
Abuse
iis.se

Abuse

IIS Registry
Abuse and Prevention
Peter Forsman

photo:@kalexanderson

IIS Registry since 2009, Domain industry since 2002, Computer training since 1994

Alter ego

Publicist, Lecturer
Analyst, Investigator

Pro Bono

photo: Magazine Café

Contributor / Awareness

Alter ego

Mass Media

Law Enforcement

Trends, Modus Operandi
OSINT

Alter ego

Mass Media

Law Enforcement

Trends, Modus Operandi

OSINT

Sometimes need to dig deep..

photo: imagecollectiononline.com

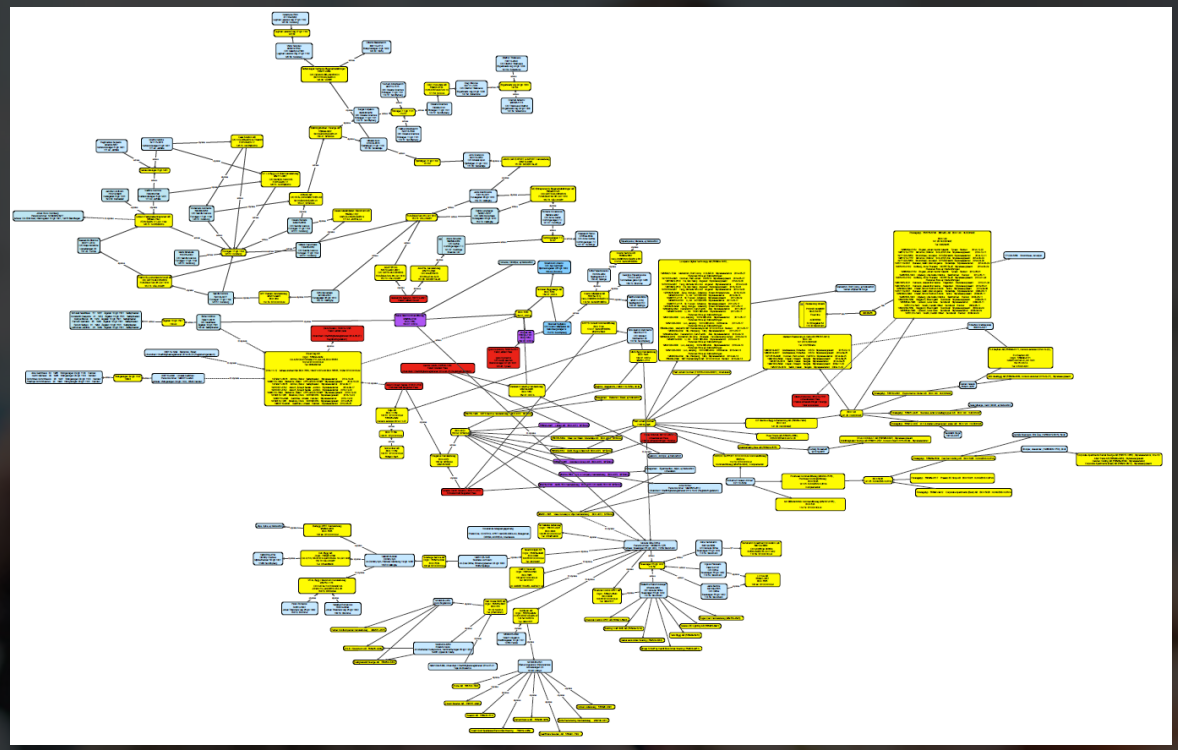
Alter ego

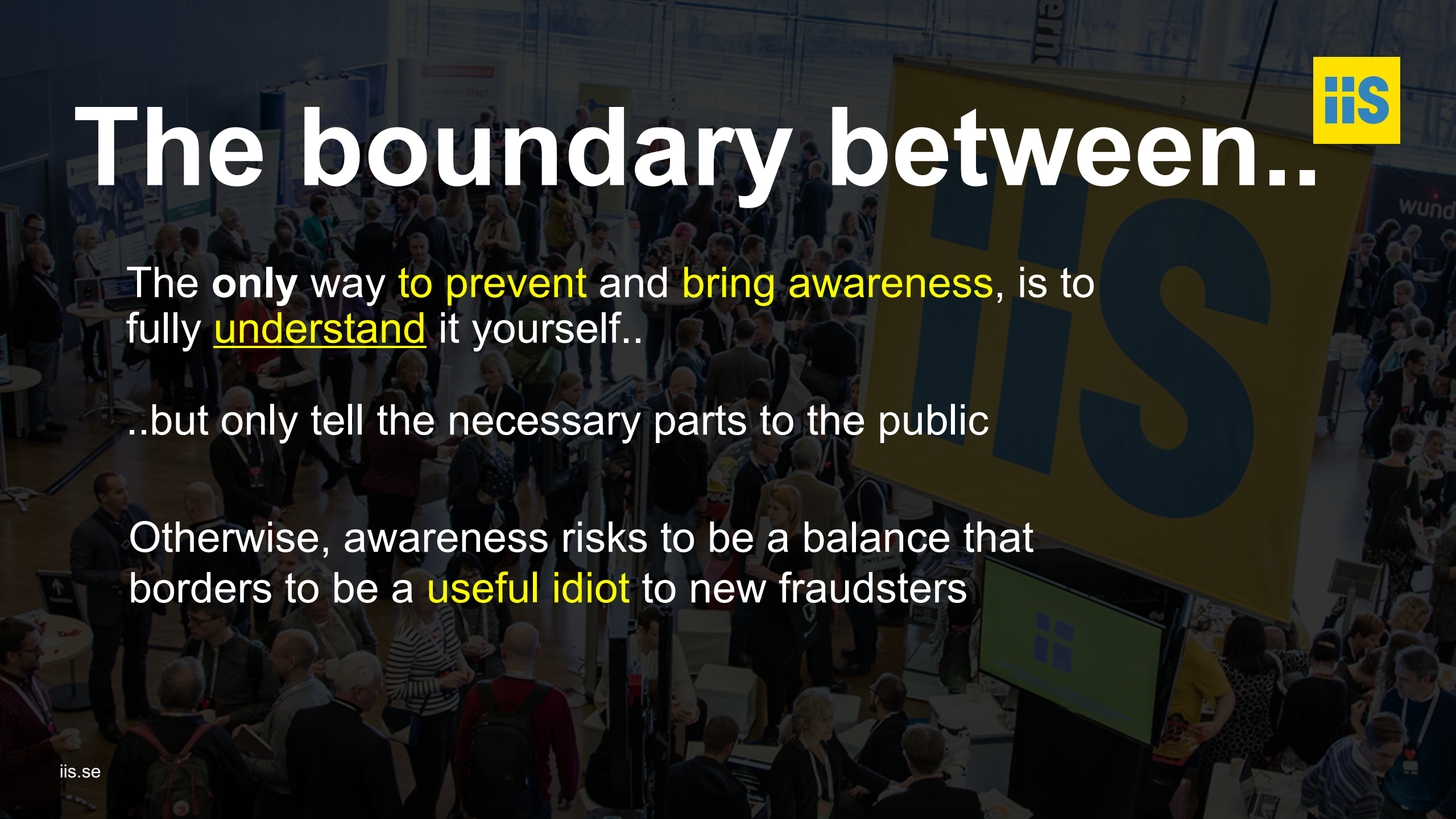
Mass Media

Law Enforcement

Trends, Modus Operandi
OSINT
Open Source Intelligence
(Open sources on the internet)

..and largely to get the whole picture.





The boundary between..

The **only** way to prevent and bring awareness, is to fully understand it yourself..

..but only tell the necessary parts to the public

Otherwise, awareness risks to be a balance that borders to be a useful idiot to new fraudsters

Traditional smörgåsbord

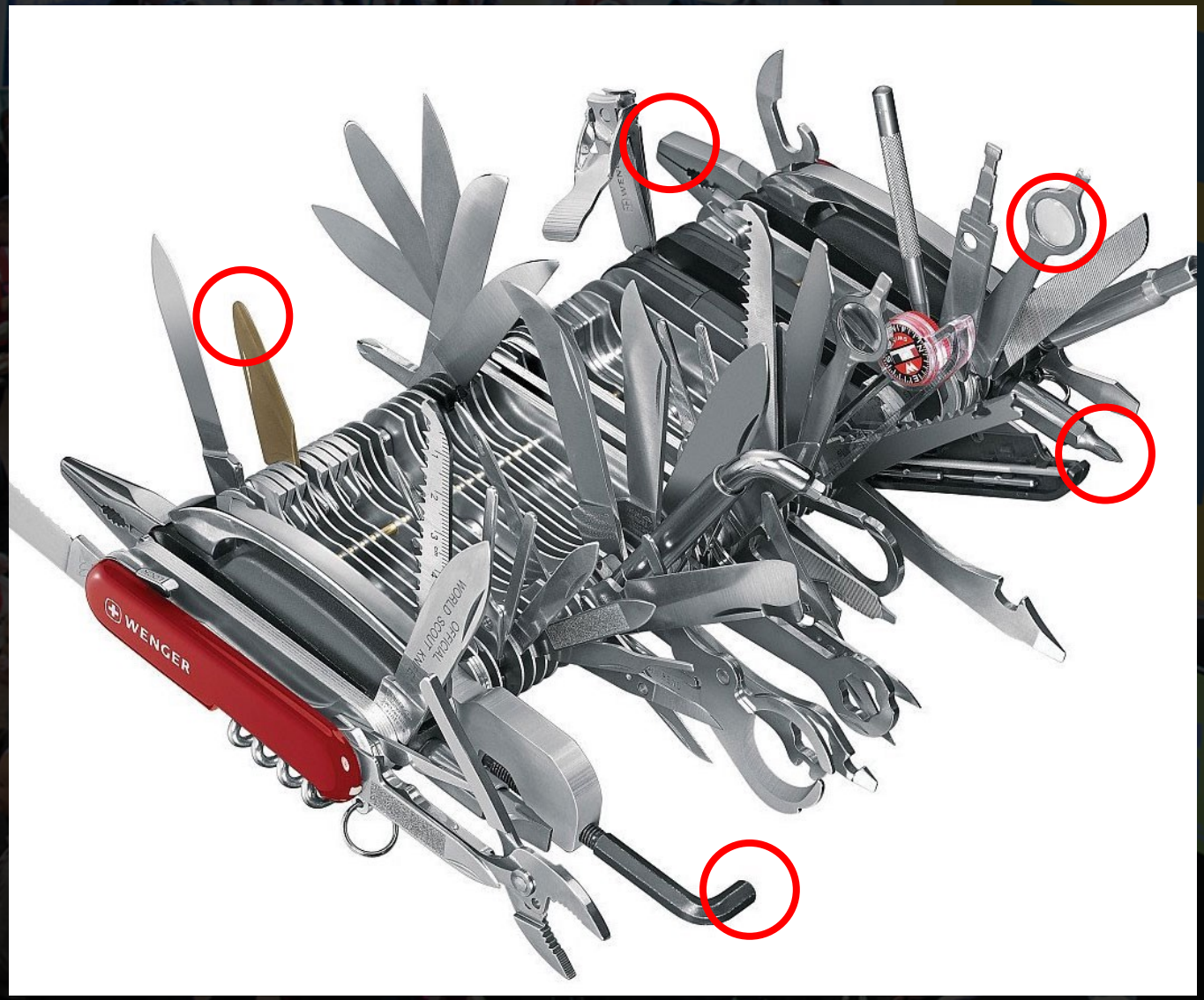
naah..

