

Collaboration: Key to Keep a Nation Safe



SWITCH

Michael Hausding
Dr. Serge Droz

michael.hausding@switch.ch
serge.droz@switch.ch

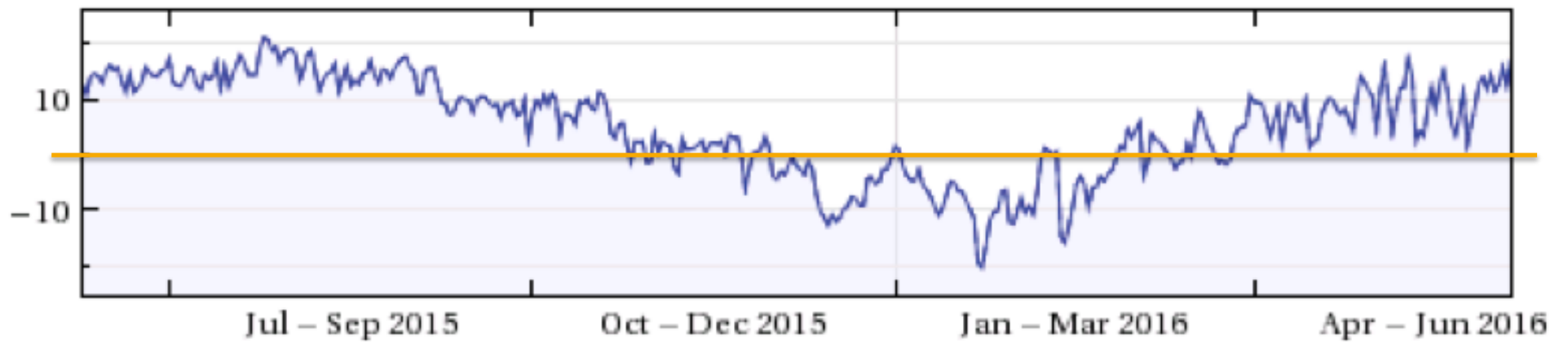
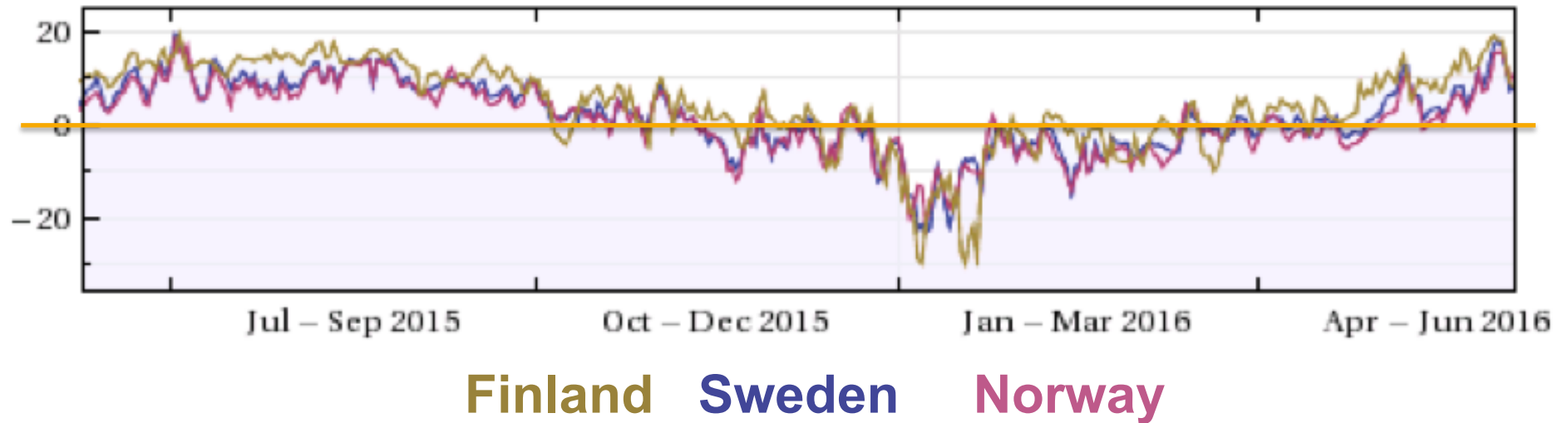
Seoul, 17.6.2016

