TLP:CLEAR

ÉTAT DE LA MENACE CIBLANT LE SECTEUR DES TÉLÉCOMMUNICATIONS

18 décembre 2023

Sommaire

Synthèse

Le secteur des télécommunications peut se diviser en plusieurs grandes familles et intègre à cet égard une typologie d'acteurs variée allant des opérateurs de communications électroniques (OCE) aux équipementiers, en passant par les hébergeurs web ou les points d'interconnexion Internet. Secteur central pour beaucoup d'autres, le secteur des télécommunications est qualifié de « **supercritique** » en raison des conséquences immédiates et systémiques qu'engendrerait un incident l'affectant.

De ce fait, la préoccupation majeure des organisations du secteur des télécommunications est la **disponibilité** de leurs services, parfois **au détriment de la confidentialité** des données et de l'**intégrité** des systèmes d'information. Pour ce secteur **massivement ciblé par des acteurs cybercriminels à des fins lucratives et étatiques à des fins d'espionnage ou de déstabilisation**, la pratique de la « sécurité par l'obscurité [1] » est insuffisante. La taille importante des réseaux des opérateurs, leur hétérogénéité suite à l'intégration continue de nouvelles entités et l'importante dette technique accumulée compliquent leur sécurisation et rend plus cruciale encore une prise en compte des menaces ciblant ce secteur.

Durant les trois dernières années, l'ANSSI a été informée de plus de 150 événements de sécurité [2], dont **près de 50 incidents traités par l'agence**, affectant des entités du secteur des télécommunications. Les deux tiers des événements recensés ont touché des entreprises stratégiques du secteur, dont une très grande part d'opérateurs régulés. **Certains incidents ont entraîné un engagement opérationnel important de la part de l'ANSSI**.

Attaques à finalité d'espionnage

La menace la plus préoccupante touchant le secteur des télécommunications est l'espionnage. Les opérations d'espionnage portent d'abord sur de l'exfiltration de données, traitées en masse par les entités du secteur. Les attaquants réputés liés aux intérêts stratégiques chinois et iraniens sont documentés comme très actifs dans ce domaine. L'historique des incidents connus de l'ANSSI montre cependant que le secteur fait régulièrement l'objet de ciblage par des acteurs stratégiques plus divers.

Ces dernières années, l'ANSSI observe une hausse préoccupante de compromissions touchant des équipements, notamment des routeurs en cœur de réseau des opérateurs. Ces attaques, d'un haut niveau de sophistication, sont souvent menées dans une temporalité longue et difficilement détectées. Elles compromettent l'intégrité du réseau des opérateurs et permettent aux attaquants d'avoir un accès direct aux communications d'entités stratégiques et d'individus. **Elles ont un impact majeur sur la confidentialité des données échangées.**

Les équipements réseau, tels que des routeurs domestiques, utilisés par des entités de moindre taille sont également ciblés par des attaquants qui s'en servent pour créer des **réseaux d'anonymisation destinés à mener des attaques sophistiquées**. Enfin, les **équipements satellitaires** voient leurs usages détournés par certains groupes associés à des modes opératoires réputés liés à la Russie en sources ouvertes, afin de conduire des attaques à but d'espionnage contre des cibles dans le monde entier.

1. Le principe de la *sécurité par l'obscurité* repose sur la non-divulgation d'informations concernant le fonctionnement, la structure ou les technologies utilisées par une organisation, afin d'en assurer la sécurité.
2. Il est à noter que le nombre d'incidents portés à la connaissance de l'ANSSI ne reflète pas nécessairement de manière exacte la réalité de la menace touchant ce secteur : en dehors des déclarations obligatoires d'incidents affectant des Systèmes d'Information d'Importance Vitale (SIIV), les opérateurs ne rapportent en général que les cas les plus graves ou nécessitant l'assistance de l'agence.

Attaques à finalité de déstabilisation

La menace à finalité de déstabilisation pèse également sur le secteur des télécommunications. Bien que les principales attaques recensées dans les trois dernières années sont le fait d'**hacktivistes**, qui pratiquent du chantage au déni de service distribué (DDoS) et de l'exposition de données personnelles associés à des revendications politiques, les opérations de plus grande envergure et à des fins de sabotage restent une menace majeure du secteur.

L'attaque qui a ciblé le réseau de communication satellitaire KA-SAT dans la nuit de l'invasion russe en Ukraine en février 2022 a montré l'**impact massif d'une opération de sabotage**. Attribuée par l'Union européenne et ses États-membres à la Russie le 10 mai 2022, cette attaque a mis hors service **plusieurs dizaines de milliers de modems** dont un grand nombre en France. Cette menace de sabotage s'ajoute aux **destructions physiques** régulièrement constatées dans le secteur, qu'il s'agisse de coupures intentionnelles de câbles ou d'une destruction physique d'infrastructures dans un contexte de conflit armé (en Ukraine par exemple).

Attaques à finalité lucrative

Enfin, les attaques à finalité lucrative sont fréquentes dans le secteur des télécommunications. Une part importante d'entre elles concerne la **fraude aux communications**, qui cible les opérateurs comme leurs clients et représente un préjudice financier et d'image important, notamment pour les opérateurs de téléphonie mobile.

Les opérateurs de télécommunications sont également ciblés par des attaques opportunistes s'intéressant à la masse de données personnelles détenues par les opérateurs. Les données alors exfiltrées sont revendues par des cybercriminels ou sont utilisées dans le cadre d'**attaques par rançongiciel** comme chantage à la divulgation de données.

Tout comme les attaques par rançongiciel, les chantages à l'**attaque par DDoS** affectent la disponibilité des services des opérateurs mais sont plus fréquents.

Enfin, les compromissions menées par des **personnes internes** aux organisations du secteur sont également présentes dans l'éventail des attaques portées à la connaissance de l'ANSSI. Elles peuvent entraîner de l'exfiltration de données personnelles ou le déploiement de logiciels malveillants au sein des systèmes d'information des opérateurs et entraîner des **dommages importants**.

1. Périmètre du secteur

Le secteur des télécommunications peut se diviser en plusieurs grandes familles d'activités :

- les fournisseurs d'accès à Internet ;
- les fournisseurs de services de téléphonie ;
- les fournisseurs de câbles de distribution de télécommunications ;
- les entreprises de câblage et d'infrastructures (antennes, satellites) ;
- les fournisseurs de services de télécommunication connexes.

Cet état de la menace ne traite pas des entreprises qui fournissent des services de communications électroniques (messagerie notamment) basées sur des infrastructures logicielles de type *Software as a Service - SaaS* (Microsoft Azure, AW, OVHCloud, Scaleway, etc.) : les évolutions du marché et les solutions technologiques employées les rapprochent davantage des infrastructures de *Cloud Computing* et d'hébergement.

L'interdépendance entre le secteur des télécommunications et les activités de *Cloud Computing* est cependant de plus en plus importante et est amenée à se renforcer encore avec le développement de la 5G. Il est par conséquent nécessaire de comprendre la menace ciblant le secteur des télécommunications dans un environnement plus large qui intègre également les activités d'hébergement de données et de services nuagiques.

Cadre législatif français et européen

Le secteur des communications électroniques intègre des acteurs privés tels que les opérateurs de communication électronique (OCE), les équipementiers (Nokia, Ericsson…) et les entreprises d'infrastructures numériques telles que les hébergeurs web ou les points d'interconnexion Internet (OVH, Interxion, Equinix, etc.). Les principaux opérateurs de communications électroniques (Orange, SFR, Bouygues Telecom, Free) fournissent des services aux administrations et aux entreprises, dont des Opérateurs d'Importance Vitale (OIV).

Le secteur des télécommunications est, à ce titre, identifié comme un secteur « supercritique » dans la mesure où une attaque réussie contre un ou plusieurs acteurs du secteur aurait des conséquences immédiates et systémiques sur l'ensemble ou une large partie des secteurs d'importance vitale [1]. Les enjeux du secteur en matière de sécurité et de défense nationale sont en premier lieu la confidentialité (protection du secret des correspondances) et la disponibilité des communications, notamment pour les communications d'urgence.

Ces aspects de confidentialité et de disponibilité sont encadrés réglementairement par plusieurs dispositifs qui font du secteur des communications électroniques un secteur fortement régulé :

- code des postes et des communications électroniques (CPCE) : dispositions législatives et réglementaires applicables à l'ensemble des opérateurs de communications électroniques comprenant la mise en place de mesures de sécurité adaptées, la notification d'incidents de sécurité significatifs, la possibilité pour l'ANSSI de mener des contrôles de sécurité et de prescrire des mesures spécifiques en cas de menace sur les OIV ou l'Administration ;
- article L2321 du code de la défense : dispositif de cybersécurité des OIV et dispositif de détection des attaques ;
- code pénal – Article 226-3 (R226) : relatif aux autorisations de commercialisation, d'acquisition et d'utilisation d'équipements susceptibles de permettre l'interception de communications privées. L'article R226 adresse le volet confidentialité au niveau des cœurs de réseaux ;
- article L34-11 (Loi 5G) : loi supplémentaire à l'article R226, applicable uniquement aux équipements 5G déployés par les OIV. L'article L34-11 adresse le volet confidentialité et disponibilité au niveau des cœurs de réseaux et des antennes ;
- directive *Network Information Security 2* (NIS2) : la révision de la directive NIS intègre désormais le secteur des communications électroniques.

2. Menace à finalité lucrative

2.1. Fraude aux communications

La fraude aux communications recouvre de nombreux types d'attaques, dont certaines ciblent essentiellement des utilisateurs finaux, qui sont victimes de redirections vers des numéros surtaxés à leur insu. Des acteurs cybercriminels peuvent également mener des arnaques en usurpant des numéros de téléphones nationaux. Ils y parviennent en exploitant des défauts de sécurisation dans le protocole SIP (*Session Initiation Protocol*) qui est le standard de la téléphonie sur IP. Des cas de pourriels ou d'hameçonnages par SMS ont également pu être reliés à de fausses antennes relais mobiles permettant d'envoyer massivement des messages aux téléphones mobiles situés dans une zone géographique précise [2].

Si les clients sont les principales victimes de ces attaques, les opérateurs de télécommunications peuvent également subir des dommages réputationnels indirects.

Les entreprises de télécommunications ou leurs clients professionnels sont pour leur part ciblés par des attaques visant les réseaux internes de communications. Ainsi, les attaques sur les autocommutateurs téléphoniques privés (*Private Automatic Branch eXchange* ou PABX [3]) touchent fréquemment des entreprises [3].

