RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Date : 28 novembre 2024
Version : 1
Nombre de pages : 21

SECTEUR DE L'EAU

ÉTAT DE LA MENACE INFORMATIQUE

TLP:CLEAR

PAP:CLEAR

Table des matières

SYNTHÈSE

En 2024, le secteur de l'eau a fait l'objet d'une attention particulière par des attaquants informatiques aux motivations et profils hétérogènes. Si le secteur est critique par essence à la fois pour la population et les industries, l'importance portée à la qualité de l'eau de la Seine dans le contexte des Jeux Olympiques et Paralympiques 2024 a accentué son exposition. À plusieurs reprises au cours de l'année, des groupes hacktivistes pro-russes ont ciblé ou menacé des infrastructures du secteur dans un objectif de médiatisation et de fragilisation des pouvoirs publics.

Le secteur est la cible de différents types d'acteurs malveillants qui cherchent à exploiter plusieurs faiblesses telles que l'héritage d'installations anciennes, le dispersement géographique des sites ou le faible budget alloué à la sécurité. L'hétérogénéité des opérateurs, en termes de statut, de taille d'organisation et de maturité de la sécurité des systèmes d'information (SI) constitue également des opportunités d'action pour les attaquants. Les nombreuses compromissions d'interfaces homme-machine exposées sur Internet, parfois sans authentification, illustrent le manque de prise en compte de la sécurité informatique en particulier par les acteurs de petite taille.

De plus, l'emploi généralisé de la télégestion et le passage à l'industrie 4.0 [1], notamment pour la maîtrise des fuites, ont entraîné des évolutions rapides des SI parfois insuffisamment sécurisés, augmentant ainsi la surface d'attaque.

Si ces différentes faiblesses sont des cibles faciles pour les attaquants, le risque de compromission par la chaîne d'approvisionnement demeure aussi un enjeu important qui doit être pris en compte par les organisations dans le cadre de leurs relations avec leurs partenaires, fournisseurs et prestataires.

Entre janvier 2021 et août 2024, 46 entités du secteur de la gestion de l'eau ont été touchées par un évènement de sécurité [2] d'origine informatique traité par l'ANSSI. Parmi ces entités, 12 sont des opérateurs régulés [3], représentant 34% des évènements de sécurité traités et 7 ont fait l'objet de multiples évènements de sécurité sur la période étudiée.

Au-delà des campagnes de déstabilisation, la menace cybercriminelle, qui poursuit des objectifs lucratifs, reste la menace la plus importante. Le faible niveau de sécurité permet à des attaquants de compromettre des SI à travers différents vecteurs. Sur 28 compromissions signalées à l'ANSSI [4], 8 ont mené au déploiement d'un rançongiciel.

L'espionnage et le positionnement stratégique sur des SI en vue de mener des actions ultérieures sont également des menaces qui visent ce secteur et peuvent s'inscrire dans le cadre de campagnes plus globales de ciblage de secteurs stratégiques comme l'énergie. Ces attaques ont lieu plus particulièrement dans des zones de forte tension, notamment en mer de Chine méridionale. Enfin, le sabotage d'entités du secteur de l'eau opéré par des modes opératoires réputés étatiques reste aujourd'hui à la marge et restreint aux zones de conflit.

1. Les usines sont équipées de capteurs avancés, de logiciels intégrés et de robotique pour analyser les données et ainsi améliorer la prise de décision, l'efficacité et la réactivité vis-à-vis des clients.
2. Évènements portés à la connaissance de l'ANSSI et ayant donné lieu à un traitement.
3. Ces entités peuvent être des organisations d'importance vitale (OIV) identifiées par l'État comme ayant des activités indispensables à la survie de la Nation ou dangereuses pour la population, ou des opérateurs de service essentiel (OSE) tributaires des réseaux ou systèmes d'information, qui fournissent un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.
4. Les compromissions sont des incidents de sécurité, c'est-à-dire des évènements de sécurité pour lesquels l'ANSSI confirme qu'un acteur malveillant a conduit des actions avec succès sur le système d'information de la victime.

1 AVANT-PROPOS

1.1 Périmètre

Cet état de la menace traite le petit cycle de l'eau, c'est-à-dire le prélèvement de l'eau brute, la potabilisation, le stockage, la distribution, la collecte des eaux usées et des eaux de pluie, l'assainissement et enfin le rejet en milieu naturel.

Deux tiers de l'eau prélevée pour la potabilisation provient de nappes souterraines, un tiers des eaux de surface, telles que les rivières, fleuves, lacs, prélevées en amont de l'agglomération [5] [1, 2]. Les acteurs liés à ce dernier tiers, pouvant être apparentés au secteur fluvial, ne seront pas traités comme appartenant au petit cycle de l'eau. Les barrages fluviaux ou hydroélectriques sont également exclus du périmètre. En effet, cette étude ne couvre pas les problématiques et les spécificités de ces équipements et de leur ciblage, même si certaines opérations notables sont mentionnées à titre illustratif au sein du rapport.

Si la période étudiée s'étend de janvier 2021 à août 2024, les exemples récents sont privilégiés.

1.2 Méthodologie

Ce document reflète la connaissance actuelle de l'ANSSI sur l'état de la menace informatique pesant sur le secteur de l'eau. Il s'appuie sur des incidents traités par l'ANSSI, des rapports officiels de gouvernements, d'exploitants, d'éditeurs de sécurité ainsi que des informations pertinentes issues de sources ouvertes. Les éléments présentés dans cet état de la menace ne sont pas exhaustifs.

La menace informatique se définit par des capacités au service d'intentions cherchant à saisir des opportunités d'agir :

- les capacités sont constituées des Techniques, Tactiques et Procédures (TTP), d'outils malveillants, d'infrastructures d'attaque, de ressources humaines, financières et techniques qui dépendent du profil des attaquants ;
- l'intention concerne l'objectif poursuivi de l'attaquant ciblant le secteur ou la victime objet de l'étude et ses fins (gain financier, espionnage, déstabilisation, prépositionnement) ;
- les opportunités d'agir peuvent être contextuelles (évolution du contexte géopolitique, appel d'offres, opération de fusion-acquisition) ou techniques (exploitation d'une vulnérabilité, accès au système d'information mis en vente).

5. Le prélèvement d'eau douce provient majoritairement des eaux de surface pour d'autres usages, comme les usages agricoles, industriels, l'alimentation des canaux et le refroidissement des centrales électriques.

2 CONTEXTE

2.1 Problématiques et changements dans les structures françaises du secteur

En France, l'alimentation en eau potable et l'assainissement des eaux usées est une mission de service public opérée sous la responsabilité des collectivités locales [3].