COUNTRIES WITH THE LOWEST RATES OF INFECTION IN THE FIRST QUARTER OF 2016

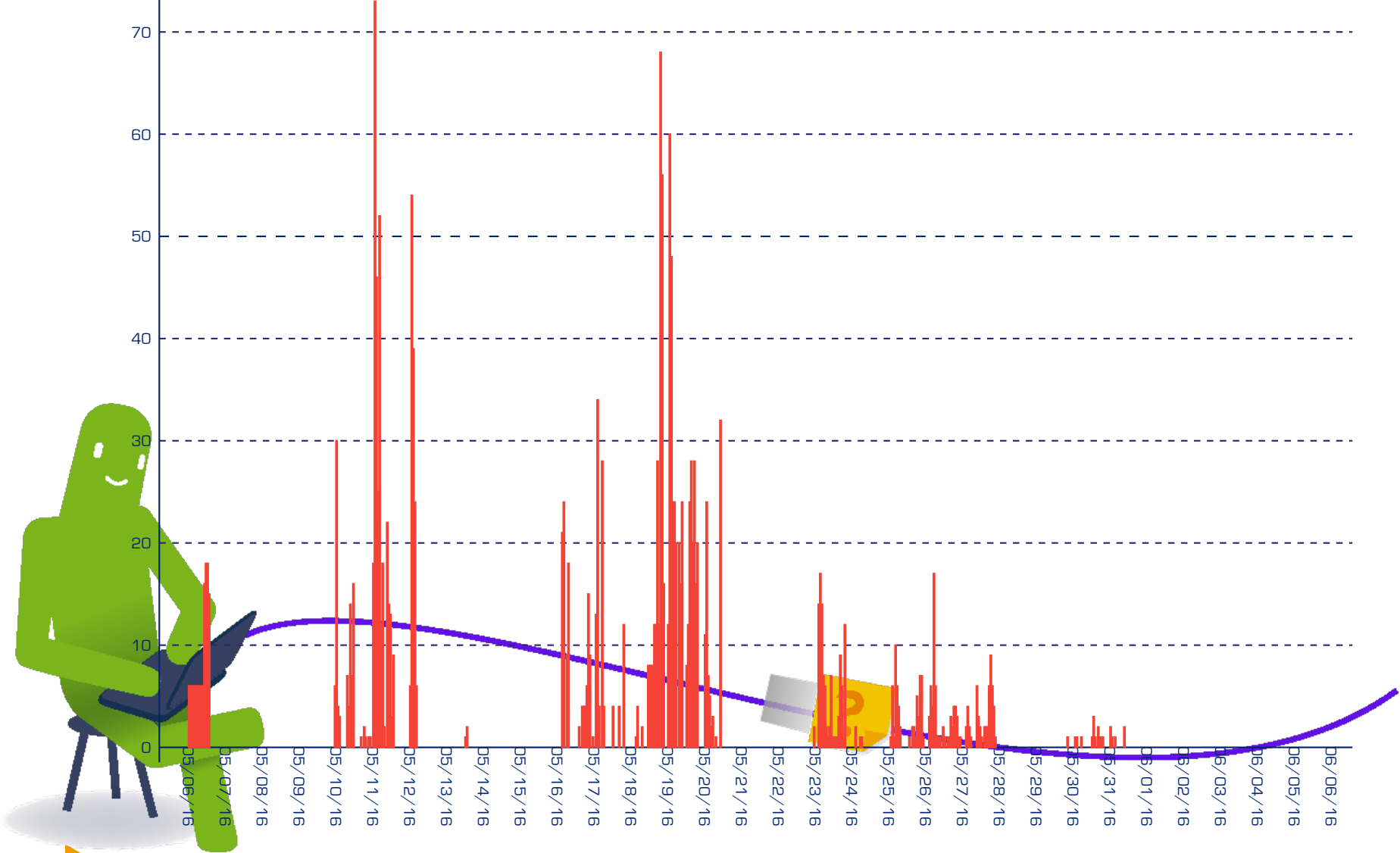


<http://www.pandasecurity.com/mediacenter/news/pandalabs-study-q1/>

Temperature



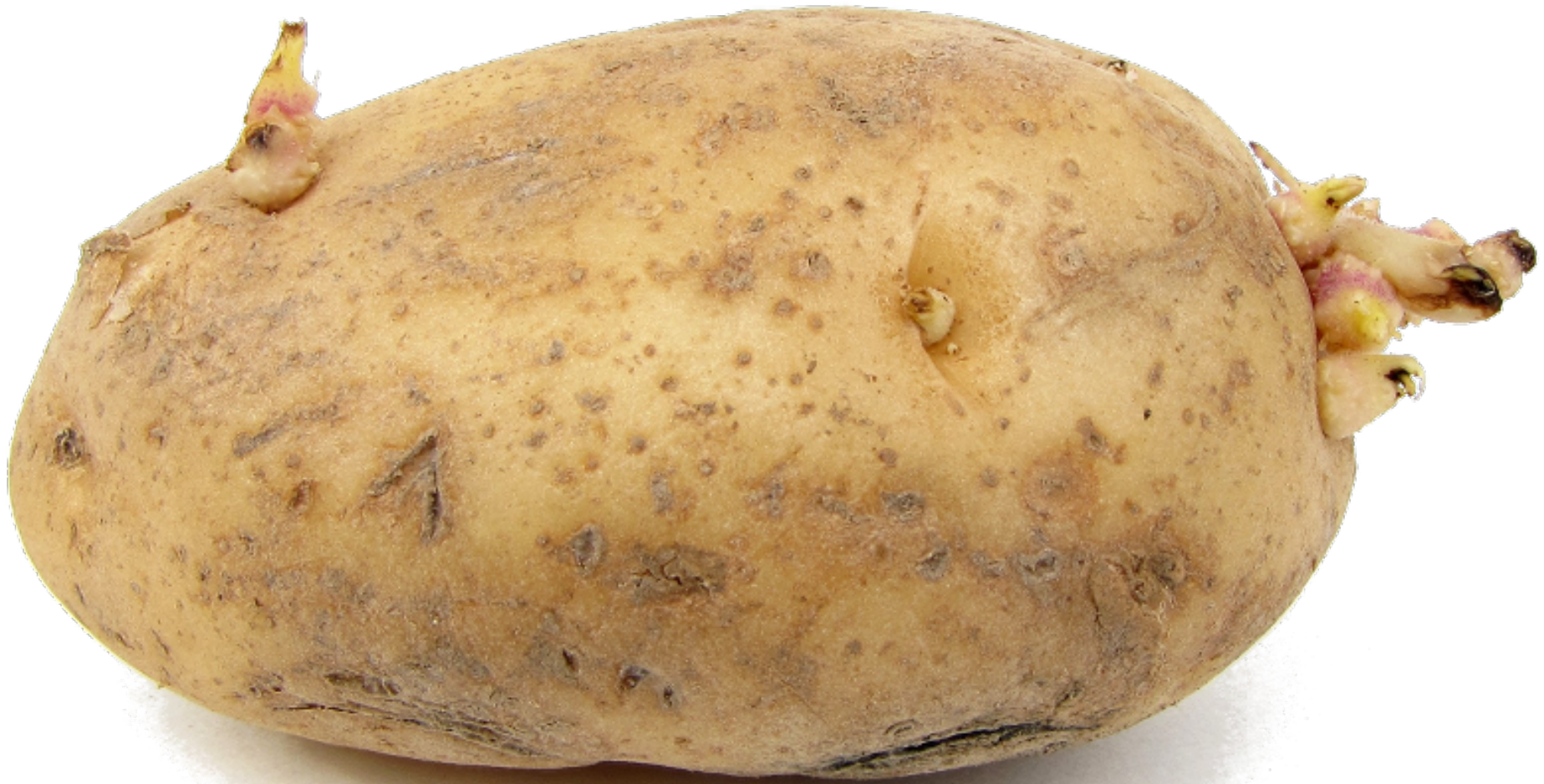
Infection Path



DriveBy



Traditional IH Process



Wrong Question!

Stop the blame game!
Act!

The internet underground is financially driven!

Sabotage the criminals business case!

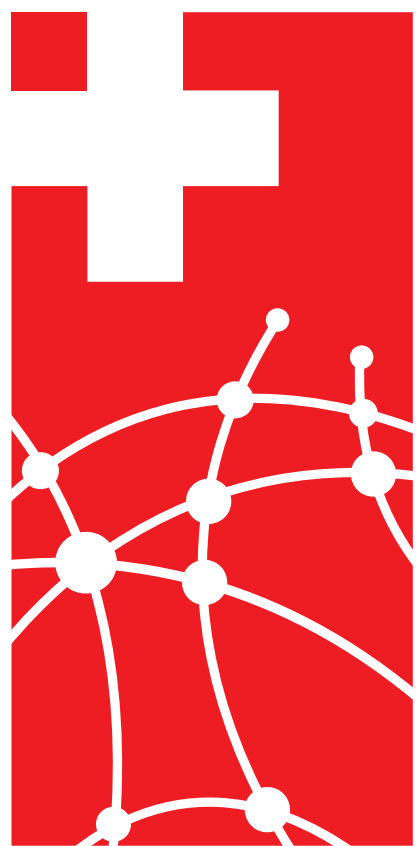
Collaboration

Every player has unique possibilities to interrupt the criminal value chain!

- Bank Customer: Be careful
- Bank: Detect and stop fraud
- ISP: Block, mitigate help customers
- Hostler: Mitigate
- Website Owner: Protect
- Registry: Mitigate
- Registrar: Mitigate
- Government: Create ground for action

Weak players

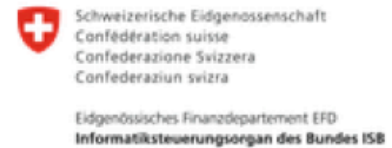
- **Bank Customer: Be careful**
- Bank: Detect and stop fraud
- ISP: Block, mitigate help customers
- Hostler: Mitigate
- **Website Owner: Protect**
- Registry: Mitigate
- Registrar: Mitigate
- Government: Create ground for action



SWISS INTERNET SECURITY ALLIANCE



@Banking but secure!







Focus: Enduser

**Empower to keep is
systems clean!**