En exploitant des vulnérabilités connues, les attaquants peuvent ainsi passer des appels, voire monter des services éphémères d'appels internationaux à bas prix vendus sur Internet, qui utilisent les réseaux d'une entreprise victime. Ces attaques sur les PABX peuvent aussi être utilisées pour générer des appels sur des numéros surtaxés dont les profits sont reversés aux attaquants [3]. Ces attaques sont fréquemment réalisées durant les jours de congé, les week-ends et les nuits, afin de n'être pas détectées rapidement par les entreprises.

La fraude aux communications représente la première perte financière pour les opérateurs de télécommunications, selon le rapport publié par l'entreprise de cybersécurité Trend Micro pour le compte de l'Europol European Cybercrime Center (EC3) en 2019, qui l'estime entre 3 et 10% des revenus bruts du secteur. L'organisation de contrôle des fraudes aux télécommunications des opérateurs états-uniens rapporte des chiffres du même ordre de grandeur, autour de 3% des revenus des opérateurs [3].

2.2. Exfiltration et vente de données clients d'opérateurs

Les entreprises du secteur des télécommunications, et particulièrement les opérateurs de téléphonie fixe et mobile, traitent une grande quantité de données financières et à caractère personnel de leurs clients.

Elles sont donc fréquemment ciblées, dans l'ensemble du monde, par des groupes cybercriminels qui peuvent avoir comme objectif la revente des données des clients. Ces données traitées par les opérateurs peuvent servir à pratiquer de l'hameçonnage ciblé ou des arnaques de tous types. L'association des informations contenues sur les cartes SIM et des identités des clients est une opportunité supplémentaire pour les cybercriminels et augmente la valeur de ces données. En possédant ces deux types d'informations, les cybercriminels peuvent pratiquer le *SIM Swapping*, c'est-à-dire usurper l'identité des clients *via* la portabilité des numéros mobiles et contourner l'authentification à double facteur lors d'achats. L'exfiltration des secrets d'authentification présents sur les téléphones peut également entraîner des compromissions de l'ensemble des services utilisant celles-ci pour authentifier leurs utilisateurs.

Les exfiltrations de données de ce type sont donc considérées comme particulièrement graves par les opérateurs, qui pour certains ont été amenés à remplacer l'ensemble des cartes SIM de leurs clients [4] [5] [6] [7].

Les employés des opérateurs de télécommunications ont accès à de nombreuses données et peuvent représenter une menace interne en cas d'utilisation malveillante de celles-ci ou de leurs accès techniques au sein d'une entreprise. C'est également le cas des employés de filiales ou prestataires de ces opérateurs qui peuvent avoir des accès privilégiés aux systèmes d'information des opérateurs.

3. Le PABX est un système qui permet de relier entre eux les différents terminaux téléphoniques d'un réseau (ses lignes internes) avec un réseau téléphonique public. Ces PABX ont donc une fonction de routage des communications et sont opérés grâce à des logiciels spécifiques, souvent mal connus de leurs utilisateurs et insuffisamment sécurisés.

L'opérateur américain de télécommunications AT&T a ainsi été victime d'une activité cybercriminelle interne avancée. Entre 2012 et 2017, deux cybercriminels pakistanais (jugés en 2019) ont corrompu des employés de l'entreprise, tout d'abord pour contourner les blocages de *smartphones* Apple (*SIM lock*) afin de pouvoir les utiliser hors du réseau d'AT&T. Par la suite, les cybercriminels ont fait installer, par ces mêmes employés, un logiciel malveillant sur le réseau interne de l'opérateur, permettant de cartographier le fonctionnement de l'infrastructure réseau. Un second logiciel malveillant aurait ensuite été installé afin de pouvoir exfiltrer de l'information directement, sans plus avoir besoin du concours des employés corrompus d'AT&T. Les employés mis en cause auraient été recrutés sur les réseaux sociaux et auraient été généreusement rétribués (avec des sommes dépassant plusieurs centaines de milliers de dollars sur cinq ans). Les pertes ont été estimées à 5 millions de dollars par AT&T uniquement pour les contournements de blocages Apple [8].

Commentaire : la compromission ayant touché AT&T semble avoir été menée à des fins purement lucratives, mais la nature des informations exfiltrées reste inconnue. Ce type de menace interne pourrait être utilisée par des attaquants répondant à des intérêts stratégiques, à des fins d'espionnage.

2.3. Attaques par DDoS à des fins d'extorsion

La disponibilité des services de télécommunications des opérateurs est une priorité de leurs activités, qui détermine la qualité de leurs services et la confiance que leurs clients peuvent y accorder. Dans certaines zones géographiques davantage isolées où il n'existe pas ou peu de redondance entre opérateurs, la disponibilité des infrastructures de télécommunications est particulièrement critique.

Des groupes cybercriminels font pression sur cet aspect des activités du secteur, en pratiquant régulièrement des attaques par déni de service distribué (DDoS) qui peuvent avoir comme objectif l'extorsion de fonds. Ainsi en septembre 2020, plusieurs fournisseurs d'accès Internet européens auraient été ciblés par des attaques en déni de service distribué, opérées par un acteur inconnu. Ces attaques auraient été menées en saturant les services DNS de ces opérateurs par des requêtes en résolution de noms de domaine, amplifiant ainsi l'effet des attaques par DDoS pour l'opérateur. Les fournisseurs d'accès à Internet (FAI) touchés auraient été EDP, Bouygues Telecom, FDN, K-Net, SFR, Caiway, Delta, FreedomNet, ou encore Online.nl [9].

Le fournisseur nord-américain VoIP.ms, qui opère un service de voix sur IP dans le monde entier, aurait également été victime de ce type d'attaque par déni de service distribué ciblant ses serveurs DNS en septembre 2021. L'attaque a eu comme conséquence une impossibilité de recevoir ou de passer des appels pour les clients de l'opérateur. Les dégâts ont été jugés importants par la victime, malgré ses tentatives d'atténuation de l'attaque. La rançon demandée initialement par les attaquants était de 45 000 dollars. La demande de rançon a été publiée sur Internet par un groupe se présentant comme le groupe cybercriminel REvil, qui aurait augmenté par la suite le montant de la rançon demandée à près de 4,3 millions de dollars. Ce chantage à l'attaque par DDoS accompagné de demande de rançon ne correspondait pas aux pratiques du groupe cybercriminel REvil, à l'époque connu davantage pour mener des attaques par rançongiciel [10]. Il est possible qu'un autre groupe d'attaquants ait usurpé ce nom pour effrayer la victime.

Commentaire : à cette même période, d'autres organisations, hors du secteur des télécoms bien qu'ayant également des besoins vitaux de disponibilité (notamment des opérateurs du secteur de la finance), ont été victimes de chantage au DDoS avec demande de rançon, opérés sous le nom de groupes d'attaquants connus pour leurs activités cybercriminelles. C'est donc probablement davantage l'importance de la disponibilité des services que la qualité d'opérateur de télécommunications qui a déterminé le ciblage de ces opérateurs de VoIP.

2.4. Attaques par rançongiciel

Les entités du secteur des télécommunications sont ciblées comme de nombreux autres secteurs par des attaques par rançongiciel.

Entre 2019 et 2022, l'ANSSI a traité 13 attaques par le biais de rançongiciels touchant des entités du secteur des télécommunications. Ces attaques ont principalement ciblé des entités de taille moyenne ou des filiales d'opérateurs nationaux. Cela représente 36% de l'ensemble des compromissions touchant ce secteur, et 2% de l'ensemble des

attaques par rançongiciel signalées à l'ANSSI. Le nombre des incidents traités par l'ANSSI ne reflète pas de manière exacte la réalité des événements cyber affectant le secteur des télécommunications, mais il ne semble pas que ce dernier soit ciblé spécifiquement.

Commentaire : comme cela est constaté pour d'autres secteurs économiques et industriels, il est probable que ces organisations soient visées du fait de leur moindre sécurisation par rapport à des organisations de taille plus importante.

Le secteur n'apparaît pas ciblé de façon spécifique. Les attaques sont le fait d'opérateurs de rançongiciels très variés qui semblent agir par opportunisme. L'exfiltration et les menaces de divulgation de données faites par les opérateurs de rançongiciels peuvent entraîner des conséquences importantes en matière de réputation pour les entités ciblées et leurs clients. L'indisponibilité potentielle des services due à une compromission par le biais d'un rançongiciel peut également entraîner des dommages importants pour l'opérateur.

2.5. Compromission à des fins de cryptominage

Les instances de *Cloud Computing* des opérateurs de télécommunications peuvent être ciblées par des groupes cybercriminels pratiquant le minage de cryptomonnaie.

Ainsi, en 2019, sans qu'un ciblage délibéré ne semble exister, l'opérateur britannique Vodafone aurait été compromis dans le cadre d'une attaque plus massive opérée par une ancienne employée d'Amazon Web Services. Cette attaque de nature interne à AWS aurait conduit à la compromission de plusieurs instances de *Cloud Computing* appartenant à divers clients, dont Vodafone, pour y opérer du cryptominage [11].

Commentaire : ce ciblage n'est pas spécifique au secteur des télécommunications et concerne plus globalement l'ensemble des entreprises qui a recours au Cloud Computing pour héberger leurs données. La convergence accrue entre Télécommunications et Cloud Computing dans le cadre du développement des technologies 5G invite à une attention particulière relative à cette menace souvent sous-évaluée, mais aux conséquences financières qui peuvent être importantes pour les entités compromises.

3. Menace à finalité d'espionnage

La menace à finalité d'espionnage est la principale menace touchant le secteur des télécommunications. Elle entraîne des compromissions massives, qui non seulement touchent les organisations du secteur, mais peuvent également concerner leurs très nombreux clients, individus ou organisations. Il convient de distinguer, dans cette finalité d'espionnage, ce qui relève d'une volonté d'accès aux données commerciales des opérateurs, de ce qui relève d'une volonté d'accès aux communications entre utilisateurs des infrastructures de télécommunications (qu'ils soient des individus ou des organisations).

3.1. Exfiltration de données

De nombreuses attaques touchant le secteur des télécommunications ont comme objectif l'exfiltration de données des opérateurs de télécommunications. Ces données peuvent être des données de clients des services de télécommunications ou des données internes des opérateurs. Du fait du nombre important d'utilisateurs de ces services, les entreprises de télécommunications sont des cibles très intéressantes pour des groupes d'attaquants divers, qui peuvent y trouver de nombreuses informations personnelles, techniques ou commerciales, qui sont utilisables telles quelles ou afin de préparer des attaques plus perfectionnées.

3.1.1. Ciblage par le biais de modes opératoires réputés chinois

Ciblage extérieur à la Chine

Le secteur des télécommunications dans son ensemble est ciblé de façon très régulière et importante par les groupes d'attaquants mettant en œuvre des modes opératoires d'attaque (MOA) réputés liés en sources ouvertes à la Chine, particulièrement en Asie. Les nombreuses compromissions décrites par les éditeurs de sécurité font état d'exfiltration de données, sans que la nature exacte de ces dernières ne soit toujours détaillée.