L'exploitation de ces services peut être opérée directement par la collectivité ou les collectivités concernées. Cette gestion peut aussi être indirecte et réalisée par un tiers dans le cadre d'une délégation de service public (DSP) [6] [4].

Commentaire : *parmi les entités ayant rapporté des évènements de sécurité à l'ANSSI, 74% sont des entités publiques, dont le statut juridique est très hétérogène (établissements publics de coopération intercommunale (EPCI) sans fiscalité propre, syndicat mixte, établissement public administratif (EPA), établissemet public industriel et commercial (EPIC), etc.). Cette prépondérance du secteur public est à mettre en perspective avec le mode de gestion de l'eau en France, qui est de la responsabilité légale des collectivités locales.*

En 2021, 32% des services d'eau potable étaient gérés par DSP et approvisionnaient près de 60% de la population française, avec une concentration de la majorité des activités par trois entreprises privées : Veolia, Suez et la Saur [5, 6]. Seulement 25% des services d'assainissement collectif étaient gérés en DSP et représentaient 40% de la population. Pour l'eau potable ou l'assainissement collectif, la taille moyenne d'un service en délégation est donc plus importante que celle d'un service en régie [5]. L'hétérogénéité de ces acteurs se reflète sur le niveau de sécurité des systèmes d'information.

Recommandations

Il est recommandé d'intégrer directement les enjeux de sécurité informatique aux contrats de délégation de service public, notamment dans des clauses opposables qui peuvent faire l'objet de pénalités ou d'obligations de correction [a].

a. Un ensemble de clauses types et une base d'exigences de sécurité sont disponibles dans le guide Externalisation et sécurité des systèmes d'information.

Un transfert des compétences en eau et assainissement des communes vers les établissements publics de coopération intercommunale (EPCI) est fixé au 1er janvier 2026 [7]. La moitié des intercommunalités sont à ce jour compétentes sur la production d'eau potable et d'assainissement collectif [8].

Commentaire : *les interconnexions réseau réalisées dans le cadre de ces intercommunalités peuvent générer une augmentation des impacts en cas d'attaques informatiques. Les difficultés de gouvernance en multipartie et la dilution potentielle de la responsabilité sont d'autres problématiques engendrées par ce transfert de compétence.*

Les financements du secteur proviennent majoritairement du système de redevance et nécessitent d'équilibrer le budget entre les recettes et les dépenses [4].

Le Plan Eau, établi en 2023, est axé sur la réduction des consommations, la réutilisation des eaux usées, la lutte contre les fuites et la modernisation du réseau. Des financements supplémentaires

6. Ces délégations peuvent être des concessions, des affermages, ou des régies intéressées.

ont été dédiés aux agences de l'eau pour sécuriser l'approvisionnement en eau potable, mais également pour la mise aux normes des stations d'épuration ou la mise en place de gouvernance [9].

Commentaire : la nécessité d'investir dans le renouvellement des infrastructures d'acheminement devrait être associée à l'investissement nécessaire en matière de sécurité informatique. De plus, la délégation de service public, qui ne donne pas la propriété des infrastructures aux opérateurs, peut être un frein à l'investissement sur le long terme pour la sécurisation des systèmes, en particulier des technologies opérationnelles (operational technology) (OT).

2.2 Des infrastructures vulnérables

Le contexte opérationnel du secteur de l'eau en fait un environnement vulnérable et présentant des opportunités d'agir pour les acteurs malveillants en cas de d'absence d'une sécurité informatique appropriée.

La télégestion est fortement employée pour optimiser la maintenance des différentes infrastructures physiques réparties sur le territoire. Si elle n'est pas accompagnée d'efforts de sécurisation, elle peut conduire à l'exposition directe d'interfaces métier d'équipements industriels ou d'interfaces d'administration d'équipements périphériques [10]. À ce titre, les intégrateurs de systèmes de contrôle industriels (*industrial control systems*) (ICS) doivent allier la réalité du terrain et des utilisateurs d'une part, et la sécurité des systèmes d'information d'autre part.

La disparité du budget alloué à la sécurité informatique en fonction des acteurs et l'obsolescence des équipements compliquent le cloisonnement entre les différentes infrastructures et la mise en place de mesures de sécurité.

Recommandations

Il est recommandé de mettre en place une gouvernance informatique et une approche par les risques industriels et métiers. Une analyse prenant en compte trois risques majeurs de compromission des équipements OT est nécessaire :

- l'accès d'un attaquant aux équipements de terrain d'un site non surveillé ;
- une compromission depuis Internet d'un acteur malveillant exploitant la porosité des systèmes IT et OT ;
- des pratiques d'administration inadaptées.

De plus, les besoins et les contraintes particuliers de la technologie opérationelle, notamment le temps de réponse et le volume d'échange, ont mené à un nombre élevé et à une hétérogénéité des protocoles utilisés par des systèmes de contrôle industriels [7]. Des protocoles tels que MODBUS ou S7Com, spécifiques aux ICS, présentent souvent une sécurité faible, avec l'absence de chiffrement ou d'authentification.

Commentaire : l'exploitation de vulnérabilités complexes sur des systèmes de contrôle industriels est peu observée dans le secteur de l'eau et pourrait illustrer les nombreux vecteurs déjà disponibles pour des acteurs malveillants.

7. Ces protocoles permettent la visualisation de l'état des processus, l'accès en lecture et écriture aux données traitées ainsi que les prestations d'ingénierie industrielle.

Recommandations

Il est recommandé de mettre en œuvre des protocoles sécurisés au sein des systèmes industriels. Ces protocoles doivent permettre :

- l'authentification du client/secondaire auprès du serveur/primaire ;
- l'intégrité des communications entre les équipements (indépendamment de leur rôle client/secondaire ou serveur/primaire).

Il est par exemple possible :

- d'utiliser OPC-UA (avec authentification et configuré en mode *sign* ou *sign & encrypt* en fonction du besoin) ;
- d'encapsuler les protocoles industriels dans des tunnels IPsec ou TLS.

Cette recommandation vient en complément des mesures de sécurité périmétrique des ICS [a] et participe à la défense en profondeur. Elle est d'autant plus critique dans le secteur de l'eau que les communications industrielles sont plus à même de traverser des réseaux non maîtrisés (réseaux opérateurs).

a. Se référencer aux guides sur La cybersécurité des systèmes industriels.

