RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Date : 24 février 2025
Version : 1.0
Nombre de pages : 11

COLLECTIVITÉS TERRITORIALES

SYNTHÈSE DE LA MENACE

TLP:CLEAR

Table des matières

1 INTRODUCTION

Les collectivités territoriales sont des personnes morales de droit public exerçant, sur un territoire défini, des compétences qui lui sont déléguées par l'État. En France, ces collectivités revêtent plusieurs formes : les communes, plus petit échelon des collectivités territoriales, les Établissements Publics de Coopération Intercommunale (EPCI), les départements et les régions. La France dispose également de collectivités à statut particulier, regroupant parfois les compétences des départements et des régions (collectivités territoriales de Martinique, de Guyane, département de Mayotte), ou les compétences d'une commune et d'un département (Ville de Paris, Métropole de Lyon), ou bien encore en Outre-mer des collectivités disposant de compétences spécifiques (Polynésie française, Nouvelle-Calédonie, *etc*.).

Les collectivités territoriales gèrent de nombreux services selon leurs compétences, en matière administrative et régalienne (état civil), éducative (gestion des écoles, collèges et lycées), sociales (prestations sociales, centres sociaux), médicales (EHPAD), d'urbanisme, de gestion des ressources en énergie et en eau (approvisionnement et traitement), *etc*. Ces compétences sont exercées soit directement par les collectivités, soit en mutualisation par le biais de régies intercollectivités. Maillons essentiels de la relation entre l'État et les citoyens, les collectivités territoriales sont de fait dépositaires d'un très grand nombre de données personnelles de leurs administrés.

Les conséquences d'attaques informatiques peuvent donc être majeures à l'échelle d'une collectivité, et affecter de multiples champs de compétences et de nombreux citoyens.

2 BILAN DES INCIDENTS PORTÉS À LA CONNAISSANCE DE L'ANSSI EN 2024

De janvier à décembre 2024, l'ANSSI a traité **218 incidents cyber** affectant les collectivités territoriales, soit une **moyenne de 18 incidents par mois**. Le périmètre étudié prend en compte les communes, les établissements publics de coopération intercommunales (EPCI)[1] , les départements, les régions, les collectivités territoriales uniques et collectivités d'outre-mer. **Ces incidents représentent 14% de l'ensemble des incidents traités par l'ANSSI sur la période**.

Au cours de l'année 2024, la majorité des évènements de cybersécurité touchant les collectivités territoriales portés à la connaissance de l'ANSSI concerne des communes et/ou des EPCI à fiscalité propre. Néanmoins, la prépondérance des communes et EPCI à fiscalité propre est à mettre en perspective avec leur nombre en France : il existe près de 35 000 communes, 1250 EPCI à fiscalité propre et près de 9000 EPCI sans fiscalité propre en 2023 sur l'ensemble du territoire national.

Au cours de la période étudiée, l'ANSSI a traité **44 incidents affectant des départements** et **29 incidents affectant des régions**. Ces chiffres se révèlent élevés en comparaison du nombre de départements (101) et de régions (18) sur le territoire français et pourraient indiquer un ciblage

1. Les EPCI sont des structures administratives françaises regroupant plusieurs communes afin d'exercer certaines de leurs compétences en commun. Il existe deux catégories d'EPCI : les EPCI à fiscalité propre (communauté de communes, communauté d'agglomérations, communauté urbaine et métropole) et les EPCI sans fiscalité propre (syndicats intercommunaux et syndicats mixtes).

plus important de ces structures et/ou un signalement d'incidents auprès de l'ANSSI effectué de façon plus systématique par ce type de collectivités territoriales. Enfin, l'ANSSI a traité 2 évènements de cybersécurité ciblant des EPCI sans fiscalité propre.

