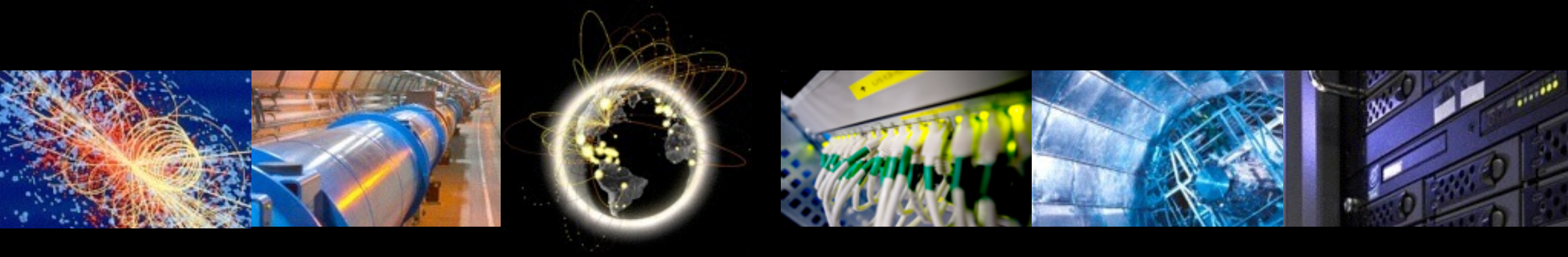
# Computer Security Landscape



*ISGC 2016, 15th March 2016, Taipei*

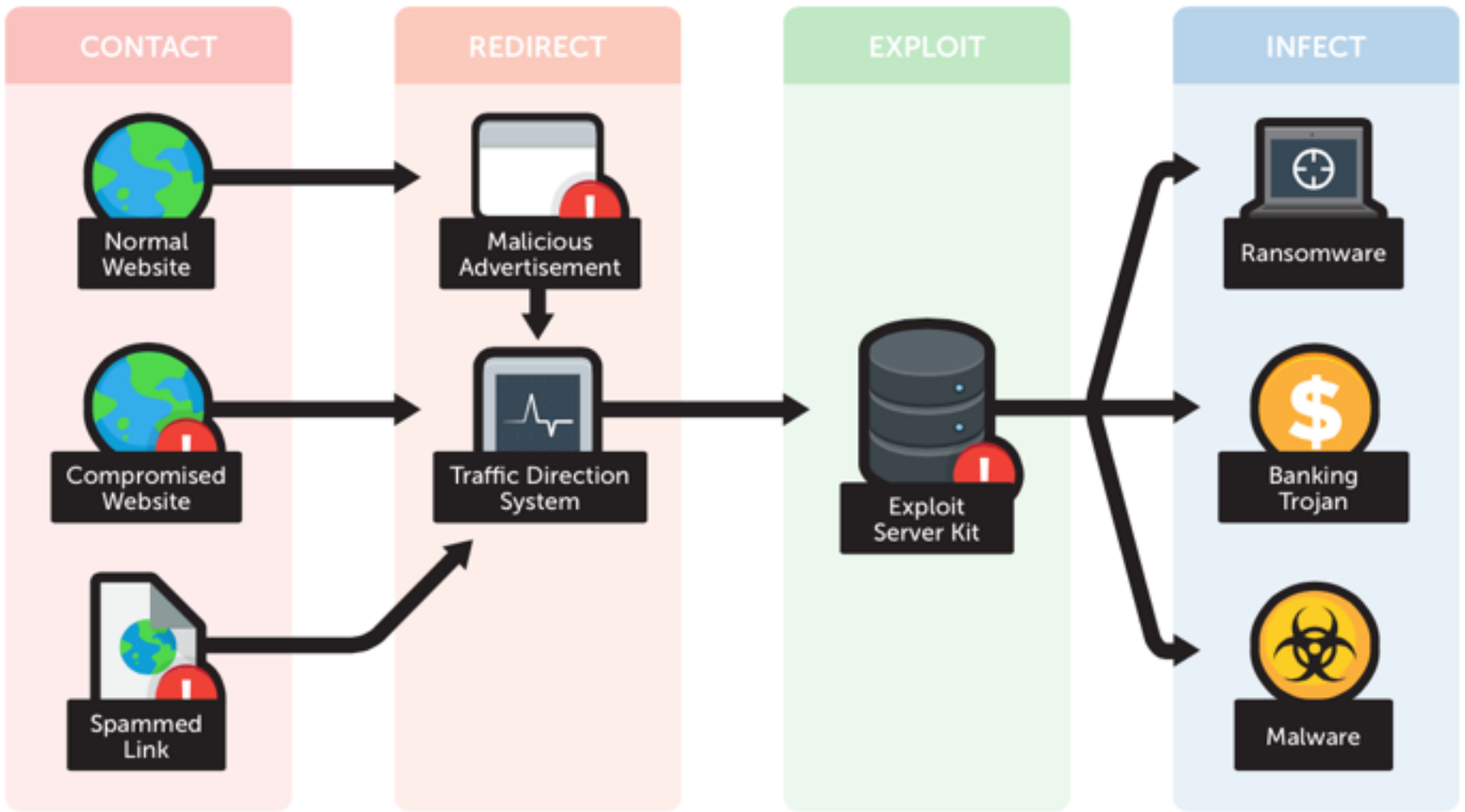
*Romain Wartel, CERN*

WLCG
Worldwide LHC Computing Grid

# Typically attack workflow

*"If we can get the target to visit us in some sort of Web browser, we can probably own them. The only limitation is 'how'." — Internal NSA memo*

## Mail, Web, App, or phone (SMS, call)




Malware framework + Malicious infrastructure

Entry point becomes pivoting point within organisation

Exfiltration tools
Remote access tools

*Source: Trend Micro*

"Click"

0-day

# Who? for-profit organisations

- Tools:
  - Commercial exploit kits
  - Known exploits and zero days
  - Large distributed malicious infrastructure
  - Global, 24x7 operations
  - Growing trend: memory-only


- Cashing out:
  - Interested in immediate profit
  - Data sold on dedicated underground markets
  - Stolen credit cards, money mules, etc.

- Example: Dridex, NewGoz, etc.

# Who? for-profit organisations


INTERPOL

"Organised international gangs are behind most internet scams and that cyber crime's estimated cost is more than that of cocaine, heroin and marijuana trafficking put together."