Free (online) tools too:

- Check router settings
- Browser plugins
- 2nd opinion scanner

Member goodies

May refer customer to check with an identifier

Receive the results to better support customer



Cooperation for Awareness

Awareness



STOP

THINK

CONNECT™



de / fr

Cyberkriminelle haben die Erpressung für sich entdeckt. Mit Verschlüsselungstrojanern, sogenannter Ransomware, machen Sie Daten von Privatpersonen und Firmen unzugänglich. Um die eigenen Daten zurückzubekommen, fordern sie von ihren Opfern hohe Lösegelder und erzielen damit Gewinne in Millionenhöhe.

Was ist Ransomware?

Ransomware bezeichnet Schadsoftware (Viren), welche Dateien auf dem befallenen

Weitere Informationen

- [Merkblatt von MELANI](#)
- [Detaillierte technische Information \(in Englisch\)](#)
- [Schutz für Mac OS](#)
- [Informationen zu Erpressungen im Internet](#)

Partner

Diese Kampagne wird in Zusammenarbeit mit folgenden Partnern durchgeführt:



Melde- und Analysestelle Informationssicherheit



Staatssekretariat für Wirtschaft SECO



SWITCH



CERN



Stiftung für Konsumentenschutz



Schweizerischer KMU Verband



Schweizerische Kriminalprävention



eBanking - aber sicher!



