Take or Buy

DNS and Domain Abuse in Switzerland

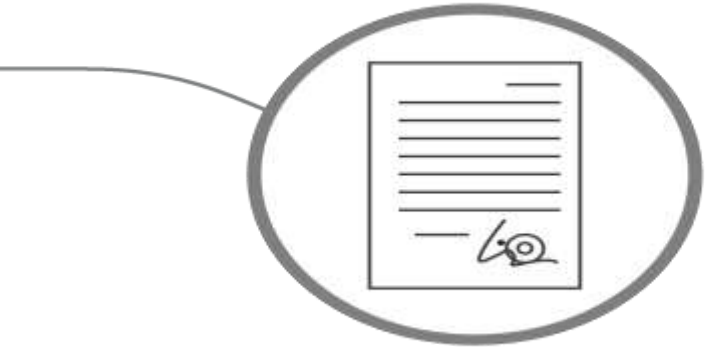
SWITCH

Michael Hausding
michael.hausding@switch.ch
@mhausding

Cyberchess Riga, 5.10.2017

Foundation purpose

Excerpt from the deed of foundation
Berne, 22 October 1987



"The foundation has as its objective to create, promote and offer the necessary basis for the effective use of modern methods of telecomputing in teaching and research in Switzerland, to be involved in and to support such methods.

It is a non-profit foundation that does not pursue commercial targets."

Registry for .ch and .li

SWITCH - Registry for .ch

- **Registry for .ch for 25 years**
- **Contract with the office of communication**
- **5 year contract (2017-2021)**


jp
jp
jp
fr
fr
net
net
net
de
de
gov
gov
biz
biz
biz
name
name
no
no
dk
dk
es
es
org
org
org
fi
fi
info
info
info
com
com
com
se
se
se
mobi
mobi

“The key to any online presence is the domain name”

https://www.verisign.com/en_US/website-presence/online/choose-a-domain-name/index.xhtml

Internet criminals need domain names

Criminals need domain names for

- Phishing
- Malware
- CC
- Social engineering
- Fraud
- Infrastructure
- Ransomware
- ……

To get access to domain names criminals need to make a decision

Take or Buy


jp
jp
jp
fr
net
de
gov
biz
biz
no
dk
info
info
com
com
se
se
org
org
name
fi
fi
mobi

Take

Criminals take domain names by

- **Domain Hijacking**
- **DNS compromise (shadowing)**
- **Web Compromise**

Criminals take domain names for

- Phishing
- Malware
- CC
- Social engineering
- Fraud
- Click fraud
- Dropzones

Criminals take domain names for

- **Short periods**
- **A few hours to days**

- **Web hosters and domain owners clean up fast**


jp
jp
jp
net
de
gov
biz
biz
org
org
name
no
dk
info
info
com
com
se
se
mobi
fi

Buy

Criminals buy domain names with

- **Faked identities**
- **Stolen identities**
- **Stolen CC**
- **Crypto currencies**

Criminals buy domain names for

- Phishing
- CC
- Social engineering
- Fraud
- DNS
- Infrastructure
- Ransomware

Criminals buy domain names for

- **Short periods (phishing)**
- **Longer periods**
- **Sometimes they can use them for years**

The answer from the domain name industry:

“Complaints about website content are outside of ICANN's scope and authority”

https://www.icann.org/resources/pages/content-2013-05-03-en

Suggested Solutions by ICANN

- You may want to contact a law enforcement agency in your jurisdiction
- You may want to file a complaint with a consumer protection entity such as the International Consumer Protection and Enforcement Network or the US Federal Trade Commission
- You may want to contact the website's Internet Service Provider
- You may want to contact the registrar of the website's domain name

Domain Abuse in Switzerland (.ch)

Situation for .ch in Switzerland

- .ch is a ccTLD
- .ch under a single, Swiss jurisdiction
- .ch is regulated by OFCOM
- Regulation on domain names

- SWITCH runs the ccTLD .ch and .li
- Home for SWITCH-CERT

Regulation on domain names

- **The registry has a active role in fighting domain abuse:**
  - **Phishing**
  - **Malware**
  - **Support of Phishing or Malware**

- **May support authorities in other cases**

https://www.bakom.admin.ch/bakom/de/home/das-bakom/organisation/rechtliche-grundlagen/verordnungen/internet.html

The registry is allowed

- Suspend a domain name for 5 days
- For 30 days with confirmation from MELANI
- Request the identity of the domain holder
- Delete domain name after 30 days
- Sinkhole domain name for 5 days
- Sample domain names from DGAs to sinkholes

https://www.bakom.admin.ch/bakom/de/home/das-bakom/organisation/rechtliche-grundlagen/verordnungen/internet.html

Take

Activities against compromised domain names and websites


SWITCH
Domain holders are victims of cybercrime

Domain holders need to take action!

