Incident Response for .ch

Drive-By Exploits – Mitigation and Takedown for .ch/.li

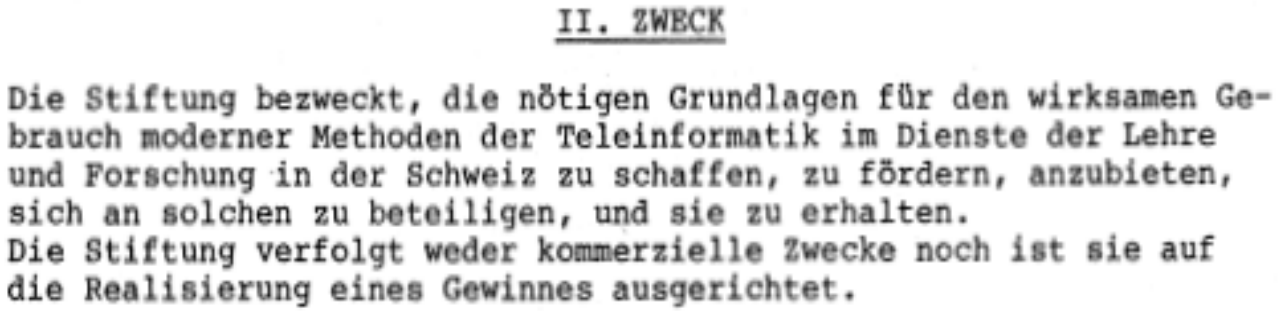
SWITCH

Michael Hausding
michael.hausding@switch.ch

Bern 22. October 2014 – TLP White

SWITCH

- Private foundation under Swiss law
- Established 1987 by the Swiss federation the university cantons.



II. ZWECK

Die Stiftung bezweckt, die nötigen Grundlagen für den wirksamen Gebrauch moderner Methoden der Teleinformatik im Dienste der Lehre und Forschung in der Schweiz zu schaffen, zu fördern, anzubieten, sich an solchen zu beteiligen, und sie zu erhalten.
Die Stiftung verfolgt weder kommerzielle Zwecke noch ist sie auf die Realisierung eines Gewinnes ausgerichtet.

'The foundation's purpose is to establish, to foster, to offer, to participate in and to maintain the basis for an effective use of up-to-date methods of teleinformatics in research and education in Switzerland. The foundation has no commercial targets, nor is it aligned with profit-making.'

- Today SWITCH offers high quality services in key areas where no commercial alternatives exist

© 2014 SWITCH

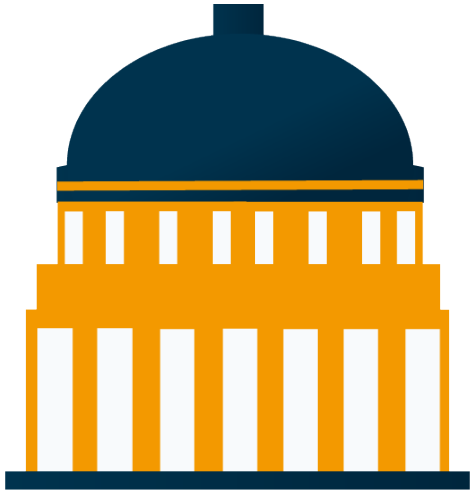
Security-Team

- Established 1996
- Ten fulltime Members
- Internationally acclaimed experts
- Comprehensive Expertise

