SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Internetový podvod v praxi

Skutočný príbeh so zmenenými menami

Boris Mutina

WHOIS boris.mutina

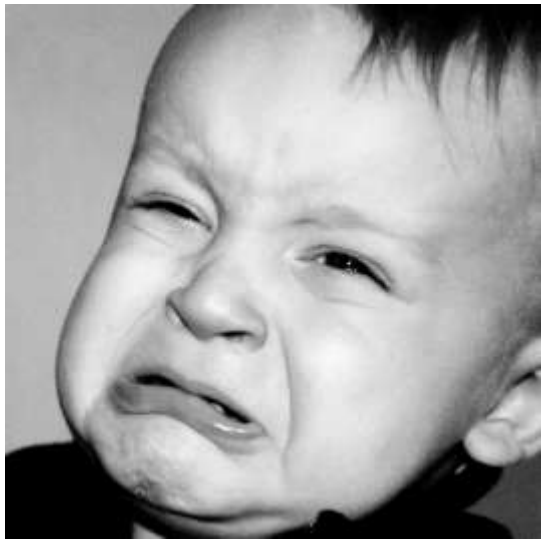
- [vyberte_si] v informačnej bezpečnosti
  - Lektor hackingu
  - Pentester/audítor
  - Bádateľ na poli internetového zločinu
  - Designer extreme security riešení
  - …
    - …určite je toho viac, len si neviem spomenúť ;)))
    - som aj bývalý admin, takže chápem obidve strany

Začiatok je jednoduchý...

- Bola raz obyčajná investičná banka, peniaze požičiavala a investovala, skrátka úplne bežný biznis. Aby šla s dobou, mala aj jednoduchú webstránku, bez bežných retailových služieb to bola len statická prezentácia. Až jedného dňa...

...čo sa to deje???

- Nahnevaný a podvedený klient kontaktoval banku
- FAKT1 – niekto vystupoval ako zástupca banky
- FAKT2 – niekto vytvoril kópiu stránky banky, mal funkčné mailové adresy
- FAKT3 – podvedený nebol jediným poškodeným



...a čo teraz?

AKO SA TO STALO???

PREČO NEMÔŽEME NAKÚPIŤ VŠETKY TIE DOMÉNY?

KOĽKO???

Sumár základných informácií

- Meno banky: JosephBank
- Bežná doména: josephbank.com
- Podvodná doména: groupjoseph.com

  - WHOIS groupjoseph.com

  Registered through WildWest Domains
  [cybersquatting]

  Administrative contact:

  David Stein, 33 Small Lane, LONDON

Zastavenie #1

- Databáza Artists Against 419 obsahuje viac ako 55 tisíc záznamov falošných stránok
- Kvalita stránok je väčšinou pochybná, ale nájdu sa aj (takmer) dokonalé
- Metódy sa už dávno neobmedzujú len na klasický phishing
- Podvodné weby bývajú súčasťou väčšej kriminálnej kampane

Hosting #1

- Podvodná webstránka bola hostovaná na systémoch Agava Software
- Spoločnosť je známa aj programami Antispam, Antispam for Bat, Antispyware...

Hosting #1

- Agava hostovala aj dalšie iné podvodné stránky

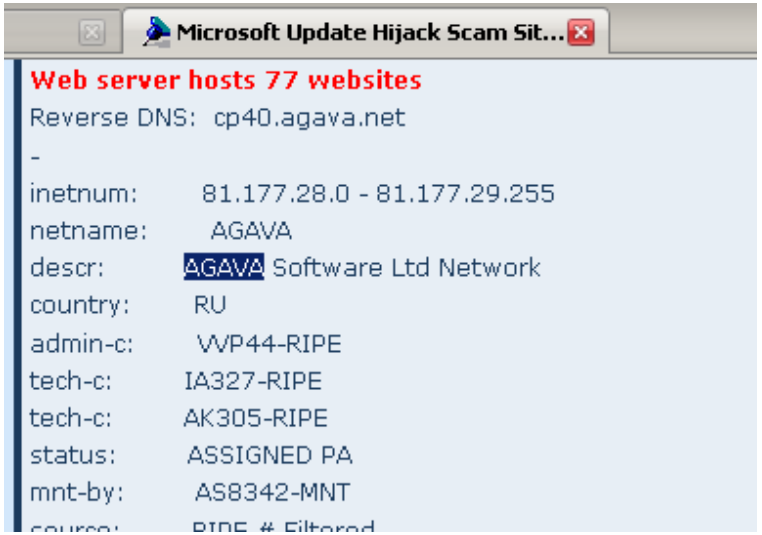
  http://db.aa419.org/fakebankslist.php?x_Web_Host=agava