Le secteur des télécommunications est souvent ciblé en même temps que d'autres secteurs qui présentent le même intérêt en matière de collecte de données : ainsi, l'éditeur de sécurité Symantec a documenté en 2019 le ciblage de plusieurs organisations singapouriennes en 2017 et 2018 par le biais du MOA WHITEFLY, parmi lesquelles certaines organisations relèvent du secteur des télécommunications [12].

Le même éditeur a documenté en 2019 le ciblage au long cours de plusieurs entités du secteur, mais également des secteurs de la recherche et des technologies, en Asie du Sud-Est, en Belgique et au Luxembourg, par le biais du MOA APT3 (également connu sous le nom de GOTHIC PANDA), réutilisant des outils liés au MOA EQUATION GROUP depuis 2016 [13].

En France, l'ANSSI a traité la compromission en septembre 2020 d'un opérateur national par le biais d'un MOA réputé chinois, dans un but probable d'espionnage.

Parmi les modes opératoires réputés liés à la Chine, le plus spécifiquement utilisé contre le secteur des télécommunications est le MOA GALLIUM, décrit par Microsoft depuis 2019 [14].

Ainsi, Microsoft a décrit en 2019 la compromission de fournisseurs de télécommunications dans le monde entier lors d'une opération connue sous le nom de « *Soft Cell* » débutée en 2017. Les informations ciblées par les attaquants auraient été très spécifiques : ils auraient cherché à exfiltrer les *Call Detail Records* (CDR), qui comprennent les enregistrements d'appels avec leurs sources, les destinations et durées d'appels, ainsi que des informations sur les appareils utilisés et la localisation physique des appareils, permettant l'analyse des comportements et relations des personnes ciblées [4]. Lors de cette opération, les attaquants auraient cherché également des données contenues dans l'*Active Directory* des opérateurs compromis, ainsi que des informations de facturation. Ces attaques, particulièrement persistantes, ont été menées à l'aide de codes et outils malveillants reliés en source ouverte à des modes opératoires liés à la Chine, tels que le *webshell* China Chopper, le *RAT* (outil d'administration à distance) Poison Ivy ou l'outil HTran [15]. Selon l'agence de presse Reuters, la victimologie de cette campagne était répartie dans plus de 30 pays différents [16].

L'ANSSI a traité récemment une compromission liée à ce mode opératoire et a pu constater que ses opérateurs poursuivent activement leurs campagnes, notamment contre le secteur des télécommunications.

Ces exemples ne reflètent pas l'exhaustivité du ciblage du secteur des télécommunications par des attaquants liés aux intérêts stratégiques chinois. Ils montrent cependant que plusieurs groupes d'attaquants réputés liés au gouvernement chinois, aux objectifs et affiliations différents, ciblent dans les mêmes zones géographiques des organisations du secteur des télécommunications.

Ciblage à des fins de surveillance domestique

Le ciblage des réseaux de communication par des groupes d'attaquants réputés liés au gouvernement chinois se fait également à des fins de surveillance politique et domestique. Ainsi, des individus de la communauté Ouïghour voyageant en Asie centrale ou en Asie du Sud-Est ont été ciblés au travers de la compromission de réseaux de télécommunications, ainsi qu'au Kazakhstan, en Turquie, en Inde, en Thaïlande ou en Malaisie.

Les attaques documentées ont cherché à espionner les enregistrements de métadonnées d'appel et des données de localisation des abonnés.

4. Les *Call Detail Records* correspondent à ce qu'on appelle « fadettes » ou FADET dans le langage judiciaire français.

Certaines attaques auraient également ciblé des diplomates et militaires étrangers hors de la communauté Ouïghour [17].

3.1.2. Ciblage par des modes opératoires réputés iraniens

Les modes opératoires associés aux intérêts stratégiques de l'Iran sont fréquemment utilisés pour cibler le secteur des télécommunications, essentiellement au Moyen-Orient. De façon similaire à ce qui est observé en Chine, les entreprises du secteur des télécommunications semblent être ciblées prioritairement en raison des données personnelles dont elles disposent et sont rarement les cibles uniques des attaquants qui les compromettent [18].

3.1.3. Ciblage par d'autres acteurs stratégiques

Les acteurs offensifs liés à la Chine et à l'Iran ne sont cependant pas les seuls à cibler le secteur des télécommunications. De nombreux acteurs stratégiques offensifs suivis par l'ANSSI ou documentés par les éditeurs de sécurité et partenaires de l'agence ont ciblé ce secteur dans les dernières années.

Ainsi en 2021, des opérateurs de télécommunications, FAI et hébergeurs auraient été ciblés par le biais du MOA réputé lié au Hezbollah libanais LEBANESE CEDAR. Les victimes de ces compromissions à finalité d'espionnage seraient situées aux États-Unis, en Grande-Bretagne et au Moyen-Orient (Égypte, Israël, Jordanie, Autorité palestinienne, Arabie saoudite et Émirats arabes unis) [19].

3.2. Ciblage des câbles de télécommunication

Les câbles sous-marins et terrestres de télécommunication font l'objet de soupçons ou d'opérations d'espionnage, au même titre que les câbles télégraphiques ou téléphoniques depuis la fin du 19e siècle. Les publications de documents internes de la NSA par Edward Snowden en 2013 ont notamment révélé un potentiel ciblage du câble sous-marin de fibres optiques SEA-ME-WE 4 opéré par Orange en Méditerranée [20].

Les méthodes utilisées pour exfiltrer de l'information depuis ces câbles sous-marins restent aujourd'hui peu claires, du fait d'un manque de documentation sur les attaques qui auraient pu être réalisées. Des capacités d'interception globale de flux par un acteur stratégique en dehors de son territoire national demanderaient des capacités de stockage importantes proches du lieu d'interception, ce qui rend ce type d'attaque difficile, et potentiellement réservée à de rares acteurs stratégiques [21].

De fait, il y a peu d'attaques documentées qui concernent les entreprises opérant des câbles sous-marins de télécommunications. Si la prise de contrôle des interfaces d'administration de ces organisations permettrait de détourner des flux de communications ou de les couper, aucune attaque de ce type n'a pour l'heure été publiquement documentée.

En 2022, un seul incident se rapportant à une organisation de ce secteur a été rapporté, avec peu de détails. Les autorités du *Department of Homeland Security* (DHS) de l'État américain d'Hawaï ont ainsi annoncé en avril 2022 avoir stoppé une cyberattaque ciblant un opérateur de câble sous-marin, sans donner de détails supplémentaires sur la finalité ou le commanditaire de ce ciblage [22].

Commentaire : les évolutions du secteur vers une gestion en direct de certains câbles sous-marins par de très importants opérateurs de contenus peuvent avoir un impact sur l'évaluation de la menace concernant ces infrastructures. Les stations d'atterrage constituent également un point d'entrée potentiel sur le réseau des opérateurs de télécommunications.

3.3. Ciblage des équipementiers réseau

Les équipements réseau sont une cible privilégiée des attaquants cherchant à compromettre des réseaux de télécommunication. Ce ciblage permet à la fois d'observer le trafic qui y circule, potentiellement de l'altérer et d'en exfiltrer des informations. La compromission de ces équipements permet aussi de se servir de ces derniers pour opérer des attaques ultérieures.

3.3.1. Compromission de routeurs

La compromission de routeurs domestiques (SOHO - *Small Office and Home Office*) par des MOA réputés liés aux intérêts stratégiques chinois est une pratique observée par l'ANSSI depuis au moins 2021, ainsi que par de nombreux partenaires et éditeurs de sécurité. Les routeurs ciblés, bien qu'utilisés par une très grande variété de clients (individus, TPE et PME, collectivités territoriales, etc.), sont le plus souvent fournis par des opérateurs de télécommunication spécialisés. Ces compromissions ont pour objectif d'intégrer ces routeurs dans des réseaux de *botnets*. Ainsi, l'ANSSI a publié en 2021 un rapport décrivant le ciblage de routeurs d'organisations françaises par le biais du MOA APT31 [23].

La CISA a également émis une alerte sur le sujet en juin 2022 [24]. Ces compromissions exploitent des vulnérabilités parfois connues, mais non corrigées par les propriétaires des routeurs. Devant la vulnérabilité de leurs produits, certains fabricants américains ont mené des opérations de remédiation.

La découverte et la publication par le NCSC-UK au début de l'invasion russe en Ukraine, d'une large compromission de routeurs domestiques des constructeurs WATCHGUARD et ASUS en Europe et aux États-Unis par le réseau de *botnets* Cyclops Blinks, opéré *via* le MOA SANDWORM, réputé lié en source ouverte au GRU (service de renseignement militaire russe), a laissé craindre une utilisation dans le cadre du conflit [25].

Les routeurs sont également ciblés pour espionner le trafic des opérateurs de télécommunication.

Ainsi en 2018, l'éditeur de sécurité KASPERSKY a décrit le ciblage de routeurs du constructeur MIKROTIK par le biais du MOA SLINGSHOT. Il fait état d'un ciblage de long terme, au moins de 2012 à 2018, et particulièrement sophistiqué. Les victimes auraient été compromises au travers d'un utilitaire de configuration des routeurs MIKROTIK. Cette compromission à but d'exfiltration de données et d'espionnage aurait affecté des entités situées en Afrique (principalement au Kenya et au Yemen) ainsi qu'au Moyen-Orient. Elle aurait touché des individus comme des institutions [26].

L'ANSSI a traité en 2022 la compromission d'équipements réseau d'un opérateur, opérée au moyen d'un MOA lié à un acteur étatique, dans un but probable d'espionnage de télécommunications.

Commentaire : d'une part, l'ANSSI observe que des attaquants ciblent spécifiquement des protocoles d'administration non sécurisés afin de compromettre des équipements réseau. D'autre part, ils profitent de l'utilisation de protocoles n'assurant pas, par défaut, le chiffrement des communications dans le but d'intercepter le trafic en clair des clients des opérateurs. Il est donc nécessaire que les opérateurs soient particulièrement attentifs à cesser l'utilisation de protocoles d'administration faibles tandis que leurs clients doivent s'assurer du chiffrement de bout en bout de leurs communications transitant, même partiellement, via des protocoles non sécurisés.

3.3.2. La question des équipementiers réseau dans le cadre du déploiement de la 5G

Le développement des réseaux de télécommunications 5G entraîne des évolutions dans la gestion des réseaux. La 5G permet de faire circuler davantage de données vers davantage de terminaux mobiles, elle rend possible des communications à très faible latence et entraîne une utilisation plus massive de cellules de couverture mobile [27].