Kantonspolizei Zürich



Scuola universitaria professionale della Svizzera italiana



Symantec Schweiz



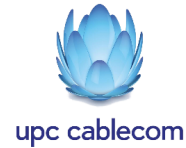
Trendmicro Schweiz



Swisscom



Sunrise



upc cablecom



HOSTPOINT



PostFinance



Hochschule Luzern



Zürcher Hochschule der Künste



ISOC Switzerland Chapter



CERT.at

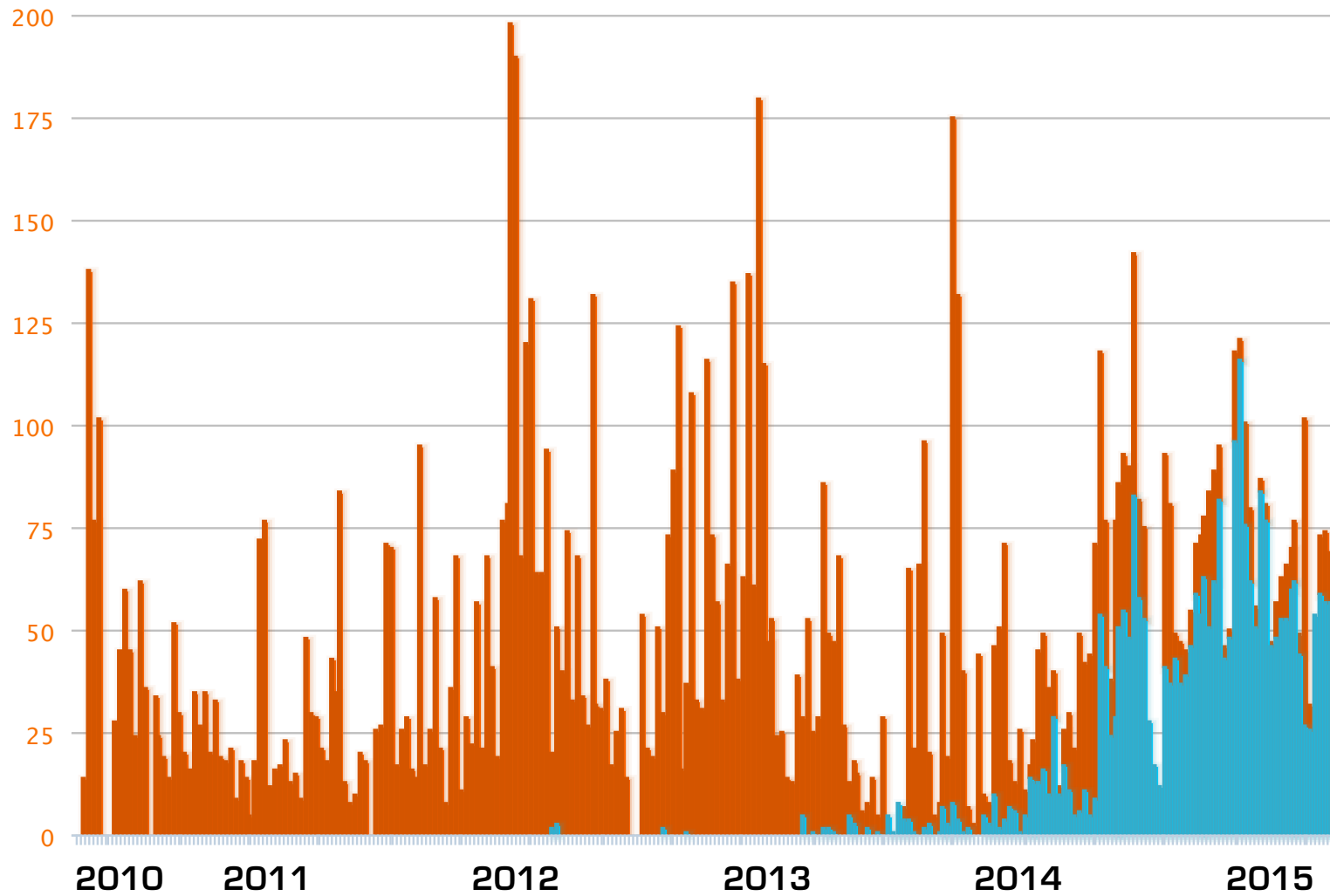


Microsoft Malware Protection Center



Cooperation against Phishing

ch/li ccTLD misuse





[Startseite](#) | [Informationen](#) | [Kontakt](#)

Haben Sie ein Phishing E-Mail erhalten?

Leiten Sie Phishing E-Mails an reports@antiphishing.ch weiter.

Achtung: Diese Mailbox wird nicht gelesen sondern maschinell verarbeitet. Falls Sie eine Anfrage haben und / oder eine Antwort von MELANI wünschen, wenden Sie sich bitte an reply@melani.admin.ch oder verwenden Sie das [MELANI Meldeformular](#).

Haben Sie eine Phishing-Seite gefunden?

Melden Sie Phishing-Seiten via Web-Formular:

Über antiphishing.ch

antiphishing.ch wird von der [Melde- und Analysestelle Informationssicherheit MELANI](#) des Bundes betrieben, um der Bevölkerung eine einfache Möglichkeit zu geben, Phishing-Versuche zu melden.

Report phishing

You can help us fight phishing by using the simple form below to report e-mails. Your report will be analysed by security experts at SWITCH, and measures will be taken to block dangerous websites as soon as possible. Web browsers will get updates of known phishing pages, thus protecting users.

