Fraudulent Webshops

Targeting teens with fake webshops

Michael Hausding
michael.hausding@switch.ch
@mhausding

Wien, 29.8.2017

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

Registry for .ch

- **Contract with the office of communication**
- **Fight against Cybercrime is part**
- **Law about internet domains (VID)**

Internet criminals need domain names

Internet criminals need domain names for:

- **Phishing**
- **Malware**
- **CC**
- **Social engineering**
- **Fraud**
- **DNS**
- **Ransomware payments**
- **…………**

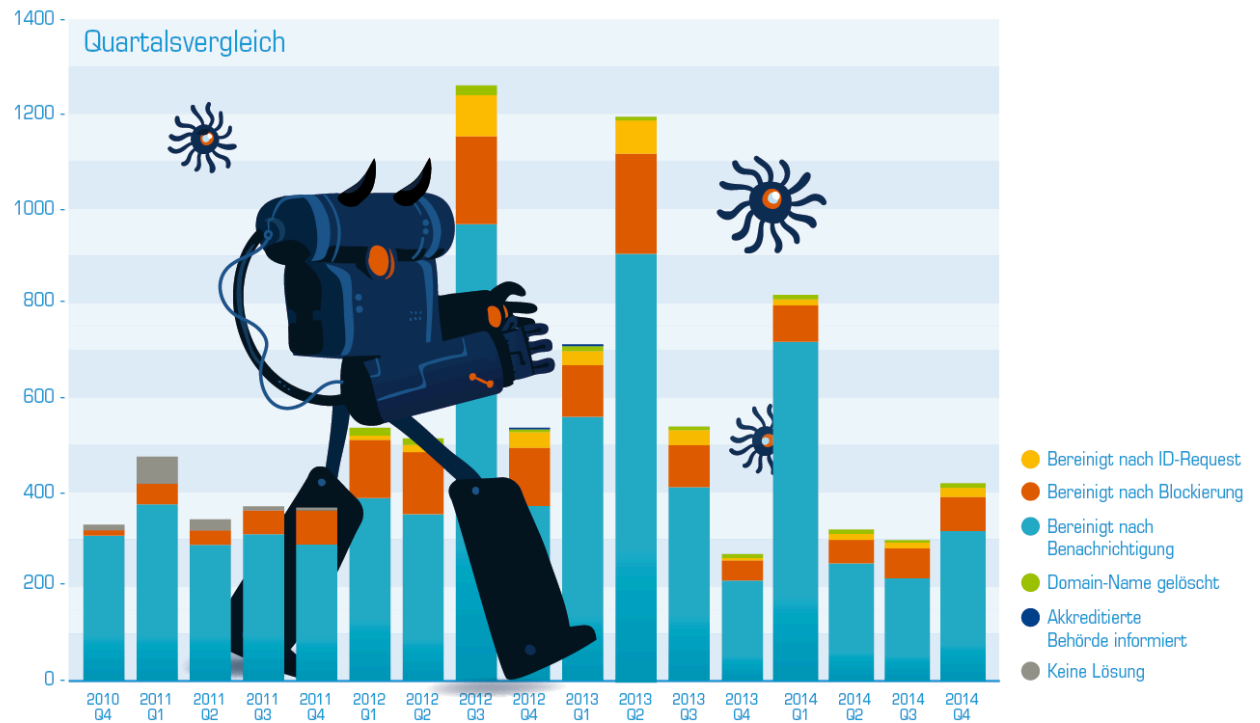# To get access to domain names they need to make a decision
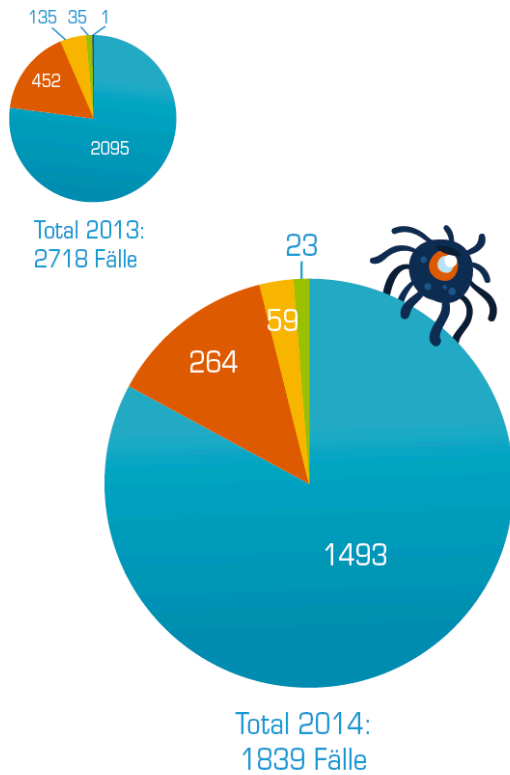
Take or Buy

Take

Internet criminals take domain names for:

