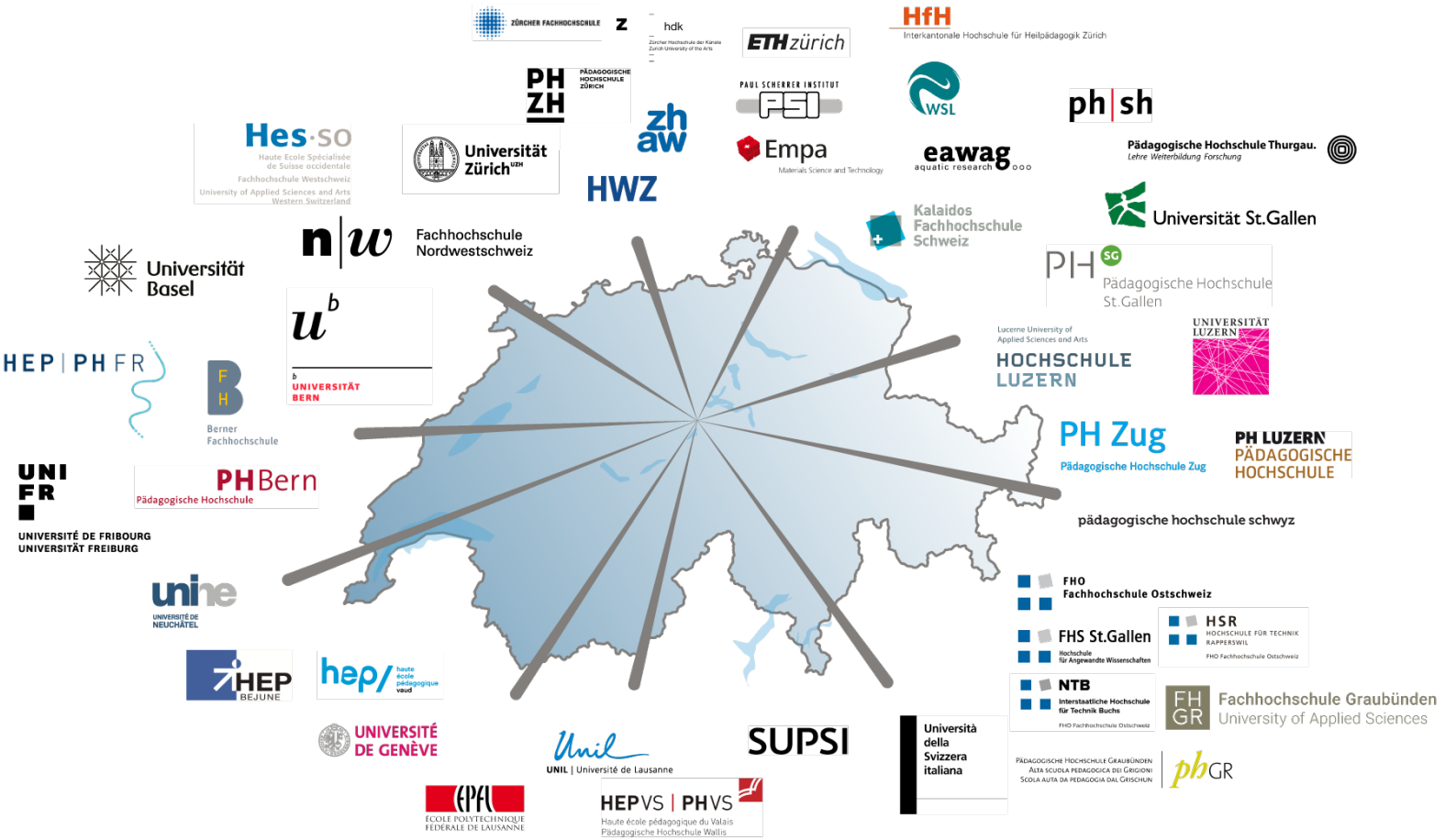
Bekämpfung von Cyberkriminalität bei .ch Domain Namen

Zürich, 22.2.2020
Digitale Gesellschaft
Winterkongress

Michael Hausding
michael.hausding@switch.ch
@mhausding

SWITCH - NREN


ZÜRCHER FACHHOCHSCHULE
hdk
ETH zürich
HfH
Interkantonale Hochschule für Heilpädagogik Zürich
PH ZH
PÄDAGOGISCHE HOCHSCHULE ZÜRICH
PAUL SCHERRER INSTITUT
PSI
WSL
ph|sh
Hes·so
Haute Ecole Spécialisée de Suisse occidentale
Fachhochschule Westschweiz
University of Applied Sciences and Arts Western Switzerland
Universität Zürich
zh aw
Empa
Materials Science and Technology
eawag
aquatic research
Pädagogische Hochschule Thurgau.
Lehre Weiterbildung Forschung
HWZ
Kalaidos Fachhochschule Schweiz
Universität St.Gallen
n|w
Fachhochschule Nordwestschweiz
Universität Basel
PH SG
Pädagogische Hochschule St.Gallen
u b
UNIVERSITÄT BERN
Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN
UNIVERSITÄT LUZERN
HEP | PH FR
Berner Fachhochschule
PH Zug
Pädagogische Hochschule Zug
PH LUZERN
PÄDAGOGISCHE HOCHSCHULE
UNI FR
UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG
PH Bern
Pädagogische Hochschule
pädagogische hochschule schwyz
unine
UNIVERSITÉ DE NEUCHÂTEL
FHO
Fachhochschule Ostschweiz
FHS St.Gallen
Hochschule für Angewandte Wissenschaften
HSR
HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz
HEP BEJUNE
hep
haute école pédagogique vaud
NTB
Interstaatliche Hochschule für Technik Buchs
FHO Fachhochschule Ostschweiz
FH GR
Fachhochschule Graubünden
University of Applied Sciences
UNIVERSITÉ DE GENÈVE
Unil
UNIL | Université de Lausanne
SUPSI
Università della Svizzera italiana
PÄDAGOGISCHE HOCHSCHULE GRAUBÜNDEN
ALTA SCUOLA PEDAGOGICA DEI GRIGIONI
SCOLA AUTA DA PEDAGOGIA DAL GRISCHUN
phGR
EPFL
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
HEP VS | PH VS
Haute école pédagogique du Valais
Pädagogische Hochschule Wallis

SWITCH – Registry für .ch & .li

- Autoritative Nameserver .ch & .li
- Registry Datenbank
- Registrar Schnittstelle (EPP)
- Whois
- Security-Awareness
- DNSSEC Förderung

