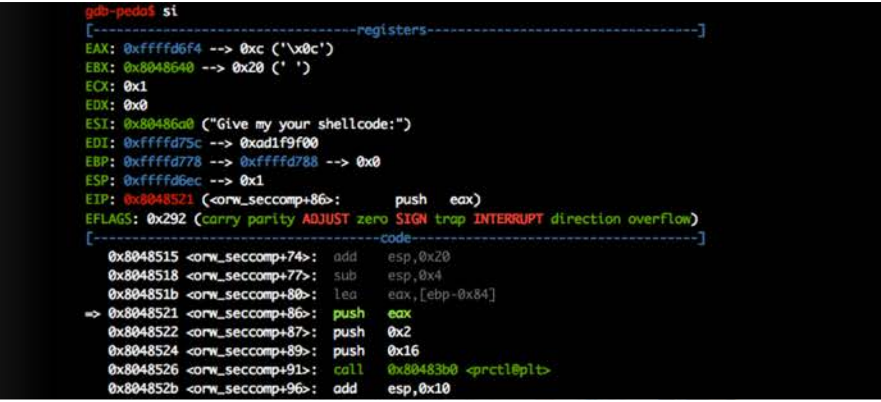
Cyber Risk Scenarios at Universities



```
gdb-peda$ si
[----------------------------------registers-----------------------------------]
EAX: 0xffffd6f4 --> 0xc ('\x0c')
EBX: 0x8048640 --> 0x20 (' ')
ECX: 0x1
EDX: 0x0
ESI: 0x80486a0 ("Give my your shellcode:")
EDI: 0xffffd75c --> 0xad1f9f00
EBP: 0xffffd778 --> 0xffffd788 --> 0x0
ESP: 0xffffd6ec --> 0x1
EIP: 0x8048521 (<orw_seccomp+86>:       push   eax)
EFLAGS: 0x292 (carry parity ADJUST zero SIGN trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x8048515 <orw_seccomp+74>:  add    esp,0x20
   0x8048518 <orw_seccomp+77>:  sub    esp,0x4
   0x804851b <orw_seccomp+80>:  lea    eax,[ebp-0x84]
=> 0x8048521 <orw_seccomp+86>:  push   eax
   0x8048522 <orw_seccomp+87>:  push   0x2
   0x8048524 <orw_seccomp+89>:  push   0x16
   0x8048526 <orw_seccomp+91>:  call   0x80483b0 <prctl@plt>
   0x804852b <orw_seccomp+96>:  add    esp,0x10
```

Antoine Neuenschwander
antoine.neuenschwander@switch.ch

eduhub.ch Security Awareness Workshop

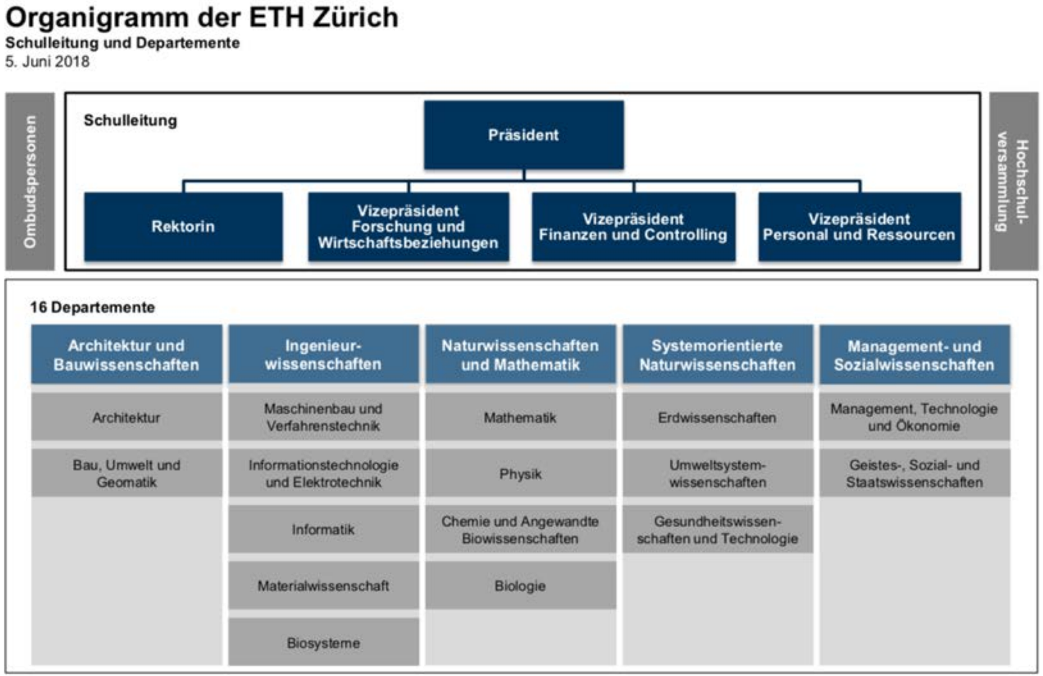
Thursday, August 16th 2018

Characteristics of the Research & Education Sector

A very diverse environment

Organizational Entities

Different independent authorities



Organigramm der ETH Zürich

Schulleitung und Departemente

5. Juni 2018

Ombudspersonen
Schulleitung
Präsident
Rektorin
Vizepräsident Forschung und Wirtschaftsbeziehungen
Vizepräsident Finanzen und Controlling
Vizepräsident Personal und Ressourcen
Hochschul-versammlung

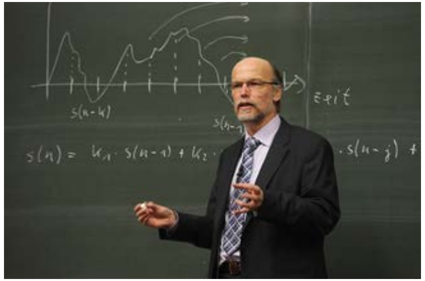
16 Departemente

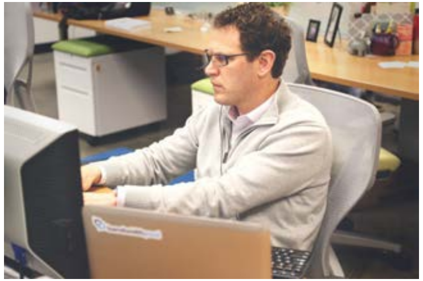
Architektur und Bauwissenschaften	Ingenieurwissenschaften	Naturwissenschaften und Mathematik	Systemorientierte Naturwissenschaften	Management- und Sozialwissenschaften
Architektur	Maschinenbau und Verfahrenstechnik	Mathematik	Erdwissenschaften	Management, Technologie und Ökonomie
Bau, Umwelt und Geomatik	Informationstechnologie und Elektrotechnik	Physik	Umweltsystemwissenschaften	Geistes-, Sozial- und Staatswissenschaften
	Informatik	Chemie und Angewandte Biowissenschaften	Gesundheitswissenschaften und Technologie	
	Materialwissenschaft	Biologie		
	Biosysteme			

End Users

Many different roles

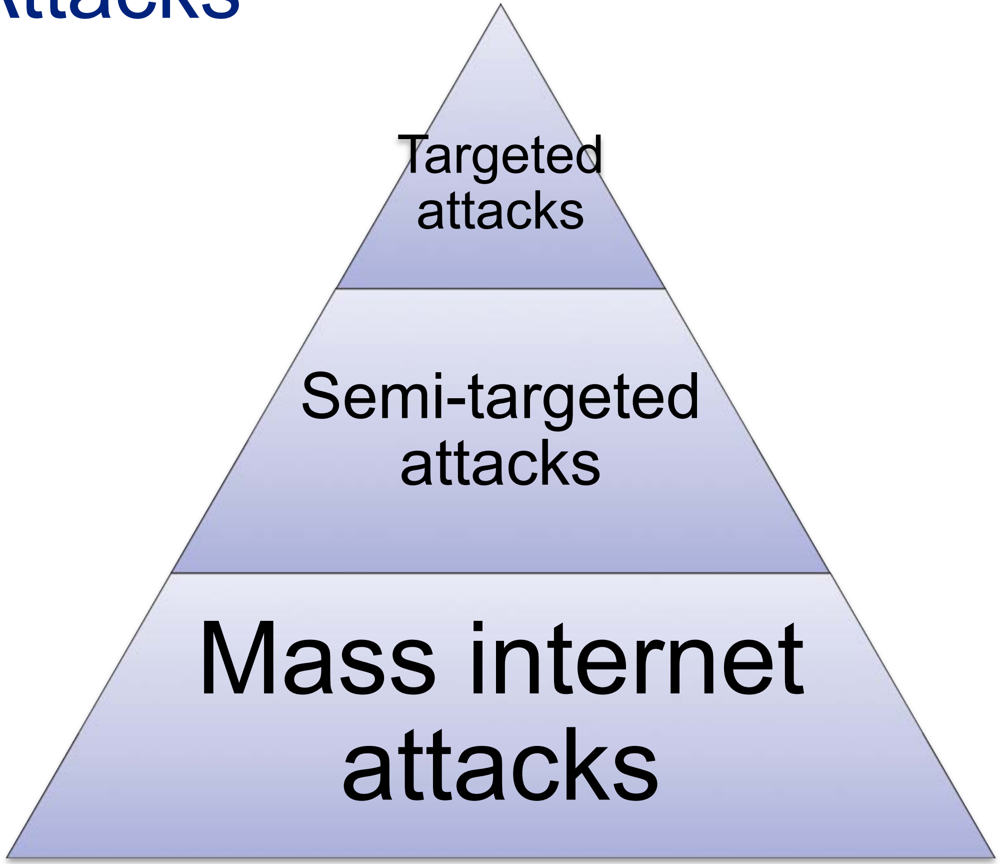
- Administration, researchers, students, teaching staff, service providers, etc