We protect our customer's critical ICT Infrastructure

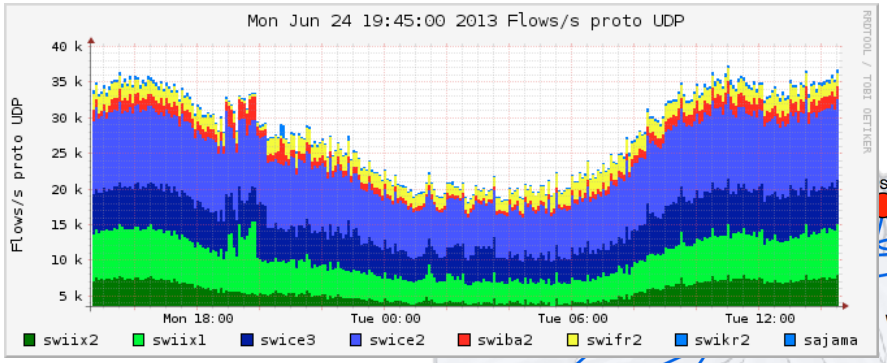
© 2014 SWITCH

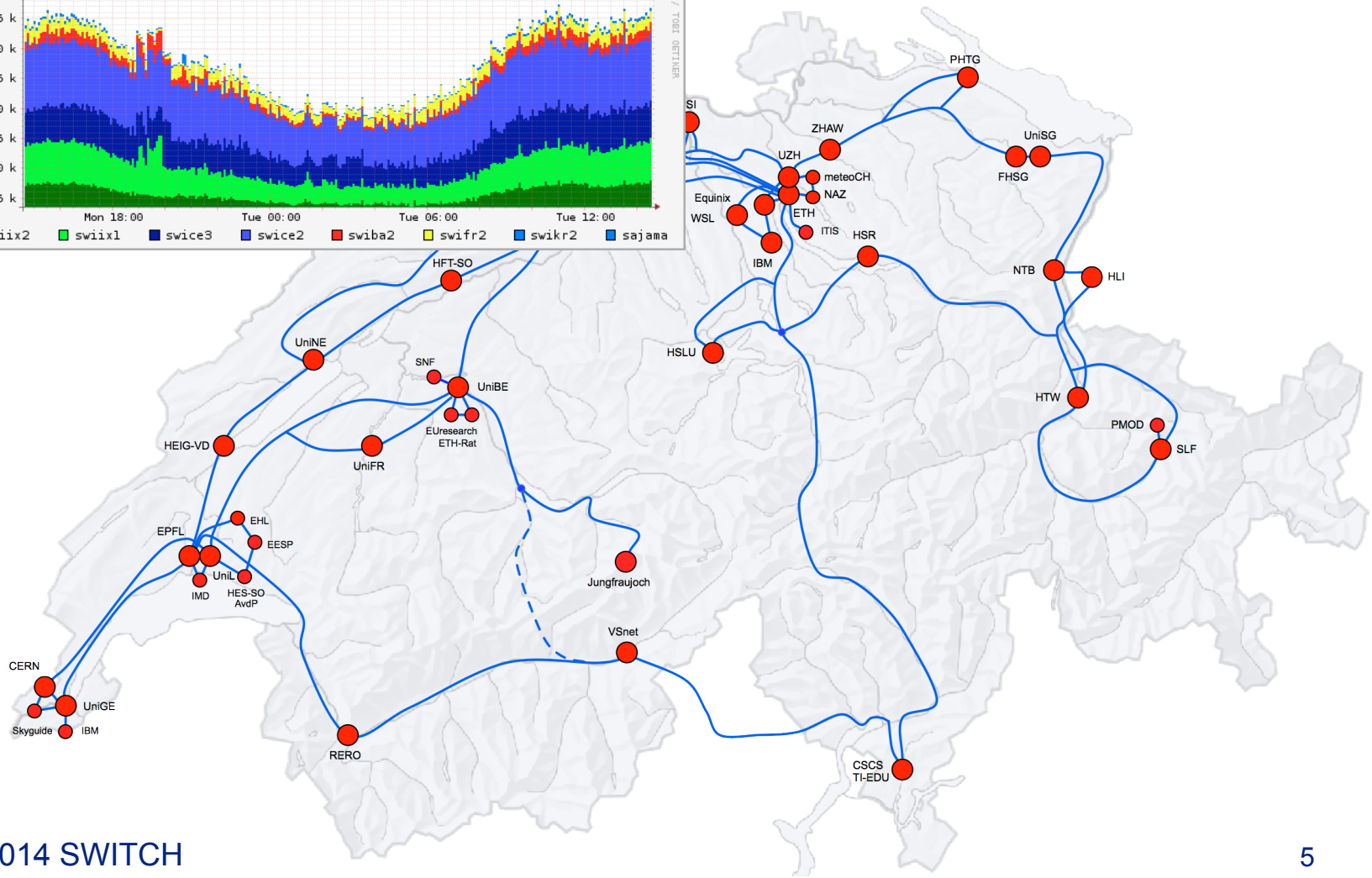
Customers



© 2014 SWITCH

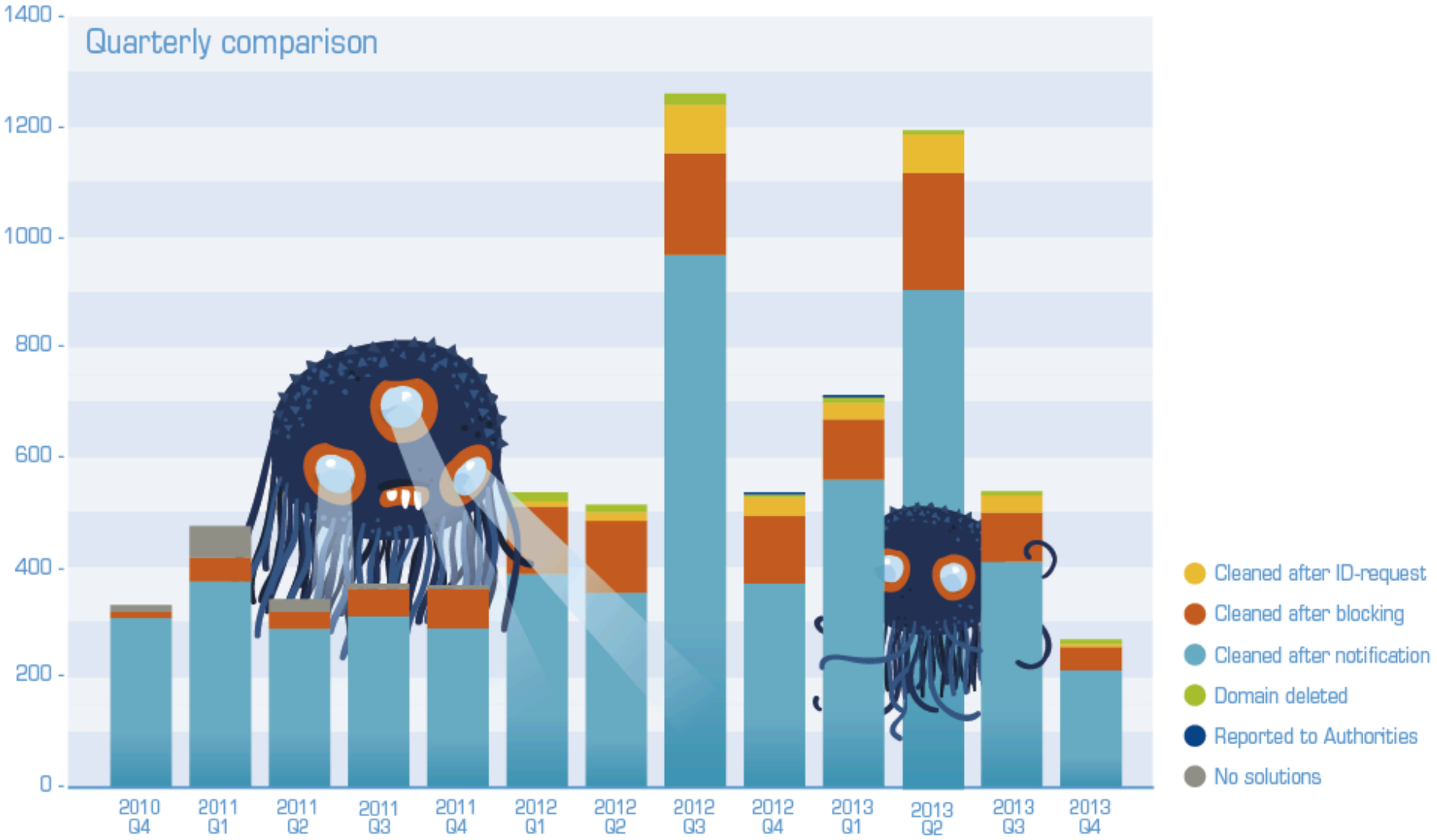
Universities





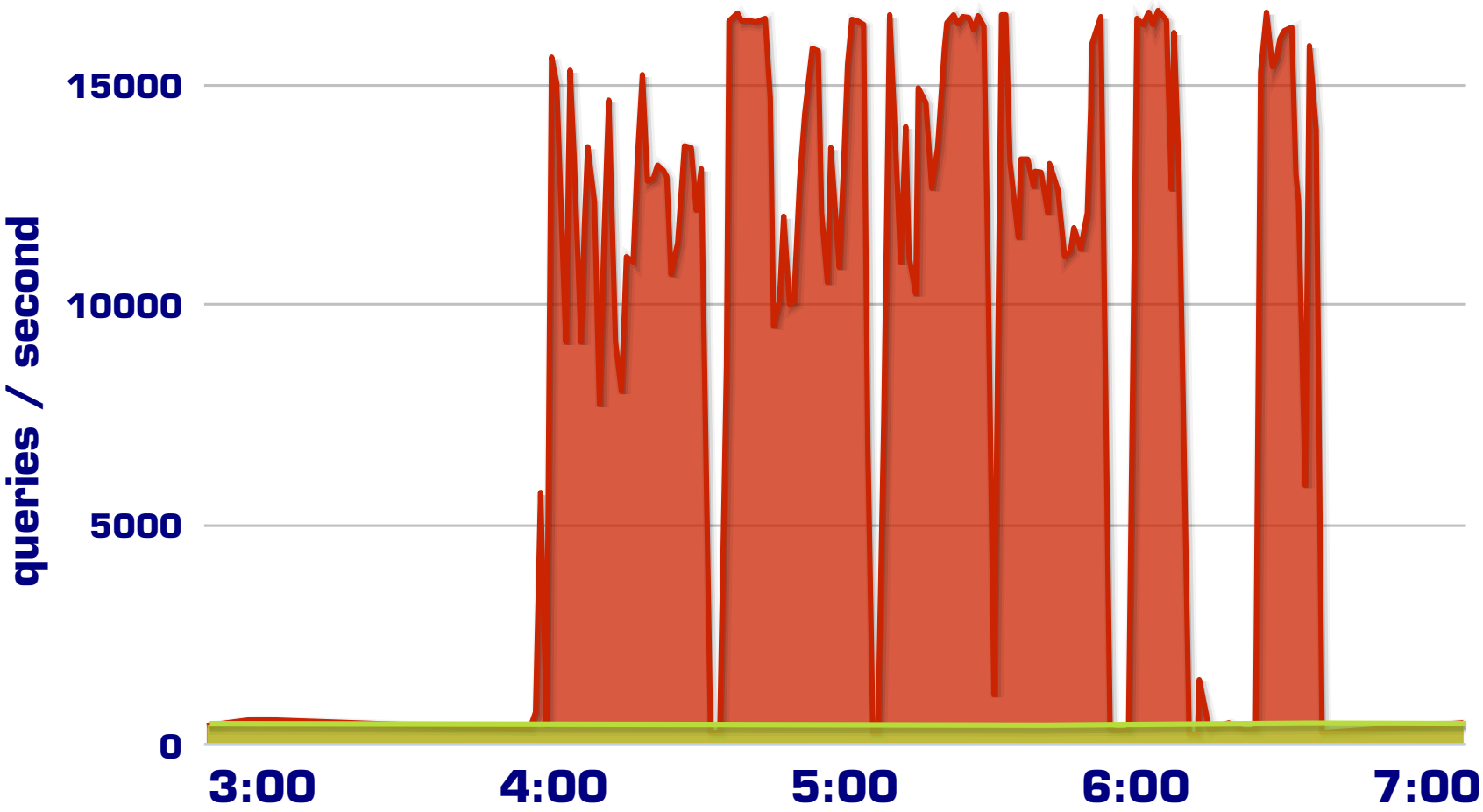
© 2014 SWITCH

Cleaned .ch&.li websites



© 2014 SWITCH

DNS: a critical infrastructure



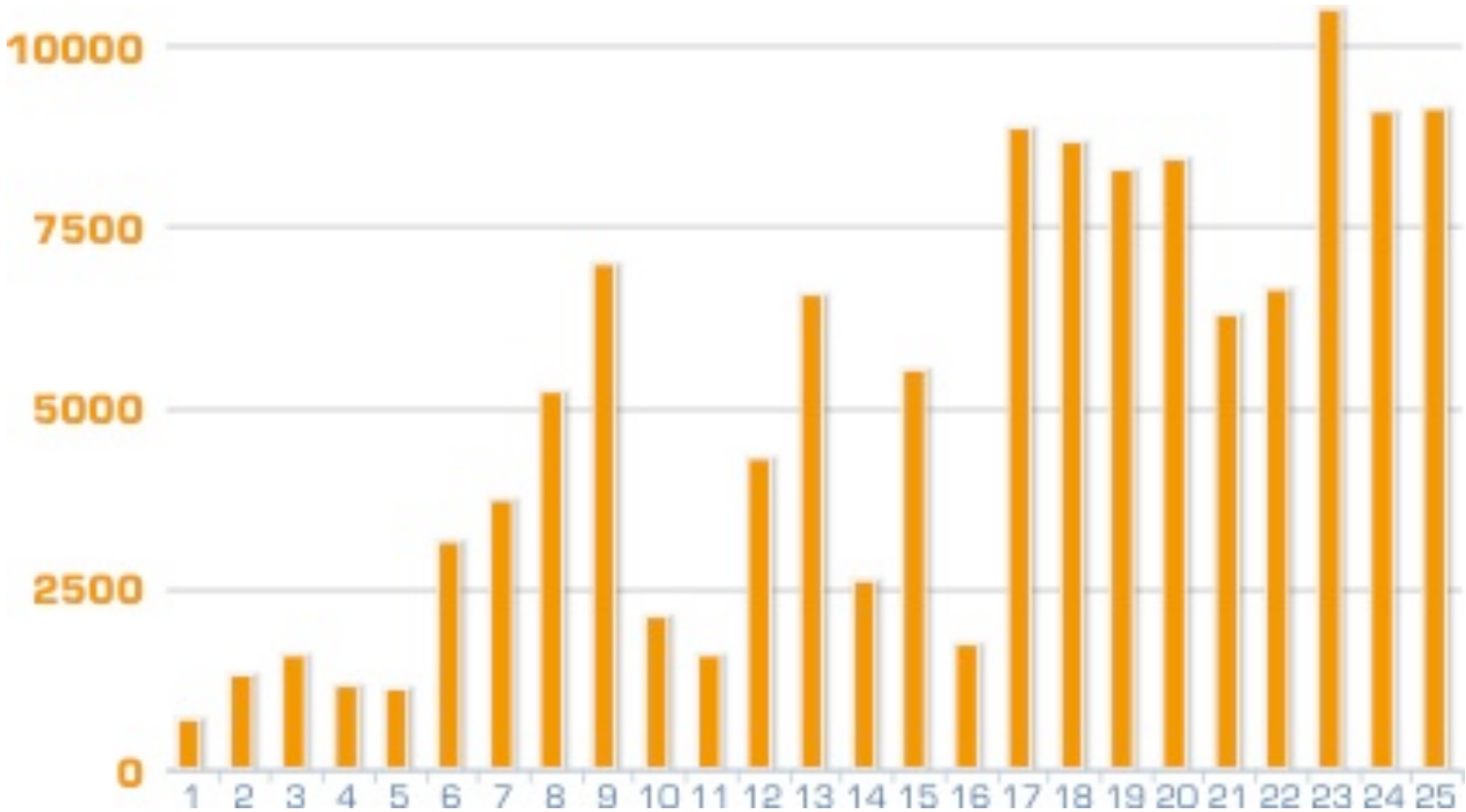
© 2014 SWITCH

Banks: A profitable Target