Si la transformation numérique du secteur et l'adoption de l'Internet des objets (*Internet of Things*) (IoT) visent à contrôler la réduction des consommations et à mieux lutter contre les fuites, ces systèmes restent fragiles, vulnérables et facilement perturbables, où le *security by design* est trop rarement mis en œuvre [11]. L'intégration de nouvelles technologies, telles que le *Cloud*, l'IoT ou les traitements statistiques et la systématisation des interconnexions avec des SI bureautiques tiers augmentent l'exposition des ICS, notamment aux menaces présentes dans les réseaux IT. Or, ces réseaux ICS sont des systèmes d'exploitation rarement mis à jour pour préserver les processus industriels de toute rupture d'activité, et donc souvent obsolètes.

2.3 Une ressource sensible

D'ici à 2030, selon les projections de la Banque Mondiale, la demande en eau pourrait être supérieure de 40% aux disponibilités de la planète [12]. Aujourd'hui, la « diagonale de la soif » s'étend du Maroc au nord-est de la Chine en passant par le Moyen et le Proche-Orient.

Un accroissement des conflits et des foyers de tensions liés à l'eau est observé depuis plusieurs années, concernant, entre autres, les fleuves transfrontaliers [13, 14].

L'eau peut être une cible stratégique en cas de conflit. Ce levier a été employé dans le cadre de la guerre en Ukraine et du conflit entre Israël et le Hamas par la destruction physique d'infrastructures critiques, tels que des sites de production, d'assainissement ou d'approvisionnement en eau, mais également de barrages [15, 16, 17]. Des attaques informatiques à des fins de sabotage restent à ce jour à la marge sur le secteur de l'eau, mais peuvent intervenir en appui d'opérations cinétiques.

Commentaire : aujourd'hui, la France ne fait pas face à de tels risques de stress hydrique, mais plus de 100 bassins versants connaissent des tensions structurelles [9]. La criticité de ce secteur et son importance vitale peuvent en faire une cible pour de la déstabilisation. De plus, des acteurs privés français du secteur de l'eau sont largement implantés à l'international dans des régions où l'eau est un facteur de tension. Leur présence dans des zones à fort stress hydrique, mais également leurs volontés d'expansion sur certains marchés pourraient faire d'eux des cibles d'actions de déstabilisation ou d'espionnage.

3 MENACES CIBLANT LE SECTEUR DE L'EAU

Entre janvier 2021 et août 2024, l'ANSSI a traité 31 compromissions liées à des entités du secteur de la gestion de l'eau. Si aucune augmentation notable ne peut être observée sur la période, des changements d'acteurs et d'intentions sont à noter en fonction des années. En effet, 12 incidents en 2023 étaient opérés par des acteurs aux motivations lucratives, tandis que 16 signalements [8] en 2024, majoritairement entre mai et juillet, étaient liés à des menaces ou des revendications de DDoS [9] par des groupes hacktivistes dans le contexte particulier des Jeux Olympiques et Paralympiques de Paris 2024.

3.1 Attaques informatiques à des fins lucratives

En 2023 et 2024, le secteur de l'eau en France a été victime de plusieurs attaques informatiques opérées par des cybercriminels aux motivations financières, qui restent la première menace identifiée en terme de nombre d'attaques à l'encontre du petit cycle de l'eau.

Depuis 2019, la double extorsion, par le déploiement d'un rançongiciel d'une part et la menace de divulgation de données d'autre part, est la tactique la plus utilisée par les groupes cybercriminels. De plus, une professionnalisation de l'écosystème cybercriminel a entraîné une séparation des différentes tâches [10] entre les acteurs et une industrialisation des compromissions. Le secteur de l'eau, par ses nombreuses possibilités de vecteurs initiaux, est fréquemment une cible opportuniste de ces groupes.

Plusieurs groupes cybercriminels ont ciblé le secteur de l'eau :

- en avril 2024, le système d'information d'une commune française a été chiffré par le biais du rançongiciel Babyk/Babuk. De nombreux services considérés comme critiques ont été affectés, incluant la gestion de l'eau. Si la distribution de l'eau demeurait possible, sa facturation ainsi que le pilotage de sa production, c'est-à-dire la supervision de la distribution et la télé-intervention, étaient inopérants. En réaction, la commune a adopté un mode de fonctionnement dégradé permettant d'assurer la continuité du service ;
- une entité américaine de la société Veolia a été ciblée par un rançongiciel en janvier 2024. La société a préféré mettre ses systèmes de sauvegarde et ses serveurs hors ligne en prévention, perturbant ainsi la possibilité de paiement des clients [18] ;
- la compagnie d'aménagement du Bas Rhône et du Languedoc (BRL) a été chiffrée par le rançongiciel Lockbit 3.0 en mars 2023 [19] ;
- le Syndicat Mixte Départemental d'Eau et d'Assainissement de l'Ariège (SMDEA) a été ciblé par le rançongiciel Qilin en mai 2023 [20] ;
- en 2023, une entreprise en charge de l'aménagement des ouvrages hydrauliques a été victime du rançongiciel 8base qui aurait rendu inopérant son système d'information [21] ;
- lors de la compromission de l'Office d'Équipement Hydraulique de Corse en 2022, la partie bureautique, c'est-à-dire la gestion clientèle, l'accueil et la facturation auraient été touchés [22] ;
- en juillet 2022, la préfecture d'une collectivité d'outre-mer a signalé la compromission et le chiffrement d'un syndicat des eaux par le rançongiciel Lockbit. Le syndicat, en charge

8. Évènement de sécurité informatique avec un faible impact sur le SI de la victime, requérant une intervention minimum de l'Agence.

9. Le déni de service distribué est une action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu.

10. Certains obtiennent les accès initiaux, d'autres fournissent l'infrastructure, ou encore développent et maintiennent les codes malveillants ou les souches de rançongiciels.

de l'eau et de l'assainissement, avait confié l'exploitation de ces services à deux sociétés. Son SI demeurait ainsi indépendant des délégataires et aucun impact sur la distribution n'a donc été constaté.

Commentaire : les impacts des incidents affectant une entité du secteur de la gestion de l'eau, dont, a minima, une dizaine de collectivités territoriales/locales, portent principalement sur les services administratifs (en particulier la facturation de l'eau), le pilotage et la supervision de la distribution de l'eau ou de l'assainissement des eaux usées. De manière plus rare, des activités particulièrement sensibles peuvent être affectées, telles que le contrôle de la qualité de l'eau.

Le montant des rançons demandées lors de ces attaques informatiques n'est désormais plus publié sur les sites de divulgation de données [11] des groupes de rançongiciels. Les cybercriminels déterminent aujourd'hui ces montants en fonction de critères comme la taille des entités et de leur chiffre d'affaires quand celui-ci est public. Une étude de l'éditeur de sécurité SOPHOS indique que la rançon demandée aurait augmenté cette dernière année pour les secteurs de l'eau et de l'énergie, pour atteindre 2,5 millions de dollars américains en moyenne en 2024 [23].

