responsables de compromissions sur le *cloud* entre 2023 et 2024 (31% des compromissions), suivis par l'exploitation de vulnérabilités (28% des compromissions) [6, 8].

2.3 Enjeux de protection face à l'application de lois-extraterritoriales

Le recours à un service de *cloud* opéré par un prestataire non européen présente plusieurs risques spécifiques, liés à l'application de lois à portée extraterritoriales. De telles lois imposent, en effet, aux hébergeurs l'obligation de transmettre à leurs autorités les données de leurs clients, sans voie de recours ou même d'information de ces derniers. Un risque qui porte dès lors sur

la confidentialité des données hébergées dans le *cloud*. Le seul chiffrement des données n'offre d'ailleurs pas une protection adéquate contre ces risques, dès lors que les clés de chiffrement sont également dans le *cloud* (ce qui est généralement le cas lorsque les données chiffrées font l'objet de traitement dans le *cloud*, et non d'un simple stockage).

Ainsi, certains hébergeurs sont soumis à des législations spécifiques telles que le *Cloud* Act (Clarifying Lawful Overseas Use of Data Act) et le FISA (Foreign Intelligence Surveillance Act) américains, ou encore à la loi sur le renseignement chinois, permettant aux autorités de ces pays d'accéder aux données conservées dans le *cloud*, y compris en dehors de leurs territoires [9, 10]. Pour répondre à cette menace, la version 3.2 du référentiel d'exigences pour les prestataires de services d'informatique en nuage SecNumCloud intègre des exigences assurant une protection face à l'application de ces lois extraterritoriales [11].

L'usage de services *cloud* étrangers peut également présenter des difficultés en matière de sécurité des données hébergées. Des différences de normes de sécurité, de transparence, ou l'absence de contrôle direct sur les infrastructures, peuvent en effet complexifier la gestion de la sécurité des infrastructures et des données. Par ailleurs, une telle situation peut également soulever des risques sur la disponibilité des données et applications hébergées dans le *cloud*, la fourniture de la prestation *cloud* étant dans ce cas potentiellement soumise à des restrictions à l'exportation ou à d'éventuelles sanctions, qui peuvent évoluer dans le temps. Il est indispensable d'évaluer ces risques au cas par cas.

En cohérence avec les recommandations de l'ANSSI pour l'hébergement de systèmes d'information sensibles dans le *cloud*, les clients de fournisseurs de services *cloud* doivent évaluer, selon la nature des données qu'ils souhaitent héberger et la typologie de menaces à laquelle ils peuvent être confrontées, quels sont les types de services *cloud* qu'ils peuvent envisager d'utiliser [1].

3 MENACES CIBLANT LES FOURNISSEURS ET OPÉRATEURS D'INFRASTRUCTURES CLOUD

Les opérateurs de services *cloud* sont ciblés par des attaquants poursuivant des finalités lucratives, d'espionnage et de déstabilisation. La compromission d'un fournisseur de service *cloud* peut octroyer un accès centralisé à des données sensibles, souvent en grande quantité, et offrir un point d'entrée unique vers de nouvelles victimes.

3.1 Attaques à des fins lucratives

Les attaquants poursuivant des finalités lucratives ciblent les opérateurs de services *cloud* à des fins d'extorsion par rançongiciel mais également dans l'objectif d'accéder à des secrets d'authentification permettant de se latéraliser vers des systèmes d'information (SI) en aval.

Attaques par rançongiciel

En portant atteinte à la confidentialité et à l'intégrité de leurs données, les opérateurs de rançongiciels constituent une menace d'importance majeure pour les fournisseurs de services *cloud*.

Incident ANSSI

En 2024, l'ANSSI a traité la compromission et le chiffrement du SI d'un opérateur de communications électroniques proposant différents services dont une solution PaaS. La compromission d'un équipement de sécurité de bordure PaloAlto vulnérable à la CVE-2024-3400, connu publiquement depuis le mois d'avril 2024, puis la latéralisation et les actions malveillantes qui s'en sont suivies ont entraîné l'indisponibilité des ressources du bénéficiaire et de ses clients durant plusieurs semaines.

En mai 2023, les systèmes d'information de SCANSOURCE, une société américaine spécialisée dans les services de migration sur le *cloud* et propriétaire du fournisseur de service *cloud* INTELISYS, auraient été compromis par les opérateurs du rançongiciel Cactus [12]. Les données volées ont ensuite été mises en vente sur le site de divulgation de données du groupe cybercriminel.

Dans un registre similaire, en août 2023, tous les serveurs, systèmes de sauvegardes inclus, de l'hébergeur danois CLOUDNORDIC auraient été compromis puis chiffrés, menant à la perte de la totalité des données clientes de l'entreprise. Pour compromettre l'intégralité des SI de CLOUDNORDIC, les attaquants auraient tiré profit d'une migration de serveurs effectuée par les équipes de la société durant l'été 2023. En effet, pendant cet intervalle de temps, les systèmes de gestion et de sauvegarde du prestataire auraient été temporairement installés sur un réseau partagé composé de serveurs potentiellement déjà compromis. La société AZEROCLOUD, liée à CLOUDNORDIC par la même maison mère CERTQA HOLDINGS, aurait également été compromise. À la suite de cet incident, les sociétés CLOUDNORDIC et AZEROCLOUD ont été contraintes de déposer le bilan [13, 14].

Incident ANSSI

En 2024, un opérateur de solution SaaS à destination de professionnels de santé a été ciblé par une attaque par rançongiciel contraignant ses clients à travailler dans un mode de fonctionnement dégradé pendant plusieurs jours. Le prestataire a été compromis au moyen du rançongiciel Lockbit 3.0 qui a causé l'indisponibilité de sa plateforme SaaS. Cette compromission était liée à l'exploitation d'un équipement de sécurité de bordure CITRIX NetScaler vulnérable à la CVE-2023-4966, qui a permis à l'attaquant de récupérer les informations d'authentification d'un compte utilisateur.

Vol de données d'authentification et compromission de la chaîne d'approvisionnement

Les attaquants motivés par des objectifs lucratifs s'intéressent également aux fournisseurs de services *cloud* parce qu'ils peuvent constituer des points d'entrée vers leurs clients. La compromission d'une de ces sociétés peut accroître les risques de vols de secrets d'authentification et les attaques par la chaîne d'approvisionnement. À cet égard les sociétés spécialisées en gestion d'accès et d'identité constituent des cibles privilégiées.

En janvier 2022, les opérateurs du groupe cybercriminel Lapsus$ se seraient introduits sur l'ordinateur professionnel d'un ingénieur de la société OKTA, spécialisée dans la gestion des identités. Cette intrusion aurait permis à l'attaquant de réinitialiser les mots de passe et les jetons d'authentification multifacteur (MFA) d'une partie des clients de l'entreprise. Selon un communiqué publié par OKTA, 2,5% des clients de la société, soit 366 entités, auraient été affectés par cette compromission [15].

Entre le 28 septembre et le 17 octobre 2023, l'entreprise OKTA a de nouveau été confrontée à un incident de sécurité. Un acteur malveillant, muni d'identifiants d'authentification volés et aux motivations inconnues, a pu accéder au système d'assistance client de la société. Cette intrusion aurait ensuite permis aux attaquants d'obtenir des fichiers d'archives HTTP (« .HAR ») téléversés par les clients de OKTA sur la plateforme compromise et dont certains contenaient des *cookies* et jetons de session. D'après OKTA, 134 clients auraient été affectés par cette campagne d'attaques [16, 17].

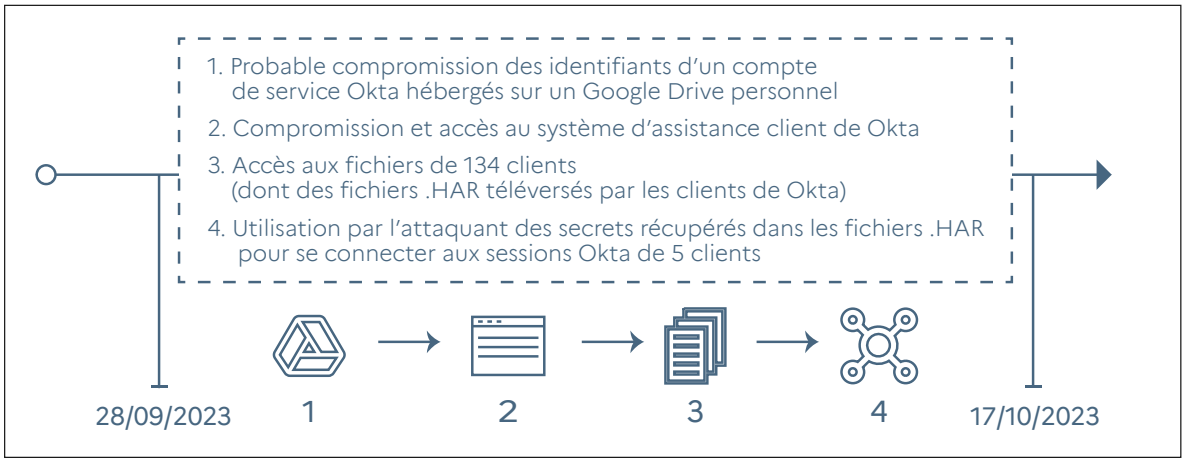

FIGURE 2 – MOA employé contre OKTA entre les mois de septembre et octobre 2023 (production : ANSSI)

La compromission d'OKTA en octobre 2023 aurait permis aux attaquants de se latéraliser vers les SI de CLOUDFLARE, un autre fournisseur de services *cloud* également client de OKTA[1].

Au-delà du vol de données d'authentification, la compromission d'un prestataire de service *cloud* rend également possibles les attaques sur la chaîne d'approvisionnement logicielle. En juin 2023, la société JUMPCLOUD, un prestataire de *cloud* en SaaS spécialisé en service de gestion d'identités et d'accès, aurait été ciblé puis compromis par les opérateurs du MOA réputé nord-coréen UNC4899. Après une campagne d'hameçonnage leur ayant octroyé un accès de niveau développeur, les opérateurs du MOA seraient parvenus à se latéraliser avant de diffuser une application JUMPCLOUD piégée vers certains clients de l'entité. D'après JUMPCLOUD, 10 machines dans 5 sociétés différentes auraient reçu la charge malveillante. Les attaquants, motivés par des objectifs lucratifs, cherchaient à compromettre des entités spécialisées dans le secteur des cryptomonnaies [20, 21, 22].

1. Grâce à la récupération de fichiers « .HAR », les opérateurs du MOA employé auraient utilisé un jeton d'accès et les identifiants de trois comptes de service pour accéder au wiki interne de l'entreprise et à une base de donnée de débogage. Cinq jours plus tard, ils auraient utilisé l'application ScriptRunner pour obtenir des moyens de persistance sur le *cloud* de l'entreprise, avant de s'introduire dans ses systèmes de gestion de code source et d'essayer, sans succès, d'accéder à un serveur de console [18]. Un autre client aurait observé une tentative de connexion à son *tenant* OKTA moins de trente minutes après le téléversement d'un fichier « .HAR » sur la plateforme d'OKTA compromise [19].

3.2 Attaques à des fins d'espionnage

Les fournisseurs de services *cloud* sont également des cibles pour des opérateurs de MOA sophistiqués poursuivant des objectifs d'espionnage. Entre 2023 et 2024, les services *cloud* de MICROSOFT auraient été ciblés puis compromis au moyen de deux MOA distincts : Storm-0558 réputé lié aux intérêts stratégiques chinois, et Midnight Blizzard (Nobelium), publiquement attribué au service de renseignement extérieur russe (SVR) [23].

Commentaire : dans ces deux cas de figure, les attaquants cherchaient à compromettre les SI de Microsoft en amont pour se latéraliser ou obtenir des informations sur des utilisateurs des services cloud de l'entreprise.

Compromission au moyen du MOA Storm-0558

En mai 2023, les opérateurs du MOA Storm-0558, réputé lié aux intérêts stratégiques chinois, auraient obtenu des accès aux boites messageries Microsoft Exchange Online de 500 individus liés à 22 entités différentes, dont certaines localisées aux États-Unis et au Royaume-Uni. Les messageries électroniques de représentants du Département d'État américain (*U.S. Department of State*), du Département du Commerce (*U.S. Department of Commerce*) ainsi que de la chambre des représentants (*U.S. House of Representatives*), dont les fonctions ont trait aux relations bilatérales sino-américaines, auraient été compromises. Lors de cet incident, l'obtention d'une clé de signature client MSA (Microsoft Account)[2] datant de 2016[3] aurait permis aux opérateurs de Storm-0558 d'obtenir un accès potentiel à n'importe quel compte Exchange Online dans le monde [24, 25].