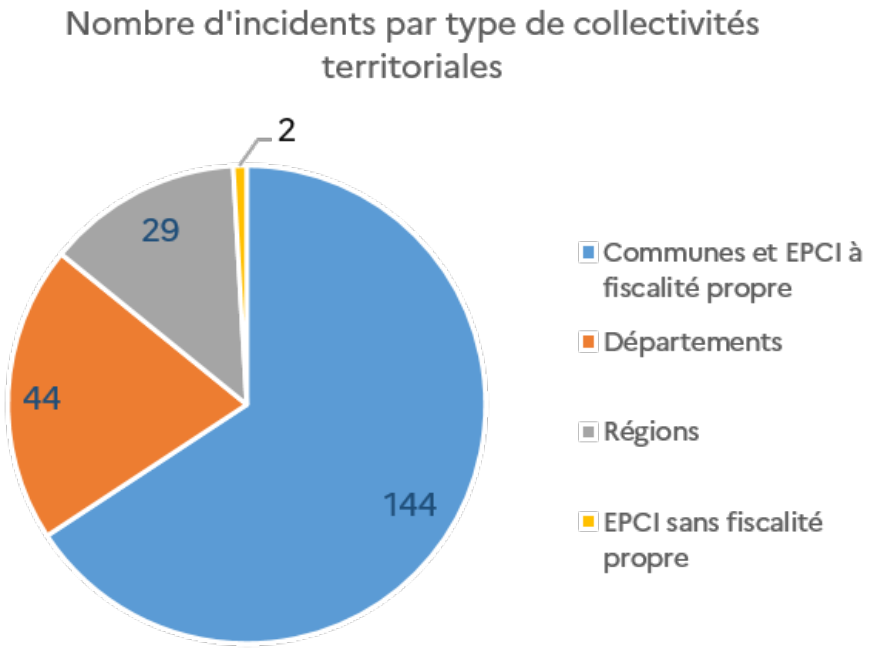

FIGURE 1 – Répartition des incidents portés à la connaissance de l'ANSSI en 2024

3 ATTAQUES À BUT LUCRATIF

Les attaques à but lucratif représentent la principale menace cyber pour les collectivités territoriales. Quelle que soit leur taille, elles sont ciblées de façon opportuniste par l'ensemble des acteurs de l'écosystème cybercriminel.

Les collectivités territoriales sont en effet des cibles de choix pour ces acteurs : souvent peu ou mal sécurisées, gestionnaires de systèmes d'information nombreux et disparates, elles peuvent éprouver des difficultés à maîtriser la cartographie de leurs réseaux et à les garder dans de bonnes conditions de sécurité.

3.1 Attaques au moyen de rançongiciels

Ainsi, de nombreuses municipalités en France et dans l'ensemble du monde sont victimes d'attaques menées par des groupes cybercriminels au moyen de rançongiciels. Ces attaques représentent une part importante de l'engagement opérationnel de l'ANSSI, tant au sein de l'Hexagone que dans les collectivités d'Outre-mer.

Au cours de la période étudiée, les collectivités territoriales se sont révélées être des cibles privilégiées de la **menace cybercriminelle**. Ainsi, parmi les incidents ayant affecté les collectivités portés à la connaissance de l'ANSSI, on retrouve majoritairement des **compromissions de comptes de messagerie** (66, soit 30% des événements signalés) puis les **attaques en déni de service distribué** (DDoS) (58).

L'ANSSI a également traité divers incidents relatifs à des **intrusions sur les systèmes d'information** (hors attaques par rançongiciel) allant de la **connexion illégitime réussie** jusqu'au **dépôt de code malveillant** sur le réseau de la victime. De nombreuses collectivités territoriales ont été victimes d'une intrusion sur leur système d'information via **l'exploitation de vulnérabilités**[a] [1].

25 incidents touchant des collectivités territoriales liés à des compromissions et chiffrements par rançongiciel ont été rapportés à l'ANSSI au cours de l'année 2024, soit 11% des incidents en lien avec ce secteur. La majorité des victimes de rançongiciel sont des **communes** et **EPCI à fiscalité propre**. Sur la période étudiée, 21 de ces 25 incidents ont engendré des effets importants sur le fonctionnement des collectivités territoriales ciblées. Les souches de rançongiciel les plus signalées à l'ANSSI sont **LOCKBIT** (5), suivie de **RAMSOMHUB** (3), **BABUK** (2) et **8BASE** (2). Des **exfiltrations de données** à caractère technique, personnelle ou administrative ont été identifiées au cours de **12 incidents**.

a. Majoritairement des vulnérabilités affectant des équipements de bordure (CVE-2023-46805, CVE-2024-21887, CVE-2024-21893, CVE-2024-3400 et CVE-2024-47575).