Customize

Pick what components you need!

photo: thisiswhyimbroke.com

Variations..



Targets
Setups
Approach
Marketing
Distribution
Layers of decoys

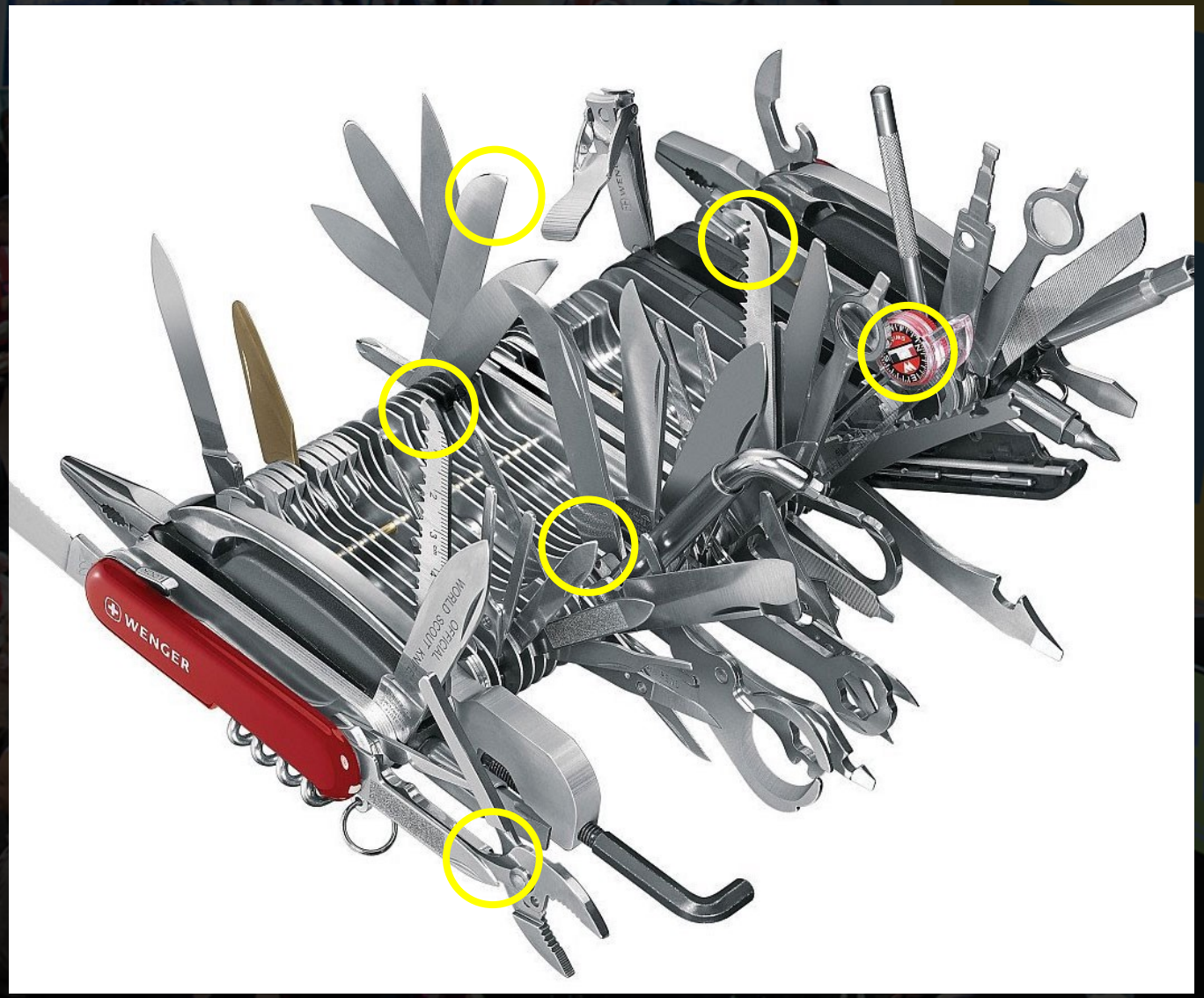
photo: thisiswhyimbroke.com

Next phase..

When you got your victims.

photo: dreamstime.com

Hide and seek..



Targets
Setups
Approach
Marketing
Distribution
Layers of decoys

Payment methods
Layers of payees
Decoys
Risk spreading
Money laundering
Etc.

Squeeze value from info

photo: thisiswhyimbroke.com

In the past few year(s)

Domain name related abuse

False registrant data

Q1 2017:

Appr. 6500 .se-domains were deactivated and later released. (Reason: Reuse of names, orgno, email etc.) fictive identities

False registrant data

”Learn and adapt”

But since May 2017:
The contacts is only related to 2 domains each.
And the problems continues.
What kind of problems?

False registrant data

It may be a new look, but it's the "same coin"

photo: riksbank.se

- False "generated" information
  (often with own valid email and phone)
- "Hijacked" information from other registrants – looks valid!
  (often with own valid email and phone)

Contact information for domain

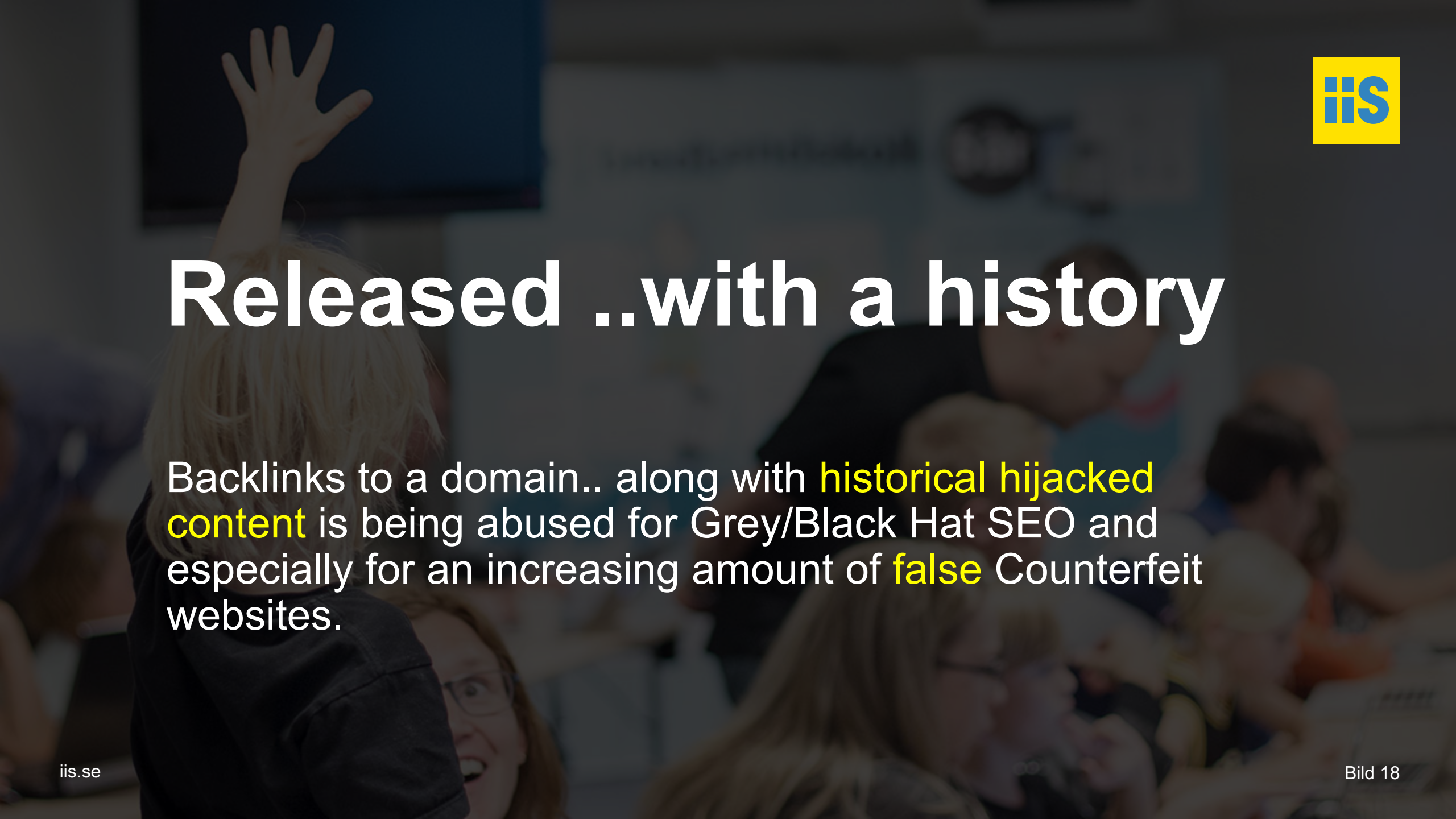
As of June 3, 2013 the contact information for private persons/sole traders will only be shown if the holder of the domain name has approved the publication.