SWITCH-CERT

NREN
400.000 people
100 GB/s
Network Security Monitoring

ccTLD Registry
2.3 Mio Domains

Malware, Phishing, Fraud

Swiss Banks
10 Banks
10 Years
E-Banking-Fraud -Malware

Industry & Logistics
Started 2017 with 6

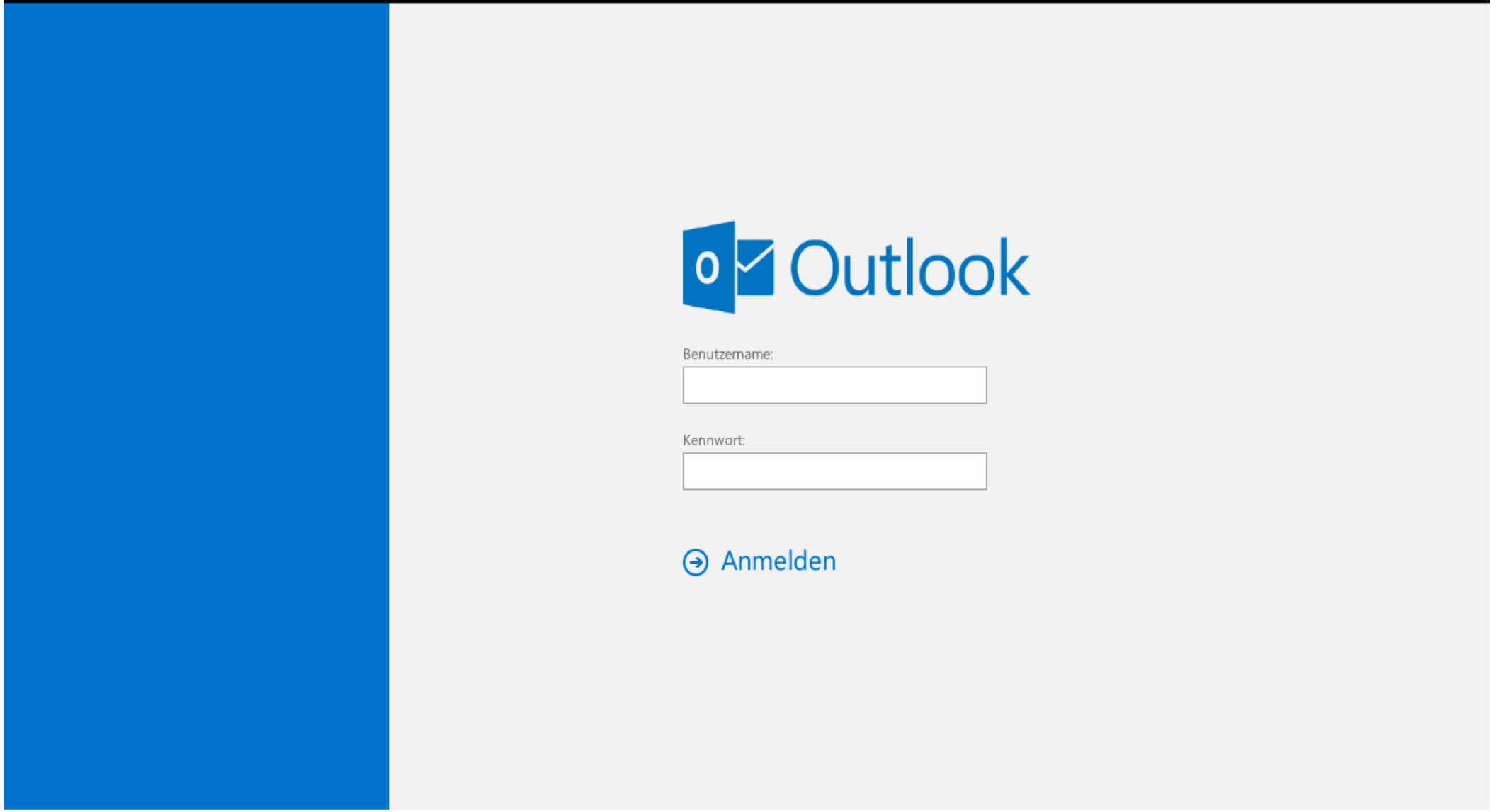