De plus, en raison d'interconnexions ou de regroupement de systèmes d'information entre collectivités, les compromissions observées peuvent également avoir des effets de bord sur d'autres collectivités territoriales.

Le CERT-Bund, dans son rapport annuel pour 2024, mentionne ainsi la compromission par rançongiciel d'un fournisseur de services informatiques dédié aux collectivités territoriales allemandes en octobre 2023. Cette compromission a touché en même temps un nombre important de collectivités, le prestataire gérant les services informatiques de 72 collectivités et 20 000 postes de travail. Les conséquences de cette attaque, revendiquée par le groupe cybercriminel Akira, ont pesé sur 1,7 millions d'habitants concernés par les interruptions de service des collectivités clientes de ce fournisseur.

La gestion de l'incident a, selon le CERT-Bund, impliqué de nombreux acteurs et **la restauration complète des services des collectivités n'était pas complète plusieurs mois après l'attaque** [2].

En avril 2024, l'ANSSI est alertée de la **compromission** et du **chiffrement** d'une commune par le biais du rançongiciel LOCKBIT 3.0. En raison de l'ampleur de la compromission, la commune a été contrainte d'**isoler** son système d'information d'internet et de **couper l'ensemble des interconnexions** avec d'autres communes. Le système d'information du bénéficiaire **hébergeant** ceux d'autres organisations, la coupure des accès a rendu les services de ces dernières **indisponibles**. La réouverture des flux a été permise **progressivement** dans les semaines suivant l'incident.

L'arrêt des services des collectivités en cas d'attaque, notamment par rançongiciel, revêt une gravité particulière et renforce la pression sur ces entités.

À la suite de la compromission du parc informatique d'une entité, de multiples services pu-

blics (aides sociales, état civil, urbanisme, administration des cimetières, gestion de l'eau et des déchets, *etc.*) et services internes à la collectivité (téléphonie, messagerie, finances, ressources humaines, *etc.*) ne sont plus opérationnels. Ces difficultés obligent souvent la collectivité affectée à basculer vers un mode de fonctionnement dégradé, voire manuel, affectant son activité opérationnelle et ses missions de service public auprès des usagers. Ce fonctionnement dégradé est observé également, avec une ampleur moindre, lors d'incidents sans impact majeur. En effet, les mesures d'endiguement mises en place pour remédier aux incidents affectent également la qualité de service des collectivités.

Lors d'incidents présentant une criticité importante, **plusieurs mois sont souvent nécessaires avant le retour à un fonctionnement en mode nominal**. Cette situation est causée par le délai important nécessaire à la reconstruction et au durcissement du système d'information ainsi qu'à la remontée progressive des différentes applications métiers de la collectivité.

Ainsi, certaines attaques peuvent non seulement avoir des conséquences sur la continuité des services publics, mais également entraîner des pertes financières importantes pour une collectivité. La compromission du site de vente de billets de transports urbains de l'État de l'Uttar Pradesh en Inde en 2023, a entraîné une interruption de vente de plus de dix jours et une perte significative de revenus pour la collectivité [3].

Au cours de l'année 2024, 33 incidents affectant des collectivités territoriales ont eu une **criticité élevée**, soit 15% du nombre total d'incidents sur le périmètre étudié. Ces incidents sont majoritairement constitués d'attaques par rançongiciel et/ou d'actions illégitimes menant à des exfiltrations de données.

> En avril 2024, l'ANSSI est informée de la **compromission** et du **chiffrement** de plusieurs serveurs du système d'information d'une commune de taille importante par le biais du **rançongiciel BABUK**. Contrainte de déconnecter son système d'information d'Internet, la commune a subi la **mise à l'arrêt de l'ensemble de ses services publics et internes**. Ceux-ci ont pu être redémarrés petit à petit dans les semaines suivant l'incident.

> En novembre 2024, un **conseil départemental** signale à l'ANSSI la compromission de son environnement ***Active Directory*** et une **exfiltration de données**. L'ensemble du système d'information a été isolé d'internet, provoquant de **forts impacts métiers**, notamment du fait de la perte d'accès à la messagerie.