80% crime committed online is now connected to organised gangs operating across borders



*Interpol report from 2012*

WLCG Worldwide LHC Computing Grid
LCG

# Malware-as-a-service

Blackhole β | STATISTICS | THREADS | FILES | SECURITY | PREFERENCES | Logout

Adv: Selling Iframe traffic in a huge amount JID#1: buldozer790@jabber.ru icq#1: 609347060 JID#2: technicalsupport911@jabber.org icq#2: 622729573
Adv: IframeShop.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.

Start date: End date: Apply Autoupdate interval: **10 sec.**

**STATISTIC**

TOTAL INFO — 43605 HITED — 23249 HOSTS — 3273 LOADS — 14.08% LOADS

TODAY INFO — 32645 HITED — 18160 HOSTS — 2543 LOADS — 14.01% LOADS

| OS ↓ | HITS | HOSTS | LOADS | % |
|---|---|---|---|---|
| Windows 7 | 20162 | 10843 | 740 | 6.82 |
| Windows Vista | 1971 | 1160 | 206 | 17.76 |
| Windows XP | 21479 | 12256 | 2410 | 19.68 |

| EXPLOITS ↓ | LOADS | % |
|---|---|---|
| FLASH | 427 | 12.14 |
| HCP | 93 | 2.64 |
| JAVA SKYLINE | 168 | 4.78 |
| Java OBE | 1236 | 35.14 |
| Java SMB | 541 | 15.38 |
| MDAC | 65 | 1.85 |
| PDF ALL | 105 | 2.99 |
| PDF LIBTIFF | 882 | 25.08 |