Commentaire : dans de nombreux cas, le coût de la première étape d'un programme de sécurisation serait donc bien inférieur au montant des rançons demandées et de la remédiation.

Les vecteurs initiaux de ces compromissions sont principalement le vol ou l'achat d'identifiants et l'exploitation de vulnérabilités.

Pour deux compromissions précédemment mentionnées, les attaquants auraient eu des accès à des passerelles de VPN [12], dont l'un était un compte légitime d'un prestataire.

Recommandations

Il est recommandé de prendre en compte la sécurisation de la chaîne d'approvisionnement, en particulier les accès des prestataires externes aux SI industriels. La mise à disposition de postes dédiés pour les prestataires de maintenance est un exemple de sécurisation.
Une procédure de gestion des outils de maintenance des prestataires est également recommandée.

Des campagnes d'hameçonnage peuvent également être mises en œuvre par des cybercriminels. Une campagne déployant le code malveillant Pikabot a été détectée dans un syndicat en charge de l'assainissement, où plus de 300 postes auraient été affectés. Ce code est notamment employé en amont du déploiement d'un rançongiciel.

En 2021, lors de deux incidents aux États-Unis, des acteurs malveillants ont récupéré des identifiants TeamViewer d'un employé et ont tenté de supprimer les programmes utilisés pour traiter l'eau potable pour l'un en Californie, et de modifier le niveau d'hydroxyde de sodium pour l'autre en Floride [24, 25, 26].

Commentaire : les motivations de ces deux attaques restent inconnues, mais témoignent de la facilité d'accès à des identifiants de logiciels de contrôle à distance, qui peuvent être compromis par l'attaquant ou achetés auprès d'un fournisseur. L'usage massif de la télégestion dans le secteur de l'eau participe à son ciblage important.

En 2021, les stations d'assainissement d'Oloron Sainte-Marie dans les Pyrénées-Atlantiques ont été victimes d'un rançongiciel, à la suite de l'exploitation d'une faille dans un logiciel de super-

11. Ces sites sont également appelés DLS (*Data Leak Site*).
12. *Virtual Private Network* : interconnexion de réseaux locaux *via* une technique de tunnel sécurisé ou non, généralement à travers Internet.

vision [27]. Après le déploiement du rançongiciel, une partie des données a été détruite par les cybercriminels, qui n'ont cependant pas pris le contrôle des stations d'assainissement [28].

Commentaire : les attaques opérées par des cybercriminels sur le secteur de l'eau ont à ce jour affecté l'IT et rarement l'OT. Malgré le peu de données sensibles traitées et la possibilité de continuer les opérations manuellement, deux facteurs pouvant réduire la pression exercée sur les victimes de payer la rançon, le secteur de l'eau reste une cible opportuniste des groupes cybercriminels.

3.2 Attaques informatiques à des fins de déstabilisation

Dans le cadre d'attaques informatiques, la déstabilisation peut se matérialiser sous la forme d'attaques par déni de service, de divulgations d'information associées ou non à des campagnes informationnelles ou par du sabotage informatique. Ces opérations sont menées par différents types d'acteurs : hacktivistes, étatiques, employés ou ex-employés.

3.2.1 Hacktivisme

Des campagnes de sabotage peuvent être menées à des fins de déstabilisation par des modes opératoires réputés étatiques sous une couverture hacktiviste, par des groupes soutenus par des États, ou des groupes hacktivistes indépendants. Même si les capacités de ces groupes restent faibles, le secteur ciblé et leur potentielle affiliation à des États entraînent une forte médiatisation de ces attaques.

En novembre 2023, le groupe hacktiviste CyberAv3ngers a attaqué Israël en ciblant des automates du fabricant israélien Unitronics, employés dans les systèmes d'approvisionnement en eau et de traitement des eaux usées, et d'autres secteurs comme l'énergie, l'alimentation, la manufacture de boisson et la santé à travers le monde. Selon la CISA [13], ce groupe hacktiviste anti-israélien serait opéré par le Corps des gardiens de la révolution islamique iranien et revendique des attaques contre des systèmes critiques depuis 2020 [29].

Dans cette campagne, plusieurs faiblesses sur les infrastructures ont été exploitées par les attaquants, telles que l'exposition directe de l'automate sur Internet et l'utilisation d'un mot de passe d'administrateur par défaut présent dans le système tel qu'il est fourni par le fabricant [29, 30].

Différentes entités dans le monde utilisant ces automates auraient ainsi été victimes de l'attaque informatique. Les attaquants ont pu prendre le contrôle des stations de pompage qui desservaient deux châteaux d'eau dans la municipalité d'Aliquippa en Pensylvannie et défigurer une interface homme-machine. L'attaque aurait aussi touché le comté de Mayo en Irlande, où près de 160 maisons ont été privées d'eau pendant 48 heures, et différentes usines de production d'eau ou des brasseries en Roumanie, en République Tchèque et aux États-Unis [30].

Commentaire : par ses conséquences aux États-Unis et en Europe alors que la cible initiale était israélienne, cet incident témoigne de l'ampleur du ciblage géographique que peut avoir une attaque quand un équipement spécifique est ciblé.

13. *Cybersecurity and Infrastructure Security Agency*, agence fédérale américaine.

Recommandations

Il est recommandé de limiter la surface d'exposition aux attaquants en effectuant un durcissement des configurations des automates quand cela est possible.
En particulier, seuls les logiciels, les services et les protocoles nécessaires doivent être installés ou activés. Les protocoles et fonctionnalités vulnérables et non sécurisés (FTP, Telnet, HTTP, etc.) doivent être désactivés systématiquement.
Les modes de configuration et de programmation à distance sur les installations critiques qui peuvent être définis par exemple par un commutateur ou une clé physique sur le CPU pour les automates doivent être désactivés ou positionnés en lecture seule.

En mars 2024, le groupe hacktiviste pro-palestinien Handala Hack Team a revendiqué la compromission et l'exfiltration de 79 Go de données d'un SI appartenant à une société de traitement des eaux israélienne spécialisée dans la désalinisation [31]. Apparu en décembre 2023 en réponse au conflit entre Israël et le Hamas, ce groupe se pose en défenseur de la Palestine et cible majoritairement des organisations israéliennes. Son mode opératoire repose sur la divulgation de données exfiltrées parfois associées à l'utilisation d'un rançongiciel [32].