Dans de nombreux cas, la présence d'un **plan de reprise d'activité** (PRA) recensant et priorisant les différentes applications ainsi que la disponibilité de **sauvegardes saines et déconnectées du réseau** permettent d'améliorer significativement le temps nécessaire aux actions de remédiation.

3.2 Exfiltration et vente de données et d'accès

Les **données administratives, financières et personnelles des administrés** détenues au sein des collectivités sont nombreuses et présentent un intérêt pour les attaquants, qui peuvent accentuer le **chantage à la publication** de ces données lors de leurs attaques.

Ainsi, en 2024 de nombreuses collectivités territoriales ont fait l'objet de vente d'accès à leurs systèmes d'information ou à leurs données par des acteurs cybercriminels sur des forums du *darknet*. Ces ventes peuvent découler d'attaques par rançongiciel précédées d'une exfiltration

massive de données (comme cela aurait été le cas pour la municipalité de Dubaï en juin 2024, victime du groupe cybercriminel Daixin) [4], ou bien de l'utilisation d'*infostealers*[2]. L'origine des données mises en vente reste parfois inconnue.

Ces cas mettent en évidence des **atteintes importantes à la vie privée** (accès à des registres d'état civil et de gestion de biens et propriétés, accès aux modules de facturation des collectivités etc.) des administrés et des agents des collectivités concernées.

Les cas d'exfiltration et de publication de données constituent enfin un véritable enjeu pour les collectivités territoriales sur les plans **juridiques** et **réputationnels**.

> En janvier 2024, l'ANSSI est informée qu'une commune est affectée par une **fuite de données**. L'ensemble de l'**annuaire** de la commune a été exfiltré et partagé sur plusieurs forums cybercriminels, exposant des **données personnelles des employés de la ville**.

3.3 Autres types d'attaques à but lucratif

Les collectivités sont également la cible d'autres types d'attaques à but lucratif menées par des cybercriminels : arnaques dites « au président », hameçonnage à des fins de collecte de données personnelles (ensuite revendues sur des forums cybercriminels), spam *etc.* Ainsi, en 2023, une grande collectivité territoriale française a fait l'objet d'une compromission de ses comptes de messageries : les attaquants ont pu récupérer les identifiants d'un agent de cette collectivité, puis de là ont pu mener des campagnes d'hameçonnage envers les autres agents et les partenaires de cette collectivité. Suite à la compromission des comptes de messagerie, des données potentiellement sensibles ont probablement été exfiltrées.

Les compromissions de messagerie ainsi que les attaques par point d'eau (ajout de liens illégitimes sur un site web en vue de compromettre de nouvelles cibles), constituent un vecteur de compromission plus large qu'il peut être possible d'éviter par la mise en œuvre de mesures de **sécurisation** et de **durcissement** ainsi que par des mesures de **sensibilisation** auprès des utilisateurs.

4 ATTAQUES À BUT DE DÉSTABILISATION

Les attaques à but de déstabilisation revêtent deux grandes réalités : d'une part des attaques menées par des groupes plus ou moins informels d'activistes aux motivations politiques, d'autre part des attaques menées par des groupes affiliés à des États ayant des objectifs de sabotage. Si les collectivités françaises sont aujourd'hui davantage ciblées par des groupes dits « hacktivistes », d'autres collectivités dans le monde ont pu être ciblées par des attaques destructrices, notamment conduites par des attaquants réputés étatiques.

2. Les *infostealers* sont des programmes malveillants ayant pour fonction d'exfiltrer des identifiants de connexion, des informations bancaires ou d'autres types de données personnelles. Les *infostealers* sont souvent opérés par des acteurs malveillants spécialisés, qui revendent ensuite ces données à d'autres acteurs cybercriminels. Les attaques menées au moyen d'*infostealers* ont fortement progressé depuis quelques années.

4.1 Hacktivisme

Les attaques à but de déstabilisation sont fortement dépendantes du contexte national et international, notamment géopolitique. Ainsi depuis 2022, les collectivités territoriales françaises ont été régulièrement ciblées dans les contextes successifs de l'invasion de l'Ukraine par la Russie et du soutien apporté à l'Ukraine par la France, du conflit au Proche-Orient depuis le 7 octobre 2023, mais également de l'organisation des Jeux Olympiques et Paralympiques en France à l'été 2024.

