

Harvesting boarding passes

28C3 – Lightning Talks – Day3



Andrei Costin <andrei@andreicostin.com>
andreicostin.com/papers

Intro



Modern concerns



Online check-in is established trend



Seat plan for your flight

Heraklion - Gatwick (London)
BA6703, 22:25 Tue 04 September 2007

Euro Traveller
Aircraft type : Airbus A320 jet


Available seat 24C

Continue

Exit without changes

We can learn airline preferences



 **UNITED**

AIR CANADA 

 **AMERICA WEST**

 **U.S. AIRWAYS**


CATHAY PACIFIC

American Airlines®

BRITISH AIRWAYS 

ANA 

Alitalia


sabena 

AIR FRANCE 

virgin atlantic 

 **QANTAS**

JAL 

 **Delta Air Lines**


AIR NEW ZEALAND

 **NORTHWEST**

 **VARIG**

 **Lufthansa**

 **Thai**
Thai Airways International

swissair 

SINGAPORE AIRLINES 

SAS


KLM

FTdetails – checkins, logins, other actions



Preferred hours – predictable time



VERTREK		DEPARTURES		
Tijd Time	Vlucht Flight	Bestemming Destination	Balie Desk	Opmerking Remarks
00:00	HV-000	BAGGAGE DROPOFF	05 05	TRANSAVIA
00:00	HV-001	BAGGAGE DROPOFF		TRANSAVIA
00:00	VG-000	ALL VG-FLIGHTS	01	VLM AIRL.
00:00	VG-000	BAGGAGE DROPOFF	01	VLM AIRL.
•14:00	AAG-001	• COVENTRY		• ATLANTIQUE
14:05	HV-5053	ALICANTE	04	TRANSAVIA
14:55	HV-5023	MALAGA	07 07	TRANSAVIA
15:10	VG-287	LONDON/CITY AIRPORT	02 03	VLM AIRL.
15:45	HV-213	EINDHOVEN	08	TRANSAVIA
15:45	HV-213	TENERIFE	08	TRANSAVIA
16:20	HV-6093	FARO	04	TRANSAVIA
17:00	VG-291	LONDON/CITY AIRPORT	02 03	VLM AIRL.

Roken in het gebouw en op het platform is niet toegestaan **12:0**

SAMSUNG

Preferred routes/ports – predictable space



Predictable \$HOME



Various /dev/random ideas



- **Track reconstruction/following**
 - and eventually analysis and alarm in case out-of-pattern/out-of-plan actions occur
- **Learn travelling habits**
 - so that next “moves” can be predicted/evaluated and attacker-actions planned accordingly, etc.

Various /dev/random ideas



- Impersonate the person with a higher degree of credibility given level of details learned
- Learn very-near future plans
 - every 24h window try to check-in given FT-number and last name and see what flights are scheduled for the person)

Various /dev/random ideas



- **Direct effects on victim's plans**
 - checkin cancelation
 - checkin seat-assignment convenient to the attacker so that next-phases of social engineering can be conducted
 - group-checkin impersonation so that person is being more or less associated with a group of persons (good or bad) without their own will

Various /dev/random ideas



- Marriage cheating cases more easily detectable, etc.
 - Useful for private-detective services
- Deliberate “leakage” of fake/misleading boarding passes by the “victim”
 - “victim” is actually an attacker in this case
 - so that intelligence gathering dudes will have a hard time tracking down the so called “victim” 😊

Useful “google dorks”



"BOARDING PASS" "Please keep this document until the end of your trip" file



About 43 results (0.17 seconds)

[\[PDF\] Internet Check-In](#)

www.sarv.ee/ftp/henn/Kommertskool/Magistrid/Eksam.pdf

File Format: PDF/Adobe Acrobat - [Quick View](#)

BOARDING PASS. Please keep this document until the end of your trip. Sec. nr.: KL1674: 055, KL1329: 024. Name. ██████████. E-ticket #. ██████████...

[\[PDF\] Internet Check-In](#)

ludde.starkast.net/dokument/Boardingpass-ludde.pdf

File Format: PDF/Adobe Acrobat - [Quick View](#)

BOARDING PASS. Please keep this document until the end of your trip. Sec. nr.: AF1263: 36, AF7680: 71. Name. ██████████. E-ticket #. ██████████...

Useful “google dorks”



- **KLM**

- “BOARDING PASS” “Please keep this document until the end of your trip” filetype:pdf
- intitle:“Internet Check-In” filetype:pdf
- “Internet-CheckIn-Boarding-Docs.pdf“

- **LUFTHANSA**

- “API+Boarding+Pass”+filetype:pdf
- (name OR nome) “etix” “Boarding Pass” filetype:pdf
- boarding pass etix intitle:lufthansa intitle:pdf filetype:pdf

Useful “google dorks”



- **AMERICAN AIRLINES**
 - "Print+Boarding+Pass(es)"
- **EASYJET**
 - "easyJet.com Internet check-in boarding pass" filetype:pdf
- **AEGEAN**
 - "boardingPass.pdf"
- **JETSTAR**
 - "Web Check-in Boarding Pass" filetype:pdf

Take away: secure your sensitive details



Take away: Contribute



- <http://www.exploit-db.com/google-dorks/>

GOOGLE

HACKING-DATABASE

Take away: Don't stalk!



IT'S not A JOKE.
IT'S not ROMANTIC.
IT'S not OK.

stop
STALKING

www.ncvc.org/src

Thanks



- andrei@andreicostin.com
- andreicostin.com/papers
- [Harvesting boarding passes](#)