ICS/OT-Security

Energy
PoC started 2019

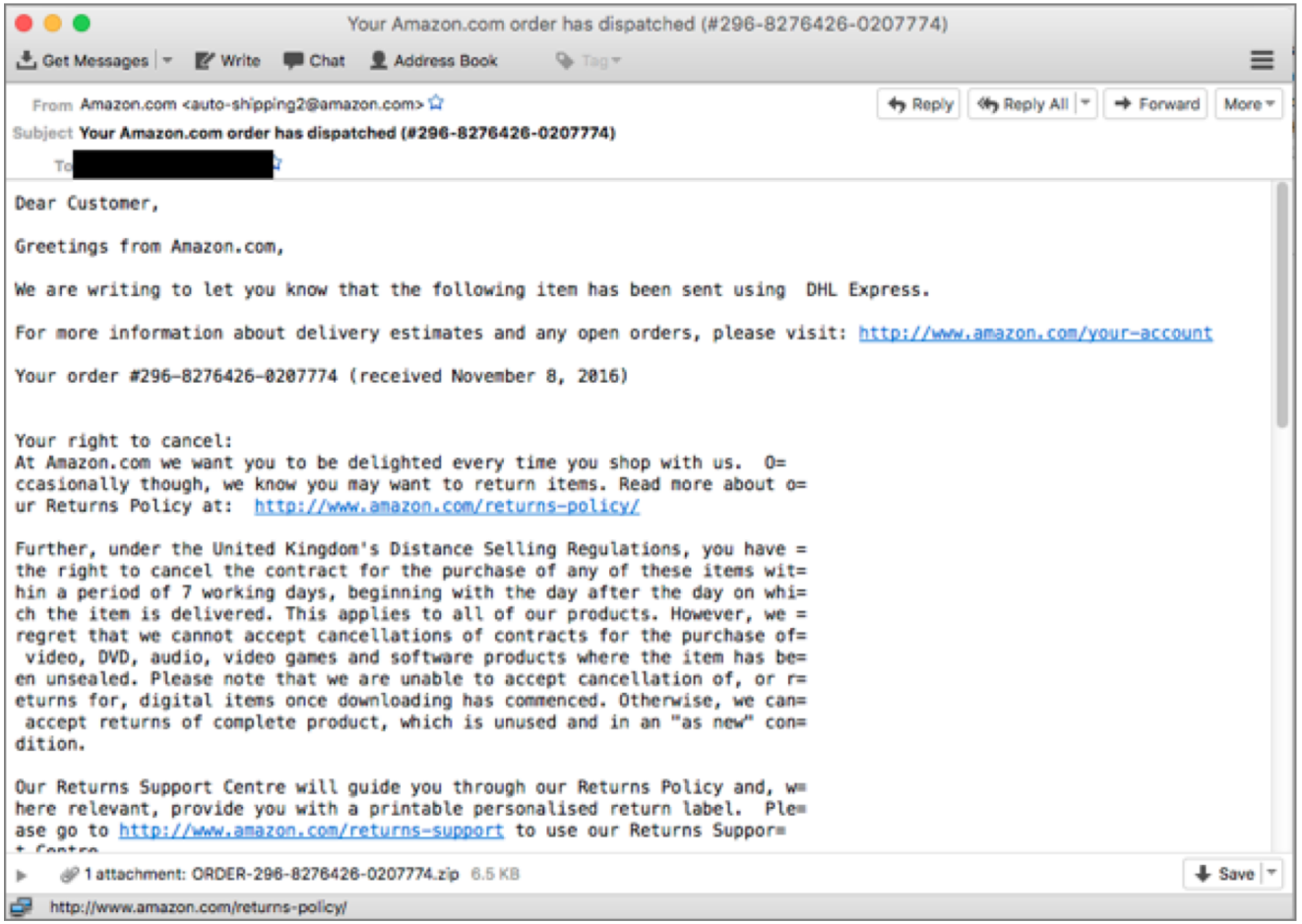

DNS
.ch
.li

DNS Missbrauch

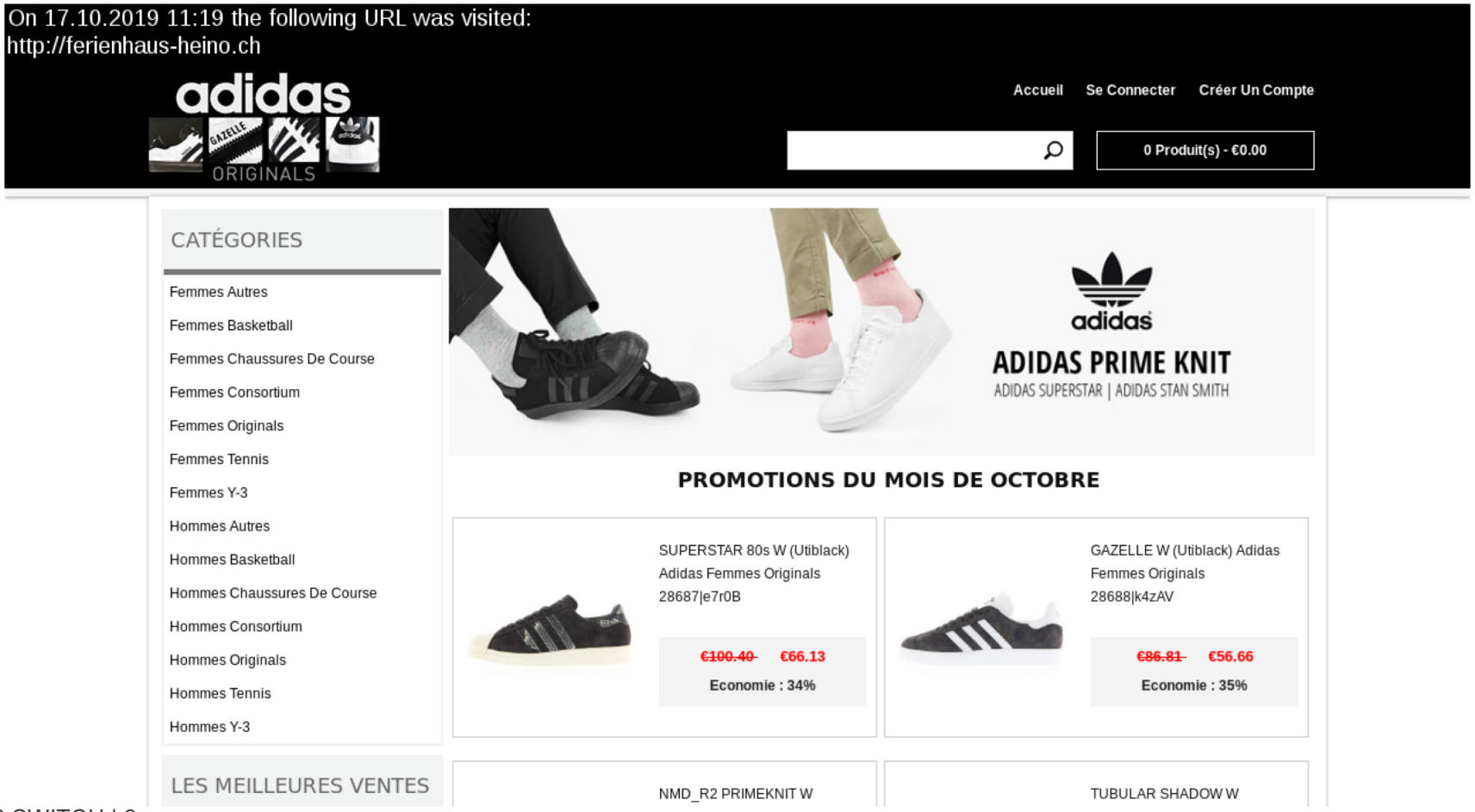
On 18.12.2019 10:09 the following URL was visited:
http://mail-walo.ch