Le soutien apporté par la France à l'Ukraine depuis le début de l'invasion de l'Ukraine par la Russie en février 2022 a entraîné des vagues régulières d'**attaques par déni de service distribué** (DDoS) contre des entités de toute nature, notamment des sites Internet de collectivités territoriales françaises. Ces attaques sont menées par des groupes hacktivistes pro-russes en représailles au positionnement de la France. Les collectivités semblent ciblées essentiellement parce qu'elles représentent l'administration française.

La vague d'attaques du 31 décembre 2024, revendiquée par le groupe hacktiviste pro-russe NoName057(16) et ayant touché (sans conséquences majeures) de nombreuses collectivités françaises (villes, départements et régions) ainsi que de nombreuses administrations, est un exemple de ces actions. Des attaques similaires ont eu lieu dans de nombreux pays européens.

Le contexte du conflit au Proche-Orient a également été exploité par des groupes hacktivistes pro-palestiniens pour mener des attaques contre des collectivités. Si la majorité des collectivités sont victimes de DDoS, certaines (notamment en Israël) ont également subi des attaques entraînant des exfiltrations et publications de données ou des défigurations de leurs sites Web.

La période des Jeux Olympiques et Paralympiques de Paris 2024 a été particulièrement propice à ce type d'attaques par DDoS contre des entités de toute nature, parmi lesquelles de nombreuses collectivités territoriales.

Depuis une dizaine d'années les collectivités ont subi des vagues d'attaques par des groupes d'hacktivistes cherchant une visibilité au moyen de **défiguration de sites Internet**. Exploitant des failles de sécurité dans les sites Internet de nombreuses communes, ces attaquants modifient le contenu des pages affichées et y inscrivent des revendications politiques ou religieuses, souvent liées au contexte géopolitique. Ces défigurations touchent des collectivités territoriales dans le monde entier. Ainsi, plusieurs dizaines de sites Internet de mairies françaises ont fait l'objet de défigurations portant des messages pro-russes en mai 2023 [5].

Si ces attaques ne sont pas d'une grande sophistication, elles portent atteinte à l'image de ces collectivités et peuvent susciter la crainte chez leurs administrés.

4.2 Sabotage par des acteurs réputés étatiques

Dans le cadre de tensions géopolitiques ou de conflits, certaines collectivités territoriales sont également ciblées par des attaques ayant pour but de **saboter des infrastructures**. Les infrastructures liées à l'approvisionnement en eau et en énergie, souvent opérées ou sous la responsabilité des collectivités, sont des cibles récurrentes de ce type d'attaque.

Ainsi, un groupe d'attaquants réputé lié à l'Iran et soutenant les revendications palestiniennes (Cyber Av3ngers) aurait compromis en novembre 2023 une infrastructure municipale de gestion de l'eau en Pennsylvanie (États-Unis). Les attaquants auraient pris le contrôle de la station mais sans réussir à y créer de dommages, au travers de la compromission d'un logiciel métier édité par une société israélienne, probablement la cible initiale des attaquants, ceux-ci ayant des liens

présumés avec l'Iran[6]. Toujours aux États-Unis, la CISA et le FBI ont publié en août 2024 un avis de sécurité mentionnant, entre autres secteurs, le ciblage de collectivités territoriales états-uniennes par le MOA Pioneer Kitten, utiliser pour mener des attaques par rançongiciel. Le FBI considère que ce MOA est aligné avec les intérêts stratégiques iraniens [7].

Dans le cadre de l'invasion russe de l'Ukraine, des entités du secteur de l'énergie gérées par des municipalités en Ukraine ont été ciblées par le biais de MOA liés aux intérêts russes. Ces attaques visent des protocoles couramment utilisés dans des infrastructures critiques et s'ajoutent aux destructions physiques dues au conflit.

Selon les données portées à la connaissance de l'ANSSI, les collectivités territoriales françaises n'ont pas fait l'objet d'attaques par sabotage dans une période récente. Cependant, dans **le contexte d'une hausse de la menace à but de déstabilisation liée au conflit en Ukraine et de l'organisation des Jeux Olympiques et Paralympiques de Paris 2024**, plusieurs infrastructures d'envergure locale, notamment liées à la gestion de l'eau ont pu faire l'objet de campagnes de reconnaissance par des acteurs offensifs durant l'année 2024 [8].

