Security on the Internet

Trends, threats, strategies

SWITCH

Internet landscape: Switzerland going digital at high speed

The Internet can make handling various processes simpler, faster and cheaper compared with physical alternatives. With this in mind, Switzerland's government is pushing ahead to provide the country with high-speed Internet. Some 91% of Swiss households had an Internet connection in 2013. This makes Switzerland one of the best-connected countries in the world.

At the same time, e-government efforts are placing more and more parts of the Federal Administration and the public sector online. The strategic plan for the period 2016–2019 sets the target of the Swiss population being able to register a new place of residence, vote in elections and referendums and pay VAT online by 2019.

Threat landscape: shadow economy flourishing

Criminals are seeking to profit from the steady growth in administrative and business processes being moved to the Internet. In recent years, cybercrime has developed into a highly lucrative sector of the economy that has to be taken seriously. The risk of being caught is relatively small in the virtual realm. A 2014 study by the Center for Strategic and International Studies in Washington concluded that cyberattacks cause damage totalling USD 375–575 billion a year worldwide. By way of comparison, Switzerland's gross domestic product was equivalent to USD 686 billion in 2013.

Cybercrime is diversified

Internet criminals used to favour targeting banks, but their interests are spread much more widely these days. Their focus is currently on the software and technology sector, corporate and consulting services, retail, construction and engineering, and government organisations.

How targets are chosen

The two things that attract cybercriminals most of all are big profits and minimal effort. To achieve the first of these, they are even prepared to use the advanced persistent threat (APT), a labour-intensive approach tailored specifically to an individual target. Once the preserve of spies, APT is now serving a financial purpose. As regards minimal effort, comparatively cheap and versatile malware can now be bought online. One example is the Tinba toolkit, which gave Swiss banks a headache or two in 2015. It costs just a few thousand francs.

USD 375–575 billion

in damage is caused by cybercrime every year, according to the Center for Strategic and International Studies in Washington.

439 million

malware variants currently exist, according to Germany's Federal Office for Information Security. This number is rising fast because programs are being generated automatically.

205

days on average is how long the security firm Mandiant claims it takes to confirm an APT attack after the first evidence is identified. It can sometimes take several years.

.ch: one of the world's most secure domains

We can count ourselves lucky in Switzerland, since a variety of studies have shown that .ch is among the most secure domains in the world. This is no accident. In fact, it is the result of concerted efforts to optimise security at every turn. The .ch registry is backed up by tried-and-tested procedures, long-standing relationships based on trust and expertise built up over many years. The goal must now be to maintain this high level of security for the .ch domain.

World first: outlawing domain misuse

The malware process is right at the heart of the security efforts to protect the top-level domain .ch. The first of its kind in the world, it is an efficient and well rehearsed way of dealing with cybercrime through cooperation between SWITCH, the authorities and the registrars. It was enshrined in Swiss law in 2010. Article 15 of the Ordinance on Internet Domains (OID) provides for a rapid response to suspected misuse of domains. When malware is reported on .ch websites, SWITCH informs the domain owners about the infected sites. If they fail to respond within one working day, SWITCH deactivates the domain names concerned. This means that the infected sites can no longer be accessed, so they can no longer spread viruses, Trojans or other malware. The OID stipulates that sites can be deactivated for five working days.

Exemplary collaboration with authorities

The deactivation period can only be extended by order of an authority accredited by the Federal Office of Communications (OFCOM). Without such an order, SWITCH must reactivate the website after five days. At this point, however, we check the domain holder's identity and forward the matter to the authorities. If the holder neither removes the malware nor provides confirmation of identity within 30 days, SWITCH permanently deletes the domain names affected. This systematic approach makes .ch domains unattractive as a means of spreading malware because it creates a lot of work for the cybercriminals.

Art. 15 OID

is central to the fight against cybercrime in Switzerland, making it possible to neutralise attacks on website visitors in Switzerland quickly.