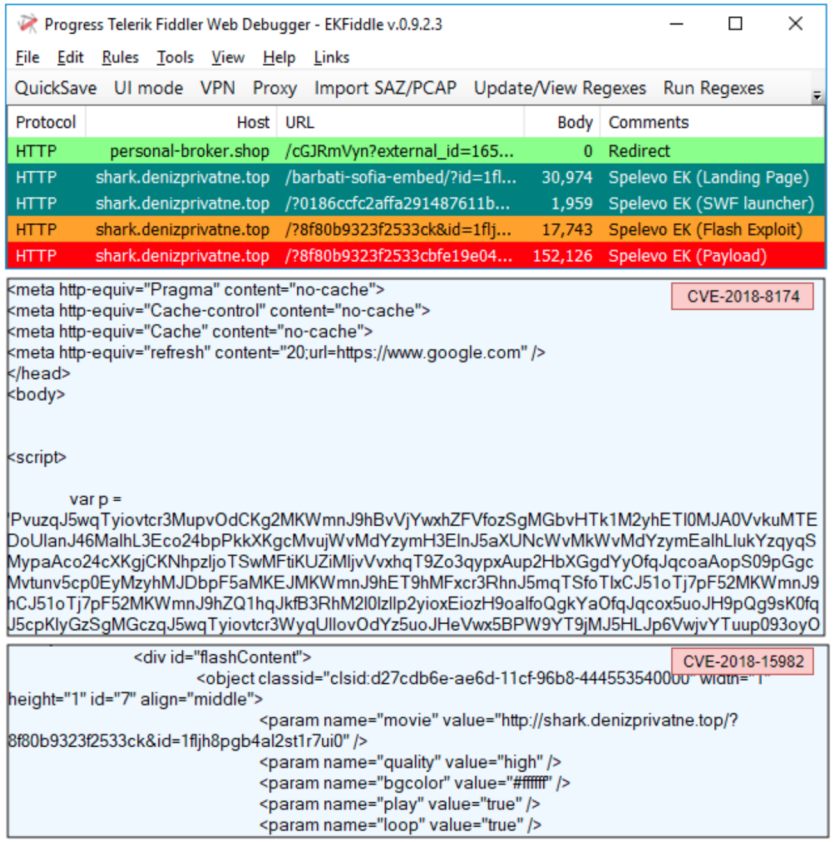
Spam Email (Locky Ransomware)



Fake Webshops



Drive-By Infections



Iranian hackers suspected in worldwide DNS hijacking campaign

Mysterious group hijacks DNS records to reshape and hijack a company's internal traffic to steal login credentials.

By Catalin Cimpanu for Zero Day | January 10, 2019 -- 11:46 GMT (11:46 GMT) | Topic: Security

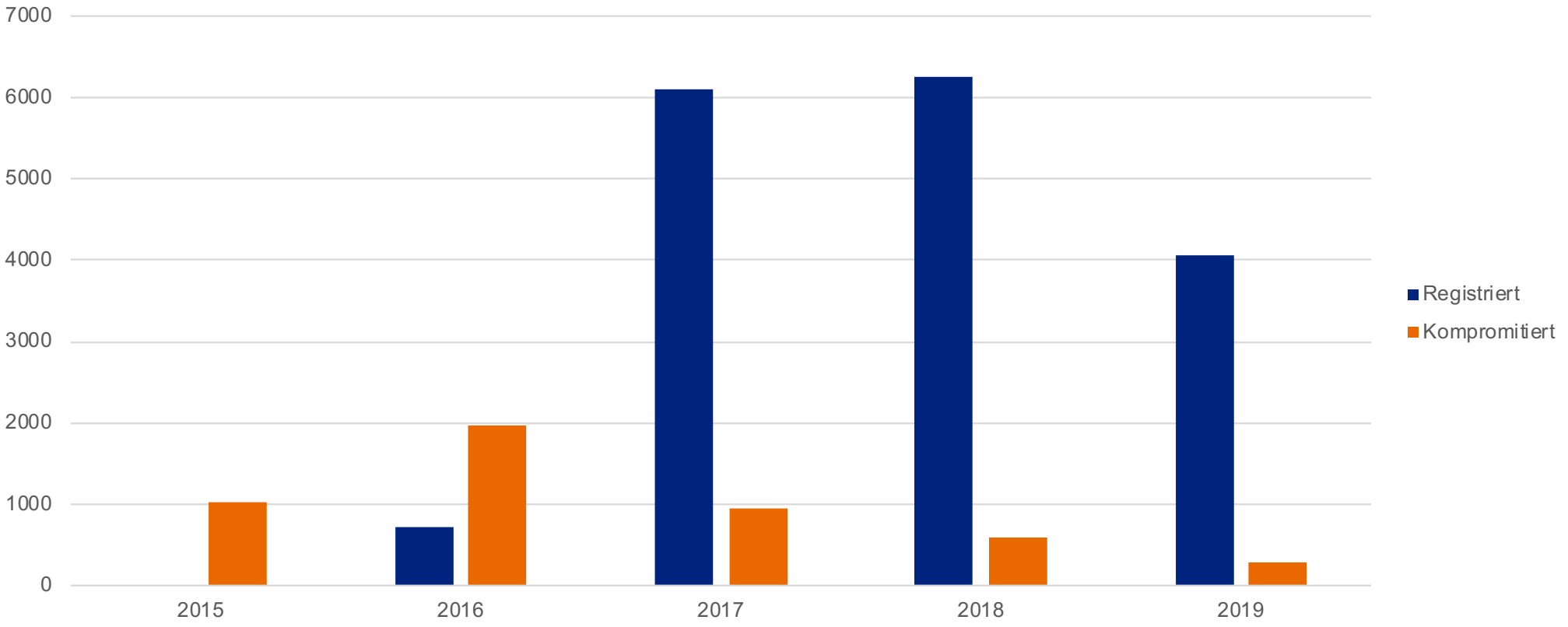
US cybersecurity firm FireEye has uncovered an extremely sophisticated hacking campaign during which a suspected Iranian group redirected traffic from companies all over their globe through their own malicious servers, recording company credentials for future attacks.

Affected organizations include telecoms, ISPs, internet infrastructure providers, government, and sensitive