- Servery Agava sa zapojili aj do tzv. Microsoft Update hijacku

  http://www.bluetack.co.uk/forums/index.php?showtopic=13436

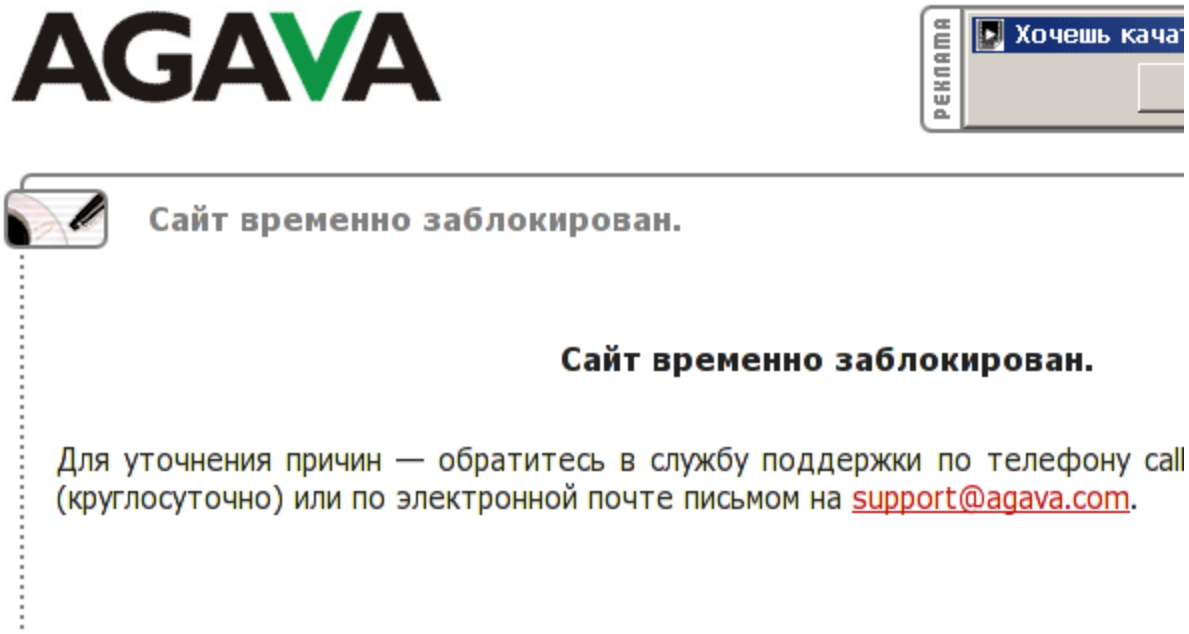
- Agava hostovala aj tzv. Russian Carder Clan

  http://news.netcraft.com/archives/2004/03/01/fraud_hosting_services_widely_promoted.html



Ako sa zbaviť stránky?

- Keďže stránka bola hostovaná v Rusku -> RuCERT, výsledok za 2 dni...



O 20 dní...

- Je tu nová doména aj webstránka
  - joseph-fin-group.com
- Registrovaná AIT Domains (alebo THE NAME IT CORPORATION DBA NAMESERVICES.NET)

2007 ICANN Registrar Statistics

63	174,716	3,943	6,032	7,760	10,645	30,402	PlanetDomain
64	166,592	488	2,912	-151	411	3,660	Easyspace Ltd.
65	162,702	13,456	23,231	6,681	5,644	49,012	Active 24
66	158,531	-12	1,654	812	2,348	4,802	StarGate
67	157,869	3,480	14,232	-3,350	-2,465	11,897	AitDomains.com
68	148,879	-3,025	10,220	3,346	1,812	12,353	PSI Japan
69	143,712	-660	-2,588	-257	-1,356	-4,861	Gabia, Inc
70	137,519	7,863	4,002	7,790	5,253	24,908	Register.it SPA
71	136,369	1,828	2,792	188	2,582	7,400	NordNet

O čom je AIT Domains?

- Registrovanie domén vo veľkých množstvách pre potreby spamu

  http://www.scamfraudalert.com/f42/name-corporation-dba-nameservices-net-5508/

- Sponzoring spamu a botnetov

  http://www.spamhaus.org/rokso/evidence.lasso?rokso_id=ROK7235

- Spoločnosť podporuje rôzne iné formy podvodov a kriminálnych aktivít, napríklad dating scam

  http://news.netcraft.com/archives/2004/03/01/fraud_hosting_services_widely_promoted.html

Kto zaregistroval doménu?