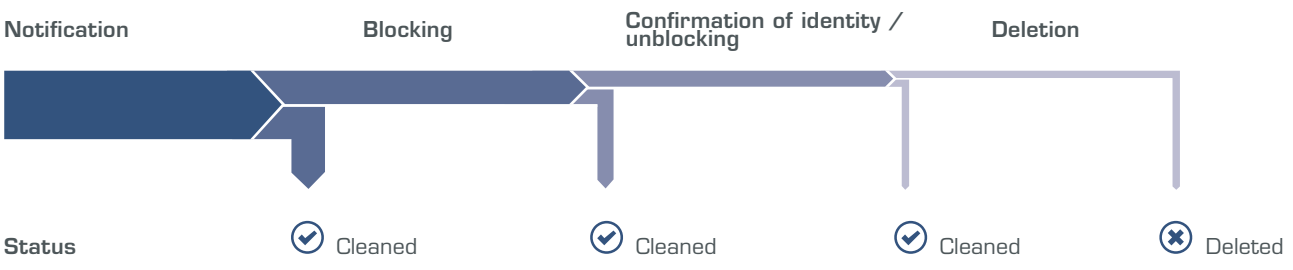
Unique

The .ch registry is the only one in the world that works together with the regulator and other partners to combat malware. This approach has proven its worth as the Swiss top-level domain is among the most secure in the world.

Unattractive

for cybercriminals: it is becoming too expensive for them to keep finding replacements for domains that have been deleted or cleaned in response to malware infections.

Malware process



.ch first for security

As mentioned above, the shadow economy is motivated by minimal effort. When they are looking for top-level domains on which to use their scams, cybercriminals especially favour those that offer low prices and an open registration policy. They should therefore find .ch extremely attractive because it meets both of these criteria. However, a 2015 study by US Internet analysis firm Architelos focusing on the misuse of websites for malware and phishing in Europe put .ch in first place for security among the top-level domains. This makes it clear that all the hard work being done to keep .ch secure is bearing fruit. The goal must now be to maintain this high level of security for the Swiss registry and ensure that security measures always keep pace with the fast-moving world of cybercrime.

Security at SWITCH: ISO-certified and award-winning

Keeping the .ch registry secure is one of SWITCH's core tasks. We are aided by an established information security management system (ISMS) that continuously checks and optimises security. It was certified according to ISO 27001 in 2014. We are working together with our counterparts in Austria and Germany to review each other's registry security procedures. In October 2015, we won the the CENTR Security Award for this cooperation. CENTR is the Council of European National Top Level Domain Registries.

CENTR

The Council of European National Top Level Domain Registries presented SWITCH with its Security Award in October 2015.

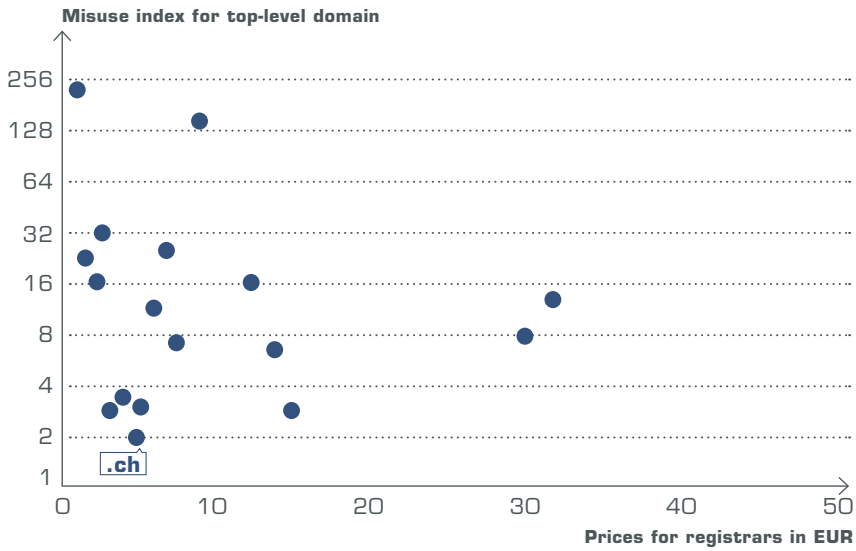
DNSSec

The cryptographic keys for .ch are hosted by SWITCH in Switzerland. These are signatures for secure https domains that are particularly hard to hack.