FIGURE 3 – Emploi du MOA Storm-0558 contre MICROSOFT entre 2021 et 2023 (production : ANSSI)

Selon le département de la sécurité intérieure américain (*Department of Homeland Security*), cet incident a mis en évidence les failles de sécurisation et de configuration du *cloud* de MICROSOFT, dont l'absence de systèmes d'alerte pour les clés trop anciennes, la possibilité de créer de faux jetons non générés avec les algorithmes internes de l'entreprise et enfin, l'absence de journalisation et données nécessaires aux investigations pour expliquer le vol de la clé de signature client MSA en 2016 [25].

2. Clé de signature client utilisée pour valider les jetons d'authentification sur les services *cloud* de MICROSOFT.
3. La principale hypothèse retenue par MICROSOFT implique la récupération de cette clé dans un journal de plantage (*crash dump*) advenu au cours d'une attaque menée contre Microsoft en 2021. Toutefois, malgré ses recherches, l'éditeur américain n'est pas parvenu à récupérer de journal de plantage contenant cette clé [24].

Compromission au moyen du MOA Nobelium

Au mois de janvier 2024, les opérateurs du MOA réputés liés aux intérêts stratégiques russes Nobelium auraient mis en œuvre des techniques de *password-spraying* ciblées contre un nombre limité de comptes Microsoft Exchange Online d'employés de MICROSOFT, avant de parvenir à compromettre un compte de test disposant de privilèges élevés mais sans authentification multifacteur activée. Ils seraient ensuite parvenus à élever leurs privilèges pour accéder aux comptes courriels Office 365 Exchange de l'entreprise. À la suite de cette campagne d'attaques, des répertoires contenant des éléments du code source de MICROSOFT ainsi que les systèmes d'information internes de l'entreprise auraient été compromis [26].

Les informations exfiltrées au cours de cette intrusion auraient ensuite été utilisées par l'attaquant pour se latéraliser vers de nouvelles interfaces *cloud*. Les opérateurs du MOA auraient notamment exfiltré des secrets échangés entre MICROSOFT et ses clients par courriel [27].

Exploitation de vulnérabilités

L'exploitation de vulnérabilités constitue un levier couramment utilisé par des MOA réputés liés à des États pour cibler le secteur du *cloud computing*. En septembre 2022, des médias japonais ont rapporté le ciblage et la compromission de l'entreprise japonaise FUJITSU, qui fournit notamment des services *cloud*, à la suite de l'exploitation d'une vulnérabilité touchant l'équilibreur de charge (*load balancer*) de la société. D'après des médias japonais, le délai d'une semaine entre la publication de la vulnérabilité et l'application d'un correctif a rendu possible l'exploitation de la vulnérabilité et la compromission de FUJITSU [28]. Le nom du MOA employé lors de cette attaque n'a pas été partagé publiquement.

Ces compromissions peuvent également impliquer l'usage de vulnérabilités jour-0[4]. En 2024, le fournisseur de services *cloud* RACKSPACE aurait fait l'objet d'une compromission causée par l'exploitation d'une vulnérabilité sur un programme hébergé sur les serveurs Web internes mais vendu par le fournisseur de logiciels et de services SCIENCELOGIC. Ce programme servait à la surveillance des systèmes et à la fourniture d'un tableau de bord aux clients de RACKSPACE. Après l'exploitation de la vulnérabilité, les attaquants seraient parvenus à s'introduire sur trois serveurs Web de la société et auraient exfiltré des informations sur les clients de l'entreprise, incluant : les noms et numéros de compte client, les identifiants de clientèle, les adresse IP des appareils clients et des identifiants de connexion chiffrés[5] [29].

Commentaire : l'ANSSI n'a pas connaissance du nom et des objectifs du mode opératoire utilisé lors la compromission de RACKSPACE mais les données exfiltrées et l'utilisation d'une vulnérabilité jour-0 pourrait indiquer l'emploi d'un MOA lié aux intérêts stratégiques d'un État à des fins d'espionnage ciblé. Le vol de secrets clients depuis les systèmes d'information de l'entreprise aurait pu permettre à l'attaquant de se latéraliser sur les environnements des clients de RACKSPACE.

3.3 Attaques à des fins de déstabilisation par déni de service

En 2024, de nombreux opérateurs *cloud* ont été confrontés à des attaques par déni de service (DoS/DDoS) atteignant des intensités toujours plus importantes. Plusieurs CSP ont partagé au

4. Vulnérabilités n'ayant pas encore été rendue publiques au moment de leur exploitation.
5. Par un outil interne de RACKSPACE.

cours de cette année des retours d'expérience permettant d'apprécier leur ampleur et leurs spécificités.

A titre d'exemple au niveau réseau (couche 3-4 du modèle OSI), OVH a mis en avant le rôle joué par certains équipements de cœur de réseau détournés à des fins de saturation [30]. De son côté, Cloudflare a décrit une attaque impliquant plus d'une dizaine de millier d'équipements de type internet des objets (IoT) compromis [31]. Ces deux CSP rappellent ainsi que ces attaques peuvent être volumétriques tant par leur taille de trafic que par leur nombre très important de paquets réseau à traiter.

L'ANSSI constate que les attaques DDoS ciblant la couche applicative (couche 7 du modèle OSI) sont fréquentes, celles-ci sont décrites plus bas.

4 MENACES CIBLANT LES CLIENTS DE SERVICES CLOUD

Les attaques contre les clients de services *cloud* peuvent entraîner des compromissions de données sensibles, de l'extorsion *via* rançongiciel et des perturbations plus ou moins importantes de service. Les outils spécialisés en gestion des accès et des identités ainsi que les applications de messagerie et de travail collaboratif sont particulièrement ciblés.

4.1 Attaques à des fins lucratives

Attaques menées au moyen de secrets d'authentification volés

Le vol de données sur le *cloud* expose les entreprises à des risques majeurs, qu'il s'agisse de données sensibles ou de secrets d'authentification. D'après la société THALES, 47% des données professionnelles hébergées sur le *cloud* peuvent être considérées comme sensibles [6], tandis que 44% des organisations ont déjà subi une fuite de donnée *cloud* [8].

Les causes de ces fuites de données sont nombreuses. Une base de données mal sécurisée peut permettre à des attaquants d'accéder à des informations confidentielles (comme des informations financières ou personnelles) en exploitant des failles de sécurité, telles que des mots de passe faibles ou des permissions mal configurées. Par exemple, un espace de stockage de type *bucket* S3 mal configuré peut entraîner une fuite de données sensibles si les règles de partage sont trop permissives, rendant les fichiers accessibles à toute personne disposant d'un lien direct. Des mauvaises configurations découvertes en juin 2023 dans le *cloud* de TOYOTA MOTOR auraient exposé pendant huit ans les données de plus de 260 000 clients de l'entreprise [32]. De la même façon, en novembre 2023, le plus grand fournisseur d'énergie slovène aurait été compromis suite à un vol de mot de passe exposé sur une instance de stockage *cloud* non protégée [33]. Les secrets d'authentification comme les clés API non protégées peuvent également être récupérés et utilisés pour accéder aux services *cloud*, notamment des bases de données ou des applications critiques.

6. La sensibilité mentionnée par l'étude de THALES ne correspond pas à la notion de SI sensibles retenue dans les recommandations pour l'hébergement des SI sensibles dans le cloud publiées en juillet 2024 [1]. L'évaluation de la sensibilité des données impose une analyse de risques nécessaire à l'identification des protections adaptées aux menaces pouvant cibler une organisation.

Les secrets d'authentification de ces interfaces sur le *cloud* peuvent ensuite servir à des attaques de plus grande ampleur. En juin 2024, l'éditeur MANDIANT a rapporté le ciblage systématique d'instances clientes SNOWFLAKE, une plateforme de stockage de données dans le *cloud*, par les opérateurs du MOA UNC5537 [34]. Plusieurs intrusions sur des instances SNOWFLAKE auraient été observées sans que les SI de SNOWFLAKE n'aient été compromis au préalable. D'après MANDIANT, les opérateurs de UNC5537 auraient obtenu des identifiants d'accès d'utilisateurs de SNOWFLAKE, volés suite à l'usage de plusieurs *infostealers*[7]. Plus de 165 organisations auraient été exposées à un risque de compromission lié à ces vols de données d'authentification. D'après l'éditeur, la majorité des comptes compromis n'utilisaient pas de mécanisme d'authentification multifacteur tandis que les données récupérées par les *infostealers* dataient parfois de 2020. Dans certains cas, les utilisateurs des *infostealers* seraient parvenus à voler des identifiants de connexion suite à des usages personnels d'un ordinateur professionnel [34].

Commentaire : cette chaîne de compromission met en lumière le rôle des infostealers comme outils privilégiés de la menace cybercriminelle et l'importance de la supervision de toute potentielle fuite de données d'authentification, même après plusieurs années. Au moins une société française a indiqué à l'ANSSI avoir détecté des activités malveillantes sur une de ses instances SNOWFLAKE.

Latéralisation des environnements *on-premise* vers le *cloud*

L'émergence d'infrastructures hybrides composées à la fois d'infrastructure *on-premise* et sur le *cloud* augmente le nombre de vecteurs d'entrées et de latéralisation potentiels. Les problèmes de configuration entraînés par ces nouveaux types de SI sont exploités par des groupes d'attaquants dont les compétences en matière d'intrusion informatique sur le *cloud* ont également augmenté.

Depuis 2022, le groupe cybercriminel Scattered Spider (également documenté sous les noms de Octo Tempest, UNC3944, Muddled Libra) a exploité à plusieurs reprises des problèmes de configuration entre des environnements *on-premise* et *cloud* pour se latéraliser de l'un à l'autre. Les erreurs de configuration de « Microsoft Entra ID Connect », passerelle entre les *Active Directory* (AD) locaux et le service Entra Connect vers le *cloud*, sont particulièrement ciblées[8] [7].

Dans d'autres contextes, des opérateurs de Scattered Spider ont employé des techniques d'ingénierie sociale avancées pour compromettre les infrastructure *cloud* de leurs cibles. Ils auraient, à plusieurs reprises, contacté par téléphone le support technique des entreprises ciblées en usurpant l'identité d'un employé à haut privilège et demandé ensuite la réinitialisation des mots de passe administrateur. Dans le cadre de leur campagne d'hameçonnage, ils auraient également créé des noms de domaine usurpant l'identité de fournisseurs de services PaaS et SaaS, tel que SERVICENOW, pour récolter des identifiants de connexion [35].

En 2024, les opérateurs du MOA cybercriminel Storm-0501, utilisateurs de plusieurs rançongiciels dont Hive, BlackCat ou LockBit, se sont également latéralisés vers des environnements *cloud* après avoir obtenu un accès aux environnements *on-premise* de leur victime. Ils obtiendraient de premiers accès initiaux en utilisant des identifiants d'authentification volés ou en exploitant des vulnérabilités connues d'équipements exposés sur internet. Une fois l'environnement *on-premise* compromis, les opérateurs de Storm-0501 exploiteraient des identifiants d'accès au compte Microsoft Entra ID collectés sur les SI *on-premise* ou en compromettant un compte *on-premise* disposant d'un compte miroir sur le *cloud* sans double-authentification activée. Une

7. Un *infostealer* est un type de code malveillant conçu pour voler des informations sensibles telles que des identifiants de connexion, des données bancaires ou des informations personnelles.

8. Entra Connect (anciennement Azure AD Connect) est un outil utilisé pour synchroniser des identités *on-premise* avec Microsoft Entra ID (anciennement Azure AD), la solution de gestion des accès et des identités sur le *cloud* de MICROSOFT.

fois l'environnement *cloud* de la victime totalement compromis, les opérateurs de Storm-0501 y déposeraient une porte dérobée [36].

Commentaire : ces TTP ne sont pas exclusives aux MOA utilisés à des fins lucratives. Elles sont également susceptibles d'être utilisés par les opérateurs de MOA motivés par des finalités d'espionnage ou de déstabilisation.

Extorsion aux données volées

Les attaques à des fins d'extorsion sur le *cloud* n'impliquent pas nécessairement le chiffrement de données. Dans certains cas de figure les attaquants procèdent à l'exfiltration et à la suppression des données sur le *cloud* avant de demander une rançon à la victime en échange de la récupération des données volées. Dans un cas rapporté par l'éditeur de sécurité INVICTUS en 2024, l'attaquant aurait exfiltré les données d'un espace de stockage bucket S3 avant de procéder à leur suppression et de déposer une note de rançon [37].