| BROWSERS ↓ | HITS | HOSTS | LOADS | % |
|---|---|---|---|---|
| Firefox | 11552 | 7208 | 1099 | 15.26 |
| MSIE | 10963 | 5838 | 1119 | 19.17 |
| Opera | 21090 | 11477 | 1164 | 10.14 |

| COUNTRIES ↑ | HITS | HOSTS | LOADS | % |
|---|---|---|---|---|
| United States | 16 | 3 | 0 | 0.00 |
| Russian Federation | 43579 | 23243 | 3273 | 14.08 |
| Netherlands | 3 | 1 | 0 | 0.00 |
| Germany | 5 | 2 | 0 | 0.00 |

WLCG Worldwide LHC Computing Grid

# Malware-as-a-service

| | 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<br>CVE-2014-0322<br>CVE-2014-6332 | CVE-2013-2551<br>CVE-2013-3918<br>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<br>CVE-2014-0569 | CVE-2014-0515<br>CVE-2014-0569 | CVE-2013-0634<br>CVE-2014-0497<br>CVE-2014-0515<br>CVE-2014-0569 | CVE-2014-0569 | CVE-2014-0515<br>CVE-2014-0569 | CVE-2014-0515 | CVE-2014-0497<br>CVE-2014-0569 | CVE-2014-0515 |
| Adobe Acrobat/ Reader | CVE-2010-0188 | | | | | | CVE-2010-0188 | |
| Oracle Java | CVE-2012-0507 | | CVE-2013-2460<br>CVE-2013-2471 | | CVE-2013-2465 | | CVE-2012-0507 | |
| XMLDOM ActiveX | CVE-2013-7331 | | | CVE-2013-7331 | CVE-2013-7331 | | | CVE-2013-7331 |

# Who? State-sponsored (APT?)

- Tools:
  - Custom attacks, aiming at exfiltrate specific data
  - Multiple 0-Days (in-house)
  - Targeted social engineering
  - Small distributed malicious infrastructure
  - Operate mostly during working hours
  - Complex frameworks developed over the course of years (+ $ Millions)


- Cashing out:
  - Not interested in money
  - Attribution extremely difficult

- Example: Stuxnet, Duqu, Regin, APT3, etc.