Safer Internet - SWITCH

Michael

SWITCH [CH] https://www.switch.ch/saferinternet/

SWITCH

EN

Safer Internet | Your website | Drive-by | Phishing | Other Threats | Advices | Search

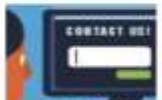
Secure websites for a safer Internet

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 the Internet safe in Switzerland and Liechtenstein is one of SWITCH's core tasks, hence the decision to launch this Safer Internet website with information about preventing the misuse of domain names. The site explains why websites are being targeted more and more frequently, the threats that exist and how you can protect your own website and your visitors.

If you would like to know more about security for computers and mobile devices, please take a

Contact

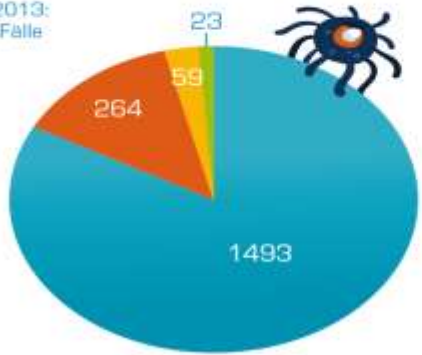


Contact point Safer Internet

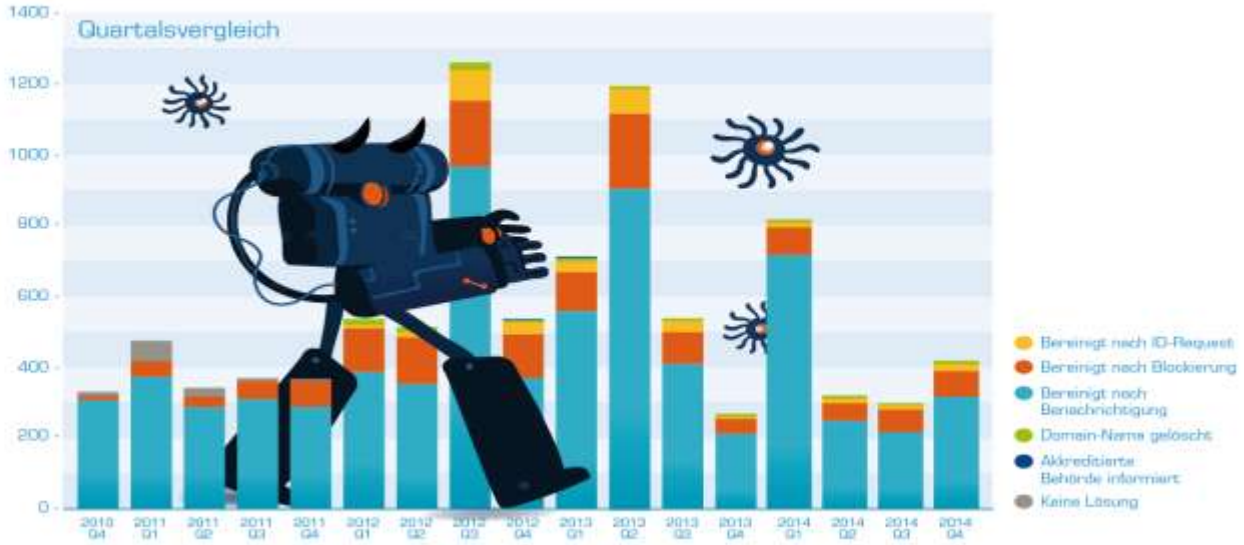
Malware-Bekämpfung in der Schweiz

SWITCH

Total 2013:
2718 Fälle



Total 2014:
1839 Fälle



Activities against compromises

- **Awareness**
- **Cleanup process**
- **Partner with registrars and hosters**
- **Suspension if no action after 24 hours**

SWITCH Security Blog

94 .ch & .li domain names hijacked and used for drive-by

07/07/2017 by Michael Hausding | 16 Comments

★★★★★ 9 Votes

A Swiss domain holder called us today telling us that the .ch zone points to the wrong name servers for his domain.

The NS entries were ns1.dnshost[.]ga and ns2.dnshost[.]ga. We contacted the registrar and soon realized that this is not the only domain that had unauthorized changes. We identified 93 additional .ch and .li domain names that pointed to the two rogue name servers. While domain hijacking by pointing to a rogue NS is a known attack, 94 domains on a single day is very unusual. So we

SEARCH

FOLLOW US VIA RSS-FEED

RSS - Posts

RECENT POSTS

- A new issue of our SWITCH Security Report is available!
- 11th October 2017, DNSSEC key rollover of the root zone, be ready the key is here!