```
Record: 37
          id: 20007
        type: 0x10000001
        size: 633
   real-size: 1546
 url trigger: 'values: 0x353064, 0x10, 0x0,
0x0
https://inba.aikb.ch/WEB_XSA_LOGIN/*

values: 0x1f3064, 0x10, 0x0, 0x0
http*.akb.ch/*

values: 0x2d3064, 0x10, 0x0, 0x0
https://eb.akb.ch/akbLogin/*

values: 0x363064, 0x10, 0x0, 0x0
https://inba.appkb.ch/WEB_XSA_LOGIN/*
```

© 2014 SWITCH

ASReports to > 500AS in Switzerland



© 2014 SWITCH

Incident Response for .ch

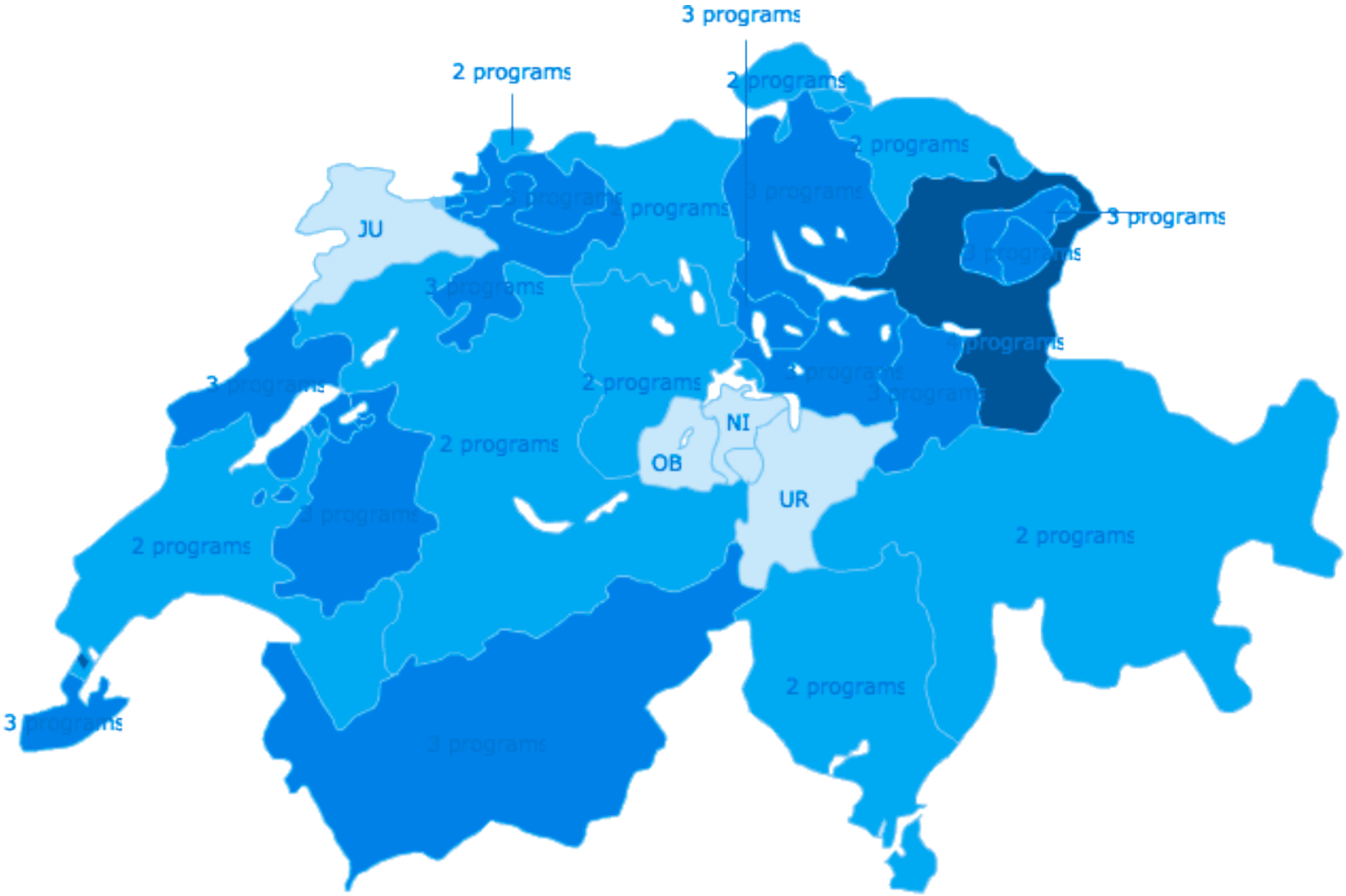
Threat landscape

	Top Threats	Trends assessed in 2012	Current trends mid 2013	
1.	Drive-by exploits	↑	↑	Interesting developments
2.	Worms/Trojans	↑	↑	
3.	Code Injection	↑	↑	Interesting developments
4.	Exploit Kits	↑	↑	
5.	Botnets	↑	↑	Interesting developments
6.	Denial of Service	→	↑	A change has been identified
7.	Phishing	→	→	
8.	Compromising Confidential Information	↑	↑	

