PERIMETRY RESEARCH

Baromètre de la sécurité des domaines de l'État

L'État protège-t-il bien ses sites et sa messagerie ? Mesures passives des domaines des préfectures, ministères, académies, ambassades et sites du Gouvernement de deux listes ouvertes, comparées à nos autres études.

Édition de novembre 2026

660
domaines avec un site à eux, notés

43,3 %
appliquent DMARC (quarantine ou reject)

13 %
ont A ou B

Perimetry Cloud
perimetry.cloud · Publiée le 14 novembre 2026

À propos de ce rapport

Perimetry Research publie des études sur la façon dont les organisations protègent leurs sites et leur messagerie, mesurée avec les mêmes contrôles passifs que Perimetry Cloud. Cette édition porte sur les 1 440 domaines de l'État de la liste des noms de domaine des organismes publics de la DINUM et de la liste des sites de l'Observatoire de l'écosystème numérique de l'État ; 1 069 sont actifs, et les 660 qui ont un site à eux sont notés. Elle ne nomme que les domaines qui font bien ; tous les autres chiffres sont des moyennes, et les problèmes graves ont été signalés au CERT-FR de l'ANSSI avant la publication.

Sommaire

01 Synthèse 3

02 Principaux constats 4

03 Notes 5

04 Contrôle par contrôle 6

05 Par catégorie 8

06 Selon le type de site 9

07 Les domaines sans site à eux 10

08 Comparaison avec nos autres études 11

09 Les domaines qui font bien 12

10 Problèmes graves 13

11 Recommandations 14

12 Méthodologie 15

13 À propos de Perimetry 17

01

Synthèse

660
domaines avec un site à eux, notés

46
note moyenne sur 100

43,3 %
appliquent DMARC (quarantine ou reject)

13 %
ont A ou B

Note moyenne des 660 domaines notés : 46 sur 100 ; médiane 44.

1. 56,7 % des domaines notés publient une politique DMARC et 43,3 % l'appliquent.
2. Côté sites : 63,8 % ont un certificat valide, 77,3 % renvoient vers HTTPS, 33,3 % utilisent HSTS d'au moins six mois.
3. DNSSEC est rare : 3,8 % des domaines notés sont signés, contre 22,1 % pour les communes.
4. 409 domaines actifs n'ont pas de site à eux ; 63,3 % d'entre eux n'appliquent pas DMARC.
5. 18,5 % des domaines actifs de l'État sont hors du .gouv.fr.

02

Principaux constats

Les indicateurs propres à l'État

18,5 % des domaines actifs sont hors du .gouv.fr, l'extension réservée à l'État.

0,9 % des domaines inscrits sont absents du DNS.

56,7 % des domaines notés publient une politique DMARC et 43,3 % l'appliquent.

Côté sites : 63,8 % ont un certificat valide, 77,3 % renvoient vers HTTPS, 33,3 % utilisent HSTS d'au moins six mois.

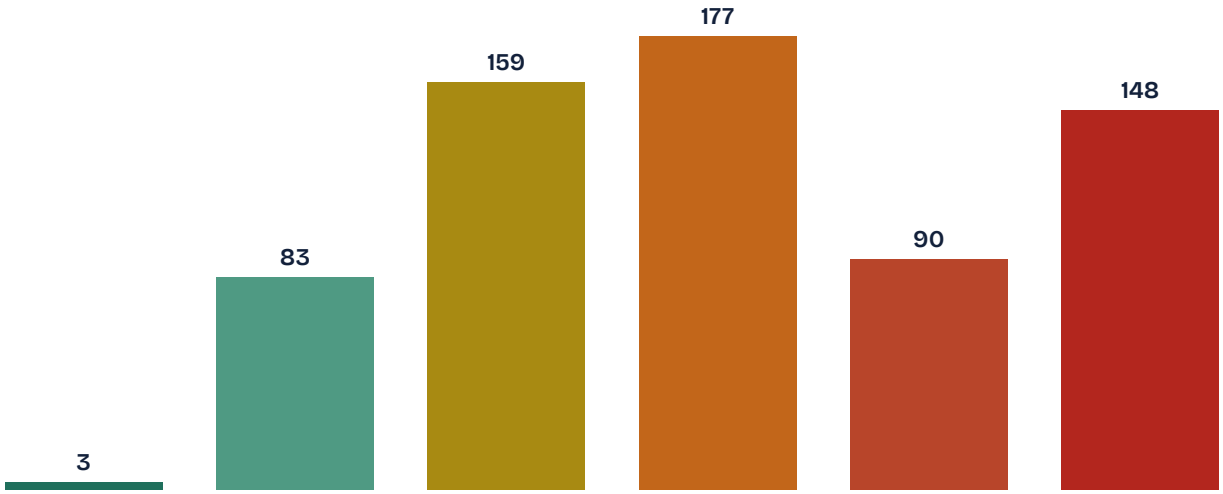
DNSSEC est rare : 3,8 % des domaines notés sont signés, contre 22,1 % pour les communes.