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

Malware-Bekämpfung in der Schweiz

Total 2013: 2718 Fälle
- 135
- 35
- 1
- 452
- 2095

Total 2014: 1839 Fälle
- 23
- 59
- 264
- 1493

Quartalsvergleich

Legend:
- Bereinigt nach ID-Request
- Bereinigt nach Blockierung
- Bereinigt nach Benachrichtigung
- Domain-Name gelöscht
- Akkreditierte Behörde informiert
- Keine Lösung

X-axis: 2010 Q4, 2011 Q1, 2011 Q2, 2011 Q3, 2011 Q4, 2012 Q1, 2012 Q2, 2012 Q3, 2012 Q4, 2013 Q1, 2013 Q2, 2013 Q3, 2013 Q4, 2014 Q1, 2014 Q2, 2014 Q3, 2014 Q4

Buy

Internet criminals buy domain names for:

- **Phishing**
- **CC**
- **Social engineering**
- **Fraud**
- **DNS**

Criminals buy domain names and register with fake or stolen identities

In 2016 737 .ch domain names where reported by the Swiss authorities to SWITCH because of (wrong) address data outside Switzerland

In 99.9% the registrant data was incorrect and the domain name was deleted after 30 days didn't reply to our emails

In 2017 the number of reported domain names was increasing and we automated the process of requesting a Swiss contact address for domain names

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Office of Police fedpol

search

Topics A-Z

Latest News	Security	Crime	Police co-operation	Passport & Identity card	Publications & services	About us

‹ Crime

Cybercrime

Dangers on the internet

Reporting form

Reporting form

Are you a victim of computer crime?

If you are in imminent danger to life or limb contact the next police station or call the emergency number 117.
If you wish to report suspicious matter on the internet to fedpol or are the victim of cybercrime, complete the online reporting form((Anker)). The specialists at fedpol require your information in writing to deal with the case. They will take the necessary measures if possible and forward the case where appropriate to the authorities responsible.

Here is what you should do:

- Submit in full all website addresses (URL) and e-mail addresses you have involving the incident you are reporting, whether it involves a specific cybercrime attack or suspicious internet content.

ANMELDEN   KONTO ERSTELLEN   im Warenko

JUST DO IT.

Währungen: Swiss Franc

Suchbegriff

STARTSEITE   NIKE AIR FORCE 1   AIR JORDAN 5   IMPRESSUM & KONTAKT

nike online shop schweiz
www.caution-de-loyer.ch

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 "Hornissen" Low Frauen Schuhe Weiß Silber-Navy-Türkis 310810

~~CHF198.31~~   **CHF81.08**

Valid Shop | CC , Fullz , TR1/TR2 , DUMPS , Paypal , RDP ...

100% COMPATIBLE Login : Password : Remember Me

validshop.cc

Validshop.su | Buy WOW GOLD. Best price.

Validshop.su Login : Password : Remember Me : **Validshop**.su Login : Password : Remember Me ...

validshop.su

Valid Shop | CC , Fullz , TR1/TR2 , DUMPS , Paypal , RDP ...

Email:* Password:* Verify:*

validshop.cc/register.php

Valid CC Seller - Buy Shop Fresh Dumps Credit Cards CVV with PIN

Valid CC Seller - best fresh dumps credit cards **shop**. CVV CVV2 ZIP DOB SSN Track 101 201 pin.

V https://validccseller.com

We identified a pattern in the registration of domain names used for fraudulent web shops and found 4'469 registrations in June 2017

On July 25th 4'469 domain names were entered into the identification process in a coordinated action from the Swiss federal police and SWITCH-CERT

On August 25th 4'468 were deleted from the registry database

Operational action to disrupt the business case of the fraudsters.

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/

Five tips
for secure
online shopping

Nike Air Max Thea/90/95 ...

www.martinahug.ch

Search

Neu Nike Flyknit Schuhe in Schwarz Orange Für Damen Zu Verkaufen

Günstige Nike Air Max 2015 3d Flyknit Schuhe in Schwarz Grün Blau Für Damen Auslauf

Neu Nike Flyknit Air Max 2014 Schuhe in Lila Orange Für Damen Auf Verkauf

Günstige Nike Air Max Flyknit Schuhe in Schwarz Lila Weiß Für Damen Zu Verkaufen

€225.1 €744   €225.1 €744   €240.2 €80.1   €240.3 €80.1

◉ Nike Air Zoom

• Nike Air Zoom Damen   • Nike Air Zoom Herren

Nike Air Zoom Damen

Günstige Nike Air Zoom Structure 18 Schuhe in Schwarz Blau Fluorescent Grün Für Damen Auf Verkauf

Günstige Nike Air Zoom Winflo 3 Schuhe in Rosa Orange Für Damen Outlet

Neu Nike Air Zoom Structure 19 Schuhe in Schwarz Silber Für Damen Verkauf Online

Günstige Nike Air Zoom 7 Schuhe in Schwarz Grün Für Damen Schweiz

€233.6 €79.1   €231.7 €77.2   €232.7 €78.2   €230.8 €76.3

Aus Sicherheitsgründen werden bei jeder Bestellung die IP-Adressen gespeichert.
Ihre IP Adresse lautet: 130.59.16.132

www.martinahug.ch/neu-nike-flyknit-schuhe-in-schwarz-orange-für-damen-zu-verkaufen-p-368.html