En 2024, le groupe Cyber Army of Russia (*Reborn*) (CARR) a pu prendre le contrôle de plusieurs interfaces homme-machine dans la production ou l'assainissement d'eau aux États-Unis, en Pologne et en France. La manipulation des machines a notamment engendré le débordement d'un réservoir à Muleshoe au Texas. Les nombreuses manipulations aléatoires opérées par les attaquants suggèrent que leur connaissance de l'OT est relativement faible [33].

Commentaire : malgré les faibles capacités nécessaires pour prendre le contrôle d'une interface homme-machine non sécurisée, une manipulation intempestive d'un équipement, notamment en forçant la marche et l'arrêt, pourrait rapidement le mettre hors d'usage et avoir un impact conséquent sur les opérations de la victime.

Le 2 mars 2024, le groupe a revendiqué la prise de contrôle à distance de la centrale hydroélectrique de Courlon-sur-Yonne dans le département de l'Yonne en France. La compromission concernait en réalité un logiciel de contrôle du moulin de Courlandon, une installation de petite taille opérée par un particulier dans le département de la Marne, sans incidence sur les installations du moulin ni pour les habitants [34]. Le 21 juin, le groupe a revendiqué la prise de contrôle à distance d'une usine de traitement des eaux dans la ville de Dittaino en Italie. Cette attaque était, d'après le groupe, une préparation à des campagnes contre des entités opérant sur la Seine dans le but de perturber la cérémonie d'ouverture et certaines épreuves des Jeux Olympiques et Paralympiques de Paris 2024 [35]. Cependant, aucune attaque revendiquée par ce groupe n'a été relevée sur des infrastructures de l'eau en France durant la période de l'évènement.

Commentaire : le ciblage de plusieurs entités du secteur du petit cycle de l'eau ou pouvant être apparentées au secteur de l'eau de manière plus globale, s'inscrit dans un contexte géopolitique tendu et où des acteurs cherchaient à tirer profit de la médiatisation des Jeux Olympiques et Paralympiques à des fins de destabilisation.

Recommandations

Les interfaces des équipements et SCADA ne doivent pas être exposées sur Internet. Si les contraintes techniques ou opérationnelles ne le permettent pas, il est recommandé de forcer l'accès aux équipements au travers d'une passerelle d'interconnexion dédiée telle qu'un boitier de pare-feu industriel, mettre en place des mots de passe robustes et activer dans la mesure du possible les options d'authentification à multiples facteurs.
Pour les connexions à partir de postes nomades, mettre en place des tunnels chiffrés de type IPsec ou TLSv1.3.
L'utilisation d'un logiciel d'accès maintenu à jour par son éditeur et dans la version la plus récente est recommandée, en effectuant des mises à jour régulières afin de bénéficier des correctifs de sécurité publiés.

Selon l'éditeur de sécurité informatique MANDIANT, le groupe CARR serait soutenu voire orienté par l'unité 74455 du GRU, le service de renseignement militaire de la Fédération de Russie [36]. Cette affiliation ne peut cependant pas être confirmée par l'ANSSI.

En décembre 2023, un groupe hacktiviste pro-ukrainien nommé BlackJack aurait mené une attaque contre l'infrastructure IT de Rosvodocanal, un fournisseur d'eau privé en Russie afin de perturber ses opérations. Les attaquants auraient revendiqué avoir chiffré plus de 6 000 ordinateurs et supprimé plus de 50 teraoctects de données, incluant la documentation interne et les copies de sauvegarde [37].

Commentaire : les campagnes de déstabilisation opérées par des groupes hacktivistes sont des ressources à faibles capacités techniques qui peuvent avoir de forts impacts réputationnels et opérationnels. Ces opérations mettent en lumière des faiblesses dans les infrastructures d'autres États et visent à altérer la confiance de la population dans un secteur d'importance vitale, en pratiquant la désinformation sur les conséquences réelles de l'attaque.

3.2.2 Ciblage par des Modes Opératoires d'Attaques réputés étatiques

Dans le cadre de l'invasion en Ukraine par la Russie, des campagnes de sabotage sur des infrastructures du secteur de l'eau ont été menées en appui à des opérations militaires sur le terrain.

En mars 2024, les opérateurs du mode opératoire d'attaque (MOA) réputé russe Sandworm auraient visé environ vingt entreprises ukrainiennes spécialisées dans l'approvisionnement en énergie, en eau et en chaleur, localisées dans dix régions de l'Ukraine. L'objectif de ces attaques était de perturber le fonctionnement des ICS des entités ciblées. Pour au moins trois des compromissions, l'attaquant aurait obtenu des accès aux SI ciblés grâce à l'installation de logiciels spécialisés qui contenaient des vulnérabilités ou aux accès permanents de prestataires sur des équipements visant à fournir de l'assistance. Pour l'accès à certains systèmes d'information, les attaquants auraient privilégié l'utilisation de comptes légitimes d'employés [38].

Deux facteurs auraient facilité cette attaque informatique :

- une segmentation incorrecte des serveurs hébergeant les logiciels spécialisés des fournisseurs conçus pour l'automatisation et la gestion des processus, avec une absence de limitation d'accès depuis et vers Internet et un manque d'isolation de ces serveurs par rapport au reste de l'infrastructure des ICS à laquelle ils appartiennent ;
- une certaine négligence des éditeurs de logiciel dans la revue du code et la présence de vulnérabilités permettant l'exécution de code arbitraire à distance [38].

Recommandations

Lors du renouvellement des équipements d'un établissement ou d'une nouvelle construction, il est recommandé de mettre en œuvre des équipements faisant l'objet d'une qualification, d'une certification ou d'un visa de sécurité de l'ANSSI et de choisir des prestataires de confiance afin de réduire le risque d'introduction de portes dérobées dans le cadre d'attaques sur la chaîne d'approvisionnement.

3.2.3 Attaquant interne

Les tentatives de sabotage peuvent émaner de malveillance interne, c'est-à-dire des employés, des anciens employés, des fournisseurs ou anciens fournisseurs de l'entité :

- en août 2007, un ancien employé d'un petit réseau de canaux en Californie, disposant encore de ses droits d'accès au site, a été accusé d'avoir installé un logiciel non autorisé sur un ordinateur utilisé pour dériver l'eau de la rivière Sacramento à des fins d'irrigation. Cette installation a endommagé un ordinateur qui faisait partie du système SCADA [14] [39];
- en mars 2019, un employé de la Post Rock Rural Water District aux États-Unis aurait volontairement arrêté les processus de nettoyage et de désinfection au sein de l'usine [40].