ISO-27001

is an international standard for information security management systems (ISMSs) like the one used for the .ch registry. SWITCH is continually working to optimise its ISMS.

Price/security profiles of European registries



The chart shows that, among the European registries with an open policy, .ch is in first place for security.

Statistics compiled by Architelos; the registries are not named for reasons of confidentiality.

Help for administrators of hacked websites

Website administrators are usually surprised to find out that their websites are spreading harmful content. They are victims of cybercrime. SWITCH tells them how to get rid of malware. In 2015, SWITCH identified 761 cases of malware on .ch websites. In most of these cases (556, to be exact), the domain holder removed the malicious code immediately after being informed for the first time.

Strategies to combat phishing

Phishing is an attempt to gain access to confidential information by illegal means. SWITCH identified a total of 320 such cases in 2015. Given the rapid growth in cases worldwide, SWITCH expanded its malware process in 2014 to combat phishing as well. This has proven successful: we are not currently seeing an increase in phishing on .ch.

Security is our mission

To keep the top-level domain .ch clean, the Swiss population must be informed about the risks lurking in cyberspace. They must know how to protect themselves efficiently. With this in mind, SWITCH helped to form the Swiss Internet Security Alliance (SISA – www.swiss-isa.ch) in 2014. SISA brings together key players from the telecom and Internet industry with the aim of reducing the damage caused by cybercrime. We have also created our own informative website, www.switch.ch/safer-internet, with tips on how to guard against attacks.

761

cases of malware being spread via websites were identified by SWITCH in 2015.

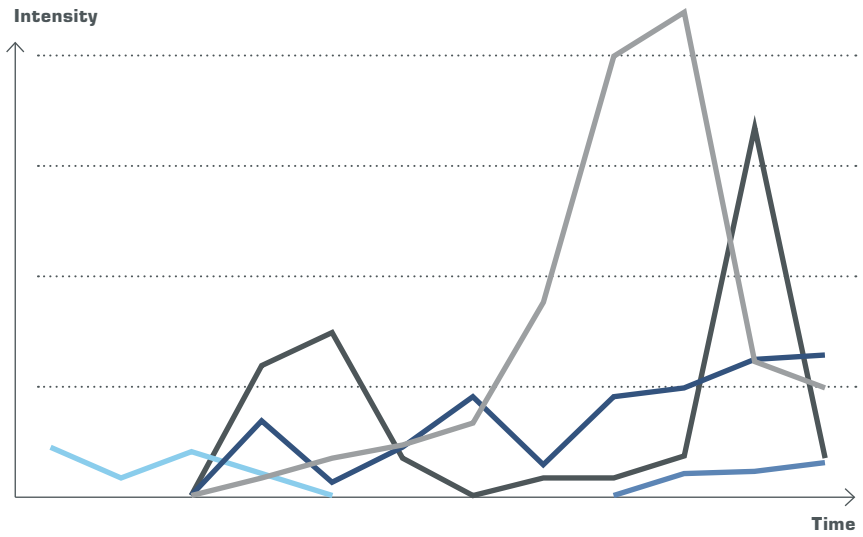
320

cases of phishing were identified by SWITCH in 2015. SWITCH blocked the domain in 53 of these. SWITCH intends to step up its efforts to combat phishing in cooperation with international partners.

SISA

was co-founded by SWITCH. The Swiss Internet Security Alliance brings together key players from the Swiss telecom and Internet industry in the fight against cybercrime.

Malware trends



Different malware families exhibit different trend profiles. The chart shows some examples of attacks recorded in Switzerland over the course of a year.