IT Systems in the R&E Sector

Types of Attacks



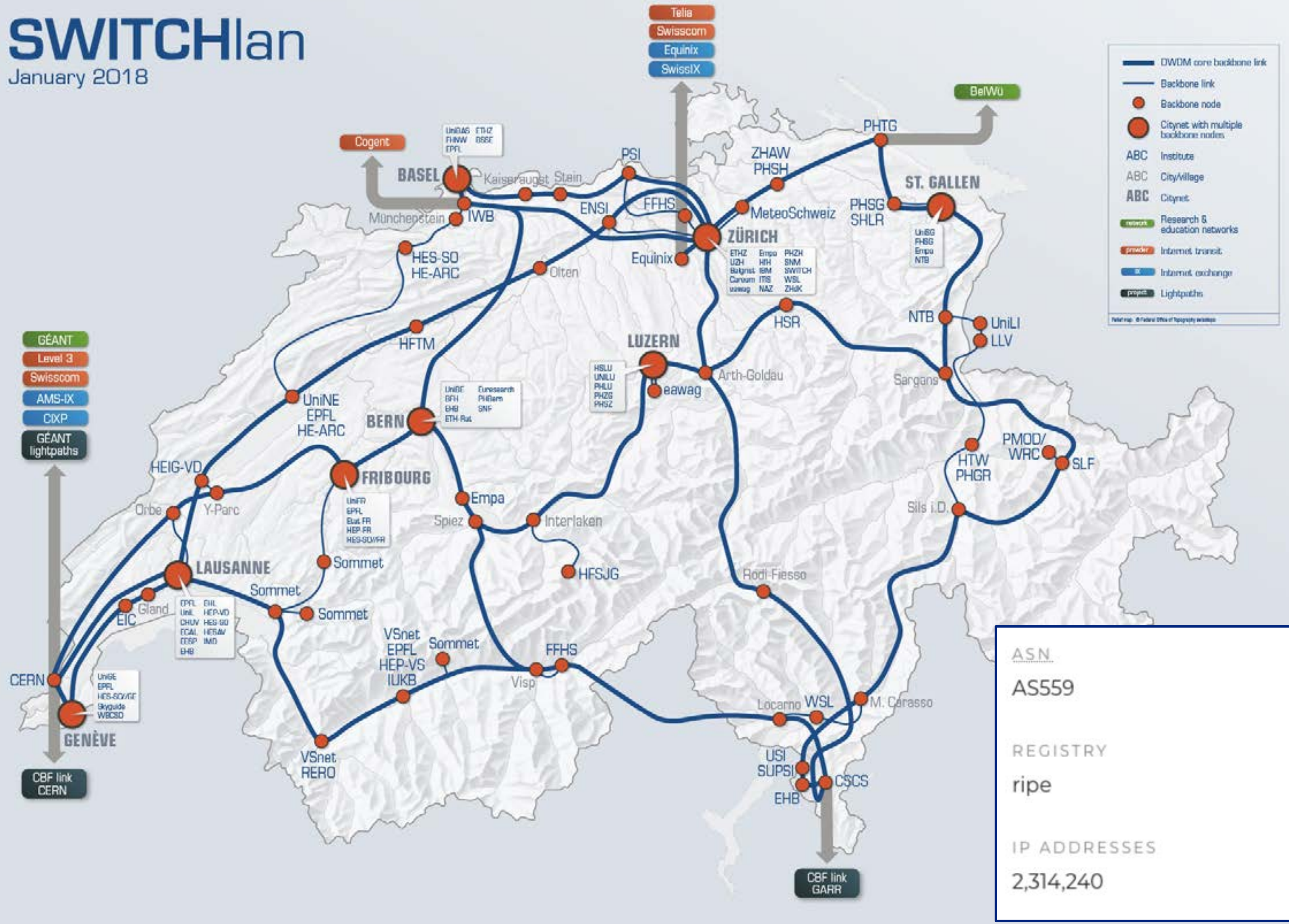
Targeted attacks

Semi-targeted attacks

Mass internet attacks

SWITCHlan

January 2018



ASN
AS559

ALLOCATED
2002-09-04T09:28:22Z

REGISTRY
ripe

DOMAIN
switch.ch

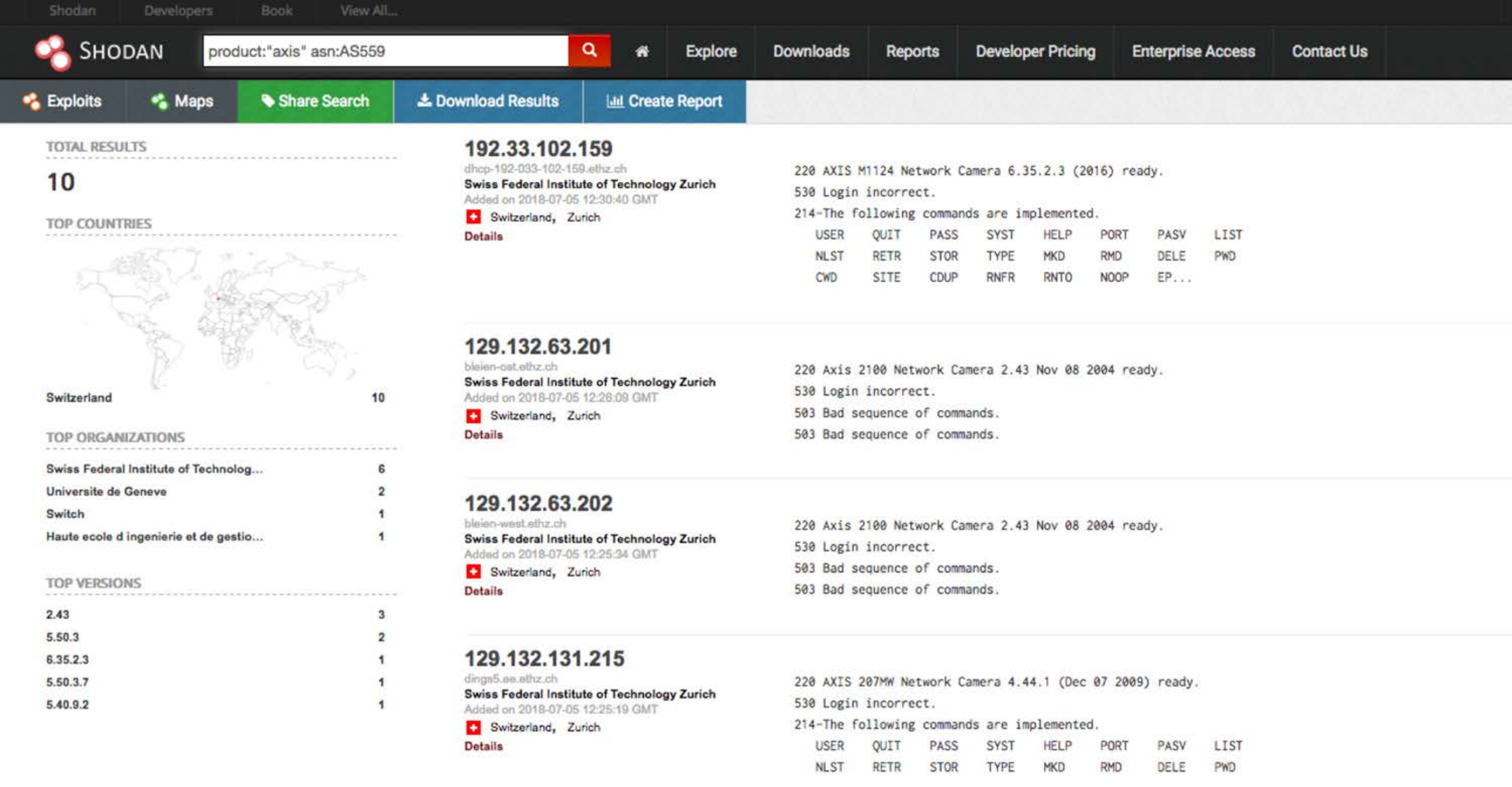
IP ADDRESSES
2,314,240

COUNTRY
🇨🇭 Switzerland

Mass Internet Attacks

- Opportunistic and Random
- Affect every system on the Internet

- Motivations:
  - Because it's possible
  - Get (moderately) rich fast



product:"axis" asn:AS559

TOTAL RESULTS

10

TOP COUNTRIES

Switzerland	10

TOP ORGANIZATIONS

Swiss Federal Institute of Technolog...	6
Universite de Geneve	2
Switch	1
Haute ecole d ingenierie et de gestio...	1

TOP VERSIONS

2.43	3
5.50.3	2
6.35.2.3	1
5.50.3.7	1
5.40.9.2	1

192.33.102.159
dhcp-192-033-102-159.ethz.ch
Swiss Federal Institute of Technology Zurich
Added on 2018-07-05 12:30:40 GMT
Switzerland, Zurich
Details

```
220 AXIS M1124 Network Camera 6.35.2.3 (2016) ready.
530 Login incorrect.
214-The following commands are implemented.
   USER    QUIT    PASS    SYST    HELP    PORT    PASV    LIST
   NLST    RETR    STOR    TYPE    MKD     RMD     DELE    PWD
   CWD     SITE    CDUP    RNFR    RNTO    NOOP    EP...
```