La virtualisation croissante des cœurs de réseau, gérée dans un *Cloud* interne aux opérateurs, rend plus critique la fonction de gestion et d'orchestration du réseau. L'architecture du réseau est davantage basée sur les services et les logiciels que sur une infrastructure physique. La multiplication des équipements de proximité permettant de réduire la latence et de densifier le réseau entraîne des conséquences sur la géographie de la sécurité des opérateurs : la gestion de la sécurité doit se rapprocher des extrémités du réseau, tout en restant maîtrisable par les opérateurs [27].

Ainsi la question des équipementiers qui vont déployer et gérer sur le réseau 5G un nombre grandissant de routeurs aux fonctions virtualisées, a pris au cours des années 2010 une importance majeure du fait de la concentration du marché entre trois principaux fournisseurs, l'entreprise chinoise HUAWEÏ et les groupes européens NOKIA et ERICSSON. Les analyses de risque faites par les autorités européennes ou nord-américaines ont mis en évidence le fait que certains équipementiers ne pouvaient être considérés comme totalement indépendants de la menace en matière d'espionnage ou de déstabilisation. Cette menace (notamment concernant l'intégrité et la disponibilité des

réseaux) concerne particulièrement les fournisseurs équipant les stations de base ou opérant les fonctions clés de gestion technique des réseaux [27].

La sécurité de la 5G est également dépendante des logiciels qui servent à administrer les réseaux. Les risques liés aux failles de sécurité potentielles de ces logiciels, ainsi qu'à l'ensemble des menaces ciblant la chaîne d'approvisionnement de ces logiciels, sont évalués comme importants. La dépendance à un nombre restreint de fournisseurs amène à prendre en considération l'environnement politique et législatif dans lequel ces derniers opèrent.

Depuis 2018 les États-Unis, le Canada, la Grande-Bretagne et les États-membres de l'Union européenne ont, à des degrés divers, fortement contrôlé, pour les opérateurs de télécommunications, les choix d'équipementiers à hauts risques (« *High risk vendors* ») pour tout ou partie des réseaux 5G. Les équipements placés en cœur de réseau font l'objet d'une surveillance particulière, en raison des capacités potentielles de l'équipementier à détourner, intercepter ou interrompre les communications. La question des équipementiers est devenue un enjeu de souveraineté technologique, quand bien même aucune attaque informatique ne semble pour l'heure avoir été documentée [28].

Commentaire : le déploiement des réseaux 5G donne l'opportunité à de nombreux équipementiers et fournisseurs de logiciels d'entrer sur ce nouveau marché. Une grande partie d'entre eux sont des nouveaux entrants, souvent exclusivement actifs sur le segment de la 5G. Leur capacité à sécuriser leurs équipements et leurs dépendances potentielles à des acteurs offensifs restent à ce jour non évaluées.

3.4. Attaques sur le DNS

En 2018, une attaque a ciblé l'opérateur suédois NetNod, qui route une grande partie du trafic européen et est l'un des 13 serveurs racines du DNS. Les attaquants ont pratiqué une compromission de type *Adversary-in-the-Middle* (AiTM), manipulant des enregistrements DNS pour rediriger le trafic et voler des identifiants et mots de passe. La victimologie associée à cette attaque est vaste et principalement localisée au Moyen-Orient [29].

Le registraire de domaine de premier niveau grec aurait également fait l'objet d'une compromission visant son DNS par le biais du MOA présumé turc SEA TURTLE en 2019 [30].

Commentaire : les grands opérateurs de télécommunication sont fréquemment fournisseurs de résolveurs DNS, ce qui multiplie les opportunités d'attaques.

3.5. Usage détourné de trafic satellitaire

Le MOA TURLA, attribué au 16e Centre du Service fédéral de la Sécurité russe (FSB) par les autorités états-uniennes [31], serait employé depuis 2015 au moins, utilisant des infrastructures satellitaires pour dissimuler du trafic de commande et contrôle (C2). Les attaquants profiteraient de la moindre sécurisation des protocoles utilisés pour mener des attaques contre des cibles finales au Moyen-Orient, en Europe et en Afrique principalement. Les opérateurs du MOA TURLA usurperaient des adresses IP d'équipements terminaux et intercepteraient le trafic descendant, souvent non chiffré, des satellites vers les terminaux. Les opérateurs du MOA TURLA exploiteraient des faiblesses dans les protocoles sans compromettre aucun équipement satellitaire [32] .

Commentaire : si les attaquants utilisant le MOA TURLA ne portent pas véritablement atteinte à l'intégrité des infrastructures satellitaires qu'ils utilisent dans leurs campagnes offensives, celles-ci sont cependant présentes dans la chaîne d'attaque du mode opératoire. Le chiffrement des données transitant par le biais de ces infrastructures satellitaires est donc particulièrement nécessaire, notamment avec l'inclusion progressive des réseaux satellitaires dans les réseaux 5G.

3.6. Ciblage au travers des réseaux de téléphonie mobile

Les technologies de surveillance individuelle développées par les entreprises de lutte informatique offensive (LIO) les plus sophistiquées impliquent souvent une utilisation des réseaux mobiles dans la chaîne d'attaque.

L'ONG Amnesty International a documenté en 2019 et 2020 la compromission de journalistes marocains par l'espiogiciel *Pegasus*, commercialisé par l'entreprise israélienne NSO Group. Les investigations menées par l'ONG sur les téléphones des journalistes ont révélé des ciblages au moyen d'injection réseau [33].

Les réseaux de téléphonie mobile peuvent également être utilisés pour localiser une cible qu'un attaquant souhaiterait compromettre. En effet, les nécessités d'interconnexion entre réseaux mobiles pour router les appels, par le biais des réseaux de signalisation IPX/GRX et du protocole SS7, entraînent une absence de chiffrement entre les infrastructures ainsi que l'utilisation de protocoles et de messages de signalisation en clair. Il suffit alors à un opérateur de téléphonie mobile d'être connecté avec ces infrastructures de signalisation ouvertes pour localiser un abonné dans le monde entier, en lançant une procédure d'adressage imitant une demande légitime de communication. Ce mode opératoire peut être utilisé pour permettre des compromissions de *smartphones* nécessitant une localisation fine [34].

Ainsi, l'éditeur Lookout a documenté l'utilisation par l'entreprise italienne de LIO privée RCSLab d'une entreprise-paravent, Tykelab, déclarée comme opérateur de solutions de communication [35]. Les chercheurs du site néerlandais Lighthouse Report ont ensuite documenté un important trafic de communications lié à Tykelab et provenant de petits opérateurs de télécommunications, principalement situés dans des îles du Pacifique. Ce trafic à destination de pays européens ou d'Asie centrale ne pourrait correspondre, selon ces chercheurs, qu'à une activité de surveillance utilisant les infrastructures de signalisation ouvertes des réseaux de téléphonie mobile [36].

De tels accords entre une entreprise de LIO privée proposant des services de compromission de *smartphones* et des petits opérateurs de télécommunications ont été documentés précédemment, notamment concernant l'entreprise israélienne Rayzone, dont les liens avec l'opérateur anglo-normand Sure Guernsey ont laissé penser qu'elle utilisait ce réseau pour avoir accès aux capacités de localisation de l'opérateur. Les autorités britanniques, par le biais du *Telecommunications Security Bill* voté à la fin 2021, ont tenté de limiter la capacité pour les opérateurs anglo-normands (indépendants en matière de télécommunications) de pouvoir servir de plateformes d'accès à des sociétés d'interceptions [37].

Commentaire : l'utilisation du protocole SS7 et des infrastructures ouvertes de signalisation perdure depuis le développement de la 2G, mais pourrait progressivement disparaître avec le développement de la 5G. Cependant, la problématique de la localisation précise des appareils, et donc de personnes potentiellement ciblées, demeure. En effet, les initiatives d'interconnexion des matériels et logiciels impliqués dans la 5G, telles qu'OpenRAN, bien qu'elles fournissent des opportunités de sécurisation, permettront aussi la vente de localisation en temps réel pour de multiples applications. Des attaquants pourraient saisir cette opportunité pour accéder aux données de localisation en se faisant passer pour des partenaires légitimes des opérateurs de télécommunications.

4. Menace à finalité de déstabilisation

Le secteur des télécommunications est susceptible d'être la cible d'attaques ayant pour finalité la déstabilisation. Le besoin de disponibilité constante des réseaux de télécommunications entraîne une vulnérabilité particulière du secteur à ces attaques, qui peuvent être effectuées au moyen de déni de service ou par du sabotage. L'exposition publique de données des opérateurs peut parfois relever également de la déstabilisation.

4.1. Attaques par déni de service distribué

En 2019, un ressortissant anglais agissant comme attaquant mercenaire a été jugé pour avoir pratiqué des attaques par déni de service distribué (DDoS) intermittentes contre l'opérateur de télécommunications du Liberia Lonestar MTN, à l'aide de réseaux de *botnets* (dont Mirai), à partir de 2015. Il aurait été recruté par un dirigent de CellCom, opérateur rival de Lonestar MTN au Liberia. Ses attaques auraient eu un fort impact, allant jusqu'à interrompre totalement l'accès à Internet au Liberia en novembre 2016. Elles ont entraîné des pertes de plusieurs millions de dollars pour l'opérateur ciblé. Lors de son arrestation en 2017, cet attaquant mercenaire aurait été extradé vers l'Allemagne pour y être jugé pour des faits similaires à l'encontre de l'opérateur Deutsche Telekom [38].

Un fournisseur d'accès Internet sud-africain a subi en septembre 2019 deux jours d'attaque par DDoS très intense,

rendant inopérantes ses connexions avec les autres fournisseurs d'accès. Afin de contourner les mesures anti-DDoS de l'entreprise, les attaquants ont envoyé le trafic non pas sur le serveur principal du FAI, mais sur de nombreuses adresses IP publiques différentes du FAI [39].

Dans le cadre des vagues d'attaques par DDoS ciblant régulièrement des entités occidentales depuis le début de l'invasion russe de l'Ukraine en février 2022, de nombreux opérateurs de télécommunications européens ont été ciblés par des groupes hacktivistes pro-russes.

4.2. Attaques entraînant la publication de données

En novembre 2019, l'opérateur Lyca Mobile a été ciblé par la branche italienne des hacktivistes d'*Anonymous* et de *LulzSecITA*, qui par un moyen non détaillé dans la presse, a exfiltré et publié des données d'identité, de téléphonie et de cartes de crédit, dans le but affiché de dénoncer le manque de sécurité de l'entreprise [40].