Détournement de ressources et nouvelles tendances

Les applications de virtualisation sont régulièrement ciblées dans l'objectif d'y déposer des cryptomineurs. Ces codes malveillants, utilisés pour miner des cryptomonnaies depuis des infrastructures compromises mais légitimes, sont responsables d'une consommation de ressources excessive au détriment des machines virtuelles s'exécutant légitimement sur l'équipement.

Incident ANSSI

Le dépôt d'un cryptomineur a été observé dans le cadre de plusieurs compromissions récentes dont celle d'une machine appartenant à une entreprise française d'infogérance proposant des services *cloud*. Le ralentissement des machines virtuelles des clients a été à l'origine de la détection du code malveillant.

Les opérateurs du MOA TeamTNT seraient spécialisés dans ce domaine et ciblent de manière opportuniste des solutions de virtualisation exposées sur Internet. En octobre 2024, l'éditeur AQUASEC a rapporté l'utilisation par les opérateurs du MOA de serveurs Web et de registres Docker Hub (service de gestion d'images docker) compromis pour distribuer l'outil d'intrusion Sliver ainsi que des cryptomineurs [38].

Incident ANSSI

En janvier 2023, les opérateurs du MOA TeamTNT auraient compromis une partie de l'environnement *cloud* d'une entreprise française du secteur de la santé dans l'objectif d'y déposer des cryptomineurs. Après un premier accès initial depuis un serveur hôte de conteneur docker exposé sur Internet, les opérateurs du MOA se sont latéralisés sur l'infrastructure *cloud* de la victime et ont créé quatre nouvelles machines virtuelles dédiées au minage de cryptomonnaies.

En parallèle de l'usage de cryptomineurs, une nouvelle pratique impliquant le détournement de modèles de langage[9] sur le *cloud* et mieux connue sous le nom de *LLM hijacking* (*large language model*) s'est développée. Elle désigne l'utilisation illégale d'un modèle de langage hébergé sur le

9. Un modèle de langage est un modèle d'intelligence artificielle basé sur l'apprentissage. Son fonctionnement entraîne une consommation importante de ressources informatiques et matérielles.

cloud, souvent *via* des identifiants volés, pour exploiter ses ressources à des fins malveillantes, entraînant des coûts élevés et des risques pour la sécurité des entités compromises.

Les coûts associés au LLM *Hijacking* sont élevés car les attaquants utilisent des modèles de langage basés sur des services *cloud*. Ces derniers génèrent des frais liés à l'utilisation des ressources (calculs, stockage, etc.), ils peuvent dépasser les 100 000$ par jour avec des modèles avancés comme Claude 3 Opus. La société SYSDIG a observé une augmentation du nombre et du niveau de sophistication de ce type d'attaques [39].

4.2 Attaques à des fins d'espionnage

Les technologies *cloud* sont également ciblées par des attaquants à la recherche de renseignements d'intérêt.

Selon un rapport de MICROSOFT, les opérateurs du MOA Nobelium ont ciblé à plusieurs reprises les clients de services *cloud* à des fins de récolte d'identifiants de connexion et pour obtenir des accès administrateurs aux serveurs *Active Directory Federation Services* (ADFS)[10] ciblés. Dans un cas observé par MICROSOFT en 2021, les opérateurs de ce MOA seraient parvenus à se latéraliser d'un environnement client *cloud* vers son environnement *on-premise* en utilisant des services Microsoft Azure[11] pour se latéraliser vers les machines virtuelles de la victime [40].

Les opérations menées au moyen du MOA Nobelium se traduisent aussi par la compromission de comptes de messagerie électronique sur le *cloud*. En 2023, ce MOA aurait été utilisé pour cibler et compromettre les environnements de messagerie *cloud* de l'entreprise HEWLETT PACKARD ENTERPRISE. Les attaquants auraient obtenu un accès à la messagerie électronique de certains employés de l'entreprise, dont certains étaient spécialistes en cybersécurité. Cette intrusion serait liée à une première compromission ayant impliqué l'exfiltration de plusieurs fichiers du serveur de partage de fichiers SharePoint de l'entreprise. Si les motivations des attaquants demeurent inconnues, ceux-ci auraient pu chercher à obtenir des informations relatives aux produits HP dans le but d'améliorer leurs capacités offensives [23].

Incident ANSSI

Au cours d'investigations sur des cas de compromission de comptes de messagerie OFFICE 365, l'ANSSI a pu observer à plusieurs reprises que les attaquants, pour maintenir le plus longtemps possible leurs accès frauduleux, avaient ajouté des adresses courriels de secours, généré de jetons de secours à usage unique, enregistré des identifiants ou des équipements de confiance additionnels, voire activé des règles de transfert automatique de courriels. Ces actions rendent de fait inopérante l'éviction de l'acteur malveillant *via* la seule mise en place d'une politique d'authentification multi-facteurs.

Plus récemment, en octobre 2023, l'agence spatiale japonaise, la JAPAN AEROSPACE EXPLORATION AGENCY (JAXA), aurait été touchée par une campagne d'attaques ayant mené à la compromission de ses services *cloud* O365. Les opérateurs du MOA employé auraient d'abord exploité une vulnérabilité contre le VPN de la JAXA avant de se latéraliser pour compromettre son environnement O365. Des informations personnelles appartenant à des employés de la société

10. ADFS est une fonctionnalité permettant aux ordinateurs clients d'un réseau d'accèder à travers Internet et *via* un partage d'identité, aux applications et services situés en dehors du réseau de l'entité.
11. Azure RunCommand couplé à Azure admin-on-behalf-of (AOBO).

pourraient avoir été compromises ainsi que certaines données ayant trait aux activités de l'entité avec des organisations externes et dont les noms n'ont pas été divulgués [41, 42]. L'ANSSI n'a pas connaissance du nom du MOA utilisé lors de cette campagne d'attaques.

Les attaquants s'emploient à rechercher la furtivité lors de leurs tentatives d'intrusion sur le *cloud*. L'utilisation de réseaux d'anonymisation et d'outils de tunnelisation de trafic disponibles en sources ouvertes, sont de nouveaux facteurs complexifiant la détection d'intrusion sur le *cloud*. Les équipes de GOOGLE CLOUD auraient observé des opérateurs de MOA réputés liées à la Chine s'introduire dans des environnements *cloud* en utilisant des techniques pour se dissimuler dans le trafic réseau légitime et ainsi complexifier la détection [6].

Commentaire : l'ANSSI constate également un intérêt grandissant des opérateurs de MOA réputés liés aux intérêts chinois pour les environnements cloud, notamment par l'usage d'outils disponibles en sources ouvertes adaptés à des opérations de reconnaissance et de compromission des environnements cloud.

Incident ANSSI

L'ANSSI a récemment traité des cas de compromission d'environnement *cloud* servant d'une part, à compromettre les informations de l'entité ciblée et d'autre part, à atteindre des entités d'intérêt notamment *via* l'envoi de courriels d'hameçonnage depuis les comptes de messagerie électronique compromis.

4.3 Attaques à des fins de déstabilisation

Des interfaces *cloud* clientes peuvent également être ciblées à des fins de déstabilisation. En juillet 2022, le MOA Mango Sandstorm, réputé lié au ministère du Renseignement de la république islamique d'Iran, aurait été utilisé pour chiffrer et détruire les environnements *on-premise* et *cloud* de plusieurs entités israéliennes. Après avoir compromis des serveurs non mis-à-jour, notamment *via* l'exploitation de la vulnérabilité Log4Shell, les attaquants se seraient latéralisés sur le *cloud* grâce au service AdSync et en exploitant les comptes utilisateurs ADConnect et AADconnect. Ils auraient ensuite procédé à la destruction totale de l'environnement Azure en supprimant des fermes de serveurs, des machines virtuelles, des comptes de stockage et des réseaux virtuels. Enfin les attaquants auraient utilisé leur accès au compte de messagerie de l'entité compromise pour envoyer des campagnes d'hameçonnage depuis les comptes de la victime [7].

Le MOA Volt Typhoon, réputé lié à la Chine et utilisé pour compromettre des infrastructures critiques potentiellement à des fins de prépositionnement, voire de déstabilisation, aurait également été employé pour cibler des environnements *cloud*. La CISA a publié des éléments mentionnant une tentative de latéralisation de l'attaquant d'un environnement *on-premise* vers un environnement *cloud* [43].

Commentaire : une intrusion sur un environnement cloud octroie potentiellement à un attaquant un accès complet aux systèmes de l'entité compromise ; la poursuite d'objectifs de déstabilisation, en particulier via la suppression des données de l'environnement, peut donc s'avérer particulièrement dévastatrice pour l'entité ciblée.

Attaque par déni de service distribué contre la couche 7

L'ANSSI constate que les attaques DDoS ciblant la couche applicative (couche 7 du modèle OSI) sont fréquentes. À titre d'exemple, CLOUDFLARE met en avant sur son périmètre que le nombre d'attaques visant la couche HTTP a été supérieur à celui visant les couches 3 et 4[31].

Ces attaques reposent sur le principe qu'une application, pour satisfaire une demande, va devoir effectuer des traitements et souvent renvoyer une réponse plus conséquente que la demande reçue. Ainsi, les applications devant effectuer des traitements lourds ou ne sachant traiter qu'un faible nombre de demandes en parallèles sont particulièrement vulnérables. Pour réaliser une telle saturation, un attaquant n'a généralement pas besoin d'émettre beaucoup de trafic réseau (couche 3 et 4), ne déclenchant par conséquent pas les mesures anti-DDoS spécifiques à la protection de ces couches réseau. Or, l'ANSSI constate que nombre de clients CSP ignorent encore ces limites et ne prennent pas suffisamment en compte cet enjeu dans leurs développements applicatifs et dans le choix des mesures de sécurité additionnelles permettant d'y faire face.

Menaces internes

Les menaces internes, opérées par des employés mécontents ou motivés par des objectifs lucratifs, sont également susceptibles de cibler les infrastructures *cloud* de leurs organisations. Celles-ci sont souvent accessibles à distance et un employé ou sous-traitant peut donc causer des dégâts considérables. En 2023, un employé de la banque américaine FIRST REPUBLIC a ainsi été condamné à 24 mois de prison pour avoir porté atteinte à l'environnement *cloud* de son entreprise ainsi que pour avoir volé du code source de valeur. Il aurait notamment supprimé des répertoires de code source internes, exécuté un script malveillant pour effacer les journaux, laissé des moqueries à l'intention de ses anciens collègues dans le code source de la banque et usurpé l'identité d'autres employés en ouvrant des sessions à leur nom [44].

5 MENACES CIBLANT LES APPLICATIONS DE VIRTUALISATION ET COMPOSANTS DE GESTION MATÉRIELLE

5.1 Définitions

La plupart des services *cloud* repose sur la mise en œuvre de technologies de virtualisation. Ces technologies permettent la cohabitation des usages en créant une couche d'abstraction au dessus des ressources matérielles tout en dynamisant et en optimisant leur utilisation. Il existe différents types et technologies de virtualisation selon les niveaux d'abstraction souhaités (fonction, applicatif, service, conteneur, micro machine virtuelle, machine virtuelle, etc). Ils n'offrent pas nécessairement les mêmes niveaux et garanties de sécurité, notamment en matière de cloisonnement. Certaines compétitions de recherche de vulnérabilités, comme le PWN2OWN, ont déjà mis en évidence le ciblage de ces technologies [45]. Elles mettent régulièrement en lumière des cas d'exploitation réussies de vulnérabilités. En outre, des vulnérabilités sur ce type de technologie sont parfois exploitées : le *patch Tuesday* de janvier 2025 a mis en évidence la correction de vulnérabilités activement exploitées affectant des hyperviseurs Hyper-v [46].

Par ailleurs, les ressources matérielles, notamment les serveurs, sont généralement équipés de composants de gestion matérielle permettant de les piloter à distance (gestion de l'alimentation, surveillance des capteurs, mises à jour des micrologiciels, mode de démarrage, etc.). La compromission de ces équipements ou des infrastructures les pilotant peut générer des problèmes en matière d'indisponibilité et d'intégrité des services hébergés, et dans certains cas, des atteintes significatives sur la confidentialité. En 2023, des attaquants motivés par des objectifs de déstabilisation, auraient ciblé puis détruit les serveurs iDRAC [12] (*Integrated Dell Remote Access Controller*) d'un hébergeur israélien [47].