Contact ID	stifte0702-00242
Name	Måns Jonasson
Organization	IIS
Organization number	[SE]802405-0190
Holder e-mail address	varadomaner@iis.se
Address row 1	Box 7399
Address row 2	-
Address row 3	-
Zip code	10391
City	Stockholm
Country	SE
Phone	+46.84523500
Fax	+46.84523502
Contact created	2007-02-09
Contact last updated	2016-04-21
Registrar	SE Direkt

Contact information for domain

As of June 3, 2013 the contact information for private persons/sole traders will only be shown if the holder of the domain name has approved the publication.

Contact ID	petint7829-00001
Name	(not shown)
Organization	(not shown)
Organization number	(not shown)
Holder e-mail address	(not shown)
Address row 1	(not shown)
Address row 2	(not shown)
Address row 3	(not shown)
Zip code	(not shown)
City	(not shown)
Country	(not shown)
Phone	(not shown)
Fax	(not shown)
Contact created	2012-12-01
Contact last updated	-
Registrar	Loopia AB



Released ..with a history

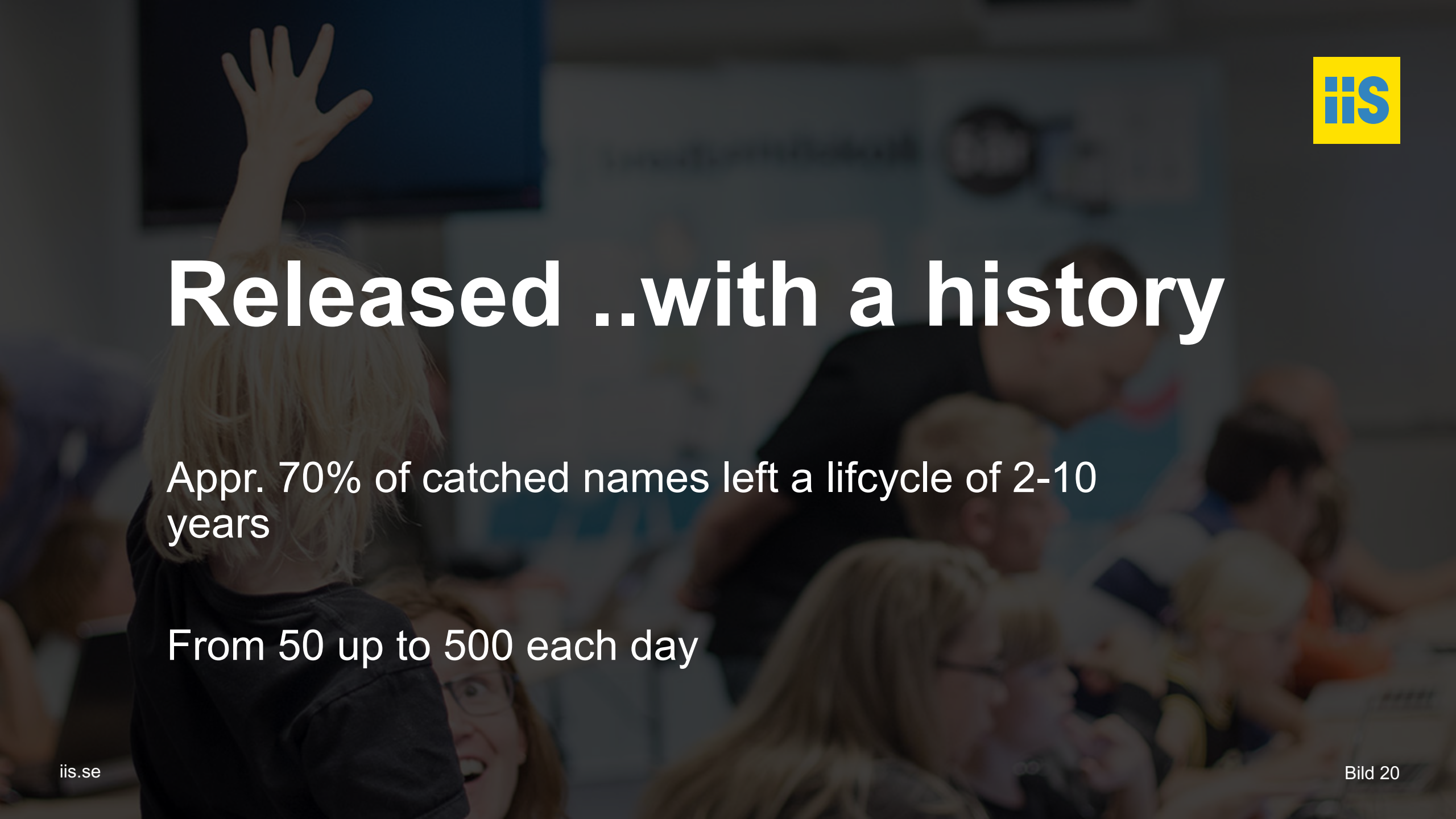
Backlinks to a domain.. along with historical hijacked content is being abused for Grey/Black Hat SEO and especially for an increasing amount of false Counterfeit websites.

Domännamn som blir lediga att registrera imorgon 04:00 UTC

Inloggade gratisanvändare ser data 2 dagar fram, 20 dagar för betalande användare.

Sektion 1: Domäner med inlänkar

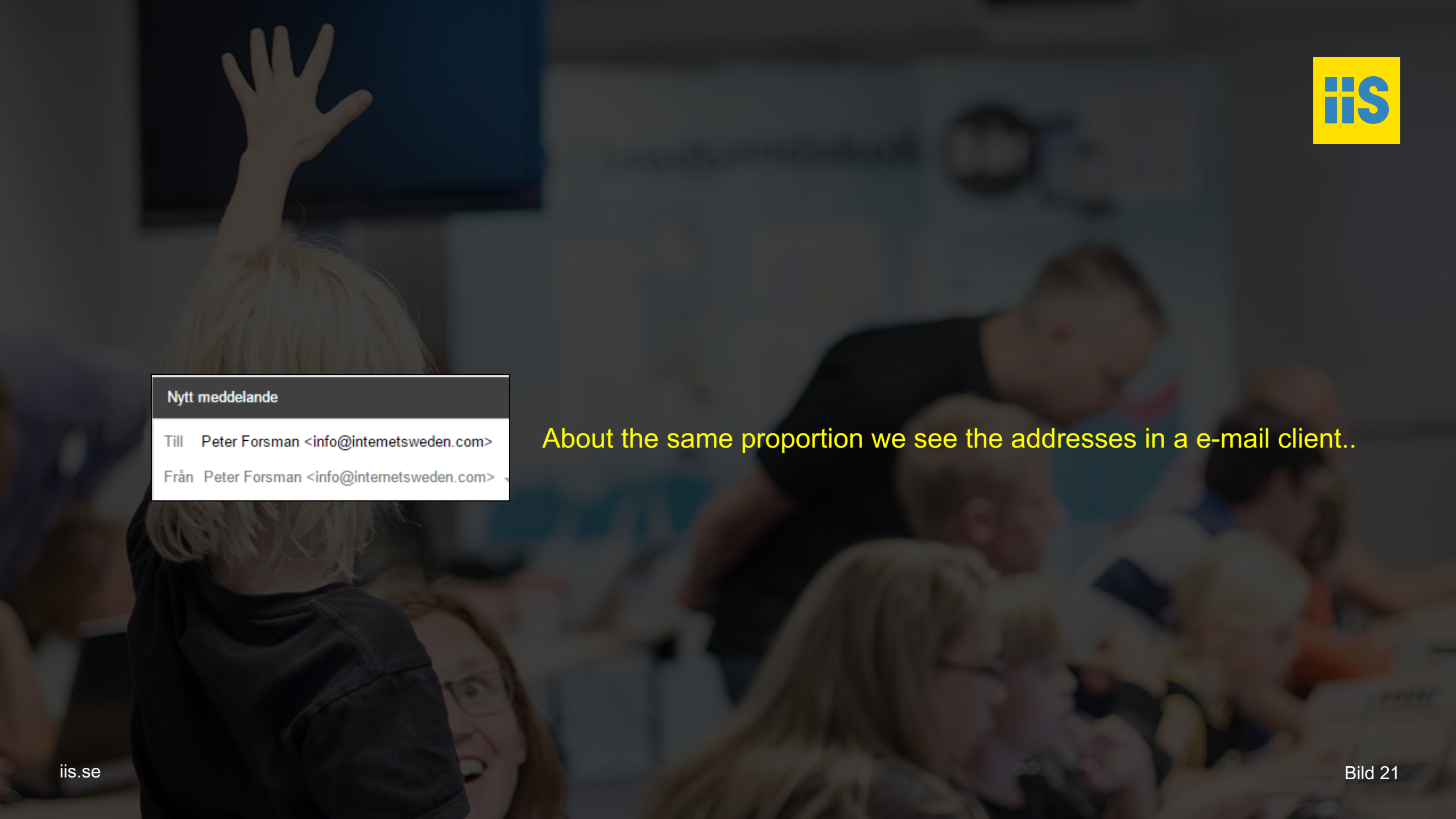
Domän med Majestic Kategori	DomainStats.io Backlink Score	Ahrefs Linking Domains	Ahrefs URL Rating	Majestic Trust Flow	Moz Domain Authority	Google PageRank	Facebook	Wayback Archive	Domain Score	Dropdatum
instagramlikes.se	-20	16 (-49)	16 (-13)	0 (+0)	10 (-2)	N/A	846	4 gånger sedan 2015	0	16 Nov 2017
vintagehoneymoon.se Business > Arts and Entertainment Språket på inlänkar: svenska	227	110 (+29)	28 (+3)	8 (-5)	28 (+1)	3	426	21 gånger sedan 2012	4	16 Nov 2017
landvetterlekland.se	-22	10 (+4)	12 (+4)	0	10 (+2)	0	291	11 gånger sedan 2013	0	16 Nov 2017
freddiessportsbar.se		13 (-5)	17 (-2)	0 (-7)	11 (-11)	2	227	17 gånger sedan 2013	1	16 Nov 2017
tunnelloppet.se Sports > Organizations Språket på inlänkar: svenska	9	29 (+1)	19 (-3)	14 (+0)	17 (-1)	1	76	52 gånger sedan 2003	0	16 Nov 2017
hudhalsan.se	-16	12	14	0	10		53	56 gånger sedan 2004	1	16 Nov 2017
kidzshop.se Home > Family Språket på inlänkar: svenska	18	37 (+22)	22 (+5)	8 (-1)	19 (+6)	1	45	61 gånger sedan 2006	1	16 Nov 2017