# Who? for-profit organisations

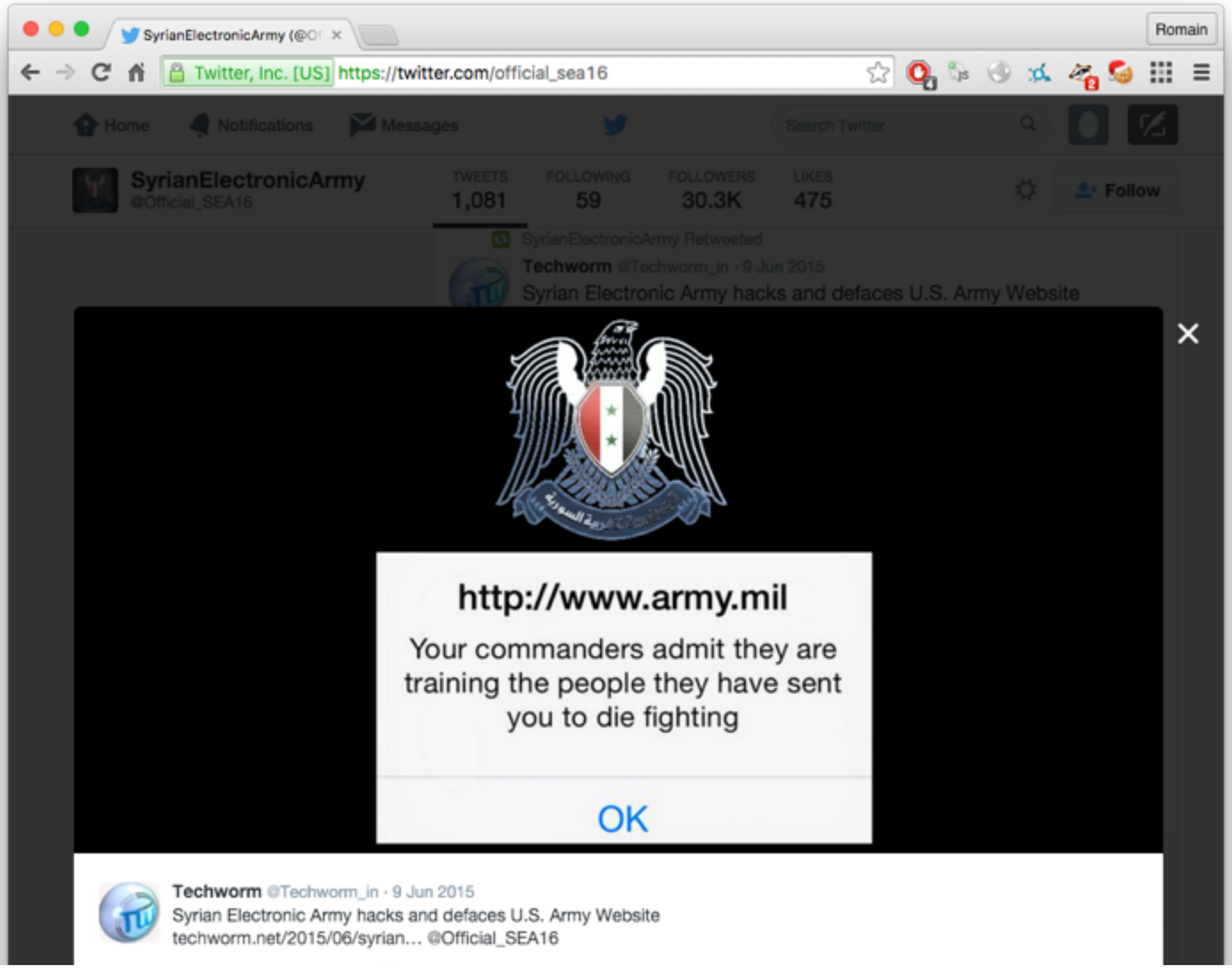
- Enable "deniable cyber operations" + outsource the work

- Tools:
  - Custom attacks, aiming at exfiltrate specific data
  - 0-Days (in-house or purchased)
  - Social engineering
  - Small distributed malicious infrastructure
  - Global, 24x7 operations

- Cashing out:
  - Few large private/government customers (cash, bank transfer)

- Usually try to keep a very low profile

# Hacktivists




- Goal:
  - Destruction for publicity
  - Concerns over SCADA capabilities

# Impact for grid and clouds

- Financial impact
  - Salaries, fraudulent transfert, fake invoices
    - Some cybercriminal organisations specialise in this (Dridex, etc.)
- Reputation or legal impact
  - Vendors/contractors and technologies developed locally: confidential/strategic documents, tenders, pricing, proprietary technologies or roadmap
- Employees
  - Medical information is worth more than credit cards
  - Personal information highly marketable
- Infrastructure damage (data centers, accelerator, etc.), SCADA
  - Accelerator complex, Computer Centre
  - Ukraine power blackout affecting 600,000 homes
- Concerns about malicious groups gaining SCADA capabilities
  - Goal: Disrupt and damage to get media visibility and create fear

# Response & strategy

- Treat security as a global issue
  - Invest in global trust frameworks
  - Including: operations, traceability, incident handling, policies
  - Contribute to global efforts against cybercrime
    - Focus on major threats that are known to cause significant damage (Dridex, etc.)
- Shift security emphasis from services to people
  - Next big breach likely via phishing, unlikely via SSH/grid 0-day

- Involve security vendors in monitoring/incidents/forensics
- Obtain indicators of compromise (threat intelligence)
  - Establish a solid network of security contacts?
  - Outsource and hire a security vendor (jointly or alone)?
  - Build the technical means to use them (SoC infrastructure, storage, etc.)
- Involve law enforcement for serious breaches
  - Attackers rarely decide they have had enough data/money…
- Continue to raise the bar
  - Make it as difficult and expensive possible to break-in