Ces technologies sont donc des cibles de choix du fait de la cohabitation des activités, données et clients. Les scénarios les plus couramment redoutés sont :

- qu'une ressource virtualisée malveillante puisse nuire à d'autres ressources virtualisées mitoyennes ;
- que le système assurant la virtualisation soit compromis, mettant à mal les ressources virtualisées hébergées ;
- que le système d'orchestration puisse être compromis, mettant à mal un ensemble de systèmes assurant la virtualisation.

5.2 Attaques à des fins lucratives

Les technologies de virtualisation et d'hypervision sont ciblées par des opérateurs de rançongiciels ayant adapté leur arsenal à ces environnements, notamment en développant des rançongiciels spécialement conçus pour chiffrer les environnements VMWare.

En 2023, les opérateurs du MOA Scattered Spider auraient par exemple utilisé des accès au portail client de la société MGM CASINOS pour se latéraliser sur l'environnement *cloud* de l'entreprise et procéder, à l'aide du rançongiciel BlackCat, au chiffrement des 100 hyperviseurs ESXi de son réseau. Les attaquants seraient également parvenus à exfiltrer les données de la société dont les pertes sèches pendant cet incident se seraient élevées à 8,4 millions de dollars par jour [48].

Cette même année, les opérateurs du rançongiciel ESXiArgs auraient exploité la CVE-2021-21974 affectant le protocole OpenSLP de VMWare ESXi, pour compromettre et chiffrer plusieurs milliers de serveurs hyperviseurs [49].

5.3 Attaques à des fins d'espionnage

D'autres campagnes d'attaques témoignent du ciblage des ces technologies à des fins d'espionnage. Par exemple, les opérateurs du MOA réputé lié aux intérêts chinois UNC3886 auraient exploité la vulnérabilité jour-0 CVE-2023-34048, affectant le produit VMware vCenter, une plateforme de gestion centralisée pour administrer, configurer et administrer les environnements virtuels, pour cibler plusieurs entités considérées comme « stratégiques » par l'éditeur GOOGLE CLOUD [50]. Les premiers signes de l'exploitation de cette vulnérabilité en tant que jour-0 par l'attaquant remonteraient à 2021. Outre la CVE-2023-34048, les opérateurs de ce MOA auraient exploité pas moins de trois vulnérabilités jour-0 supplémentaires au cours de cet incident. Les

12. Un serveur iDRAC facilite la gestion à distance de serveurs Dell en offrant des outils de surveillance, de diagnostic et de gestion du matériel.

opérateurs de ce MOA auraient utilisé de services d'hébergement *cloud* pour leurs activités de commande et de contrôle (C2) [50].

6 LE CLOUD COMME INFRASTRUCTURE DES ATTAQUANTS

Les attaquants ont massivement intégré à leur campagnes d'attaques l'usage d'infrastructures situées dans le *cloud* (serveurs privés virtuels notamment) louées auprès d'hébergeurs de services *cloud*.

Les services *cloud* peuvent également être utilisés en tant qu'infrastructure d'attaque par les opérateurs des MOA qui les utilisent. L'emploi de services *cloud* à ces fins permet aux attaquants d'héberger leur arsenal d'outils malveillants de manière plus durable et d'exfiltrer des données volées en limitant les risques de détection. D'après l'éditeur NETSKOPE, en mars 2023, 58% des codes malveillants observés lors de compromissions auraient été téléchargés depuis une application *cloud* légitime [51].

En 2024, les opérateurs du MOA lié aux intérêts stratégiques nord-coréens Kimsuky, auraient utilisé Microsoft OneDrive et Google Drive comme infrastructure de stockage et de C2. StarCruft, un autre MOA nord-coréen, partagerait ces TTP en utilisant notamment de l'infrastructure PCLOUD, un service d'hébergement et de stockage sur le *cloud*, à des fins de C2 [52].

Incident ANSSI

Lors d'un cas récent de compromission affectant une société de services numériques, un développeur travaillant au sein de l'entité a notamment été contacté via une plateforme de travail *free-lance* et incité à télécharger du code malveillant en dissimulant les flux *via* l'API GitHub à destination d'un compte créé par l'attaquant.

L'API Microsoft Graph, utilisée de manière légitime pour accéder aux ressources de Microsoft Cloud, est également employée par plusieurs attaquants à des fins de C2 et d'exfiltration. Ainsi, la porte dérobée GoGra, utilisée en novembre 2023 contre une organisation sud-asiatique à des fins d'espionnage, utiliserait l'API Microsoft Graph pour interagir avec son serveur C2 hébergé sur des services Microsoft Mail. Une autre porte dérobée, baptisée Onedrivetools, utiliserait l'API Microsoft Graph pour télécharger une seconde charge utile hébergée sur OneDrive. Selon SYMANTEC, Onedrivetools aurait été utilisée pour cibler des entreprises des services numériques en Europe et aux États-Unis. Enfin, les opérateurs du MOA FireFly, réputé lié à la Chine, auraient employé cette API à des fins d'exfiltration en utilisant un outil accessible publiquement et chargé de déposer les données récoltées sur un serveur d'hébergement GoogleDrive [53].

D'autres infrastructures *cloud* sont régulièrement utilisées pour des opérations d'exfiltration. Selon KASPERSKY, depuis 2019, les opérateurs du MOA TheMask, motivés par la récolte de renseignements stratégiques, se serviraient de l'API OneDrive pour exfiltrer les données récupérées au cours de leurs campagnes d'attaques [54].

Incident ANSSI

Les investigations menées par l'ANSSI lors d'une compromission ont mis en évidence l'utilisation d'un outil d'accès à distance (*Remote access tool*) afin d'exfiltrer des données en dissimulant les flux dans du trafic vers l'API de GITHUB à destination d'un compte créé par l'attaquant.

Les attaquants peuvent également usurper l'identité de certains services *cloud* dans leur infrastructure. En 2023, un MOA associé à la Chine par l'éditeur de sécurité UNIT42 aurait été utilisé pour créer une infrastructure de noms de domaine usurpant l'identité de fournisseurs de service *cloud*. Au moins 24 entités gouvernementales compromises par les opérateurs de ce MOA auraient communiqué avec cette infrastructure malveillante [55]. Le cybersquattage impliquant l'usurpation de l'identité de services *cloud* est répandu. Outre un usage potentiel en tant qu'infrastructure de C2, les noms de domaine créés peuvent être utilisés pour distribuer des codes malveillants ou récolter des identifiants de connexion [34].

7 RECOMMANDATIONS

Ces recommandations sont adressées aux clients de fournisseurs de services *cloud* et aux fournisseurs de services *cloud* eux-mêmes. Ces recommandations sont destinées à éclairer les entités évoquées en matière de bonnes pratiques de cybersécurité à adopter afin de se prémunir contre les menaces abordées. Elles ne sont pas exhaustives, ne se substituent pas aux réglementations spécifiques et doivent être adaptées et complétées dans le cadre du contexte opérationnel et fonctionnel des systèmes d'information considérés.

7.1 Recommandations à destination des clients de CSP

7.1.1 Mesures générales

R1

Appliquer les mesures du guide d'hygiène de l'ANSSI

Les 42 mesures du guide d'hygiène de l'ANSSI représentent le socle essentiel à respecter pour protéger les informations d'une organisation. En plus des recommandations parfois plus spécifiques propres à ce document, il est fortement recommandé aux clients de services *cloud* d'appliquer les mesures générales de ce guide d'hygiène, en particulier :

- la formalisation d'une analyse de risques ;
- la mise en œuvre de moyens d'administration sécurisés, y compris dans ses accès aux ressources hébergées dans le *cloud* ;
- la mise en œuvre de moyens sécurisés dans un contexte de nomadisme.

Le guide décrit deux indicateurs de niveau (standard ou renforcé) guidant le lecteur vers les mesures à mettre en œuvre en priorité selon le niveau visé.

Pour aller plus loin : ANSSI, *Guide d'hygiène informatique*, septembre 2017 [56].

R2

Maintenir des contacts techniques joignables

Il est généralement possible pour un client d'associer des informations de contact à des ressources louées dans le *cloud*. Il est même parfois possible de spécifier un contact technique aux comptes dits de gestion.

Par conséquent, il est fortement recommandé de spécifier ces contacts, de les maintenir à jour et d'identifier un personne ou un service apte à traiter un signalement d'incident de sécurité.

Pour aller plus loin, si des informations détaillées peuvent être spécifiées, la RFC2350 liste les options pertinentes pour un contact de sécurité : IETF, *Expectations for Computer Security Incident Response*, juin 1998 [57].

7.1.2 Maîtriser sa surface d'exposition

R3

Mettre en œuvre une politique de cloisonnement

Le niveau de sécurité et le niveau de confiance des systèmes d'information (SI) locaux d'un bénéficiaire et de ses systèmes hébergés dans le *cloud* peuvent être très hétérogènes. Si le besoin d'interconnexion de ces SI s'avère nécessaire, il est alors indispensable de mettre en œuvre des moyens de cloisonnement adaptés entre ces systèmes. À titre d'exemple :

- une passerelle d'interconnexion sécurisée intégrant des fonctions de filtrage, de rupture protocolaire et de journalisation/détection ;
- des authentifications et modes d'authentification spécifiques.

R4

Auditer l'exposition de ses services *cloud*

Un client de service *cloud* devrait auditer régulièrement l'exposition des services qu'il a déployé, la chaîne d'intégration qui a permis ces déploiements, ainsi que les applicatifs et modules autorisés à accéder aux données.

Ces audits devraient avoir pour objectif de s'assurer que la surface des services exposés soit réduite au strict nécessaire, que les comptes et délégations de droits soient cohérents, que les règles de contrôles d'accès aux ressources soient bien configurées et que les secrets employés soient protégés de façon efficace.

Ces audits devraient également s'assurer que l'ensemble des mécanismes de traçabilité permettant une supervision et une investigation sur incident soit activé.

Pour aller plus loin s'appuyer sur la partie 1 du guide : ANSSI, *Crise Cyber, les clés d'une gestion opérationnelle et stratégique)*, décembre 2021 [58].

R5

Privilégier des offres cloisonnées entre clients de type SecNumCloud pour des activités sensibles

Le référentiel SecNumCloud propose un ensemble de règles de sécurité à suivre garantissant un haut niveau d'exigence tant du point de vue technique, qu'opérationnel ou juridique. Le référentiel couvre les thématiques de sécurité suivantes :

- le chiffrement des données clients ;
- le cloisonnement des clients entre eux (réseau, stockage, traitements…) ;
- la protection des moyens d'accès au service (portail, API) ;
- la protection contre les lois extraterritoriales.

Pour le traitement et l'hébergement de données sensibles, il est recommandé de privilégier les services conformes au référentiel SecNumCloud.

Pour aller plus loin : ANSSI, *Prestataires de services d'informatique en nuage (SecNumCloud)*, 2022 [11].

7.1.3 Assurer une continuité d'activité

R6

Planifier et implémenter un PCA et un PRA

Il est fortement recommandé qu'un client de service *cloud* mette en œuvre les moyens techniques et humains lui permettant, suite à un incident de sécurité, de maintenir ses activités ou ses services dans un mode dégradé et de faciliter le retour à un fonctionnement nominal.

Ces éléments peuvent être formalisés au travers d'un plan de continuité (PCA) et de reprise d'activité (PRA) associé à un bilan d'impact sur l'activité. Ce plan devrait être révisé et testé régulièrement afin de s'assurer qu'il est pertinent et actionnable en situation de crise.

Enfin, un plan de communication devrait être prévu et testé afin de permettre une communication efficace en cas de crise, celui-ci devrait notamment :

- identifier la liste des parties prenantes à alerter, par exemple : les autorités, partenaires, clients, prestataires, etc. ;
- identifier les informations attendues, ainsi que la forme, les moyens et les relais pour alerter les parties prenantes ;
- sur la base de l'appréciation des risques et des scénarios identifiés, des canevas de communication à adapter peuvent être établis pour faciliter la gestion de crise le jour venu ;
- identifier les éléments devant être disponibles hors ligne.

Pour aller plus loin :

- voir le Chapitre 10 *Continuité d'activité* : ANSSI, *Prestataires de services d'informatique en nuage (SecNumCloud)*, 2022 [11];
- voir la partie 1 du guide : ANSSI, *Crise Cyber, les clés d'une gestion opérationnelle et stratégique*, décembre 2021 [58].

R7

Appliquer les bonnes pratiques de prévention contre les attaques par déni de service

Les attaques par déni de services doivent être prises en compte lors du déploiement d'infrastructure de services et infrastructure dans le *cloud*.