5 ATTAQUES À BUT D'ESPIONNAGE

Les collectivités territoriales ne sont pas réputées être les premières cibles des attaques à finalité d'espionnage menées par des attaquants liés à des États. Cependant, comme toutes entités renfermant des données, elles peuvent faire l'objet de telles compromissions. **Les collectivités peuvent gérer des données sensibles dont l'exfiltration peut être jugée intéressante pour des groupes opérant pour le compte d'États**.

Le ciblage de collectivités territoriales par des acteurs liés à des États a pu être révélé par l'analyse de campagnes de hameçonnage ciblé : en mars 2024, une campagne associée au MOA Muddywater, réputé lié aux intérêts stratégiques iraniens, aurait utilisé des envois de **mails d'hameçonnage** invitant à télécharger une application malveillante prétendant répondre à des besoins spécifiques de collectivités israéliennes [9]. De même, des mails d'hameçonnage reprenant des thématiques liées aux collectivités territoriales ont été retrouvés lors d'une campagne associée au MOA réputé lié aux intérêts russes APT 28, ciblant l'Argentine en mars 2024 [10].

Les collectivités peuvent également, à leur insu, participer à la **construction d'infrastructure d'attaques** pour des modes opératoires d'attaque : ces groupes, procédant avec un haut niveau de sophistication, cherchent en effet à compromettre des équipements informatiques légitimes afin de les enrôler dans des réseaux servant à anonymiser leur navigation, pour ensuite mener des compromissions à but d'espionnage sur leurs cibles finales. Les collectivités territoriales, par la taille de leurs réseaux informatiques et la multitude d'équipements, parfois mal sécurisés, qu'elles doivent gérer, sont fréquemment victimes de ces compromissions.

La sécurisation de ces équipements périphériques (**routeurs notamment**) **est importante pour lutter contre la prolifération de ces réseaux d'anonymisation utilisés par de nombreux groupes d'attaquants pratiquant des compromissions à but d'espionnage**.

A Références

[1] ANSSI. *Failles sur les équipements de sécurité - Retour d'expérience du CERT-FR*. 12 juin 2024.
URL : https://cert.ssi.gouv.fr/cti/CERTFR2024-CTI-005.

[2] BSI. *The State of IT Security in Germany in 2024*. 18 novembre 2024.
URL : https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html.

[3] STORMSHIELD. *Urban Mobility and Cybersecurity, at the Heart of the Smart City*. 28 mai 2024.
URL : https://www.stormshield.com/news/smart-city-and-cybersecurity-the-issue-of-urban-mobility/.

[4] CYBERNEWS. *Dubai government suffers alleged ransomware attack*. 6 juin 2024.
URL : https://cybernews.com/news/dubai-government-ransomware-attack-daixin.

[5] LE FIGARO. *Plusieurs sites Internet de mairies françaises victimes d'une cyberattaque pro-russe*. 3 mai 2023.
URL : https://www.lefigaro.fr/secteur/high-tech/plusieurs-sites-internet-de-mairies-fran%C3%A7aises-victimes-d-une-cyberattaque-pro-russe-20250503.

[6] SECURITY AFFAIRS. *Iranian hacker group Cyber Av3ngers hacked the Municipal Water Authority of Aliquippa in Pennsylvania*. 27 novembre 2023.
URL : https://securityaffairs.com/154818/hacktivism/cyber-av3ngers-hacked-municipal-water-authority-of-aliquippa.html.

[7] CISA. *Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations*. 28 août 2024.
URL : https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a.

[8] ANSSI. *Secteur de l'eau. État de la menace informatique*. 28 novembre 2024.
URL : https://cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-11/.

[9] CHECKPOINT. *New BugSleep Backdoor Deployed in Recent MuddyWater Campaigns*. 15 juillet 2024.
URL : https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/.

[10] SECURITY INTELLIGENCE. *Ongoing ITG05 Operations Leverage Evolving Malware Arsenal in Global Campaigns*. 11 mars 2024.
URL : https://securityintelligence.com/x-force/itg05-leverages-malware-arsenal/.

ANSSI/SDO/DCA

Version : 1.0 – 24 février 2025

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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