

Switch

Rapport d'activité 2023

du registry .ch

Table des matières

Éditorial	4	Indicateurs statistiques	33
<hr/>		Nombre de noms de domaine	
Fonctionnement	5	Service de renseignements	
Lutte contre la cybercriminalité		Part de marché de .ch et .li	
Mesures en cas de suspicion d'abus		Programme de résilience DNS	
Security Awareness		Développement DNSSEC	
Événements de la communauté		Validation DNSSEC en Suisse	
Événement LEO		Délégation différée	
Domain pulse 2023		Cas de règlement des différends	
Programme de résilience DNS		Évolution registrars	
Sites DNS Anycast et génération de la zone		Performance des serveurs de noms	
Recertification ISMS		Cybercriminalité	
<hr/>		DNS Health Report	
Nouveautés	22	DAAR – Domain Abuse Activity Reporting	
Domain Abuse 4.0		<hr/>	
Création du European TLD ISAC		Indicateurs économiques	51
Web Crawler		Indicateurs économiques 2023	
Nouvelle loi sur la protection des données		<hr/>	
Quad9: le rôle de la threat intelligence		Développements	53
Principales menaces pour le Web suisse		Rétrospective 2023	
Nouveau site à Lausanne		Perspectives stratégiques et objectifs	
IPv6 Evangelist		Nouveautés prévues en 2024	
Enquête clients auprès des registrars		Prévisions de croissance des noms de domaine .ch	
<hr/>		<hr/>	



*Nous mettons tout
en œuvre pour
assurer l'avenir de notre
écosystème numérique.*

Urs Eppenberger
Head of Registry, Switch

Pleine force d'innovation dans la lutte contre la cybercriminalité

Urs Eppenberger, Head of Registry

Les efforts continus de Switch dans la lutte contre la cybercriminalité ont conduit à l'élaboration du projet «Domain Abuse 4.0». L'objectif du projet: assurer l'avenir de notre écosystème numérique. Nous devons redéfinir les fondements de notre lutte contre la cybercriminalité. Les processus seront optimisés et l'ensemble de l'infrastructure technique renouvelé. Une description du projet figure à la page 23.

Alors que les poursuites pénales en Suisse relèvent en principe de la compétence des autorités en la matière, Switch occupe une position particulière. Switch exploite sa propre CERT (Computer Emergency Response Team) et propose des services de sécurité modernes aux hautes écoles et aux entreprises suisses. Grâce à la collaboration avec d'autres CERT et à l'étroite coopération avec les autorités de poursuite pénale, Switch devient une instance agile et opérationnelle, capable de gérer de manière autonome, très efficace et efficiente le flot de cas de malware et de phishing. L'OFCOM s'en est rendu compte très tôt, a créé les bases légales nécessaires et inscrit le mandat correspondant dans le contrat avec Switch.

La lutte contre la cybercriminalité chez Switch s'apparente à une machinerie très complexe. Des spécialistes de différents domaines spécialisés collaborent, tissent des réseaux avec d'autres acteurs dans ce domaine, et relie différents composants informatiques entre eux.

La vie n'a jamais été aussi simple pour les utilisatrices et utilisateurs suisses: ils réservent leur nom de domaine auprès d'un registrar et exploitent leur site auprès d'un fournisseur d'hébergement. Ils bénéficient de ces prestations à des prix attrayants. Toutefois, on ignore dans une large mesure quels efforts doivent être déployés en arrière-plan pour assurer le fonctionnement sûr et stable d'Internet dans son ensemble et de chaque nom de domaine individuel. Cela nécessite une collaboration bien rodée et bien établie entre les hébergeurs, les registrars, Switch et les autorités de poursuite pénale.

Les personnes qui travaillent dans le domaine de la lutte contre la cybercriminalité sont conscientes de l'importance et de la nécessité de ce travail. C'est pourquoi, chez Switch, nous avons décidé de redoubler d'efforts. L'enregistrement et la gestion des noms de domaine, qui constituent le cœur de métier du registry, sont organisés de manière si efficace qu'il est possible de concentrer toute la force d'innovation sur la lutte contre la cybercriminalité. Une sécurité et une stabilité maximales continuent ainsi d'être garanties pour tous les utilisateurs et utilisatrices d'Internet.

1.

Rapport d'activité – fonctionnement

Lutte contre la cybercriminalité

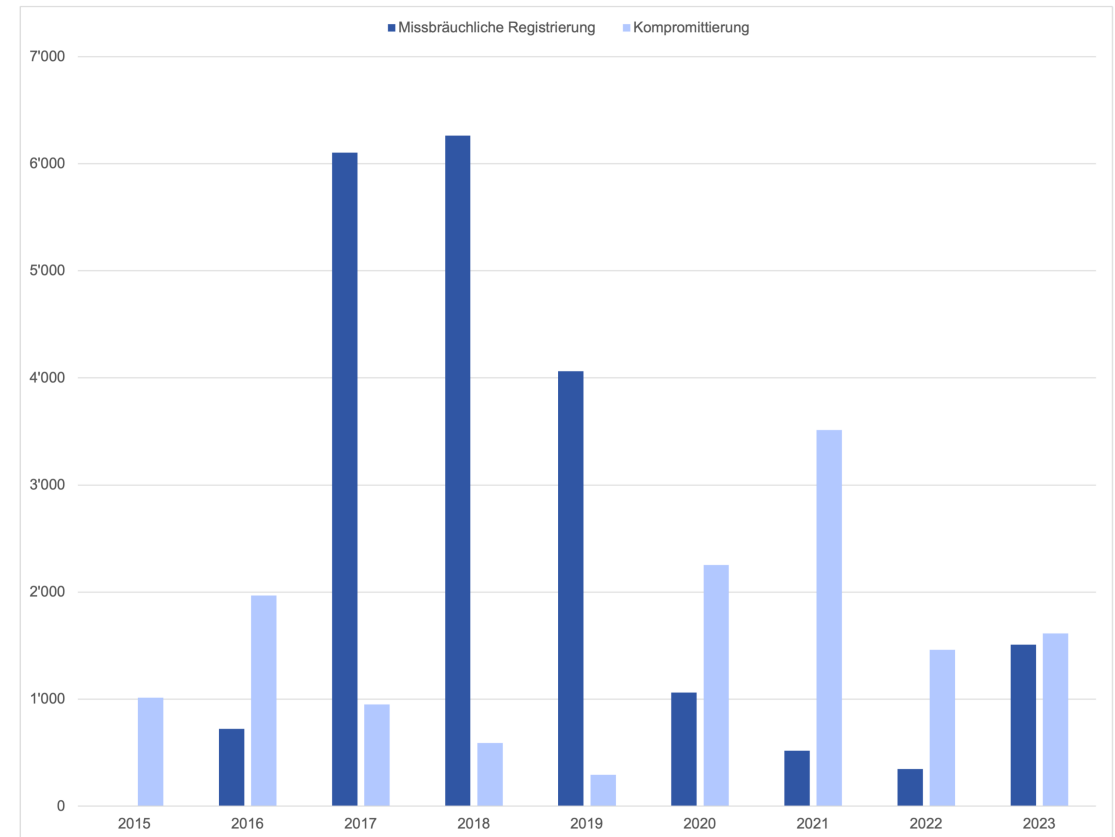
Pages Web compromises

Le nombre de pages Web compromises qui ont été utilisées à des fins de phishing et de malware est resté à peu près constant par rapport à l'année précédente.

Enregistrements abusifs

Le nombre de noms de domaine pour lesquels un enregistrement abusif a été signalé a augmenté. Une des raisons réside dans le fait que Fedpol a envoyé davantage de demandes via son projet «SWITCHoff» conformément à l'art. 15.

Page Web: <https://saferinternet.ch>



Mesures en cas de suspicion d'abus

Demandes de la part d'autorités reconnues – art. 15.1 ODI

En 2023, les autorités accréditées ont envoyé au total 426 demandes de blocage immédiat (technique/administratif) de noms de domaine concernés par des cas de phishing ou de malwares en vertu de l'art. 15.1 de l'ODI.

Demandes	Conséquence	2023
Sans réponse	Nom de domaine supprimé	410
Avec réponse	Nom de domaine réactivé	16
Total		426

Toutes les autorités reconnues par l'OFCOM sont répertoriées sur la page Web suivante: [Autorités reconnues](#)

Assistance administrative – art. 16.3 ODI

À la demande d'une administration intervenant dans le cadre de sa compétence, 1084 demandes pour une adresse de correspondance en Suisse conformément l'art. 16.3 ODI ont été envoyées.

Demandes	Conséquence	2023
Sans réponse	Nom de domaine supprimé	964
Avec réponse	Nom de domaine réactivé	120
Total		1084

Security Awareness – iBarry et SISA

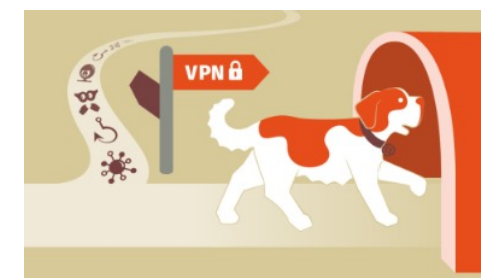
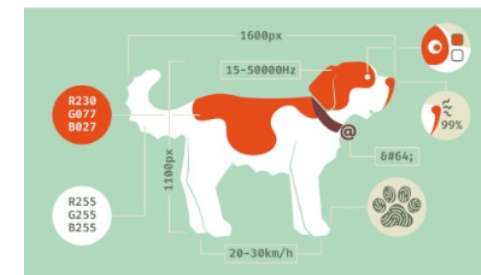
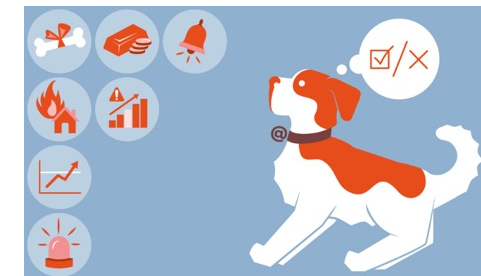
En collaboration avec SISA, Switch soutient la sensibilisation de la population suisse. Avec trois nouvelles campagnes d'information (fake news, protection des données, VPN), iBarry.ch contribue à diffuser des informations tout en offrant une orientation et un soutien en cas de doutes et de questions en lien avec le thème de la sécurité sur Internet.

<https://checkawebsite.ibarry.ch>

<https://ibarry.ch>

Afin d'optimiser l'offre pour la population suisse et de mieux positionner la plateforme iBarry, SISA a de nouveau participé à l'enquête auprès des internautes suisses de cette année.

<https://internet-sicherheit.ch>



Security Awareness Day

Le 26 octobre 2023, Switch a organisé pour la sixième fois le Swiss Security Awareness Day. Cette année, la conférence, qui ne cesse de se développer, a été organisée avec iBarry comme partenaire. Entre les conférences passionnantes, les quelque 120 participantes et participants ont pu rencontrer d'autres experts et échanger avec eux lors de diverses pauses de réseautage.

Cette année encore, le programme visait à renforcer la compréhension du thème de la Security Awareness au sein de la communauté Switch et au-delà, tout en véhiculant de nouvelles idées et en favorisant les échanges.

Toutes les conférences sont disponibles en ligne:

<https://swit.ch/ssad2023-recordings>



Security Awareness Adventures

Les Switch Security Awareness Adventures

«Hack The Hacker – l'Escape Room» était la première des trois Security Awareness Adventures de Switch, suivie de «Track The Hacker – la chasse au trésor» et de «Piece of Cake – le jeu de rôle». Ces aventures jouissent toujours d'une grande popularité: en 2023, Switch a organisé en tout 40 fois ces formations ludiques à la sécurité et aidé trois organisations à mettre en place leurs propres formations.

12 collaborateurs de l'OFCOM ont également réussi à pirater le pirate.

Page Web: <https://swit.ch/security-awareness-adventures>



Security Awareness – podcast

Podcast: Security Awareness Insider

En décembre 2023, le 38^e épisode du podcast «Security Awareness Insider» (en allemand) a été publié.

Katja Dörlemann (Switch) et Marcus Beyer (Swisscom) parlent de la sensibilisation des collaboratrices et des collaborateurs aux questions de sécurité ainsi que des moyens, outils et approches de formation nouveaux et créatifs. Ils donnent aussi un aperçu des programmes de Security Awareness des entreprises et des organisations, et bien plus encore.

Depuis son lancement, le podcast a déjà été téléchargé 17 000 fois, et chaque épisode enregistre désormais en moyenne 400 téléchargements.

Disponible sur Spotify ou ici:

<https://www.securityawarenessinsider.ch>



Communauté – Swiss Web Security Day

Le 17 octobre 2023, Switch a organisé le Swiss Web Security Day à Berne en collaboration avec SISA et Swico, parallèlement à l'événement LEO avec les autorités de poursuite pénale suisses. Avec 73 participantes et participants venus de Suisse et d'ailleurs, l'événement a remporté un franc succès et a reçu un écho très positif de la part des participantes et participants.

Le matin, des exposés ont été présentés sur les directives pour une communication sécurisée par e-mail, Mediacrime, la gestion des vulnérabilités en Suisse, les menaces pour les internautes suisses ainsi que sur une mise à jour de la révision de l'Ordonnance sur les domaines Internet (ODI). L'après-midi a été consacré à des ateliers et discussions en petits groupes, suivis d'un apéritif.

Cette fois-ci, l'événement ne s'est plus déroulé dans un format hybride, mais sur place, à Berne.

Page Web: <https://swsd2023.events.switch.ch>

Le Swiss Web Security Day sera de nouveau organisé en 2024: le 29 octobre 2024, à Welle 7, Berne.



Communauté – cours ModSecurity

ModSecurity est un pare-feu open source d'application Web très populaire et puissant. Les pare-feu d'applications Web sont eux aussi un élément important de la protection d'une application Web et sont donc intéressants pour les hébergeurs, les registrars, mais aussi, de manière générale, pour tout exploitant d'une application Web.

Afin d'offrir ici une valeur ajoutée à notre communauté, Switch a organisé un cours d'initiation sur son site à Zurich les 15 et 16 mars 2023, en collaboration avec Christian Folini de Netnea, expert mondialement renommé de ModSecurity. Switch a utilisé ses bonnes relations avec la communauté pour attirer l'attention sur le cours, a mis à disposition les locaux et sponsorisé des billets à prix réduit pour ses clients et les registrars.

Finalement, un mélange varié de registrars, d'hébergeurs et de collaboratrices et collaborateurs de hautes écoles ont participé au cours à Zurich.

Une nouvelle édition est prévue en 2024.



Événement LEO

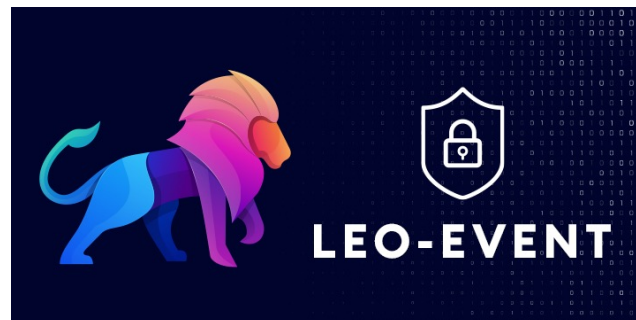
Collaboration avec les autorités de poursuite pénale

Groupe-cible

En vue d'intensifier la collaboration avec les autorités, Switch a organisé cette année l'événement LEO pour la troisième fois. LEO signifie «Law Enforcement Organizations».

Le 17 octobre 2023, la Law Enforcement Community s'est réunie à Berne. 63 personnes ont pris part à l'événement LEO. Nombre d'entre elles étaient déjà présentes l'année dernière et sont venues accompagnées de leurs collègues intéressés. On constate chaque année une augmentation.

La répartition entre les régions était très équilibrée et les conférences se sont tenues dans les langues nationales et en anglais. Les participantes et participants provenaient des polices cantonales, des ministères publics cantonaux ainsi que de la police nationale du Liechtenstein. Des autorités telles que Swissmedic, le SECO et l'OFCOM étaient également représentées.



Thèmes

Différents thèmes ont été abordés. La collaboration mise en place au sein de la communauté pour prévenir la cybercriminalité a occupé une place importante dans les débats. Différents cas ont ainsi été présentés et pu être résolus avec succès et efficacité grâce à la collaboration des partenaires de la communauté.

Une étude de cas finlandaise a été présentée à titre d'inspiration sur la manière dont les cas peuvent être résolus, même s'ils semblent très difficiles au début. Les «Lessons Learned» concernant les demandes ODI adressées à Switch et leurs éventuels pièges ont fait l'objet de discussions. Les participantes et participants de l'OFCOM se sont penchés sur les questions de la communauté.

Résonance

L'événement a rencontré un franc succès. Les participantes et participants ont parlé des développements et des projets actuels concernant les abus de noms de domaine et la cybercriminalité. Les processus et interface visant à simplifier la collaboration ont également fait l'objet de discussions. Les échanges dans le cadre de la collaboration ont nettement augmenté. Les participantes et participants souhaitent une autre manifestation en 2024.

Domain pulse 2023

Cette année, Domain pulse a réuni les 6 et 7 février 2023 des professionnels de la branche venant principalement de Suisse, d'Allemagne et d'Autriche pour discuter de la sécurité et de la stabilité d'Internet.

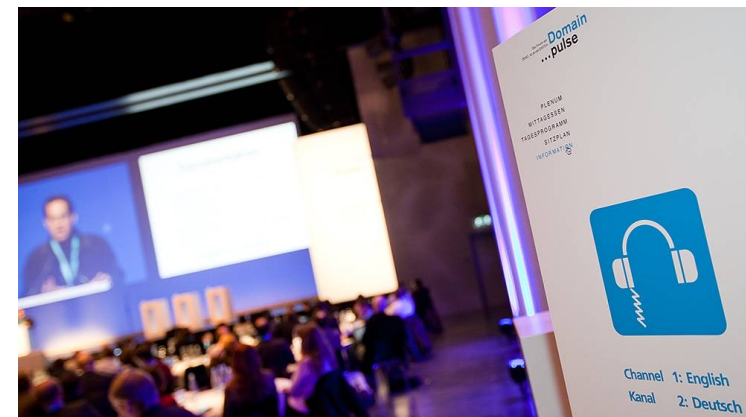
Quelque 250 participantes et participants, issus de services d'enregistrement, de registrars, d'hébergeurs, d'offices fédéraux, ainsi que d'autres experts, ont répondu à l'invitation à Winterthour.

Le titre de l'événement, «Infrastructure Internet critique: préserver la souveraineté et prévenir les abus», les a conviés à discuter des défis actuels du secteur de l'Internet.

La question centrale était de savoir comment, en période de conflits internationaux, le monde politique et les organisations d'exploitants d'infrastructures critiques préservent leur souveraineté sur Internet, se protègent contre les attaques et rendent le réseau plus résistant aux pannes.

La salle de conférence baroque a été un régal pour les yeux de nombreux participants et participantes et les longues pauses consacrées au réseautage ont été très appréciées.

Nous nous réjouissons d'accueillir à nouveau l'événement Domain pulse en 2026.



Programme de résilience DNS

50%

Au 1^{er} janvier 2024, près de 50% de tous les noms de domaine .ch étaient déjà signés.

Programme de résilience DNS

Résistance pour les noms de domaine .ch

Le programme de résilience DNS encourage l'adoption et l'utilisation de normes de sécurité ouvertes pour les noms de domaine .ch et .li. L'utilisation de telles normes est essentielle pour la résistance (résilience) aux cybermenaces. Ce programme repose sur un système d'incitations financières et s'étend de 2022 à 2026.

L'objectif principal est d'encourager la signature des noms de domaine avec DNSSEC. Pendant toute la durée du programme, les registrars se verront facturer un supplément pour les noms de domaine non signés ou signés de manière incorrecte.

Le «DNSSEC Advisory Board» définit les normes à promouvoir. Y siègent des représentants de l'OFCOM, des registrars et de Switch.

Pour 2024, les technologies de sécurité des e-mails DMARC et SPF seront intégrées au programme. L'implémentation de DMARC et de SPF sera alors déterminante pour le remboursement des recettes supplémentaires, et pas seulement DNSSEC.

L'Advisory Board a déjà décidé qu'en 2025, DANE et en 2026, IPv6 seraient encouragés en plus de DNSSEC. Les registrars disposent ainsi de suffisamment de temps pour suivre les formations continues proposées par Switch et planifier les mesures techniques.

Mesures de contrôle de la qualité

Comme c'est déjà le cas pour DNSSEC, le prestataire de services de mesure externe OpenIntel est également impliqué dans la mesure des autres technologies de sécurité. Il vérifie si tous les noms de domaine .ch et .li avec serveurs de noms répondent aux critères définis par Switch pour le programme et en informe Switch quotidiennement. En cas de configurations erronées, nous envoyons des rapports d'erreurs aux registrars.

Programme de résilience DNS

Également au cours de sa deuxième année d'exploitation, nous n'avons cessé de nous occuper du développement du programme de résilience, en plus de l'exploitation.

Évolutions 2023

- Remboursements pour 2022 aux registrars autorisés sous forme de notes de crédit (fin janvier 2023).
- Implémentation des mesures de DMARC et SPF qui seront pertinentes en 2024.
- Envoi des nouveaux rapports d'erreurs pour DMARC/SPF aux registrars à partir de septembre 2023. Bien que le critère ne soit déterminant qu'en 2024, les registrars auront ainsi la possibilité de s'y préparer.
- Extension du Dashboard pour DMARC/SPF chez le prestataire de mesure externe [OpenIntel](#) (voir capture d'écran à droite).
- Information continue des registrars, réponse à leurs demandes, assistance.

- Deux nouveaux rapports qui permettent au registrar intéressé de comprendre l'évaluation de ses noms de domaine.
- Formations sur DNSSEC et DANE à Zurich et Lausanne en octobre 2023.

SWITCH DNS Resilience Dashboard

Dashboard | Statistics | About

saferinternet.ch on 2023-12-31

Previous Date | Next Date

DNSSEC Status

Well done!

This domain name fulfills the technical DNSSEC requirements of the DNS resilience programme. No action required.

Evaluation Report

Measurement data available	✓
Compliant algorithm	✓

DMARC/SPF Status

Well done!

This domain name fulfills the technical DMARC/SPF requirements of the DNS resilience programme. No action required.

DMARC Evaluation Report

Measurement data available	✓
DMARC record present	✓

Sites DNS Anycast et génération de la zone

Sites Anycast

En 2023, nos partenaires d'hébergement DNS Anycast ont ajouté plusieurs sites en Suisse et à l'étranger sur lesquels la zone DNS est mise à disposition via Anycast. Il existe par exemple un point de présence à Genève depuis janvier 2023.

Génération de la zone

L'infrastructure de génération et de distribution de la zone a été entièrement rénovée en 2023. Les «Hidden Primary Server», qui créent la zone et génèrent les signatures DNSSEC, ont été équipés d'un nouveau matériel.

En raison de la proportion désormais élevée de noms de domaine signés DNSSEC et des nouvelles exigences liées à la publication de la zone .CH en 2020, la méthode de création des signatures DNSSEC pour les noms qui n'existent pas a également été modifiée:

Jusqu'à présent: «NSEC3 avec opt-out»

Désormais: «NSEC»



Recertification ISMS

La recertification du système de gestion de la sécurité de l'information ISMS s'est déroulée du 5 au 7 septembre 2023 selon la norme ISO 27001:2013.

Pendant trois jours, l'auditeur a pu se faire une idée de tous les aspects de l'ISMS chez Switch, conformément aux prescriptions pour une recertification. Switch a réussi l'audit sans divergences ni constatations.

L'auditeur a formulé sept recommandations sur la manière dont Switch peut améliorer concrètement l'ISMS. Ces recommandations sont prises en compte dans le processus continu d'amélioration PCA de l'ISMS.

Le rapport de l'auditeur fait état de l'impression générale positive et conclut par la remarque suivante: «La direction fait preuve d'un grand engagement et tous les collaborateurs et collaboratrices interrogés d'une grande compréhension de la sécurité de l'information. L'un des points forts de Switch est l'amélioration continue et les connaissances spécialisées élevées des collaboratrices et collaborateurs à tous les niveaux.»

ZERTIFIKAT

Nr. 860-ISMS-23

Hiermit wird bestätigt, dass das Managementsystem der

SWITCH

Werdstrasse 2 - 8021 - Zürich (Zürich, Switzerland)

Geschäftsstellen:

Werdstrasse 2 - 8021 - Zürich (Zürich, Switzerland)

die Anforderungen der Norm für das Information Security Management Systems

ISO/IEC 27001:2013

für folgenden anwendungsbereich erfüllt:

Domain Namen Registrierung

SOA Ausführung	Erstausgabedatum	Datum der Änderung	Ablaufdatum des Zertifikats
Version 1.4 vom 14.10.2021	05/12/2017	09/10/2023	05/12/2026



Für die Zertifizierungsstelle
SV Certification Sro



(Gaetano Spera CEO SV CERT.)

Die Gültigkeit des Zertifikats unterliegt einer regelmäßigen jährlichen Überwachung und einer vollständigen Überprüfung des Systems alle drei Jahre. Die Verwendung und Gültigkeit dieses Zertifikats unterliegen der Einhaltung der Zertifizierungsbestimmungen der SV Certification Sro.

«L'un des points forts de Switch est l'amélioration continue et les connaissances spécialisées élevées des collaboratrices et collaborateurs à tous les niveaux.»

Rapport d'audit ISO 27001

2.

Rapport d'activité – nouveautés

Domain Abuse 4.0

Exigences croissantes

Grâce à une équipe d'experts performante et au soutien de solutions logicielles qu'elle a développées, Switch lutte depuis des années contre l'utilisation abusive des noms de domaine en Suisse. Les cybercriminels sont de plus en plus rusés, ce qui accroît les exigences adressées aux experts et aux solutions logicielles.

Défi de la solution logicielle actuelle

La base de code de la solution logicielle actuelle de lutte contre la cybercriminalité remonte à 2008. La solution repose sur une architecture informatique obsolète. Elle est lente, coûteuse en maintenance et n'est plus à la hauteur des défis croissants de la lutte contre l'utilisation abusive des noms de domaine.

Lutte moderne et prometteuse contre les abus

Une nouvelle solution logicielle tournée vers l'avenir est développée dans le cadre du projet «Domain Abuse 4.0». Elle repose sur les technologies les plus modernes et la toute dernière infrastructure de Switch, «Switch Cloud». L'équipe de développement du registry et l'équipe de développement du CERT mettent en commun leur expérience et leurs compétences pour développer une solution rapide, nécessitant peu de maintenance et évolutive. Les processus sont également révisés, adaptés aux nouvelles réalités et nos experts sont formés à cet effet. Grâce à ces mesures, Switch conserve un rôle de premier plan mondial dans la lutte contre la cybercriminalité.

Domain Abuse 4.0

Faits et chiffres

- 20 workflows (processus contre les abus) ont été définis à l'aide de l'ODI.
- 14 composants logiciels doivent être créés ou perfectionnés.
- Plus de 50 cas d'utilisateurs ont été rédigés (liste non exhaustive).
- 16 variantes de solution ont été évaluées.
- Jusqu'à présent, 12 personnes occupant différents postes ont travaillé sur le projet.

2022



Début

Le projet a débuté en octobre 2022 par la définition des workflows et de l'architecture informatique.

2023



Évaluation

Parmi les 16 variantes de solution, un développement interne a été sélectionné comme solution porteuse d'avenir.

2024



Évolution

La solution logicielle est développée de manière itérative avec des mises à jour régulières.

2025



Exploitation

La nouvelle solution devrait être implémentée d'ici fin 2025.

Création du European TLD ISAC

Le European TLD Information Sharing and Analysis Center (ISAC) a été créé sous l'égide de CENTR en 2023.

Le Centre européen d'échange et d'analyse d'informations sur les domaines de premier niveau (European Top Level Domain Information Sharing and Analysis Center, TLD ISAC) vise à renforcer la sécurité et la résilience des registrars de domaines de premier niveau en Europe par l'échange d'informations, la coopération et le partage des meilleures pratiques.

Il réunit les exploitants, les professionnels de la sécurité et d'autres parties prenantes afin d'échanger des informations sur les menaces, d'identifier les nouvelles tendances et de développer des mesures proactives pour prévenir et contrer les cyberattaques.

Switch est, avec d'autres exploitants de ccTLD européens, membre fondateur et membre actif du comité de pilotage, du groupe de travail et du groupe de Threat Intelligence Sharing.

La première conférence ISAC TLD a eu lieu le 13 novembre 2023 à Bruxelles, Switch y était représentée par deux participants.

Page Web: <https://www.tld-isac.eu>



Web Crawler

Dans le cadre de la lutte contre la cybercriminalité, un nouvel outil a été développé chez Switch vers la fin de l'année 2023: un robot d'indexation (web crawler) qui analyse systématiquement les ressources accessibles au public dans les zones .ch et .li afin de détecter à temps les noms de domaine compromis ou malveillants et d'éliminer ainsi tout danger pour les internautes.

Afin que nous soyons toujours à jour et que nous puissions travailler efficacement, notre équipe Cyber Threat Intelligence met régulièrement à jour les critères qui nous aident à identifier les dangers. Nous échangeons également activement avec les autorités et d'autres registries.

Si notre web crawler détecte des noms de domaine qui font du phishing ou diffusent des malwares, nous pouvons bloquer le nom de domaine après en avoir informé le détenteur et avoir respecté un délai d'attente.

Ainsi, Switch peut apporter une contribution importante à l'amélioration de la sécurité des zones .ch et .li, non seulement de manière réactive, mais aussi proactive grâce à une recherche autonome.

Nouvelle loi sur la protection des données

La nouvelle loi suisse sur la protection des données est entrée en vigueur le 1^{er} septembre 2023. Switch a commencé très tôt à mettre en œuvre les nouvelles dispositions légales.

Conseiller à la protection des données

Switch a nommé un nouveau conseiller à la protection des données le 1^{er} mars 2023 et en a informé le préposé fédéral à la protection des données et à la transparence (PFPDT). Angelo Marchetta exerce cette fonction pour Switch. Il conseille et soutient Switch dans l'application des dispositions relatives à la protection des données et dans la formation des collaboratrices et collaborateurs. Ses tâches comprennent également la surveillance et la coordination de toutes les activités pertinentes en matière de protection des données au sein de l'entreprise. De plus, il est chargé du développement d'un système de gestion de la protection des données (SGPD).

Registres de traitement

L'introduction de la disposition relative à la tenue d'un registre des activités de traitement a remplacé l'ancienne obligation de déclaration des collectes de données. Switch a enregistré ses activités de traitement des données en tant que registry, d'une part, dans le registre interne des activités de traitement et, d'autre part, dans le registre public DataReg.

Sécurité des données

Dans le cadre de la nouvelle loi sur la protection des données, Switch a mis en œuvre des modifications dans le processus de signalement des violations de la sécurité des données. Cela permet de signaler rapidement les incidents susceptibles de présenter un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

SGPD

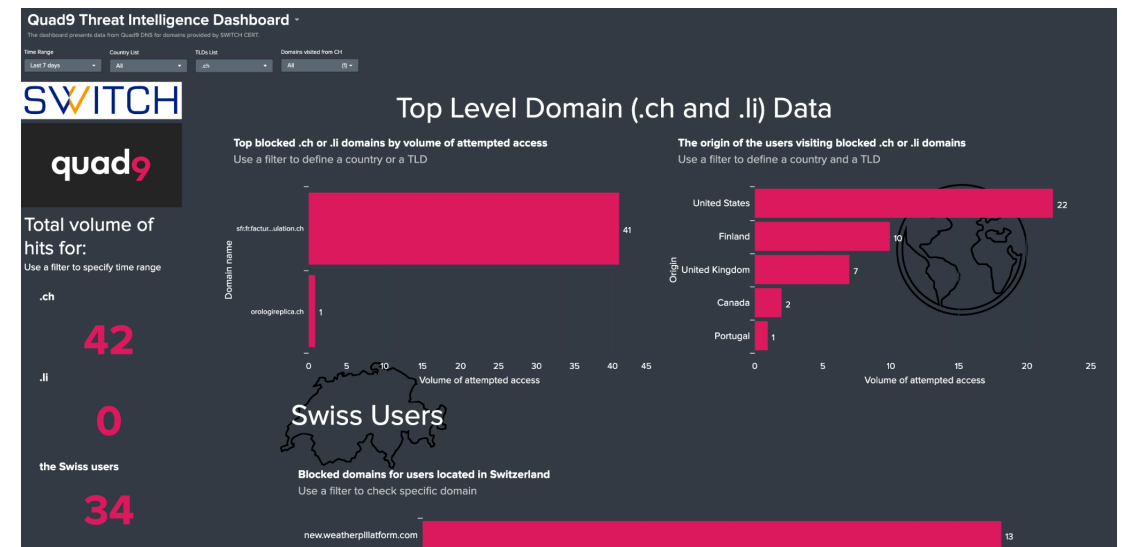
Switch attache une grande importance à la protection des données personnelles, et pas seulement depuis la mise en œuvre de la nouvelle loi sur la protection des données. En plus du système de gestion de la sécurité de l'information ISMS, Switch développera au cours des prochaines années un système de gestion de la protection des données afin d'offrir une garantie systématique et l'amélioration continue de la protection des données.

Quad9: le rôle de la threat intelligence

Quad9 et Switch collaborent pour analyser les menaces qui pèsent sur l'Internet suisse. Cela comprend, entre autres:

- Développement et mise en œuvre d'une stratégie de threat intelligence pour Quad9 et pour Domain Abuse chez Switch.
- Analyses des principales menaces mensuelles bloquées par Quad9 dans le monde entier et rédaction de rapports réguliers transmis à la communauté de sécurité concernée et aux organisations gouvernementales locales de cybersécurité. Exemples de rapports: [Q9 Cyber Insights Report](#), [Malawi Report](#)
- Acquisition de nouveaux partenariats de threat intelligence pour Quad9. Exemples: Rapport Phish, [SISA](#)
- Exposés sur des thèmes liés aux données sur les menaces, à Quad9 et à la protection des données. Exposés: [Swiss Web Security Day](#), M3AAWG, [Women in Cyber](#)

- La création d'un «Quad9 Threat Intelligence Product pour Switch CERT». L'objectif de ce projet était de développer une solution pour Switch CERT afin de collecter, d'agréger et d'analyser les données de menace du DNS Quad9. Les résultats ont été utilisés pour le Switch Threat Radar et présentés lors du Swiss Web Security Day.



Principales menaces pour le Web suisse

Sur la base des données collectées par Quad9, les campagnes suivantes ont été lancées en 2023 et représentaient un danger pour les internautes suisses:

Fake jQuery Domain

L'infection est injectée dans des fichiers Javascript légitimes et exécute un script du domaine malveillant jqueryns[.]com. Celle-ci redirige vers divers sites de fraude. Ce sont ici surtout les pages Web WordPress vulnérables qui ont été touchées. Plus de 8000 demandes DNS ont été bloquées par Quad9 en Suisse et 47 noms de domaine .ch ont été concernés.

WordPress SocGholish Injections

SocGholish est une campagne malveillante de plusieurs années, largement diffusée, qui vise à distribuer de fausses mises à jour de navigateurs, y compris aux internautes suisses. Une fois installées, les fausses mises à jour du navigateur infectent l'ordinateur de la victime avec différents types de logiciels malveillants, y compris des chevaux de Troie d'accès à distance (RAT). En un mois, Quad9 a bloqué environ 1700 requêtes DNS depuis la Suisse.

Phishing contre la Poste Suisse

La page de phishing contre la Poste Suisse était hébergée sur campaign-image[.]eu. La campagne a été active du 20 au 26 avril. En Suisse, plus de 870 requêtes ont été bloquées par Quad9 en une semaine au mois d'avril. Plus de 24 900 requêtes ont été bloquées par Quad9 dans le monde.

Malware «ndsw/ndsx»

Il s'agit d'une autre variante du malware SocGholish. Toutes les variantes de malwares contiennent l'instruction «if(ndsw===undefined)», d'où le nom. L'objectif est d'installer les malwares «Fake Update» sur des ordinateurs Windows. 92 noms de domaine .ch ont été concernés.

Black Hat Ad Network et Balada Injector

Il s'agit d'une campagne massive qui utilise les pages Web WordPress piratées comme plateforme d'inventaire pour le placement d'annonces et les redirections. Les pages Web infectées redirigent vers de fausses mises à jour de navigateurs et vers l'assistance frauduleuse. 37 noms de domaine .ch ont été concernés.

Nouveau site à Lausanne

Le 2 mai 2023, Switch a ouvert un nouveau site en Suisse romande. Dans l’Innovation Park de l’EPFL, la fondation reprend des bureaux pouvant accueillir jusqu’à 15 collaborateurs et collaboratrices. Tom Kleiber, directeur de Switch, explique le moteur principal de cette étape: «Pour pouvoir assumer notre rôle national dans le secteur des hautes écoles de manière plus efficace et plus crédible, nous avons besoin d’un site en Suisse romande. La proximité avec la communauté et l’échange direct avec elle sont très importants pour nous.»

Dans son discours lors de la cérémonie d’ouverture, Martin Vetterli, président de l’EPFL, s’est exprimé en termes très positifs sur le nouveau site: «Les hautes écoles de Suisse romande sont impatientes de renforcer leur collaboration avec Switch.»

Le registry est ainsi plus proche des registrars spécialisés sur la Suisse romande. De plus, le nouveau site en Suisse romande offre aux talents locaux l’opportunité de s’engager dans la région pour des missions qui ont du sens, comme l’utilisation durable des données de recherche, la cybersécurité ou les identités numériques.



Martin Vetterli, EPFL; Tom Kleiber, Switch; Claudia Lienert, Switch; Alexandre Gachet, conseiller de fondation Switch

IPv6 Evangelist

Switch s'engage depuis 1996 pour l'introduction de la norme IPv6, que nous considérons comme essentielle pour le développement durable d'Internet. Outre l'implémentation dans le réseau des hautes écoles et dans le registry, nous avons également soutenu les activités de la communauté Internet suisse dans ce domaine sous la forme d'événements tels que des conférences et des cours, de travaux de normalisation au sein de l'Internet Engineering Task Force (IETF) et de conseils aux instances politiques.

Nous contribuons ainsi à faire en sorte que la Suisse est depuis de nombreuses années l'un des pays où IPv6 est bien établi et ne cesse de se répandre.

Ces efforts ont été salués en 2023 par le Forum international IPv6 lorsque Simon Leinen, collaborateur de longue date de Switch, a été admis au [IPv6 Hall of Fame](#) en tant qu'«IPv6 Evangelist». Actuellement, il n'y a qu'une centaine d'«IPv6 Evangelists» dans le monde.

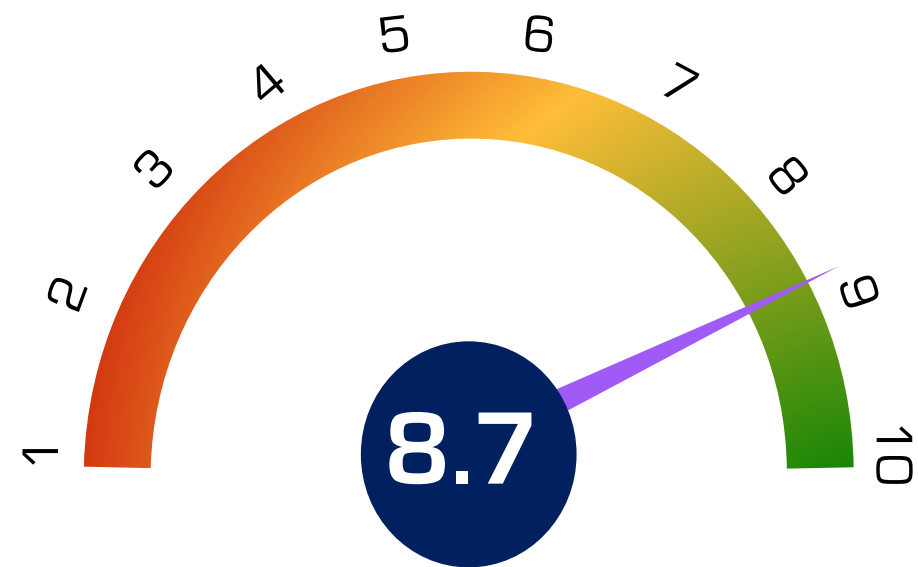


Enquête clients auprès des registrars

En novembre/décembre 2023, Switch a mené une enquête de satisfaction auprès de tous les registrars. 30 registrars sur 156 y ont participé. L'évaluation des résultats a donc une valeur indicative.

L'essentiel en bref

- Switch jouit auprès des registrars d'une réputation qui se caractérise par une fiabilité, une sécurité, une stabilité, une sympathie, un souci de la qualité et une compétence irréprochables.
- Comparée à l'ensemble des autres registries dans le monde, Switch offre de loin la meilleure prestation globale aux yeux des participantes et participants à l'enquête.
- L'impression générale qu'ont les registrars de Switch est d'un niveau très élevé (8,7 points sur 10 possibles).



Impression générale de Switch

Question: En tenant compte de tout ce que vous savez de Switch en tant que registry, quelle impression générale avez-vous de Switch?

Échelle: 1 = très négative; 10 = très positive

3.

Rapport d'activité – indicateurs statistiques

50%

Le programme de résilience DNS a permis à DNSSEC de réaliser la percée souhaitée. Aujourd'hui, près de 50% des noms de domaine sont signés.

1,6%

Croissance du domaine .ch

40 000

Croissance de près de 40 000 noms de domaine.

Nombre de noms de domaine – évolution 2023

Évolution .ch

En un an, le nombre de noms de domaine .ch a augmenté de plus de 40 000. Cela correspond à une augmentation de 1,6% par rapport à l'année précédente.

	2022	2023
Nouveaux enregistrements	281 610	294 195
Suppressions	258 724	282 649
Réactivations*	31 097	29 958
Nombre de domaines au 31 déc.	2 521 444	2 562 914

Évolution du portefeuille de noms de domaine .ch et .li

* Noms de domaine supprimés qui ont été réactivés par le registrar au cours de la période de transition de 40 jours.

Évolution .li

En l'espace d'un an, le nombre de noms de domaine .li n'a pratiquement pas changé.

	2022	2023
Nouveaux enregistrements	10 094	10 658
Suppressions	10 178	12 218
Réactivations*	1823	1699
Nombre de domaines au 31 déc.	70 478	70 607

Service de renseignements – statistiques 2023

Service de renseignements

Switch accorde à toute personne justifiant d'un intérêt légitime prépondérant l'accès gratuit aux données personnelles du détenteur ou de la détentrice du nom de domaine concerné contenues dans la base de données RDDS (Whois). Ces statistiques recensent toutes les demandes effectuées durant l'année sous revue via les formulaires du service de renseignements. Le nombre de demandes est resté stable par rapport à l'année précédente.

	Particuliers	Autorités
Renseignements fournis	304	135
Renseignements non fournis	56	5
Demandes d'ordre général *	4	0
Total des demandes	364	140

* Il s'agit ici de demandes concernant les processus, les procédures et les bases légales.

Accès simplifié via RDAP pour .ch et .li

Si une autorité ou une organisation dispose des autorisations nécessaires, elle peut consulter les noms de domaine via RDAP (Registration Data Access Protocol) et obtenir des données personnelles. Le nombre d'autorités a fortement augmenté en 2023, ce qui est également dû à notre meilleure mise en réseau avec les autorités de poursuite pénale. Fin 2022, seules 5 autorités utilisaient RDAP, contre 18 à la fin 2023. Les polices cantonales en représentent la plus grande part.

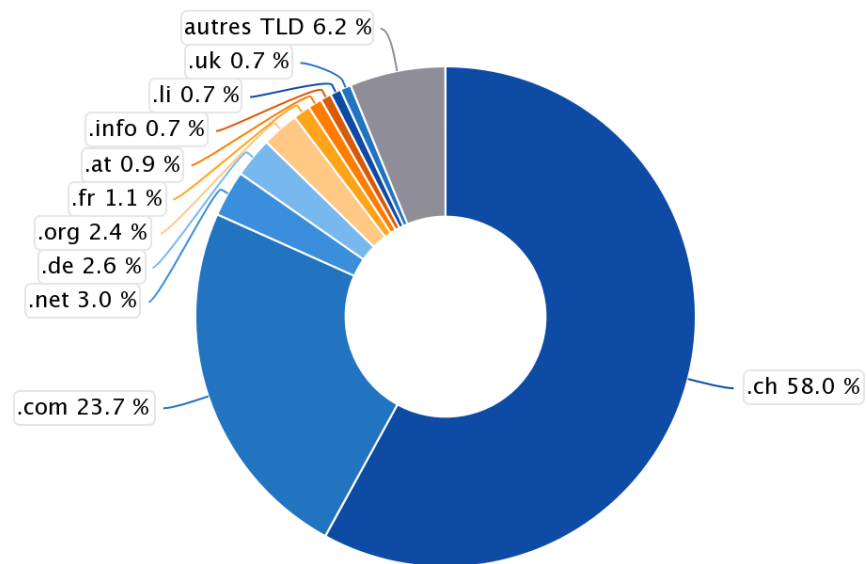
	Demandes
Renseignements fournis	3612
Renseignements non fournis	309
Total des demandes	3921

Part de marché de .ch et .li chez les détenteurs et détentrices suisses de noms de domaine

La part de marché du domaine de premier niveau (TLD) **.ch** parmi les détenteurs et détentrices en Suisse est restée pratiquement inchangée entre octobre 2022 et octobre 2023.

Octobre 2022

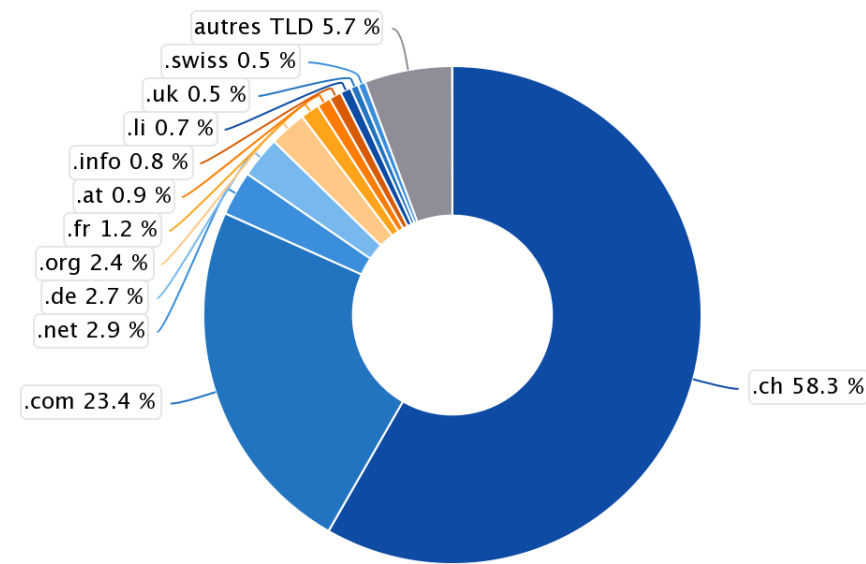
Part de marché des différents TLD chez les détenteurs et détentrices de noms de domaine en Suisse. Source: CENTR



La part de marché des TLD génériques **.com/.net/.org** a peu changé, tout comme celle des noms de domaine **.li**.

Octobre 2023

Part de marché des différents TLD chez les détenteurs et détentrices de noms de domaine en Suisse. Source: CENTR



Programme de résilience DNS – développement en chiffres

DNSSEC

- Pourcentage de noms de domaine avec DNSSEC, état au 1^{er} janvier 2024: 49,1% (1^{er} janvier 2023: 44,8%).
- Taux d’erreurs: le taux d’erreurs est resté très faible tout au long de l’année, de manière plus ou moins constante. Moins de 0,25% de tous les noms de domaine DNSSEC présentaient des erreurs (2022: moins de 0,5%).

DMARC et SPF

- 1^{er} juillet 2023 (début des mesures chez OpenIntel): 2,6% correctement configurés.
- 1^{er} janvier 2024: 4,5% correctement configurés. Chiffres pour les noms de domaine .ch et .li, configuration correcte de DMARC et de SPF. Données selon les statistiques du prestataire de services de mesure externe.

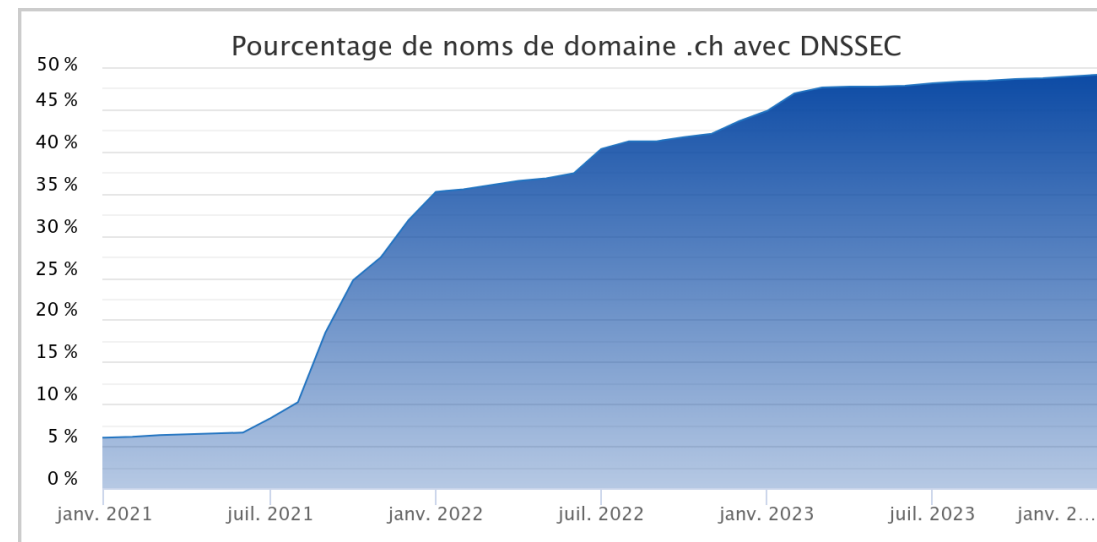
[Statistiques DNSSEC chez Switch](#)

[Statistiques chez OpenIntel](#)

Calcul du remboursement pour l’année 2023

- Recettes supplémentaires collectées grâce à la différenciation des prix: CHF 1 792 697
- Moins la compensation fixe pour Switch et le prestataire de mesure externe 2023: CHF – 444 907
- Total du remboursement CHF 1 347 790

Les remboursements seront effectués fin février 2024.



Développement DNSSEC

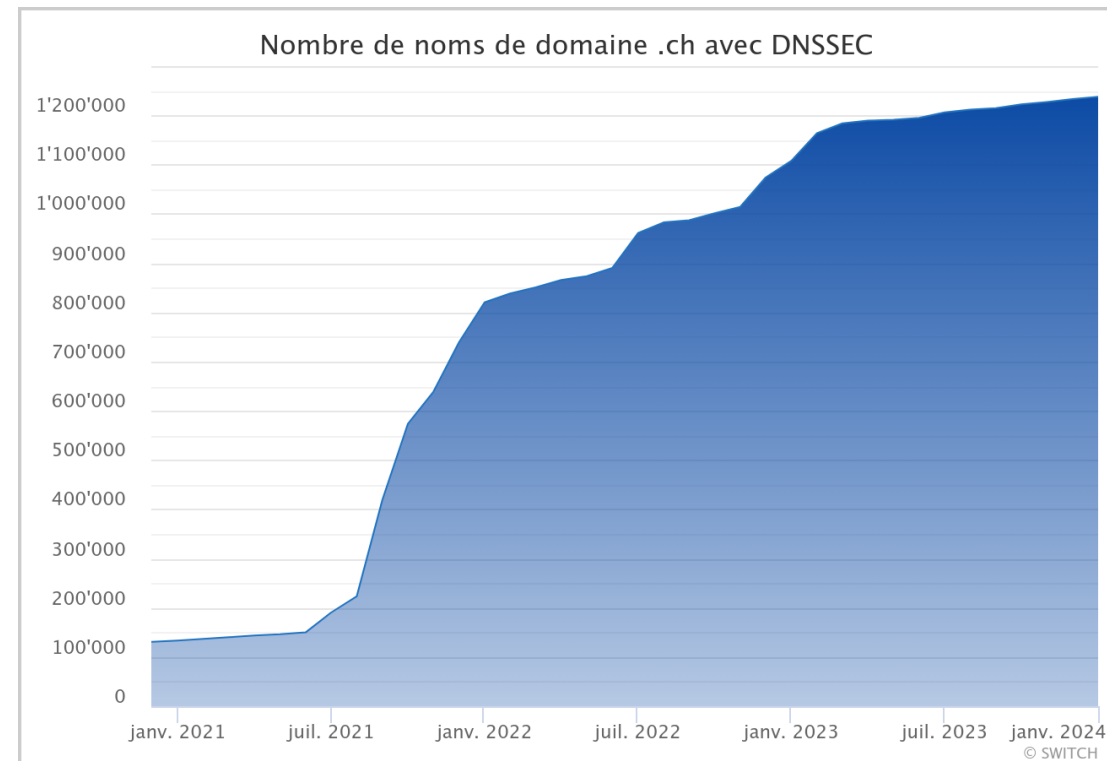
Nombre de noms de domaine signés

Fin 2023, plus de 1,2 million de noms de domaine .ch ont été signés avec DNSSEC.

Cela correspond à près de 50% de tous les noms de domaine .ch avec serveurs de noms, contre 45% fin 2022 et 35% fin 2021. La forte augmentation en 2021 et 2022 est principalement due aux registrars qui ont signé tous les noms de domaine de leurs clients dans le cadre du programme de résilience DNS. Cette croissance s'est ralentie en 2023.

Entre-temps, les grands registrars suisses ont signé leurs noms de domaine dans la mesure du possible. Si les noms de domaine ont des serveurs de noms «externes», les registrars n'ont aucune influence sur la signature. Pour les grands registrars à l'étranger, le TLD .ch ne représente qu'une très petite partie de leur activité et l'effort pour la signature n'est pas vraiment rentable pour eux. Il faut donc s'attendre à un fort ralentissement de la croissance à l'avenir.

Nombre de noms de domaine .ch avec DNSSEC



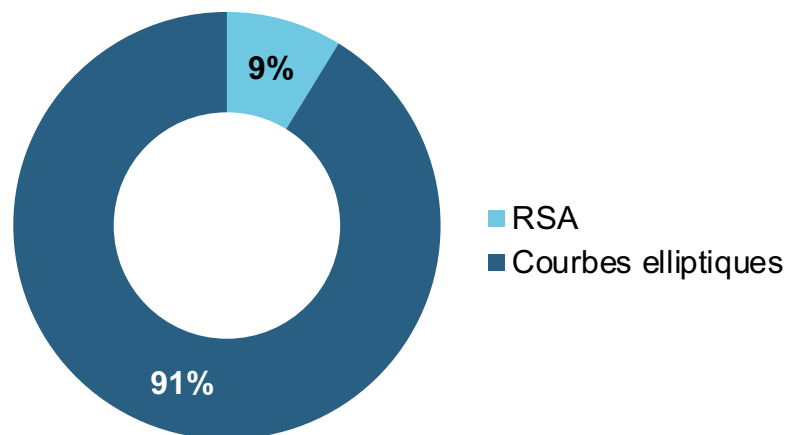
1 237 670 noms de domaine .ch signés avec DNSSEC au 1^{er} janvier 2024

Développement DNSSEC

Répartition algorithmes DS

Aujourd'hui, plus de 90% de tous les noms de domaine .ch utilisent l'algorithme 13 actuellement recommandé (ECDSAP256SHA256).

Les enregistrements DS avec les algorithmes 5 et 7, qui ne sont plus considérés comme sûrs en raison de leur signature SHA-1, ne sont plus pris en charge depuis février 2023 et ont donc été retirés de la zone.



Signatures DNSSEC utilisées

Algorithme DNSSEC	Nombre	Part
5 – RSASHA1	0	0,00%
7 – RSASHA1-NSEC3-SHA1	0	0,00%
8 – RSASHA256	111 923	9,04%
10 – RSASHA512	59	0,00%
13 – ECDSAP256SHA256	1 225 464	90,93%
14 – ECDSAP384SHA384	142	0,01%
15 – ED25519	42	0,00%
16 – ED448	90	0,00%

Validation DNSSEC en Suisse

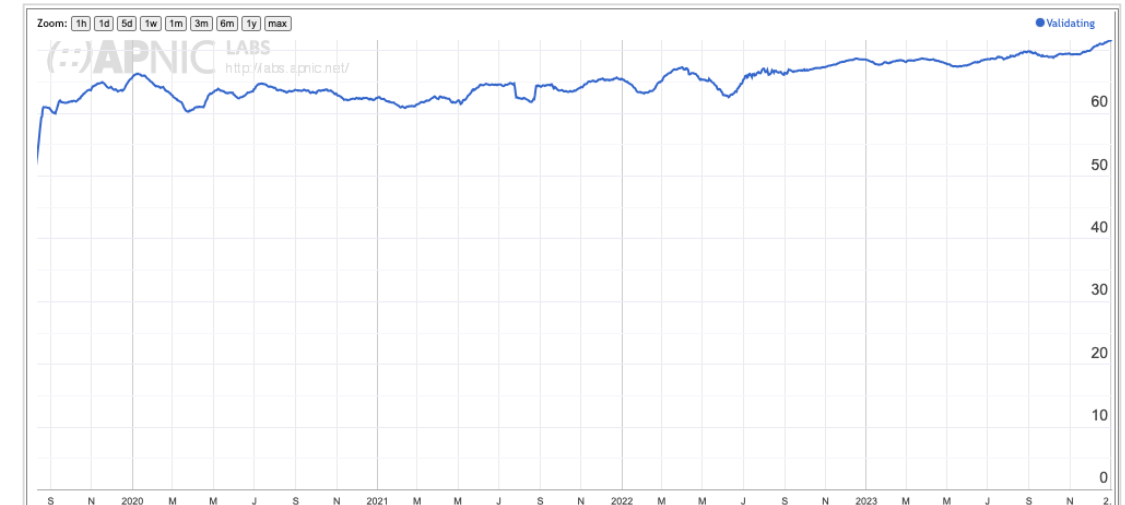
Validation DNSSEC

Pour protéger les utilisatrices et utilisateurs contre l'usurpation de DNS, les noms de domaine doivent être signés d'une part, et ces signatures doivent d'autre part être validées par le résolveur DNS.

Selon les mesures de l'APNIC, le taux de validation DNSSEC sur les résolveurs des FAI suisses a dépassé pour la première fois les 70% l'année dernière.

Page Web: <https://stats.labs.apnic.net/dnssec/CH>

Validation DNSSEC sur les résolveurs suisses



Délégation différée – statut

Base légale

Avec l'article 25 de l'ODI, «Conditions générales d'attribution», l'OFCOM a créé la base légale permettant au registry, en cas de suspicion d'utilisation ou de but illicites d'un nom de domaine, de ne pas l'activer dans un premier temps et de ne pas entrer les serveurs de noms dans le fichier de zone. Ce processus est appelé «délégation différée» (Deferred Delegation en anglais).

Adaptations de processus

Grâce au durcissement des règles, nous avons pu retenir et supprimer beaucoup plus d'enregistrements en 2023.

Après la mise en production, nous continuons à réviser régulièrement les critères. En outre, de nouveaux critères et de nouvelles méthodes de vérification sont étudiés afin de mieux détecter les enregistrements abusifs. Ce dernier point en tenant toujours compte des utilisatrices et utilisateurs autorisés, qui ne doivent pas être gênés.

Nous sommes en contact avec d'autres registries afin de continuer à nous améliorer et à échanger nos expériences.

Nous avons développé un tableau de bord qui nous permet d'obtenir à tout moment une vue d'ensemble des métriques actuelles du processus. Grâce à l'analyse des données, les critères sont régulièrement révisés et affinés. Dans la mesure du possible, la délégation différée ne doit viser que les utilisations abusives et ne doit pas gêner les utilisateurs autorisés.

Indicateurs liés à la délégation différée 2023

Nombre total de nouveaux enregistrements	294 195
Noms de domaine différés	2751
Noms de domaine supprimés	1956

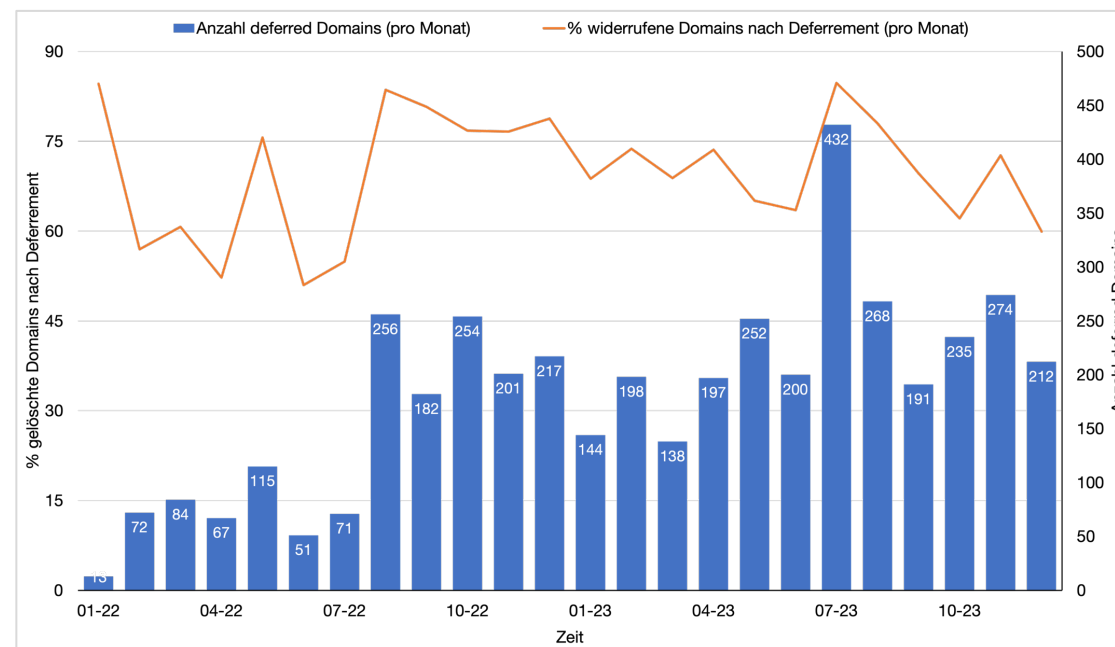
Délégation différée – statut

Rétrospective de la délégation différée

Depuis l'introduction de la délégation différée début 2022, nous avons progressivement augmenté le nombre de noms de domaine «différés» (barres bleues).

Cet objectif a été atteint grâce à un durcissement croissant des critères. Une sélection rigoureuse de ces critères a également permis de stabiliser la proportion de noms de domaine révoqués après l'absence d'identification du détenteur (courbe orange).

On remarque un grand nombre de noms de domaine «différés» en juillet 2023. Une partie est due à un seul détenteur qui avait enregistré un grand nombre de noms de domaine, mais qui n'a pas fourni d'identification.



Cas de règlement des différends

Sur mandat de l' OFCOM, Switch est chargée d'offrir un service de règlement des différends à un prix avantageux. Pour ce faire, Switch utilise depuis 2004 le service de règlement des différends de l'OMPI (Organisation mondiale de la propriété intellectuelle). L'OMPI exploite un service de règlement des litiges accrédité par l'ICANN pour plus de 70 autres registries.

En 2023, les experts ont pris des décisions pour 16 noms de domaine .ch. La décision des experts est la dernière étape de la procédure. Un nombre un peu moins grand de cas sont déjà terminés avant, par exemple pendant la tentative de conciliation ou en cas d'interruption de la procédure.

Décision de l'OMPI	2022	2023
Transfert au requérant	15	11
Plainte rejetée	2	5
Nombre de décisions	17	16

Décisions de l'OMPI (février 2024)

	Noms de domaine
Transfert au requérant	diadora.ch immoswisslife.ch albi-keramik.ch albikeramik.ch migrosbankswitzerland.ch naturoflooring.ch dallmayer.ch tmhinternational.ch solidea.ch nortonabrasives.ch dermagora.ch
Plainte rejetée	rockantenne.ch cheeze.ch schluessel-luzern.ch imageskinicare.ch zoskinhealth.ch

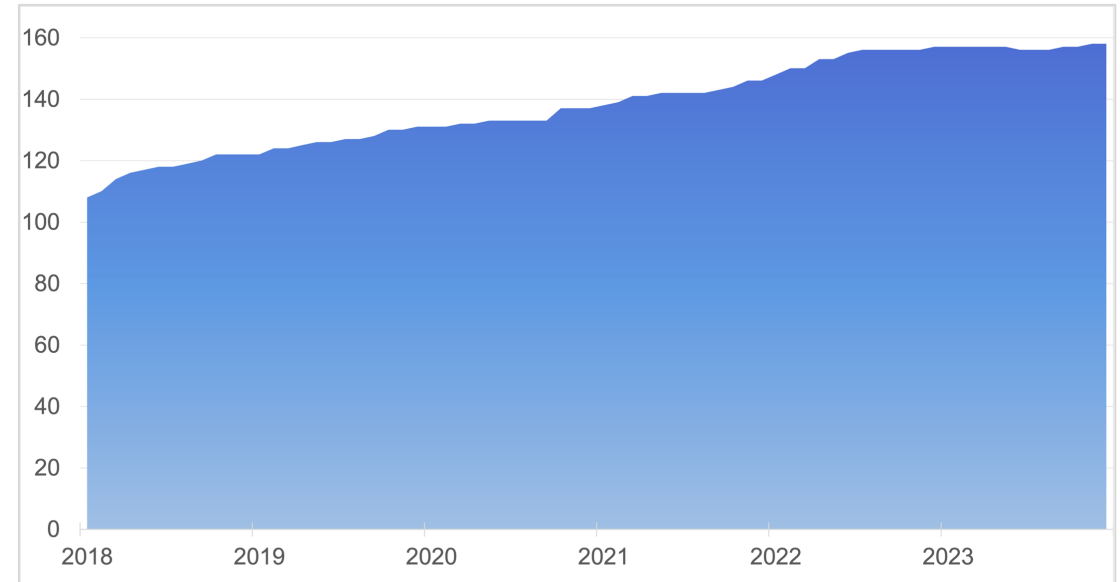
Évolution registrars

En 2018, beaucoup plus de registrars que prévu sont arrivés, si bien que nous en avons 122 à la fin de l'année.

En 2019, le nombre de registrars est passé à 131 et, fin 2020, le registry comptait 137 registrars. En 2021, le nombre de registrars a augmenté de 9 pour atteindre un total de 146.

En 2021, 11 registrars ont d'abord signé un contrat de test pour accéder au système de test. À la suite de la réussite de la phase de test et du parcours de test, nous avons pu passer ces registrars en mode productif. Le nombre total de registrars reconnus est ainsi passé à 157.

En 2023, nous n'avons pu donner accès au système de production qu'à un registrar supplémentaire et leur nombre est passé à 158.



Performance des serveurs de noms

Switch s'appuie sur l'ICANN agreement pour les exigences de mesure de performance DNS pour les temps de réponse aux requêtes DNS: les réponses aux requêtes à la zone CH doivent être données par au moins un serveur de noms logique dans un délai de 500 ms (UDP) ou de 1500 ms (TCP).

Cette exigence a été respectée en tout temps en 2023.

Les mesures sont effectuées par RIPE et sont accessibles au public.

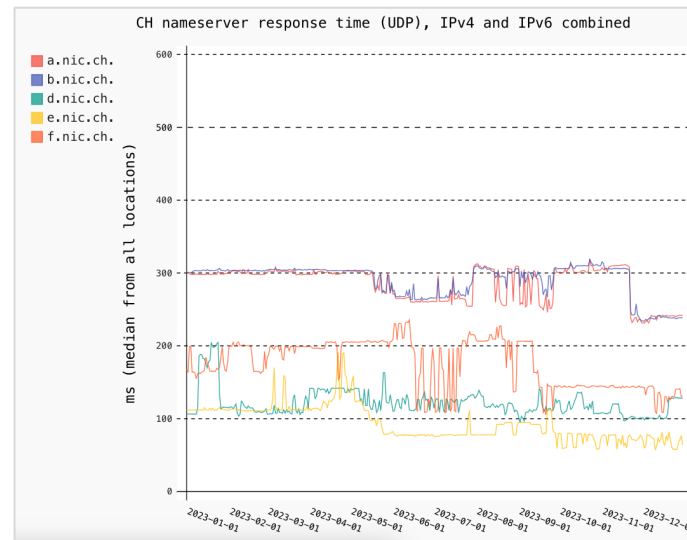
<https://atlas.ripe.net/dnsmon/group/ch>

Unicast: a.nic.ch (CH), b.nic.ch (CH),

Anycast: d.nic.ch, e.nic.ch, f.nic.ch

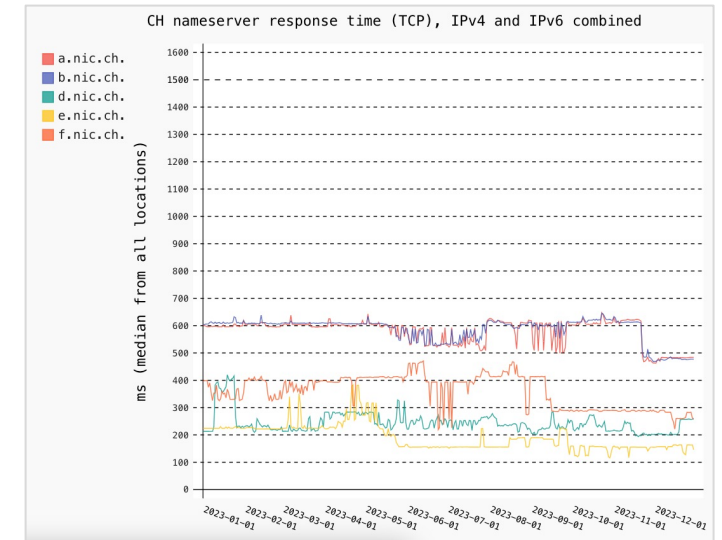
Temps de réponse UDP

Temps de réponse combinés
IPv4 et IPv6



Temps de réponse TCP

Temps de réponse combinés
IPv4 et IPv6



Cybercriminalité

Aspects quantitatifs

Les cas suivants ont été enregistrés et traités au cours de l'année sous revue:

Nombre de cas de malware et de phishing en 2023 observation quantitative

	# cas de malware	# cas de phishing
Notifications reçues	1242	942
Soupçon confirmé	505	643
Nombre de noms de domaine bloqués	187	475
Raison de la levée du blocage:		
- La durée légale est dépassée	37	17
- Corrigé après blocage	119	34
- En cours de traitement à la date de référence	4	12
Noms de domaine révoqués	27	419

Aspects qualitatifs

Le temps suivant a été nécessaire pour les cas:

Nombre de cas de malware et de phishing en 2023 observation qualitative

	Durée
Durée du blocage selon l'art. 15 al. 1, 2, 3 de l'ODI, temps de blocage max. 30 jours (720 h)	Durée minimum 0,50 h
	Moyenne 103,32 h
	Durée maximum 160,05 h
Temps de réaction de Switch après notification	Moyenne 8 h 15
Temps pour éliminer la menace après la notification au détenteur ou à la détentrice	Moyenne 104,27 h

DNS Health Report

Le DNS Health Report vérifie l'accessibilité des serveurs de noms et des noms de domaine en .ch et .li. En cas de problèmes techniques, Switch en informe les exploitants et formule des recommandations pour y remédier. Le DNS Health Report améliore ainsi la fiabilité de l'Internet suisse. Ce qui est vérifié:

- Serveurs de noms: le fonctionnement des serveurs de noms est vérifié pour s'assurer qu'il est conforme aux normes DNS.
- Noms de domaine: il est vérifié si les noms de domaine signés DNSSEC peuvent être résolus par un résolveur récursif validant.

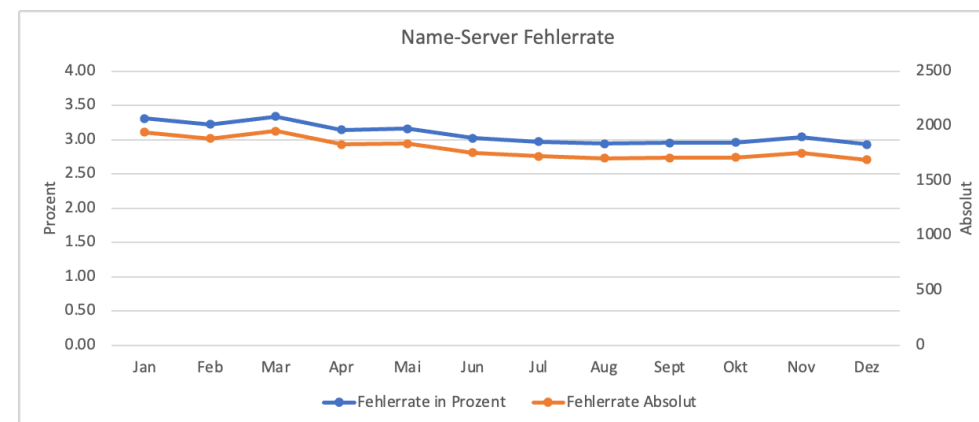
Rapport sur les serveurs de noms

Le taux d'erreur de la mesure de l'accessibilité des serveurs de noms ne diminue que légèrement depuis le début de la mesure, mais constamment. C'est une tendance très satisfaisante.

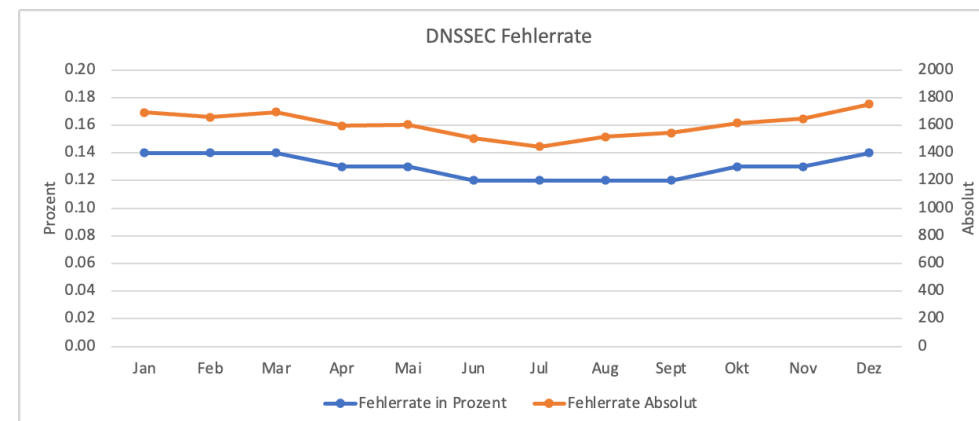
Rapport sur les noms de domaine

Le taux d'erreur de la mesure de l'accessibilité des noms de domaine a atteint un plateau. La plupart des noms de domaine erronés sont des noms de domaine parqués, pour lesquels la motivation à corriger les erreurs est faible.

Taux d'erreur de la mesure de l'accessibilité des serveurs de noms



Taux d'erreur de la mesure de l'accessibilité des noms de domaine



DAAR.ch

ICANN Domain Abuse Activity Reporting

Avec la publication de la zone .ch, Switch participe au projet DAAR (Domain Abuse Activity Reporting) de l'ICANN. Ce projet compare les signalements de soupçons d'abus pour différents TLD.

Le programme et les rapports pour les ccTLD sont encore en statut bêta. Toutefois, le graphique permet d'ores et déjà de comparer le TLD .ch avec d'autres ccTLD et gTLD.

Qu'est-ce qui est mesuré?

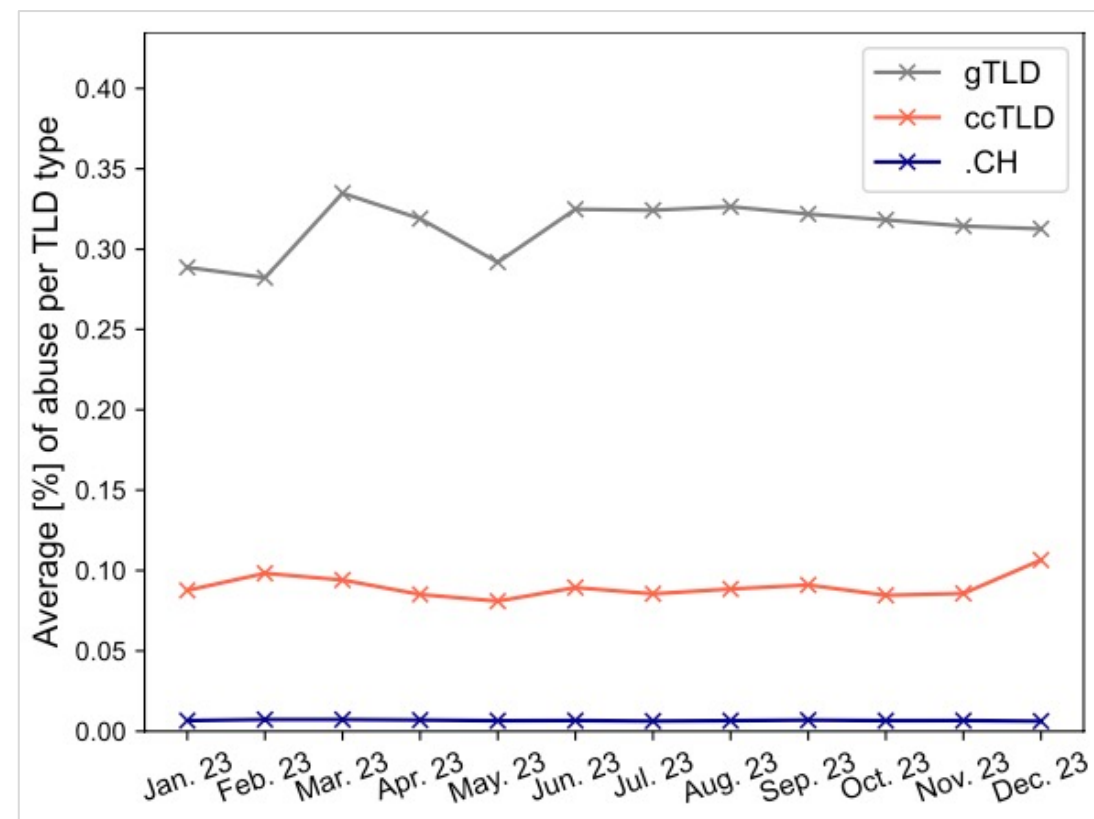
Pourcentage de noms de domaine .ch identifiés comme une menace pour la sécurité par rapport au nombre moyen de noms de domaine dans d'autres zones TLD.

Des informations détaillées sont disponibles auprès de l'ICANN:

<https://www.icann.org/octo-ssr/daar>

Analyse de .ch

Le rapport DAAR montre que les abus de noms de domaine pour le ccTLD .ch sont peu nombreux par rapport à la moyenne de tous les TLD. Cela vient confirmer l'efficacité des mesures permanentes de lutte contre la cybercriminalité et le bon fonctionnement de la collaboration avec les autorités suisses et les organisations internationales.



DAAR .li

ICANN Domain Abuse Activity Reporting

Avec la publication de la zone .li, Switch participe au projet DAAR (Domain Abuse Activity Reporting) de l'ICANN. Ce projet compare les signalements de soupçons d'abus pour différents TLD.

Le programme et les rapports pour les ccTLD sont encore en statut bêta. Toutefois, le graphique permet d'ores et déjà de comparer le TLD .li avec d'autres ccTLD et gTLD.

Qu'est-ce qui est mesuré?

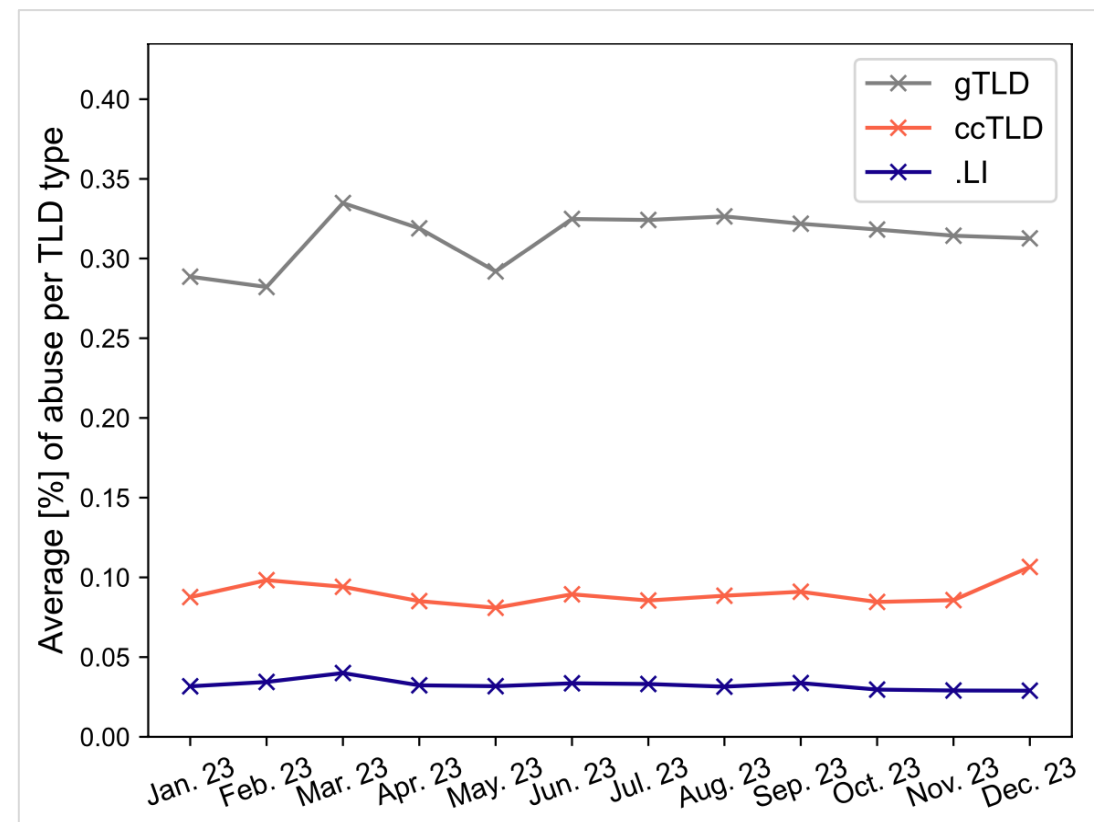
Pourcentage de noms de domaine .li identifiés comme une menace pour la sécurité par rapport au nombre moyen de noms de domaine dans d'autres zones TLD.