En particulier, il est recommandé de faire appel à des prestataires capables de gérer les attaques par déni de service distribués avant un incident. Il est généralement utile de prévoir l'intermédiation de services de distribution de contenu (CDN) pour tout téléservice dont la disponibilité est importante. Il est prudent d'identifier les types d'attaques couverts par ces services en distinguant la couverture des attaques volumétriques (saturation de bande passante ou de capacité

de traitement de paquets) de celle couvrant les attaques visant le niveau applicatif (dit « Layer 7 »).

Une vigilance particulière doit être portée sur le plafonnement des coûts aussi bien contractuellement que techniquement.

Pour aller plus loin :
- ANSSI, *Les Essentiel ANSSI - « Dénis de service distribués (DDoS) »*, avril 2024 [59];
- ANSSI, *Comprendre et anticiper les attaques DDoS*, mars 2015 [60].

R8

Utiliser les options de sauvegardes sécurisées quand elles sont disponibles

Une politique de sauvegarde des données hébergées dans le *cloud* devrait être définie et maintenue à jour. Cette dernière devrait être appliquée et testée afin de pallier la corruption ou l'indisponibilité de données dues à un incident ou une compromission. Plusieurs prestataires proposent des solutions de sauvegardes des données clients. Pour les actifs les plus critiques, une sauvegarde hors ligne devrait être prévue afin de garantir une restauration en cas de crise. En fonction du niveau de sensibilité des données, les sauvegardes devraient être chiffrées afin d'en garantir la confidentialité.

7.1.4 Protéger les identités, les accès et les données

R9

Établir et mettre en œuvre une politique de gestion des identités et des accès

De la même manière que sur un SI local, la gestion des privilèges est centrale pour le fonctionnement sécurisé d'un environnement *cloud*.

Le principe du moindre privilège devrait être appliqué pour assigner les accès strictement nécessaires à chacun. De plus, des politiques d'accès conditionnel et de l'authentification multifacteur (MFA) devraient être appliqués le plus largement possible..

Pour aller plus loin : ANSSI, *Recommandations relatives à l'authentification multifacteur et aux mots de passe*, octobre 2021 [61];

R10

Sécuriser spécifiquement les pivots entre les identités locales et le *cloud*

Un modèle de gestion d'identité régulièrement adopté par les clients de CSP est une architecture hybride où une identité valide sur le SI local du client le sera éga-

lement sur les services proposés par son CSP. Par conséquent, les équipements en charge de gérer l'hybridation côté client sont sensibles, car embarquant souvent des secrets de comptes privilégiés pour le SI local et le SI hébergé dans *cloud*.

Dans la mesure du possible, les méthodes d'hybridation nécessitant de synchroniser des dérivés de secrets d'identité directement chez le CSP devraient être évitées. De plus, les équipements en charge de gérer l'hybridation devraient être sécurisés de la même manière que tout équipement manipulant des secrets d'administration très privilégiés.

Pour aller plus loin : ANSSI, *Recommandations relatives à l'administration sécurisée des SI*, mai 2025 [62].

R11

Établir et mettre en œuvre une politique de gestion des comptes privilégiés

De la même manière que sur un SI local, la gestion des privilèges est centrale pour le fonctionnement sécurisé d'un environnement *cloud*. Il faut donc distinguer d'un côté l'administration de l'environnement *cloud* en lui-même et d'un autre l'administration des activités métier hébergées chez le CSP.

Dans ce cadre, il est recommandé d'appliquer le principe du moindre privilège pour mettre en place les accès exacts strictement nécessaires à chacun. De plus, des politiques d'accès conditionnel et du MFA devraient être systématiquement mises en place sur ces comptes. Pour les comptes les plus privilégiés, par exemple les comptes capables d'administrer l'intégralité de l'environnement *cloud*, il est recommandé que ces comptes ne soient pas hybrides, mais bien spécifiques à la base d'identité du CSP et utilisés uniquement depuis des postes d'administration dédiés à cet usage.

Pour aller plus loin : ANSSI, *Recommandations relatives à l'administration sécurisée des SI*, mai 2025 [62].

R12

Établir et mettre en œuvre une politique de classification et de chiffrement des données

Une politique de classification des données devrait être établie, évaluant le niveau de sensibilité de chaque catégorie de données.

En fonction de celle-ci, les informations devraient être autorisées à transiter par le *cloud* en clair, chiffrées, ou jamais. Dans la mesure du possible, le chiffrement devrait avoir lieu avant l'envoi des informations vers le service *cloud*.

Lorsque cela n'est pas possible, mais que le service *cloud* offre des fonctions de chiffrement, celles permettant au client de maîtriser et contrôler les clés de chiffrement doivent alors être privilégiées.

R13

Établir et mettre en œuvre une politique de gestion des secrets prenant en compte le partage de responsabilité

Il est recommandé de définir et implémenter une politique de gestion des secrets qui tienne compte du *cloud*. Cette politique doit permettre d'identifier les secrets, leur cycle de vie de la génération jusqu'au décomissionnement, leur circulation et leur protection.

La politique de gestion des secrets devrait tenir compte des cas d'échanges nécessaires avec un CSP lors d'une demande d'assistance technique.

Selon la complexité du dysfonctionnement rencontré, le prestataire peut parfois avoir besoin de plus ou moins d'informations de contexte liées au fonctionnement et à l'utilisation de son service, afin d'identifier et reproduire le problème rencontré et ainsi le résoudre. Or, des secrets peuvent être présents dans les informations collectées.

Dans la mesure du possible, seules les informations strictement nécessaires devraient être communiquées, la présence éventuelle de secrets devrait être identifiée et ceux-ci devraient si possible être nettoyés avant transmission. Lorsque cela n'a pas été possible ou en cas de doute, ils devraient alors être systématiquement invalidés et régénérés à l'issue de l'action.

La période de temps d'exposition de ces secrets devrait alors être la plus courte possible. Les personnes autorisées à réaliser de telles transmissions devraient être identifiées et les actions de support tracées.

7.1.5 Superviser, détecter et investiguer

R14

Superviser les actifs hébergés dans le *cloud*

Les actifs hébergés dans le *cloud* devraient être supervisés de façon continue et leur altération détectée.

En particulier, il est nécessaire de pouvoir superviser l'état des infrastructures IaaS, les ressources stockées dans des services SaaS, les accès à des comptes disposant de privilèges étendus, l'activation de fonctions sensibles (changement de droits, création ou altération d'objets de sécurité...), changements de configuration affectant les accès ou l'exposition des ressources, services et systèmes.

Si plusieurs infrastructures *cloud* sont utilisées, il est important d'anticiper une supervision globale des accès à ces différentes ressources.

R15

Valider les codes déployés en IAAS, PAAS, FAAS

Les codes déployés sur des services *cloud* d'infrastructure (IaaS), de plateforme (PaaS) ou d'exécution de fonction (FaaS) sont sensibles et peuvent être ciblés par des attaquants.

Ils devraient donc faire l'objet d'un suivi en version, d'une traçabilité et idéalement de signature électronique avant mise en production. Ces mesures sont particulièrement efficaces quand elles sont automatisées dans une chaîne de production de code intégrée (CI/CD). Cette chaîne devrait aussi être protégée contre les accès illégitimes.

R16

Détecter et évaluer les compromissions applicatives par *supply chain*

Il est recommandé de maintenir un inventaire des applications locales liées à des services *cloud*, quel que soit l'environnement d'exécution de ces applications (postes de travail, ordiphones ou serveurs).

La détection de compromission par *supply chain* d'une application ou d'un cadriciel (*framework*) servant à la connexion depuis un SI interne vers un service *cloud* est par nature complexe.

Cependant, dans de nombreux cas, la tenue d'un inventaire maîtrisé, à jour et historisé des applicatifs employés a permis d'identifier les instances vulnérables ou compromises et de circonscrire les conséquences d'une attaque.

R17

Investiguer les changements réalisés dans le *cloud* en cas d'incident de sécurité

En cas de compromission de son environnement *cloud*, il est recommandé au client de procéder à une investigation numérique pour déterminer les actions menées par l'attaquant. Il est pour cela nécessaire de passer en revue les changements ayant eu lieu sur son environnement. Cela inclue généralement, sans s'y limiter, d'inspecter les éléments suivants :

- les authentifications de comptes ;
- les créations ou destructions de comptes ;
- les changements de configuration de comptes existants (ajout de MFA, changement de mots de passe, ajouts de droits d'accès, utilisation de rôles temporaires...) ;
- les créations ou destructions de ressources ;
- les changements de configuration de ressources (droits d'accès modifiés...)

Pour effectuer cette analyse, il est crucial de disposer d'une journalisation des actions sur l'environnement *cloud* client. Cette journalisation devrait être activée et disposer d'une rétention de plusieurs mois. Une activité d'analyse numérique *cloud* peut être difficile à mener sans compétences spécialisées sur le sujet, il est

par conséquent conseillé de faire appel à un prestataire de réponse à incident qualifié (PRIS) pour cette tâche.

7.2 Recommandations à destination des CSP

7.2.1 Mesures générales

R18

Mettre en œuvre le guide d'hygiène de l'ANSSI

Les 42 mesure du guide d'hygiène de l'ANSSI représentent le socle essentiel à respecter pour protéger les informations d'une organisation. En plus des recommandations parfois plus spécifiques propres à ce document, il est fortement recommandé aux clients de services *cloud* d'appliquer les mesures générales de ce guide d'hygiène, en particulier :

- la mise en œuvre de moyens d'administration sécurisés et dédiés à l'administration du service *cloud* ;
- le maintien en conditions opérationnelles et de sécurité ;
- le durcissement des configurations et systèmes.

Le guide décrit deux indicateurs de niveau (standard ou renforcé) guidant le lecteur vers les mesures à mettre en œuvre en priorité selon le niveau visé.

Pour aller plus loin :

- ANSSI, *Guide d'hygiène informatique*, septembre 2017 [56] ;
- ANSSI, *Recommandations relatives à l'administration sécurisée des SI*, mai 2025 [62].

R19

Appliquer les bonnes pratiques de développement

Le développement dans un environnement *cloud* devrait suivre les bonnes pratiques communes de développement sécurisé. En particulier :

- les applications doivent faire l'objet d'analyses de risques ;
- leurs dépendances doivent être identifiées et gérées avec rigueur ;
- la sécurité devrait être testée dans des configurations réalistes ;
- les secrets, leur protection et leur cycle de vie doivent faire l'objet d'une attention particulière.

Par ailleurs, le cycle de vie applicatif de la conception à la fin de support devrait inclure la sécurité et les corrections de vulnérabilités identifiées.

Pour aller plus loin : ANSSI, *Les essentiels DEVSECOPS*, février 2024 [63].

7.2.2 Maîtriser sa surface d'exposition

R20

Cartographier et limiter la surface de services exposée

Les services utilisés par un CSP exposent des interfaces potentiellement critiques telles que des interfaces d'administration des composants de gestion de matériel, d'hyperviseur ou de gestionnaires de conteneurs.

Un inventaire de l'ensemble de ces interfaces devrait être effectué et leurs accès devrait être limités au strict nécessaire. Dans le cadre de services *cloud* privés proposés aux clients tels qu'un *cluster* de virtualisation ou de conteneurs dédiés, il est important de limiter ces accès par défaut.

R21

Cloisonner le SI de gestion de l'infrastructure métier utilisée par les clients et le reste du SI

Le prestataire devrait mettre en œuvre des mesures de cloisonnement appropriées entre le système d'information du service et ses autres systèmes d'information (bureautique, informatique de gestion, gestion technique du bâtiment, contrôle d'accès physique, etc.).

Il devrait mettre en œuvre le système d'information du service en assurant le cloisonnement entre d'une part l'infrastructure technique et d'autre part les équipements nécessaires à l'administration du service et des ressources.

Pour aller plus loin voir le Chapitre 9.7 *Restriction des accès à l'information* : ANSSI, *Prestataires de services d'informatique en nuage (SecNumCloud)*, 2022 [11].

R22

Sécuriser les postes des développeurs de l'infrastructure métier

Les postes d'opérateur disposant de rôles étendus sur la configuration d'infrastructure ou d'application dans le *cloud* doivent être considérés comme aussi sensibles que des postes d'administrateurs.

À ce titre, ils doivent faire l'objet de protections telles que décrites dans le guide d'hygiène de l'ANSSI. Cette recommandation couvre les rôles de SRE, de DevOPS, d'ingénieur d'infrastructure, ou les rôles de support amenés à pratiquer des diagnostics donnant accès à des informations sensibles sur la production.

Pour aller plus loin : ANSSI, *Les essentiels DEVSECOPS*, février 2024 [63].

R23

Offrir un service conforme au ou s'inspirant du référentiel SecNumCloud

Le référentiel SecNumCloud propose un ensemble de règles de sécurité à suivre garantissant un haut niveau d'exigence tant du point de vue technique, qu'opérationnel ou juridique.