129.132.63.201
bleien-ost.ethz.ch
Swiss Federal Institute of Technology Zurich
Added on 2018-07-05 12:28:09 GMT
Switzerland, Zurich
Details

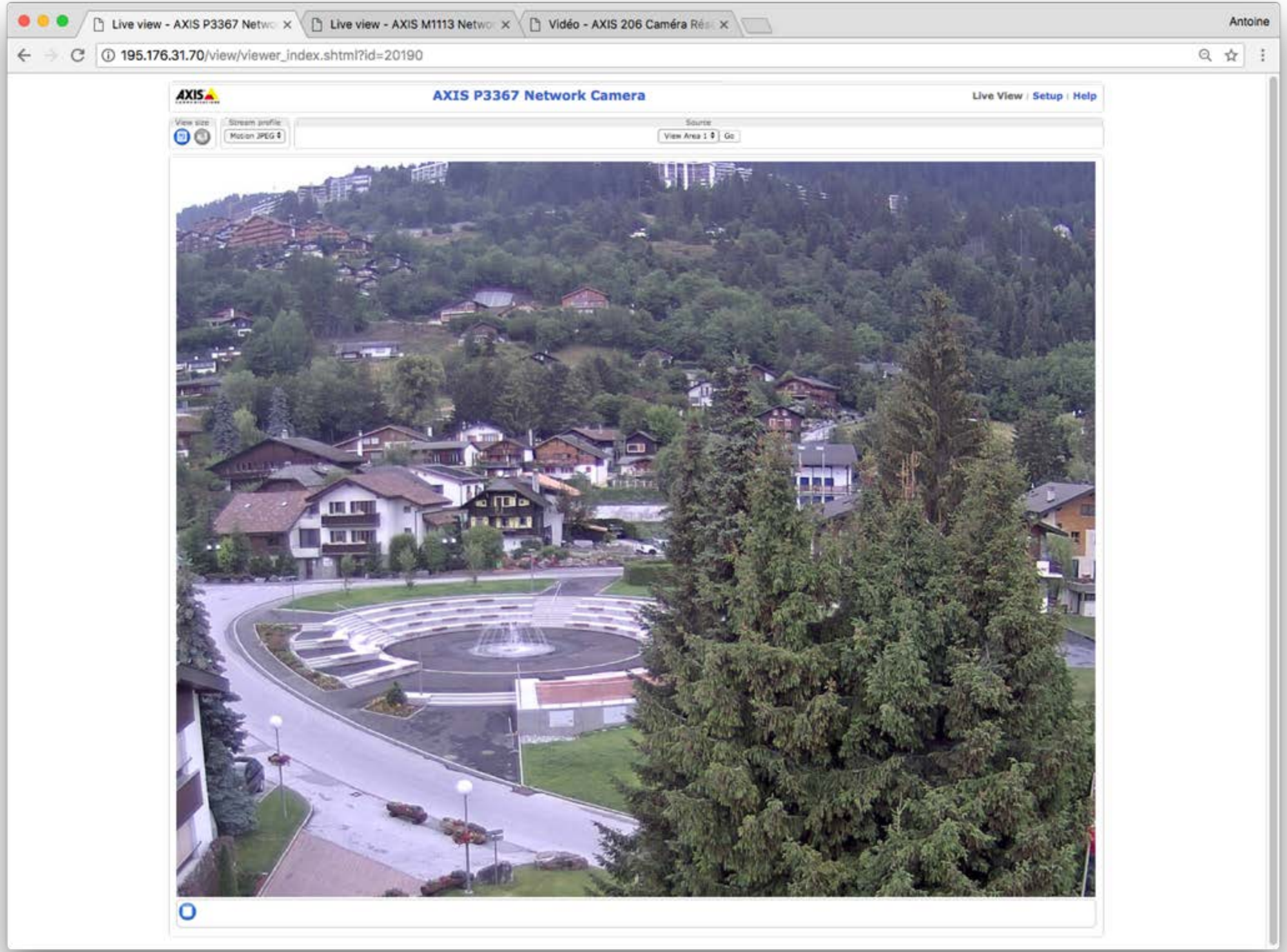
```
220 Axis 2100 Network Camera 2.43 Nov 08 2004 ready.
530 Login incorrect.
503 Bad sequence of commands.
503 Bad sequence of commands.
```

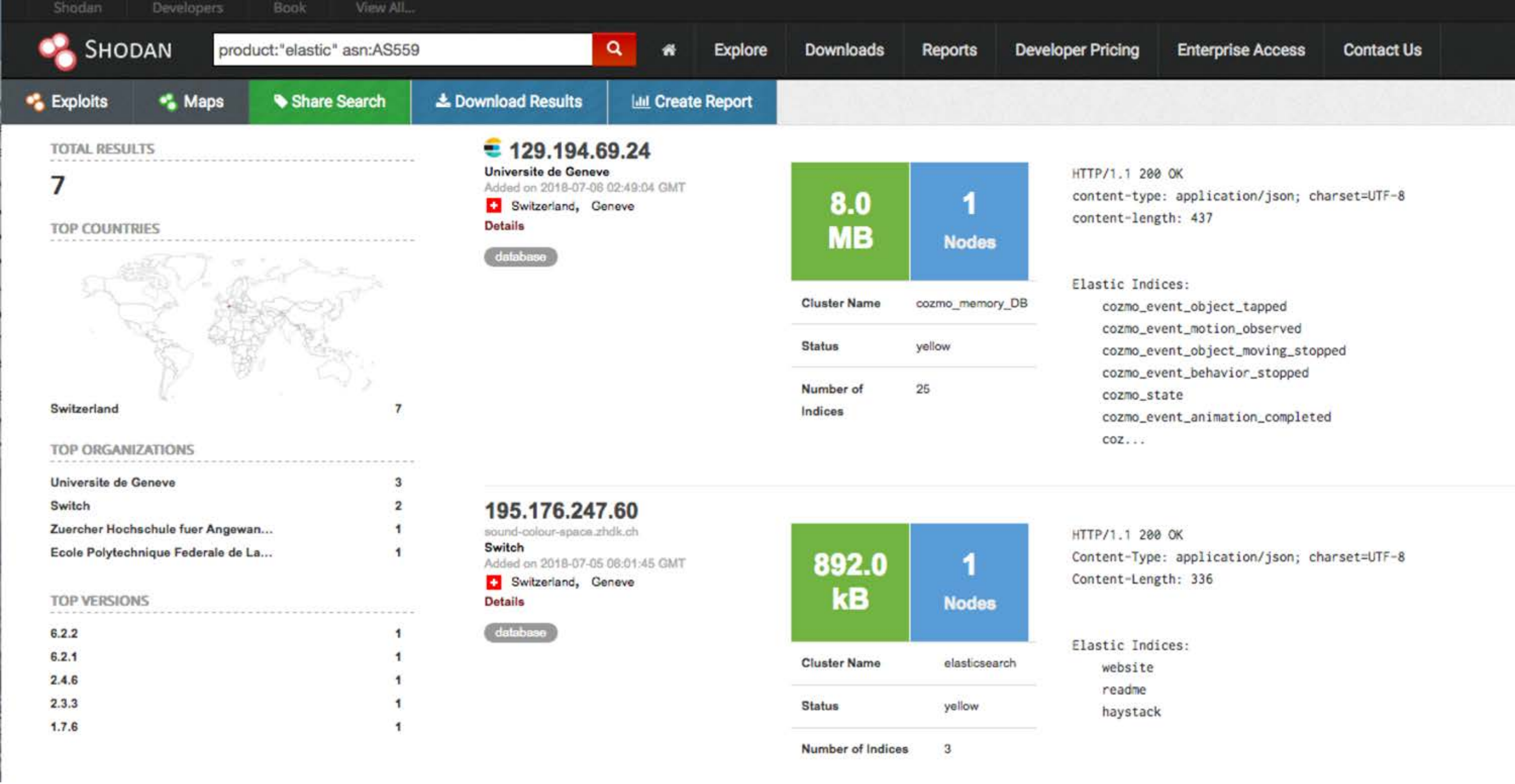
129.132.63.202
bleien-west.ethz.ch
Swiss Federal Institute of Technology Zurich
Added on 2018-07-05 12:25:34 GMT
Switzerland, Zurich
Details

```
220 Axis 2100 Network Camera 2.43 Nov 08 2004 ready.
530 Login incorrect.
503 Bad sequence of commands.
503 Bad sequence of commands.
```

129.132.131.215
dings5.ee.ethz.ch
Swiss Federal Institute of Technology Zurich
Added on 2018-07-05 12:25:19 GMT
Switzerland, Zurich
Details

```
220 AXIS 207MW Network Camera 4.44.1 (Dec 07 2009) ready.
530 Login incorrect.
214-The following commands are implemented.
   USER    QUIT    PASS    SYST    HELP    PORT    PASV    LIST
   NLST    RETR    STOR    TYPE    MKD     RMD     DELE    PWD
```


Live view - AXIS P3367 Netwo
Live view - AXIS M1113 Netwo
Vidéo - AXIS 206 Caméra Rés
Antoine
195.176.31.70/view/viewer_index.shtml?id=20190
AXIS
AXIS P3367 Network Camera
Live View | Setup | Help
View size
Stream profile
Motion JPEG
Source
View Area 1
Go



TOTAL RESULTS

7

TOP COUNTRIES

Switzerland	7

TOP ORGANIZATIONS

Universite de Geneve	3
Switch	2
Zuercher Hochschule fuer Angewan...	1
Ecole Polytechnique Federale de La...	1