How SWITCH gets the information

Knowing which .ch websites are infected is essential for eliminating malware. We at SWITCH have this information because we are part of a global alerting and knowledge transfer network. The reason we are in this privileged situation is that, in addition to operating the .ch registry, we also have our own Computer Emergency Response Team (CERT), which dates back to 1991. This means that we have more experience than any other Swiss organisation when it comes to fighting threats in cyberspace. SWITCH's CERT enjoys a good reputation internationally. People from around the globe ask us to help them set up their CERTs. SWITCH staff also provide training worldwide to help people fight cybercrime.

SWITCH is a member of the following organisations, among others:
→ FIRST (the global umbrella organisation for all CERTs)
→ TF-CSIRT (the association of European CERTs)
→ MELANI-Net (the Swiss government's Reporting and Analysis Centre for Information Assurance)
→ SISA (Swiss Internet Security Alliance; founding member)

1991

was the year SWITCH set up its CERT (Computer Emergency Response Team). It is the oldest one in Switzerland

Trust

SWITCH shares information about suspicious activity on the Internet with partners all over the world. These relationships are based on trust that has been built up over many years.

Backbone

We at SWITCH operate the Swiss universities' Internet backbone. We safeguard their network traffic.

Our second source of information: the backbone

Partner organisations are not our only source of information about suspicious activity on the Internet. SWITCH also operates the Swiss universities' Internet backbone. As well as providing the universities with the latest Internet services, we also monitor their external network traffic for anomalies. We analyse this information and correlate it with other in-house sources as well as those of our partners. This gives us a detailed picture of the current threat situation locally and the overarching trends.

Experience that benefits the whole of Switzerland

Being prime targets, banks have been calling on security services from SWITCH for years. Our experience in the financial services field has broadened the horizons of SWITCH's know-how, which is ultimately beneficial to the entire Swiss population.

About SWITCH

SWITCH is a foundation created by the federal government and the cantons that have universities. As such, it is independent, neutral and not geared to making a profit. It was formed in 1987 to provide ICT services to the universities. In this capacity, SWITCH was also responsible for connecting Switzerland to the Internet in 1990.

The general public knows SWITCH best as the original registrar for .ch Internet domains. Following a revision of the Ordinance on Internet Domains (OID), we successively handed this function over to the new registrars during the course of 2015. We continue to manage the database of domain names – the registry – under a mandate from the Federal Office of Communications (OFCOM). The Federal Council regards the registry as a critical infrastructure because Internet communication would be interrupted if it were to fail, which would practically bring large parts of public life in Switzerland to a standstill. The Federal Office for National Economic Supply (FONES) has attested that we do an outstanding job of operating and protecting this infrastructure.

1987
was the year SWITCH was formed.

1990
was the year SWITCH brought the Internet to Switzerland.

Neutral
SWITCH's legal structure as a foundation means that it is independent, neutral and not geared to making a profit.

What sets SWITCH apart

→ **Pioneers:** We brought the Internet to Switzerland almost 30 years ago and know it inside out. We built up the .ch registry ourselves. Hardly anyone can match our know-how on this subject.

→ **Proven processes in cooperation with authorities and Internet service providers:** Over the years, we have established good working relationships with authorities such as OFCOM and criminal prosecutors as well as the registrars, so we know all about their needs. Together, we have made .ch one of the most secure top-level domains in the world.

→ **International security network:** We have had our own world-renowned Computer Emergency Response Team (CERT) for 25 years, with a network to back it up both in Switzerland and worldwide. Our long-standing relationships built on trust help us in the fight against cybercrime. It takes years to cement relationships like these.

→ **Critical Infrastructure:** We operate the DNS, a critical infrastructure running as stably and reliably now as it always has. Even in the midst of a national crisis, we can guarantee that the service will continue to function under Swiss control because the core infrastructure is operated inside Switzerland.

SI DEF 1 2016, Coverphoto: Frank Bruederli

The goal must be to maintain the high level of security for the .ch domain.

SWITCH
Werdstrasse 2
P.O. Box
CH-8021 Zurich

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