4.3. Attaques par sabotage

Le 24 février 2022, au soir du déclenchement de l'invasion russe en Ukraine, une attaque a mis hors d'état de fonctionner des milliers de modems de l'opérateur satellitaire Viasat en leur envoyant une mise à jour malveillante qui a compromis l'intégrité du *firmware* (micrologiciel) des terminaux visés, les rendant ainsi inopérants. La concomitance avec le début de la guerre et les conséquences importantes sur le satellite Ka-Sat, utilisé par l'armée ukrainienne, indiquent avec une forte probabilité un ciblage initial de l'Ukraine afin de saboter les capacités de communication de son armée. Le débordement de l'attaque vers d'autres opérateurs satellitaires européens pourrait avoir été involontaire. Les conséquences de cette action de sabotage ont été importantes, y compris hors de l'Ukraine. En France, environ 10 000 abonnés ont été touchés. Des services de l'opérateur NordNet (utilisateur du satellite Ka-Sat) ont été affectés en France, en République tchèque et en Allemagne, où près de 5 800 éoliennes pilotées *via* le réseau satellitaire ont été mises à l'arrêt [41]. Cette attaque a été attribuée par l'Union européenne et ses États-membres, les États-Unis d'Amérique, le Canada et le Royaume-Uni, à la Russie le 10 mai 2022 [42].

D'après le CERT-UA ukrainien [43], entre le 11 mai et le 27 septembre 2023, un groupe organisé d'attaquants informatiques aurait mené des attaques visant à perturber les activités d'au moins 11 fournisseurs d'accès à Internet ukrainiens. Ces attaques auraient entraîné des interruptions dans la fourniture des services aux clients de ces FAI. Le CERT-UA suit ce groupe d'attaquants sous le nom UAC-0165, qui correspond au mode opératoire SANDWORM [44]. Le MOA SANDWORM est attribué publiquement au renseignement militaire russe (GRU) par plusieurs gouvernements européens et américain [45, 46]. Les opérateurs de SANDWORM concentreraient leurs efforts d'espionnage et de sabotage contre des entités ukrainiennes appartenant à de nombreux secteurs, en soutien à l'invasion militaire russe [47].

Commentaire : le ciblage de moyens de communication ukrainiens au moyen de MOA réputés russes s'inscrit dans le contexte de l'invasion de l'Ukraine par la Russie. Les forces russes cherchent ainsi à porter atteinte aux moyens de communications des forces armées ukrainiennes aussi bien que des moyens de communication et d'information de la population civile. Les effets recherchés de ces attaques sont à la fois tactiques en soutenant les forces armées russes d'occupation, et psychologiques, en portant atteinte aux services ukrainiens d'importance vitale.

4.4. Atteintes physiques au réseau

Le secteur des télécommunications, s'il est particulièrement vulnérable aux attaques informatiques, est également la cible d'attaques ou d'actions intrusives non strictement liées à des actions cyber.

Ainsi, dès le mois de mars 2022, l'opérateur ukrainien Ukrtelecom a annoncé restreindre l'accès aux consommateurs afin de privilégier et protéger les communications militaires et dédiées aux infrastructures critiques. En effet, à la fin du mois de mars les infrastructures physiques ukrainiennes étaient très largement touchées par des destructions, laissant en activité seulement 13% du réseau, avec un effet national sur la disponibilité des communications [48].

Dans les villes occupées par l'armée russe, des cas d'intervention physique des forces armées occupantes chez les FAI locaux ont été rapportés. Ainsi à Kherson en mai 2022, des FAI locaux ont déclaré avoir été forcés de se raccorder aux réseaux russes sous la menace de confiscation de leurs équipements par l'armée russe [49].

Les infrastructures des opérateurs français ont été touchées plusieurs fois par des coupures de câbles volontaires, telles que celle affectant plusieurs FAI à la fin du mois d'avril 2022 : plusieurs coupures simultanées de câbles dans l'Est et le Centre-Est de la France ont affecté les communications pendant plusieurs heures. De même, un câble sous-marin a été coupé près de Marseille en octobre 2022. Les motivations des responsables de ces opérations de sabotage physique ne sont pas connues [50].

5. Recommandations

Les recommandations suivantes visent à éclairer les OCE et à leurs clients professionnels, afin de bâtir une défense et à se prémunir des menaces détaillées précédemment. Ces recommandations ne sont pas exhaustives et doivent être adaptées et complétées dans le cadre du contexte opérationnel et fonctionnel du système d'information considéré.

Ces recommandations portent sur les thèmes suivants :

- la sensibilisation ;
- les postes de travail ;
- l'infrastructure ;
- l'administration du système d'information ;
- le maintien en conditions de sécurité ;
- la journalisation et la détection.

5.1. Sensibilisation

R1

Communiquer de manière régulière

Organiser des sessions de sensibilisation régulièrement afin de responsabiliser les administrateurs et exploitants, les prestataires, mais aussi les collaborateurs traitants des données clients. Les objectifs majeurs sont de mettre l'accent sur les enjeux de cybersécurité, et de transmettre les bonnes pratiques à adopter dans leurs missions respectives.

Pour l'ensemble des utilisateurs, des administrateurs et exploitants du système, communiquer les précautions suivantes :

- ne pas ouvrir les messages dont la provenance ou la forme est inconnue, car il pourrait s'agir d'une tentative d'attaque (par exemple un rançongiciel) ;
- se méfier des extensions de pièces jointes douteuses (exemples : .pif ; .com ; .bat ; .exe ; .vbs ; .lnk…), qui peuvent contenir des codes malveillants ;
- être vigilant face aux URL visitées depuis le poste de travail ;
- ne pas connecter sur son poste de travail une clé USB trouvée par hasard, car celle-ci pourrait être compromise par un logiciel malveillant.

Pour les administrateurs de cœurs de réseaux, il est important d'axer la communication autour des thèmes suivants :

- les administrateurs représentent des cibles particulières pour les attaquants de par la nature de leurs missions et les accès et les secrets d'authentification dont ils disposent ;
- de ce fait, les administrateurs doivent protéger leurs moyens et leurs ressources encore davantage, avec un niveau de vigilance et de sécurité supplémentaires par rapport aux utilisateurs (cf. notamment les recommandations du paragraphe 5.4) ;
- les administrateurs doivent agir sur la mise en œuvre des bonnes pratiques d'administration et d'architecture sur les SI dont ils ont la charge.

R2

S'exercer régulièrement

En complément des sessions de sensibilisation, il est nécessaire de mettre en place des exercices adaptés pour accroitre la vigilance des utilisateurs, des administrateurs et des exploitants. En particulier :

Pour les utilisateurs, administrateurs et exploitants du système d'information, mettre en pratique des exercices sur les attaques suivantes :

- hameçonnage par messagerie électronique ;
- hameçonnage par support USB ;
- ingénierie sociale visant à obtenir des informations sensibles des clients ou à mener des opérations sur les SI métier de l'OCE.

Pour les administrateurs et exploitants du SI, mettre en pratique le scénario suivant :

- intrusion sur le cœur de réseau (notamment les services d'authentification ou de routage) et sur les équipements des réseaux de collecte ;
- reconstruction de tout ou partie du cœur de réseau ;
- activation des plans de reprise et de continuité d'activité ;
- réinitialisation des secrets d'administration des équipements de cœurs de réseaux et des équipements de raccordement des clients (exemple : routeur client).

5.2. Protection du SI bureautique et des SI métier de l'OCE (exemples : SI en agence clients, SI facturation, etc.)

R3

Déployer une passerelle Internet sécurisée

Afin de protéger le SI bureautique des menaces liées à l'accès Internet, il est recommandé de construire la passerelle de la manière suivante [51] :

- rendre incontournable la passerelle Internet sécurisée pour les flux entrants et sortants du système d'information (Web et mail) ;
- mettre en œuvre des pare-feu après le routeur d'accès Internet et devant le SI interne pour constituer une ou plusieurs zones (DMZ) ;
- déployer des services applicatifs de relais dans la ou les DMZ avec des mesures de protection et de détection de codes malveillants.

R4

Segmenter et filtrer au sein du système d'information

Afin d'éviter la propagation et la latéralisation d'une attaque, il est recommandé de segmenter et cloisonner le SI en plusieurs zones de sécurité homogènes (par sensibilité, criticité ou autres critères métier). Les mesures de cloisonnement devront reposer sur des mécanismes réseau, de chiffrement, de stockage et d'identification/authentification.

Devront notamment être segmentés :

- le SI bureautique ;
- le SI opérateur : réseau hébergeant les outils annexes du cœur de réseau (facturation, gestion des abonnés, etc.) ;
- le réseau d'administration, hébergeant les outils dits O&M (« *Operation and Maintenance* ») ;
- le « cœur paquet » ou « cœur data » ;
- le cœur voix ou IMS.

R5

Appliquer une gestion stricte des comptes utilisateurs administrateurs et droits d'accès aux informations et aux services applicatifs (principe du moindre privilège)

L'objectif visé consiste à appliquer le principe de moindre privilège pour chacun des accès à tout ou partie du système d'information, en vue notamment :

- de se protéger de la menace interne (collaborateurs malveillants et prestataires) ;
- d'identifier les accès illégitimes aux informations sensibles (bases de comptes clients, EMEI, IMSI, SIMs, données de géolocalisation, etc.) ;
- de restreindre l'accès aux différentes ressources d'administration aux seules personnes en ayant le besoin.

Une revue des comptes et des privilèges devra être réalisée au moins une fois par an afin :

- de vérifier la légitimité des accès, notamment ceux des prestataires ;
- de verrouiller, voire supprimer les comptes inutilisés.

R6

Mettre en œuvre des contre-mesures aux attaques en déni de service pour protéger les services clients proposés sur Internet

Il est notamment recommandé :

- de distinguer les accès Internet des services non sensibles, de ceux pour les services critiques (par exemple, les services permettant aux clients permettant de gérer leur compte ou encore les services applicatifs métiers dédiés aux partenaires des OCE) ;
- de limiter les connexions clients ;
- de déployer une solution de protection anti-DDos [52].

R7

Mettre en œuvre une politique de MCO et MCS pour les SI

Veiller à définir et appliquer une politique de maintien en condition opérationnelle (MCO) et de maintien en condition de sécurité (MCS) afin de renforcer la sécurité et la stabilité du SI. **En priorité, appliquer les correctifs de sécurité sur les équipements et services directement exposés sur Internet, sachant qu'ils sont particulièrement exposés aux attaques cyber.**

R8

Définir une politique de sauvegarde des données métiers de l'OCE

Afin de pallier la corruption ou l'indisponibilité de données dues à un incident ou une compromission (par exemple, liée à un rançongiciel), une politique de sauvegarde régulièrement mise à jour doit être définie, appliquée et testée. Pour les éléments les plus critiques, une sauvegarde hors ligne doit être prévue afin de garantir une restauration en cas d'attaque par rançongiciel. Les sauvegardes doivent être chiffrées afin d'en garantir la confidentialité et l'intégrité. Les procédures devront notamment être adaptées pour prendre en compte le risque interne induit par le choix de la solution de sauvegarde.