SECURITY
Mozilla releases Firefox

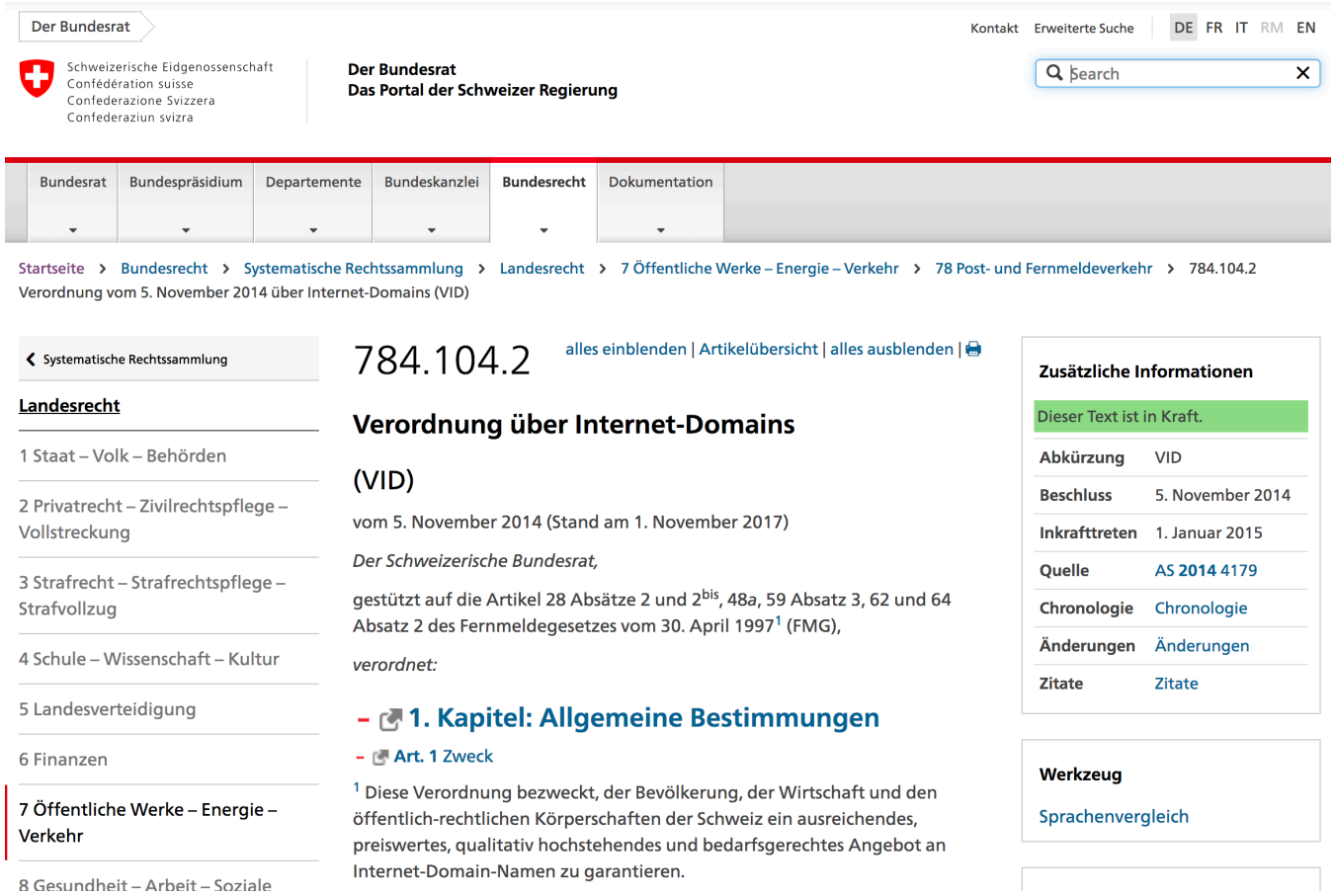
Take or Buy

Take or Buy


7000
6000
5000
4000
3000
2000
1000
0
2015
2016
2017
2018
2019
Registriert
Kompromitiert

Rechtliche Grundlage in der Schweiz

Verordnung über Internet-Domains (VID)



Der Bundesrat

Kontakt Erweiterte Suche DE FR IT RM EN

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat
Das Portal der Schweizer Regierung

Search

Bundesrat | Bundespräsidium | Departemente | Bundeskanzlei | **Bundesrecht** | Dokumentation

Startseite › Bundesrecht › Systematische Rechtssammlung › Landesrecht › 7 Öffentliche Werke – Energie – Verkehr › 78 Post- und Fernmeldeverkehr › 784.104.2
Verordnung vom 5. November 2014 über Internet-Domains (VID)

‹ Systematische Rechtssammlung

Landesrecht

1 Staat – Volk – Behörden

2 Privatrecht – Zivilrechtspflege – Vollstreckung

3 Strafrecht – Strafrechtspflege – Strafvollzug

4 Schule – Wissenschaft – Kultur

5 Landesverteidigung

6 Finanzen

7 Öffentliche Werke – Energie – Verkehr

8 Gesundheit – Arbeit – Soziale

784.104.2 alles einblenden | Artikelübersicht | alles ausblenden |

Verordnung über Internet-Domains

(VID)

vom 5. November 2014 (Stand am 1. November 2017)

Der Schweizerische Bundesrat,

gestützt auf die Artikel 28 Absätze 2 und 2bis, 48a, 59 Absatz 3, 62 und 64 Absatz 2 des Fernmeldegesetzes vom 30. April 1997[1] (FMG),

verordnet:

1. Kapitel: Allgemeine Bestimmungen

Art. 1 Zweck

[1] Diese Verordnung bezweckt, der Bevölkerung, der Wirtschaft und den öffentlich-rechtlichen Körperschaften der Schweiz ein ausreichendes, preiswertes, qualitativ hochstehendes und bedarfsgerechtes Angebot an Internet-Domain-Namen zu garantieren.

Zusätzliche Informationen

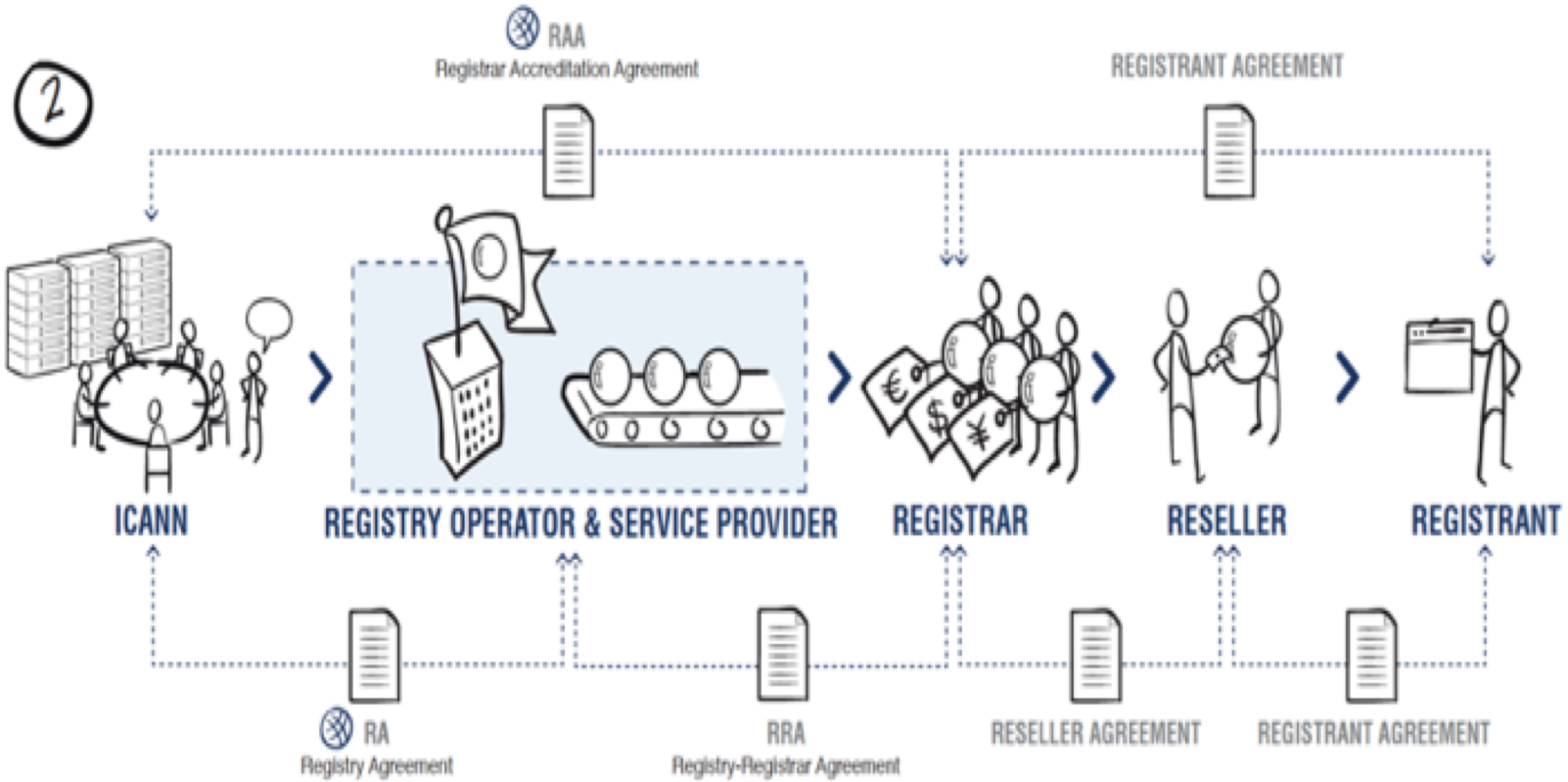
Dieser Text ist in Kraft.