TOP VERSIONS

6.2.2	1
6.2.1	1
2.4.6	1
2.3.3	1
1.7.6	1

129.194.69.24
Universite de Geneve
Added on 2018-07-08 02:49:04 GMT
Switzerland, Geneve

8.0 MB | 1 Nodes

Cluster Name	cozmo_memory_DB
Status	yellow
Number of Indices	25

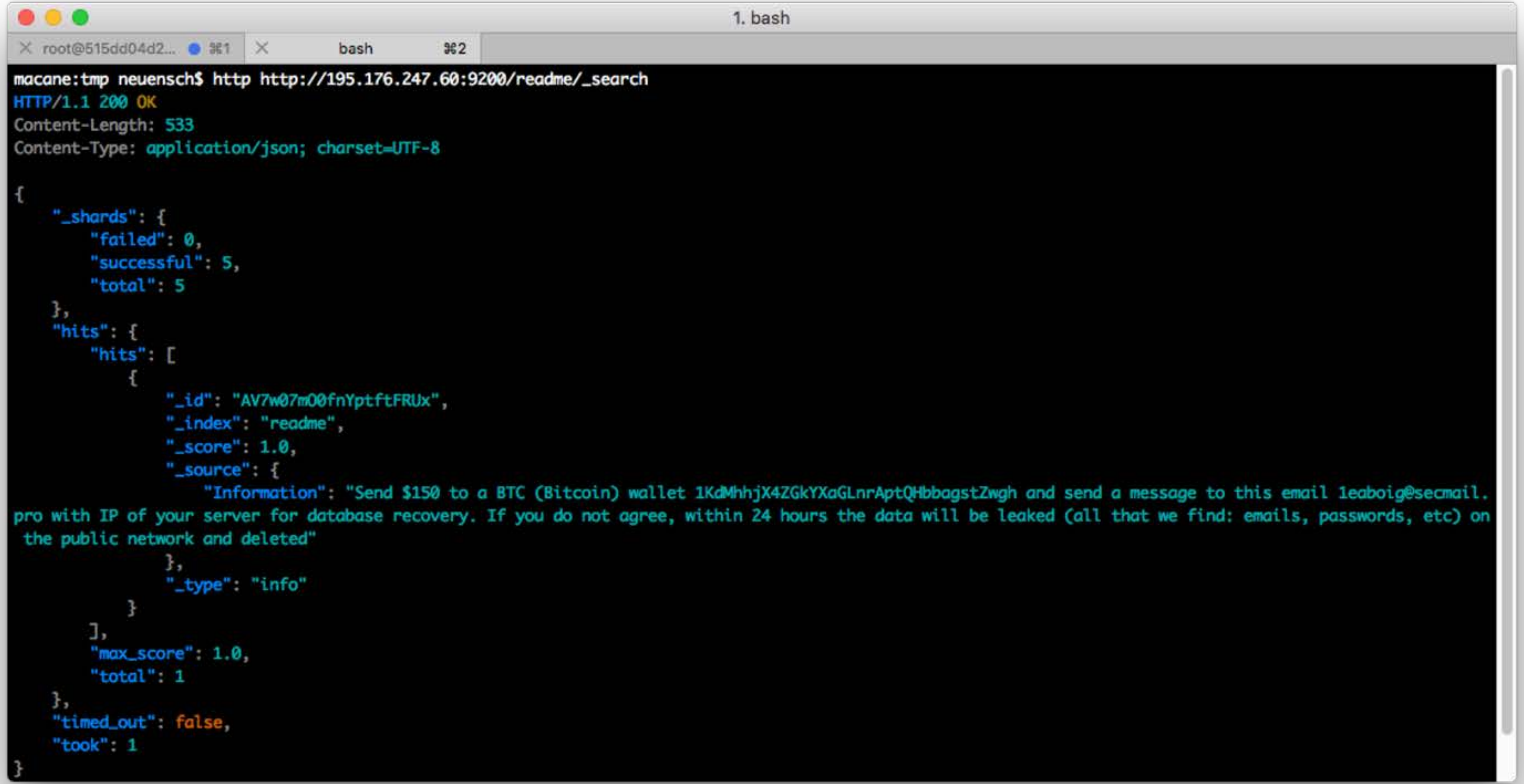
```
HTTP/1.1 200 OK
content-type: application/json; charset=UTF-8
content-length: 437


Elastic Indices:
    cozmo_event_object_tapped
    cozmo_event_motion_observed
    cozmo_event_object_moving_stopped
    cozmo_event_behavior_stopped
    cozmo_state
    cozmo_event_animation_completed
    coz...
```

195.176.247.60
sound-colour-space.zhdk.ch
Switch
Added on 2018-07-05 08:01:45 GMT
Switzerland, Geneve

892.0 kB | 1 Nodes

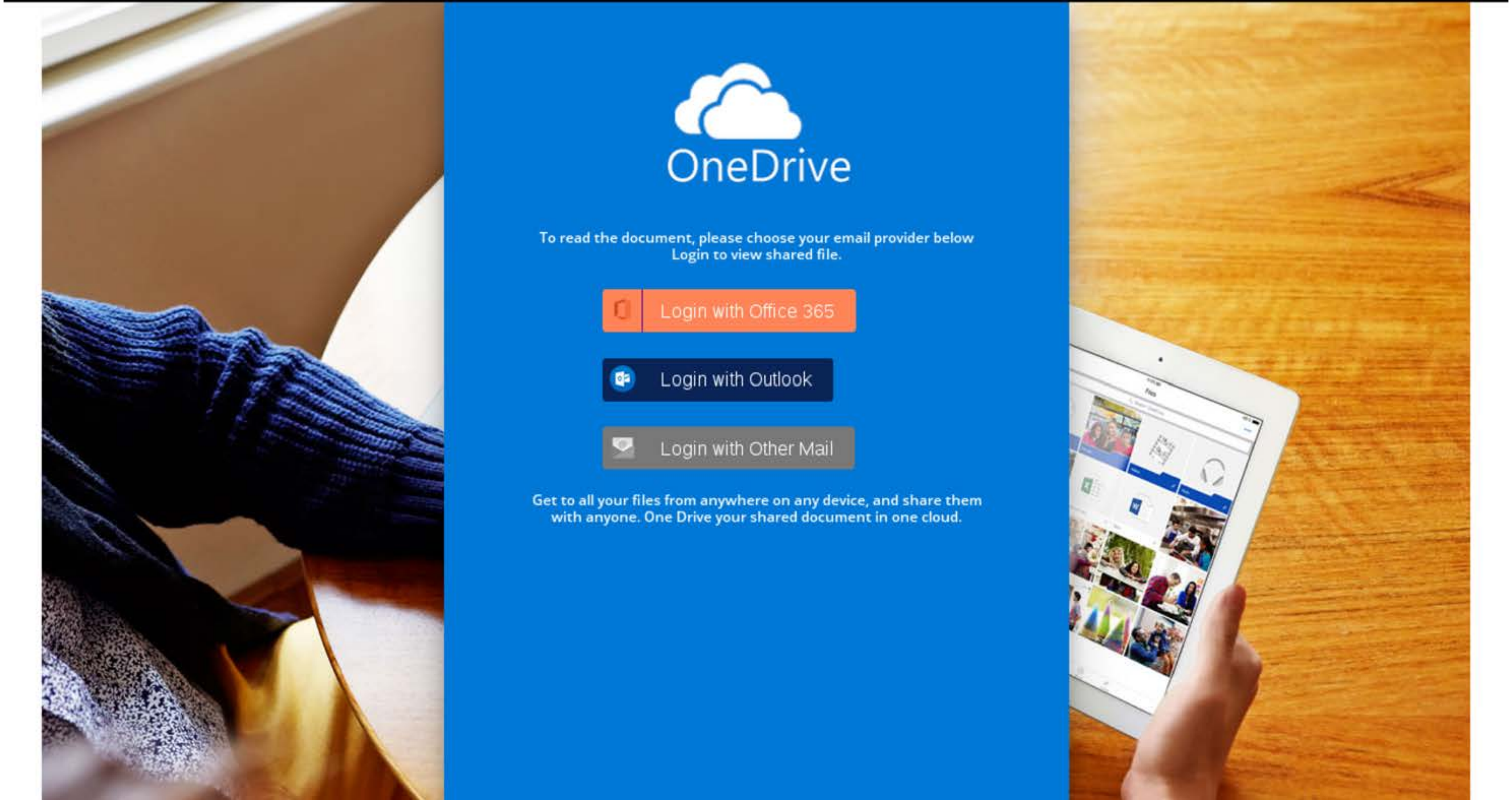
Cluster Name	elasticsearch
Status	yellow
Number of Indices	3

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 336


Elastic Indices:
    website
    readme
    haystack
```



```
macane:tmp neuensch$ http http://195.176.247.60:9200/readme/_search
HTTP/1.1 200 OK
Content-Length: 533
Content-Type: application/json; charset=UTF-8