Pour les prestataires de service *cloud*, ce référentiel couvre en particulier sur les thématiques de sécurité suivantes :

- l'usage de moyens d'administration dédiés et sécurisés ;
- la maîtrise des entrants/sortants sur la plateforme ;
- le cloisonnement du système d'information SecNumCloud des autres SI ;
- l'organisation de revue et audits réguliers pour identification des vulnérabilités.

Il est recommandé à tout CSP de s'inspirer du référentiel SecNumCloud et dans la mesure du possible d'offrir un service conforme à celui-ci.

Pour aller plus loin : ANSSI, *Prestataires de services d'informatique en nuage (SecNumCloud)*, 2022 [11].

7.2.3 Assurer une continuité d'activité

R24

Sauvegarder son infrastructure et proposer une offre de sauvegarde sécurisée

Le prestataire devrait mettre en œuvre une procédure de sauvegarde hors-ligne de la configuration de l'infrastructure technique.

Par ailleurs, le prestataire devrait aussi mettre à disposition de ses clients un service de sauvegardes sécurisée de leurs données. Celle-ci devrait être documentée dans une politique de sauvegarde et de restauration des données. Cette politique devrait prévoir des sauvegardes régulières de l'ensemble des données (informations, logiciels, configurations, etc.) ainsi que la protection de ces sauvegardes.
Pour aller plus loin voir le chapitre 12.5 « Sauvegarde des informations » : ANSSI, *Prestataires de services d'informatique en nuage (SecNumCloud)*, 2022 [11].

R25

Planifier et implémenter un PCA et un PRA

Afin de maintenir ou de restaurer l'exploitation du service et d'assurer la disponibilité des informations au niveau et dans les délais pour lesquels le prestataire s'est engagé vis-à-vis de ses clients, le prestataire devrait mettre en œuvre un plan de continuité et de reprise d'activité (PCA/PRA) ainsi qu'un bilan d'impact sur l'activité. Ces plans devraient être révisés et testés régulièrement afin de s'assurer qu'ils sont pertinents et efficaces en situation de crise.

Enfin, un plan de communication devrait être prévu et testé afin de permettre une communication efficace en cas de crise, celui-ci devrait notamment :

- identifier la liste des parties prenantes à alerter, par exemple : les autorités, partenaires, clients, prestataires, etc. ;
- identifier les informations attendues, ainsi que la forme, les moyens et les relais pour alerter les parties prenantes ;
- sur la base de l'appréciation des risques et des scénarios identifiés, des canevas de communication à adapter peuvent être établis pour faciliter la gestion de crise le jour venu ;
- identifier les éléments devant être disponibles hors ligne.

Pour aller plus loin :

- voir le Chapitre 10 *Continuité d'activité* : ANSSI, *Prestataires de services d'informatique en nuage (SecNumCloud)*, 2022 [11] ;
- voir la partie 1 du guide : ANSSI, *Crise Cyber, les clés d'une gestion opérationnelle et stratégique*, décembre 2021 [58] ;

R26

Fournir des services et options de protection contre les attaques par déni de service

Les prestataires de service *cloud* devraient prévoir des mesures de sécurité contre les attaques par déni de service dans l'élaboration de leur offre de service. Les options disponibles et les niveaux de couvertures associés (uniquement attaques capacitaires, ou couverture jusqu'au L7) devraient être clairement communiqués aux clients.

Des possibilités de plafonner la consommation de ressources, ou le coût de celles-ci, devraient être proposées afin que les clients puissent limiter l'impact financier d'une attaque par déni de service. L'atteinte de ces seuils devrait faire l'objet de notifications aux clients concernés.

L'intégration avec des services tiers devrait être communiquée au client afin que celui-ci puisse en comprendre les éventuels impacts sur la circulation de données personnelles.

R27

Proposer des mécanismes de protection contre les destructions de ressources

Des options protégeant contre la destruction de ressources sensibles ou d'un grand nombre de ressources devraient être offertes aux clients. Parmi ces mécanismes peuvent être identifiés : les mesures de verrouillage, les autorisations par autorités multiples, les délais de conservation avant purge des informations, la notification au client par des moyens tiers pour confirmation de l'action.

Les comptes « super-administrateurs » disposant de droits étendus au sein d'un même projet, sur un ou plusieurs *tenants* ou encore sur l'ensemble des ressources clients devraient par défaut, faire l'objet de ces protections.

7.2.4 Protéger les identités, les accès et les données

R28

Établir et mettre en œuvre une politique de gestion des secrets à l'état de l'art

Les fournisseurs de services *cloud* devraient établir et suivre une politique de gestion des secrets à l'état de l'art. Les catégories de secrets manipulés, leurs lieux de génération d'emploi et de transit devraient être inventoriés.

Pour chacun d'eux, leur niveau de criticité devrait être documenté. Dès que possibles les clés privées et secrètes devraient être protégées dans des enclaves matérielles (Hardware Security Modules ou HSM, TPM, secure-element, enclave processeur) et les applicatifs susceptibles de faire appel à ces éléments adaptés en conséquence.

Dès que cela est possible, il est recommandé d'offrir des options permettant aux clients de générer et gérer leurs propres clés, si possible en les hébergeant en dehors du service *cloud*.

Dans le cadre du support client, cette politique de gestion des secrets devrait prévoir une minimisation du risque de transmission des secrets par les clients. Si cette minimisation ne peut être effectuée côté client, le CSP devrait prévoir systématiquement le nettoyage des secrets à la réception, leur invalidation et régénération.

De plus, le prestataire devrait systématiquement informer la DSI de son client qu'une action de support susceptible d'avoir donné accès à des secrets a été réalisée au profit de l'un de ses membres. Cette notification devrait expliciter les mesures prises en conséquence.

R29

Proposer des options d'authentification à l'état de l'art

La granularité des options d'authentification et accès qu'un client peut configurer est déterminante pour la sécurité de son environnement.

Toute offre de CSP incluant de la gestion d'identité et accès devrait intégrer par défaut les configurations suivantes :

- possibilité de mise en place du MFA sur tous les comptes clients ;
- possibilité de mise en place de politiques d'accès conditionnel avec du filtrage par adresses IP et par pays ;
- possibilité de configurer des accès à des ressources sur des plages de temps limitées ;
- possibilité de soumettre les actions les plus structurantes sur l'environnement (création/destruction de certaines ressources ou comptes) à l'approbation de plusieurs comptes ;
- possibilité de configurer des notifications quand des comptes sont utilisés,

des authentifications échouent ou des ressources sont accédées ;
- forcer le MFA sur les comptes à privilège ;
- accepter l'authentification des comptes clients via des fournisseurs d'identité tiers ;
- proposer par défaut des types de comptes où le principe du moindre privilège s'applique.

Ces options ne devraient pas être réservées à un palier haut de coût de service, qui les rendraient inaccessibles à des organisations de petite ou moyenne taille.
Pour aller plus loin : ANSSI, *Recommandations relatives à l'authentification multifacteur et aux mots de passe*, octobre 2021 [61].

R30

Sécuriser le support client

Le support client doit par définition disposer de droits importants sur l'environnement de production d'un CSP et peut avoir accès à des données sensibles des clients.

Les accès des opérateurs de support devraient donc être configurés en suivant le principe du moindre privilège. Leurs actions devraient être particulièrement supervisées et le nombre de clients sur lesquels des actions de support sont menées par jour devrait être limité.

Enfin, un contact DSI client devrait être notifié si un membre du support client accède à des informations de son SI local ou de son environnement *cloud*, en particulier des secrets tels que des mots de passe ou clés privées.

R31

Mettre en œuvre un cycle de vie des environnements physiques comme logiques

Un cycle de vie des environnements physiques comme logiques devrait être défini. Celui-ci devrait, notamment, inclure un processus de décommissionnement entraînant la suppression sécurisée des données, accès et secrets. Toute réutilisation, même partielle, d'un environnement devrait bénéficier de cette procédure de décommissionnement, y compris lorsque cette réutilisation est faite au profit d'un même client.

R32

Revoir régulièrement comptes de test et leurs accès

Un CSP peut avoir besoin de créer des comptes pour tester de nouvelles fonctionnalités ou valider le bon fonctionnement de celles existantes. Ces comptes de test devraient cependant être maniés avec précaution, car ils peuvent bénéficier de droits particulièrement élevés et être exempts des contraintes de sécurité habituellement associées. Il est donc recommandé d'effectuer un inventaire de ces comptes, de déterminer leurs accès et de s'assurer qu'ils ne peuvent pas accéder

aux environnements de production.

7.2.5 Superviser, détecter et investiguer

R33

Superviser la sécurité des ressources client

Le prestataire devrait superviser les accès et modifications des ressources qui lui sont confiées et leurs méta-informations (accès, paramétrages, etc.).

Les configurations anormalement exposées devraient aussi être détectées et notifiées.

Le niveau de traçabilité activé par défaut devrait permettre des levées de doutes sur les évènements de sécurité les plus communs. Ces journaux devraient être horodatés précisément avec mention du fuseau horaire, et permettre de tracer les adresses sources des opérations ainsi que les identités associées. Les durées de rétention proposées devraient permettre de diagnostiquer des événements au moins antérieurs au mois courant.

Il devrait être permis au client d'accéder aux journaux de ces événements dans des niveaux de contrats ordinaires.

Il devrait être aussi permis au client de paramétrer des notifications sur des événements spécifiques, des dépassements de seuils ou des détections d'anomalies (connexions depuis des zones géographiques nouvelles, création/destruction de ressources en masse, usage élevé de ces ressources mémoire/CPU/bande passante, etc.).

R34

Mettre en œuvre une supervision renforcée des actifs transverses

Les prestataires de service *cloud* devraient mettre en œuvre une supervision de sécurité renforcée sur les éléments d'infrastructure les plus sensibles.

L'ANSSI rappelle en particulier que les éléments porteurs de la gestion d'identité de l'infrastructure ou des clients, les systèmes de gestion des ressources entre clients (création, modification, suppression), les API et portails d'administration des clients en interne, les API et portails d'administration destinés aux clients, ou encore les orchestrateurs, sont des actifs transverses.

La compromission de tels actifs a des effets potentiels sur la totalité de l'infrastructure, ou des clients, et doit être détectée le plus tôt possible.

R35

Offrir à ses clients des fonctions de gestion et de supervision de la consommation financière (finOps)

Afin de réduire les risques et les impacts en cas de d'une utilisation abusive de ressources de ses clients, que celle-ci soit la résultante d'une action malveillante ou d'une erreur, un fournisseur de service *cloud* devrait offrir à ses clients des fonctions de gestion et de supervision de la consommation financière (*finOps*) :

- allocation de quota et plafonds de consommation par utilisateur, compte de services ou encore par projet ;
- traçabilité des comptes et ressources à l'origine de ces consommations ;
- tableaux de bord permettant à la fois de voir les usages passés, mais aussi la projection des usages courants s'ils se poursuivaient sur les mois à venir (*capacity planning*) ;
- points d'API documentés permettant d'automatiser l'export des traces et données de supervision pour exploitation hors du service *cloud* ;
- alertes sur des changements de profils de consommation de ressources ;
- comptes utilisateurs métiers pouvant être dédiés à cette fonction, devant être considérés comme des comptes à privilèges lorsque ceux-ci disposent de capacités de configuration de quota/seuils, et pouvant être protégés en conséquence (ex. MFA).

R36

Effectuer une veille sur les noms de domaine

Les noms de domaine d'un CSP sont fréquemment typosquattés par des acteurs malveillants pour collecter des secrets de ses clients, prestataires ou employés. Il est par conséquent conseillé aux CSP d'effectuer une veille sur les dépôts de noms de domaine typosquattant les leurs et de mettre en place une stratégie de protection de leur marque (notifications aux bureaux d'enregistrement, dépôt de plainte, etc.).