Recommandations

Il est recommandé d'établir, de documenter et de tenir à jour la cartographie des droits et des accès, en particulier en appliquant une politique d'attribution des droits suivant le principe du moindre privilège basée sur les rôles des utilisateurs (*Role-Based Access Control*) (RBAC), couplée à une authentification des utilisateurs.
Il est également recommandé de sensibiliser les responsables des automates à la sécurité informatique.

3.3 Attaques informatiques à des fins de prépositionnement

Les modes opératoires réputés étatiques ont recours au prépositionnement [15] en cas de hausse des tensions dans le cadre d'un conflit. Après le déclenchement de l'opération, l'état final recherché peut évoluer en fonction du contexte, souvent géopolitique.

En 2020, les autorités allemandes ont publié une alerte sur une campagne attribuée aux opérateurs du MOA réputé russe Bersek Bear attribué en sources ouvertes au service de renseignement intérieur russe (FSB) contre les infrastructures critiques du pays, notamment du secteur de l'eau [41]. Le MOA était actif sur les systèmes d'information depuis plusieurs années et aurait réussi à compromettre les systèmes par la chaîne d'approvisionnement. Il aurait tenté de dérober les informations et de gagner des accès sur les systèmes industriels de ses victimes [41].

Commentaire : le ciblage d'entités du secteur de l'eau au moyen du MOA Bersek Bear entre dans la continuité d'opérations dirigées contre des ICS. En effet, ce MOA avait déjà ciblé des entreprises du secteur de l'énergie en Allemagne et aux États-Unis en 2018. Le ciblage d'ICS par les acteurs réputés

14. Systèmes de Contrôles et d'Acquisition de Données.
15. Le prépositionnement sur un réseau par un mode opératoire d'attaque est le dépôt ou le maintien d'accès à des outils malveillants dans les systèmes d'information en vue de mener des actions ultérieures.

étatiques, contrairement aux acteurs cybercriminels, témoigne de leur niveau de sophistication et de leur objectif de cibler des infrastructures industrielles, voire critiques.

En mai 2023, les autorités américaines ont imputé une attaque visant des infrastructures critiques liées aux réseaux électriques, aux communications et aux fournisseurs d'eau potable sur les bases américaines et à l'étranger aux opérateurs du MOA Volt Typhoon, un mode opératoire qui pourrait être associé à l'Armée Populaire de la Libération (APL) chinoise selon le New York Times [42, 43]. Ces attaques, qui ont ciblé des infrastructures communes aux installations militaires et civiles, auraient pu atteindre les entreprises et les foyers américains. Selon les autorités, cette présence sur les réseaux constituait un prépositionnement stratégique en cas de conflit armé avec Taiwan afin d'entraver ou de retarder le mouvement de troupes américaines en désorganisant les pouvoirs publics par une attaque informatique majeure. Cette opération souligne une évolution possible des finalités des modes opératoires chinois, qui pourraient désormais mener des opérations de sabotage [42].

Dans cette campagne, les attaquants auraient cherché à se positionner sur les réseaux bureautiques afin de mener des attaques destructrices sur les infrastructures américaines en se propageant vers les systèmes de contrôle industriels [43].

Le vecteur initial de cette opération serait l'exploitation de vulnérabilités jour-zéro sur des équipements exposés sur Internet, tels que des routeurs, des VPN ou des pare-feux. À la suite de la compromission d'un acteur du petit cycle de l'eau, les opérateurs de ce MOA seraient parvenus à accéder au SI grâce à des authentifiants d'un compte VPN et à accéder à différents serveurs pendant une période de neuf mois [16]. La récupération d'authentifiants obtenus depuis le contrôleur de domaine *Active Directory* leur aurait permis d'opérer des recherches, des collectes et de l'exfiltration sur le serveur de fichiers [43].

Enfin, le positionnement adjacent à l'infrastructure OT d'un serveur VMWare VCenter a facilité l'énumération des sessions existantes à l'aide de l'application Putty [17] et ainsi l'obtention des accès à certains profils critiques pour des usines de traitement des eaux [43].

Commentaire : le ciblage du secteur de l'eau intervient généralement dans des campagnes visant au même titre le secteur de l'énergie. L'importance vitale, le risque systémique mais aussi les problématiques techniques similaires pourraient expliquer que les mêmes acteurs réputés étatiques ciblent ces deux secteurs.

16. Ce mouvement latéral aurait été effectué sur un serveur fichier, un contrôleur de domaine *Active Directory*, deux serveurs Oracle Management Server et VMWare VCenter.

17. Putty est un outil permettant d'effectuer des connexions à distance sur des serveurs en utilisant certains protocoles comme SSH, Telnet ou Rlogin.

Recommandations

Afin de circonscrire la latéralisation d'un attaquant, il est recommandé de :

- limiter le nombre d'interconnexions des ICS vers des réseaux tiers (IT ou OT partenaires) et de les sécuriser à l'aide de zones démilitarisées (DMZ) dédiées ;
- mettre en œuvre des passerelles sécurisées unidirectionnelles (montante et descendante) avec rupture protocolaire ;
- cloisonner les systèmes et les sous-systèmes de l'ICS et de filtrer les communications entre ces derniers. Le filtrage des flux internes à l'ICS doit être effectué par un pare-feu dédié à cet usage ;
- mettre en place, au sein des systèmes géographiquement répartis, une architecture de type *Hub and Spoke* [a].

Enfin, il est également recommandé de mettre en œuvre des sondes de surveillance du trafic sur le réseau OT ou sur les interfaces IT/OT afin d'aider à détecter les phases de reconnaissance des attaquants. Des visites physiques et des audits peuvent permettre de détecter des implants.

a. Appelé également réseau en étoile, cette architecture comprend un point de connexion central qui peut atteindre les terminaisons situées à la périphérie.

3.4 Attaques informatiques à des fins d'espionnage

Les motivations des opérations d'espionnage informatique menées par des acteurs réputés étatiques peuvent être diverses. Dans le secteur de l'eau, le ciblage de pays d'une même région peut permettre de connaître les ressources en eau des pays limitrophes, surtout dans les régions sujettes au stress hydrique, et en particulier pour les pays ayant des fleuves transfrontaliers.

Une campagne d'hameçonnage ciblant des organisations du secteur de la diplomatie, mais aussi des infrastructures du secteur de l'eau de la Turquie et l'Ouzbékistan illustre le ciblage de ce secteur. Si cette campagne n'a pas été imputée à un MOA, des articles ont attribué une campagne similaire aux opérateurs de Tomiris. Les opérateurs de ce MOA mènent des campagnes d'espionnage en Asie Centrale [44, 45].