Abkürzung	VID
Beschluss	5. November 2014
Inkrafttreten	1. Januar 2015
Quelle	AS **2014** 4179
Chronologie	Chronologie
Änderungen	Änderungen
Zitate	Zitate

Werkzeug

Sprachenvergleich

Governance bei gTLDs



Mögliche Massnahmen

- VID Art. 15 Massnahmen bei Missbrauchsverdacht
- VID Art. 16 Amtshilfe

- Identitätsüberprüfung (VID Art. 30)

- Verfügung einer Schweizer Behörde

VID Art. 16
Amtshilfe

– Art. 16 Amtshilfe und Zusammenarbeit

[1] Die Registerbetreiberin kann mit Dritten zusammenarbeiten, die ihre Mitarbeit zur Feststellung und Beurteilung von Bedrohungen, Missbräuchen und Gefahren anbieten, welche die von ihr verwalteten Domains, die dazugehörende Infrastruktur oder das DNS betreffen oder betreffend könnten. Sie sorgt dafür, dass die betreffenden Dritten mit ihr auf freiwilliger Basis und in gesicherter Form personenbezogene Informationen und Personendaten im Zusammenhang mit solchen Bedrohungen, Missbräuchen und Gefahren austauschen können. Sie kann ihnen solche personenbezogenen Informationen und Personendaten bekannt geben, nötigenfalls auch ohne Wissen der betroffenen Personen. Diese Bekanntgabe kann im Abrufverfahren erfolgen.[1]

[2] Sie meldet den spezialisierten Bundesbehörden Zwischenfälle im Bereich der Informationssicherheit, welche die von ihr verwaltete Domain oder das DNS betreffen. Sie kann die Personendaten im Zusammenhang mit diesen Zwischenfällen bearbeiten und den spezialisierten Stellen bekannt geben, nötigenfalls auch ohne Wissen der betroffenen Personen. Diese Bekanntgabe kann im Abrufverfahren oder durch blockweise Übertragung der Daten erfolgen.[2]

[3] Auf Verlangen einer im Rahmen ihrer Zuständigkeit intervenierenden Schweizer Behörde fordert die Registerbetreiberin die Halterin oder den Halter eines Domain-Namens ohne gültige Schweizer Korrespondenzadresse auf, innerhalb von 30 Tagen eine solche zu bezeichnen und die Identität bekannt zu geben. Die Registerbetreiberin widerruft den Domain-Namen, wenn die Halterin oder der Halter der Aufforderung nicht fristgerecht nachkommt; sie teilt den Widerruf der ersuchenden Schweizer Behörde mit.[3]

VID Art. 15
Massnahmen bei Missbrauchsverdacht

– Art. 15[1] Massnahmen bei Missbrauchsverdacht: Blockierung

[1] Die Registerbetreiberin kann einen Domain-Namen für höchstens fünf Werktage technisch und administrativ blockieren, wenn der begründete Verdacht besteht, dass der Domain-Name benutzt wird, um:

a. mit unrechtmässigen Methoden an sensible Daten zu gelangen;
b. schädliche Software zu verbreiten oder zu nutzen; oder
c. Handlungen im Sinne von Buchstabe a oder b zu unterstützen.