- CSMJBS Enterprises, 412 Lavender Ct.,
  N. Las Vegas, Nevada
- Spoločnosť registrovala viac ako 15 tisíc domén

Hmmm, very interesting. I went to domain from the support email, top-esupport.com, and the domain is not longer resolving. Through the Whois database, the top-esupport.com site is registered to a group called CSMJBS Enterprise, located in Las Vegas, NV. So I decided to conduct a Google search on CSMJBS Enterprise to see what I could find. The first site returned in my search was referencing Fake Sites Database, with a WARNING: "Please be aware that the fake banks, lotteries and companies on the list are used by dangerous criminals. We don't encourage anyone to engage in any form of communication with them. If you chose to communicate them for whatever reason, you will be doing so at your own risk". I decided to do a little poking around. I called the City of North Las Vegas and inquired about CSMJBS Enterprise. First of all the address that was listed in the Whois database was false. The company went into default in April of 2007. Jeremy Stamper, the head of the company resides in Seattle, Washington and has recently been accused by the Department of Financial Institutions Securities Division as running several fraudulent financial websites that has tricked numerous numbers of people into sending in money. Over $2 million dollars have been seized by Las Vegas police.

Kto je za CSMJBS?

- Podľa dostupných informácií je hlavou CSMJBS Enterprises Mr. Jeremy M. Stamper

- Pôvodne zbohatol údajne predajom svojej The Delaware Company LLC (1 milión dolárov)
- V roku 2002 a 2003 zaregistroval domény a vyrobil niekoľko stránok, ktoré spájali politikov s rasizmom a inými absurdnosťami
- Bol prezidentom The Progressive Homesellers
- Zaregistroval niekoľko domén podobných ako svetové značky (jediný súdny spor s Estée Lauder vyhral)
- Prevádzkoval niekoľkých neúspešných projektov (Topic5.com, PersonRatings.com, AskAmerica)
- Bol zapojený do job-scamu – TooSpoiled.com

Profesionálny podvodník?

Paul Thebaud

Views : 75

Boston, MA USA

PAUL THEBAUD **OVERVIEW** Add

Paul is a highly regarded personal plaintiff's attorney who graduated with honors from Boston University. Mr. Thebaud earned his JD from Boston College and has been a practicing attorney for 10 years.

more »

Jeremy Stamper

- Prevádzkoval spoločnosti Federal Savings LLC, JMA Northwest Investment a First Bancshares
  - Ponúkal úrok od 6,25 do 8,85% - bez finančného krytia
  - Úrady prikázali vrátiť vklady a zastaviť činnosť

http://www.dfi.wa.gov/sd/orders/S-07-054-07-CO01.pdf

STATE OF WASHINGTON
DEPARTMENT OF FINANCIAL INSTITUTIONS
SECURITIES DIVISION

IN THE MATTER OF DETERMINING whether there has been a violation of the Securities Act of Washington by: Federal Savings, LLC; First Bancshares Inc.; JMA Northwest Investments, LLC; Jeremy M. Stamper Respondents.	Order Number S-07-054-07-CO01 CONSENT ORDER

Stránka migruje

- Stránka joseph-fin-group.com bola hostovaná na serveroch spoločností
  - Mochahost
  - FastDomain (BlueHost)
  - Promohosting
  - Starline.ee
  - ISP System UUNet...
- Všetky tieto spoločnosti aspoň raz hostovali nejaký e-podvod
- Kooperovali sme s CERT teamami, APWG a inými

Zastavenie #2

- BlueHost vôbec nie je neznámym menom...
  - Štatistika hosterov iných podvodných stránok neexistuje

Phishiest Hosters

Hoster	Phishing Sites	% of phishing sites hosted
Softlayer Inc	18544	23.9
UK2 Group	7867	10.1
Nsentry	3681	4.7
inmotionhosting.com	2895	3.7
Lunarpages	2500	3.2
Bluehost	2347	3.0
iWeb Technologies inc	2260	2.9
VPLS, Inc.	2012	2.6
Synergetic AG	1842	2.4
NedZone Internet	1794	2.3
kinghost.com.br	1723	2.2
almouroltec.com	1488	1.9

Veľký deň

- Webstránka zmigrovala 21.septembra 2008 na servery spoločnosti Intercage Inc.
- V ten deň Pacific Internet Exchange odpojil „z racku“ siete Atrivo/Intercage

'Malware-friendly' Intercage gets PIE in the face

Net provider goes dark after all

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Security, 22nd September 2008 19:08 GMT

Updated California-based network provider Intercage has gone completely offline following weeks of scathing criticism that it hosts an inordinate number of sites engaged in phishing, malware propagation, and other illegal activities.

Pacific Internet Exchange, which only began providing upstream service to Intercage in the last week or so, pulled the plug on Saturday night, according to someone who answered PIE's phone and would identify himself only by the first name of Brian. He refused to say why PIE had terminated service.

It's a safe bet that PIE's move was in response to recent efforts to isolate Intercage following a report that it enables a rogue's gallery of customers to punt spam, malware, and online (illegal) pharmaceuticals. The report so tarnished Intercage's already struggling reputation that both of its longterm providers canceled service. Intercage would have gone dark then

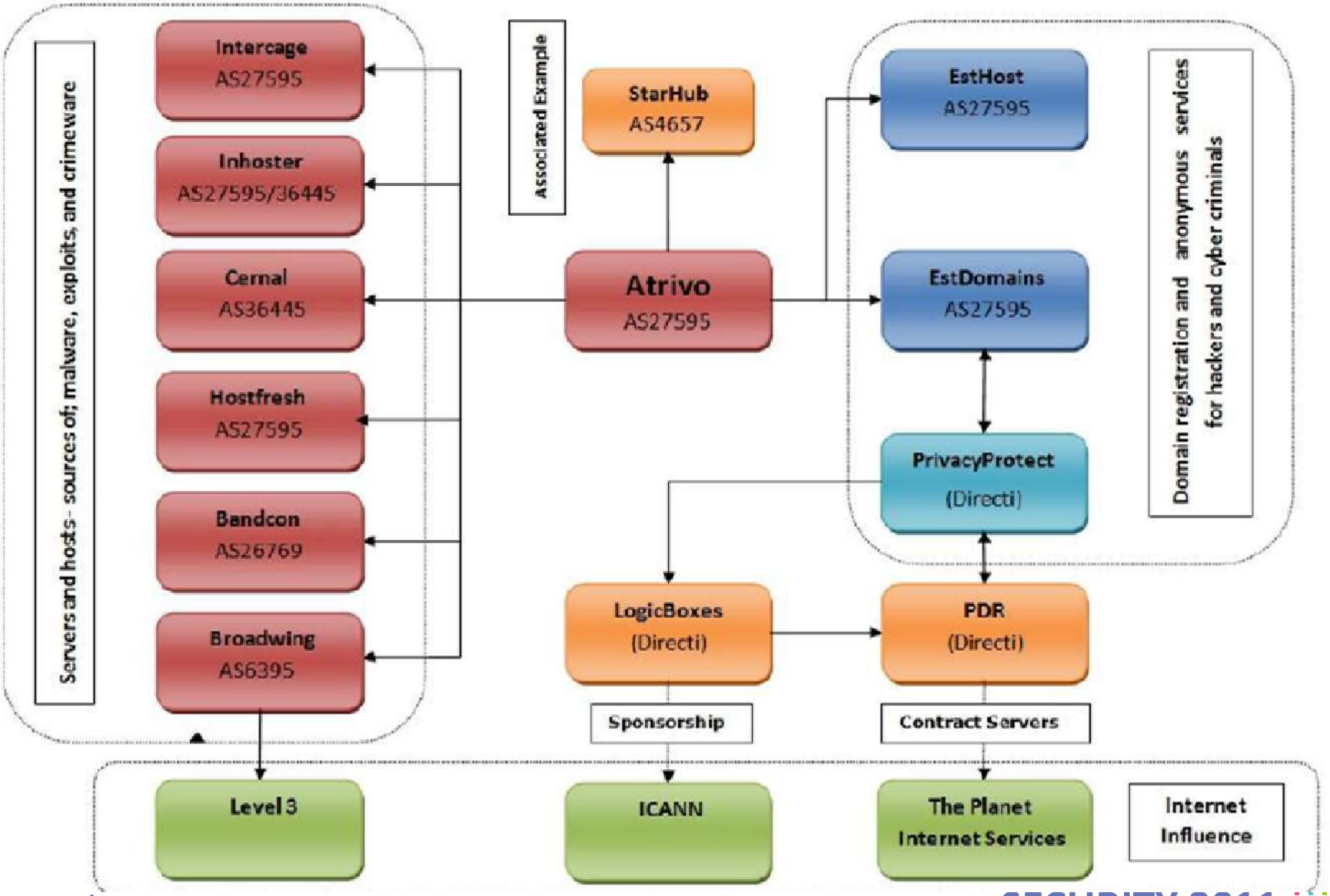
Atrivo/Intercage?

- Jart Armin/HostExploit.com vo svojej správe v roku 2008 o cyber-zločine v USA hovorí o Atrivo/Intercage ako o pravej ruke RBN

SPAMHAUS

SBL Live and Historic for Atrivo/Intercage				
Date	Record	IP Involved	Host	Reason
2008-08-25 23:49:36	SBL67373	69.50.181.122/32	atrivo.com	Spam/cybercrime support: ANTI-CAPTCHA.COM/SUPERGENA.COM
2008-08-05 17:13:57	SBL66649	85.255.118.42/32	atrivo.com	More hijack malware on Cernel/inhoster/Intercage
2008-07-30 07:47:24	SBL66515	85.255.113.226/32	atrivo.com	Malware dropper cybercrime gang
2008-07-30 08:35:02	SBL66408	85.255.117.163/32	atrivo.com	Virus writers, malware spreaders, C&C servers
2008-08-08 21:27:23	SBL66405	85.255.117.205/32	atrivo.com	Virus writers, malware spreaders, C&C servers
2008-08-08 21:07:21	SBL66404	85.255.117.202/32	atrivo.com	Virus writers, malware spreaders, C&C servers
2008-08-08 21:27:24	SBL66401	85.255.118.171/32	atrivo.com	Virus writers, malware spreaders, C&C servers
2008-07-26 21:10:23	SBL66400	85.255.120.0/24	atrivo.com	Virus writers, malware spreaders, C&C servers
2008-07-02 16:20:35	SBL65349	85.255.120.234/32	atrivo.com	Myspace spambot malware
2008-07-05 19:06:08	SBL65305	69.50.160.212/32	atrivo.com	Malware installer - "video codec"
2008-06-03 22:21:02	SBL65091	69.50.173.43/32	atrivo.com	Russian Cybercrime: rootdns.ru / swerjr.ws
2008-05-20 22:53:05	SBL64850	85.255.118.180/32	atrivo.com	"video codec" malware installer
2008-06-25 20:15:19	SBL64779	85.255.113.219/32	atrivo.com	Malware installer - "video codec" (atrivo.com)
2008-05-11 08:48:49	SBL64676	216.255.190.26/32	atrivo.com	Storm worm installer host
2008-05-11 08:47:30	SBL64675	216.255.189.210/32	atrivo.com	Storm worm installer host
2008-05-11 08:42:02	SBL64672	69.50.166.234/32	atrivo.com	Storm worm installer host

Atrivo/Intercage



Čo alebo kto je RBN?

- RBN=Russian Business Network
- Najväčšia a najaktívnejšia zločinná organizácia na internete
  - Údajná podpora ruskej vlády
  - V pozadí útokov na Estónsko a Gruzínsko
  - Obrovský obrat z rôznych aktivít
    - Spam, podvody, phishing
    - Vírusy, botnety, malware, rootkity
    - Pornografia, pedofília
    - Carding...

Záver #1

- Jeremy Stamper zmizol v auguste 2010 z internetu, pred tým zanechal túto správu na svojom blogu

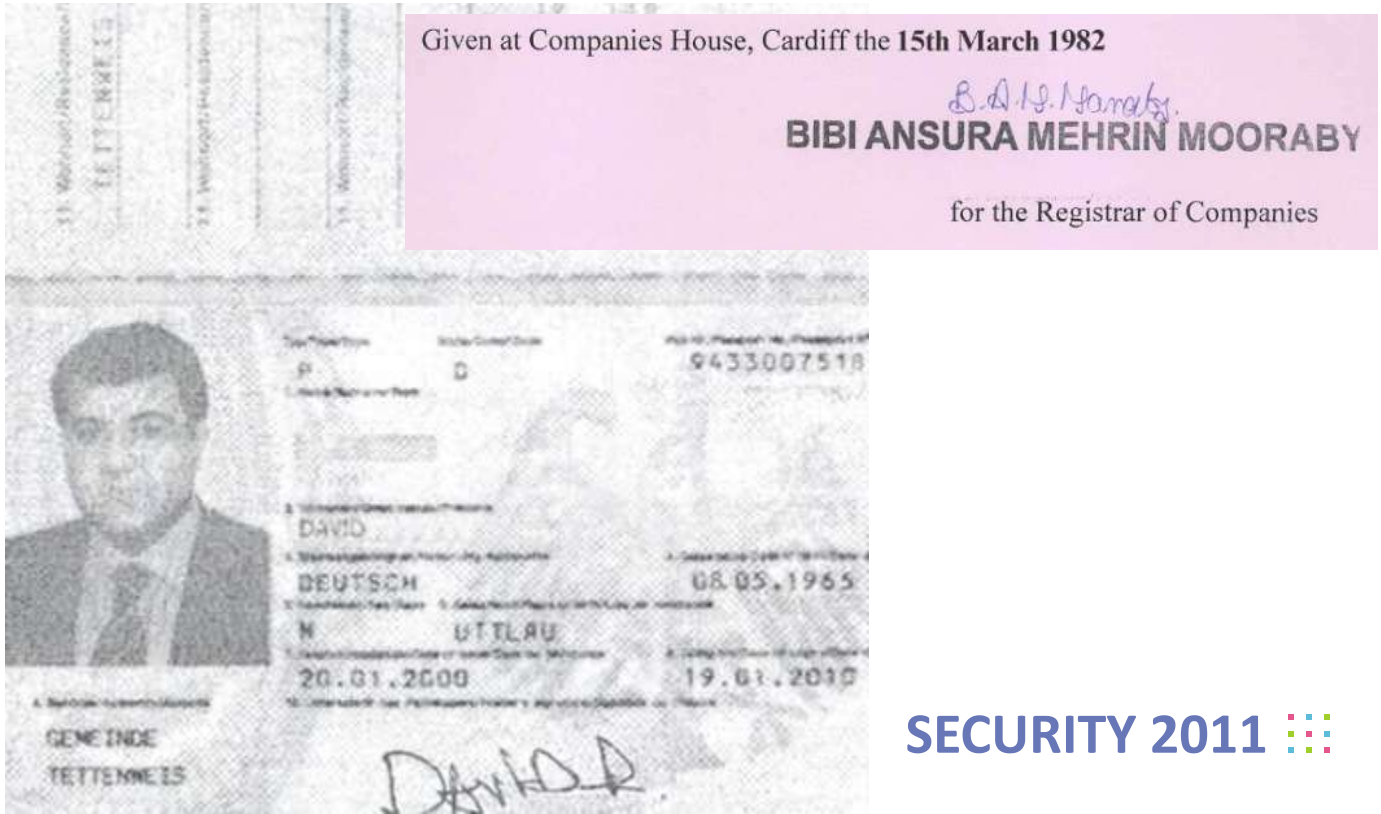
Since then, my name has been linked to spammers, phishers, boiler rooms, threatened lawsuits, and more. Not only has my name been used, but my home address and phone numbers as well. The worst part: I can't really complain about it. I didn't have my identity stolen; I rented it out.

- Jeho sestra Meaghan Stamper McKaige zasa takúto...

Within a few months of offering the service, 'Meaghan McKaige' was listed as 'director' or 'President' of dozens of companies. Unfortunately, a number of these companies ended up being nothing more than scams. Since then, my formerly good name is a lot worse for wear. So, what does this have to do with my mail being stolen? Since then, not only has my name been used, but my home address, phone numbers and (I believe) my social security number. The police have been...well, totally uninterested.

Záver #2

- Podvodníci nakoniec narazili...
  - David Stein kontaktoval finančného analytika v Istanbule, ktorý pozná predstaviteľov Joseph Bank
  - Poskytol falošné doklady o sebe a spoločnosti



Záver #3

- Zástupcovia banky a analytik aj pomocou našich dôkazov presvedčili tureckú políciu
- Analytik zorganizoval stretnutie, na ktorom mal predať peniaze na „investovanie“
- Polícia zatkla štyri osoby, medzi inými aj Davida Steina...
  - september 2008 bol najúspešnejším mesiacom Turecka v boji proti cyber-zločinu (náš prípad, Chao...)
- Kópia stránky sa už nikdy neobjavila online...

A čo bude ďalej?

- Jediný prípad svojho druhu (pretože bol vyšetrovaný a zverejnený) poukazuje na komplexnú štruktúru kriminálnej siete
- Denne pribúdajú stovky nových podvodných stránok – kto je za nimi?
- Aká je trestná zodpovednosť zločincov?
  - A schopnosti vyšetrovateľov?

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Ďakujem za pozornosť.

Boris Mutina
Security Lab SAGL
boris.mutina@sec-lab.com