En particulier :

- ne pas oublier d'inclure les médias d'installation et les configurations des applications métier dans les sauvegardes ;
- réaliser régulièrement et impérativement des sauvegardes hors-ligne (déconnectées du SI) pour les données et les services les plus sensibles pour l'OCE ou ses clients ;
- définir une stratégie de restauration, en lien avec votre PRA et en tenant compte des principaux scénarios d'attaque identifiés sur les SI (rançongiciel, espionnage, etc.) ;
- tester régulièrement et impérativement les procédures de restauration.

R9

Mettre en œuvre un contrôle d'accès physique

Afin de protéger physiquement l'accès aux locaux de l'OCE du public et de toutes personnes non autorisées, il est recommandé de mettre en œuvre un système de contrôle d'accès physique et si possible un système de vidéoprotection [53].

5.3. Sécurisation des cœurs de réseau fixe et mobile

R10

Disposer d'une cartographie précise du cœur de réseau

Recenser tous les éléments constitutifs du cœur de réseau afin d'en connaître les moindres détails, en particulier les interconnexions entre chaque zone de sensibilité et avec des systèmes tiers. L'objectif de la cartographie du SI est de connaître l'ensemble des éléments qui le constituent pour en obtenir une meilleure lisibilité et donc un meilleur contrôle. La cartographie doit permettre de représenter le système d'information sous forme de vues : l'écosystème, métier, applicatif, logique, physique [54].

R11

Identifier précisément l'ensemble des services nécessitant une interconnexion et donc une exposition à Internet ou avec des SI tiers

Établir de manière exhaustive la liste des services du cœur de réseau (identification/authentification des clients, équipements de *roaming*, services applicatifs de facturation, etc.). Cette liste doit permettre de protéger ces interconnexions de la manière la plus adaptée, notamment :

- en n'autorisant que les flux strictement utiles ;
- en mettant en œuvre une veille spécifique sur les vulnérabilités et les correctifs de sécurité ;
- en déployant un dispositif de détection des incidents de sécurité adapté.

Cette liste doit être à jour et revue régulièrement.

R12

Segmenter et filtrer les systèmes et les sous-systèmes par zones de sécurité ou de fonctions métiers homogènes en portant un soin particulier à protéger les cœurs de réseau

Notamment, cloisonner et filtrer par des mesures réseaux, d'authentification et de chiffrement et/ou applicatives :

- les cœurs de réseaux des autres SI de l'OCE (SI bureautiques de OCE, SI de facturation, des SI des agences clients, etc.) ;
- dans les cœurs de réseaux, les fonctions « *user plane* » et « *control plane* » (pour la 4G+ et la 5G) ;
- les différents sous-réseaux au sein du cœur de réseau (déploiement, métier, O&M, IL (interceptions légales), etc.). Par exemple, les interfaces d'administrations ne doivent pas être accessibles depuis une interface métier.

R13

Limiter au strict besoin l'exposition des équipements composants l'infrastructure de cœur de réseau à Internet ou à des services tiers

L'objectif consiste à limiter au strict minimum la surface d'exposition aux attaques et à adopter des mesures particulières de protection et de défense.

R14

Protéger les interconnexions avec les cœurs de réseaux avec les autres opérateurs

Ces mesures de protection doivent concerner les équipements d'interconnexion, mais également les flux techniques et les communications clientes. Pour ces dernières, il est important de s'assurer de l'authenticité et de la légitimité des communications traitées.
Il conviendra notamment de mettre en place des instances dédiées des NF de signalisation pour assurer le *roaming* qui soient différentes de celles utilisées pour la signalisation des communications domestiques.

R15

Maîtriser les infrastructures d'hébergement des équipements et des services constituant le cœur notamment les infrastructures basées sur les technologies de virtualisation

À l'instar de n'importe quel système d'information virtualisé ou s'appuyant sur des technologies *Cloud*, la compromission ou l'accès frauduleux à l'infrastructure d'hébergement garantit *in fine* à l'attaquant un accès total aux services qu'elle héberge. Il est donc primordial de s'assurer que l'infrastructure d'hébergement :

- est de confiance ;
- offre un niveau de garantie et de sécurité suffisant (notamment dans ses pratiques d'administration et d'exploitation) et au moins équivalent à ceux attendu pour la sécurité du cœur de réseau ;
- est accédée uniquement par des personnes dûment autorisées.

Une attention particulière devra être portée sur les éventuels prestataires et sous-traitants disposant de droits d'administration, d'exploitation et de supervision. Ces tiers utiliseront nécessairement des accès techniques en administration et des comptes à privilèges qu'un attaquant pourrait exploiter pour compromettre le cœur de réseau. De la même manière, un personnel interne malveillant pourra utiliser ses droits et privilèges pour mener des actions frauduleuses pour le compte d'un attaquant externe.

R16

Mettre en œuvre une politique d'identification d'authentification et de gestion des droits (RBAC) permettant de gérer l'ensemble des équipements constitutifs du cœur de réseau et des différents comptes y ayant accès

L'objectif consiste à appliquer au mieux le principe de moindre privilège sur l'ensemble des accès techniques ou humains nécessaires au bon fonctionnement du service, afin de se prémunir des menaces internes (collaborateurs malveillants et prestataires) ou externes souhaitant compromettre tout ou partie du système. En complément, il est également primordial de mettre en œuvre des procédures techniques et organisationnelles visant à identifier et détecter les accès illégitimes ou frauduleux aux services et aux informations sensibles.

R17

Assurer une revue périodique des droits d'accès et des privilèges et de leur alignement avec la politique de sécurité

L'objectif de cette revue est de s'assurer que tous les comptes sont légitimes et que les droits des personnes ayant changé de fonction ont bien été modifiés en conséquence. La périodicité de cette revue doit être adaptée à la criticité des comptes et

- au moins annuelle pour une revue globale
- trimestrielle pour les comptes ayant de plus hauts privilèges ou pouvant avoir un impact systémique sur le système

R18

Sécuriser la configuration des équipements et des logiciels utilisés

Afin de contribuer à la réduction de la surface d'attaque, la configuration des équipements du SI doit être minimaliste et durcie, et l'intégrité de ces équipements doit être vérifiée régulièrement.
En particulier :

- n'installer que les services strictement utiles sur les équipements ;
- les configurations des serveurs (physique et virtuel) sont durcies (suppression des mots de passe par défaut, suppression des programmes inutile, etc.) ;
- l'intégrité des *firmware* et microcodes installés sur les équipements du SI (serveurs, équipements réseau, poste de travail, etc.) sont vérifiés ;
- les accès aux interfaces de gestion matérielle (IDRAC, ILO, IPMI) sont maîtrisés (exemple : accessibles depuis un VPN avec une authentification double facteur si exposés sur internet…).

R19

Maîtriser le processus et l'hébergement des mécanismes de personnalisation des cartes SIMs

En particulier :

- l'hébergement des services et des équipements contribuant à la confection et la personnalisation des cartes ;
- la génération (notamment la qualité de l'aléa) et la gestion des secrets qui ont vocation à être déployés sur les cartes SIMs ;
- le processus de personnalisation des cartes SIMs pour l'OCE.

Ces mesures de sécurité doivent également prendre en compte les cas de sous-traitance et les risques d'attaques liés à ces tiers (cf. attaque par « *supply chain* »). Il conviendra de déterminer toutes les mesures de sécurité appropriées pour protéger les accès privilégiés à ces dispositifs et services.

R20

Prévenir et contrôler les actions de « *SIM swapping* »

Les actions de « *SIM swapping* » consistent à migrer le numéro de téléphone d'un abonné sur une autre carte SIM que celle précédemment utilisée. Cette action peut être détournée par un acteur malveillant pour prendre le contrôle du compte d'un abonné afin de d'accéder à ses données ou prendre possession de ses secrets d'authentification. Cette pratique frauduleuse peut être également utilisée pour contourner les protections apportées par certaines implémentations d'authentification multifacteurs (M2FA), s'appuyant sur les SMS.

Afin de protéger les usagers du réseau, mais aussi les personnels de l'OCE utilisant des authentifications M2FA par SMS, il convient de renforcer les processus autorisant le *SIM swapping*, notamment :

- en temporisant de 24h la mise en œuvre effective de la nouvelle carte SIM ;
- en prévenant l'usager, propriétaire de la carte SIM, de l'action demandée.

5.4. Sécurisation des échanges entre les terminaux des usagers et le cœur de réseau

R21

Identifier et authentifier les appels des usagers acheminés par les cœurs de réseau

L'objectif de cette mesure consiste à éviter les usurpations d'appels traités et acheminés par les cœurs de réseaux. Ceci peut être mis en œuvre en appliquant conjointement une série de mesures, par exemple :

- déployer STIR-SHAKEN sur l'ensemble du réseau opérateur, en prenant soin de protéger les clés de signature des OCE contre tout vol ou altération ;
- identifier et authentifier les usagers du réseau de communication sur les équipements d'extrémité du réseau (par exemple les équipements RAN) ;
- appliquer une signature électronique, basée sur des mécanismes cryptographiques, sur les paquets de signalisation des communications voix (par exemple, la signature électronique des en-têtes SIP).

R22

S'assurer que les algorithmes cryptographiques d'identification et d'authentification sont conformes aux recommandations du guide des mécanismes cryptographiques

Voir le Guide de l'ANSSI sur les mécanismes cryptographiques [55].

5.5. Administration du système d'information

R23

Supprimer les accès d'administration *via* des interfaces exposées directement sur Internet

Les services d'administration sont particulièrement ciblés lors des attaques cyber. Leur exposition sur Internet facilite le travail des attaquants. Il convient de ne pas les exposer directement sur Internet et de limiter strictement leur accès aux administrateurs de l'entité. Par exemple, en protégeant les accès opérateurs non sécurisés des administrateurs (ex : telnet, tftp, etc.) au travers d'un VPN avec une authentification à double facteurs.
Pour les OCE, cela concerne plus particulièrement :

- les équipements de cœur de réseau ;
- les équipements de raccordement au réseau (eNode B, etc.) ;
- les équipements de raccordement des abonnés et clients ;
- les accès d'administration des prestataires et sous-traitants.

R24

Administrer le SI depuis un réseau dédié

Les ressources d'administration (ex. : postes d'administration, serveurs et outils d'administration) restent à ce jour une cible privilégiée des attaquants. Leur compromission garantit un accès général et discret à l'ensemble de l'infrastructure de l'OCE. Elles doivent être déployées sur un réseau dédié à cet usage et ne pas être exposées aux menaces provenant d'Internet.
L'objectif consiste essentiellement à se prémunir des risques de compromission liés à une navigation Internet par la présence, par exemple, d'un code malveillant (de type javascript) sur une page Web, ou à l'accès à un courriel ou une pièce jointe malveillants [56].