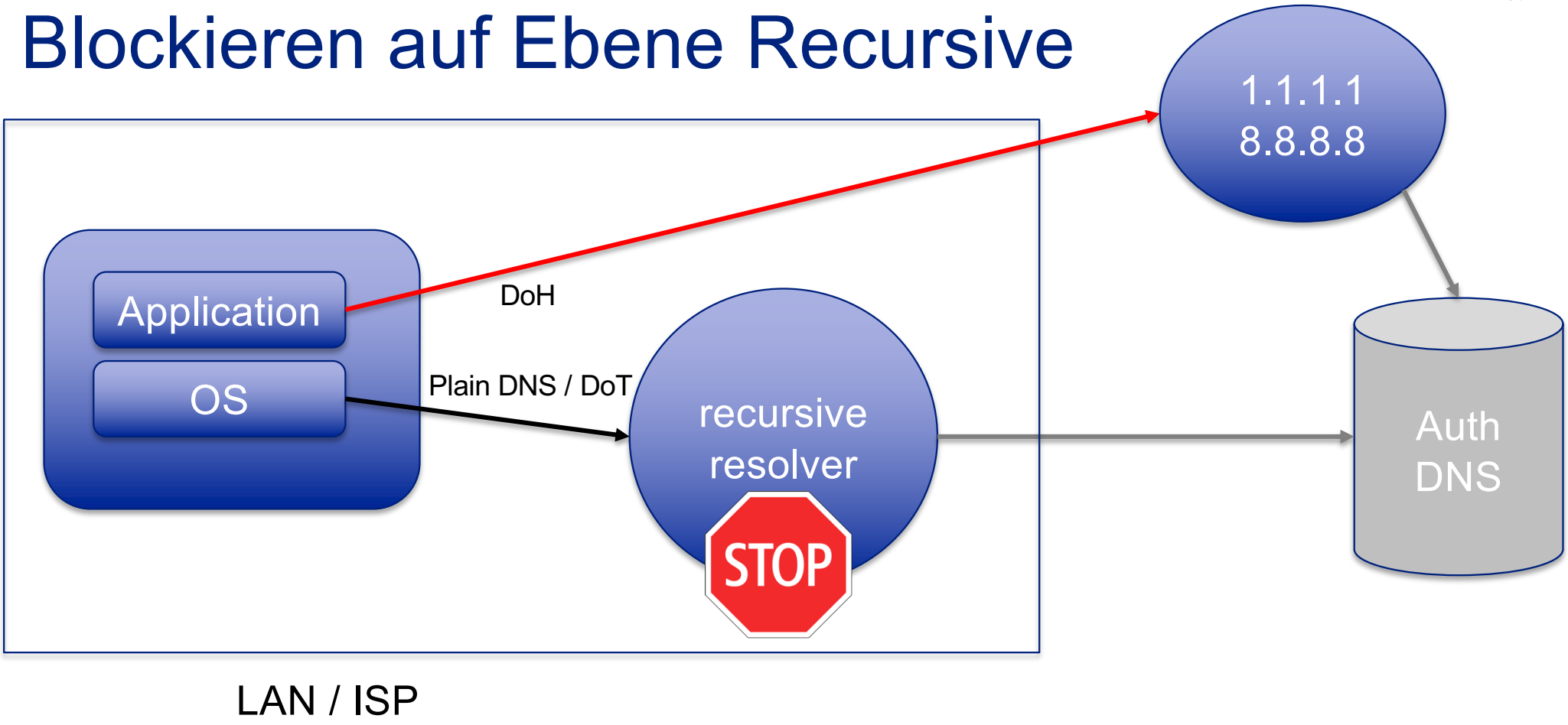
[2] Sie kann die Blockierung um höchstens 30 Tage verlängern, wenn:

a. der begründete Verdacht besteht, dass die Halterin oder der Halter falsche Identifizierungsangaben macht oder unrechtmässig die Identität eines Dritten verwendet; und
b. die zeitliche Dringlichkeit besteht, einen drohenden, nicht leicht wiedergutzumachenden Nachteil abzuwenden.

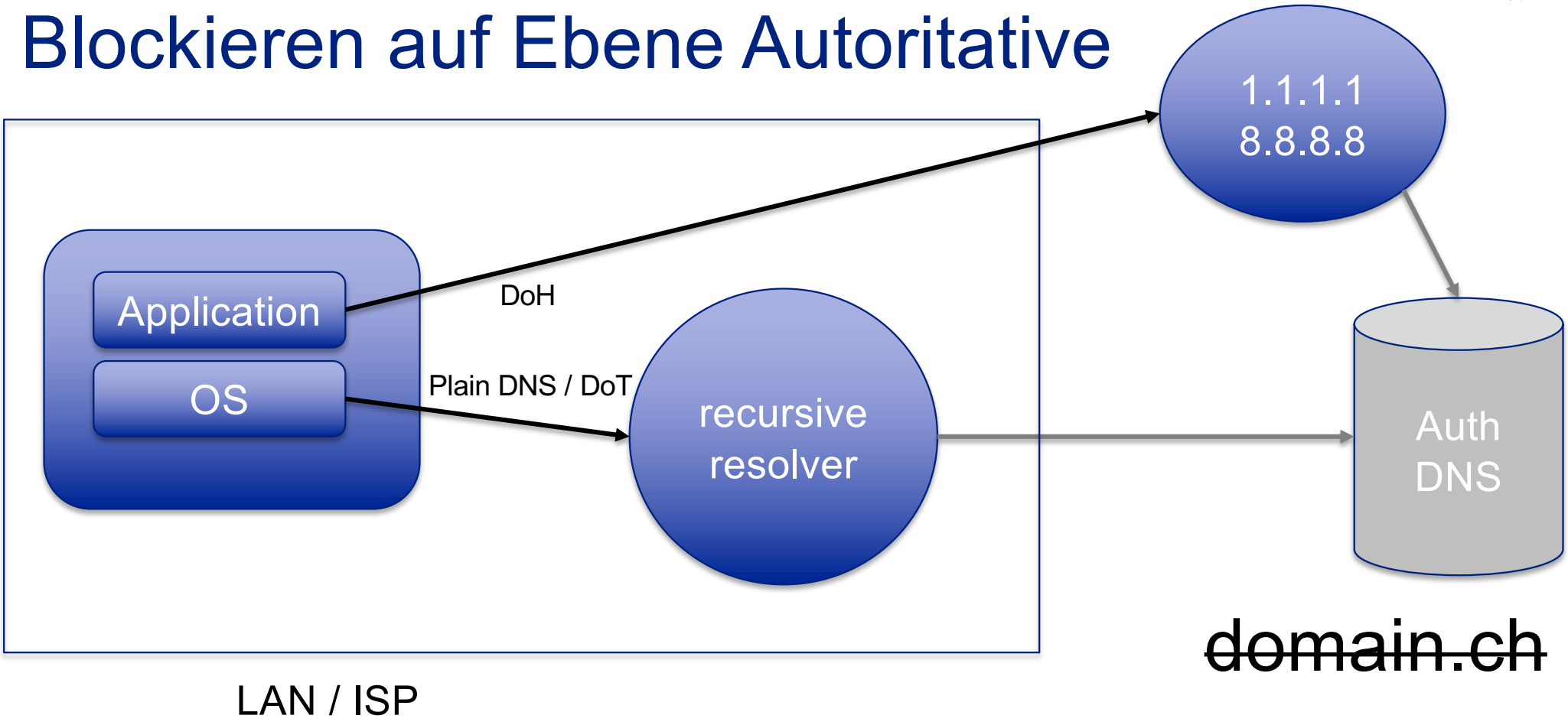
[3] Eine zur Bekämpfung der Cyberkriminalität vom BAKOM anerkannte Stelle kann die Blockierung für höchstens 30 Tage verlangen, wenn die Voraussetzungen nach Absatz 1 erfüllt sind.

[4] Eine Blockierung über die in diesem Artikel genannten Maximalfristen hinaus kann nur aufrechterhalten werden, wenn das Bundesamt für Polizei (fedpol) dies anordnet.