Please report your phishing mail using the form below:

Sender: Michael Hausding <michael.hausding@switch.ch> *(Information from your AAI login)*

URL:

Dangerous URL contained in the phishing mail:

[Click here to learn how to extract this URL from your e-mail program.](#)

E-mail: [▶ Click here to show a box where you can paste in the full e-mail you received.](#)
[optional]

Phish Reports

- End users (via antiphishing.ch)
- University users
- Spamtraps
- Community (APWG, CERTs, SISA)

Detection



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verification



Takedown & Notice



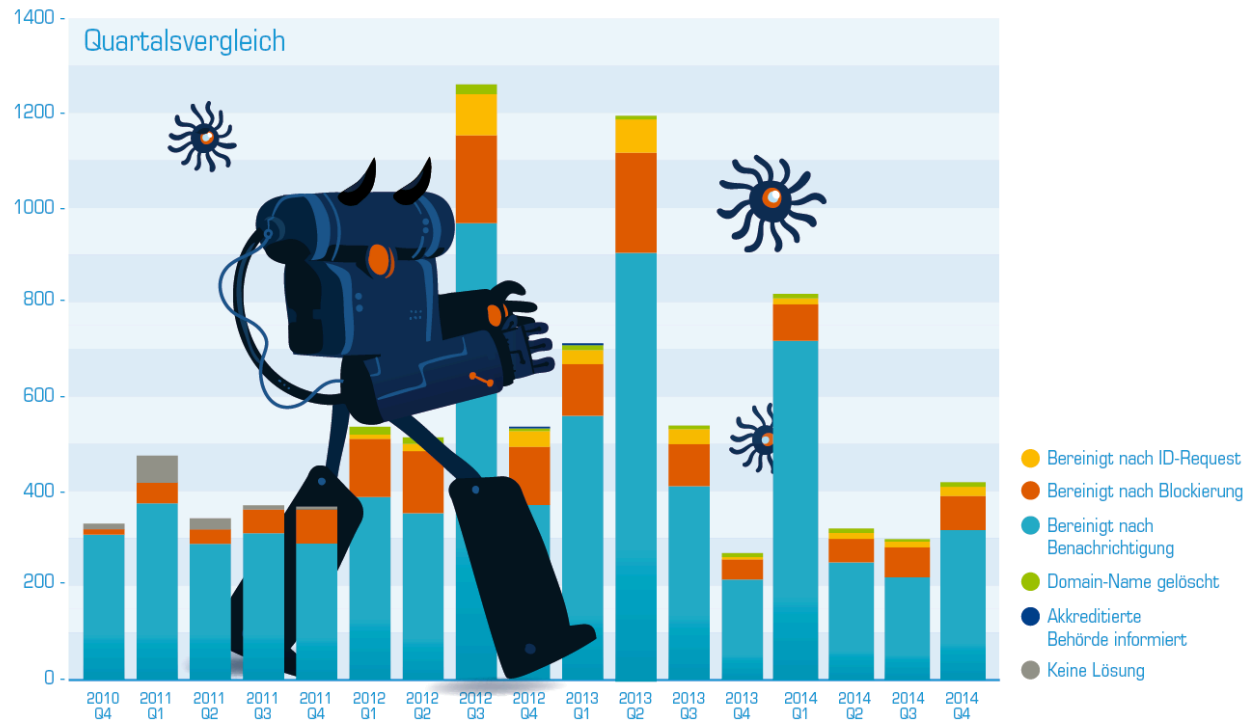
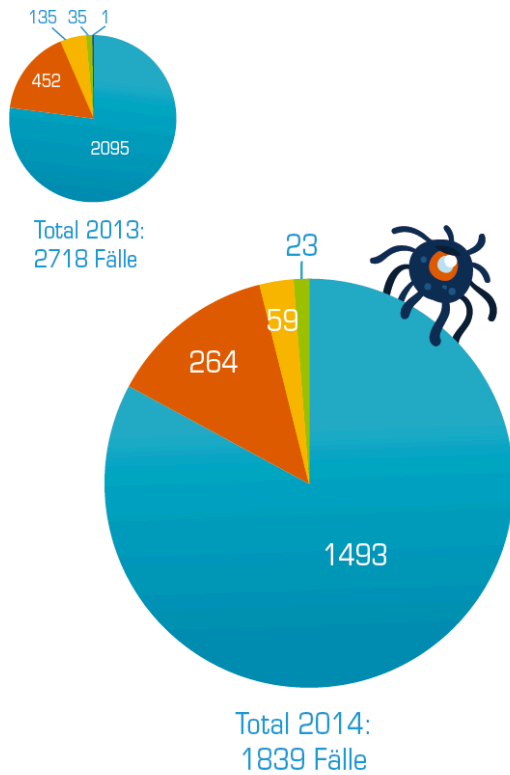
Filtering