{
    "_shards": {
        "failed": 0,
        "successful": 5,
        "total": 5
    },
    "hits": {
        "hits": [
            {
                "_id": "AV7w07mO0fnYptftFRUx",
                "_index": "readme",
                "_score": 1.0,
                "_source": {
                    "Information": "Send $150 to a BTC (Bitcoin) wallet 1KdMhhjX4ZGkYXaGLnrAptQHbbagstZwgh and send a message to this email 1eaboig@secmail.
pro with IP of your server for database recovery. If you do not agree, within 24 hours the data will be leaked (all that we find: emails, passwords, etc) on
 the public network and deleted"
                },
                "_type": "info"
            }
        ],
        "max_score": 1.0,
        "total": 1
    },
    "timed_out": false,
    "took": 1
}
```

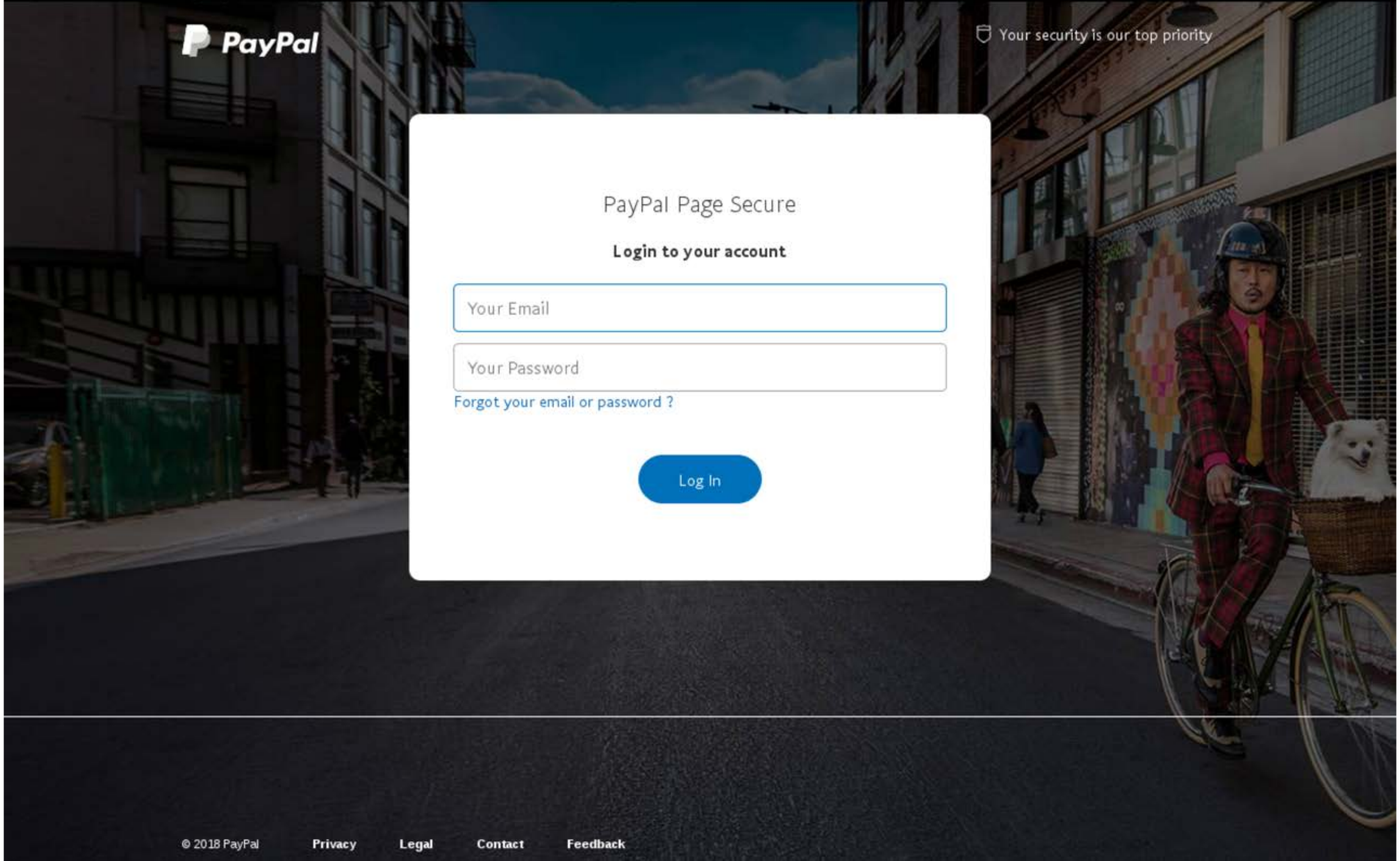
On 06.07.2018 08:39 the following URL was visited:
http://verindia.tk/one/index.php



To read the document, please choose your email provider below
Login to view shared file.

Get to all your files from anywhere on any device, and share them with anyone. One Drive your shared document in one cloud.

On 06.07.2018 04:32 the following URL was visited:
http://www.franelasjoey.com/cv/js/Secure/Login-account/index.php



Your security is our top priority

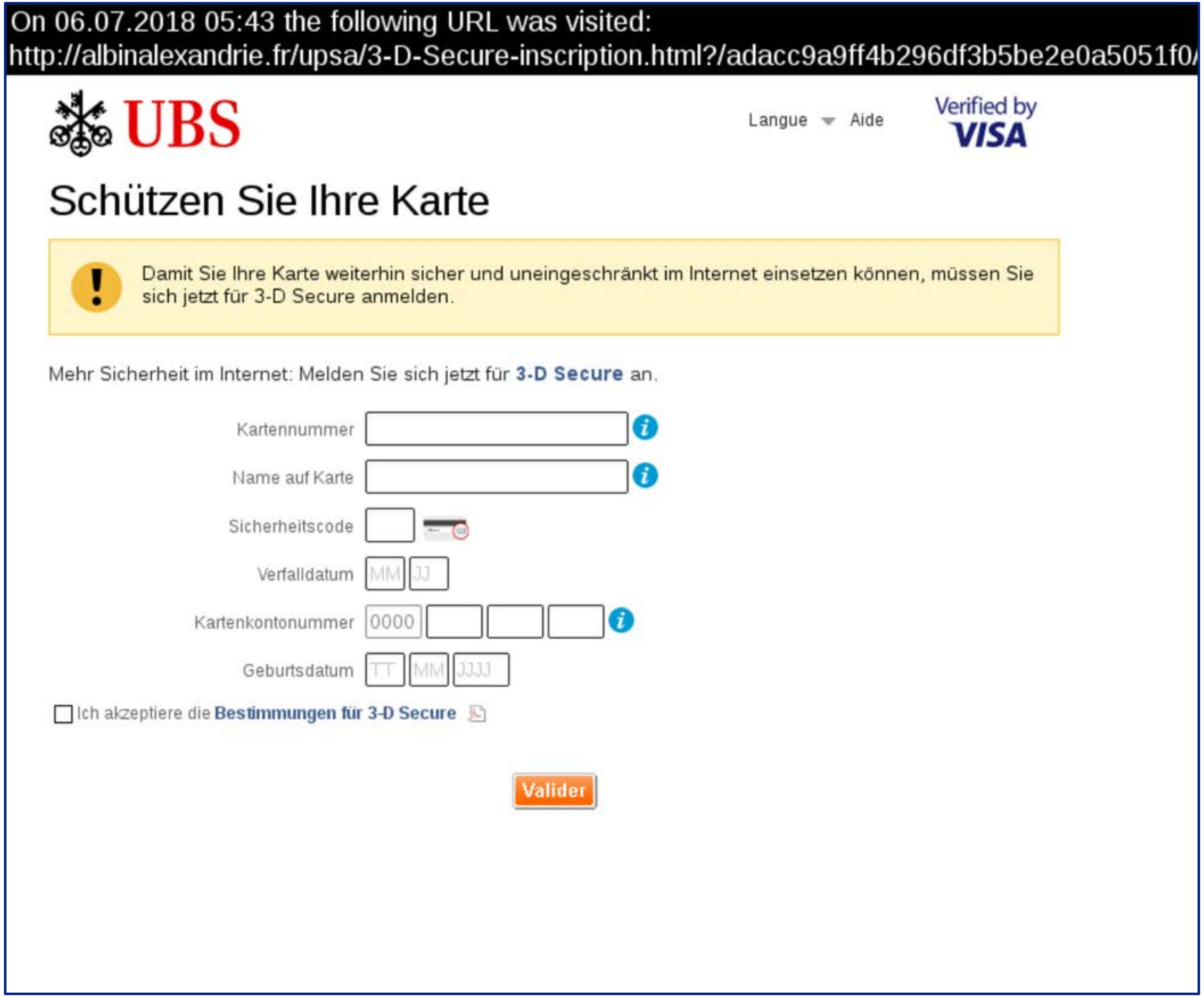
PayPal Page Secure

Login to your account

Your Email

Your Password

Forgot your email or password ?



On 06.07.2018 05:43 the following URL was visited:
http://albinalexandrie.fr/upsa/3-D-Secure-inscription.html?/adacc9a9ff4b296df3b5be2e0a5051f0/

Schützen Sie Ihre Karte

Damit Sie Ihre Karte weiterhin sicher und uneingeschränkt im Internet einsetzen können, müssen Sie sich jetzt für 3-D Secure anmelden.

Mehr Sicherheit im Internet: Melden Sie sich jetzt für **3-D Secure** an.

Kartennummer

Name auf Karte

Sicherheitscode

Verfalldatum MM JJ

Kartenkontonummer 0000

Geburtsdatum TT MM JJJJ

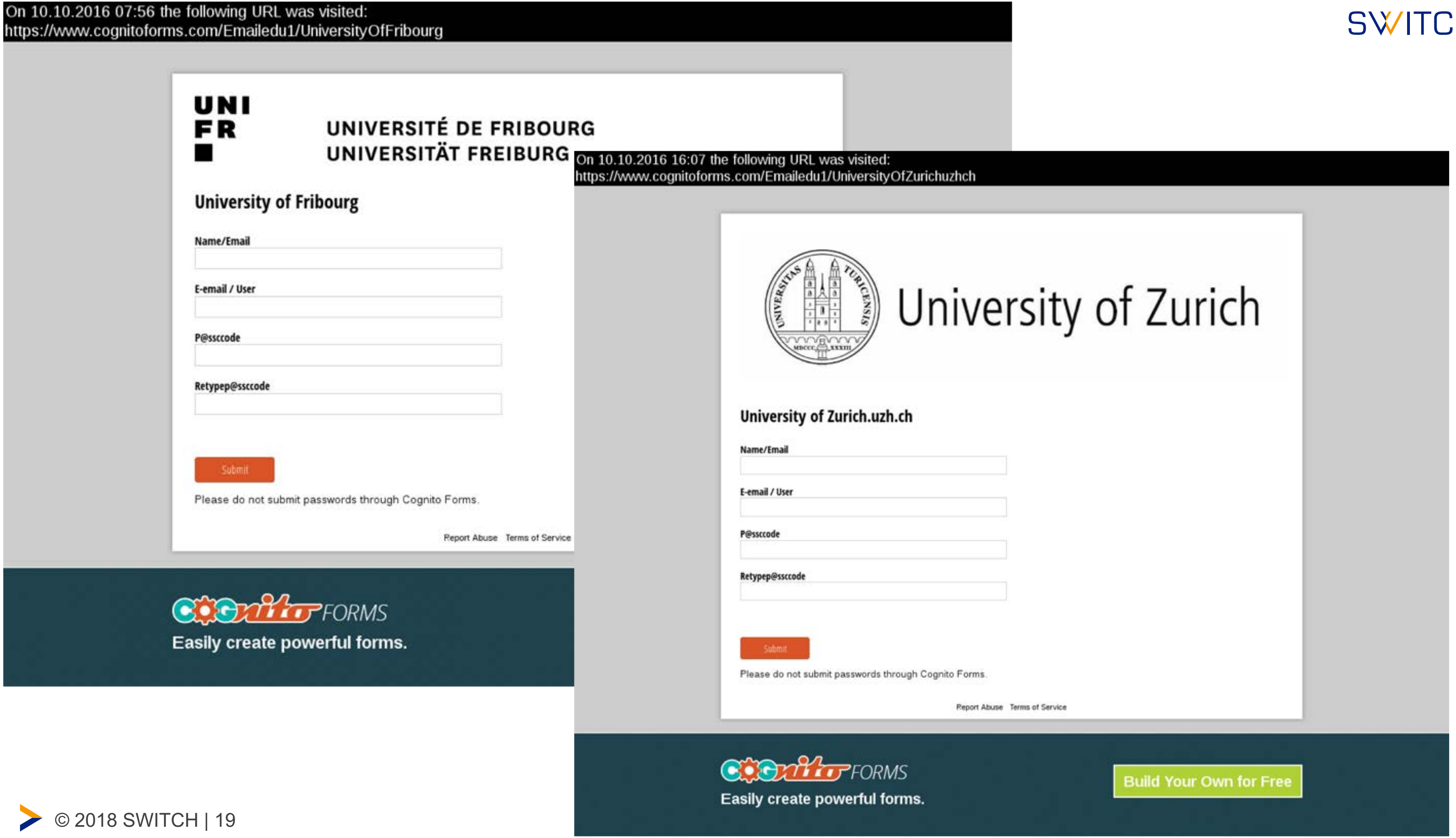
□ Ich akzeptiere die **Bestimmungen für 3-D Secure**

Sextortion