Buy

Activities against malicious registrations

>99% correlation between complaints on website content and registrations with faked or stolen identities

ONLINE PHARMACY
ONE OF THE BEST DRUG STORES

About us | Bestsellers | Testimonials | FAQ | Policy | Contact us

OUR DRUG PRICES
ARE 70%
LESS THAN IN YOUR LOCAL PHARMACY

This content requires the Flash Player. Download Flash Player. Already have Flash Player? Click here.

Quick search

For example: Viagra

Search Drugs by First Letter

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Change language

English

Special Offer

Bestsellers

- Viagra
- Cialis
- Levitra
- Trial Erection packs 1
- Brand Viagra
- Brand Cialis
- Dapoxetine
- Tadapox
- Sildalis
- Extra Super Viagra
- Extra Super Cialis
- Extra Super Levitra
- Malegra FXT
- Malegra DXT
- Viagra Professional
- Cialis Professional
- Viagra Super Active
- Cialis Super Active
- Kamagra Effervescent
- Viagra Soft
- Cialis Soft

categories / Bestsellers / Viagra

Viagra

Active Ingredient: Sildenafil Testimonials

Viagra is indicated for the treatment of erectile dysfunction in men.

Other names for this medication
Intagra, Sildenafila, Sildenafilo, Sildenafilum, Veega

Analogs of Viagra:
Brand Viagra, Sildalis, Extra Super Viagra, Malegra FXT, Malegra DXT, Viagra Professional, Viagra Super Active, Kamagra Effervescent, Viagra Soft, Female Viagra, Silvitra, Kamagra, Kamagra Polo, Kamagra Super, Malegra FXT Plus, Malegra DXT Plus, Penegra, Viagra Extra Dosage, Kamagra Soft, Kamagra Oral Jelly, Kamagra Gold, Kamagra Chewable, Nizagara, Viagra Plus, Red Viagra, Silagra, Viagra Jelly, Zenegra, Viagra Vigour, Viagra Sublingual, Viagra Soft Flavored, Suhagra, Sildigra, Lady era, Caverta, Fildena, Aurogra

Viagra 100MG

Package	Per Pill	Price	Savings	Bonus	Order
100mg × 10 pills	$3.8	$38		+ Levitra	Add to Cart
100mg × 20 pills	$2.46	$49.17	$26.83	+ Viagra	Add to Cart

US: +1-760-284-3222
EU: +4420-3286-3820

Shopping cart

0 items $0 USD

Recently viewed

Nike Schuhe Schweiz Outl...

www.caution-de-loyer.ch

Search

ANMELDEN KONTO ERSTELLEN im Warenkor

JUST DO IT.

Währungen: Swiss Franc

Suchbegriff

STARTSEITE NIKE AIR FORCE 1 AIR JORDAN 5 IMPRESSUM & KONTAKT

Kategorien

- 2016 Neue Artikel
- 2016 Nike Air Max
- New Jordans
- Nike Air Foamposite
- Nike Air Force 1
- Nike Air Huarache Damen
- Nike Air Huarache Herren
- Nike Air Jordan Damen
- Nike Air Jordan Herren