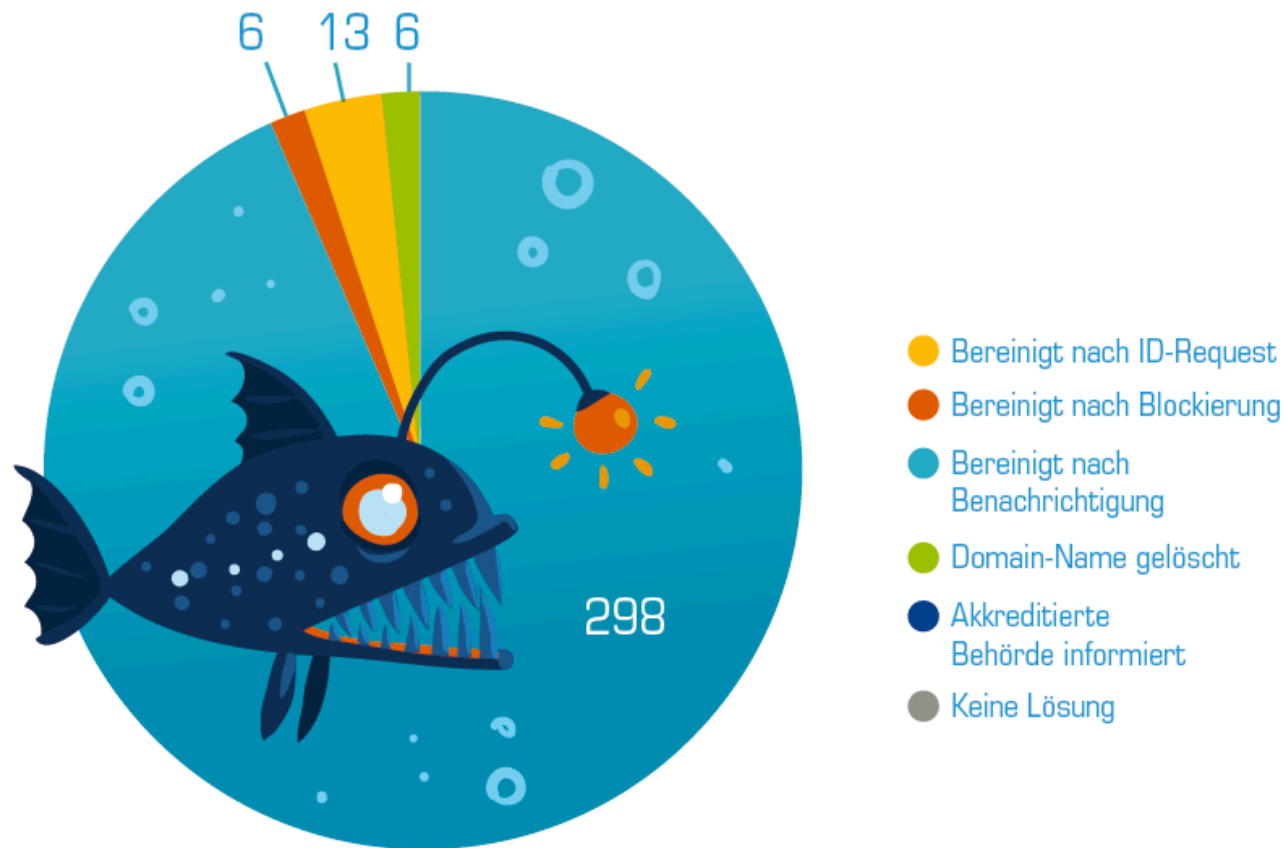


Cooperation for a Safer Internet

Malware-Bekämpfung in der Schweiz



Phishing Domains 2014



Total 2014:
323 Fälle



25'000

Reported Domains
processed

12'000

Misused Domains
cleaned

Take or buy?

7

Bought

11'993

Domains taken



1. Awareness

2. Domain Abuse Process

3. Working with Partners



1. Awareness

Safer Internet

Your website

Drive-by

Phishing

Other Threats

Advices

Secure websites for a safer Internet

The best websites attract lots of visitors – some of whom they could well do without. Internet criminals are increasingly exploiting third-party websites to spread malware such as viruses and Trojans or to gain access to protected data including login details and passwords.



Websites infected by malware cause immense damage online. Making

[Safer Internet](#)[Your website](#)[Drive-by](#)[Phishing](#)[Other Threats](#)[Advices](#)

Make your website safer

Internet crime has taken on a new, particularly sophisticated and professional dimension with drive-by infections and new phishing methods. Protecting against these requires a careful approach and precautionary measures.



Tip 1: Get professional support for your website

Always use a dependable, trusted partner to develop and operate your website. Choose your registrar and hosting provider with care. When you first commission your website, discuss security issues with your webmaster or agency.



2. Domain Abuse Process

Notification Emails

- From: SWITCH - Safer Internet <cert@switch.ch>
- Subject: [SWITCH-CERT #271111] Missuse of your website test[.]ch
- Subject: [SWITCH-CERT #271111] Missuse of your website test[.]ch stopped
- Different RTIR# for each role

Notification emails

notification emails go to “case contacts”:

- Registrar
- Tech-c (if in whois)
- Domain holder (opt-out for first email)
- Webhoster (if identified by SOA)


All “Case contacts” will get email-updates

Notification to domain holder

“Please get in touch with your technical contact, hosting provider or registrar as soon as possible.”

Antwort an: SWITCH - Safer Internet

[SWITCH-CERT #276908] Missuse of your website test[.]ch

Sicherheit:  Signiert (michael.hausding@switch.ch)



Pour la version française, voir plus bas.
Per la versione italiana vedi in basso.
Please see below for english version.

Sehr geehrte(r) Hoster

Sie sind als Hoster für den Domain-Namen test[.]ch eingetragen.

Wir haben festgestellt, dass die Webseite test[.]ch für Drive-By missbraucht wird.

Wir möchten Sie bitten den Missbrauch bis 28.8.2015 17:46 zu beseitigen.

Sollten ihre Webseite am 28.8.2015 17:46 immer noch missbraucht werden, wird der Domain-Name von SWITCH zum Schutz der Internetnutzer vorübergehend deaktiviert.