Die offizielle adidas Websi...   Jetzt Kaufen Nike Free 5.0 ...

www.setar.ch

Search

Günstig OnSuper Heiß Männer Nike Kobe Bryant IX Elite Schuhe Schwarz

CHF141.21- **CHF82.88**

Factory Direct Männer Nike Kobe Bryant IX Elite Schuhe Schwarz

CHF134.51- **CHF78.57**

Zu Verkaufen Männer Nike Kobe Bryant IX EM Schuhe Schwarz-Weiss

CHF135.35- **CHF79.15**

ON SALE

ON SALE

Rabatte Preis Männer Nike Kobe Bryant IX Elite Schuhe

CHF141.21- **CHF82.88**

Heißer Rabatt Männer Nike Kobe Bryant IX Elite Schuhe Blau Schwarz

CHF134.51- **CHF78.67**

Rabatte Verkauf Männer Nike Kobe Bryant IX EM Schuhe Blau Grün

CHF135.35- **CHF79.15**

Herren New Balance Schuhe
Kinder New Balance Schuhe
Männer Nike Jordan Schuhe
MBT Sandalen Damen
MBT Sandalen Herren
MBT Schuhe Damen
MBT Schuhe Herren
Mens Free Haven 3.0
Neue MBT Schuhe Damen
Neue MBT Schuhe Herren
Nike Flyknit Air Max
Nike Huarache Free 2012
Nike Kobe IX
Salomon Schuhe Damen
Salomon Schuhe Herren

Top Artikel

Ausgezeichnet Adidas Originals...

100% Garantie Donna Adidas...

Factory Direct Männer Nike Free...

Niedrige Preise a0aexMZ0eN Schuhe...

Startseite   Mein Konto   Datenschutzbestimmungen   Schreiben Sie uns   Preise und Versand

WESTERN UNION   MasterCard   VISA   DHL   UPS   Trustwave   TNT   McAfee SECURE

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Polizei fedpol

🔍 Suche

Themen A-Z ▾

❮ Kriminalität

Cybercrime

Gefahren im Internet

Meldeformular

Meldeformular

🖨

Wurden Sie Opfer eines Angriffs oder Missbrauchs?

Bei unmittelbarer Gefahr für Leib und Leben wenden Sie sich bitte an die nächste Polizeidienststelle oder den Polizeinotruf Tel. 117.

▸ **Meldungen betreffend Facebook-Inhalte**

Bitte beachten Sie auch unsere Rubriken Gefahren im Internet sowie Die verschiedenen Betrugsarten mit allen Informationen zu wichtigen und aktuellen Phänomenen der Internetkriminalität.

Gefahren im Internet
Betrugsarten

Meldung (Web-Adresse, E-Mail,...) *	_____ (Obligatorisch)
Inhalt	_____
Datum	_____
Zeit	_____
Ihre E-Mail	_____
Bemerkungen	

[senden] [löschen]

www.diezaunprofis.ch

Q Search

schuh

Suchbegriff

Startseite   **Stiefelette Herren**   **Bunker**   **Paul & Joe**   **Neue Artikel**   **Alle Artikel**   **Impressum & Kontakt**

Kategorien

Ballettschuhe Damen->

Clogs Damen->

Flip Flops Damen->

Flip Flops Herren->

Hausschuhe Damen->

Hausschuhe Herren->

High Heels Damen->

Loafers Damen->

Loafers Herren->

Sandalen Damen->

Sandalen Herren->

Schnürschuhe Damen->

Schnürschuhe Herren->

Sneakers Damen->

Sneakers Herren->

Sportschuhe Damen->

Sportschuhe Herren->

Stiefel Damen->

Stiefel Herren->

Stiefelette Damen->

Stiefelette Herren->

Schuhe Online

MONATLICHE SONDERANGEBOTE

Nike Wmns T-lite XI Sneakers Blk Arctc Pnk Fchs Frc Fchs Fr Damen - Nike Kaufen(515 77799)

CHF44.76 **CHF34.91**

No Box Alma Sneakers Schwarz Damen - No Box Kaufen Online(245 60775)

CHF47.51 **CHF38.49**

No Box Alma Sneakers Dentelle Schwarz Damen - No Box Online(641 97910)

CHF57.76 **CHF46.21**

No Box Alma Sneakers Matelassé Schwarz Damen - No Box Bestelle(935 99719)

CHF68.59 **CHF52.13**

Tageslieferung Argus

66
Artikel

28.08.2017 - 29.08.2017

Pressreview: PDF

Hoi mitenand

Hier kommen die neusten Clippings von Argus der Presse als Newsletter. Ein Klick auf die Artikel-Überschrift oder "pdf" öffnet das PDF-Clipping.

Gruss Roland

Print (33)

Print

pdf | ocr

5000 .ch-Webshops wegen Betrug gelöscht

20 Minuten Zürich

Publikationsdatum: 29.08.2017   Lieferdatum: 29.08.2017

Thema: Security

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
- The domain name industry needs to be proactive to fight domain name abuse

michael.hausding@switch.ch
@mhausding

http://securityblog.switch.ch/