R25

Utiliser un poste d'administration dédié et durci

L'utilisation d'un poste d'administration physiquement dédié et durci pour les actions d'administration est recommandée. Ce poste d'administration doit être distinct du poste bureautique et doit faire partie intégrante du SI d'administration. Ce poste d'administration ne doit pas disposer d'accès à Internet. L'usage de ce type de poste dédié est notamment considéré comme indispensable pour les actions nécessitant des privilèges élevés (comptes dit « rouges ») permettant l'administration des ressources les plus sensibles :

- des cœurs de réseaux : serveurs d'authentification, base de gestion des abonnés, service de gestion des secrets et des certificats ;
- et des infrastructures d'hébergement sous-jacentes.

À défaut d'un poste dédié, il conviendra d'atteindre l'objectif de sécurité visant à protéger le poste et les ressources d'administration des menaces provenant d'Internet (Web/mail). Le principal risque à traiter consiste en la compromission d'un poste d'administration après une navigation sur Internet, la réception d'un mail piégé ou l'ouverture d'un document contenant un code malveillant. Cette primo-compromission permet à un attaquant de prendre le contrôle du poste et de se latéraliser sur le SI d'administration puis sur le cœur de réseau.

R26

Protéger les secrets de chiffrement et d'authentification permettant la gestion et l'administration des réseaux de collecte et de transport

En particulier :

- utiliser des protocoles et mécanismes cryptographiques qui assurent la confidentialité des secrets et l'authentification mutuelle des flux d'administration, conformément aux guides de l'ANSSI [5] ;
- pour les protocoles ne permettant pas la mise en œuvre de la règle précédente, encapsuler les flux dans des protocoles de transport sécurisés (IPsec ou TLS par ex.). Ceci permet d'assurer confidentialité et l'authentification conformément aux guides précédemment cités ;
- ne pas réutiliser un même secret pour différents périmètres techniques d'exploitation (administration, zones de sensibilité, différents sous-traitants, etc.) ;
- ne pas utiliser un même secret pour différents équipements, situés dans des zones de confiance et de sécurité distinctes ;
- s'assurer que les secrets sont générés et sélectionnés conformément aux recommandations de l'ANSSI [6] ;
- s'assurer que le cycle de vie des secrets est conforme aux recommandations de l'ANSSI [7].

R27

Déployer une authentification forte pour les accès administrateurs voire une authentification multi-facteur pour les accès à hauts privilèges et les équipements critiques

5.6. Sécurisation des services DNS

R28

Cloisonner physiquement les infrastructures entre services DNS internes et externes

Le niveau de menace induit par une exposition à Internet impose un cloisonnement physique des infrastructures entre différents services DNS, qu'ils soient internes ou externes (par exemple, ceux proposés aux clients et abonnés). Comme tous les services exposés ou accédant à Internet, les services DNS externes doivent être placés dans une passerelle d'interconnexion sécurisée avec des ressources dédiées (serveurs, pare-feux, commutateurs). À l'inverse, le service DNS interne doit rester à l'intérieur du SI de l'entité.
En particulier :

- déployer les services DNS internes et externes sur des serveurs physiquement distincts et traiter des zones DNS différentes ;
- interdire les flux entre services DNS internes et externes.

R29

Déployer des serveurs primaires cachés (*Hidden masters*)

Un serveur *hidden master* est un serveur primaire ayant la particularité de n'interagir qu'avec les serveurs secondaires et, plus particulièrement, de n'autoriser les transferts de zone qu'à destination de ces derniers. En particulier, les clients finaux et les serveurs récursifs ne sont pas autorisés à lui soumettre de requêtes. Dans le contexte d'un service d'hébergement des noms de domaine Internet, ces serveurs *Hidden masters* n'apparaissent pas dans les enregistrements de la zone DNS.

R30

Restreindre la capacité de procéder à des transferts de zones

Les actions de transfert de zone ne doivent être autorisés que pour les serveurs DNS en ayant strictement le besoin pour le bon fonctionnement du système. Par ailleurs, la protection en intégrité des transferts de zones entre les serveurs primaires et secondaires doit être assurée au minimum avec le protocole TSIG.

5. « Règles et recommandations concernant les choix et le dimensionnement de mécanismes cryptographiques [55]» et « Guide de sélection d'algorithmes cryptographiques [57] ».
6. Voir le « Guide de sélection d'algorithme cryptographiques » pour les choix de tailles de clé [57], et « Règles et recommandations concernant les choix et le dimensionnement de mécanismes cryptographiques » pour le cycle de vie des clés [55].
7. Voir le guide « Recommandations relatives à l'authentification multifacteurs et aux mots de passe » [58].

R31

Suivre les recommandations du guide de l'ANSSI sur la gestion des noms de domaine

Pour assurer le maintien en disponibilité du service DNS d'hébergement des noms de domaine Internet, il est nécessaire d'appliquer les recommandations du guide de l'ANSSI sur l'exploitation de noms de domaine [8], en particulier son chapitre sur la résilience des services.
En particulier :

- la mise à jour des serveurs DNS secondaires est réalisée directement sur le serveurs primaire « *hidden master* » ;
- si besoin, la mise à jour des serveurs DNS secondaires hébergés à l'extérieur du SI est réalisée à travers un serveur intermédiaire dit « tampon » qui assure à la fois une fonction de serveur primaire pour les secondaires externes, et une fonction de serveur secondaire vis-à-vis du serveur primaire « *hidden master* » ;
- tous les transferts de zone doivent être protégés en intégrité au moyen du protocole TSIG ;
- les accès au serveur primaire « *hidden master* » depuis les serveurs secondaires et tampon doivent être filtrés entre la zone des services relais et la zone des services internes.

R32

Mettre en œuvre des mesures de protection anti-DDoS pour le service DNS externe exposé à Internet

Il est recommandé de mettre en place un service anti-DDoS avec des mesures de détection et de remédiation adaptées spécifiquement au service DNS d'hébergement des noms de domaine Internet.

5.7. Journalisation et détection

R33

Mettre en place un système de journalisation adapté

Les journaux d'événements représentent une source d'information essentielle, tant pour la recherche et la correction d'incidents d eproduction que pour la détection d'incidents de sécurité, et doivent couvrir l'ensemble des domaines techniques (systèmes, réseaux, tentatives de connexion, etc.).
En raison de la grande variété de journaux pouvant être collectés sur une infrastructure de communication et du volume important que cela peut représenter pour le stockage et le traitement, la politique de journalisation devra déterminer la finesse de collecte de chaque source afin de répondre au besoin sans surcharger le système. L'architecture de ce système devra permettre la collecte, la conservation, la sécurisation et la gestion, quelle que soit la nature et la taille de ces journaux. Pour une infrastructure de communication et vu les éléments de menace décrits dans ce document, il convient de prendre en compte au moins la journalisation pour les équipements de collecte, les interfaces d'administration, les systèmes de virtualisation ainsi que les fonctions réseau les plus sensibles pour le fonctionnement de l'infrastructure [60].

8. Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine [59]

R34

Déployer un dispositif de détection des incidents de sécurité sur les cœurs de réseaux

S'appuyant sur une stratégie de détection des incidents de sécurité et la collecte adaptée des journaux d'événements, ce dispositif de détection doit permettre d'identifier au plus tôt tous comportements malveillants (tentative d'attaque) ou frauduleux (actions illégitimes de la part d'un employé ou sous-traitant) sur les équipements du cœur de réseau ou les autres SI métier de l'OCE (ex : SI de facturation, accès aux SI de gestion de clients, etc.)

R35

Anticiper la gestion d'une crise cyber

La préparation des équipes d'administration et d'exploitation de l'OCE à la gestion d'une crise cyber est essentielle pour assurer une réaction rapide et adaptée en cas d'attaque réelle.
En particulier :

- prévoir une organisation et des procédures de gestion de crise ;
- consolider un annuaire de gestion de crise avec les coordonnées de l'ensemble des acteurs utiles ;
- identifier et préparer les équipes aux premières actions d'urgence et conservatoires pour protéger *a minima* le service et restreindre les activités malveillantes ;
- élaborer un PRA/PCA ;
- réaliser des exercices de gestion de crise

5.8. Voir également

- ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory*, 2023 [61] ;
- ANSSI, *Recommandations sur le nomadisme numérique*, 2018 [62].

A. Bibliographie

[1] SGDSN. *Revue stratégique de cyberdéfense*. 12 février 2018.
URL : http://www.sgdsn.gouv.fr/publications/revue-strategique-de-cyberdefense.

[2] IBTIMES. *China Arrests 1,500 People for Sending Spam Text Messages from Fake Mobile Base Stations*. 27 mars 2014.
URL : https://www.ibtimes.co.uk/china-arrests-1500-people-sending-spam-text-messages-fake-mobile-base-stations-1442099.

[3] EUROPOL. *Cyber-Telecom Crime Report 2019*. 21 mars 2019.
URL : https://www.europol.europa.eu/publications-documents/cyber-telecom-crime-report-2019.

[4] ZDNET. *Cybersécurité : un opérateur italien propose de remplacer les cartes SIM de ses abonnés après une attaque*. 6 janvier 2021.
URL : https://www.zdnet.fr/actualites/cybersecurite-un-operateur-italien-propose-de-remplacer-les-cartes-sim-de-ses-abonnes-apres-une-attaque-39915645.htm.

[5] IT WORLD CANADA. *Koodo Admits February Data Breach, Data Already Being Sold on Dark Web*. 9 mars 2020.
URL : https://www.itworldcanada.com/article/koodo-admits-february-data-breach-data-already-being-sold-on-dark-web/428249.

[6] GBHACKERS ON SECURITY. *Virgin Media Hacked - Hackers Breached the Database*. 6 mars 2020.
URL : https://gbhackers.com/virgin-media-hacked/.

[7] KREBS ON SECURITY. *A Closer Look at the LAPSUS$ Data Extortion Group – Krebs on Security*. 23 mars 2022.
URL : https://krebsonsecurity.com/2022/03/a-closer-look-at-the-lapsus-data-extortion-group/.

[8] ZDNET. *AT&T Employees Took Bribes to Plant Malware on the Company's Network*. 6 août 2019.
URL : https://www.zdnet.com/article/at-t-employees-took-bribes-to-plant-malware-on-the-companys-network/.

[9] ZDNET. *European ISPs Report Mysterious Wave of DDoS Attacks*. 3 septembre 2020.
URL : https://www.zdnet.com/article/european-isps-report-mysterious-wave-of-ddos-attacks/.