Die genauen Informationen zu diesem Missbrauch, alle betroffenen URLs, den aktuellen Status sowie die für greg[.]ch eingetragenen Kontakte finden sie auf <https://www-test.switch.ch/de/saferinternet/domainstatus/?domain=test.ch&auth=276908>.

Kontaktstelle Safer Internet

saferinternet@switch.ch

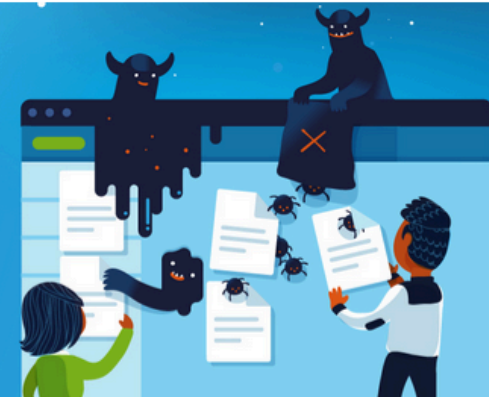
<http://www.switch.ch/de/saferinternet>



Status Portal

Domain Misuse

Hacked websites cause a huge amount of damage online. SWITCH's Status Portal informs affected owners of domains and helps to minimise risks for Internet users.



Status for domain name fischerei-bedarf.ch

⊖ Your website is being misused for Drive-By.

What has to be done?

Remove the Drive-By infection from all the URLs listed below with the aid of your technical contact (tech-c), hosting provider or registrar. Their contact details are shown below.

You can let us know directly here as soon as you have cleaned your website. SWITCH will then check your website again and tell you the result.

[Check website again](#)

About SWITCH's role as registry

SWITCH acts as registry for domain names ending in .ch and .li.

[Further info](#)

About the domain name misuse process

Working on behalf of the Swiss Federal Office of
Communication (OFCOM) and the Swiss Federal Office of
Culture (CFCM).

Current status of misuse for Drive-By


Our analysis results for each URL checked:

 **hxxp://fischerei-bedarf.ch**

- IP: 62.75.143.243
- Misused for: Drive-By
- Last checked: 2015-09-15 14:36
- Result: <https://misc.www.switch.ch/saferinternet/reports/drive-by/UV742GJ68eQomhowo409Guc8.html>

Blocking information

Domain name deactivation

 We have identified misuse of fischerei-bedarf.ch for Drive-By.

Please clean your website within one working day. If you fail to do so, SWITCH will temporarily deactivate your domain name as of 2015-09-16 14:37.

Blocklist information

 The domain name fischerei-bedarf.ch is not in the [Safe Browsing blocklist](#) . You can see any other potential blocklist entries [here](#) .

hxxp://fischerei-bedarf.ch/

Notice from our analyst:

Malicious external frame on line 1: hxxp://hwpszz.tefjbjtiozhgrx.gq:3778/colour/home-medical-granny-34131966

Malicious (i)frames found on line 1:

```
<iframe height="250" src="hxxp://hwpszz.tefjbjtiozhgrx.gq:3778/colour/home-medical-granny-34131966" width="250"></iframe>
```

Technical details

URL	hxxp://fischerei-bedarf.ch/
IP	62.75.143.243
Date and time	15.09.2015 at 14:35 CEST
Request header	Referer: hxxp://www.google.ch/search?q=&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official Accept-Encoding: gzip, deflate Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.2)
Response status	200
Response header	content-length: 4977 pragma: no-cache content-encoding: gzip set-cookie: _PHP_SESSION_PHP=832; expires=Tue, 22-Sep-2015 12:35:53 GMT; path=/ 76f3245fc1ba4d3076daadd36a4f727b=6v4156otijnvmpaskugk0ua9o5; path=/; HttpOnly expires: Mon, 1 Jan 2001 00:00:00 GMT vary: Accept-Encoding server: Apache/2.2.22 (Ubuntu) last-modified: Tue, 15 Sep 2015 12:35:54 GMT server_ip: 62.75.143.243 cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 date: Tue, 15 Sep 2015 12:35:53 GMT p3p: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM" x-powered-by: PHP/5.3.10-1ubuntu3.19 content-type: text/html; charset=utf-8

Response body (click inside the text and scroll to see the whole content)

On 11.09.2015 11:22 the following URL was visited:
<http://serviceclients.sav-services.ch/>



Adresse e-mail :

Mot de passe

Date de naissance

Jour ▼ Mois ▼ Année ▼

[2014 2015 SUNRISE COMMUNICATIONS SA](#)

Contact information

Domain holder

Bekri Lika

Phone number:

E-mail: @gmail.com

Technical contact

Bekri Lika

Phone number:

E-mail: @gmail.com

Hosting provider

ipage.com

Registrar

Desk Help

GoDaddy.com, LLC

<http://www.godaddy.com> 

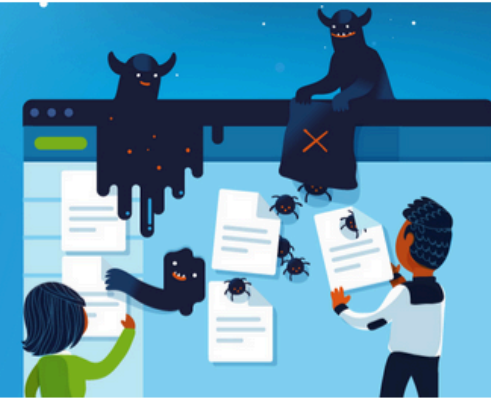
Phone number: +1 4805058800

E-mail: nicola.wirczakowski@switch.ch

E-mail: HQ@godaddy.com

Domain Misuse

Hacked websites cause a huge amount of damage online. SWITCH's Status Portal informs affected owners of domains and helps to minimise risks for Internet users.