409 domaines actifs n'ont pas de site à eux ; 63,3 % d'entre eux n'appliquent pas DMARC.

03

Notes

Chaque domaine qui a un site à lui reçoit une note : la part des neuf contrôles qu'il réussit, parmi ceux qui le concernent (la note de nos autres études, sans le contrôle de l'adresse de contact, que les listes ne donnent pas). A à partir de 90, B de 75, C de 60, D de 40, E de 20, F en dessous.

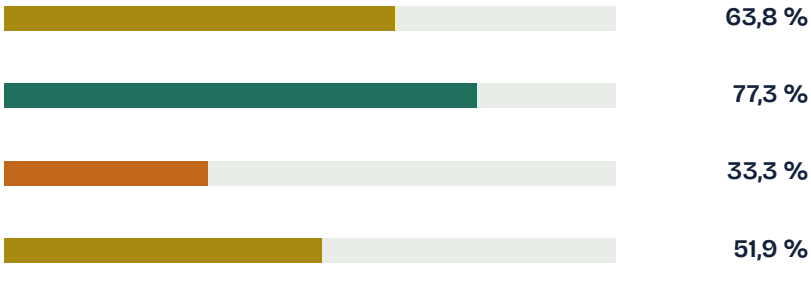


04

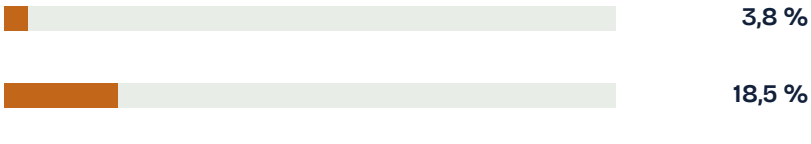
Contrôle par contrôle

Part des domaines notés qui réussissent chaque contrôle, parmi ceux qu'il concerne.

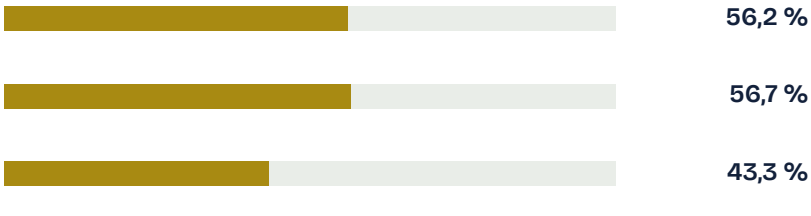
Site web



DNS



E-mail



Les neuf contrôles	
Site web · Certificat HTTPS valide	Le site répond en HTTPS avec un certificat en cours de validité, émis pour son nom et reconnu par les navigateurs.
Site web · HTTP renvoie vers HTTPS	Quelqu'un qui tape l'adresse arrive sur le site chiffré, et non sur une page que n'importe qui sur le réseau peut lire ou modifier.
Site web · HSTS d'au moins six mois	Les navigateurs retiennent qu'il faut utiliser HTTPS : la première requête non chiffrée ne peut pas être détournée.
Site web · En-têtes de protection de base	X-Content-Type-Options: nosniff, et une protection contre l'affichage du site dans le cadre d'un autre site (X-Frame-Options ou frame-ancestors dans la CSP).
DNS · DNSSEC	Les réponses DNS du domaine sont signées : on ne peut pas faire croire à un résolveur que le site ou la messagerie de l'administration sont ailleurs.
DNS · Enregistrement CAA	Le domaine désigne les autorités de certification autorisées à émettre des certificats à son nom.
E-mail · SPF strict	Le domaine liste les serveurs autorisés à envoyer son courrier et demande de rejeter ou de signaler les autres (-all ou ~all).

Les neuf contrôles	
E-mail · Enregistrement DMARC	Le domaine publie une politique DMARC, la norme qui relie SPF et DKIM à l'expéditeur affiché.
E-mail · DMARC appliqué	La politique est quarantine ou reject : un message falsifié au nom de l'administration, adressé à des usagers par exemple, part en indésirables ou est refusé, au lieu d'être distribué.