It appears that, *********'s your password. You may not know me and you are probably wondering why you are getting this e-mail, right? actually, I setup a trojans on the adult videos (porno) web-site and guess what, you visited this website to have fun (you know very well what What i'm saying is). Whilst you were watching videos, your internet browser started out operating like a RDP (Remote Desktop) which provided me accessibility to your screen and web cam. and then, my computer software obtained your entire contacts from the Messenger, Outlook, Facebook, along with emails. What did I really do? I produced a double-screen video recording. First part shows the video you were seeing (you've got a good taste haha . . .), and Second part shows the recording of your webcam. what exactly should you do? Well, in my opinion, $1300 is a fair price for our little hidden secret. You will make the payment by Bitcoin (if you do not know this, search "how to purchase bitcoin" in Google). BTC Address: 1PVnEqFZivhKce9sVS9SFjZ2bT75fJjNjK (It is case sensitive, so copy and paste it) Important: You've one day in order to make the payment. (I've a completely unique pixel in this e-mail, and at this moment I am aware that you have read this email message). If I do not get the BitCoins, I will certainly send out your video recording to all of your contacts including family members, colleagues, and so forth. Having said that, if I receive the payment, I'll destroy the video immidiately. If you'd like evidence, reply with "Yes!" and I will certainly send out your videos to your 6 contacts. It is a non-negotiable offer, that being said don't waste my personal time and yours by answering this message.

Semi-Targeted Attacks

- (Spear-)Phishing
- Motivation:
  - Sell Network Access (VPN)
  - Gain access to Intellectual Property (IP) shared exclusively in the higher education community



On 10.10.2016 07:56 the following URL was visited:
https://www.cognitoforms.com/Emailedu1/UniversityOfFribourg

UNI FR

UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG

University of Fribourg

Name/Email

E-email / User

P@ssccode

Retypep@ssccode

Please do not submit passwords through Cognito Forms.

On 10.10.2016 16:07 the following URL was visited:
https://www.cognitoforms.com/Emailedu1/UniversityOfZurichuzhch

University of Zurich

University of Zurich.uzh.ch

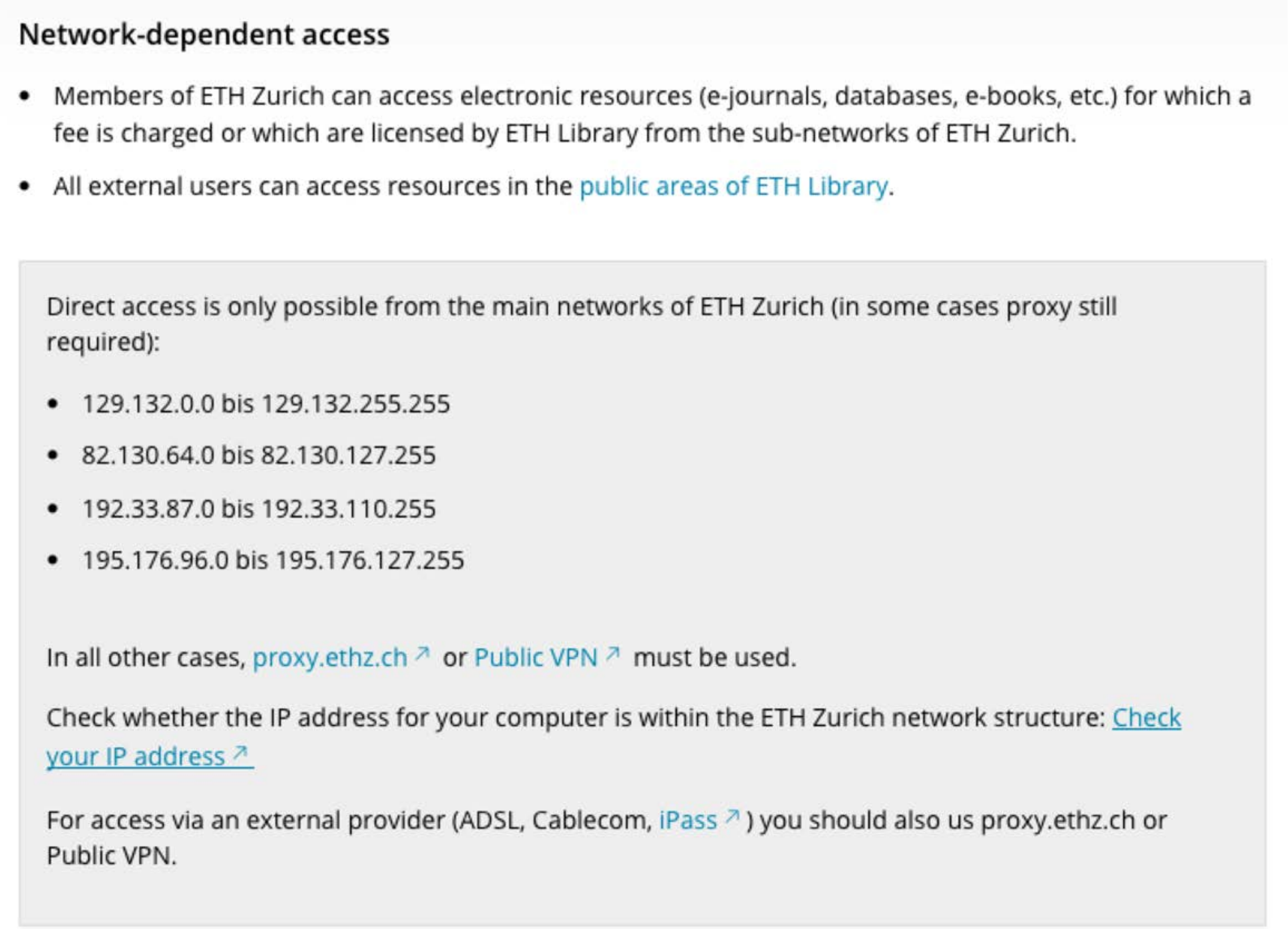
Name/Email

E-email / User

P@ssccode