Status for domain name fischerei-bedarf.ch

⊖ Your website is being misused for Drive-By.

What has to be done?

Remove the Drive-By infection from all the URLs listed below with the aid of your technical contact (tech-c), hosting provider or registrar. Their contact details are shown below.

You can let us know directly here as soon as you have cleaned your website. SWITCH will then check your website again and tell you the result.

[Check website again](#)

About SWITCH's role as registry

SWITCH acts as registry for domain names ending in .ch and .li.

[Further info](#)

About the domain name misuse process

Working on behalf of the Swiss Federal Office of
Communication (SFCOM) and the Swiss Federal Office of
Information Security (SFCIS).



3. Working with Partners

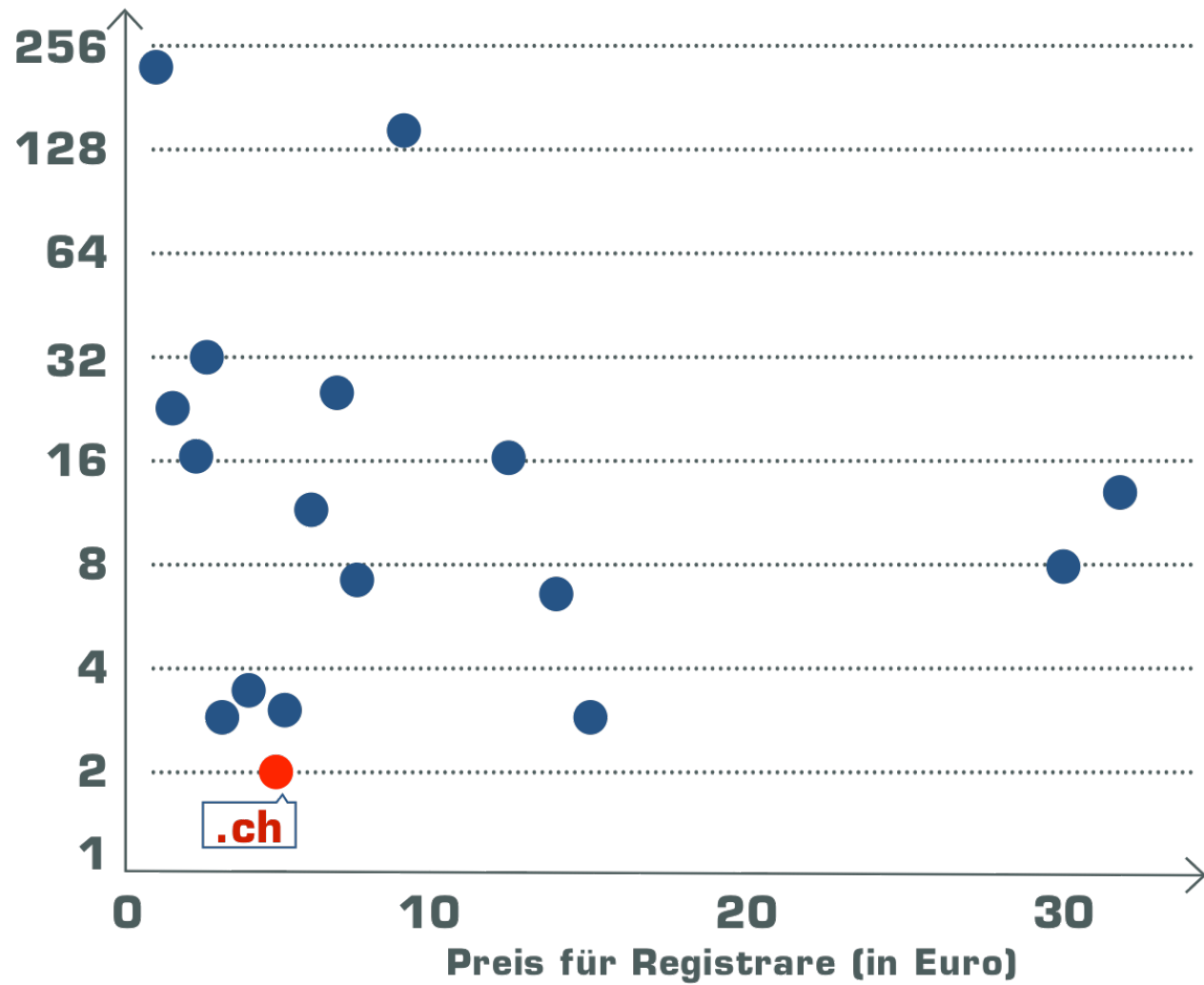
Working with Partners

- Registrars
- Webhoster
- Swiss Internet Security Alliance (SISA)
- Data Feed Providers
- CMS Community

Working with Partners II

- Meetings twice a year
- Information about domain abuse process
- Listen to feedback
- Exchange data
- Discuss best practices
- Share information
- Trainings (planned)

Misuse of Domain Names





Share your data

cert@switch.ch

michael.hausding@switch.ch

serge.droz@switch.ch



<http://securityblog.switch.ch/>