8 ANNEXES

8.1 Glossaire

- ***Application Programming Interface*** (API): une interface de programmation d'application permet de définir l'ensemble des éléments nécessaires et utiles pour interagir avec une application ou un service.
- **Authentification multifacteur** (*Multi-Factor Authentication*, MFA) : processus de sécurité qui exige deux ou plusieurs facteurs (comme un mot de passe et un code envoyé par SMS) pour vérifier l'identité d'un utilisateur.
- ***Cloud* dit application en « hybride »** : infrastructure incluant à la fois des ressources hébergées en propre (*on-premise*) et des ressources hébergées dans le *cloud*
- ***Content Delivery Network*** (CDN): un réseau de diffusion de contenu correspond à un ensemble de serveurs placés au plus proche des consommateurs afin d'être en mesure de leur partager rapidement et efficacement du contenu ou des données issues d'un serveur d'origine, facilitant ainsi la répartition de la charge de travail tout en réduisant les risques de congestion réseau.
- **Conteneur** (*Docker*) sur le *cloud* : permet d'exécuter des applications de manière isolée et portable, en emballant l'application et ses dépendances dans un conteneur léger, qui peut être déployé sur n'importe quelle infrastructure *cloud*.
- ***Common vulnerability and exposure*** (CVE): dictionnaire des informations publiques relatives aux vulnérabilités de sécurité.
- **Déni de Service Distribué/Réparti** (DDoS): attaque consistant à saturer une ressource en la sollicitant intensivement depuis plusieurs sources.
- **Fournisseur de service *cloud*** (*Cloud Service Provider*, CSP) : entreprise qui propose des ressources informatiques (serveurs, stockage, réseaux, applications etc.) *via* Internet, souvent sous forme d'abonnement.
- **Hyperviseur** : logiciel qui permet de créer et gérer des machines virtuelles (*virtual machine*, VM) en virtualisant les ressources matérielles d'un système physique.
- **Gestion des accès et des identités** (*Identity and Access Management*, IAM) : cadre de gestion qui permet de contrôler l'accès aux ressources d'une organisation en vérifiant l'identité des utilisateurs et en gérant leurs permissions.
- **Mode opératoire d'attaque** (MOA) : il s'agit de l'ensemble des techniques, tactiques et procédures (TTP) spécifiques mises en oeuvre par un acteur offensif, dans le but de réaliser des attaques. Il intègre des outils, des infrastructures, des manières de procéder etc. qui sont cohérents entre eux et permettent de relier différentes activités offensives en s'appuyant sur ces similarités.
- ***on-premise*** : désigne des solutions informatiques déployées et gérées localement plutôt que dans le *cloud*. Cela inclut des serveurs, des logiciels et des données hébergées sur place.
- **Request For Comments** (RFC) : série numérotée de documents décrivant les aspects et spécifications techniques, dont certains d'entre eux sont devenus de standards au sens normatif terme. Les documentations émises par l'Internet Engineering Task Force (IETF) sont sous la forme de RFC.

- **Réseau privé virtuel** (**VPN**) : mécanisme permettant d'établir une connexion réseau sécurisée entre deux ressources, afin de protéger en intégrité et confidentialité l'ensemble des données qui seront échangées.
- ***Tenant*** ou locataire sur le *cloud* : désigne une entité ou une organisation qui utilise des ressources *cloud* partagées, où ses données et applications sont isolées des autres *tenants*.
- **Virtualisation** : la virtualisation consiste à créer des ressources informatiques virtuelles, comme des machines ou des réseaux, qui peuvent notamment être gérées et utilisées à distance sur le *cloud*.

8.2 Inventaire des scénarios

- Menaces ciblant les fournisseurs et opérateurs d'infrastructures *cloud* :
  - **Scénario 1 :** Chiffrement d'un OCE à travers un équipement de sécurité de bordure vulnérable
  - **Scénario 2 :** Compromission de ScanSource par les opérateurs du rançongiciel Cactus
  - **Scénario 3 :** Compromission et dépôt de bilan de CloudNordic et AzeroCloud
  - **Scénario 4 :** Compromission à travers un équipement de sécurité de bordure vulnérable d'un opérateur de solution SaaS destiné aux professionnels de santé
  - **Scénario 5 :** Compromission de Okta, spécialiste en gestion d'identités, à travers la compromission d'un poste utilisateur
  - **Scénario 6 :** Nouvelle compromission de Okta à l'aide d'identifiants d'authentification volés
  - **Scénario 7 :** Compromission, après une campagne de hameçonnage, de JumpCloud, spécialiste en gestion d'identités et d'accès
  - **Scénario 8 :** Compromission de messageries Microsoft Exchange Online et obtention d'une clé MSA
  - **Scénario 9 :** Accès à des comptes courriels Office 365 après compromission d'un compte de test Microsoft Exchange Online sans MFA activée
  - **Scénario 10 :** Compromission de Fujitsu à travers un équilibreur de charge vulnérable pour lequel un correctif a été appliqué trop tardivement
  - **Scénario 11 :** Compromission du CSP RackSpace à travers l'exploitation d'une vulnérabilité jour-0 d'un logiciel de supervision et de reporting pour les clients
  - **Scénario 12 :** Déni de service distribué (DDoS) couches L3-L4, retours d'expérience OVH et Cloudflare
- Menaces ciblant les clients de services *cloud* :
  - **Scénario 13 :** Exposition pendant plusieurs années de données clients de Toyota Motor en raison de mauvaises configurations
  - **Scénario 14 :** Fuite de données ou de secrets et compromissions liées à de mauvaises configurations
  - **Scénario 15 :** Compromissions, suite à des vols d'identifiants via des infostealers, d'instances clientes SnowFlake, dont la majorité n'utilisait pas de MFA
  - **Scénario 16 :** Exploitation de problèmes de configuration entre des environnements *on-premise* et *cloud* afin de se latéraliser de l'un à l'autre
  - **Scénario 17 :** Latéralisation vers des environnements *cloud* après obtention d'un accès aux environnements *on-premise*
  - **Scénario 18 :** Exfiltration et suppression de données sur le *cloud* suivies d'une demande de rançon contre récupération
  - **Scénario 19 :** Détournement de ressources *cloud* au moyen de cryptomineurs
  - **Scénario 20 :** Incident ANSSI : Compromission d'une partie de l'environnement *cloud* d'une entreprise du secteur de la santé en vue d'y déposer des cryptomineurs
  - **Scénario 21 :** Détournement de modèles de langage sur le *cloud* (ou *LLM hijacking*) afin d'exploiter leurs ressources à des fins malveillantes
  - **Scénario 22 :** Récolte d'identifiants de connexion sur le *cloud* en vue d'obtenir des accès administrateurs à des serveurs ADFS ciblés par le MOA Nobelium
  - **Scénario 23 :** Compromission de comptes de messagerie électronique sur le *cloud* de l'entreprise Hewlett Packard Enterprise
  - **Scénario 24 :** Incident ANSSI : Ajout de moyens de persistance sur le *cloud*
  - **Scénario 25 :** Compromission de l'agence spatiale japonaise à travers un VPN vulné-

rable suivie d'une latéralisation dans son environnement O365
  - **Scénario 26 :** Discrétion croissante des attaquants sur le *cloud*
  - **Scénario 27 :** Incident ANSSI : utilisation de l'environnement *cloud* compromis pour atteindre des entités d'intérêt via des courriels de hameçonnage utilisant des comptes usurpés
  - **Scénario 28 :** Compromission à des fins de déstabilisation (chiffrement puis destruction d'environnements *on-premise* et *cloud*) via l'exploitation de vulnérabilités connues et non corrigées
  - **Scénario 29 :** Latéralisation vers des environnements *cloud* depuis des environnements *on-premise* à des fins de prépositionnement, voire de déstabilisation
  - **Scénario 30 :** Dénis de service distribué (DDoS) observés contre la couche applicative L7
  - **Scénario 31 :** Ciblage des infrastructures *cloud* par un employé de l'entité victime
- Menaces ciblant les applications de virtualisation et composants de gestion matérielle :
  - **Scénario 32 :** Ciblage des composants de gestion matérielle permettant de piloter à distance les ressources matérielles
  - **Scénario 33 :** Ciblage des technologies de virtualisation et d'hypervision
  - **Scénario 34 :** Exploitation d'une vulnérabilité jour-0 affectant le produit VMWare vCenter afin de cibler des entités stratégiques
- Le *cloud* comme infrastructure des attaquants :
  - **Scénario 35 :** Utilisation par les attaquant de l'hébergement *cloud* comme infrastructure de C2, d'exfiltration et de stockage
  - **Scénario 36 :** Incident ANSSI : Utilisation d'un dépôt GITHUB pour stocker du code malveillant que la victime était ensuite incitée à télécharger
  - **Scénario 37 :** Utilisation de l'API Microsoft Graph par les attaquants à des fins de C2 et d'exfiltration
  - **Scénario 38 :** Utilisation de l'API OneDrive par les attaquants pour de l'exfiltration de données
  - **Scénario 39 :** Incident ANSSI : Utilisation d'un *Remote access tool* pour exfiltrer des données en dissimulant les flux dans du trafic vers l'API de GITHUB
  - **Scénario 40 :** Utilisation de services *cloud* afin de créer une infrastructure de noms de domaine usurpant l'identité de CSP

8.3 Inventaire des recommandations

- Recommandations à destination des clients de CSP :
  - **R1 :** Appliquer les mesures du guide d'hygiène de l'ANSSI
  - **R2 :** Maintenir des contacts techniques joignables
  - **R3 :** Mettre en œuvre une politique de cloisonnement
  - **R4 :** Auditer l'exposition de ses services
  - **R5 :** Privilégier des offres cloisonnées entre clients de type SecNumCloud pour des activités sensibles
  - **R6 :** Planifier et implémenter un PCA et un PRA
  - **R7 :** Appliquer les bonnes pratiques de prévention contre les attaques par déni de service
  - **R8 :** Utiliser les options de sauvegardes sécurisées quand elles sont disponibles
  - **R9 :** Établir et mettre en œuvre une politique de gestion des identités et des accès
  - **R10 :** Sécuriser spécifiquement les pivots entre les identités locales et le *cloud*
  - **R11 :** Établir et mettre en œuvre une politique de gestion des comptes privilégiés
  - **R12 :** Établir et mettre en œuvre une politique de classification et de chiffrement des données
  - **R13 :** Établir et mettre en œuvre une politique de gestion des secrets prenant en compte le partage de responsabilité
  - **R14 :** Superviser les actifs hébergés dans le *cloud*
  - **R15 :** Valider les codes déployés en IAAS, PAAS, FAAS
  - **R16 :** Détecter et évaluer les compromissions applicatives par *supply chain*
  - **R17 :** Investiguer les changements réalisés dans le *cloud* en cas d'incident de sécurité
- Recommandations à destination des CSP :
  - **R18 :** Mettre en œuvre le guide d'hygiène de l'ANSSI
  - **R19 :** Appliquer les bonnes pratiques de développement
  - **R20 :** Cartographier et limiter la surface de services exposée
  - **R21 :** Cloisonner le SI de gestion de l'infrastructure métier utilisée par les clients et le reste du SI
  - **R22 :** Sécuriser les postes des développeurs de l'infrastructure métier
  - **R23 :** Offrir un service conforme au, ou s'inspirant du référentiel SecNumCloud
  - **R24 :** Sauvegarder son infrastructure et proposer une offre de sauvegarde sécurisée
  - **R25 :** Planifier et implémenter un PCA et un PRA
  - **R26 :** Fournir des services et options de protection contre les attaques par déni de service
  - **R27 :** Proposer des mécanismes de protection contre les destructions de ressources
  - **R28 :** Établir et mettre en œuvre une politique de gestion des secrets à l'état de l'art
  - **R29 :** Proposer des options d'authentification à l'état de l'art
  - **R30 :** Sécuriser le support client
  - **R31 :** Mettre en œuvre un cycle de vie des environnements physiques comme logiques
  - **R32 :** Revoir régulièrement comptes de test et leurs accès
  - **R33 :** Superviser la sécurité des ressources client
  - **R34 :** Mettre en œuvre une supervision renforcée des actifs transverses
  - **R35 :** Offrir à ses clients des fonctions de gestion et de supervision de la consommation financière (finOps)
  - **R36 :** Effectuer une veille sur les noms de domaine

9 Références

[1] ANSSI. *Recommandations pour l'hébergement dans le cloud des systèmes d'information sensibles*. 9 juillet 2024.
URL : https://cyber.gouv.fr/sites/default/files/document/20240814_np_anssi_recommandations_hebergement_cloud_si_a5_v1g_fr.pdf.

[2] INTEL. *IaaS, PaaS, SaaS –Présentation du modèle de service Cloud*.
URL : https://www.intel.com/content/www/fr/fr/cloud-computing/as-a-service.html.

[3] CARTELIS. *L'architecture Cloud : Les concepts clés*. 16 février 2019.
URL : https://www.cartelis.com/blog/concepts-architecture-cloud/.

[4] MICROSOFT. *Responsabilité partagée dans le cloud –Microsoft Azure*. 29 septembre 2024.
URL : https://learn.microsoft.com/fr-fr/azure/security/fundamentals/shared-responsibility.

