TLP:CLEAR

SYNTHÈSE DE LA MENACE CIBLANT LES COLLECTIVITÉS TERRITORIALES

23 octobre 2023

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 EPCI, les départements et les régions. La France dispose également de collectivités à statut particulier, regroupant parfois les compétences des départements et des régions (collectivité territoriale 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 inter-collectivités. 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 impacts d'attaques informatiques peuvent donc être majeurs à l'échelle d'une collectivité, et affecter de multiples champs de compétences et de nombreux citoyens.

Incidents traités par l'ANSSI

De janvier 2022 à juin 2023, l'ANSSI a traité **187 incidents cyber** affectant les collectivités territoriales, soit une **moyenne de 10 incidents par mois**. Le périmètre étudié prend en compte les communes, les établissements publics de coopération intercommunales (EPCI [a]), les départements, les régions, les collectivités territoriales uniques et collectivités d'outre-mer. **Ces incidents représentent 17% de l'ensemble des incidents traités par l'ANSSI sur la période**.

Depuis janvier 2022, la majorité des incidents (126) affectant les collectivités territoriales portés la connaissance de l'ANSSI concernent des communes et/ou des EPCI à fiscalité propre (dont les chiffres sont agrégés du fait des imbrications fréquentes entre les SI de ces deux types d'entités). 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, 5 incidents ont affecté des EPCI sans fiscalité propre. La nature de ces structures administratives les rend particulièrement sensibles, avec de potentielles **fortes conséquences pour les collectivités territoriales ayant mutualisé leurs services**.

Au cours de la période étudiée, **42 incidents affectant un département** et **12 incidents ciblant une région** ont été constatés. Ces chiffres se révèlent élevés en comparaison du nombre de département (101) et de régions (18) sur le territoire français et pourraient indiquer un ciblage 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.

a. 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 (syndicat intercommunaux et syndicat mixtes).

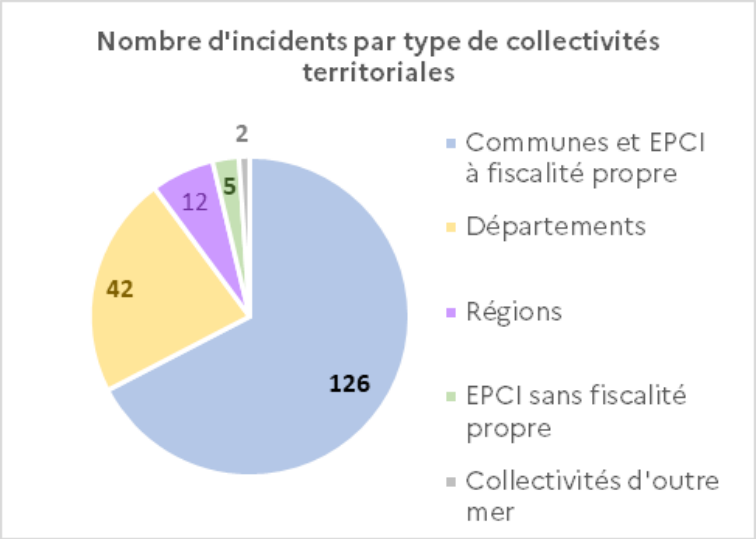

FIG. 1.1 – Nombre d'incidents par type de collectivités territoriales entre janvier 2022 et septembre 2023

2 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.

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.

En outre, 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.

> **40 incidents touchant des collectivités territoriales liés à des compromissions et chiffrements par rançongiciel** ont été rapportés à l'ANSSI au cours de la période étudiée (2022-2023), soit 22% des incidents signalés. Sur la période étudiée, ces incidents ont engendré les effets les plus importants sur le fonctionnement des collectivités territoriales ciblées. Parmi les souches de rançongiciels observées, la souche LOCKBIT a été observée à 18 reprises, soit près de la moitié des cas constatés. De façon plus marginale, les souches HIVE, CONTI et PLAY ont également été observées à plusieurs reprises.

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 publics (aides sociales, état civil, urbanisme, administration des cimetières, gestion de l'eau et des déchets, *etc.*) et services internes à la collectivité (téléphonie, messagerie, finance, ressources humaines, *etc.*) ne sont plus opérationnels. Ces difficultés obligent à 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.

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

En 2022, l'ANSSI est informée de la **compromission et du chiffrement des systèmes d'information d'une collectivité**, probablement par le biais du rançongiciel PLAY. Contrainte d'isoler son système d'information d'Internet et de couper toutes ses interconnexions, la collectivité indique que la **quasi-totalité des 158 services hébergés en interne est à l'arrêt**. Les services publics de la collectivité ont pu être maintenus, mais avec un mode de fonctionnement dégradé début 2023.

Lors d'incidents possédant 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.

Au cours de la période étudiée, 42 incidents possédant une criticité élevée ont été recensés concernant les collectivités territoriales, soit 22% 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.

Dans de nombreux cas, la présence d'un plan de reprise d'activité 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.

En 2022, l'ANSSI reçoit un signalement relatif à la **compromission et au chiffrement** des systèmes d'information d'une collectivité territoriale par le biais d'un rançongiciel. En raison de l'ampleur de la compromission du système d'information, le bénéficiaire, accompagné par un prestataire, a reconstruit un nouveau système d'information. Cette mesure, **coûteuse en temps et en argent**, implique un fonctionnement en mode dégradé pour la collectivité territoriale en attendant une reconstruction complète. Ainsi, il a fallu près de **quatre mois** pour que l'ensemble des services soient à nouveau opérationnels. La collectivité a poursuivi un **plan de durcissement** du système d'information jusqu'en 2023.