© 2014 SWITCH

https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/

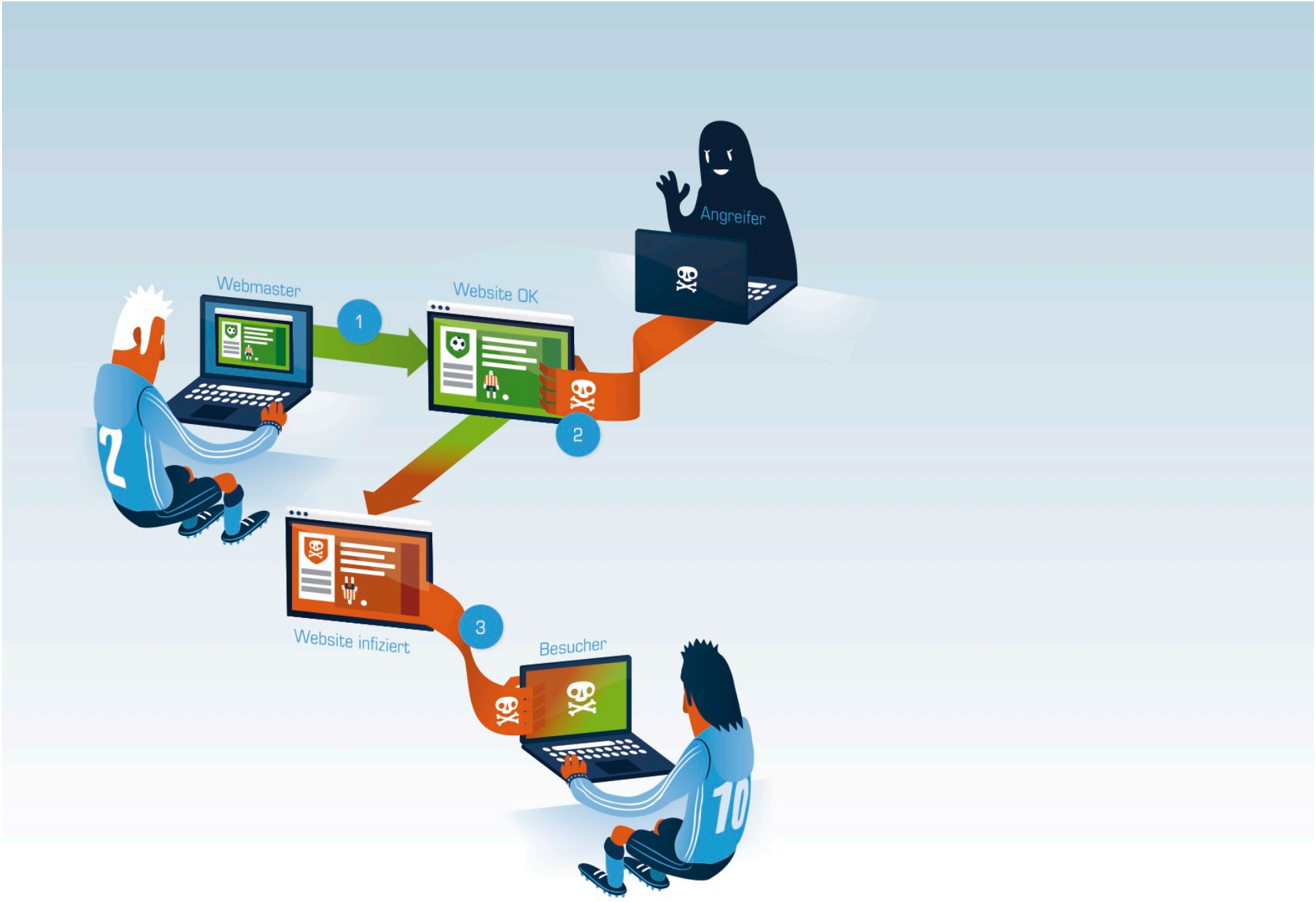
Insecure Programs on Swiss PCs



© 2014 SWITCH

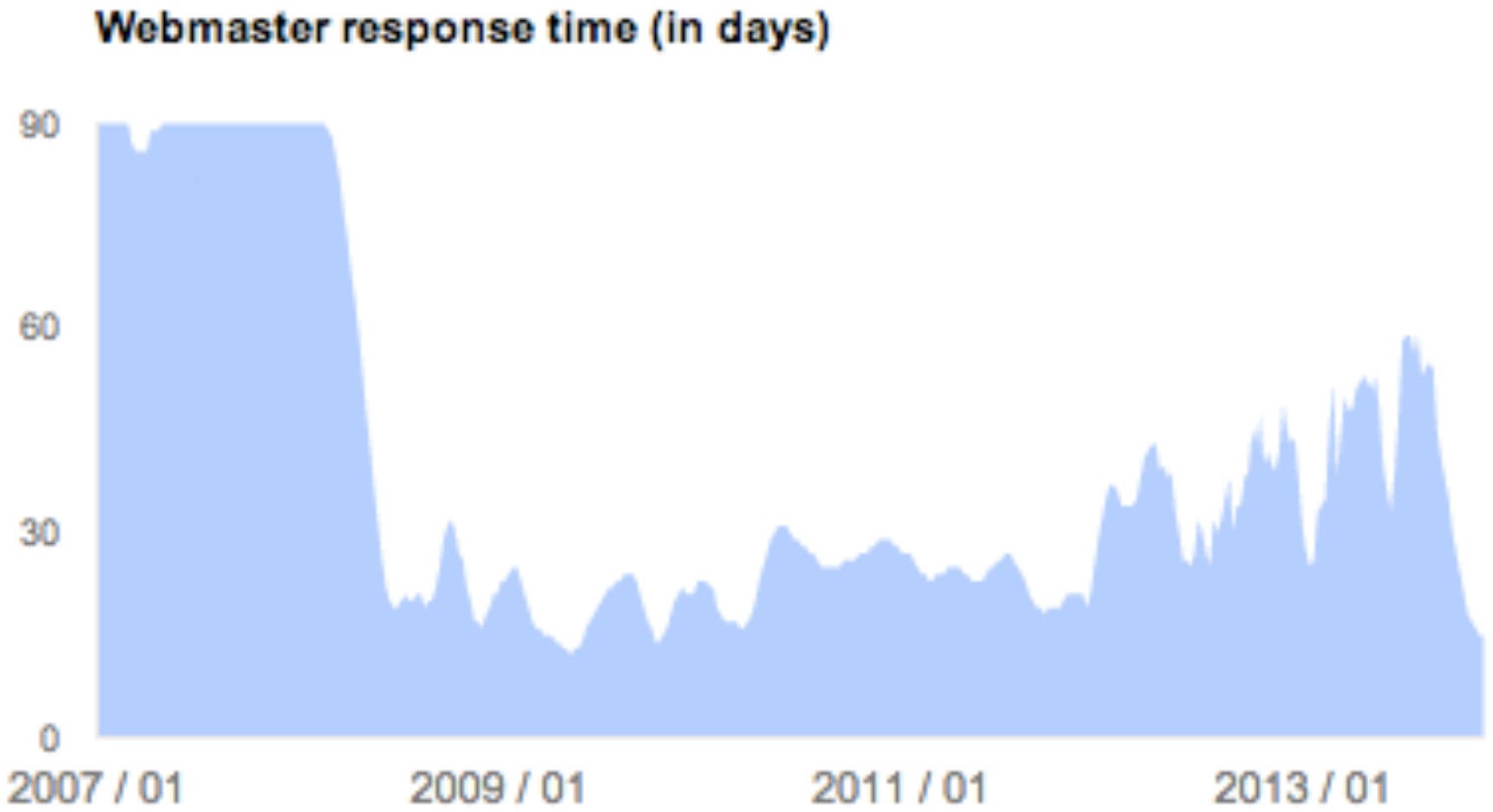
Source: Secunia

Drive-By Exploit?


Webmaster
1
Website OK
Angreifer
2
Website infiziert
3
Besucher

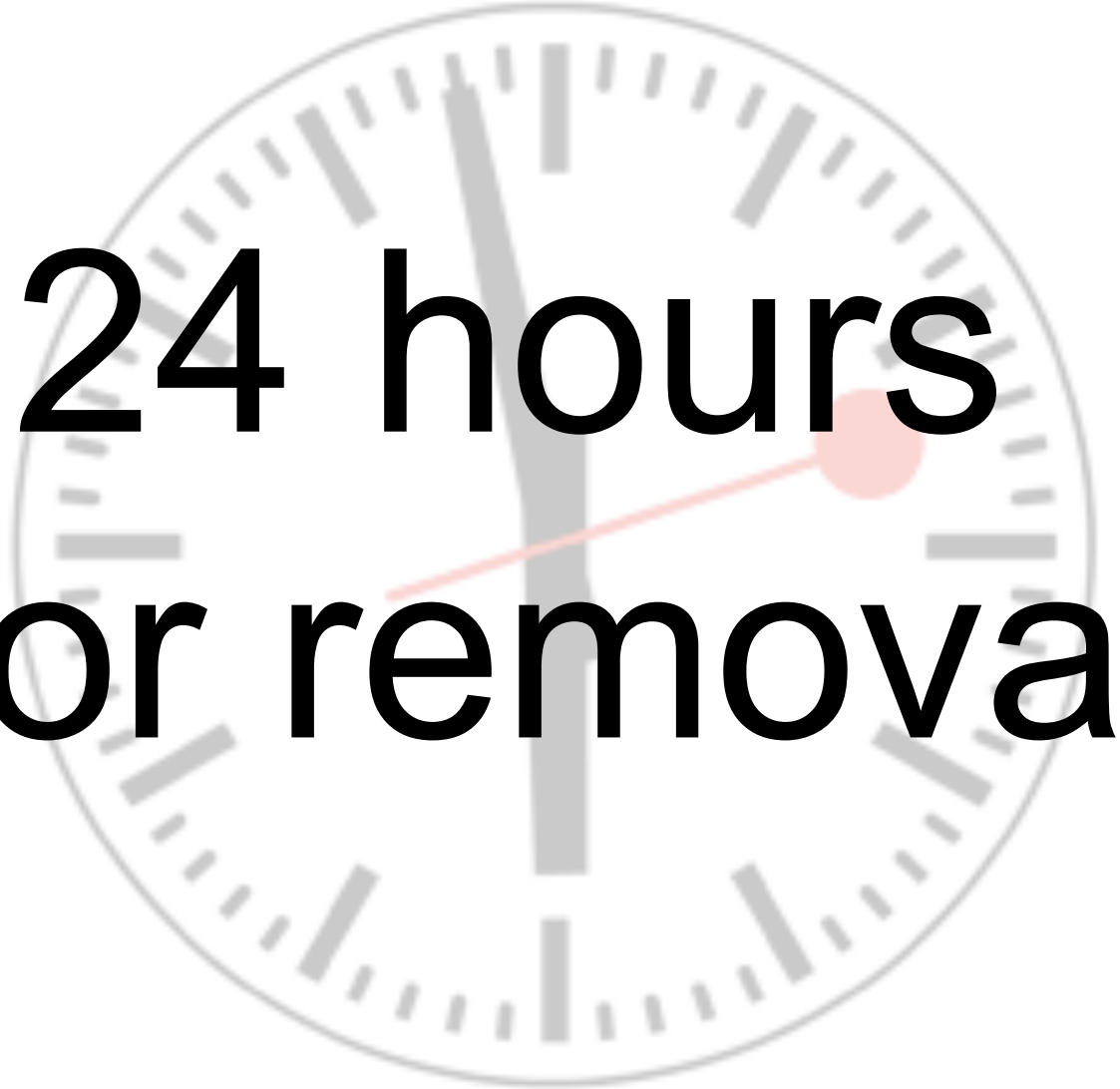
SWITCH-CERT fights Drive-By Exploits

© 2014 SWITCH



http://www.google.com/transparencyreport/safebrowsing/

© 2014 SWITCH



24 hours for removal

© 2014 SWITCH

Malicious url process

- Information about malicious URL
- Verify the suspicion
- Notify owner/tech-c & hoster
- Remove NS if code is not removed after 1 day
- Deblock after 5 days
- Identification-request

© 2014 SWITCH

Community Statistics Documentation FAQ About English Join our community Sign in

virustotal

SHA256: 16146f4afcdda6487979673085d70a9631be29f11f44a5c5e204f63bc56c844b

File name: Crack SAM v4.9.1.exe

Detection ratio: 22 / 54

Analysis date: 2014-10-04 10:43:54 UTC (2 weeks, 3 days ago)

Analysis | File detail | Relationships | Additional information | Comments 0 | Votes

Antivirus	Result	Update
AVware	Trojan.Win32.Generic!BT	20141004
Ad-Aware	Trojan.Generic.KD.624991	20141004
Baidu-International	Malware.Win32.HackTool.67	20141004
BitDefender	Trojan.Generic.KD.624991	20141004
Bkav	W32.Clod317.Trojan.a225	20141003
ClamAV	Trojan.Spy.Banker-5850	20141004
Comodo	UnclassifiedMalware	20141004
Cyren	W32/Trojan.LBEX-6879	20141004
Emsisoft	Trojan.Generic.KD.624991 (B)	20141004
F-Secure	Trojan.Generic.KD.624991	20141004

© 2014 SWITCH

Experiences with DN Owners

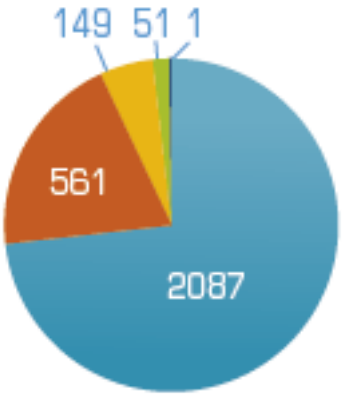
- Grateful
- Unable to cope with the problem
- 24 short time period
- Do not understand the reasons
- Need immediate support from
  - Hoster
  - Webmaster
  - SWITCH

© 2014 SWITCH

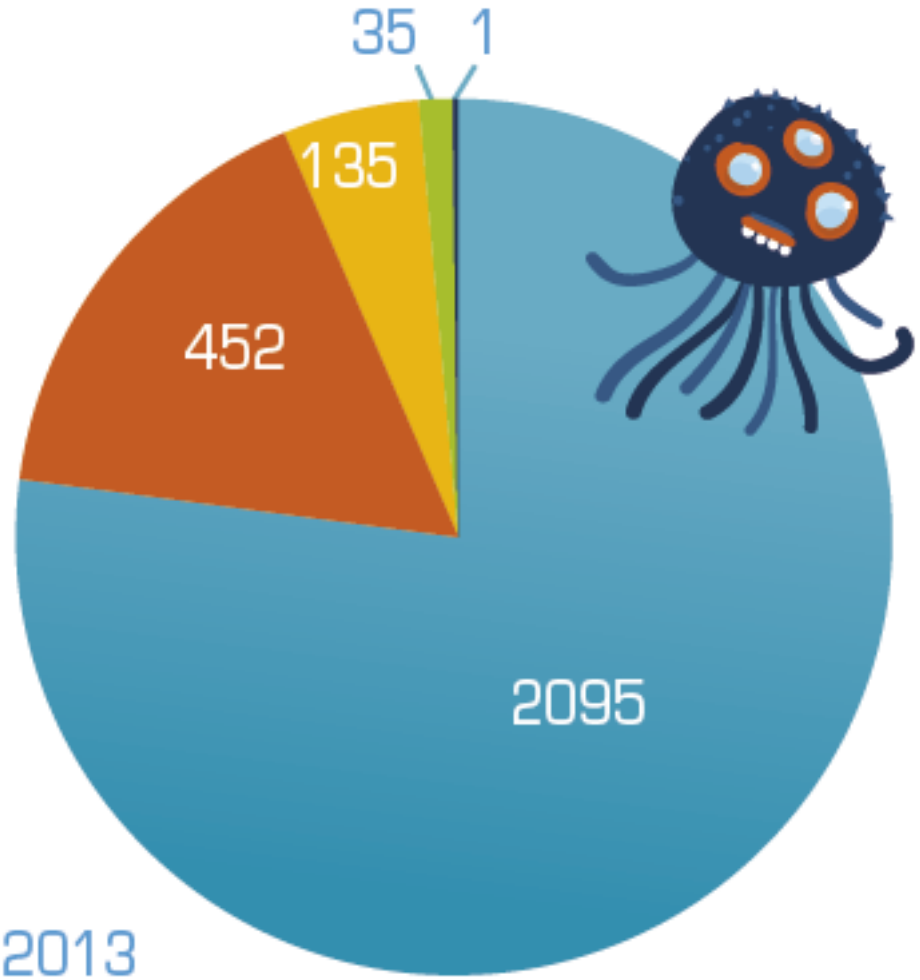
Experiences with Hosters

- Reactive
- Different approaches
- # of blocking for Swiss Hosters declines
- Quality of abuse handling at most ISPs rises after some time

© 2014 SWITCH



Total 2012



Total 2013

- Cleaned after ID-request
- Cleaned after blocking
- Cleaned after notification
- Domain deleted
- Reported to Authorities

© 2014 SWITCH

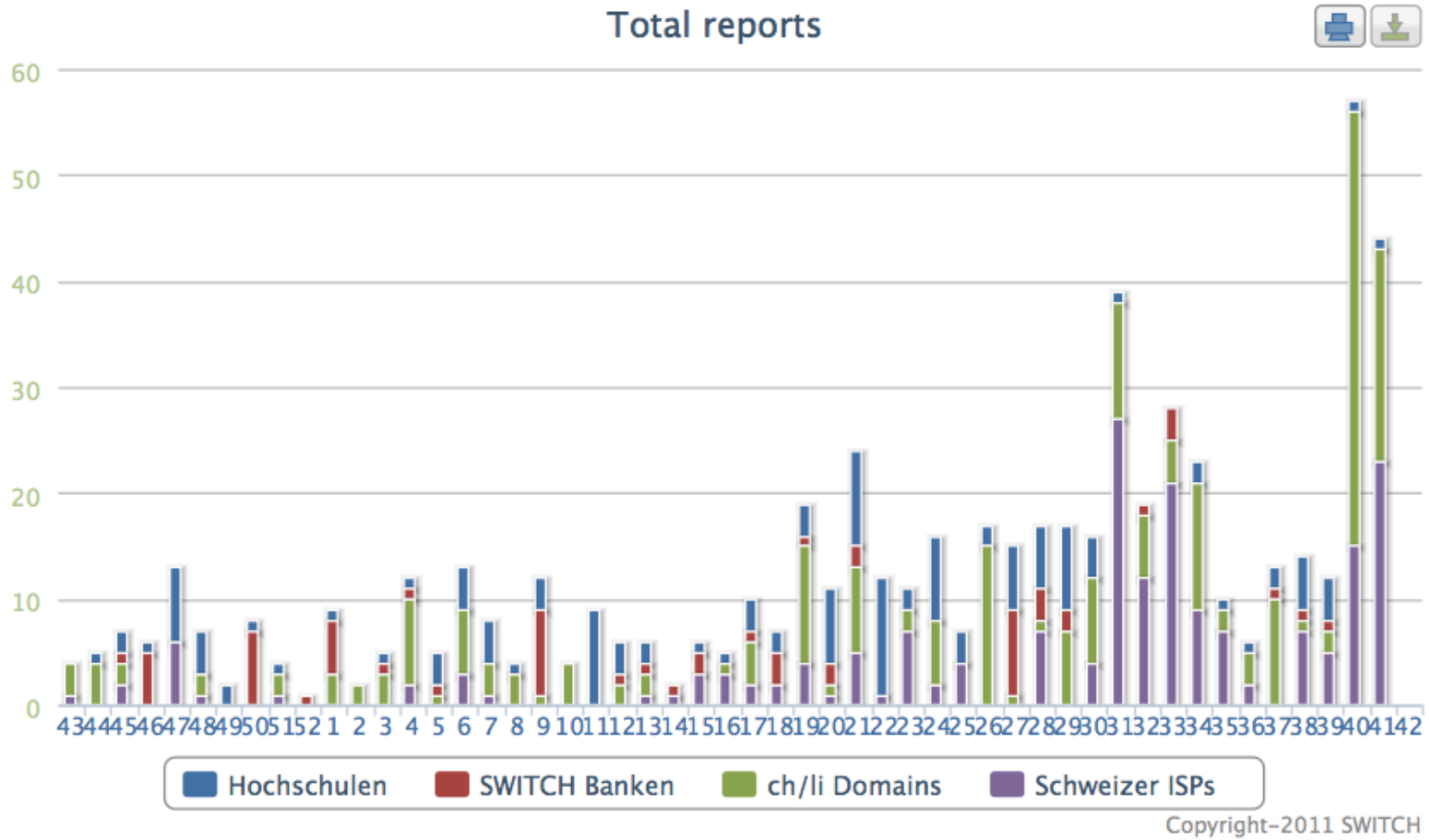
Lessons learned

- Drive-By problem is hard to understand
- Collaboration essential for success
- It takes time to establish trust and a process across organisations

© 2014 SWITCH

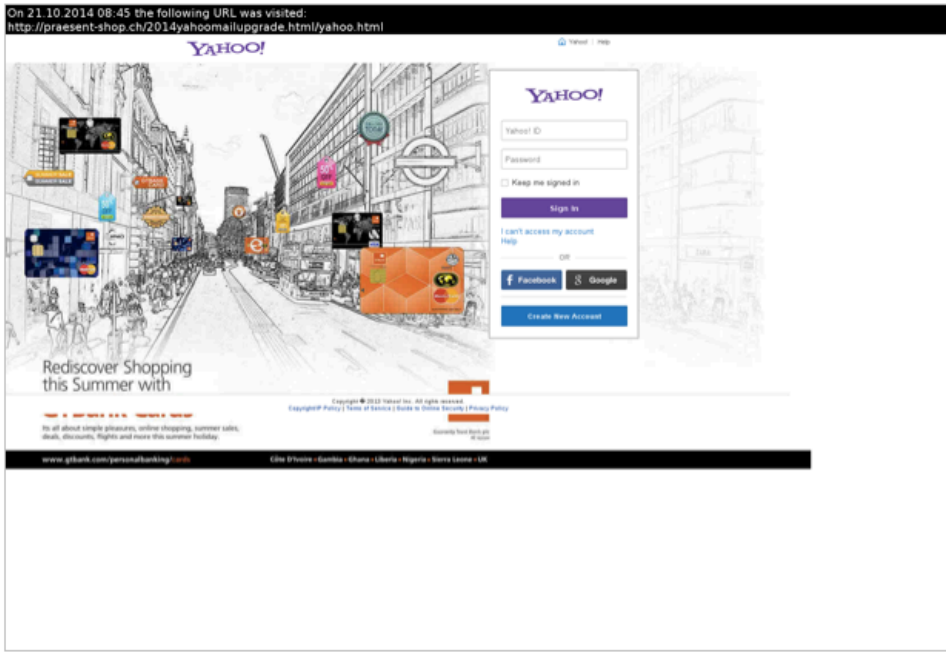
Phishing

Phishing Statistics per week 2014



© 2014 SWITCH

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8">
<title>Yahoo! Mail: The best web-based email!</title>

<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="Expires" content="0">
<script type='text/javascript'>
var startTime = new Date().getTime();
var loadTime = null;
</script>

<link rel="stylesheet" type="text/css" href="https://s.yimg.com
/lq/i/reg/css/yregbase_sec_ui_1_9.css">
<style type="text/css">
.clear{clear:both}
#yreglg select, #yreglg input, #yreglg p, #yreglgtb td,
#yreglgtb th{font-size:93%}
div.yregdsilu h2.yregdnt, div.yregdsilu p.yregsueasy{width:110px}
/*popup template css */
#yregtpopup #yregtxt {width:260px;margin:0 0 10px} /* popup
template */
#yregtpopup #yregwp, #yregtpopup #yregmst{width:525px}
#yregtpopup #yregmst{margin-bottom:5px}
#yregtpopup #yreglg{margin-bottom:0}
#yregtpopup #yregft{padding-top:5px}

#yregtgen #yregtxt h2, #yregtpopup #yregtxt h2, #yregpmtxt
h3{font:bold 152%/152% arial;color:#333;margin:0}
```



More collaboration

The Initiative of Swiss ISPs
Banks and Public Sector

© 2014 SWITCH

asut
Schweizerischer Verband der Telekommunikation
Association Suisse des Télécommunications
Swiss Telecommunications Association

CENTRALWAY

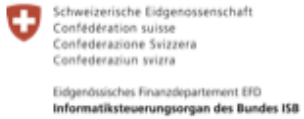
CREDIT SUISSE

cyscon

eBanking but secure!

Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN
Business
Institute of Business Information
Technology

HOSTPOINT


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB

MIGROSBANK

PostFinance

RAIFFEISEN

Sunrise

AECS
swisscard

swisscom

SWITCH

UBS

upc cablecom

VISECA
card services

© 2014 SWITCH

Goal

SWISS INTERNET SECURITY ALLIANCE

Make Switzerland the cleanest Internet country in the world!

© 2014 SWITCH

Security Check

This web service is a free online tool. Based on the results we lead you through a variety of checks step by step.

Start

asut
Schweizerischer Verband der Telekommunikation
Association Suisse des Télécommunications
Swiss Telecommunications Association

CENTRALWAY

CREDIT SUISSE

cyscon

eBanking but secure!

Lucerne University of
Applied Sciences and Arts
HOCHSCHULE
LUZERN
Business
Institute of Business Information
Technology

HOSTPOINT

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB

MIGROSBANK

PostFinance

RAIFFEISEN

Sunrise

AECS
swisscard

swisscom

SWITCH

3. Browser- and Plugincheck

When it comes to IT security, experts always point out that the most important key value is an up-to-date computer system. On about 87% of all checked and analyzed computers critical software security updates are missing. Especially risky applications like browsers and their plugins are not up-to-date.

Start Browser- & Plugin-Check

Details	Result	Action
RealPlayer Plugin.plugin	0.0.1.d.1	Up-To-Date
Flip4Mac Windows Media Plugin	2.5.0.1	Up-To-Date
Google Talk Plugin Video Accelerator	0.1.44.29	Up-To-Date
Google Talk Plugin	5.1.4.17398	Up-To-Date
QuickTime Plug-in 7.7.1	7.7.1.0	Up-To-Date
Shockwave Flash	15.0.0.152	Up-To-Date
Shockwave Flash 15.0 r0		

Next

Join us

SWISS INTERNET SECURITY ALLIANCE

https://www.swiss-isa.ch

info@swiss-isa.ch

© 2014 SWITCH

michael.hausding@switch.ch

http://securityblog.switch.ch/

© 2013 SWITCH