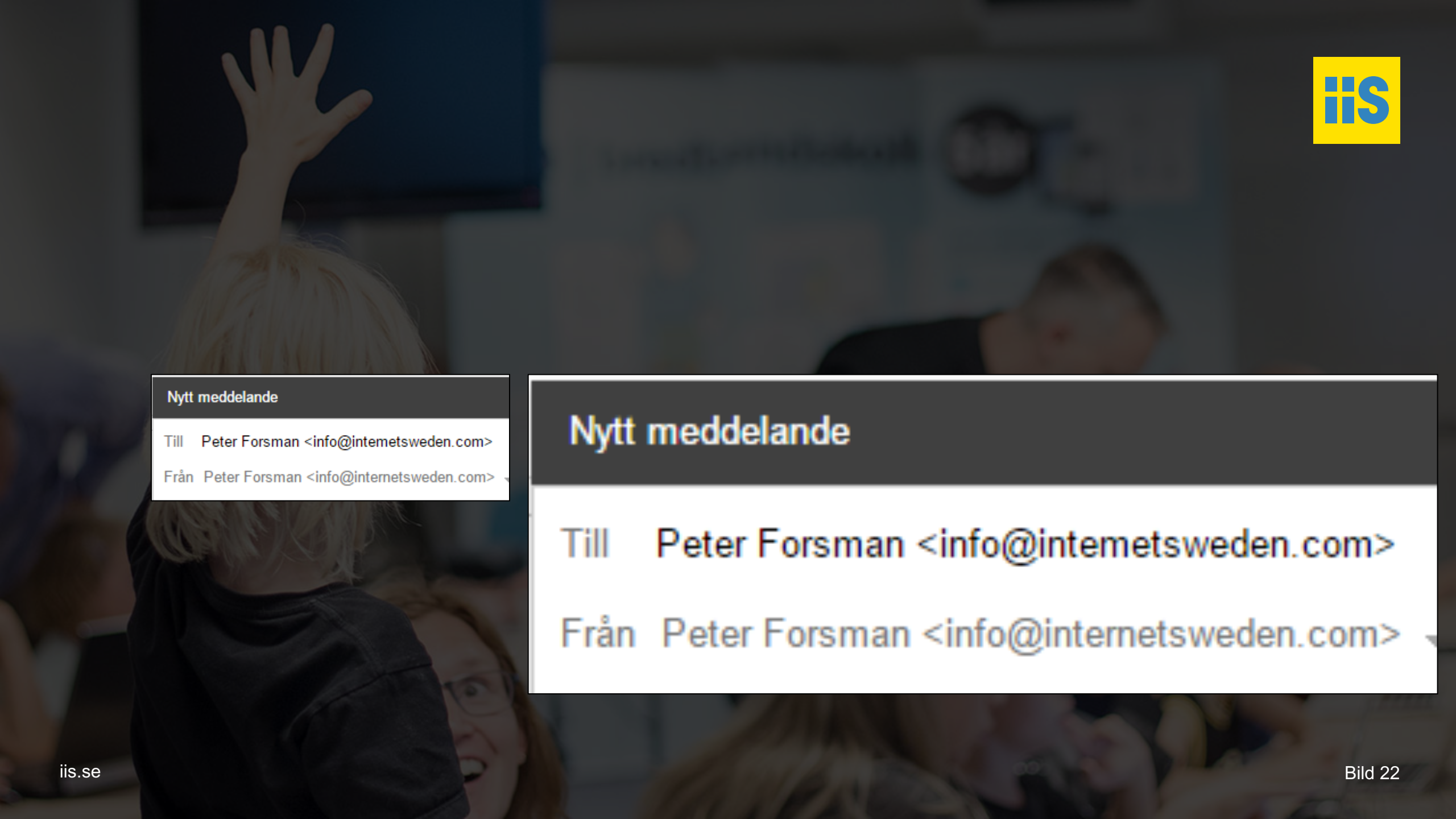
Released ..with a history

Appr. 70% of catched names left a lifcycle of 2-10 years

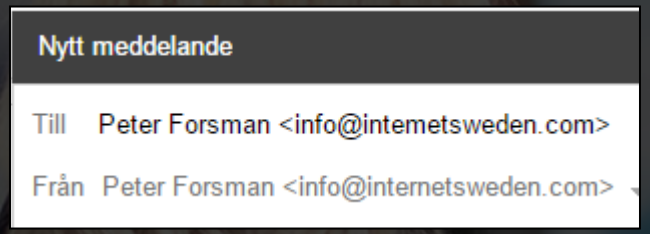
From 50 up to 500 each day



About the same proportion we see the addresses in a e-mail client..


Nytt meddelande
Till Peter Forsman <info@intemetsweden.com>
Från Peter Forsman <info@internetsweden.com>
Nytt meddelande
Till Peter Forsman <info@intemetsweden.com>
Från Peter Forsman <info@internetsweden.com>

CEO Frauds / BEC - typos



CEO Frauds / BEC - typos

l instead of i

q instead of g

0 instead of o

r+n instead of m

n instead of m

Dashes (-) in domains

svenska*
sveriges*
swedish*

*ab.se

*sverige.se

*sweden.se

CEO Frauds / BEC

Spoofed e-mail addresses (one way communication)
E-mail under **Typo Domains** (Two-way communications)
E-mail under **Alt. TLD** (Two-way communications)
Free web mail, **Displayed Names** (Two-way communications)
+ other types, that I will show you!

BEC is the ”new” 419 type of scams..

CEO Frauds / BEC

- But comes in variations.. Either pretty simple comparble to spear phishing mail (Usually either 9 600 or 36 000 EUR)
- Or advanced and sophisticated, often initiated by a trojan, man-in-the-email, etc
  Many phases and steps, before ”the hit”
  More comparable with romance scams

  ..up to 50 000 000 EUR or even 100 000 000 USD

screen: softpedia.com

Cyber-Scammers Steal €50 Million from Austrian Airplane Manufacturer

FACC falls victim to a Business Email Compromise attack

Jan 21, 2016 13:55 GMT · By Catalin Cimpanu · Share:

FACC Operations GmbH, an Austrian company that produces various airplane parts for companies like Airbus and Boeing, has announced a cyber-incident during which cyber-fraudsters managed to steal around €50 million from their bank accounts.

screen: fortune.com

Exclusive: Facebook and Google Were Victims of $100M Payment Scam

By Jeff John Roberts April 27, 2017

Cyber-Scammers Steal €50 Million from Austrian Airplane Manufacturer

FACC falls victim to a Business Email Compromise attack

Jan 21, 2016 13:55 GMT · By Catalin Cimpanu · Share:

FACC Operations GmbH, an Austrian company that produces various airplane parts for companies like Airbus and Boeing, has announced a cyber-incident during which cyber-fraudsters managed to steal around €50 million from their bank accounts.

screen: softpedia.com

Law Enforcement estimates that ***20 percent of BEC succeeds***

screen: fortune.com

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 04, 2017

Alert Number
I-050417-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE
E-MAIL ACCOUNT COMPROMISE
THE 5 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to Business E-mail Compromise (BEC) PSAs 1-012215-PSA, 1-082715a-PSA and I-061416-PSA, all of which are posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data as of December 31, 2016.

DEFINITION
Business E-mail Compromise (BEC) is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The E-mail Account Compromise (EAC) component of BEC targets individuals that perform wire transfer payments.

screen: ic3.gov

Exclusive: Facebook and Google Were Victims of $100M Payment Scam

By Jeff John Roberts April 27, 2017

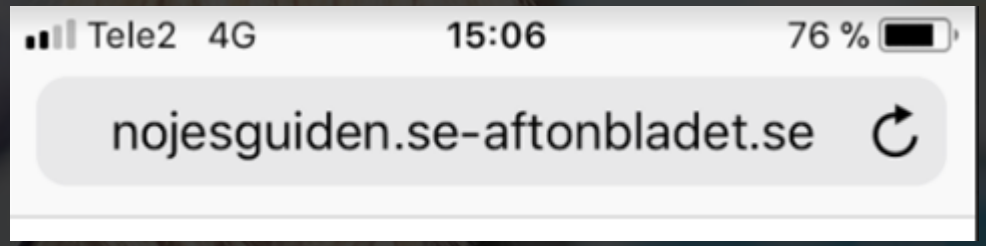
next..

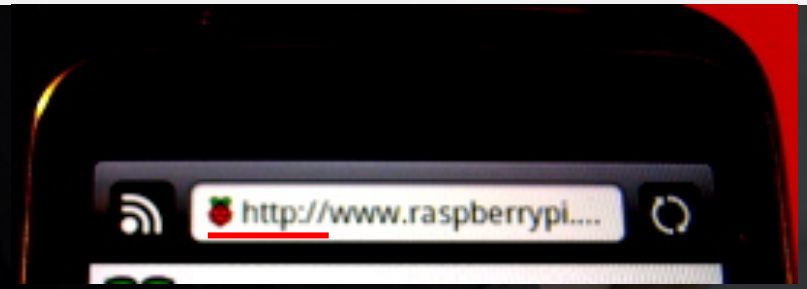
Lack of understanding of the domain name hierarchy / addressing

FROM

TO

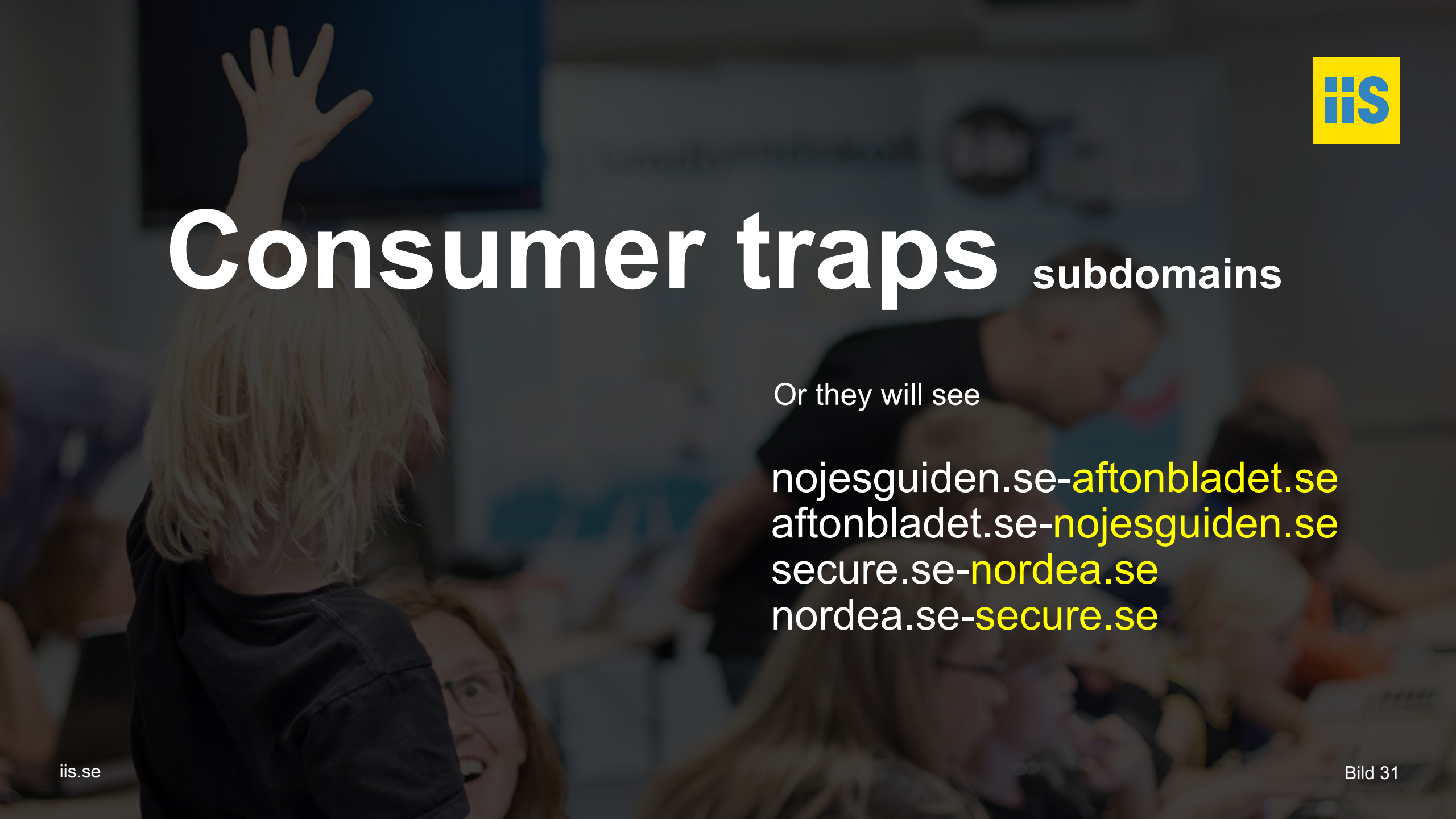
Consumer traps subdomains





What consumers see

nojesguiden.se-aftonbladet.se
aftonbladet.se-nojesguiden.se
secure.se-nordea.se
nordea.se-secure.se



Consumer traps subdomains

Or they will see

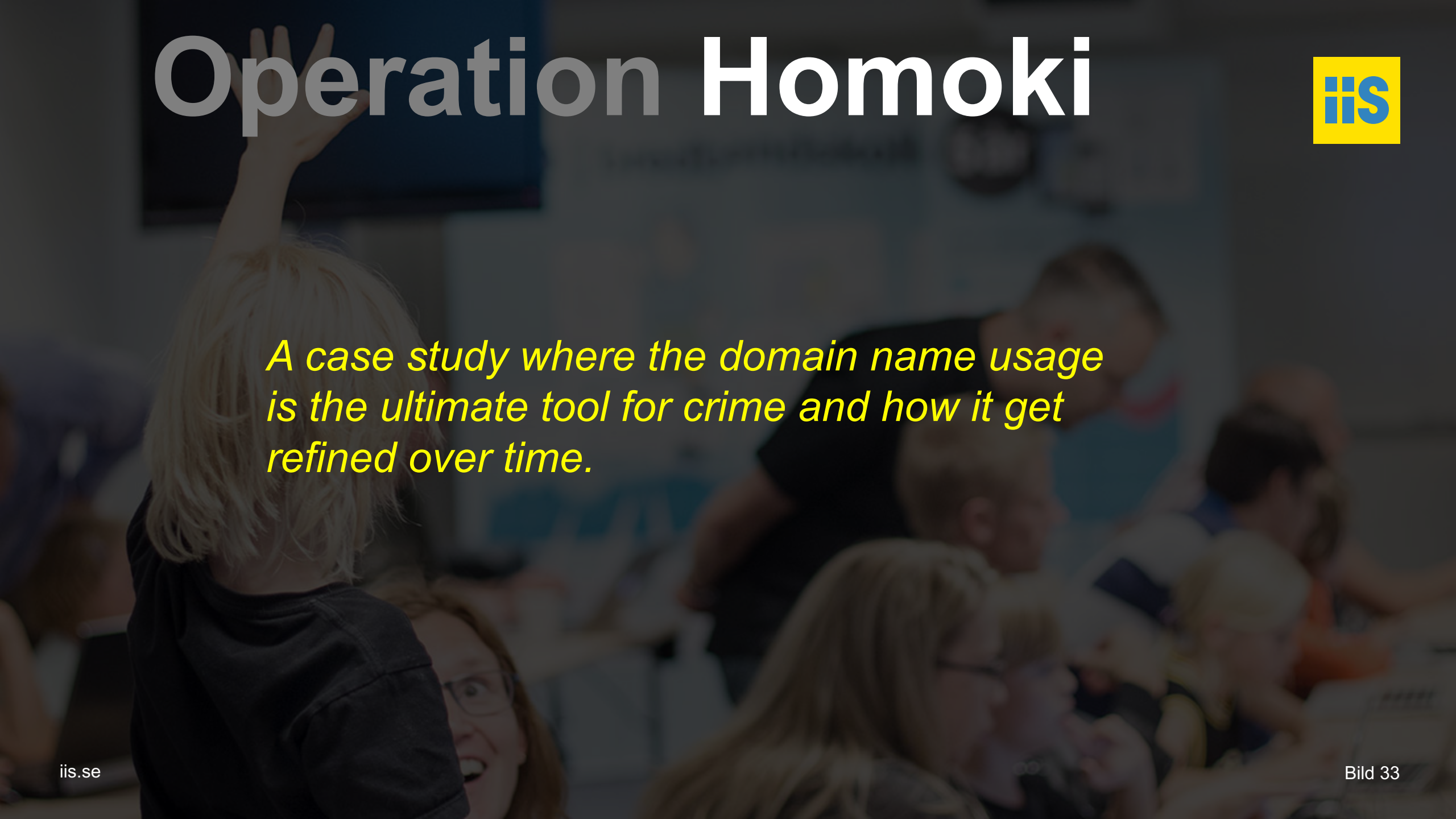
nojesguiden.se-aftonbladet.se
aftonbladet.se-nojesguiden.se
secure.se-nordea.se
nordea.se-secure.se

Consumer traps

Monitoring new types

se-aftonbladet.se
se-nojesguiden.se
se-nordea.se
se-secure.se

Operation Homoki



A case study where the domain name usage is the ultimate tool for crime and how it get refined over time.

Operation Homoki

Since early 2014, hundreds of domains have been registered with hijacked valid company information, except for tele and e-mail.

The domain names have been used by a group for credit frauds, BEC, social engineering and Bank frauds ..in different and changing combinations.

Operation Homoki

Liga misstänks ligga bakom tusentals dataintrång – kan vara största it-härvan någonsin

En av de största dataintrångshärvorna i Sverige någonsin rullas nu upp, kan SVT Nyheter avslöja. Åtta personer åtalas på måndag i Malmö misstänkta för tusentals dataintrång mot företag, myndigheter och ett riksdagsparti – Sverigedemokraterna.

Screen: svt.se
September 2017

Gang suspected to be behind thousands of computer breaches - may be the largest IT-investigation ever

One of the largest data intrusion investigations in Sweden ever rolled up, SVT News can reveal. Eight people are being charged on Monday in Malmo suspected of thousands of data violations against companies, authorities and a parliamentary party - the Swedish Democrats.

Operation Homoki
timeline

2013 2014 2015 2016 2017

Feb 2013
Jan Nowak AB | 2 millions in unpaid demands
Homoki Sweden AB | 2 millions in unpaid demands

Credit frauds

and..
(Authorities dont do credit controls in Sweden..)
Maps and register over real estates and owners
Company register / Swedish companies

2013 2014 2015 2016 2017

Feb 2013
Jan Nowak AB | 2 millions in unpaid demands
Homoki Sweden AB | 2 millions in unpaid demands

Credit frauds

and..
(Authorities dont do credit controls in Sweden..)
Maps and register over real estates and owners
Company register / Swedish companies

2013-12-09	2 043	Bet.förel. utslag
2013-12-09	13 273	Bet.förel. utslag
2013-12-09	52 171	Bet.förel. utslag
2013-12-09	411 910	Bet.förel. utslag
2013-12-02	12 415	Restf. Skattekonto
2013-09-25	395 055	Bet.förel. utslag
2013-09-23	1 995	Bet.förel. utslag
2013-09-23	4 823	Bet.förel. utslag
2013-09-23	18 638	Bet.förel. utslag
2013-09-23	21 888	Bet.förel. utslag

Registered unpaid demands

2013-12-09	651 863	Bet.förel. utslag
2013-12-09	3 465	Bet.förel. utslag
2013-12-09	3 823	Bet.förel. utslag
2013-12-09	6 049	Bet.förel. utslag
2013-12-09	7 513	Bet.förel. utslag
2013-12-09	11 218	Bet.förel. utslag
2013-12-09	8 749	Bet.förel. utslag
2013-12-09	46 973	Bet.förel. utslag
2013-12-09	8 370	Bet.förel. utslag
2013-12-09	22 388	Bet.förel. utslag
2013-12-09	42 668	Bet.förel. utslag
2013-12-09	68 683	Bet.förel. utslag
2013-12-09	58 965	Bet.förel. utslag
2013-12-09	44 113	Bet.förel. utslag
2013-12-09	36 446	Bet.förel. utslag
2013-12-09	22 454	Bet.förel. utslag
2013-12-09	45 056	Bet.förel. utslag
2013-12-09	18 951	Bet.förel. utslag
2013-12-09	60 206	Bet.förel. utslag
2013-12-09	9 217	Bet.förel. utslag
2013-12-09	67 893	Bet.förel. utslag
2013-12-09	128 481	Bet.förel. utslag
2013-12-09	73 535	Bet.förel. utslag
2013-12-09	98 183	Bet.förel. utslag
2013-12-09	78 100	Bet.förel. utslag
2013-12-09	97 858	Bet.förel. utslag

2013 2014 2015 2016 2017

Jan 2014
Register domain names on existing companies, with their own mail and phone number

mail
create one page websites
(with false postal address and phone numbers)

purchase@**acme.se**

purchase@**acmeab.se**

2013 2014 2015 2016 2017

Jan 2014
Register domain names on existing companies, with their own mail and phone number

mail
create one page websites
(with false postal address and phone numbers)

purchase@**acme.se**

purchase@**acmeab.se**

10-15 large orders

”Techretail providers”

Procucts

Invoice

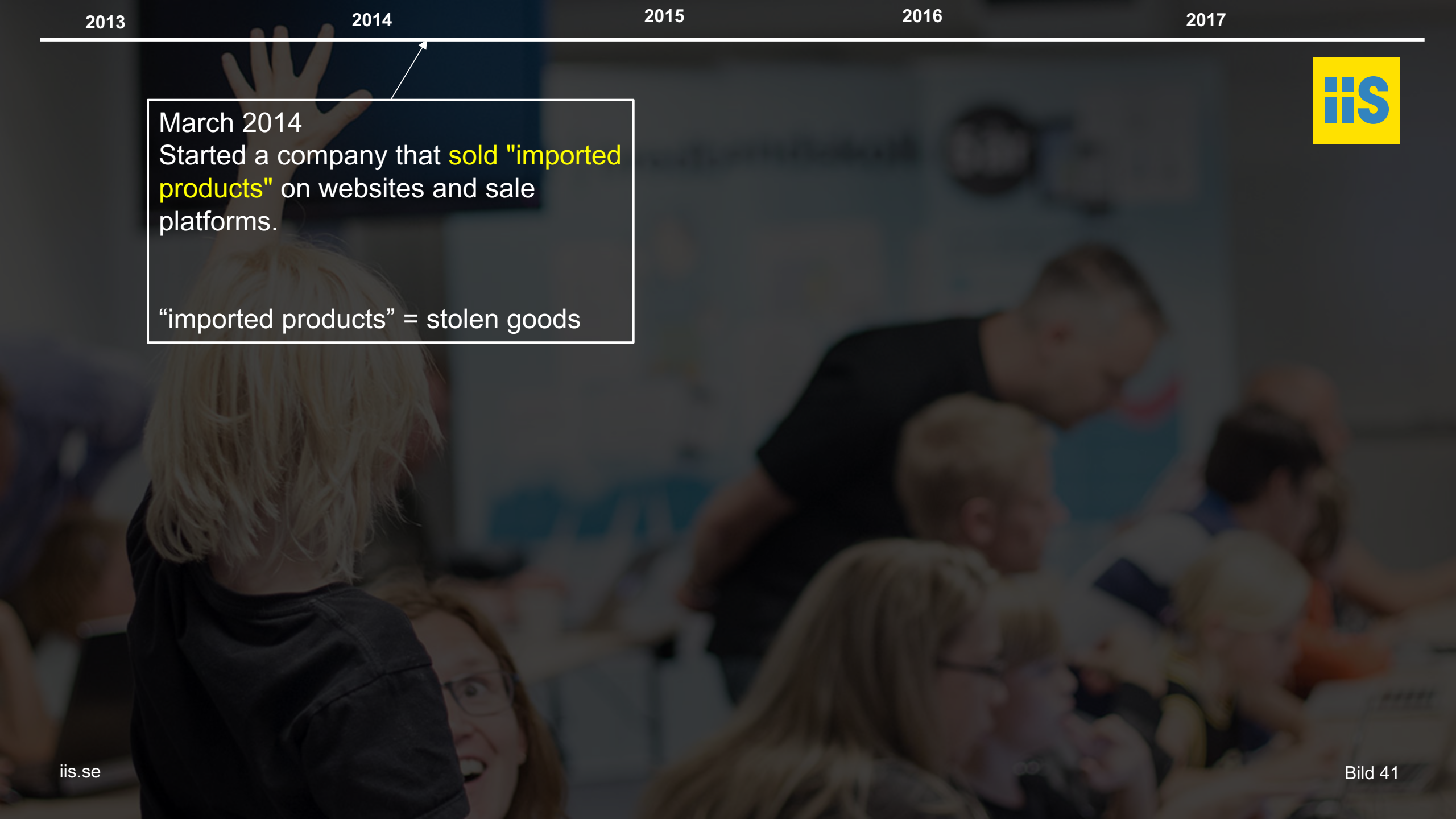
Delivery address

Acme AB

2013 2014 2015 2016 2017

March 2014
Started a company that sold "imported products" on websites and sale platforms.

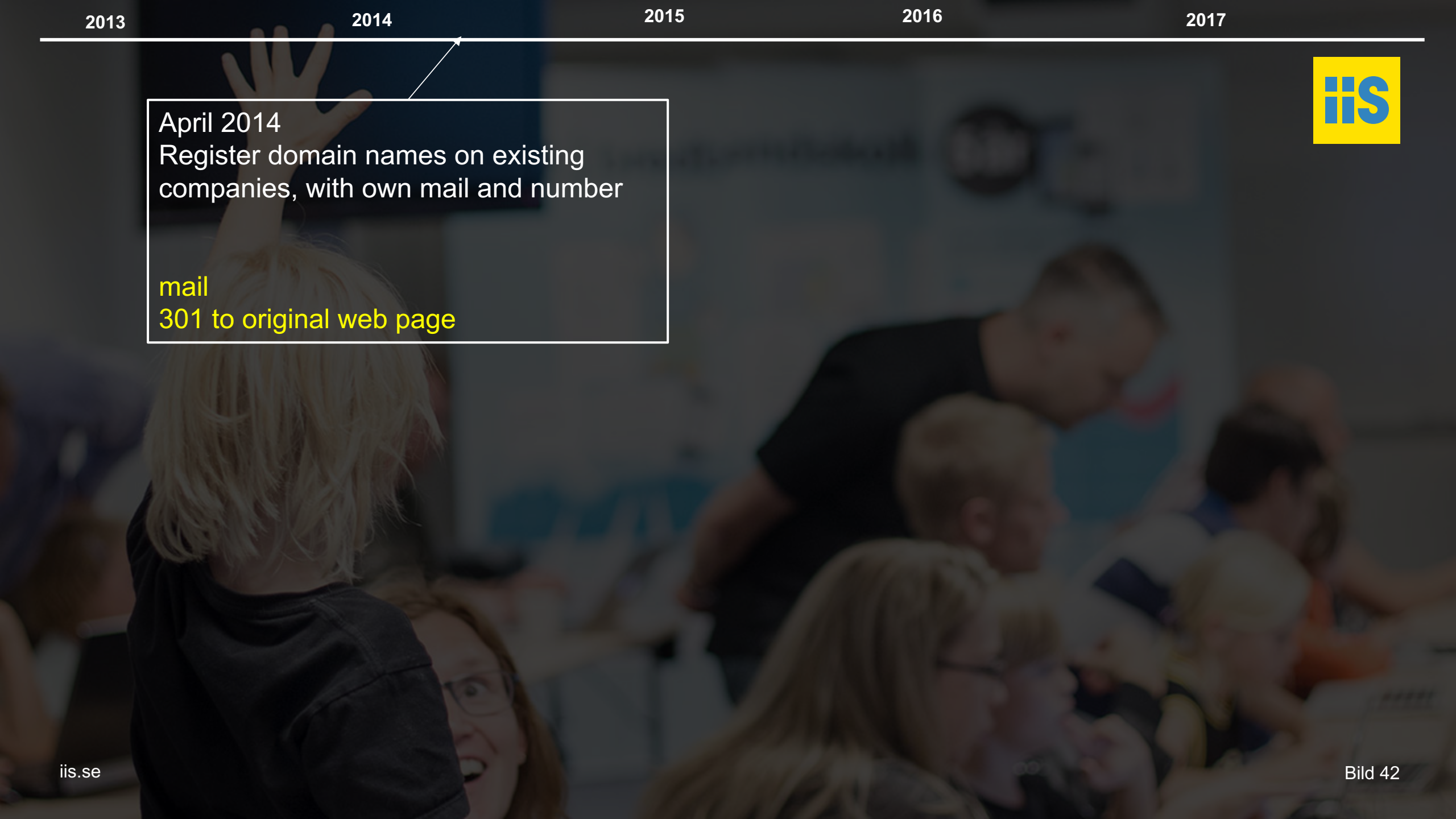
“imported products” = stolen goods



2013 2014 2015 2016 2017

April 2014
Register domain names on existing companies, with own mail and number

mail
301 to original web page



2013 2014 2015 2016 2017

June- 2014
Register domain names on existing companies, with own mail and number

Changed addresses and phone numbers on online registers for the hijacked company, to manipulate check ups.

mail
301 to original web page

2013 2014 2015 2016 2017

Q1 2015
Register domain names on existing companies, with own mail and number

Changed addresses and phone numbers on online registers

mail
301 to original web page

1 Registrar (Domain)
1 NS provider
1 Hosting Provider (301/php)

”Learning the infrastructure and responsibilities”

2013 2014 2015 2016 2017

Q2 2015
Starts to send invoices and tender requests, with malicious attachments.
Trojans, keyloggers etc (.docm/.pdf)

Depending on who and what information they steal, the victim get impersonated in different ways.
Logins, e-mail conversations get hijacked etc.

Control No.: P-338/7-2015

Requesting country: United Kingdom

File No.: 2015/52766-1

Date of publication: 31/07/15

INTERPOL PURPLE NOTICE

MODUS OPERANDI

Type(s) of offence:	European Distribution Fraud
Date of the offence:	2014 to Current
Place of offence:	London and other UK locations
Country of offence:	UK
Circumstances of offence:	UK based fraudsters are placing fraudulent orders with European Companies to supply goods to the UK, resulting with the victims sustaining significant financial loss.
Description of modus operandi: Object/ device/concealment method/procedure.	European legitimate businesses are being targeted by UK criminals who are purporting to be well known UK national and international companies based in the United Kingdom. The criminals place large fictitious orders via telephone or email using the details of well-known UK companies. In some cases multiple orders have been made in a short space of time resulting with a greater financial loss to the victim suppliers.

2013 2014 2015 2016 2017

Q3 2015
Hijack persons e-IDs

And sign changes of board members in companies.

I some cases, they open accounts and take new credits/loans

In other cases, they open up new accounts with new suppliers

2013 2014 2015 2016 2017

Q1 2016
Impersonates to be CEO of a company and emailing their bank, claiming they have a new leasing partner. And asking the bank to send a large sum to the new partners account.

The new partner is a newly formed company, signed with hijacked e-ID

Since this worked, they repeated this modus to a number of banks and financial institutes..

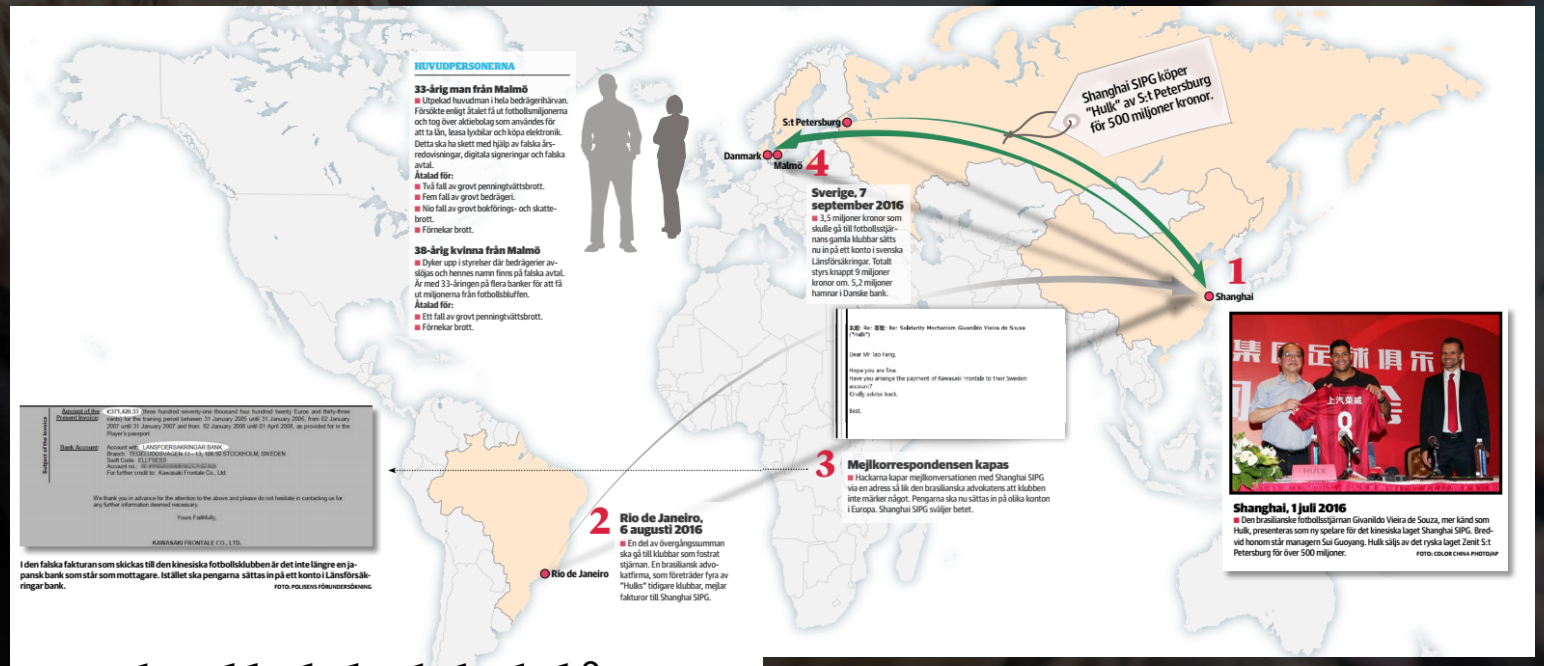
2013 2014 2015 2016 2017

Aug 2016
It is confirmed that they have hacked several thousands of clients and to show another type, say hello to the Brazilian soccer player “Hulk”!

screen: sydsvenskan.se

Hulk is being sold from S:t Petersburg (Russia) to SIPG (Shanghai) via Hulks manager in Brazil..for 50 000 000 Euro

And our fraudsters manage to fool SIPG to pay 1 million Euro to **Malmoe, Sweden**, by man-in-the-email!



screen: sydsvenskan.se

And now for the devil in the details..

-------- Mensagem original --------
De : fangtao@sipg-fc.com
Data: 2016/08/08 04:11 (GMT-03:00)
Para: Victor Eleuterio <victor.eleuterio@bicharaemotta.com.br>
Assunto: Re: Solidarity Mechanism Givanildo Vieira de Sousa ("Hulk")

Dear Sir,
Thanks for your email. we will check all the invoice with each amount refer to the player passport. If the payment is executed, we will inform you at once.
Thanks again
sincerely
Tao Fang

Shanghai -> Brazil

And now for the devil in the details..

-------- Mensagem original --------
De : fangtao@sipg-fc.com
Data: 2016/08/08 04:11 (GMT-03:00)
Para: Victor Eleuterio <victor.eleuterio@bicharaemotta.com.br>
Assunto: Re: Solidarity Mechanism Givanildo Vieira de Sousa ("Hulk")

Dear Sir,
Thanks for your email. we will check all the invoice with each amount refer to the player passport. If the payment is executed, we will inform you at once.
Thanks again
sincerely
Tao Fang

Shanghai -> Brazil

发件人: Victor Eleuterio <victor.eleuterio@bicharaemotta-br.com>
收件人: fangtao@sipg-fc.com
抄送: - Marcos Motta - <mm@bicharaemotta-br.com>

日期: 2016 年 08 月 24 日(星期三) 下午06:01
主题: Re: Solidarity Mechanism Givanildo Vieira de Sousa ("Hulk")

历史记录: 已答复此消息。

Dear Mr Tao Fang,

Hope you are fine.

Brazil -> Shanghai

Preparation

You have sent a email to a CEO, with a malicious attachement, that is sending you screenshots of what the CEO sees on his screen.

1. Impersonate the CEO of one of Swedens largest techretailers

(25 physical shops and webshop, 1.7 billion SEK)

2. Email their payment partner, asking them to change paying account for the company (4 shops) along with a correct filled form and a copy of passport.

3. The day after, recieve a email that the change is completed along with status of the account.

4. Transferred 420 000 SEK to another account.

2016-05-09 13:02:23 [webhallensverige.se] get registered

Sid 817 2016-05-09 13:09:25 webhallensverige.se ?

7 minutes from registration

---------- Original Message ----------
From: Wilhelm Sporrong // Webhallen Sverige AB [wilhelm.sporrong@webhallensverige.se]
Sent: 2016-05-09 16:37
To: merchant@klarna.com
Subject: Konto

Hej

Vi håller på och omstrukturera inom vår organisation och vi har öppna konto som är avsett enbart för utbetalningar av Klarna fakturor .
Alla utbetalningar skall ske till angivet konto enligt bifogat dokument.

Var god bekräfta på mail när ändringen är genomfört.
--

Med vänlig hälsning / Best regards,

Wilhelm Sporrong VD

WEBHALLEN.com

****

Webhallen Sverige AB

2 hours 28 minutes later


PASS
PASSPORT
PASSEPORT

SVERIGE SWEDEN SUÈDE

Typ/Type P
Kod/Code SWE
Pass nr./Passport No. 84554606

1. Efternamn/Surname
SPORRONG
2. Förnamn/Given names
CARL JOHAN WILHELM
3. Nationalitet/Nationality
SVENSK SWEDISH
4. Födelsedatum/Date of birth
05 MAR/MAR 80
5. Kön/Sex
M/M
6. Utfärdad/Date of issue
05 JUL/JUL 12
7. Sista giltighetsdag/Date of expiry
05 JUL/JUL 17
8. Födelseort/Place of birth
STOCKHOLM SWEDEN
9. Myndighet/Authority
POLISMYNDIGHETEN I SKÅNES LÄN

3a. Personnr./Pers. id. No.
800305-0476
4a. Längd/Height
186 CM

10. Namnteckning/Signature

P<SWESPORRONG<<CARL<JOHAN<WILHELM<<<<<<<<<<<<<<
84554606<6SWE8003059M2134323198003050476<<<<<<<78

Polisen

16

Passkopia som inkom till Klarna

Signerat av

Signerat datum

Enhet
Polisregion Syd, Bedrägeribrott 2 Rgn Syd

Diarienr
5000-K558623-16

Orginalhandlingens förvaringsplats

Datum
2016-05-18

Tid
10:12

[redacted]

Funktion
Uppgiftslämnare

Berättelse

Sporrong är VD för Webhallen.

Passbilden stämmer inte med Sporrongs verkliga pass.

Passnumret går till ett barn som är född 2006.

Polisen

16

Passkopia som inkom till Klarna

Signerat av

Signerat datum

Enhet
Polisregion Syd, Bedrägeribrott 2 Rgn Syd

Diarienr
5000-K558623-16

Orginalhandlingens förvaringsplats

Datum
2016-05-18

Tid
10:12

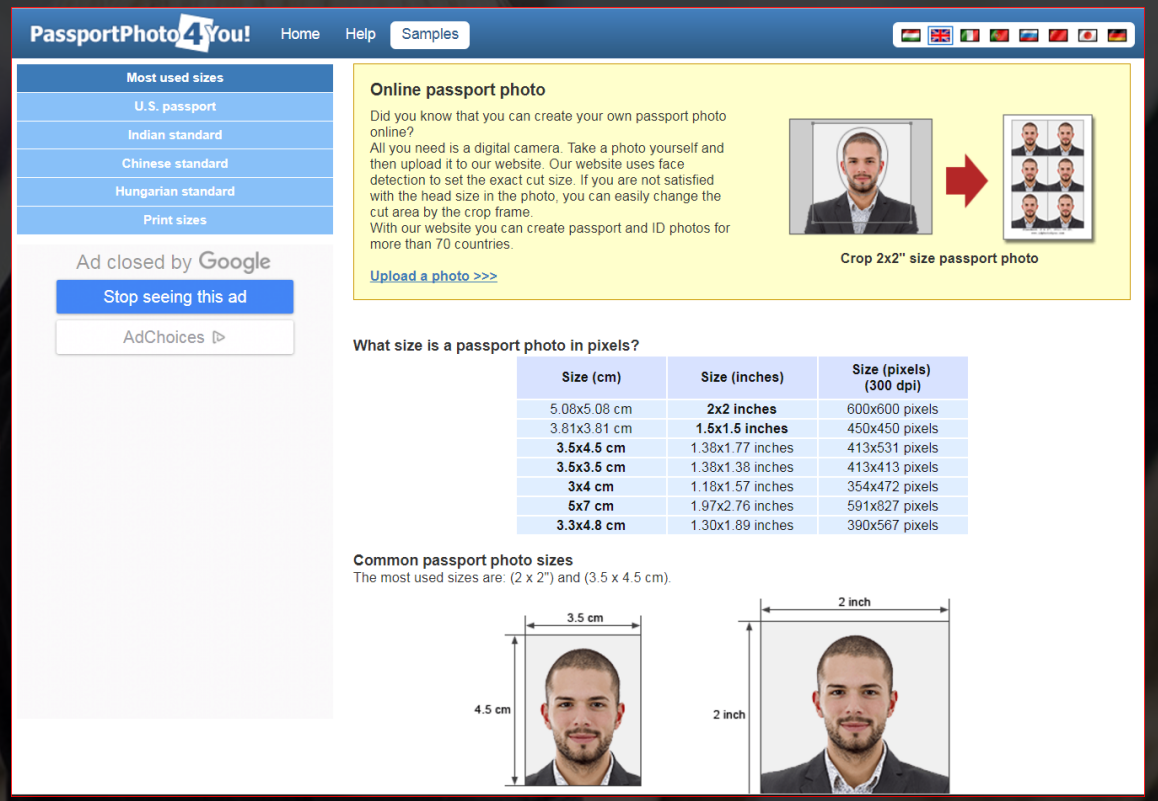
Funktion
Uppgiftslämnare

Berättelse

Sporrong är VD för Webhallen.

Passbilden stämmer inte med Sporrongs verkliga pass.

Passnumret går till ett barn som är född 2006.



Polisen

16

Passkopia som inkom till Klarna

Signerat av

Signerat datum

Enhet
Polisregion Syd, Bedrägeribrott 2 Rgn Syd

Diarienr
5000-K558623-16

Orginalhandlingens förvaringsplats

Datum
2016-05-18

Tid
10:12

Funktion
Uppgiftslämnare

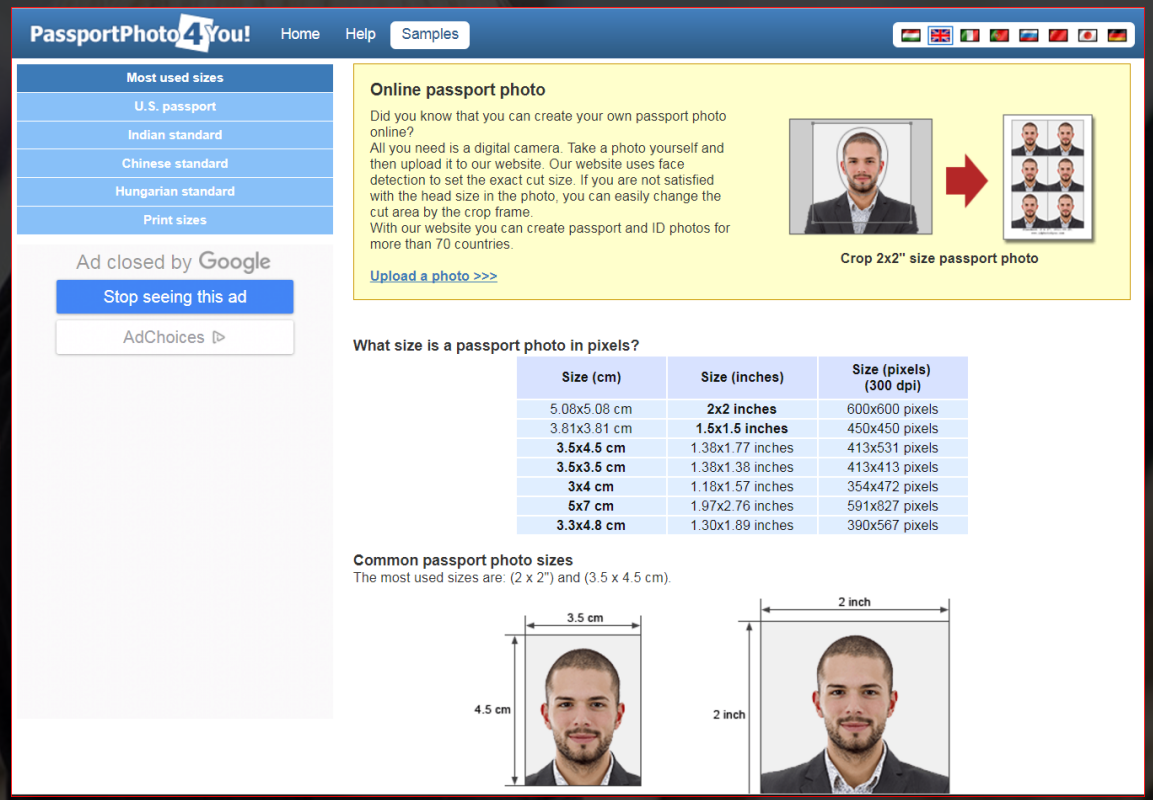
Berättelse

Sporrong är VD för Webhallen.

Passbilden stämmer inte med Sporrongs verkliga pass.

Passnumret går till ett barn som är född 2006.

screen: ehandel.se



WILHELM SPORRONG, EJ FALSKBESTÄLLARE

Webhallens VD används i stort bedrägeriförsök

screen: trustmapp.com

My challange was:

1. To find the domain names ”ad hoc”
Reused of registrant data, patterns, small details, used the same 10 registars

2. Match investigators at the police with the correct registrar/Hosting partner (to secure evidence)

3. Contact the hijacked company to ensure they were informed..

Operation Homoki

Heard in a wire tapping in the summer of 2016, between two suspects when they were planning to register a new domain name:

"We can not register .se, because that damn Forsman is working there!“

Operation Homoki

> *Polismyndigheten kan i sin brottsbekämpande verksamhet inte exkludera externa samarbetspartner. De har i flera stora nationella insatser mot grov organiserad brottslighet visat sig vara värdefulla.*
>
> *Framförallt IIS och Peter Forsman har varit behjälpliga när det gäller internetrelaterad brottslighet. Det har varit en brottslighet med modus som i en samlad bild bedömts som synnerligen allvarlig och samhällshotande. Specifikt brottsförebyggande verksamhet med modus inriktat mot fakturabedrägeri i operation Fafne, Gungner och Draupner samt bedrägeri som föregåtts av dataintrång i operation Homoki.*

[redacted]
Nationell Seriebrottslighet
Polismyndigheten

Homoki I+II
Since 2013 and continuously.
”Special national event”

”Hundreds” of .se- and .nu-domains

Gigantic investigation.
Every police region i Sweden, 13 prosecutors, 50 full time investigators.

1 of 5 trials
Split by modus, so that different parts are judged separately.

Stop and think..

Change of focus:

FROM the *usual* usage as aliases of content and e-mail addresses

TO complete tools of crime.

(Domains solely registered for hoax emails used in BEC and credit frauds.)

Thank you!

IIS Registry
Abuse and Prevention
Peter Forsman
peter.forsman@iis.se