Les sociétés françaises peuvent être ciblées en raison de leur implantation dans une zone de conflit entre deux pays. Celles-ci sont ainsi susceptibles de devenir des vecteurs d'entrée pour des actions de surveillance ou de déstabilisation.

La filiale d'une entité française du secteur de l'eau aurait été la cible d'opérateurs d'un MOA réputé chinois. Après avoir compromis une entreprise de télécommunication, les attaquants auraient employé un accès VPN d'une société en charge de la télé-maintenance pour accéder à un serveur interne de l'entité chargée de la gestion de l'eau. Au cours de cette campagne, les opérateurs de ce MOA auraient ciblé plusieurs entités stratégiques localisées dans la même zone géographique, mais appartenant à des secteurs différents.

Commentaire : les campagnes d'espionnage informatique ciblant le secteur de l'eau restent peu fréquentes. À ce jour, ces campagnes ne semblent pas chercher à récupérer les secrets industriels d'entreprises employant des technologies avancées. Le ciblage de ce secteur semble intervenir dans des campagnes de ciblage global d'une zone géographique. Ces campagnes pourraient servir pour de la collecte d'informations, de la surveillance, ou du prépositionnement.

Recommandations

Il est recommandé de mettre en place une gouvernance informatique et une approche par les risques commerciaux. Une analyse de risque est nécessaire pour s'assurer que les données sensibles commerciales ou relatives à des secrets industriels sont bien identifiées et sécurisées.

4 Références

[1] DEVELOPPEMENT-DURABLE.GOUV.FR. *L'eau en France : ressource et utilisation – Synthèse des connaissances en 2023*. 30 novembre 2023.
URL : https://www.statistiques.developpement-durable.gouv.fr/leau-en-france-ressource-et-utilisation-synthese-des-connaissances-en-2023.

[2] LE CENTRE D'INFORMATION SUR L'EAU. *L'eau potable : sa définition, ses origines, ses critères de potabilité et ses traitements | Centre d'information sur l'eau*. 7 mars 2019.
URL : https://www.cieau.com/espace-enseignants-et-jeunes/les-enfants-et-si-on-en-apprenait-plus-sur-leau-du-robinet/la-definition-de-leau-potable/.

[3] EAUFRANCE. *Les services publics d'eau et d'assainissement*.
URL : https://www.eaufrance.fr/les-services-publics-deau-et-dassainissement.

[4] COLLECTIVITES-LOCALES.GOUV.FR. *L'eau et l'assainissement | Collectivites-Locales.Gouv.Fr*.
URL : https://www.collectivites-locales.gouv.fr/competences/leau-et-lassainissement.

[5] EAUFRANCE et SISPEA. *Observatoire Des Services Publics d'eau et d'assainissement - Rapport Nationales Des Données SISPEA - Synthèse - Edition de Juin 2023 - Données 2021*. 1er juin 2023.

[6] MONRESEAUDEAU.FR. *40 chiffres à savoir sur les réseaux d'eau en France en 2021*. 30 septembre 2021.
URL : https://www.monreseaudeau.fr/actualites/40-chiffres-reseaux-eau-potable-france-2021/.

[7] LA GAZETTE DES COMMUNES. *Le transfert des compétences eau et assainissement des communes vers les EPCI*. 23 octobre 2023.
URL : https://www.lagazettedescommunes.com/887195/le-transfert-des-competences-eau-et-assainissement-des-communes-vers-les-epci/.

[8] INTERCOMMUNALITÉS.FR. *Les enjeux du transfert des compétences eau potable et assainissement*. 4 février 2023.
URL : https://www.intercommunalites.fr/domaines-daction/environnement-et-amenagement/politique-globale-de-leau/eau-et-assainissement-se-preparer-au-transfert-des-competences/eau-potable-et-assainissement-les-enjeux-du-transfert-des-competences/.

[9] ECOLOGIE.GOUV.FR. *53 Mesures pour l'eau - Plan d'action pour une gestion résiliente et concertée de l'eau*. 30 mars 2023.

[10] CISA. *Ongoing Cyber Threats to U.S. Water and Wastewater Systems*.
URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a.

[11] LIBÉRATION. *Franck Galland : «Ces régions en stress hydrique sont encore plus en tension depuis le Printemps arabe»*. 3 janvier 2017.
URL : https://www.liberation.fr/evenements-libe/2017/01/03/franck-galland-ces-regions-en-stress-hydrique-sont-encore-plus-en-tension-depuis-le-printemps-arabe_1538789/.

[12] THE GUARDIAN. *Global Fresh Water Demand Will Outstrip Supply by 40% by 2030, Say Experts*. 17 mars 2023.
URL : https://www.theguardian.com/environment/2023/mar/17/global-fresh-water-demand-outstrip-supply-by-2030.

[13] TEDXSACLAY. *L'Eau, un enjeu géopolitique majeur*. 25 mars 2021.
URL : https://tedxsaclay.com/fr/actualites/l-eau-un-enjeu-geopolitique-majeur.

[14] Assemblée Nationale. *Rapport d'information n°1101*. 21 juin 2018.
URL : https://www.assemblee-nationale.fr/dyn/15/rapports/mieau/l15b1101_rapport-information.

[15] The Water Diplomat. *Rivers and Water Systems as Weapons and Casualties of the Ukraine War*. 19 octobre 2023.
URL : https://www.waterdiplomat.org/story/2023/10/rivers-and-water-systems-weapons-and-casualties-ukraine-war.

[16] Conflits : Revue de Géopolitique. *L'eau. L'autre enjeu de la guerre en Ukraine. Entretien avec Franck Galland*. 27 février 2022.
URL : https://www.revueconflits.com/franck-galland-guerre-eau-ukraine/.

[17] Oxfam. *Israël utilise l'eau comme arme de guerre, à l'heure où l'approvisionnement de Gaza s'effondre de 94 %, provoquant une catastrophe sanitaire mortelle*. 18 juillet 2024.
URL : https://www.oxfamfrance.org/communiques-de-presse/israel-utilise-leau-comme-arme-de-guerre-a-lheure-ou-lapprovisionnement-de-gaza-seffondre-de-94-provoquant-une-catastrophe-sanitaire-mortelle/.

[18] Wisdiam. *9 Recent Cyber Attacks on the Water and Wastewater Sector*. 5 mai 2024.
URL : https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/.

[19] Le Monde Informatique. *Lockbit menace de divulguer les données de BRL volées - Le Monde Informatique*. 17 avril 2023.
URL : https://www.lemondeinformatique.fr/actualites/lire-lockbit-menace-de-divulguer-les-donnees-de-brl-volees-90164.html.