[10] BLEEPING COMPUTER. *VoIP.Ms Phone Services Disrupted by DDoS Extortion Attack*. 20 septembre 2021.
URL : https://www.bleepingcomputer.com/news/security/voipms-phone-services-disrupted-by-ddos-extortion-attack/.

[11] FORTUNE. *Capital One Hacker Also Hit a Major University and Telecom Provider Indictment Says*. 29 août 2019.
URL : https://fortune.com/2019/08/29/indictment-capital-one-hacker/.

[12] SYMANTEC. *Whitefly : Espionage Group Has Singapore in Its Sights*. 6 mars 2019.
URL : https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/whitefly-espionage-singapore.

[13] SYMANTEC. *Buckeye : Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak*. 7 mai 2019.
URL : https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit.

[14] MICROSOFT. *GALLIUM : Targeting Global Telecom*. 12 décembre 2019.
URL : https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/.

[15] CYBEREASON. *Operation Soft Cell : A Worldwide Campaign Against Telecommunications Providers*. 25 juin 2019.
URL : https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers.

[16] REUTERS. « Hackers Steal Data from Telcos in Espionage Campaign : Cyber Firm ». 25 juin 2019.
URL : https://www.reuters.com/article/us-cyber-telecoms-cybereason-idUSKCN1TQ0BC.

[17] REUTERS. « China Hacked Asian Telcos to Spy on Uighur Travelers : Sources ». 5 septembre 2019.
URL : https://www.reuters.com/article/us-china-cyber-uighurs-idUSKCN1VQ1A5.

[18] CYBERSCOOP. *Suspected Espionage Campaign Targets Telecoms, IT Service Firms in Middle East*. 14 décembre 2021.
URL : https://cyberscoop.com/new-iranian-hacking-activity-muddywater-seedworm/.

[19] Security Affairs. *Lebanese Cedar APT Group Broke into Telco and ISPs Worldwide*. 28 janvier 2021.
URL : https://securityaffairs.co/wordpress/113975/apt/lebanese-cedar-apt-attacks.html.

[20] Nextinpact. *Espionnage de la NSA via un câble sous-marin : Orange réagit*. 30 décembre 2013.
URL : https://www.nextinpact.com/article/10240/85134-espionnage-nsa-via-cable-sous-marin-orange-reagit.

[21] Mer et Marine. *Câbles sous-marin et espionnage : le point avec Jean-Luc Vuillemin | Mer et Marine*. 9 juin 2021.
URL : https://www.meretmarine.com/fr/marine-marchande/cables-sous-marin-et-espionnage-le-point-avec-jean-luc-vuillemin.

[22] CyberScoop. *DHS Investigators Say They Foiled Cyberattack on Undersea Internet Cable in Hawaii*. 13 avril 2022.
URL : https://www.cyberscoop.com/undersea-cable-operator-hacked-hawaii/.

[23] ANSSI. *Campagne d'attaque du mode opératoire APT31. Description et contre-mesures*. 25 novembre 2021.
URL : https://cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-012/.

[24] CISA. *People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices | CISA*. 7 juin 2022.
URL : https://www.cisa.gov/uscert/ncas/alerts/aa22-158a.

[25] NSCS-UK. *Cyclops Blink*. 23 février 2022.
URL : https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf.

[26] Kaspersky. *The Slingshot APT*. 9 mars 2018.
URL : https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/09133534/The-Slingshot-APT_report_ENG_final.pdf.

[27] NCSC-UK. *The Future of Telecoms in the UK*. 28 janvier 2020.
URL : https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk.

[28] Computerworld. *FCC Revokes Authorisation of China Telecom's US Unit - Telco/ISP - Security - iTnews*. 27 octobre 2021.
URL : https://www.itnews.com.au/news/fcc-revokes-authorisation-of-china-telecoms-us-unit-571820.

[29] Netnod. *Statement on Man-in-the-Middle Attack against Netnod*. 5 février 2019.
URL : https://www.netnod.se/news/statement-on-man-in-the-middle-attack-against-netnod.

[30] ZDNet. *Hackers Breached Greece's Top-Level Domain Registrar*. 9 juillet 2019.
URL : https://www.zdnet.com/article/hackers-breached-greeces-top-level-domain-registrar/.

[31] DHS. *Hunting Russian Intelligence 'Snake' Malware*. 9 mai 2023.

[32] Kaspersky. *Satellite Turla : APT Command and Control in the Sky*. 15 septembre 2015.
URL : https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/.

[33] Amnesty International. *Un journaliste marocain victime d'attaques par injection réseau au moyen d'outils conçus par NSO Group*. 22 juin 2020.
URL : https://www.amnesty.org/fr/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/.

[34] P1 Security. *La signalisation chez les opérateurs mobiles. Conférence donnée au SSTIC 2022*. 1er juin 2022.
URL : https://www.sstic.org/2022/presentation/la_signalisation_chez_les_oprateurs_mobiles/.

[35] Lookout. *Lookout Uncovers Android Spyware Deployed in Kazakhstan*. 16 juin 2022.
URL : https://www.lookout.com/blog/hermit-spyware-discovery.

[36] Lighthouse Reports. *Revealing Europe's NSO*. 28 août 2022.
URL : https://www.lighthousereports.nl/investigation/revealing-europes-nso/.

[37] The Guardian. *Israeli Spy Firm Suspected of Accessing Global Telecoms via Channel Islands*. 16 décembre 2020.
URL : http://www.theguardian.com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands.

[38] National Crime Agency US. *International Hacker-for-Hire Jailed for Cyber Attacks on Liberian Telecommunications Provider*. 25 mai 2019.
URL : https://nationalcrimeagency.gov.uk/news/international-hacker-for-hire-jailed-for-cyber-attacks-on-liberian-telecommunications-provider.

[39] ZDNet. *'Carpet-Bombing' DDoS Attack Takes down South African ISP for an Entire Day*. 24 septembre 2019.
URL : https://www.zdnet.com/article/carpet-bombing-ddos-attack-takes-down-south-african-isp-for-an-entire-day/.

[40] It Security News. *Anonymous and LulzSecITA Hacked Professional Orders and Telephone Operator Lyca Mobile | | IT Security News*. 6 novembre 2019.
URL : https://www.itsecuritynews.info/anonymous-and-lulzsecita-hacked-professional-orders-and-telephone-operator-lyca-mobile/.

[41] Euractiv. *L'UE accuse la Russie d'avoir piraté des satellites juste avant l'invasion de l'Ukraine*. 10 mai 2022.
URL : https://www.euractiv.fr/section/economie/news/lue-accuse-la-russie-davoir-pirate-des-satellites-juste-avant-linvasion-de-lukraine/.

[42] Conseil de l'Union européenne. *Cyberopérations russes contre l'Ukraine : déclaration du haut représentant au nom de l'Union européenne*. 10 mai 2022.
URL : https://www.consilium.europa.eu/fr/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/.

[43] CERT-UA. *Attaques destructrices contre plusieurs FAI ukrainiens*. 15 octobre 2023.
URL : https://cert.gouv.ua/article/6123309.

[44] CERT-UA. *WinRAR comme "cyber-arme". Attaque informatique destructrice d'UAC-0165 (problament Sandworm) contre le secteur public ukrainien avec RoarBat*. 29 avril 2023.
URL : https://cert.gov.ua/article/4501891.

[45] US Department of Justice. *United States of America v Yuriy Sergeyevich Andrienko, Sergey Vladimirovich Detistov, Pavel Valeryevich Frolov, Anatoliy Sergeyevich Kovalev, Artem Valeryevich Ochichenko, Petr Nikolayevich Pliskin*. 15 octobre 2020.
URL : https://context-cdn.washingtonpost.com/notes/prod/default/documents/f736f5b9-27be-42e9-b03f-b4c7a0214740/note/6929e5ba-7faf-4152-953a-9d629e34babe.

[46] NCSC UK. *Infamous Chisel*. 31 août 2023.
URL : https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/infamous-chisel/NCSC-MAR-Infamous-Chisel.pdf.

[47] Microsoft. *Special Report : Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine*. 27 avril 2022.
URL : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[48] BBC News. « Ukraine War : Major Internet Provider Suffers Cyber-Attack ». 28 mars 2022.
URL : https://www.bbc.com/news/60854881.

[49] CyberScoop. *Russians Allegedly Storm Ukrainian ISP, Blackmail It to Switch to Russian Networks*. 16 mai 2022.
URL : https://www.cyberscoop.com/russian-forces-ukrainian-isp-blackmail/.

[50] 01Net. *Sabotage de fibres optiques à Paris : l'identité des auteurs est toujours un mystère*. 27 juillet 2022.
URL : https://www.01net.com/actualites/sabotage-fibres-optiques-paris-identite-auteurs-toujours-mystere.html.

[51] ANSSI. *Recommandations relatives à l'interconnexion d'un système d'information à Internet*. 19 juin 2020.
URL : https://cyber.gouv.fr/guide-interconnexion-si-internet.

[52] ANSSI. *Comprendre et anticiper les attaques DDoS*. 1er mars 2015.
URL : https://cyber.gouv.fr/guide-ddos.

[53] ANSSI. *Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection*. 4 mars 2020.
URL : https://cyber.gouv.fr/guide-controle-acces-videoprotection.

[54] ANSSI. *Cartographie du système d'information*. 1er novembre 2018.
URL : https://cyber.gouv.fr/publications/cartographie-du-systeme-dinformation.

[55] ANSSI. *Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*. 1er janvier 2020.
URL : https://cyber.gouv.fr/publications/mecanismes-cryptographiques.

[56] ANSSI. *Recommandations relatives à l'administration sécurisée des systèmes d'information*. 11 mai 2021.
URL : https://cyber.gouv.fr/guide-admin-si.

[57] ANSSI. *Guide de sélection d'algorithmes cryptographiques*. 8 mars 2021.
URL : https://cyber.gouv.fr/publications/mecanismes-cryptographiques.

[58] ANSSI. *Recommandations relatives à l'authentification multifacteur et aux mots de passe*. 8 octobre 2021.
URL : https://cyber.gouv.fr/guide-authentification.

[59] ANSSI. *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine*. 11 novembre 2017.
URL : https://cyber.gouv.fr/guide-dns.

[60] ANSSI. *Recommandations de sécurité pour l'architecture d'un système de journalisation*. 28 janvier 2022.
URL : https://cyber.gouv.fr/guide-journalisation.

[61] ANSSI. *Recommandations relatives à l'administration sécurisée des systèmes d'information reposant sur Microsoft Active Directory*. 2 octobre 2023.
URL : https://cyber.gouv.fr/guide-admin-si-ad.

[62] ANSSI. *Recommandations sur le nomadisme numérique*. 23 novembre 2023.
URL : https://cyber.gouv.fr/guide-nomadisme-numerique.

18 décembre 2023

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
cert.ssi.gouv.fr / cert-fr@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité