La sécurité sur Internet

Tendances, dangers, stratégies

SWITCH

Environnement Internet: la Suisse se numérise à grande vitesse

Internet permet de rendre de nombreuses opérations plus simples, plus rapides et plus économiques que par des moyens physiques. C'est pourquoi la Confédération favorise l'approvisionnement de la Suisse en Highspeed-Internet. En 2013, 91 pourcent des ménages de notre pays disposaient d'un raccordement Internet. La Suisse compte ainsi parmi les pays les mieux desservis du monde.

Parallèlement à cela, la Confédération, dans le cadre de l'e-government, met sur le réseau de plus en plus de parties de l'administration et du domaine public. C'est ainsi que le plan principal de 2016–2019 prévoit que la population suisse puisse, d'ici 2019, changer d'adresse, voter et élire ainsi qu'au déroulement de la taxe sur la valeur ajoutée sous forme électronique.

Le paysage des dangers: l'économie clandestine en profite

Le transfert progressif des processus administratifs et commerciaux sur Internet inspire les profiteurs criminels: le crime sur Internet est devenu, ces dernières années, une branche économique fort lucrative et à prendre au sérieux. Car le risque de se faire prendre dans l'espace virtuel est relativement restreint. Dans une étude de 2014, le Center for Strategic and International Studies à Washington arrive à la conclusion que les cyberattaques entraînent au niveau mondial des pertes de 375 à 575 milliards de dollars US par an. A titre comparatif: le produit intérieur brut de la Suisse équivalait en 2013 à 686 milliards de dollars US.

Le crime sur Internet est diversifié

Tandis que les criminels sur Internet concentraient autrefois leurs activités sur les banques, ils s'intéressent maintenant à des domaines plus vastes. Actuellement, ils se concentrent sur le secteur du logiciel et de la technologie, les services conseils et en entreprise, le commerce de détail, la construction et l'ingénierie, et maintenant aussi les organisations étatiques.

Voici comment ils sélectionnent leurs cibles

Il y a deux choses qui caractérisent les cybercriminels: grands bénéfices et peu de travail. Pour la première, les auteurs ont même quelquefois recours à des Advanced Persistent Threats (APT), soit à des méthodes complexes faites sur mesure pour la cible concernée. Tandis que les APT étaient autrefois une méthode d'espionnage, ils servent actuellement aussi à des buts monétaires. Pour la seconde, il y a sur Internet du logiciel malveillant au prix relativement abordable et utilisable à volonté. Un exemple en est le Toolkit Tinba, qui a causé beaucoup de soucis aux banques en 2015. Il ne coûte que quelques milliers de francs.

375 – 575 milliards

de dollars US par an: tel est le dommage provoqué par la cybercriminalité dans le monde selon l'estimation du Center for Strategic and International Studies à Washington.

439 millions

de variantes de programmes pernicieux existent actuellement selon l'office fédéral allemand pour la sécurité en technique informatique. Le nombre augmente à une vitesse vertigineuse étant donné que les programmes sont en partie générés automatiquement.

205

journées en moyenne s'écoulent, selon la société de sécurité Mandiant, jusqu'à ce que les premières traces d'une attaque par APT puissent vraiment être décelées, ce qui peut parfois durer plusieurs années.

.ch – un des domaines les plus sûrs du monde

En Suisse, nous pouvons être heureux que .ch compte parmi les domaines les plus sûrs du monde, comme le confirment diverses études. Ce n'est pas un hasard mais le résultat d'efforts bien organisés et constamment optimisés. La registry .ch dispose de déroulements bien rodés, de longues relations de confiance ainsi que d'une expertise acquise au fil des années. Et l'objectif doit maintenant être de maintenir le haut niveau de sécurité du domaine .ch.

Avant-gardiste: la lutte imposée par la loi contre l'abus de domaines

La pièce maîtresse des efforts en vue d'assurer la sécurité du Top-Level Domain .ch porte de toute manière sur la procédure contre le malware, qui est unique en son genre dans le monde. Il s'agit d'une procédure commune, efficace et bien rodée contre la criminalité sur Internet, englobant la collaboration entre SWITCH, les autorités et les registrars. Depuis 2010, cette procédure est inscrite dans la loi. L'article 15 de l'Ordonnance sur les domaines Internet (ODI) permet une réaction rapide lorsqu'il y a soupçon d'abus: dès que du malware sur un site .ch est annoncé, SWITCH en avise les détenteurs de domaines des sites infectés. Si ceux-ci ne réagissent pas en l'espace d'un jour ouvrable, SWITCH désactive les noms de domaine correspondants. Ainsi, les sites infectés ne sont plus accessibles de l'extérieur et ne peuvent plus diffuser de virus, chevaux de Troie ou autre logiciels pernicieux. En vertu de l'ODI, la désactivation est possible durant cinq jours ouvrables.

Une collaboration bien rodée avec les autorités

La désactivation ne peut être prolongée que sur proposition d'une autorité accréditée par l'OFCOM. Autrement, SWITCH doit réactiver le site à l'échéance du délai. Mais chez SWITCH, nous vérifions l'identité du détenteur et remettons le cas aux autorités. Si le détenteur du domaine ne supprime pas les contenus malveillants et ne prouve pas son identité, SWITCH efface définitivement les noms de domaine concernés. Cette procédure conséquente ôte aux domaines .ch leur attrait pour la diffusion de malware car les cybercriminels doivent faire beaucoup d'efforts pour arriver à leurs fins.

L'article 15 de l'ODI

est la pièce maîtresse de la lutte contre la criminalité sur Internet en Suisse. Il autorise le blocage rapide des attaques sur les visiteurs de sites web en Suisse.

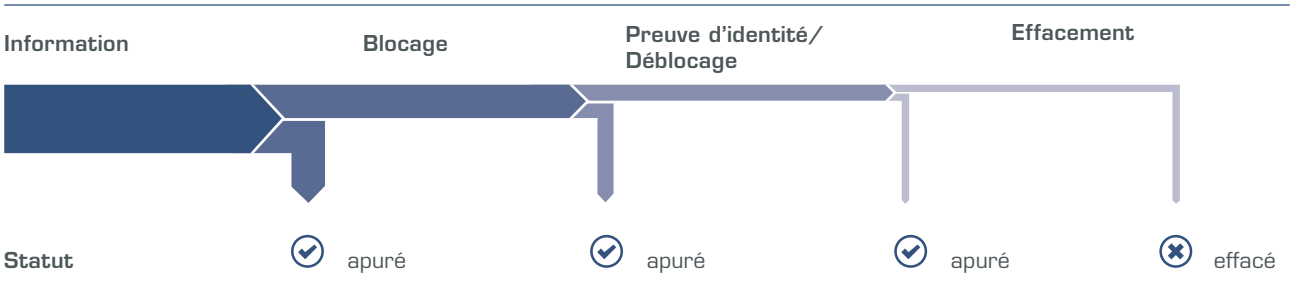
Unique en son genre

.ch est, dans le monde, la seule registry agissant contre le malware de concert avec le régulateur et des partenaires. Et le succès lui donne raison: Le Top-Level Domain compte parmi les plus sûrs du monde.

Il n'est guère intéressant

pour les criminels sur Internet de s'attaquer à .ch. Il leur coûte trop cher de toujours devoir chercher des remplacements pour des domaines qui ont été effacés en raison de la diffusion de malware ou ont été débarrassés du code malveillant.

Processus malware



La première place pour .ch au niveau de la sécurité

Comme dit précédemment, c'est entre autres le peu de travail nécessaire qui attire l'économie clandestine. Lorsque des criminels cherchent des Top-Level Domains pour leurs agissements, ceux qui les intéressent avant tout sont ceux à bas prix et à politique ouverte d'enregistrement. .ch serait ainsi extrêmement attrayant pour la criminalité sur Internet car ces deux critères s'appliquent à ce Top-Level Domain. En 2015, la société américaine Architelos, spécialisée en matière d'analyse Internet, a étudié les abus sur sites web (malware et phishing) en Europe et les a affectés aux différents Top-Level Domains. Au niveau de la sécurité, .ch a obtenu la première place. On peut donc en conclure que ceci est dû aux efforts de sécurité pour .ch. Le but doit maintenant être de maintenir le haut niveau de sécurité de la registry en Suisse et d'adapter constamment les mesures de sécurité aux changements dynamiques de l'économie du crime sur Internet.

La sécurité chez SWITCH: certifiée ISO et primée

La sécurité de la registry .ch est une tâche centrale de SWITCH. Nous disposons chez SWITCH d'un système bien établi de management de la sécurité informatique (ISMS) qui contrôle et optimise continuellement la sécurité. En 2014, nous avons obtenu pour cela la certification ISO-27001. Nous coopérons avec nos pendants en Autriche et en Allemagne et vérifions réciproquement les déroulements de sécurité de nos registries. En octobre 2015, nous avons gagné pour cela le prix de la sécurité du CENTR. CENTR, le Council of European National Top-Level Registries, est l'association européenne des services d'enregistrement des Top-Level Domains.

CENTR

Le Council of European National Top-Level a décerné son prix de la sécurité à SWITCH en octobre 2015.

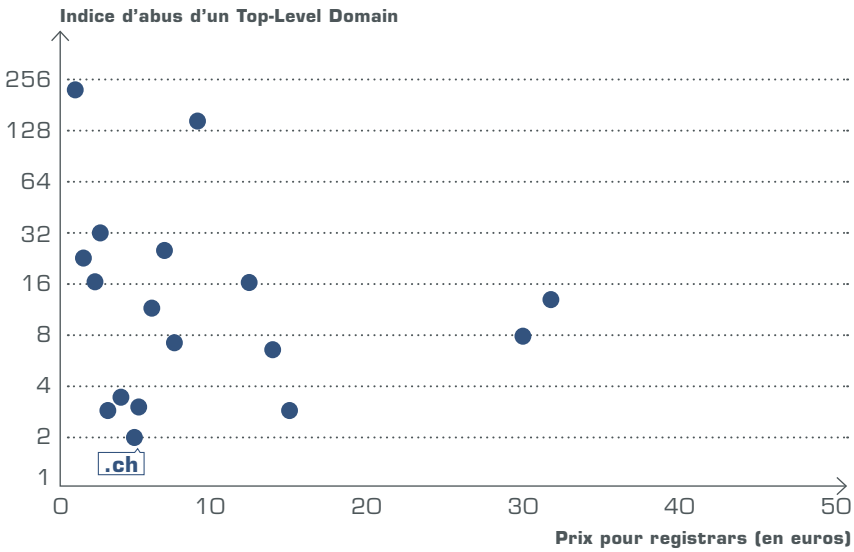
DNSSec

Les codes cryptographiques pour .ch sont hébergés chez SWITCH en Suisse. Il s'agit de signatures pour les domaines https, sûrs et difficilement attaquables.

ISO-27001

est le certificat pour un système de management de la sécurité informatique (ISMS), dont dispose la registry .ch. SWITCH optimise constamment son ISMS.

Rapport prix/sécurité des registries européennes



● Registry européenne à politique ouverte

Le tableau montre que parmi les registries européennes à politique ouverte, .ch occupe la première place au niveau de la sécurité.

Chiffres: Architelos; les registries sont anonymes pour des raisons de confidentialité.

Assistance aux exploitants de sites piratés

La plupart du temps, les exploitants de sites sont eux-mêmes surpris lorsque leurs sites diffusent des contenus malveillants. Ils sont victimes d'agissements de cybercriminels. SWITCH leur donne des instructions sur la manière dont ils peuvent supprimer le malware. En 2015, SWITCH a découvert du malware sur des sites .ch dans 761 cas. Dans la plupart des cas, 556 pour être précis, les détenteurs des domaines ont supprimé le code malveillant dès le premier avis.

Stratégie contre le phishing

Phishing désigne les tentatives d'obtenir des informations confidentielles de manière illégale. SWITCH a identifié au total 320 cas de ce genre en 2015. Etant donné que le nombre de cas de phishing augmente rapidement dans le monde, SWITCH a étendu la procédure contre le malware à la lutte contre le phishing en 2014. Avec succès: actuellement, nous ne constatons pas, chez SWITCH, d'augmentation des cas de phishing sur sites .ch.

La sécurité: une mission

Afin d'assurer la propreté du Top-Level Domain .ch, la population suisse doit être au courant des dangers qui rôdent dans le cyberspace. Elle doit savoir comment se protéger efficacement. C'est pourquoi SWITCH a co-fondé en 2014 la Swiss Internet Security Alliance (SISA – www.swiss-isa.ch). Celle-ci réunit d'importants acteurs de la branche de télécommunication et Internet dans le but de réduire les dommages provoqués par la criminalité sur Internet. Chez SWITCH, nous avons en outre mis sur le net le site d'information www.switch.ch/safer-internet avec des conseils pour se protéger des attaques.

761

cas de diffusion de malware sur des sites ont été constatés par SWITCH en 2015.

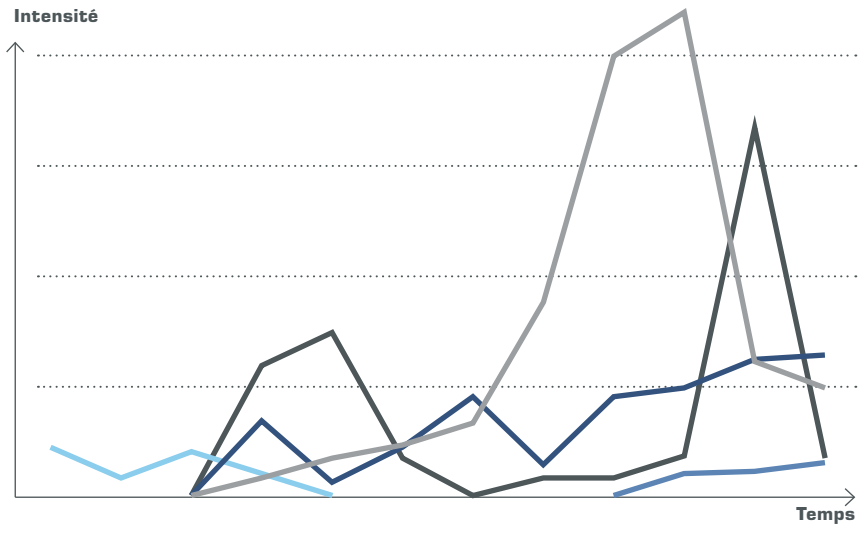
320

cas de phishing ont été constatés par SWITCH en 2015. Dans 53 cas, SWITCH a bloqué le domaine. SWITCH souhaite combattre encore davantage le phishing en collaboration avec des partenaires internationaux.

SISA

a été cofondée par SWITCH. La Swiss Internet Security Alliance réunit d'importants acteurs de branche suisse des télécommunications et d'Internet dans la lutte contre la criminalité sur Internet.

Le malware et sa dynamique



Les familles de malware n'ont pas toutes la même dynamique. Le graphique montre à titre d'exemple les attaques enregistrées en Suisse au cours d'une année.

Comment SWITCH obtient ses informations

En vue de supprimer du logiciel malveillant, il est très important de savoir quels sont les sites .ch infectés. Nous disposons de ces informations chez SWITCH car nous faisons partie d'un réseau mondial d'alarme et d'échanges scientifiques. Nous sommes dans cette situation privilégiée du fait que nous sommes non seulement gestionnaires de la registry .ch mais disposons d'un CERT (Computer Emergency Response Team), ceci déjà depuis 1991. Nous sommes ainsi l'organisation de Suisse disposant de la plus longue expérience dans la lutte contres les dangers sur Internet. Le CERT de SWITCH est de réputation internationale. Nous recevons du monde entier des demandes d'assistance dans la constitution de CERTs. Des collaborateurs de SWITCH donnent en outre, dans le monde entier, des cours de lutte contre la cybercriminalité.

→ SWITCH est membre entre autres des organisations suivantes:
→ FIRST (organisation faîtière mondiale de tous les CERTs)
→ TF-CSIRT (association des CERTs européens)
→ MELANI-Net (plateforme de la Centrale d'enregistrement et d'analyse de la Confédération pour la sûreté de l'information)
→ SISA (Swiss Internet Security Alliance; membre fondateur)

Seconde source d'informations: le Backbone

Les organisations partenaires ne sont cependant pas la seule source d'informations sur les agissements suspects sur Internet. SWITCH est également gestionnaire du Backbone Internet des hautes écoles suisses auxquelles nous ne fournissons pas que les prestations Internet les plus modernes. Nous observons également leur trafic externe sur le réseau pour détecter toute anomalie. Nous analysons ces informations et les mettons en corrélation d'une part avec d'autres propres sources, d'autre part avec celles de partenaires. Nous disposons ainsi d'une image détaillée de la situation locale de danger et des tendances.

Des expériences au profit de toute la Suisse

En tant que cibles principales, les banques ont depuis des années recours aux services de sécurité de SWITCH. Les expériences faites dans le domaine des instituts financiers étendent l'horizon de savoir-faire de SWITCH et profite, en fin de compte, à tout le public suisse.

1991

fut l'année de fondation du CERT (Computer Emergency Response Team) de SWITCH, qui est le plus ancien de Suisse.

Confiance

SWITCH échange, avec des partenaires du monde entier, des informations sur les activités suspectes sur Internet. Ces relations nécessitent la confiance et ont été étendues durant des années.

Backbone

Chez SWITCH, nous entretenons le Backbone Internet des hautes écoles suisses et nous protégeons leur trafic sur le réseau.

A PROPOS DE SWITCH

SWITCH est une fondation créée par la Confédération et les cantons de hautes écoles. En tant que telle, elle est indépendante, neutre et sans but lucratif. Elle a été fondée en 1987 en vue de proposer des services TIC aux hautes écoles. C'est également SWITCH qui, dans cette fonction, a raccordé la Suisse à Internet en 1990.

SWITCH est connue du public comme registrar de domaines Internet .ch de la première heure. Par suite d'un changement dans l'Ordonnance sur les domaines Internet (ODI), SWITCH a peu à peu cédé cette fonction aux registrars au cours de 2015. Nous continuons de tenir la banque de données avec les noms de domaine, ou registry, à la demande de l'Office fédéral de la communication (OFCOM). Il s'agit, selon le Conseil fédéral, d'une infrastructure critique. Si elle tombait en panne, la communication par Internet serait interrompue. Des parties considérables de la vie publique en Suisse seraient pratiquement paralysées. L'Office fédéral pour l'approvisionnement économique du pays (OFAE) nous a attesté que nous exploitions et protégions cette infrastructure de manière optimale.

1987
année de fondation de SWITCH.

1990
SWITCH a raccordé la Suisse à Internet.

Neutre
SWITCH est, du fait de son statut juridique en tant que fondation, indépendante, neutre et sans but lucratif.

Ce qui distingue SWITCH

→ **Pionniers:** Nous avons introduit Internet en Suisse voici bientôt 30 ans et le connaissons en profondeur. Nous avons nous-mêmes constitué la registry.ch. Il n'est guère quelqu'un disposant d'autant de savoir-faire que nous à ce sujet.

→ **Processus bien rodés avec les autorités et fournisseurs d'accès Internet:** Au cours de toutes ces années, nous avons établi une bonne coopération avec les autorités comme l'OFCOM et les autorités de poursuites judiciaires ainsi que les registrars et connaissons leurs besoins. Ensemble, nous avons fait de .ch un des Top-Level Domains les plus sûrs du monde.

→ **Réseau de sécurité international:** Nous disposons depuis 25 ans de notre propre Computer Emergency Response Team (CERT) réputé dans le monde entier et d'un réseau correspondant en Suisse et à l'étranger. Nous profitons de nos longues relations de confiance dans la lutte contre la cybercriminalité. Il faut des années pour établir de telles relations de confiance.

→ **Infrastructure critique:** Avec le DNS, nous exploitons une infrastructure critique qui fonctionne jusqu'à présent de manière stable et fiable. Mais même en cas de crise nationale, nous pouvons garantir que le service continue de fonctionner sous contrôle suisse car l'infrastructure centrale est exploitée en Suisse.

SI DEF 1 2016, Coverphoto: Frank Bruederli

L'objectif doit être de maintenir le haut niveau de sécurité du domaine .ch.

SWITCH
Werdstrasse 2
Case postale
CH-8021 Zurich

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