NEUE ARTIKEL IM AUGUST

2016 Nike Air Jordan 13 Retro Low "Quai 54" Sneakers Schwarz Khaki AJ Männer Schuhe

~~CHF201.24~~ CHF82.06

2016 Nike Air Jordan 13 Retro Low "Quai 54" Sneakers Weiß Universität Blau AJ Männer Schuhe

~~CHF202.22~~ CHF82.06

2016 Nike Air Jordan 30Th Xiii 13 Retro "Homiesen" Low Frauen Schuhe Weiß Silber-Navy-Türkis 310810

~~CHF198.31~~ CHF81.08

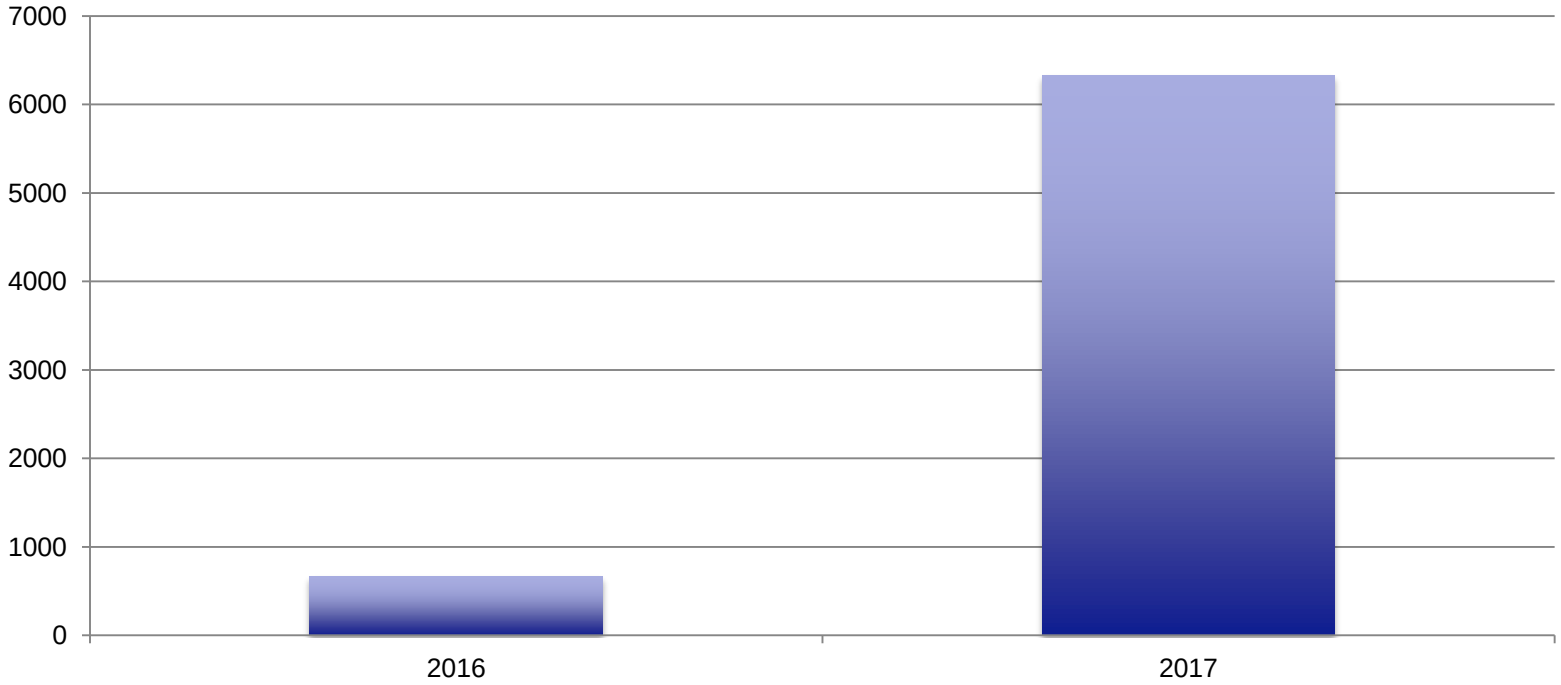

GS7

MERCURIAL

Activities against malicious registrations

- **Cooperation with the authorities**
- Federal police
- Local police
- Finma (finance regulator)
- Gambling regulator
- Swissmedic (medical regulator)
- **Request Id and Swiss correspondence address**
- **Delete domain name if no answer within 30 days**

Requests by Swiss authorities for domain holder data



News

Internet fraud: 5,000 online shops deleted

Brand-name shoes for CHF 49 instead of CHF 149 – a tempting offer. Internet bargain hunters may fall victim to fraudsters. The security experts at SWITCH warn that the number of fraudulent offers online has increased drastically in 2017. Together with the Swiss authorities, SWITCH is taking measures to fight this threat and has reported its first successes in combating e-commerce crime.

Published on 28.08.2017

Shoppers who find brand-name products offered online at sensationally low prices should proceed with caution. E-commerce crime is nothing new, but it has increased greatly in 2017. In 2016, SWITCH deleted around 700 web addresses of online shops with a .ch domain ending. By August 2017, the figure had already passed the 5,000 mark. Michael Hausding, a security expert in domain name fraud and a member of the 14-person SWITCH-CERT team of security experts, explains: 'Thanks to close cooperation with the authorities and improved processes, our targeted campaign allowed us to remove 4,500 fraudulent .ch online shops in August 2017 alone. The fraudsters running these shops were attempting to steal money from internet users or gain access to their credit card information. By taking this approach, we are

Contact for media representatives

Roland Eugster
Tel. +41 44 253 98 77

https://www.switch.ch/news/fake-webshops/

Conclusion

- Criminals have enough resources to spend on domain names
- There are many business cases that allow the purchase of domain names
- Domain name registrations with fake or stolen identities
- The number of abusive registration is increasing for .ch
- The domain name industry needs to be proactive to fight domain name abuse

michael.hausding@switch.ch
@mhausding

http://securityblog.switch.ch/