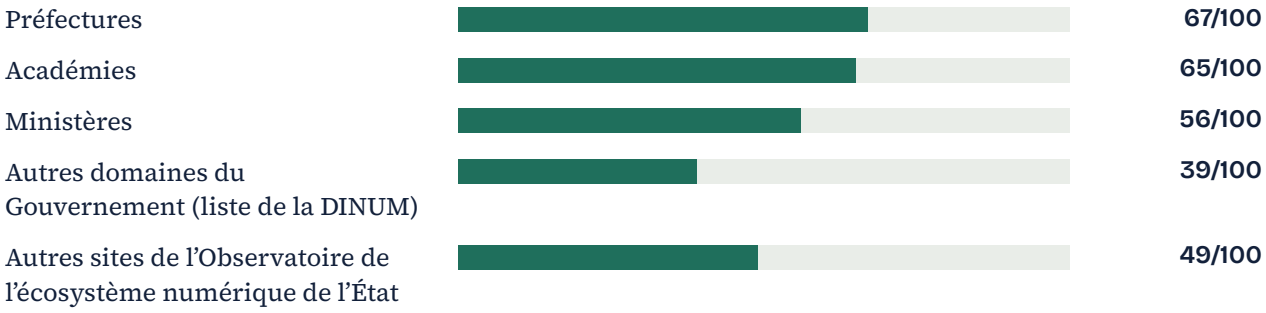
05

Par catégorie

Les catégories de moins de dix domaines notés ne sont pas détaillées. La plupart des domaines d'ambassade renvoient vers un site sur un autre domaine : ils sont comptés parmi les domaines sans site à eux.

Groupe	Notés	Moyenne	A ou B	DMARC appliqué	Médiane
Préfectures	94	67	0 %	100 %	71
Académies	34	65	29,4 %	32,4 %	67
Ambassades	2	·	·	·	·
Ministères	14	56	14,3 %	14,3 %	–
Santé	2	·	·	·	·
Autres domaines du Gouvernement (liste de la DINUM)	465	39	14,4 %	36,1 %	44
Autres sites de l'Observatoire de l'écosystème numérique de l'État	49	49	12,2 %	18,4 %	44

Moyenne



06

Selon le type de site

Les types de site de l'Observatoire, pour les domaines qu'il recense.

Groupe	Notés	Moyenne	A ou B	DMARC appliqué	Médiane
Sites institutionnels	175	65	13,1 %	74,9 %	71
Démarches en ligne	21	65	52,4 %	57,1 %	–
Sites thématiques	51	53	17,6 %	31,4 %	56
Autres (données ouvertes, recrutement, événements…)	34	56	23,5 %	29,4 %	56

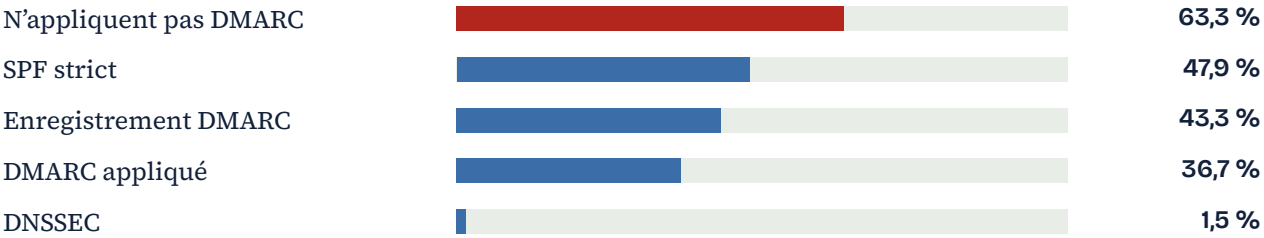
Moyenne



07

Les domaines sans site à eux

409 domaines actifs n'ont pas de site à eux : 159 renvoient vers un autre site, 250 ne servent qu'à la messagerie. Ils peuvent quand même servir à falsifier des e-mails au nom de l'État, et sont jugés sur leur DNS et leur messagerie seulement.



Note moyenne sur le DNS et la messagerie seulement : 28 sur 100.

08

Comparaison avec nos autres études

Les mêmes contrôles dans nos études des communes, des collectivités, de l'enseignement supérieur et des domaines .fr (dernières éditions) : part des domaines notés qui réussissent chacun. Les communes et les collectivités comptent dix contrôles, les autres neuf.