[20] La Gazette Ariégeoise. *Le SMDEA victime d'une cyber attaque de grande ampleur : face au vol de données les usagers doivent être vigilants*. 25 mai 2023.
URL : https://gazette-ariegeoise.fr/le-smdea-victime-dun-piratage-dampleur-de-tres-nombreuses-donnees-volees/.

[21] La Nouvelle République des Pyrénées. *Victime d'une cyberattaque, les services de la CACG fortement perturbés*. 15 décembre 2023.
URL : https://www.nrpyrenees.fr/2023/12/15/victime-dune-cyberattaque-les-services-de-la-cacg-fortement-perturbes-11644787.php.

[22] Corse Net Infos. *Suite à une cyberattaque, l'Office Hydraulique de Corse se remet doucement sur pied*. 16 novembre 2022.
URL : https://www.corsenetinfos.corsica/Suite-a-une-cyberattaque-l-Office-Hydraulique-de-Corse-se-remet-doucement-sur-pied_a67998.html.

[23] Sophos. *Le coût de récupération moyen a quadruplé en un an dans les secteurs d'infrastructures critiques de l'énergie et de l'eau pour atteindre 3 millions de dollars en un an, selon une étude Sophos*. 17 juillet 2024.
URL : https://www.sophos.com/fr-fr/press/press-releases/2024/07/median-recovery-costs-2-critical-infrastructure-sectors-energy-and.

[24] NBC News. *A Hacker Tried to Poison a Calif. Water Supply. It Was as Easy as Entering a Password.* 17 juin 2021.
URL : https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206.

[25] Dragos. *United States Water and Wastewater*. 17 avril 2024.
URL : https://www.dragos.com/blog/ot-cyber-threat-landscape-for-the-us-water-wastewater-sector/.

[26] DRAGOS. *The Oldsmar Water Treatment Facility Cyber Attack*. 9 février 2021.
URL : https://www.dragos.com/blog/industry-news/recommendations-following-the-oldsmar-water-treatment-facility-cyber-attack/.

[27] LE MONDE INFORMATIQUE. *Les stations d'assainissement d'Oloron Sainte-Marie visées par un ransomware (MAJ) - Le Monde Informatique*. 30 septembre 2021.
URL : https://www.lemondeinformatique.fr/actualites/lire-les-stations-d-assainissement-d-oloron-sainte-marie-visees-par-un-ransomware-maj-84347.html.

[28] USINE DIGITALE. *Le service d'assainissement des eaux d'Oloron-Sainte-Marie a été pris pour cible par des hackers*. 30 septembre 2021.
URL : https://www.usine-digitale.fr/article/le-service-d-assainissement-des-eaux-d-oloron-sainte-marie-a-ete-pris-pour-cible-par-des-hackers.N1145927.

[29] CISA. *IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities | CISA*. 1er décembre 2023.
URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.

[30] DELL SECUREWORKS. *Iranian Cyber Av3ngers Compromise Unitronics Systems*. 7 décembre 2023.
URL : https://www.secureworks.com/blog/iranian-cyber-av3ngers-compromise-unitronics-systems.

[31] @DAILYDARKWEB. *Dark Web Intelligence on X : "Handala Team Allegedly Hacked ROTEC - Reverse Osmosis Technologies & WFI Group in Retaliation for Cutting off Gaza's Water Supply The Group Claims to Have Dumped All Data (over 79GB) and Destroyed the Network. #DarkWeb https ://t.co/wLQx7L3Evz" / X*. 14 mars 2024.
URL : https://x.com/DailyDarkWeb/status/1768170384904319314.

[32] CYBERINT. *Handala Hack : What We Know About the Rising Threat Actor*. 16 juillet 2024.
URL : https://cyberint.com/blog/threat-intelligence/handala-hack-what-we-know-about-the-rising-threat-actor/.

[33] WIRED. *Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities*. 17 avril 2024.
URL : https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/.

[34] LE MONDE. *Comment Sandworm, les hackeurs d'élite de l'armée russe, ont piraté un moulin français en pensant attaquer un barrage*. 17 avril 2024.
URL : https://www.lemonde.fr/pixels/article/2024/04/17/comment-sandworm-les-hackeurs-d-elite-de-l-armee-russe-ont-pirate-un-moulin-francais-en-pensant-attaquer-un-barrage_6228320_4408996.html.

[35] @CYBERARMYOFRUSSIA_REBORN. *Cyber Army of Russia_Reborn Group Claims on Telegram Channel to Have Compromised Italian Water Treatment Facility*. 21 juin 2024.
URL : https://t.me/cyberarmyofrussia_reborn/8238.

[36] MANDIANT. *APT44 : Unearthing Sandworm*. 17 avril 2024.
URL : https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf.

[37] EUROMAIDAN. *Ukrainian Hackers Target Russia's Water Supply Company*. 21 décembre 2023.
URL : https://euromaidanpress.com/2023/12/21/ukrainian-hackers-target-russias-major-water-supply-company/.

[38] CERT-UA. *Плани UAC-0133 (Sandworm) щодо кібердиверсії на майже 20 об'єктах критичної інфраструктури України*. 19 avril 2024.
URL : https://cert.gov.ua/article/6278706.

[39] COMPUTERWORLD. *Insider Charged with Hacking California Canal System*. 29 novembre 2007.
URL : https://www.computerworld.com/article/1594746/insider-charged-with-hacking-california-canal-system.html.

[40] VICE. *Feds Indict Kansas Man for Allegedly Hacking Into Water Supply*. 1er avril 2021.
URL : https://www.vice.com/en/article/3anx79/feds-indict-kansas-man-for-allegedly-hacking-into-water-supply.

[41] CYBERSCOOP. *German Intelligence Agencies Warn of Russian Hacking Threats to Critical Infrastructure*. 26 mai 2020.
URL : https://cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/.

[42] THE NEW YORK TIMES. *U.S. Hunts Chinese Malware That Could Disrupt American Military Operations (Published 2023)*. 29 juillet 2023.
URL : https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html.

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

[44] CYJAX. *EMEA and APAC Governments Targeted in Widespread Credential Harvesting Campaign*. 16 septembre 2021.
URL : https://www.cyjax.com/emea-and-apac-governments-targeted-in-widespread-credential-harvesting-campaign/.

[45] KASPERSKY. *Tomiris Backdoor and Its Connection to Sunshuttle and Kazuar*. 29 septembre 2021.
URL : https://securelist.com/darkhalo-after-solarwinds-the-tomiris-connection/104311/.

Version 1 – 28 novembre 2024

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