Des informations détaillées sont disponibles auprès de l'ICANN:

<https://www.icann.org/octo-ssr/daar>

Analyse de .li

Le rapport DAAR montre que les abus de noms de domaine ont pu être éliminés pour le ccTLD .li, à l'exception d'environ deux douzaines de noms de domaine. Ce taux bas ne pourra être maintenu que si la collaboration entre le registry et les autorités continue de fonctionner aussi bien que jusqu'à présent.



4.

Rapport d'activité – indicateurs économiques

Indicateurs économiques

La séance du Conseil de fondation du 13 juin 2024 permettra de valider le rapport annuel 2023 de la fondation Switch ainsi que le bilan et le compte de résultat. La publication aura lieu à partir du 14 juin 2024.

Aucun chiffre n'est publié ici, mais il est fait référence aux documents détaillés du rapport annuel 2023 de Switch.

5.

Rapport d'activité – développements

Rétrospective 2023

Changement de l’algorithme DNSSEC

Initialement, l’algorithme NSEC3 (avec opt-out) avait été choisi pour la signature du fichier de zone. Ce mécanisme empêchait le «Zone Walking» et compliquait ainsi l’établissement d’une liste automatique de tous les noms de domaine avec la séquence typique de spams.

À présent, le fichier de zone est public. Le taux de signature élevé de 50% exige des méthodes plus efficaces, qui seront obtenues grâce au passage à l’algorithme NSEC. Le changement de paramètres de sécurité dans le DNS nécessite des clarifications techniques minutieuses en amont. Les exploitants des serveurs de noms et des résolveurs sont impliqués. La communauté technique de l’ICANN et de DNS-OARC a également été consultée. Cela a permis de donner le feu vert au changement. Le changement du 10 novembre 2023 n’a entraîné aucune perturbation des fonctions des serveurs de noms ou des résolveurs. Le fichier de zone est légèrement plus volumineux après le changement, tandis que les serveurs de noms et les résolveurs nécessitent moins de ressources de calcul.

European TLD ISAC

L’European TLD ISAC (Information Sharing and Analysis Center) a été lancé en février 2023. La phase de développement est soutenue par le CENTR et sept registries ccTLD. Switch est représenté au sein du comité et désigne un collaborateur pour l’élaboration des processus de collaboration. L’accent doit être mis sur l’échange de threat intelligence, c’est pourquoi ce sont surtout les registries dotés d’un CERT et d’un ISMS qui sont actifs ici. Une période de deux ans est prévue pour la mise en place des processus clés et l’extension à tous les registries ccTLD de l’UE. Le European TLD ISAC est entièrement financé par les registries participants.

Rétrospective 2023

Augmentation de la sécurité des e-mails

Dans le programme de résilience DNS, il a été convenu avec l'OFCOM et les registrars qu'en 2024, l'implémentation de DMARC et de SPF constituerait le critère de remboursement. Dans ce contexte, Switch a mis en place en 2023 l'infrastructure de mesure et un tableau de bord pour la vérification manuelle des critères de mesure.

DANE a été défini comme critère pour 2025. Switch a proposé des formations sur ce thème en octobre 2023 à Lausanne et à Zurich.

Par conséquent, l'infrastructure de messagerie interne de Switch a également été modifiée pour permettre l'utilisation des trois protocoles de sécurité pour l'envoi et la vérification à la réception.

Interface Web RDAP pour les autorités

L'interface Web de la base de données RDDS (Whois) est en service. Chaque utilisatrice et utilisateur auprès d'une autorité signe un contrat d'utilisation. Switch gère les droits d'utilisation. Jusqu'à présent, seules quelques petites autorités utilisent cet accès pratique, mais c'est précisément pour ces autorités que l'interface Web est conçue.

Perspectives stratégiques et objectifs

Certains projets planifiés de manière fixe sont présentés dans la rubrique «Nouveautés prévues en 2024». Le projet Domain Abuse 4.0, qui sera l'axe principal en 2024, est également présenté dans une autre section. Il s'agit ici de deux orientations qui sont plutôt de nature stratégique.

Emplacement de l'infrastructure

Au cours des cinq à huit dernières années, les grandes organisations sont d'abord passées avec leur infrastructure informatique aux hyperscalers dans le cloud afin de consolider l'infrastructure et de réduire les coûts. Les PME ont suivi un peu plus tard, notamment sous la pression de fournisseurs de logiciels tels que Microsoft, qui ne garantissent plus le fonctionnement sur site de leurs logiciels à long terme.

L'infrastructure informatique de Switch est répartie sur plusieurs sites. Ceux-ci sont reliés par une infrastructure de fibre optique qu'elle exploite elle-même. Cela garantit un contrôle maximal sur toutes les couches des composants informatiques.

La collaboration avec un fournisseur suisse de cloud permet à Switch de mettre en place de nouveaux composants informatiques et de stockage dans des centres de calcul professionnels. Ici, le niveau de sécurité contre les pannes et de contrôle d'accès est plus élevé que dans les sites proposés jusqu'à présent par les universités. Ces centres de calcul sont eux aussi raccordés au réseau de fibre optique «Switch LAN».

Au cours des années 2024 et 2025, les composants logiciels du registry passeront à une nouvelle architecture et seront exploités sur les nouveaux sites. La gouvernance de l'infrastructure et des données enregistrées incombe entièrement à Switch et le site de l'infrastructure reste en Suisse. Il s'agit de conditions marginales importantes pour l'exploitation d'une infrastructure critique et le traitement des données dans le cadre de la lutte contre la cybercriminalité.

Perspectives stratégiques et objectifs

Programme de résilience DNS 2027+

Le programme de résilience DNS fait partie du contrat de prolongation de 2022 à 2026 avec l'OFCCOM. Le DNSSEC Advisory Board détermine quels protocoles de sécurité doivent être promus par le programme de résilience. Les critères sont définis respectivement deux ans à l'avance. Switch peut ainsi proposer des formations et préparer l'infrastructure de mesure. Les registrars ont suffisamment de temps pour planifier les travaux techniques en vue d'éventuels changements avant le début des mesures.

Des discussions devraient avoir lieu en 2024 sur une éventuelle poursuite du programme après 2026 et la manière de le faire. Le programme en cours fournit déjà des informations et des expériences importantes à ce sujet. Il est recommandé de réunir les parties impliquées autour d'une table pour cette discussion.

Nouveautés prévues en 2024

Programme de résilience DNS: mesures DANE

Le protocole de sécurité DANE a été défini comme critère pour les remboursements en 2025. Switch élargit l'infrastructure de mesure en conséquence. Le tableau de bord est également complété afin que les registrars et les hébergeurs puissent vérifier s'ils ont correctement mis en œuvre la configuration conformément aux recommandations de Switch.

Le critère pour 2026 sera IPv6. Aucune formation spécifique n'est prévue à cet effet.

Domain Abuse 4.0

Le projet «Domain Abuse 4.0» assure l'avenir de la lutte contre la cybercriminalité du registry. Une description du projet figure à la page 23.

ISMS ISO27001:2022

Jusqu'à présent, la norme ISO 27001:2013 était la norme d'audit du registry. La norme révisée dans sa version 2022 tient compte d'un champ thématique plus large et adapté aux exigences technologiques et sociales.

Switch a l'intention d'adapter tous les processus et documentations pertinents pour une certification selon la nouvelle version d'ici l'automne 2024. Switch profite du fait que de nombreux nouveaux thèmes demandés par la norme sont déjà utilisés avec succès depuis des années, comme la threat intelligence par le CERT ou ses propres solutions de sécurité comme le pare-feu DNS. La certification indépendante atteste que Switch a mis en œuvre avec succès et efficacité un système de gestion de la sécurité de l'information. Cela garantit que Switch remplit ses missions en matière d'exploitation d'infrastructures critiques et de protection des données à caractère personnel, y compris en vertu de la LPD et de l'ISG.

Nouveautés prévues en 2024

Web crawler pour le registry

Pour lutter contre les malwares et le phishing, le registry est tributaire des signalements des services spécialisés. Jusqu'à la fin 2023, le NCSC exploitait un web crawler. Celui-ci interrogeait individuellement les serveurs Web de la zone .ch et analysait les réponses aux schémas suspects. En cas de soupçon de malware et de phishing, le NCSC signalait les informations à Switch. Nous analysons les sites à l'aide de nos outils et, en cas de soupçon confirmé, nous déclenchons les processus appropriés afin de retirer les pages Web du réseau ou de faire supprimer le code malveillant.

Avec la suppression du web crawler du NCSC, un intrant important manque au registry pour lutter contre la cybercriminalité. C'est pourquoi Switch a développé son propre web crawler pour les zones .ch et .li dès la fin de l'automne. Switch a les sources commerciales et informelles nécessaires pour les schémas, sans lesquels le crawler serait inutile.

La mise en service est prévue dès que possible, dans l'idéal dès janvier ou février 2024.

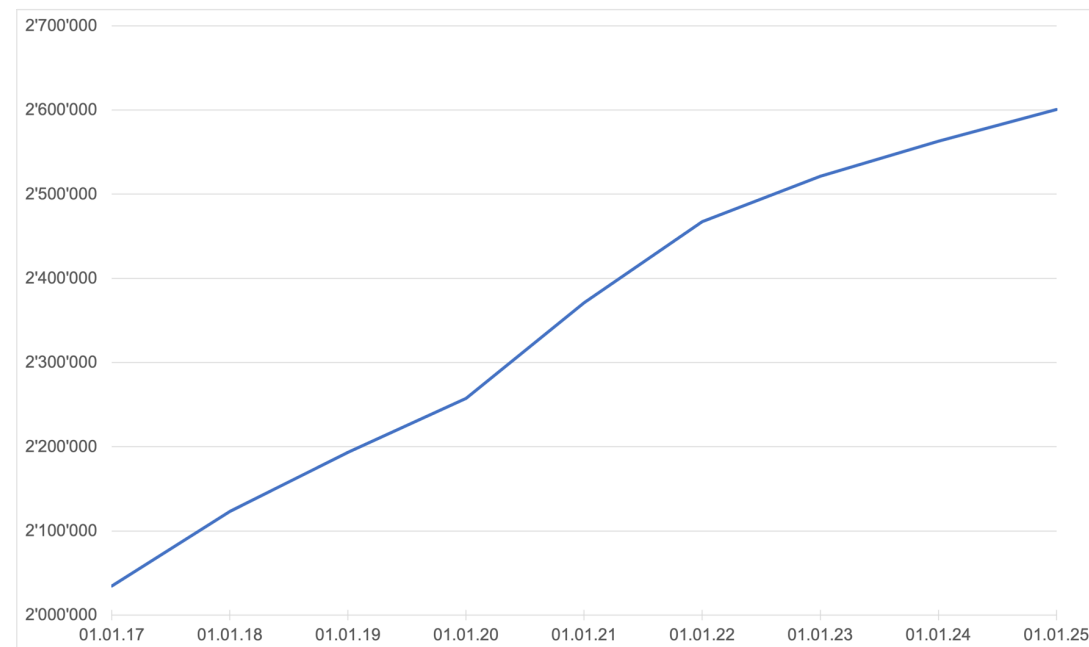
Prévisions de croissance des noms de domaine .ch

Les années 2018 et 2019 ont montré une augmentation, légèrement inférieure d'une année à l'autre. En 2020, la poussée de la numérisation due à la pandémie et les initiatives marketing des hébergeurs Web ont entraîné une augmentation de la demande et donc une croissance de 4,8%. En 2021, la croissance a diminué pour atteindre 3,9%, mais est restée plus élevée qu'avant la pandémie.

Pour 2022, le registry a encore enregistré une croissance de 2,1%. La poussée de la numérisation a donc duré deux ans et entraîné une augmentation inattendue d'environ 100 000 noms de domaine.

En 2023, l'augmentation a été de près de 40 000 noms de domaine. Cela correspond à 1,6% et n'atteint pas nos prévisions de 1,8%.

Nous observons une saturation du marché et une croissance globalement ralentie des noms de domaine. Nos prévisions pour 2024 tablent sur une augmentation de 1,45%.



Switch

Werdstrasse 2
Case postale
CH-8021 Zurich

Tél. +41 44 268 15 15
www.switch.ch
info@switch.ch