Les cas d'exfiltration et de publication de données constituent enfin un véritable enjeu pour les collectivités territoriales sur les plans juridiques et réputationnels. Les exfiltrations de données touchent autant les agents de la collectivité que les usagers qui voient leurs données (données personnelles, bulletin de paie, *etc*.) potentiellement exposées.

En février 2023, l'ANSSI est informée de la compromission des systèmes d'information d'une commune. Les investigations ont révélé qu'un groupe cybercriminel aurait procédé à l'**exfiltration de 1,3To de données personnelles**. Un mois plus tard, une partie des données exfiltrées a été publiée sur le site du groupe.

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.

51 compromissions de comptes de messagerie ont été signalées à l'ANSSI depuis janvier 2022 sur le périmètre concerné, représentant ainsi 28% des incidents rapportés sur la période.

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.

Au nombre de 43 relevées par l'ANSSI sur la période étudiée, les **intrusions sur le système d'information** (hors attaques par rançongiciel) regroupent des incidents aux **criticités diverses**, allant de la connexion illégitime réussie jusqu'au dépôt de maliciels sur le réseau compromis.

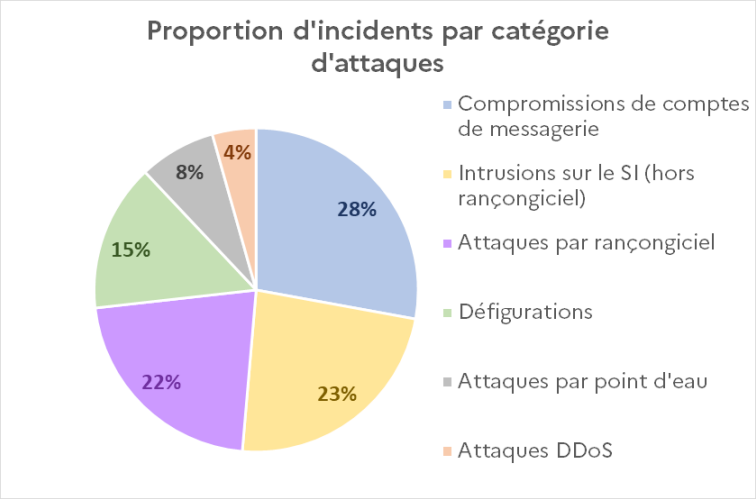

FIG. 2.1 – Proportion d'incidents par catégorie d'attaque

3 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.

3.1 Hacktivisme

Depuis une dizaine d'années les collectivités françaises 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.

Ainsi, comme à la suite des attentats de janvier 2015 où de nombreuses communes françaises avaient vu leurs sites compromis par des hacktivistes se revendiquant de l'État islamique, des collectivités françaises font régulièrement l'objet de défigurations revendiquées par des groupes pro-russes depuis le début de l'invasion de l'Ukraine en février 2022.

Certaines communes peuvent également être touchées par des attaques par déni de service distribué (DDoS) menées par des hacktivistes : ces attaques, également reliées au contexte international, restent peu nombreuses (8 ont été signalées à l'ANSSI) depuis février 2022 et souvent revendiquées par des groupes pro-russes.

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.

Ces attaques à motivation politique peuvent également revêtir d'autres aspects : ainsi, certaines collectivités ont fait l'objet d'attaques ayant pour but d'exfiltrer et de publier des données internes. En 2021, une municipalité brésilienne

a ainsi été victime d'une divulgation massive de données personnelles, cartes d'identité, informations fiscales *etc*., revendiquée par des groupes hacktivistes.

3.2 Sabotage par des acteurs réputés étatiques

Les attaques à but de sabotage visant des collectivités territoriales sont pour l'heure rares à avoir ciblé la France. Cependant, dans **le contexte d'une hausse de la menace à but de déstabilisation liée au conflit en Ukraine et à la prochaine organisation des Jeux Olympiques et Paralympiques de Paris 2024**, cette menace doit continuer à être prise au sérieux.

Les attaques à but de sabotage peuvent engendrer de nombreux dysfonctionnements et avoir un impact majeur sur le fonctionnement d'une collectivité. Ainsi, en juin 2022, la municipalité de Téhéran (Iran) a fait l'objet d'une série d'attaques (attribuées par les services de renseignement iraniens à Israël), supprimant de nombreuses données des serveurs de la municipalité, arrêtant le circuit interne des 5000 caméras de surveillance des infrastructures critiques de la ville, défigurant plus de 150 sites Internet relevant de la municipalité et prenant le contrôle du système d'alerte par SMS de la ville, envoyant 600 000 messages aux habitants avec des messages politiques. Ces attaques ont également perturbé les systèmes de tickets de transport et ceux gérant le contrôle de la qualité de l'air de la ville.

Si une telle attaque reste exceptionnelle, elle met en lumière l'**impact majeur d'une attaque par sabotage** sur une collectivité territoriale.

4 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**.

Ces collectivités peuvent également, à leur insu, participer à la construction d'infrastructure d'attaques pour de tels groupes : 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**.

23 octobre 2023

Licence ouverte (Étalab - v2.0)

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