Retypep@ssccode

Please do not submit passwords through Cognito Forms.



Network-dependent access

- Members of ETH Zurich can access electronic resources (e-journals, databases, e-books, etc.) for which a fee is charged or which are licensed by ETH Library from the sub-networks of ETH Zurich.
- All external users can access resources in the public areas of ETH Library.

Direct access is only possible from the main networks of ETH Zurich (in some cases proxy still required):

- 129.132.0.0 bis 129.132.255.255
- 82.130.64.0 bis 82.130.127.255
- 192.33.87.0 bis 192.33.110.255
- 195.176.96.0 bis 195.176.127.255

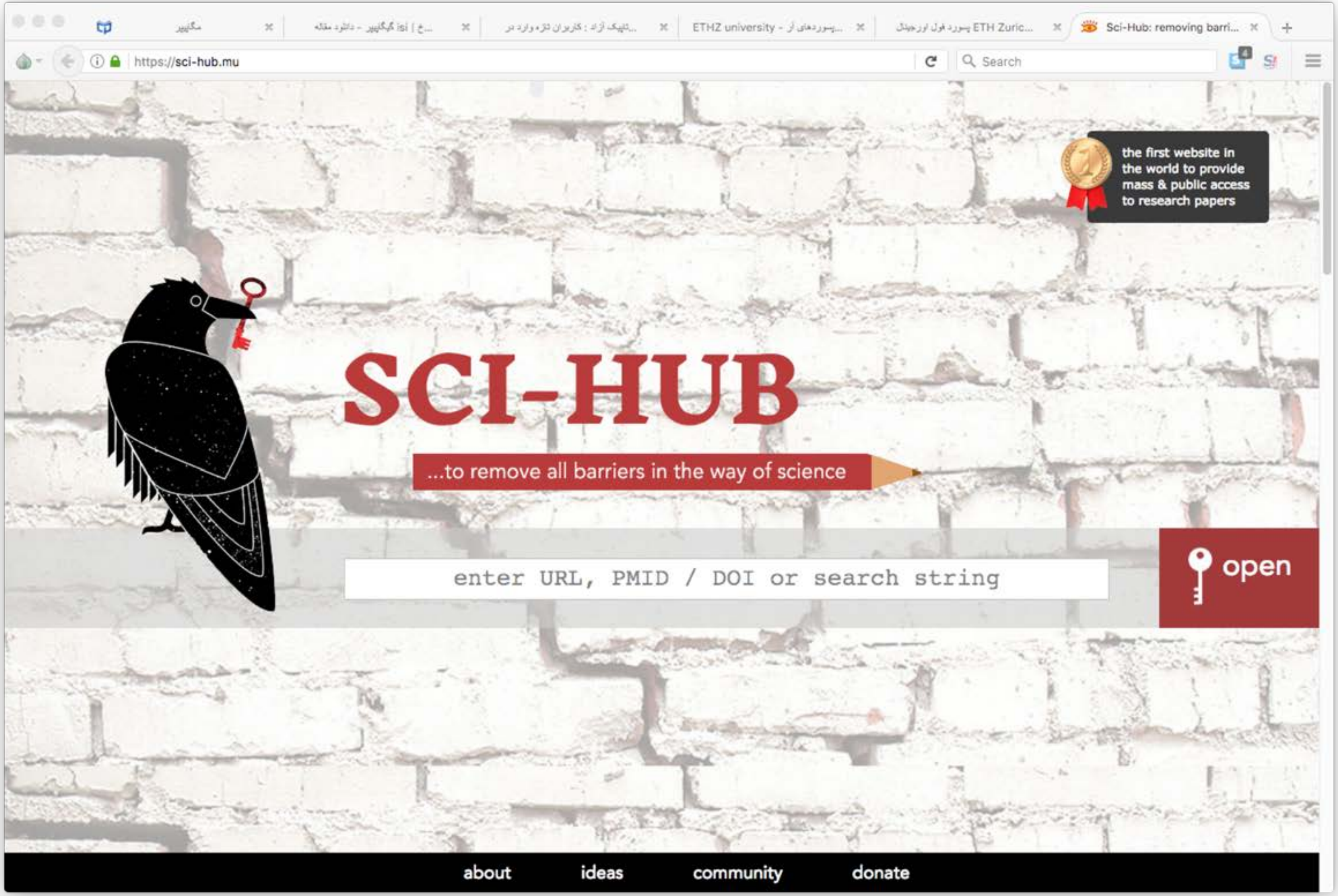
In all other cases, proxy.ethz.ch ↗ or Public VPN ↗ must be used.

Check whether the IP address for your computer is within the ETH Zurich network structure: Check your IP address ↗

For access via an external provider (ADSL, Cablecom, iPass ↗) you should also us proxy.ethz.ch or Public VPN.

ELSEVIER

JSTOR

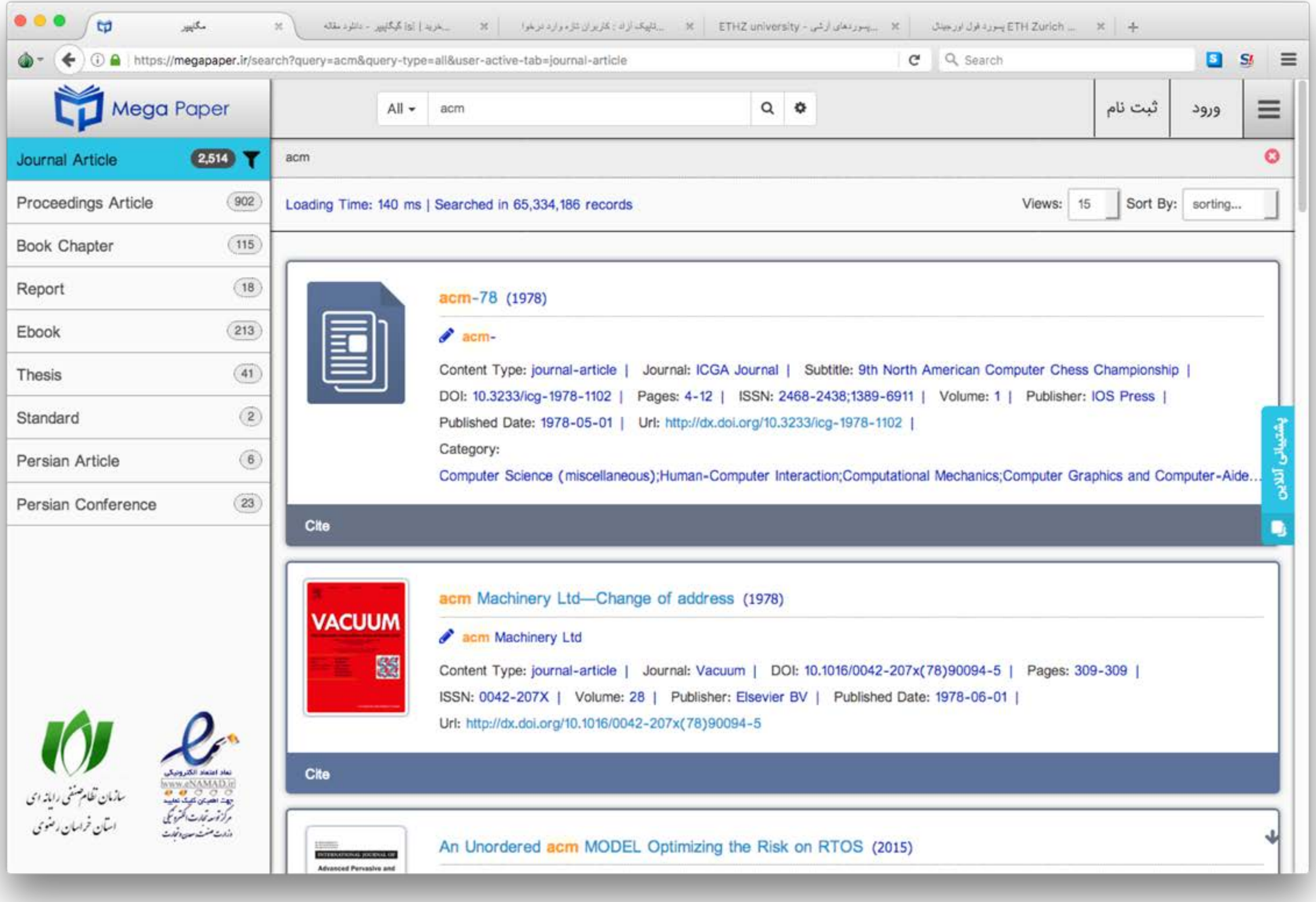


the first website in the world to provide mass & public access to research papers

...to remove all barriers in the way of science

enter URL, PMID / DOI or search string

SWITCH


مگاپیپر
...خرید | isi گیگاپیپر - دانلود مقاله
...تاپیک آزاد : کاربران تازه وارد درخوا
ETHZ university - ...پسوردهای ارشی
پسورد فول اورجینال ETH Zurich ...
Search
Mega Paper
All
ثبت نام
ورود
پشتیبانی آنلاین
سازمان نظام صنفی رایانه ای
استان خراسان رضوی
نماد اعتماد الکترونیکی
www.eNAMAD.ir
جهت اطمینان کلیک نمایید
مرکز توسعه تجارت الکترونیکی
وزارت صنعت معدن و تجارت

https://megapaper.ir/search?query=acm&query-type=all&user-active-tab=journal-article

acm

Journal Article	2,514
Proceedings Article	902
Book Chapter	115
Report	18
Ebook	213
Thesis	41
Standard	2
Persian Article	6
Persian Conference	23

acm

Loading Time: 140 ms | Searched in 65,334,186 records

Views: 15 Sort By: sorting...

acm-78 (1978)

acm-

Content Type: journal-article | Journal: ICGA Journal | Subtitle: 9th North American Computer Chess Championship |
DOI: 10.3233/icg-1978-1102 | Pages: 4-12 | ISSN: 2468-2438;1389-6911 | Volume: 1 | Publisher: IOS Press |
Published Date: 1978-05-01 | Url: http://dx.doi.org/10.3233/icg-1978-1102 |
Category:
Computer Science (miscellaneous);Human-Computer Interaction;Computational Mechanics;Computer Graphics and Computer-Aide...

Cite

acm Machinery Ltd—Change of address (1978)

acm Machinery Ltd

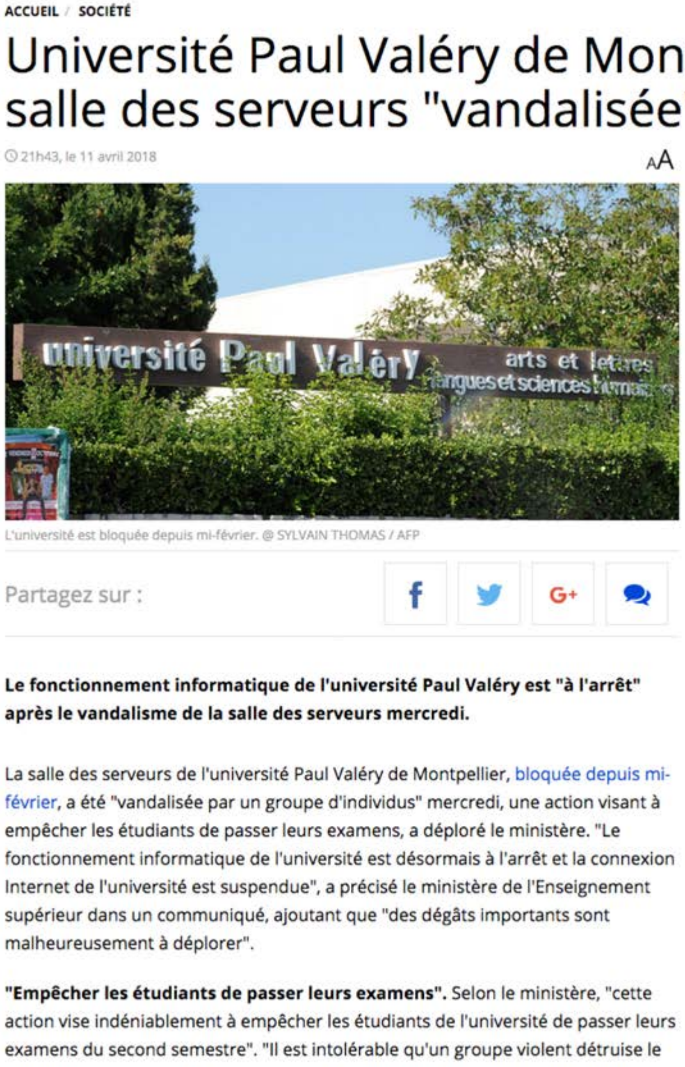
Content Type: journal-article | Journal: Vacuum | DOI: 10.1016/0042-207x(78)90094-5 | Pages: 309-309 |
ISSN: 0042-207X | Volume: 28 | Publisher: Elsevier BV | Published Date: 1978-06-01 |
Url: http://dx.doi.org/10.1016/0042-207x(78)90094-5

Cite

An Unordered acm MODEL Optimizing the Risk on RTOS (2015)

Targeted Attacks

- Sabotage
- Espionage
- Hacktivism



ACCUEIL / SOCIÉTÉ

Université Paul Valéry de Montpellier : la salle des serveurs "vandalisée"

21h43, le 11 avril 2018

L'université est bloquée depuis mi-février. @ SYLVAIN THOMAS / AFP

Le fonctionnement informatique de l'université Paul Valéry est "à l'arrêt" après le vandalisme de la salle des serveurs mercredi.

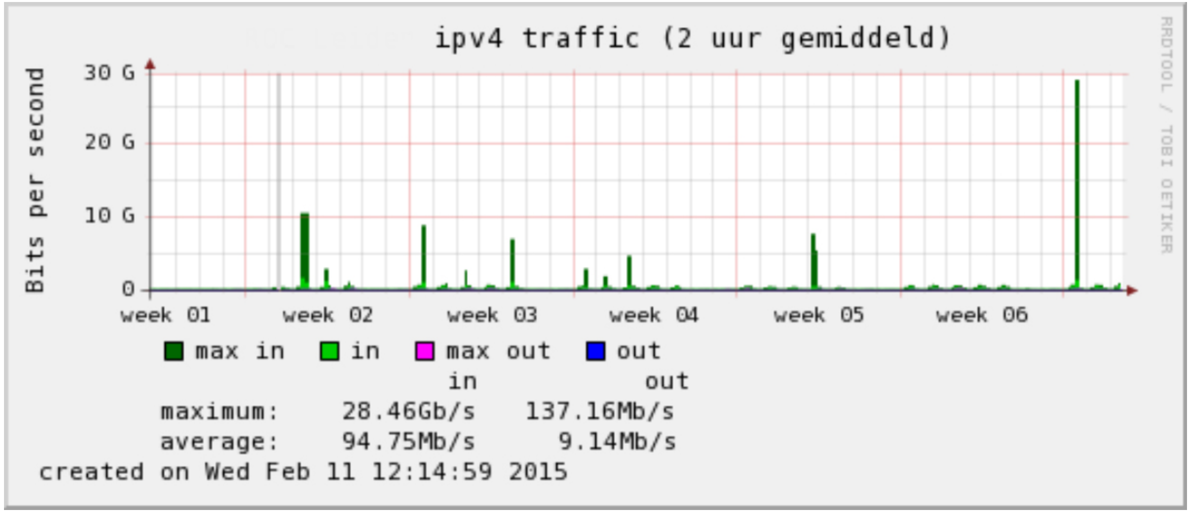
La salle des serveurs de l'université Paul Valéry de Montpellier, bloquée depuis mi-février, a été "vandalisée par un groupe d'individus" mercredi, une action visant à empêcher les étudiants de passer leurs examens, a déploré le ministère. "Le fonctionnement informatique de l'université est désormais à l'arrêt et la connexion Internet de l'université est suspendue", a précisé le ministère de l'Enseignement supérieur dans un communiqué, ajoutant que "des dégâts importants sont malheureusement à déplorer".

"Empêcher les étudiants de passer leurs examens". Selon le ministère, "cette action vise indéniablement à empêcher les étudiants de l'université de passer leurs examens du second semestre". "Il est intolérable qu'un groupe violent détruise le

Selon le ministère, "cette action vise indéniablement à empêcher les étudiants de l'université de passer leurs examens du second semestre".

http://www.europe1.fr/societe/universite-paul-valery-de-montpellier-la-salle-des-serveurs-vandalisee-3624359

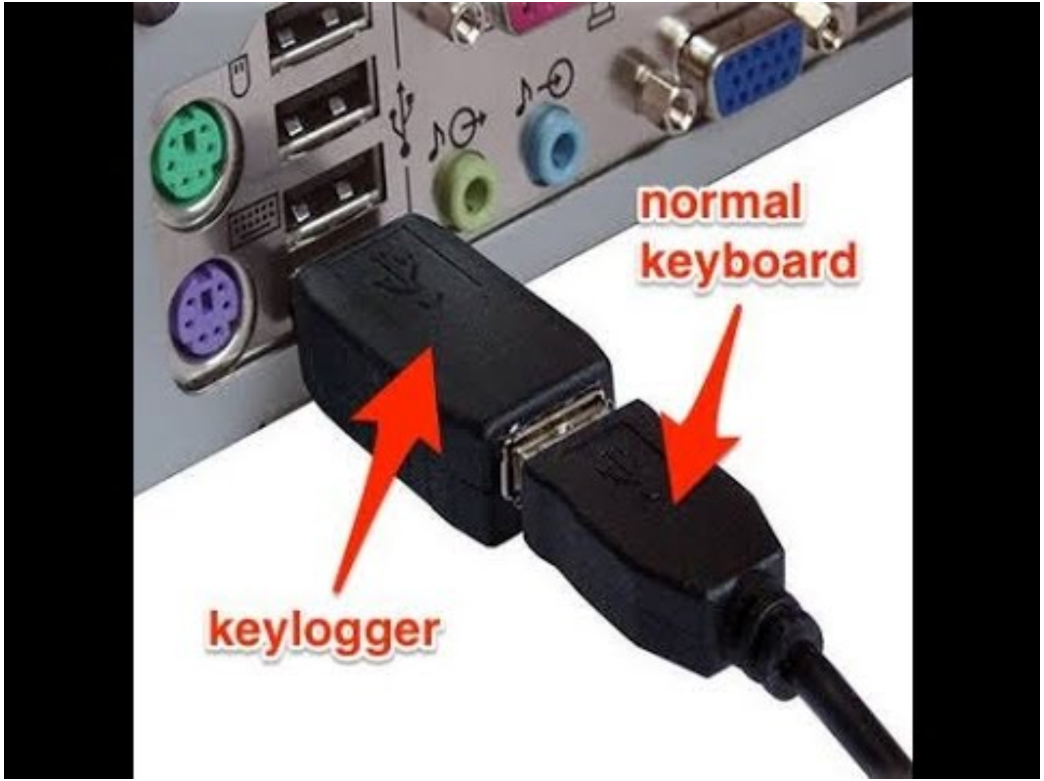
DDoS Attacks targets Online Exams



```
                 in          out
maximum:     28.46Gb/s   137.16Mb/s
average:     94.75Mb/s     9.14Mb/s
created on Wed Feb 11 12:14:59 2015
```

https://blog.surf.nl/en/surfcert-ddos-protection/

USB Keyloggers



SWITCH

Working for a better digital world