	Communes	Collectivités	Enseignement supérieur	Domaines .fr	État
Note moyenne	47	60	64	32	46
Certificat HTTPS valide	93,4 %	98,7 %	100 %	59,1 %	63,8 %
HTTP renvoie vers HTTPS	86,4 %	90,9 %	95,2 %	53,4 %	77,3 %
HSTS d'au moins six mois	28,3 %	38,8 %	46,1 %	17,3 %	33,3 %
En-têtes de protection de base	26,1 %	40,7 %	57,5 %	14,1 %	51,9 %
DNSSEC	22,1 %	25,9 %	12,7 %	25,9 %	3,8 %
Enregistrement CAA	2,8 %	2,6 %	41 %	1,2 %	18,5 %
SPF strict	85,9 %	97,1 %	93 %	71,6 %	56,2 %
Enregistrement DMARC	45,2 %	77,8 %	86,9 %	38,6 %	56,7 %
DMARC appliqué	19,2 %	32,8 %	45,4 %	11,7 %	43,3 %

09

Les domaines qui font bien

3 domaines réussissent les neuf contrôles et n'ont aucun problème grave.

Domaine	Catégorie
douane.gouv.fr	Autres domaines du Gouvernement (liste de la DINUM)
info.gouv.fr	Autres domaines du Gouvernement (liste de la DINUM)
secnumacademie.gouv.fr	Autres domaines du Gouvernement (liste de la DINUM)

10

Problèmes graves

78 domaines ont un problème grave qui pourrait être utilisé contre eux. Ils ne sont nommés ni dans ce rapport ni ailleurs : ils ont été signalés au CERT-FR de l'ANSSI avant la publication.



11

Recommandations

1 **Appliquer DMARC sur chaque domaine, y compris ceux sans site**
Un domaine qui ne fait que renvoyer ailleurs ou n'envoie que du courrier peut servir à falsifier des e-mails au nom de l'État. Chaque domaine qui n'envoie pas de courrier devrait publier un SPF qui n'autorise rien et une politique DMARC reject.

2 **Activer HSTS**
La plupart des sites renvoient déjà vers HTTPS ; HSTS le fait retenir aux navigateurs, pour que la première requête ne puisse pas être détournée.

3 **Signer les domaines avec DNSSEC**
Moins de 4 % des domaines notés de l'État sont signés. Le registre du .gouv.fr et la plupart des bureaux d'enregistrement le permettent.

4 **Retirer les domaines qui ne servent plus**
Des centaines de domaines inscrits n'ont ni site ni messagerie. Gardés, ils devraient au moins publier une politique qui refuse le courrier ; abandonnés, ils sortent des listes.

5 **Surveiller dans la durée**
Les certificats expirent, les prestataires changent, des enregistrements se perdent lors d'une migration. Un contrôle régulier le voit avant les usagers.

12

Méthodologie

Des contrôles passifs uniquement

Nous lisons ce que n'importe quel visiteur ou serveur de messagerie peut voir : les enregistrements DNS publics, l'enregistrement du domaine (RDAP), le certificat TLS, une requête sur la page d'accueil en HTTP (sa redirection est lue, pas suivie), et la page d'accueil en HTTPS (en suivant ses redirections, comme un navigateur). Rien d'autre n'est demandé au site. Quand un domaine publie une politique MTA-STS, son fichier de politique est lu aussi, comme le font les serveurs de messagerie.

Pas de balayage de ports, pas de recherche de sous-domaines, pas de tentative de connexion, pas de formulaire, pas de test de vulnérabilité. Le robot est lent exprès et répartit ses requêtes sur plusieurs heures.

Le robot

Il se présente comme PerimetryResearch/1.0 (+https://perimetry.cloud/research/methodology/). Si vous gérez un site qu'il a visité et préférez qu'il ne le fasse plus, écrivez à hello@perimetry.cloud : nous retirerons le domaine des prochaines éditions.

L'étude des domaines de l'État français

Population étudiée : les domaines de l'État de deux listes ouvertes, toutes deux sous Licence Ouverte 2.0. La première est la liste des noms de domaine des organismes publics de la DINUM (gitlab.adullact.net), ses types de l'État seulement : Gouvernement, Préfecture, Ministère, Académie, Ambassade et Santé (communes, collectivités, universités et hôpitaux ont leurs propres études). La seconde est la liste des sites de l'Observatoire de l'écosystème numérique de l'État publiée par le Service d'information du Gouvernement (data.gouv.fr, fichier « audience-liste-sites »), sans les sites qu'elle indique comme parqués. Chaque adresse est ramenée à son domaine enregistrable (interieur.gouv.fr est un domaine) ; un domaine présent dans plusieurs groupes compte une fois, dans le premier de : préfectures, académies, ambassades, ministères, santé, autres domaines du Gouvernement, autres sites de l'Observatoire. L'édition de novembre 2026 compte 1 440 domaines.