Blockieren auf Ebene Recursive



Blockieren auf Ebene Autoritative



Liste der vom BAKOM anerkannten Stellen für die Bekämpfung der Cyberkriminalität gemäss Art. 15 Abs. 3 VID (SR 784.104.2)

Ausgabe 4 vom 03.04.2019

Name, Adresse	Tätigkeit	Datum der Anerkennung
MELANI Melde- und Analysestelle Informationssicherung Schwarztorstrasse 59 CH-3003 Bern Tel. +41 (0)58 462 45 38 E-Mail: reply@melani.admin.ch https://www.melani.admin.ch	Sicherheit von Computersystemen und des Internets, Schutz der schweizerischen kritischen Infrastrukturen	15.06.2010
Kantonspolizei Zürich Abteilung Cybercrime Postfach CH-8021 Zürich Tel. +41 (0)44 247 22 11 E-Mail: cybercrime@kapo.zh.ch http://www.kapo.zh.ch	Ermittlungsverfahren im Bereich Cybercrime, Betrieb – gemeinsam mit der Staatsanwaltschaft Zürich und der Stadtpolizei Zürich – eines Cybercrime-Kompetenzzentrums	09.02.2018
Kantonspolizei Bern Kriminalabteilung Dezernat Wirtschaftsdelikte Nordring Postfach CH-3001 Bern Tel. +41 (0)78 854 34 43	Koordinationsstelle für die Ermittlungen im Bereich der Cyberkriminalität und führen von Ermittlungsverfahren	03.04.2019

Massnahmen bei Missbrauchdverdacht

- **Art. 15***b*[1] Massnahmen bei Missbrauchsverdacht: Information und Antrag auf Identifikation
- **Art. 15***c*[1] Massnahmen bei Missbrauchsverdacht: Verfügung und Widerruf
- **Art. 15***d*[1] Massnahmen bei Missbrauchsverdacht: nicht zugeteilte Domain-Namen
- **Art. 15***e*[1] Massnahmen bei Missbrauchsverdacht: Dokumentation und Bericht

Zusammenarbeit mit Behörden 2019

ANTRÄGE VON ANERKANNTEN BEHÖRDEN

Die beiden akkreditierten Behörden, Melani und die KAPO Zürich, haben im 2019 1'492 Anfragen nach VID Art. 15.1 zur sofortigen Blockierung (technisch/administrativ) gesendet. Alle Anfragen ausser einer wurden aufgrund 15.1. b «Phishing» gesendet.

		2019
Anfragen		1'492
Anfragen nicht beantwortet	Domain-Name gelöscht	1'492
Anfragen beantwortet	Domain-Name reaktiviert	0

AMTSHILFE

Auf Verlangen einer im Rahmen ihrer Zuständigkeit intervenierenden Schweizer Behörde wurden 2'507 Anfragen für eine Schweizer Korrespondenzadresse nach VID Art. 16.3 gesendet.

		2019
Anfragen		2'507
Anfragen nicht beantwortet	Domain-Name gelöscht	2'400
Anfragen beantwortet		107

Revision der VID

Änderungen VID

- Bereitstellung von Daten (Whois) (Art. 52)
- Umleitung von Verkehr (Art 15)
- Zuteilung und Delegation (Art. 25bis)
- Zugang zur .ch Zone (Art. 10)

Art 52 Bereitstellung von Daten (whois)

1 Die Registerbetreiberin veröffentlicht in der WHOIS-Datenbank die Daten, die gemäss den Regeln, die auf internationaler Ebene angewendet werden, erforderlich sind.

2 Sie kann folgende Daten in der WHOIS-Datenbank veröffentlichen:

- a. den Namen der Organisation und die UID der Halterin oder des Halters des betreffenden Domain-Namens;
- b. die Identifizierungsangaben und Kontaktdaten der Halterin oder des Halters des betreffenden Domain-Namens, wenn es sich um eine juristische Person handelt;
- c. die Identifizierungsangaben und Kontaktdaten der Halterin oder des Halters des betreffenden Domain-Namens, die oder der der Veröffentlichung zuge- stimmt hat.

Massnahmen bei Missbrauchsverdacht

1 Die Registerbetreiberin leitet den zu einem Domain-Namen führenden oder über diesen geführten Datenverkehr um, wenn folgende Voraussetzungen erfüllt sind:

2 Sie leitet den Datenverkehr zu einem Analysetool oder zu einer Informationsseite um, die Folgendes enthält:

- Informationen über den entsprechenden Missbrauchsverdacht;
- den Namen und die Kontaktdaten der Stelle oder der Behörde, die die Massnahme beantragt hat.

Zuteilung und Delegation 25 1bis - 1quater

- Die Registerbetreiberin teilt einen Domain-Namen zu und verhindert jegliche Konfiguration der mit ihm verbundenen Namensserver in der Zonendatei, die die Aktivierung des Domain-Namens ermöglicht, wenn ihr eine im Rahmen ihrer Zuständigkeit intervenierende Behörde mitteilt, dass berechtige Gründe zur Annahme bestehen, dass die Gesuchstellerin oder der Gesuchsteller den beantragten Domain-Namen zu einem unrechtmässigen Zweck oder in unrechtmässiger Weise nutzen wird.

- Sie kann einen Domain-Namen zuteilen und jegliche Konfiguration der mit ihm verbundenen Namensserver in der Zonendatei verhindern, die die Aktivierung des Domain-Namens ermöglicht, wenn berechtigte Gründe zur Annahme bestehen, dass die Gesuchstellerin oder der Gesuchsteller:
- falsche Identifizierungsangaben macht oder unrechtmässig die Identität eines Dritten verwendet; und
- den beantragten Domain-Namen zu einem unrechtmässigen Zweck oder in unrechtmässiger Weise nutzen wird.

- 1quater Wenn die Halterin oder der Halter in den in von Absatz 1bis und 1ter genannten Fällen innerhalb von 30 Tagen ihre oder seine Identität nicht korrekt bekannt gibt, widerruft die Registerbetreiberin die Zuteilung des Domain-Namens.

Zugang zur .ch Zone (Art. 10)

- 6. Gewährung des Zugangs zu den in der Zonendatei enthaltenen Informationen zum Zwecke der Bekämpfung von Cyberkriminalität oder für forschungsbezogene oder andere Zwecke im öffentlichen Interesse für jede Person, die ihre Identität korrekt bekannt gibt;

Revision der VID

Öffentliche Vernehmlassung bis 25. März

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

Besten Dank!