# Raising the bar

- 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

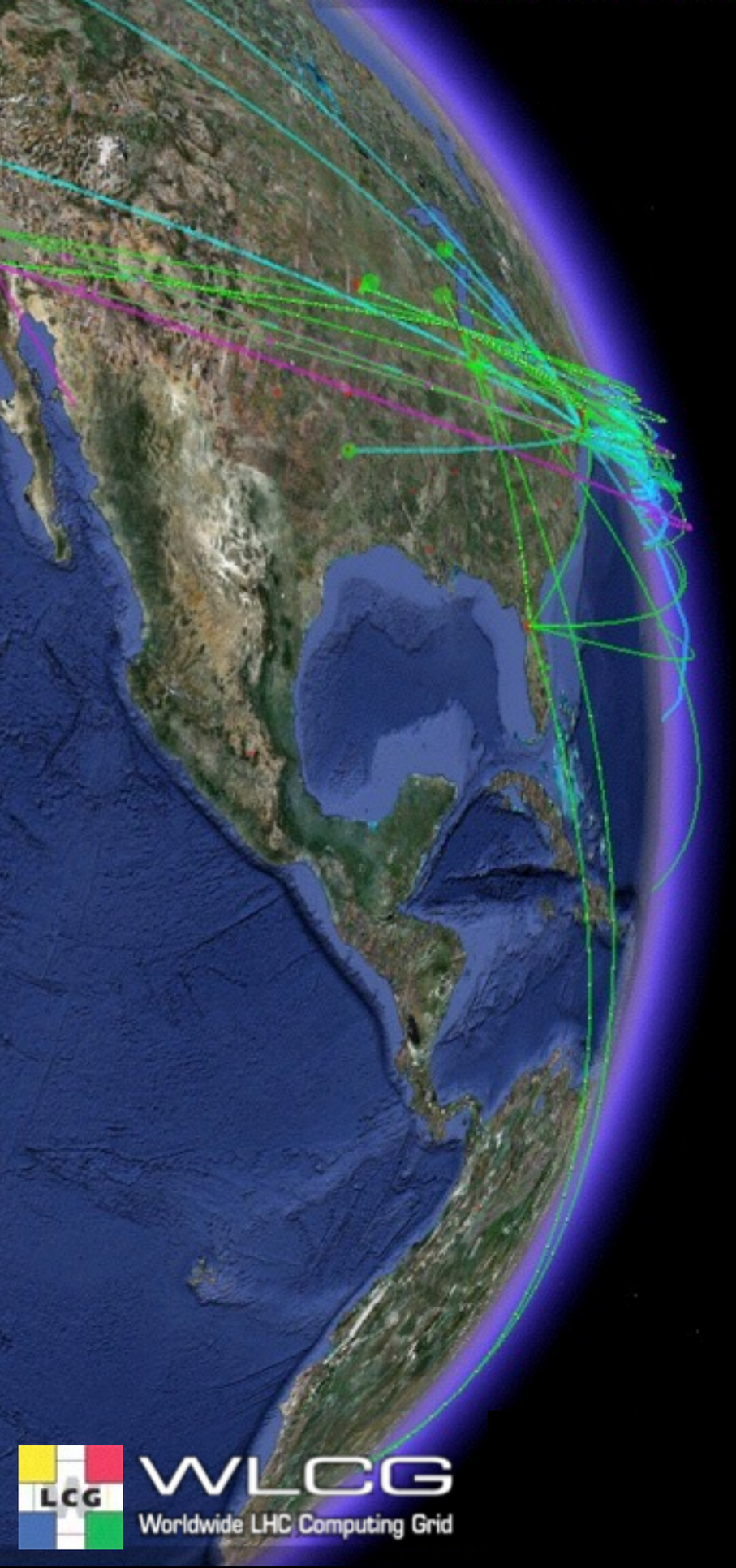
# Getting “80%” protected

- 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
  - 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

# Questions?


WLCG
Worldwide LHC Computing Grid