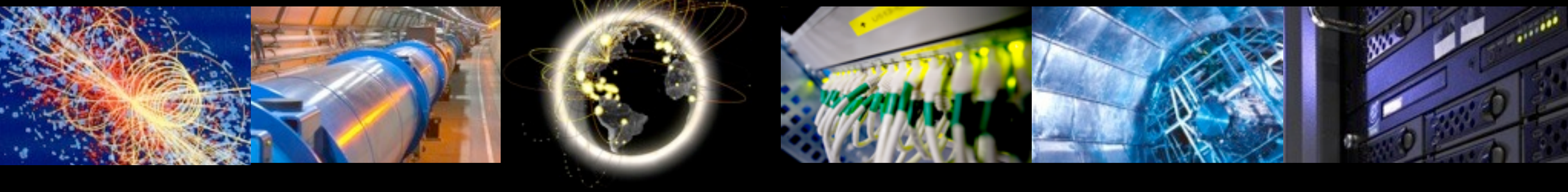
WLCG Group

Security update

HEPiX Fall 2013 Meeting, Ann Arbor, R. Wartel



WLCG
Worldwide LHC Computing Grid

News from the front

THE ILLUSTRATED
LONDON NEWS.

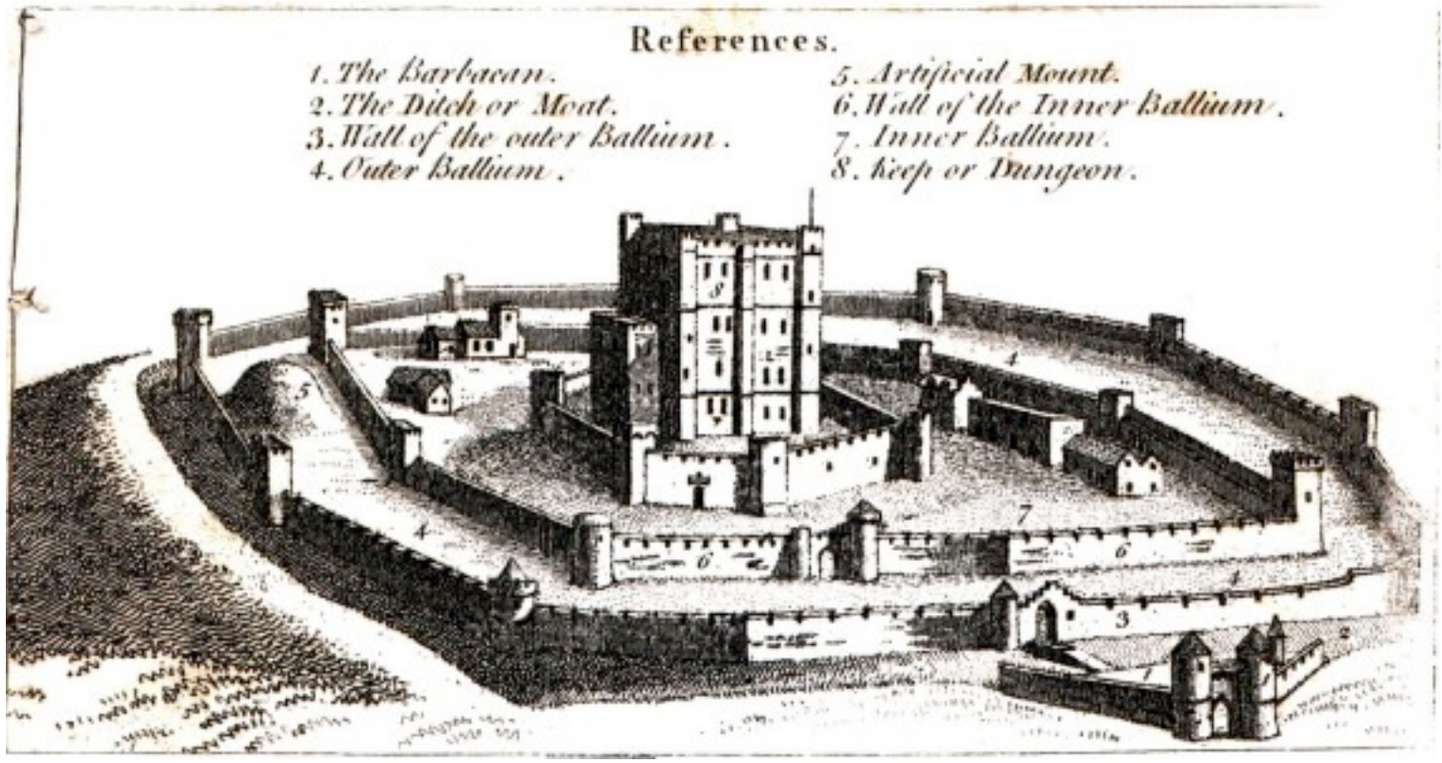
No. 2086.—VOL. LXXIV. SATURDAY, JUNE 7, 1879. WITH SUPPLEMENT | SIXPENCE

Previously on...

- Continuation of the previous HEPiX talk
  - http://cern.ch/go/xQd9
- Paradigm shift in computer security
  - Evolution from a perimeter-based security model
  - Towards an all-Internet, dynamic security model
- Landscape is more complex but not necessarily less favorable now

Security: the classic approach

- Very “medieval” approach
- Well defined security perimeters
- Goal : keep the attackers outside of the security perimeter



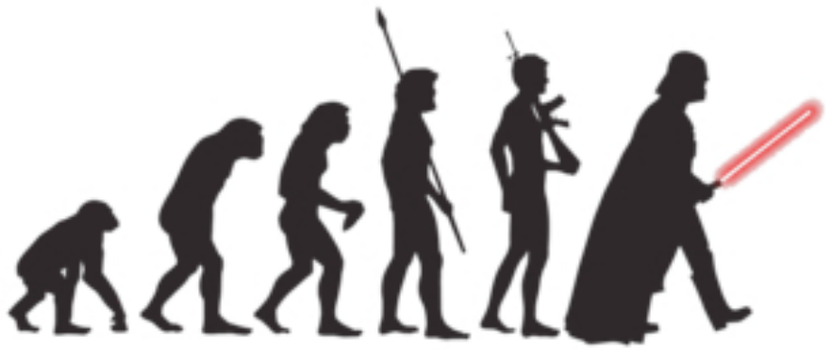
- In our environment, relying simply on controls and security perimeters is bound to fail

Security: a paradigm shift

- Evolution of the controls mechanisms over time
- Access to computing resources is granted to users:
  (Trust : both party agreed to follow a set of policies)
  - Trusted, locally registered (1990s)
  - Trusted, remotely registered at trusted (grid) sites (2000s)
  - Remotely registered users at sites in trusted federations (2010s)
  - Remotely registered users at sites with a good reputation (Facebook, Google, etc.)?
  - Remotely registered users?
  - Remote users?

Time

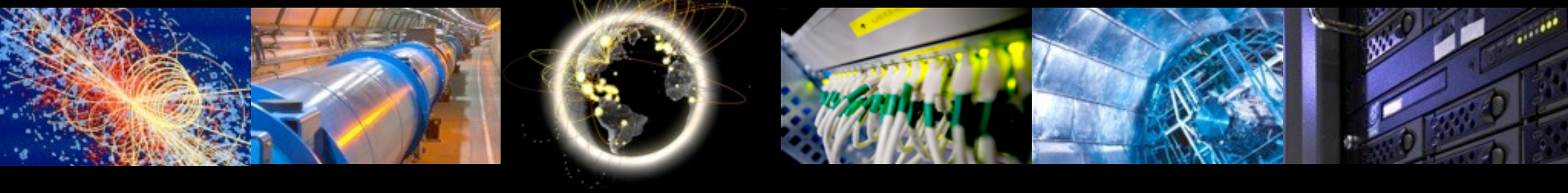
- How can we manage this?
  - Traceability and access control
  - International information sharing and trust



Old vs New

"Good old days"	2013
Local hardening and prompt patching	Local hardening and prompt patching
Local users	User communities and federations
Firewall & ports	Traceability
Malicious users	Malicious organisations
Local expertise	Global intelligence & collaboration
Malicious software	Malicious infrastructures
Local management	Press and media
No escalation possible	Law enforcement may help

Motivation and adversaries

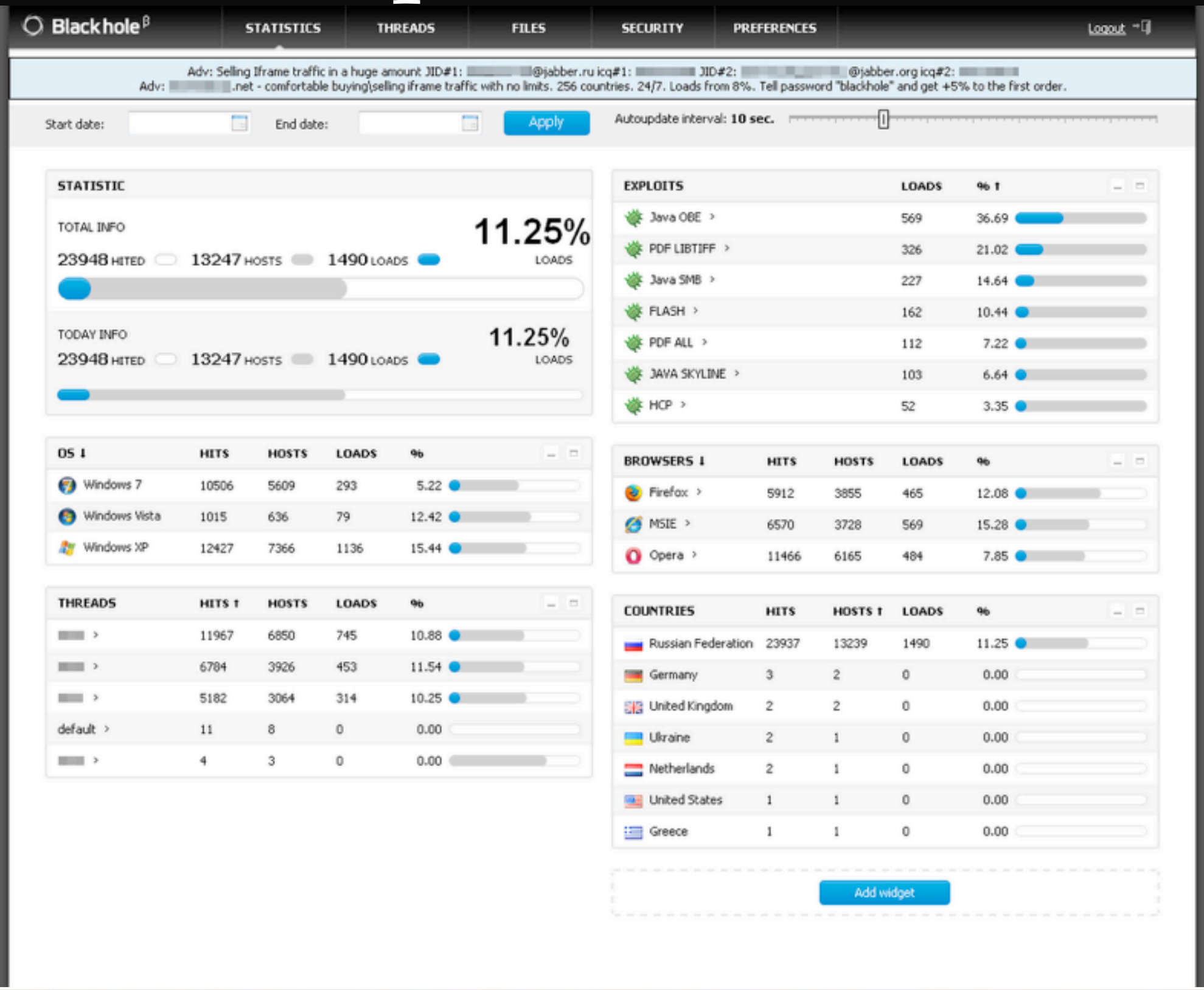


Old-school attackers

For-profit attackers

- Spent many years exposing how attacks have become professional, sophisticated, and for-profit.
- Stakes have become much higher!

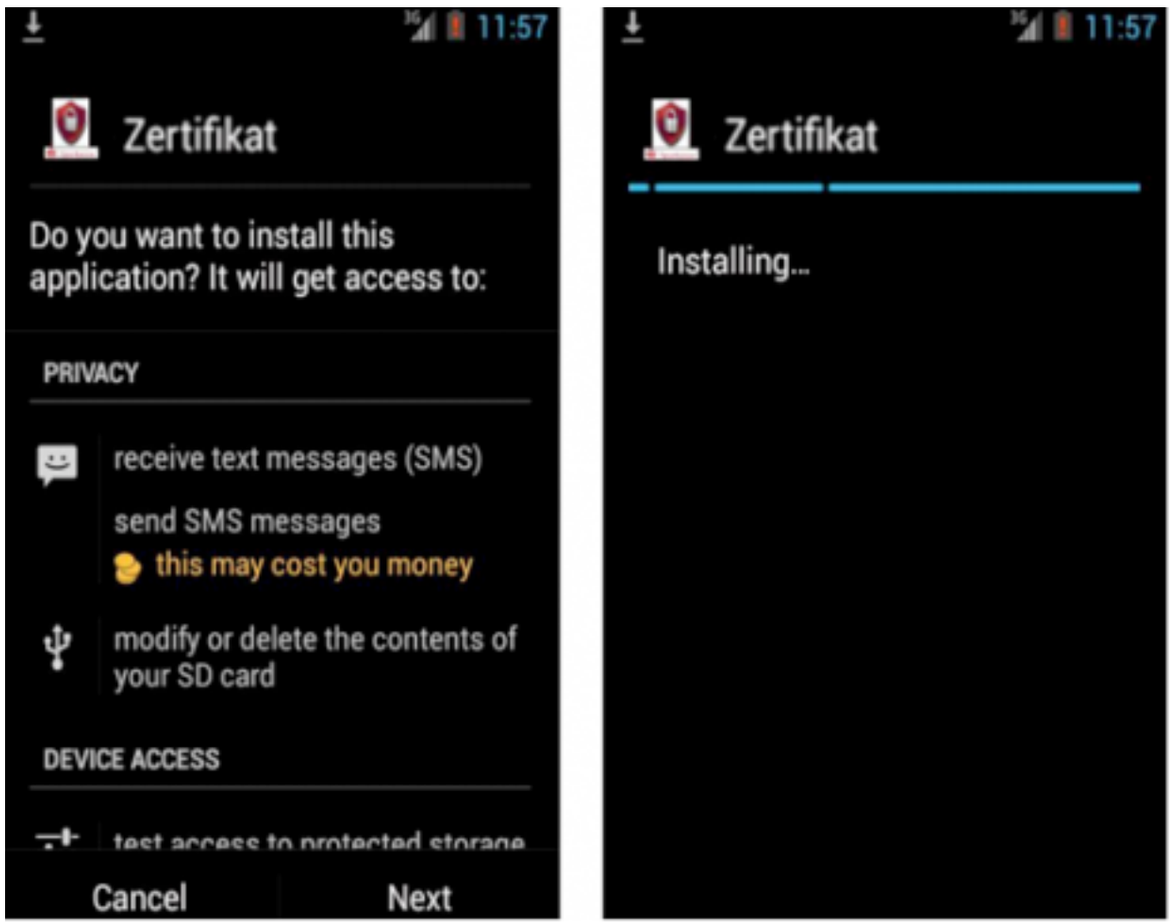
For-profit attackers

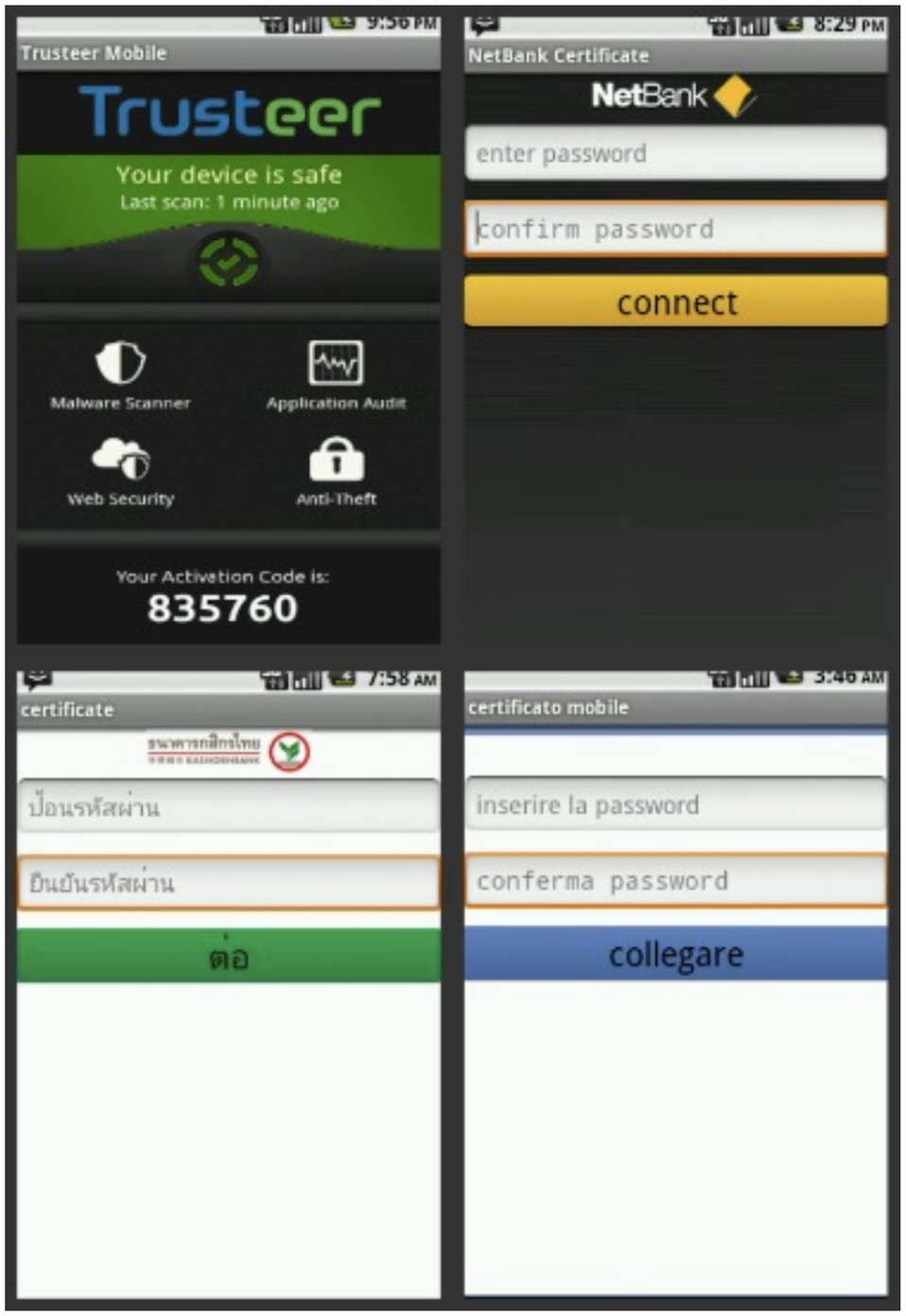


Adv: Selling Iframe traffic in a huge amount JID#1: [redacted]@jabber.ru icq#1: [redacted] JID#2: [redacted]@jabber.org icq#2: [redacted]
Adv: [redacted].net - comfortable buying\selling iframe traffic with no limits. 256 countries. 24/7. Loads from 8%. Tell password "blackhole" and get +5% to the first order.

For-profit attackers

- Perkele, used with Citadel, Zeus, etc.
  - Intercepts 2nd factor (SMS) from banks
  - $1000 for one bank support
  - $15000 for universal support





Government-class attackers

- Political motivation always existed
  - Mass-surveillance also
- Now it has become much more prevalent
- Extremely sophisticated attacks
  - Stuxnet, Flame, Duqu
  - "Experts believe that Stuxnet required the largest and costliest development effort in malware history" (http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104)
- Attacks and malware development is increasingly becoming state-based
  - Caveat: attacks might come from your own state

Government-class attackers

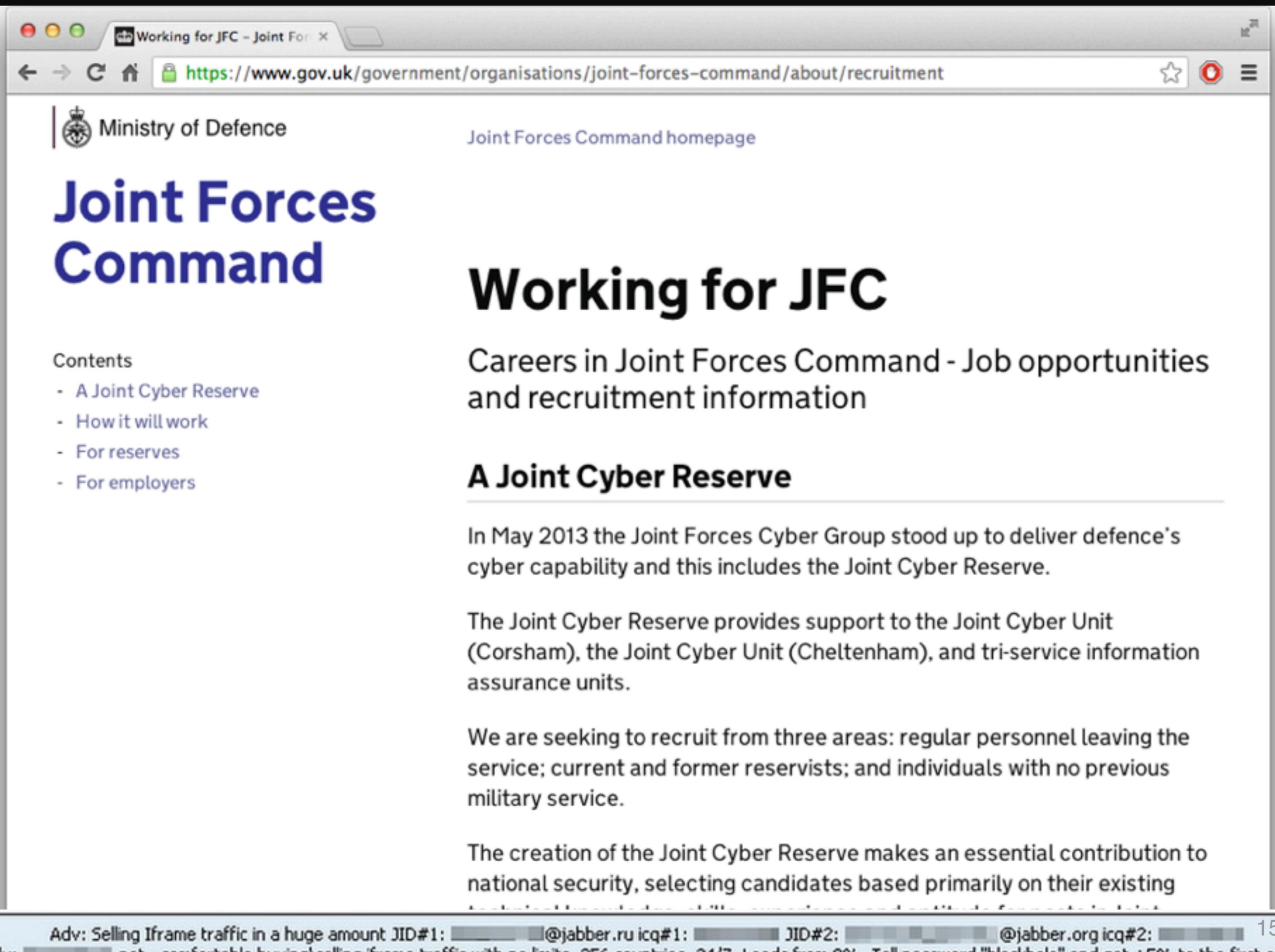
Government-class attackers

Google, Vodafone, Military, Government & other high profile websites of Qatar Defaced by Syrian Electronic Army.

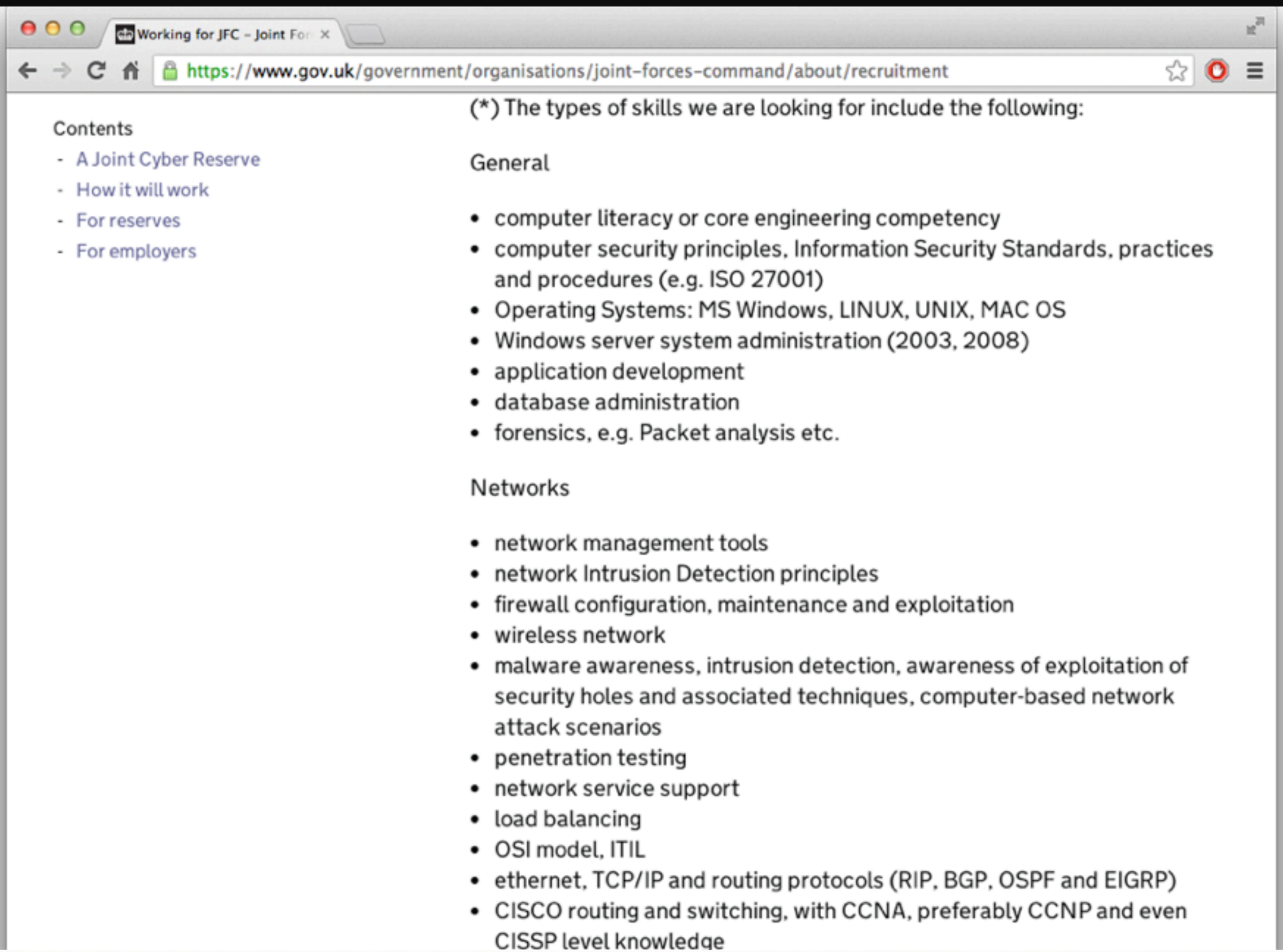
By **Abhishek kumar** on 11:06

The pro Hacker Group Syrian Electronic Army successfuly managed to get full control over the The domain registrant system of Qatar, Domain name with .qa, .biz.qa, .com.qa, .edu.qa, .gov.qa, .info.qa, .mil.qa, .name.qa, .net.qa, .org.qa, .sch.qa are regulated by ICT qatar. and were effected. Sea some how was able to get access to the admin panel and change the dns information of Many of the websites. which caused the Websites being redirected to deface page with the picture of president AL-Assad, shown in the above screenshot.

Government-class attackers



Government-class attackers



Government-class attackers

www.vupen.com/english/services/lea-index.php

VUPEN security

Home | VUPEN Products | Industry Solutions | Vulnerability Research | Contact Sales | Company & Events | Customer Area

Exclusive Exploits for LEAs

Offensive Solutions Overview

Receive More Information

VUPEN EXCLUSIVE AND SOPHISTICATED EXPLOITS
FOR OFFENSIVE SECURITY

Next

Exclusive & extremely sophisticated zero-days for offensive security

As the leading source of advanced vulnerability research, VUPEN provides **government-grade zero-day exploits** specifically designed for law enforcement agencies and the intelligence community to help them achieve their offensive **cyber missions** and **network operations** using extremely sophisticated and exclusive zero-day codes created by VUPEN Vulnerability Research Team (VRT).

While other companies in the offensive cyber security field mainly act as brokers (buy vulnerabilities from third-party researchers and then sell them to customers), **VUPEN's vulnerability intelligence and codes result exclusively from in-house research efforts** conducted by our team of world-class researchers.

Our offensive and exclusive exploits take advantage of undisclosed zero-day vulnerabilities discovered by VUPEN researchers, and bypass all modern security protections and exploit mitigation technologies including DEP (Data Execution Prevention), ASLR (Address Space Layout Randomization), and sandboxes.

Only available for trusted countries and Government agencies

Because of the sensitive nature of the information provided through this service, VUPEN has built **transparency** and defined **very strict eligibility criteria** for participants.

Access to this service is limited to Government organizations only (Law Enforcement, Defense, and Intelligence agencies) in countries members of NATO.

As a European company, **VUPEN has chosen to comply with the most restrictive European and international regulations** on technology exports. Thus we automatically refuse to work with:

- Countries which are subject to the European Union Restrictive measures in force (Article 215 TFEU)
- Countries which are subject to international embargoes adopted by United Nations
- Countries which are subject to international embargoes adopted by United States

Even if an organization fully meets all the above criteria, and complies with our "Know Your Customer" program, VUPEN solely reserves the right to deny access to the service to any agency or country. Requests from non-NATO countries will be subject to a case-by-case and thorough analysis.

Adv: Selling Iframe traffic in a huge amount JID#1: [redacted]@jabber.ru icq#1: [redacted] JID#2: [redacted]@jabber.org icq#2: [redacted]
Adv: [redacted].net - comfortable buying\selling iframe traffic with no limits. 256 countries. 24/7. Loads from 8%. Tell password "blackhole" and get +5% to the first order.

Government-class attackers

- National security agencies snooping beyond borders
  - Via “classified” agreements
  - Via “unknown” vectors, “DRTBOX”
- Not a surprise
  - However, the scale and scope was unexpected to many
  - Direct access at many vendors and service providers unexpected
  - NSA is not the only agency doing this

Impact on HEP labs?

- Politically motivated attacks and surveillance
  - Who owns your routers?
    - It is pretty difficult to determine
    - (Tip: setting your User Agent to “xmlset_roodkcableoj28840ybtide” gives instant root on many D-Link routers)
  - How can you protect your staff and users?
    - Data privacy is a significant concern
    - (And a marketable feature)
- Now facing extreme levels of sophistication (political/money)
  - Complex malware, complex infrastructures
  - Far too much expertise needed for an average site/system admin
- Important to have or be in touch with knowledgable experts
  - If not possible, then join existing efforts and contribute
  - Many groups of trusted experts always keen to help!

Impact on HEP labs?

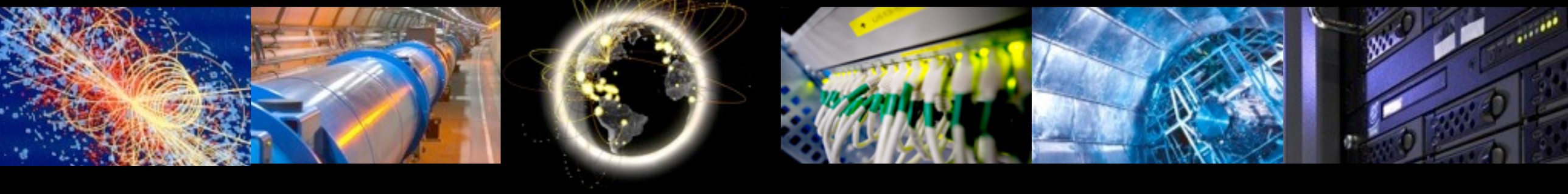
- Crucial importance of international collaboration
  - At the policy level (trust), e.g. http://www.eugridpma.org/sci/
  - At the operational level

- Real life example in Oct 2013:
  - Polish site reports compromise, identifies malicious IP and one local compromised user account
  - CERN observes SSH connection attempts
    - From the very same malicious IP
    - Using a different, but existing username
    - The user only has accounts at one Spanish and one German site
  - Obviously, some parts of the puzzle are missing!

Cooperation is crucial

- Standing out alone means
  - You will miss intel enabling you to pro-actively protect yourself
  - You will not be informed of incidents affecting the community
  - You will probably not be contacted if compromised
- If you have local security expertise
  - Make your security staff has enough expertise and contacts
  - Identify and participate in the most relevant security community
- Even if you don't have local expertise,
  - Simply getting in touch with your closest CERT
    - http://www.ren-isac.net/, national or academic CERT, etc.
  - Fully cooperate with them (trust)
  - Many ways to participate (funding, hosting, meetings, etc.)

Questions?



Who put the backdoor in the D-Link routers?

- ★ The NSA
- ★ The Chinese
- ★ Santa Claus
- ★ Bruce Schneier
- ★ Joel