Un domaine est inactif, compté et écarté, quand il n'existe pas dans le DNS ou n'a ni site en service ni serveur de messagerie : beaucoup sont d'anciens domaines de campagnes ou d'organismes disparus, toujours inscrits.

Les notes, les catégories et les types de site sont ceux des domaines qui ont un site à eux. Les domaines actifs qui n'en ont pas (un site qui renvoie vers un autre domaine, ou un domaine qui ne sert qu'à la messagerie) ne peuvent être jugés que sur leur DNS et leur messagerie : ils sont présentés à part, pour ce qu'ils sont, des domaines au nom desquels on peut falsifier des e-mails tant que DMARC n'est pas appliqué. La plupart des domaines d'ambassade (ambafrance-xx.org) renvoient vers un site sur un autre domaine : ils sont comptés parmi eux, et les ambassades ont donc trop peu de domaines notés pour être détaillées.

Les contrôles, la note et les lettres de l'étude des communes, sans le contrôle de l'adresse de contact, que

les listes ne donnent pas : neuf contrôles, comme dans les études de l'enseignement supérieur et des domaines .fr. Un domaine doit avoir trois contrôles applicables pour être noté ; un groupe n'est pas détaillé en dessous de dix domaines notés.

Le tableau d'honneur nomme les domaines qui réussissent les neuf contrôles et n'ont aucun problème grave ; aucun autre domaine n'est nommé. Les problèmes graves (un certificat expiré, des réponses DNS en échec, un domaine inscrit que n'importe qui pourrait enregistrer…) ont été signalés au CERT-FR de l'ANSSI avant la publication ; l'étude n'en donne que le nombre.

Uniquement les bons élèves

Nous nommons les communes qui font bien (le tableau d'honneur et les meilleures de chaque tranche de population), jamais celles qui font mal, et jamais une commune qui a un problème grave, quelle que soit sa note. Tout le reste est publié en moyennes : par taille de commune et par département, où un département de moins de dix communes notées n'est pas détaillé, pour qu'aucune d'elles ne puisse être reconnue.

Les plateformes de sites sont notées sur un échantillon de cinq sites de communes au plus : un contrôle compte comme réussi quand la majorité de l'échantillon le réussit.

Les problèmes graves sont signalés en privé

Certains constats pourraient servir tout de suite contre une commune : un domaine inscrit dans l'annuaire officiel qui n'existe plus (n'importe qui pourrait l'enregistrer), un domaine que le registre est en train de supprimer, un certificat expiré, un enregistrement SPF qui permet à n'importe qui d'envoyer du courrier en son nom. Ils ne sont jamais publiés. Nous prévenons d'abord la commune, discrètement, et nous les comptons dans l'étude sans nommer personne.

Limites

Chaque édition est une photographie prise en quelques heures. L'annuaire peut être en retard ou erroné ; nous l'utilisons tel qu'il est publié. Les clés DKIM ne sont cherchées que sur les sélecteurs courants : elles ne sont donc pas notées. Un site derrière un service de protection peut répondre à un robot autrement qu'à un visiteur. Les serveurs de messagerie ne sont pas testés (STARTTLS demande le port 25, que l'infrastructure de l'étude ne peut pas joindre).

13

À propos de Perimetry

Perimetry est un outil libre qui audite l'extérieur d'un domaine comme n'importe qui sur Internet le voit : authentification des e-mails, DNS, certificats, serveurs de messagerie, sites. Perimetry Cloud en est la version hébergée, avec surveillance continue, alertes et rapports, pour les organisations et les agences qui s'en occupent.

Citer : Perimetry Research, Baromètre de la sécurité des domaines de l'État, novembre 2026. https://perimetry.cloud/fr/research/french-state/

Vous pouvez réutiliser les chiffres de ce rapport avec un lien vers l'étude. La liste de la DINUM et celle de l'Observatoire restent sous Licence Ouverte 2.0.

Contact : hello@perimetry.cloud

https://perimetry.cloud/fr/research/french-state/