[5] NCSC.GOV.UK. *Cloud Security Shared Responsibility Model*. 9 juin 2022.
URL : https://www.ncsc.gov.uk/collection/cloud/understanding-cloud-services/cloud-security-shared-responsibility-model.

[6] GOOGLE. *Threat Horizons H1 2024 Threat Horizons Report*.
URL : https://services.google.com/fh/files/misc/threat_horizons_report_h12024.pdf.

[7] MICROSOFT. « Modern-Day Witchcraft : A New Breed of Hybrid Attacks by Ransomware Operators ». 3 octobre 2024.
URL : https://www.virusbulletin.com/uploads/pdf/conference/vb2024/papers/Modern-day-witchcraft-a-new-breed-of-hybrid-attacks-by-ransomware-operators.pdf.

[8] THALES. *Cloud Resources Have Become Biggest Targets for Cyberattacks, Finds Thales | Thales Group*. 25 juin 2024.
URL : https://www.thalesgroup.com/en/worldwide/defence-and-security/press_release/cloud-resources-have-become-biggest-targets.

[9] ALSTONPRIVACY.COM. *The CLOUD Act and Its Impact on Cross-Border Access to the Contents of Communications*. 25 mars 2018.
URL : https://www.alstonprivacy.com/cloud-act-impact-cross-border-access-contents-communications/.

[10] MONOLITH LAW. *Qu'est-ce que la loi chinoise sur la cybersécurité ? Explication des points clés pour la conformité*. 30 avril 2024.
URL : https://monolith.law/fr/general-corporate/china-cyber-security-law.

[11] ANSSI. *Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences*.
URL : https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf.

[12] SCANSOURCE. *ScanSource Provides Information on Cybersecurity Incident*. 16 mai 2023.
URL : https://scansource.com/about/press-releases/2023/scansource-provides-information-on-cybersecurity-incident.

[13] TECHCRUNCH. *Danish Cloud Host Says Customers 'lost All Data' after Ransomware Attack*. 23 août 2023.
URL : https://techcrunch.com/2023/08/23/cloudnordic-azero-cloud-host-ransomware/.

[14] INSIDE IT. *Ransomware-Angriff ruiniert dänischen Cloudanbieter*. 24 avril 2024.
URL : https://www.inside-it.ch/ransomware-angriff-ruiniert-daenischen-cloudanbieter-20240424.

[15] ZSCALER. *Lapsus$ Attack on Okta : How to Evaluate the Impact to Your Organization*. 24 mai 2022.
URL : https://www.zscaler.com/blogs/security-research/lapsus-attack-okta-how-evaluate-impact-your-organization.

[16] USINE DIGITALE. « Okta reconnaît que quasiment tous ses clients sont impactés par sa fuite de données ». 1er décembre 2023.
URL : https://www.usine-digitale.fr/article/okta-reconnait-que-quasiment-tous-ses-clients-sont-impactes-par-sa-fuite-de-donnees.N2201128.

[17] OKTA SECURITY. *Unauthorized Access to Okta's Support Case Management System : Root Cause and Remediation*. 3 novembre 2023.
URL : https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause/.

[18] THE CLOUDFLARE BLOG. *Thanksgiving 2023 Security Incident*. 1er février 2024.
URL : https://blog.cloudflare.com/thanksgiving-2023-security-incident.

[19] BEYONDTRUST. *BeyondTrust Discovers Breach of Okta Support Unit*. 20 octobre 2023.
URL : https://www.beyondtrust.com/blog/entry/okta-support-unit-breach.

[20] JUMPCLOUD. *[Security Update] June 20 Incident Details and Remediation*. 7 septembre 2023.
URL : https://jumpcloud.com/blog/security-update-june-20-incident-details-and-remediation.

[21] JUMPCLOUD. *[Security Update] Incident Details*. 12 juillet 2023.
URL : https://jumpcloud.com/blog/security-update-incident-details.

[22] MANDIANT. *North Korea Leverages SaaS Provider in a Targeted Supply Chain Attack*. 24 juillet 2023.
URL : https://cloud.google.com/blog/topics/threat-intelligence/north-korea-supply-chain.

[23] ANSSI. *Malicious Activities Linked to the Nobelium Intrusion Set*. 19 juin 2024.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-006/.

[24] MICROSOFT. *Results of Major Technical Investigations for Storm-0558 Key Acquisition*. 6 septembre 2023.
URL : https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/.

[25] DHS.GOV. *Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023 | Homeland Security*. 2 avril 2024.
URL : https://www.dhs.gov/news/2024/04/02/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer.

[26] Microsoft Threat INTELLIGENCE. *Midnight Blizzard : Guidance for Responders on Nation-State Attack*. 26 janvier 2024.
URL : https://www.microsoft.com/en-us/security/blog/2024/01/25/midnight-blizzard-guidance-for-responders-on-nation-state-attack/.

[27] MICROSOFT. *Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard | MSRC Blog | Microsoft Security Response Center*. 8 mars 2024.
URL : https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/.

[28] NIKKEI.COM. *Unauthorized intrusion into Fujitsu's domestic cloud due to misconfiguration of layered defense*. 3 octobre 2022.
URL : https://www.nikkei.com/article/DGXZQOUC205GH0Q2A920C2000000/.

[29] THEREGISTER. *Rackspace Systems Hit by Zero-Day Exploit of Third-Party App*.
URL : https://www.theregister.com/2024/09/30/rackspace_zero_day_attack/.

[30] OVHCLOUD. *The Rise of Packet Rate Attacks : When Core Routers Turn Evil*. 2 juillet 2024.
URL : https://blog.ovhcloud.com/the-rise-of-packet-rate-attacks-when-core-routers-turn-evil/.

[31] CLOUDFLARE. *Une attaque DDoS record de 5,6 Tb/s et les tendances mondiales en matière d'attaques DDoS au quatrième trimestre 2024*. 21 janvier 2025.
URL : https://blog.cloudflare.com/fr-fr/ddos-threat-report-for-2024-q4/.

[32] CSO ONLINE. *Cloud Misconfiguration Causes Massive Data Breach at Toyota Motor*. 6 juin 2023.
URL : https://www.csoonline.com/article/575483/cloud-misconfiguration-causes-massive-data-breach-at-toyota-motor.html.

[33] DARK READING. *Slovenia Power Provider HSE Suffers Ransomware Attack*. 28 novembre 2023.
URL : https://www.darkreading.com/cyberattacks-data-breaches/slovenia-power-provider-hse-suffers-ransomware-attack.

[34] GOOGLE CLOUD BLOG. *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*. 10 juin 2024.
URL : https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion.

[35] ECLECTICIQ. *Ransomware in the Cloud : Scattered Spider Targeting Insurance and Financial Industries*. 10 septembre 2024.
URL : https://blog.eclecticiq.com/ransomware-in-the-cloud-scattered-spider-targeting-insurance-and-financial-industries.

[36] MICROSOFT. *Storm-0501 : Ransomware Attacks Expanding to Hybrid Cloud Environments*. 26 septembre 2024.
URL : https://www.microsoft.com/en-us/security/blog/2024/09/26/storm-0501-ransomware-attacks-expanding-to-hybrid-cloud-environments/.

[37] INVICTUS-IR.COM. *Ransomware in the Cloud*. 11 janvier 2024.
URL : https://www.invictus-ir.com/news/ransomware-in-the-cloud.

[38] AQUA. *Threat Alert : Anatomy of Silentbob's Cloud Attack*. 5 juillet 2023.
URL : https://www.aquasec.com/blog/threat-alert-anatomy-of-silentbobs-cloud-attack/.

[39] SYSDIG. *The Growing Dangers of LLMjacking : Evolving Tactics and Evading Sanctions*. 18 septembre 2024.
URL : https://sysdig.com/blog/growing-dangers-of-llmjacking/.

[40] MICROSOFT SECURITY BLOG. *NOBELIUM Targeting Delegated Administrative Privileges to Facilitate Broader Attacks*. 25 octobre 2021.
URL : https://www.microsoft.com/en-us/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/.

[41] NIKKEI ASIA. *Japan Space Agency Hacking Reveals Cyber Espionage Risk*. 6 novembre 2024.
URL : https://asia.nikkei.com/Spotlight/Cybersecurity/Japan-space-agency-hacking-reveals-cyber-espionage-risk.

[42] JAXA. *Report on Unauthorized Access at JAXA*. 5 juillet 2024.
URL : https://global.jaxa.jp/press/2024/07/20240705-2_e.html.

[43] CISA. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. 7 février 2024.
URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

[44] CBS News. *Former First Republic Bank Employee Sentenced for Sabotaging Bank's Cloud Computer System - CBS San Francisco*. 12 décembre 2023.
URL : https://www.cbsnews.com/sanfrancisco/news/former-first-republic-bank-employee-sentenced-for-sabotaging-banks-cloud-computer-system/.

[45] zerodayinitiative.com. *Pwn2Own Vancouver 2024 Rules*.
URL : https://www.zerodayinitiative.com/Pwn2OwnVancouver2024Rules.html.

[46] Le Monde Informatique. *Pour débuter 2025, Microsoft livre un Patch Tuesday record - Le Monde Informatique*.
URL : https://www.lemondeinformatique.fr/actualites/lire-pour-debuter-2025-microsoft-livre-un-patch-tuesday-record-95759.html.

[47] Security Joes. *Mission "Data Destruction": A Large-scale Data-Wiping Campaign Targeting Israel*.
URL : https://www.securityjoes.com/post/mission-data-destruction-a-large-scale-data-wiping-campaign-targeting-israel.

[48] University of Hawai'i. *ALPHV : Hackers Reveal Details of MGM Cyber Attack – Westoahu Cybersecurity*. 24 octobre 2023.
URL : https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/alphv-hackers-reveal-details-of-mgm-cyber-attack/.

[49] Censys. *ESXWhy : A Look at ESXiArgs Ransomware*. 8 février 2023.
URL : https://censys.com/esxwhy-a-look-at-esxiargs-ransomware/.

[50] Google Cloud Blog. *Cloaked and Covert : Uncovering UNC3886 Espionage Operations*. 18 juin 2024.
URL : https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations.

[51] Ray Canzanese. *Netskope Threat Labs Stats for March 2023*. 21 avril 2023.
URL : https://www.netskope.com/blog/netskope-threat-labs-stats-for-march-2023.

[52] ESET. *APT Activity Report Abusing Cloud Services and VPN Platforms in the pursuit of New Prey April 2024 –September 2024 Report*. Septembre 2024.
URL : https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2024-q3-2024.pdf.

[53] Symantec. *Cloud Cover : How Malicious Actors Are Leveraging Cloud Services*. 7 août 2024.
URL : https://symantec-enterprise-blogs.security.com/threat-intelligence/cloud-espionage-attacks.

[54] Kaspersky. *The Mask Has Been Unmasked Again*. 4 octobre 2024.
URL : https://www.virusbulletin.com/conference/vb2024/abstracts/mask-has-been-unmasked-again/.

[55] Palo Alto Networks. *Chinese APT Targeting Cambodian Government*. 8 novembre 2023.
URL : https://unit42.paloaltonetworks.jp/?p=131164.

[56] ANSSI. *Guide d'hygiène informatique*.
URL : https://cyber.gouv.fr/publications/guide-dhygiene-informatique.

[57] IETF. *Expectations for Computer Security Incident Response*.
URL : https://www.ietf.org/rfc/rfc2350.txt.

[58] ANSSI. *Crise Cyber, les clés d'une gestion opérationnelle et stratégique*.
URL : https://cyber.gouv.fr/sites/default/files/2021/12/anssi-guide-gestion_crise_cyber.pdf.

[59] ANSSI. *Essentiel ANSSI "Dénis de service distribués (DDoS)*.
URL : https://cyber.gouv.fr/publications/denis-de-service-distribues-ddos.

[60] ANSSI. *Comprendre et anticiper les attaques DDoS*.
URL : https://cyber.gouv.fr/publications/denis-de-service-distribues-ddos.

[61] ANSSI. *Guide sur l'utilisation des authentifications multifacteur et des mots de passe*.
URL : https://cyber.gouv.fr/sites/default/files/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf.

[62] ANSSI. *Recommandations relative l'administration securisée des SI*.
URL : https://cyber.gouv.fr/publications/recommandations-relatives-ladministration-securisee-des-si.

[63] ANSSI. *Les essentiels DevSecOps*.
URL : https://cyber.gouv.fr/publications/devsecops.

ANSSI/SDO/DCA

Version : 1.0 – 19 février 2025

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI – 51, boulevard de la Tour-Maubourg – 75700 PARIS 07 SP
cyber.gouv.fr • cert.ssi.gouv.fr

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité