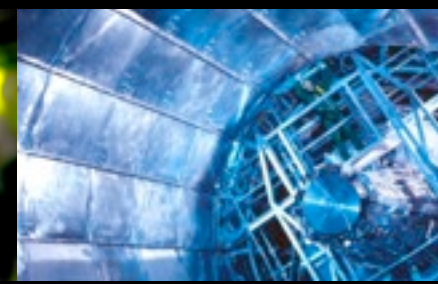
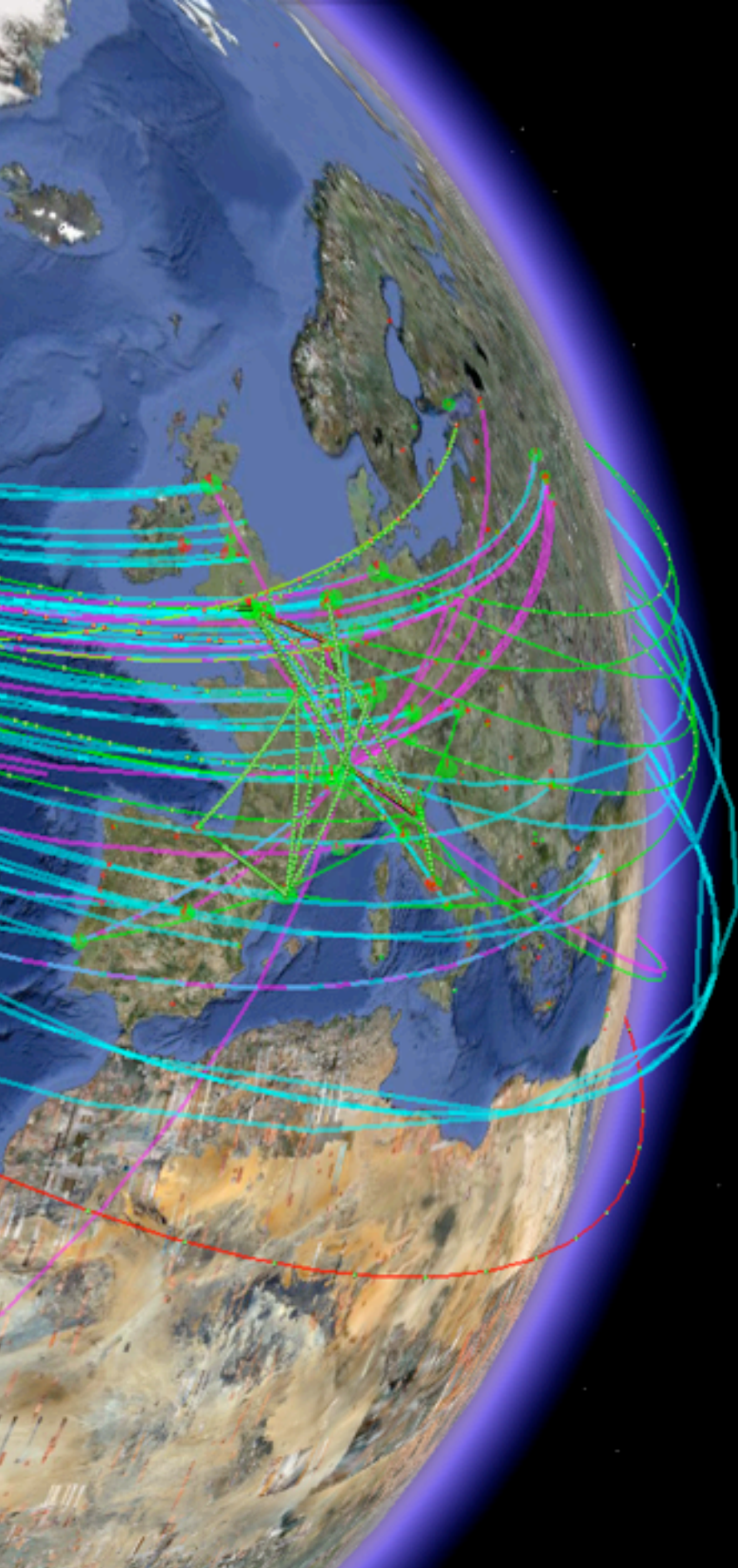


Security update

Romain Wartel





Why would someone
attack our services?



Underground market

- Main motive behind most security attacks remains **money**.

Overall Rank 2009	2008	Item	Percentage		Range of Prices
			2009	2008	
1	1	Credit card information	19%	32%	\$0.85-\$30
2	2	Bank account credentials	19%	19%	\$15-\$850
3	3	Email accounts	7%	5%	\$1-\$20
4	4	Email addresses	7%	5%	\$1.70/MB-\$15/MB
5	9	Shell scripts	6%	3%	\$2-\$5
6	6	Full identities	5%	4%	\$0.70-\$20
7	13	Credit card dumps	5%	2%	\$4-\$150
8	7	Mailers	4%	3%	\$4-\$10
9	8	Cash-out services	4%	3%	\$0-\$600 plus 50%-60%
10	12	Website administration credentials	4%	3%	\$2-\$30

Goods and services advertised on underground economy servers

Source: Symantec

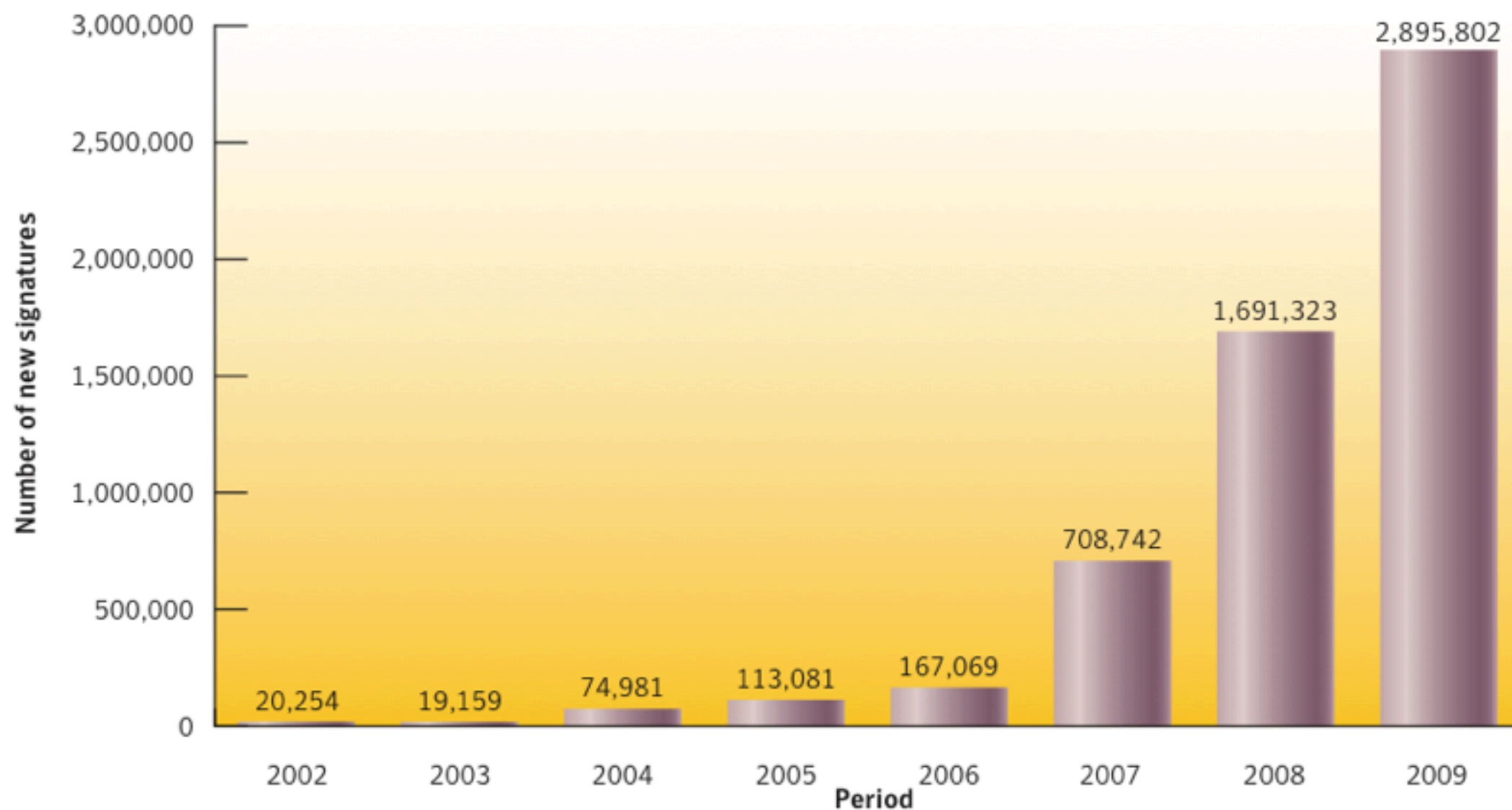


(and sometimes **hacktivism**, more rarely challenge/ego.)



Security incidents - motivation

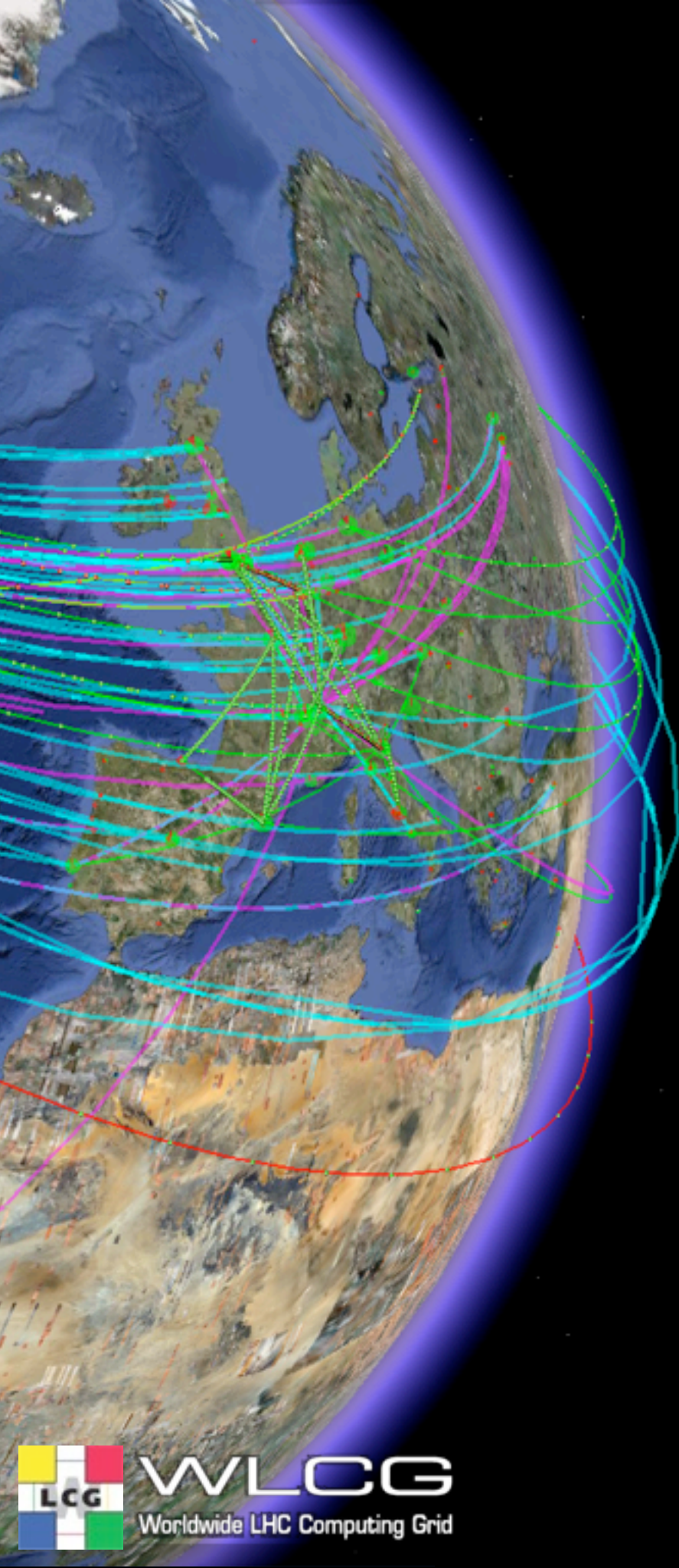
- Real business - **sophisticated** and **targeted** attacks
 - Several security vendors identified more malware in 2009 than in the last 20 years altogether



New malicious code signatures

Source: Symantec.

- How can writing malware or send spam be tied with real money?



How does this work?

Exploits, payload and
propagation infrastructure

*(or: how to make money with
little/no risk of being caught?)*



Exploits

- Exploit: software exploiting a security vulnerability
 - Objective: gain (some) remote control over the victim's host
 - Exploits can be purchased on the underground markets
 - Public/private vulnerabilities
 - “0 day exploits” are best but most expensive
 - Some claim there are governments willing to pay as high as \$1 million for a single vulnerability
 - Potential impact, privileges gained, portability, ease of use

Rank	BID	Vulnerabilities
1	36299	Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution
2	35759	Adobe Reader and Flash Player Remote Code Execution
3	33627	Microsoft Internet Explorer 7 Uninitialized Memory Code Execution
4	35558	Microsoft Windows 'MPEG2TuneRequest' ActiveX Control Remote Code Execution
5	34169	Adobe Reader Collab 'getIcon()' JavaScript Method Remote Code Execution

Top attacked vulnerabilities, 2009

Source: Symantec

- Once the attacker has an exploit, a payload needs to be added



Malicious Payload

- The payload performs the malicious work
 - Objectives:
 - Alter system's behavior
 - e.g. add popups, fake search bars, send spam with host is idle, etc.
 - Collect data without the consent of the victim
 - e.g. keylogger
 - The payload may be a framework multiple purposes:
 - Dynamically pull payload on demand
 - Auto update mechanisms built-in
 - Eliminate competitors' "products"
 - Patch the system to protect it from competitors



Propagation Infrastructure

- To propagate the malware to more victims, a strong computing infrastructure is need:
 - **Hosting** for the malicious payloads, rogue websites, etc.
 - **Bandwidth** to send spam, etc.
- Significant challenges
 - Must be very **resilient**!
 - Must **scale** to the number of victims
 - Must be **customisable** to adapt to the needs of customers
 - Must be **cheap**, to maximise profit





Propagation Infrastructure

- Solution 1
 - Enjoy existing services widely used by the victims:
 - P2P networks (“Bond_23_Unreleased_2011_[HDRips.4.iPod]”)
 - Social networks: Facebook, Twitter, MySpace, etc.
 - Inject malware via ads on large websites (BBC, etc.)

The image shows a composite of two screenshots. The left screenshot is a Twitter search results page for the query "Gulf oil ipad". It displays several tweets from users like @Danieltesfayee1, @alishamadison, @wbcom, @Call_m3h_WavY, @aVhD75, @Call_m3h_WavY, and @aVhD75, all offering a free iPad in exchange for an email address. The right screenshot is a Facebook profile page showing a "Some Errors Occured In Your Profile!" message. The message states: "Please activate this application to check out and correct the errors." and includes an "Activate" button. The Facebook navigation bar shows "Home", "Profile", "Friends", "Inbox", and "1203".



Propagation Infrastructure

- Solution 2
 - Become the Internet Service Provider:
 - Much more difficult to be taken off line, “bulletproof hosting”
 - Manage its own pool of IP addresses
 - Accreditation removal may be complex and time consuming
 - Legal complexity ensures stable operations (for a while)
 - ISP may be settled in countries with relaxed Internet laws
 - International ramification does help
 - Sell the service to other underground companies
 - Actual crime is not committed by the ISP itself
 - Popular examples:
 - <http://en.wikipedia.org/wiki/Intercage>
 - http://en.wikipedia.org/wiki/Russian_Business_Network



Propagation Infrastructure

- Solution 3

- **Get the victims to host** and spread the malware!
 - Cheap, highly distributed and **resilient**
 - Build a own network of robots, a so-called “**botnet**”
 - The victim hosts are controls by malware and **turned into "bots"**
 - Payload and malicious services are distributed across the botnet
 - Control via IRC, P2P, etc.
- “**Fast Flux**” is a common design to turn bots (victims) into:
 - Rogue DNS servers
 - Reverse proxies for rogue websites
 - Malicious domains needed to run the infrastructure
- Bots are “selected” to offer a load-balanced + resilient service:
 - Selection based on availability, bandwidth, performance, etc.
 - Short time-to-live, rapid turn over of the bots

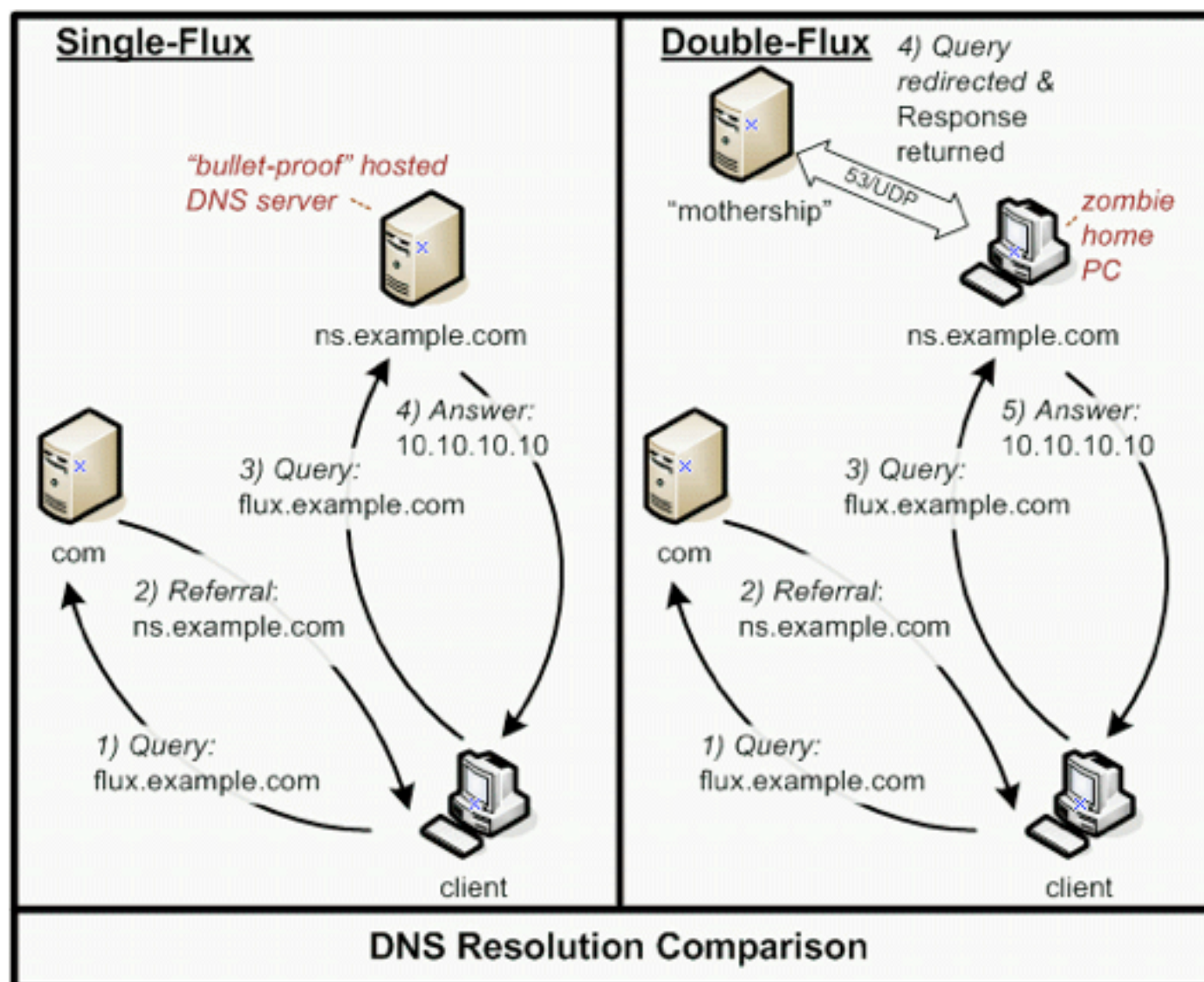


Propagation Infrastructure

- Solution 3

- Fast Flux:

- “Both the DNS A record sets and the authoritative NS records for a malicious domain are continually changed in a round robin manner”



<http://www.honeynet.org/papers/ff/>



Propagation Infrastructure

- Solution 3

- Example of Fast Flux tracking with Zeus:

- http://en.wikipedia.org/wiki/Zeus_%28trojan_horse%29
 - The Zeus botnet is targeting login credentials
 - Facebook, Yahoo, Hi5, Metroflog, Sonico and Netlog etc.
 - Targeting banking sites as well
 - The botnet is estimated to include millions of compromised computers
 - As of October 28, 2009 Zeus has sent out over 1.5 million phishing messages on Facebook.
 - On September 29, 2010, 19 people were arrested in the UK:
“The gang - hoping to evade suspicion - opened scores of “drop” bank accounts in various banks and used money mules to collect the stolen money. It is believed that they have stolen around £6 million in some three months, and possibly even more.”

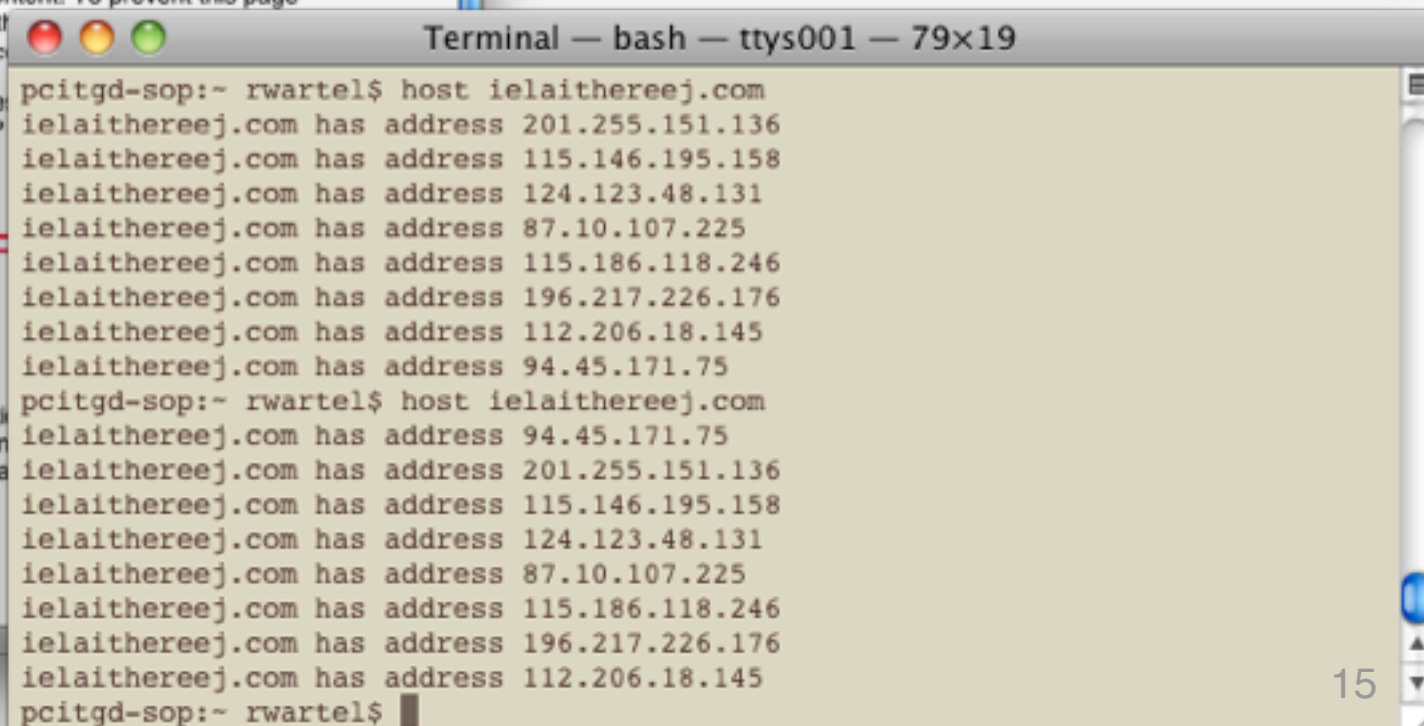


Propagation Infrastructure

- Solution 3

- Example malicious URLs:

- <http://ielaithereej.com/bin/aiphaipi.bin> (Zeus v2 + config file)
 - Where is this host?





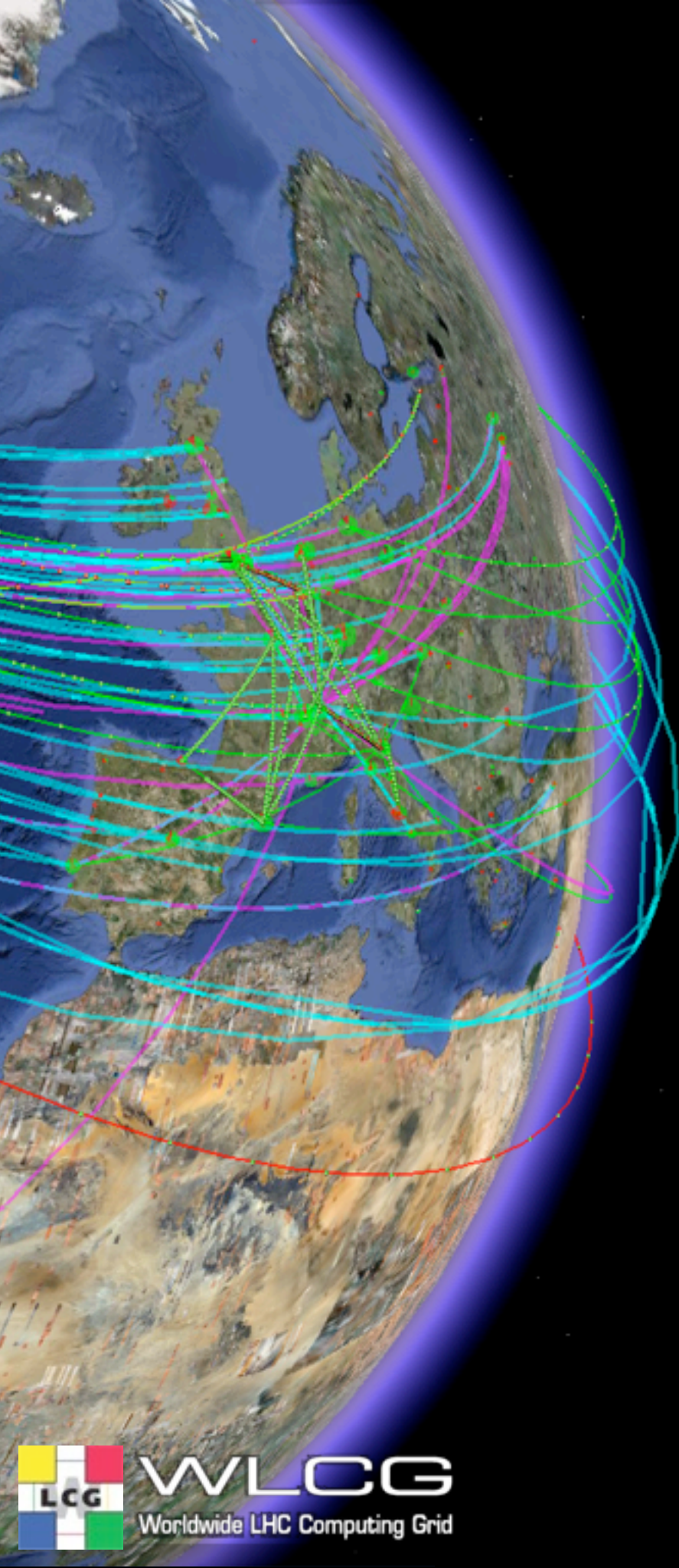
Propagation Infrastructure

- Solution 3
 - Example of Fast Flux tracking:

The 40 newest bots assigned to the domain ielaithereej.com:

Domain	Dateadded (UTC)	IP address	Hostname	AS number	Country	Counter
ielaitheereej.com	2010-05-27 16:11:14	85.175.99.10		25490		16
ielaitheereej.com	2010-05-27 16:11:13	82.131.233.62	82.131.233.62.pool.invitel.hu	12301		19
ielaitheereej.com	2010-05-27 16:11:13	121.121.34.46		9534		15
ielaitheereej.com	2010-05-27 16:11:13	178.160.84.39		35648		22
ielaitheereej.com	2010-05-27 16:06:15	201.238.58.150		8048		68
ielaitheereej.com	2010-05-27 16:06:09	79.114.224.60	79-114-224-60.rdsnet.ro	8708		72
ielaitheereej.com	2010-05-27 15:56:12	186.99.182.172		27921		34
ielaitheereej.com	2010-05-27 15:56:11	85.96.154.90	dsl.dynamic859615490.ttnet.net.tr	9121		33
ielaitheereej.com	2010-05-27 15:56:11	87.10.107.225	host225-107-dynamic.10-87-r.retail.telecomitalia.i	3269		59
ielaitheereej.com	2010-05-27 15:51:57	95.75.120.214		16232		17
ielaitheereej.com	2010-05-27 15:51:20	117.194.160.254		9829		108
ielaitheereej.com	2010-05-27 15:51:20	82.131.227.213	82.131.227.213.pool.invitel.hu	12301		19
ielaitheereej.com	2010-05-27 15:46:31	92.41.90.213	92.41.90.213.sub.mbb.three.co.uk	21327		137
ielaitheereej.com	2010-05-27 15:46:21	94.232.121.253	ppp-94.232.121.253.dobroe.ru	42322		142

<http://dnsbl.abuse.ch/fastfluxtracker.php>



How does this work?

Popular for-profit malware



Malware business

- Malware infrastructure has become more sophisticated:
 - **Malicious software developers**: provide exploits and tools
 - **Bot herders**: maintain and rent the bot infrastructure
 - **Money mules**: turn “dirty” money into real currencies
 - Malware hosting, etc.
 - Coordination via Internet forums, IRC, IM, etc.
- A closer look on the actual tools
 - **Easy** to use
 - Enable **automated** attacks
 - Very **sophisticated**





Malware

- Modern malware can be convenient and easy to use

```
Terminal — ssh — ttys000 — 97x33

/bin/truc:      file format elf64-x86-64

Disassembly of section .interp:

0000000000400200 <.interp>:
400200:      2f                (bad)
400201:      6c                insb    (%dx),%es:(%rdi)
400202:      69 62 36 34 2f 6c 64 imul    $0x646c2f34,0x36(%rdx),%esp
400209:      2d 6c 69 6e 75    sub     $0x756e696c,%eax
40020e:      78 2d             js      40023d <__cxa_atexit@plt-0xaf3>
400210:      78 38             js      40024a <__cxa_atexit@plt-0xae6>
400212:      36               ss
400213:      2d 36 34 2e 73    sub     $0x732e3436,%eax
400218:      6f               outsl   %ds:(%rsi),(%dx)
400219:      2e 32 00         xor     %es:(%rax),%al

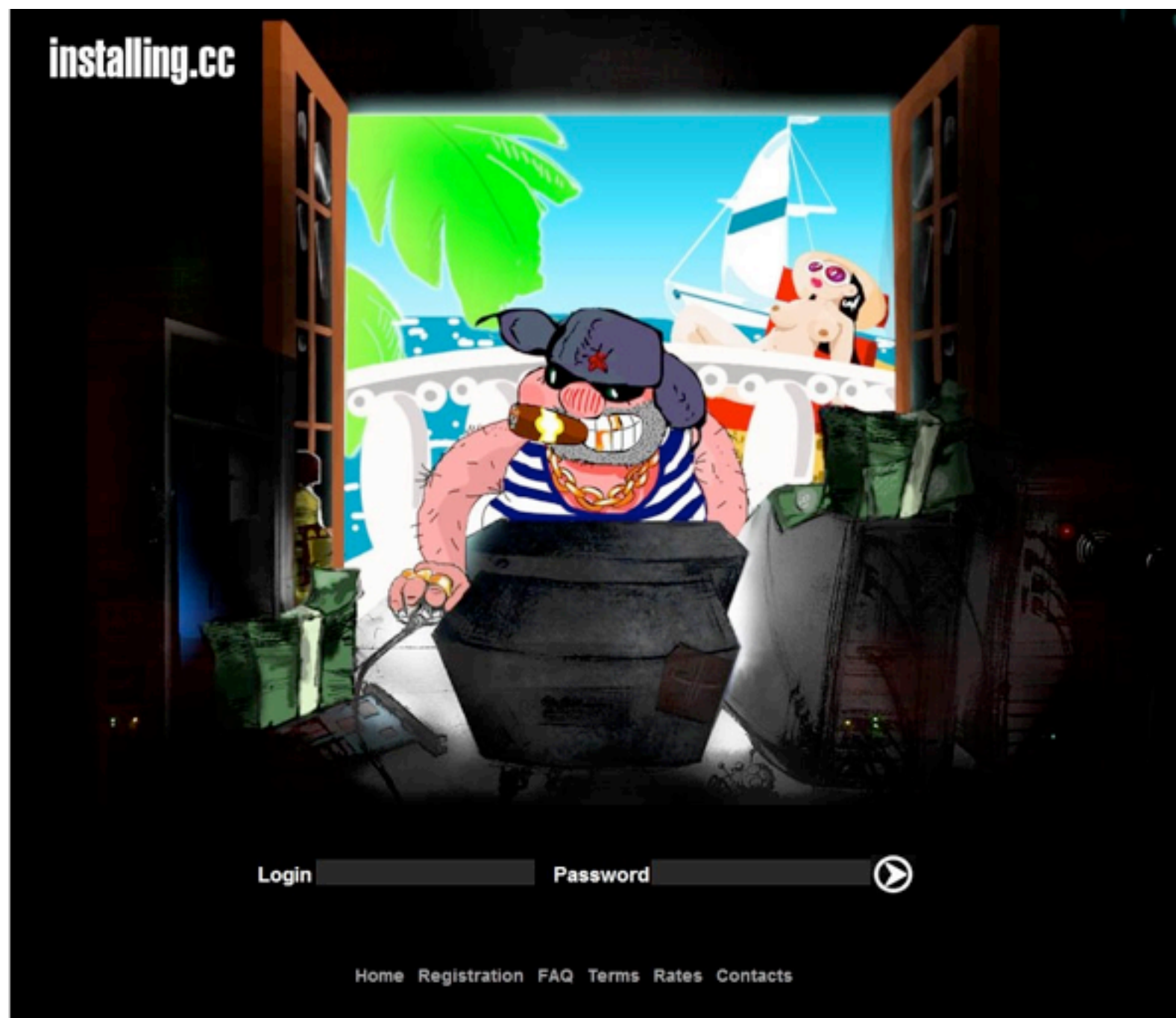
Disassembly of section .note.ABI-tag:

000000000040021c <.note.ABI-tag>:
40021c:      04 00             add     $0x0,%al
40021e:      00 00             add     %al,(%rax)
400220:      10 00             adc     %al,(%rax)
400222:      00 00             add     %al,(%rax)
400224:      01 00             add     %eax,(%rax)
400226:      00 00             add     %al,(%rax)
400228:      47               rexXYZ
400229:      4e 55             rex64XY push  %rbp
40022b:      00 00             add     %al,(%rax)
40022d:      00 00             add     %al,(%rax)
40022f:      00 02             add     %al,(%rdx)
400231:      00 00             add     %al,(%rax)
400233:      00 04 00         add     %al,(%rax,%rax,1)
```



Malware interfaces

- Modern malware can be convenient and easy to use



Zeus botnet rental and loading



Malware

- Modern malware can be convenient and easy to use

The screenshot shows the FRAGUS botnet control interface. At the top left is the FRAGUS logo, a triangle with a chain. To the right is a navigation bar with links: Statistics | Files | Sellers | Traffic links | Preferences | Logout. On the left side, under 'Total statistics:', there is a checkbox for 'Ajax autoreload' and three statistics: Hosts: 94, Frags: 22, and Percentage: 23.4%. The main area contains an 'Add file' section with three input fields for 'File description:', 'File name (for loading to victim *.exe)', and 'Uploading file:'. There is an 'Add' button and a button labeled 'Обзор...' next to the 'Uploading file:' field. Below this is a 'Files list:' section with a table. The table has columns for 'File description', 'File name', 'Frag', 'Feedbacks', and 'Percentage feedbacks'. The first row shows 'Testinge' as the description, 'updater.exe' as the file name, '22' as the frag count, '14' as the feedback count, and '63.64%' as the percentage feedback. There are 'edit' and 'delete' buttons for each row.

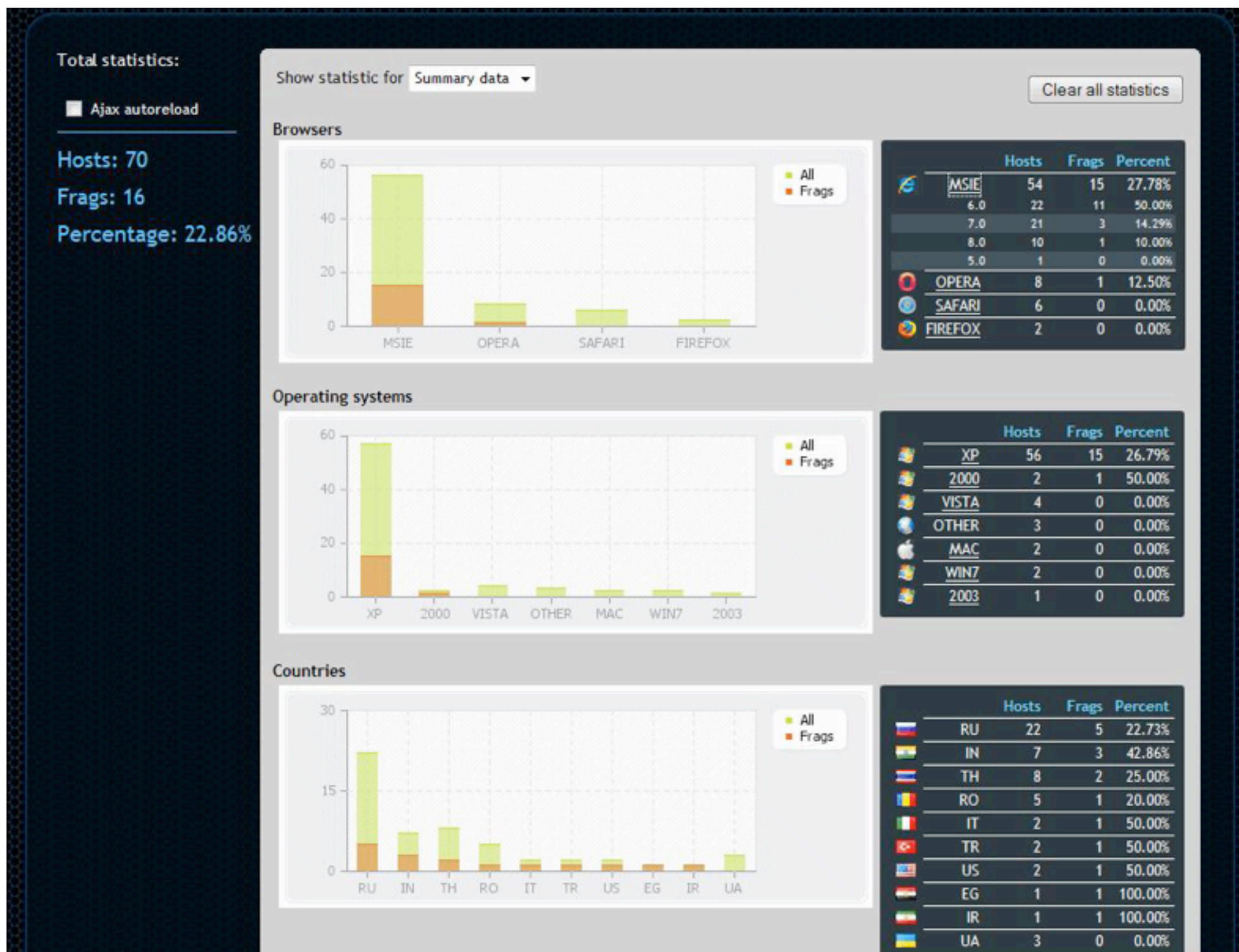
File description	File name	Frag	Feedbacks	Percentage feedbacks
edit delete Testinge	updater.exe	22	14	63.64%

Fragus botnet rental and loading



Malware

- Modern malware can be convenient and easy to use





Malware

- Modern malware can be convenient and easy to use

[\[global statistic\]](#)

[\[country statistic\]](#)

[\[thread statistic\]](#)

[\[referrer statistic\]](#)

[\[advanced statistic\]](#)

[\[time statistic\]](#)

[\[reset statistic\]](#)

[\[pack statistic\]](#)

[\[manage threads\]](#)

[\[manage loaders\]](#)

[\[global options\]](#)

[\[lucky manual\]](#)

id	Thread name	Description	Exe	Status	Link	
1	default	Default system thread	1	enabled	http://localhost:8080/main/?t=1	edit delete show stat disable pack stat clear stat
2	chicken	Default chicken thread	1	enabled	http://localhost:8080/main/?t=2	edit delete show stat disable pack stat clear stat
3	semen	hh	3	enabled	http://localhost:8080/main/?t=3	edit delete show stat disable pack stat clear stat
5	zalup	17	1	enabled	http://localhost:8080/main/?t=5	edit delete show stat disable pack stat clear stat
6	all	buda	3	enabled	http://localhost:8080/main/?t=6	edit delete show stat disable pack stat clear stat
<input type="text"/> <input type="text"/>				on/off <input type="radio"/>	Create new thread (options from default thread)	

ZeuEsta 7.0 Administration Panel

Exploit Stats

mdac xml pdf snap op9 embed
0 0 0 0 0

Bot Stats

CP :: Summary statistics

Information:
Current user: admin
GMT date: 10.07.2009
GMT time: 00:09:11

Statistics:
→ Summary
OS

Botnet:

Information

Total reports in database:	0
Time of first activity:	-
Total bots:	0
Total active bots in 24 hours:	0% - 0
Minimal version of bot:	0.0.0.0
Maximal version of bot:	0.0.0.0



Malware

- Modern malware can be convenient and easy to use

Spy Eye v1.0

2009 12/28 22:35:20

Find INFO Statistic Settings

3646 k +54882

Get \$tati\$tic

Get hosts

Day for statistic : 28/12/2009

Limit : 100

submit

host	count	[controls]
www.google.com	1021	⊗
		⊗
		⊗
		⊗
		⊗
		⊗
		⊗
		⊗
		⊗
www.delmarlearning.com	431	⊗
mc.yandex.ru	427	⊗
classic.ben.ru	342	⊗

Страница на http://www.microsoft-windows-security.com co...

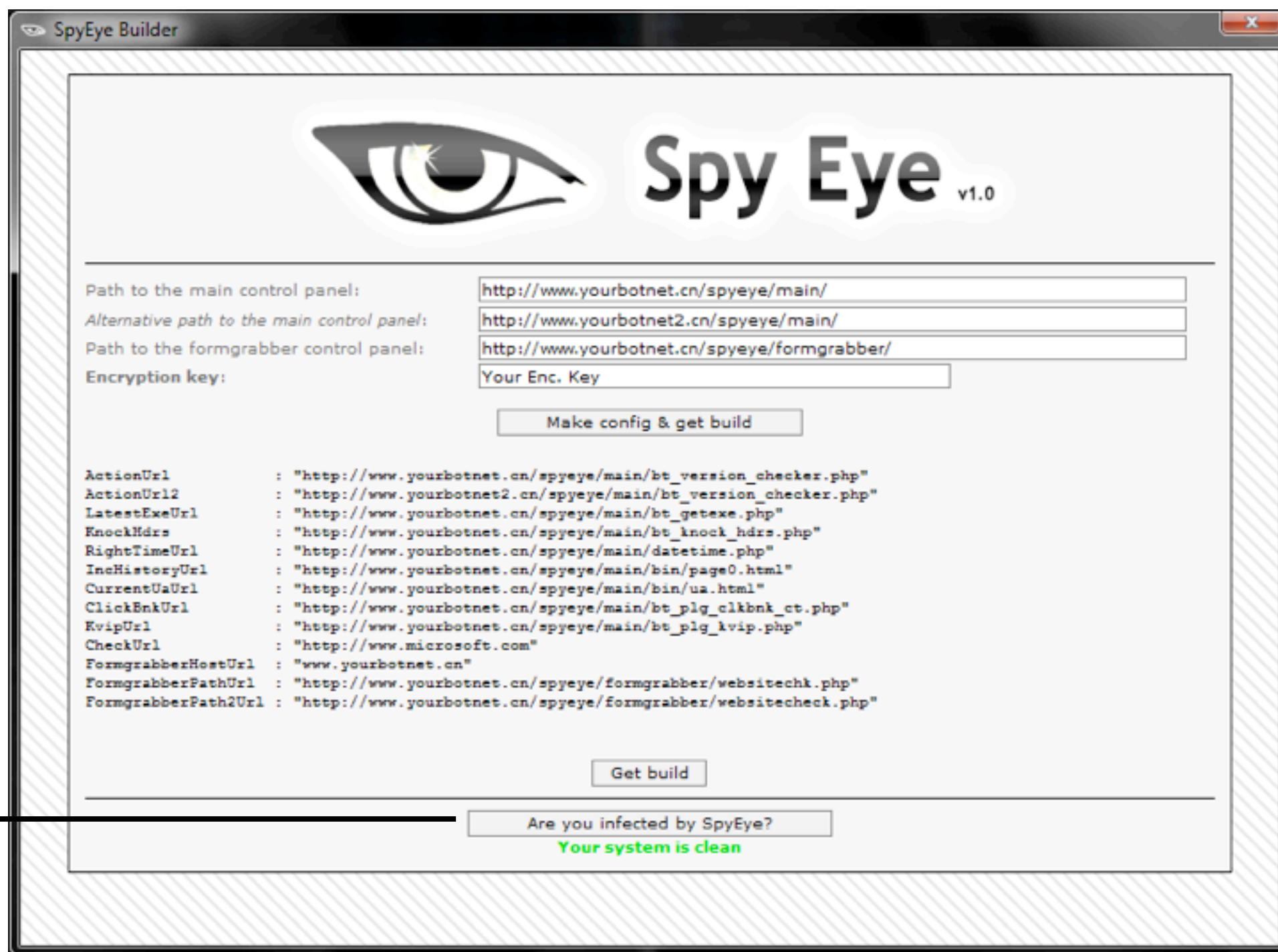
Do you really want to ban this host (www.google.com) ?

OK Отмена



Malware

- Modern malware can be convenient and easy to use



Don't get infected by your own malware



Malware

- Modern malware can be convenient and easy to use






Malware

- Modern malware can be convenient and easy to use

SpyEye Builder v1.0.7



Spy Eye v1.0

Path to the main control panel:

Alternative path to the main control panel:

Path to the formgrabber control panel:

Encryption key:

Connector interval (sec):

Compress build by UPX v3.04w: ☐

Kill Zeus: ☒

Kill
competitors
easily



Malware

- Modern malware can be convenient and easy to use



A botnet control screen featuring a Christmas theme



Malware

- Modern malware can be convenient and easy to use
 - Neon Exploit System v2.0.5 (\$ 400)
 - “Among the modules of exploits that are preinstalled and preconfigured include: IE7 MC, PDF collab, PDF util.printf, PDF foxit reader, MDAC, Snapshot and Flash 9.”
 - Eleonore Exploits Pack v1.2 (\$ 700 - \$ 1500)
 - “MDAC, MS009-02, Telnet - Opera, Font tags - FireFox, PDF collab.getIcon, PDF Util.Printf, PDF collab.collectEmailInfo, DirectX DirectShow and Spreadsheet.”
 - Limbo Trojan Kit (\$ 300)
 - ElFiesta v3 (\$ 800)
 - Unique Sploits Pack v2.1 (\$ 750)
 - YES Exploit System v2.0.1 (\$800) etc.





Rootkits

- A lookout at the state of Linux rootkits
 - Rootkit: “Designed to **hide** or obscure the fact that a system has been compromised.” (Wikipedia)
 - Software used to maintain malicious access to a compromised host
- Rootkit: first generation
 - **Change binaries** (ps, ls, netstat, lsof, ssh) or libraries (ld.so.preload, etc.)
 - *Pros*: kernel independent
 - *Cons*: need to be compiled for the target platform, easy to detect
 - *How to detect*: check system binaries against trusted instances
 - Tripwire, rpm -V, etc.





Rootkits

- Rootkit: second generation
 - Kernel level rootkits
 - Modify kernel structures (syscall table, IDT, etc.)
 - Malicious codes is loaded directly in the kernel
 - Loadable Kernel Modules
 - Direct /dev/mem access (patch kernel **on-the-fly**)
 - *Pros*: difficult to detect, usually includes backdoor features
 - *Cons*: LKM can be disabled, /dev/{k,}mem access now restricted
 - *How to detect*: search for known patterns, or known bugs.
 - rkhunter, chkrootkit, Samhain, etc.



Rootkits

- Rootkit: new trends
 - Filesystem, network stack level rootkits
 - Often used as additional features
 - Hypervisor rootkit
 - Debug register based rootkit
 - Already seen in the wild early 2010...

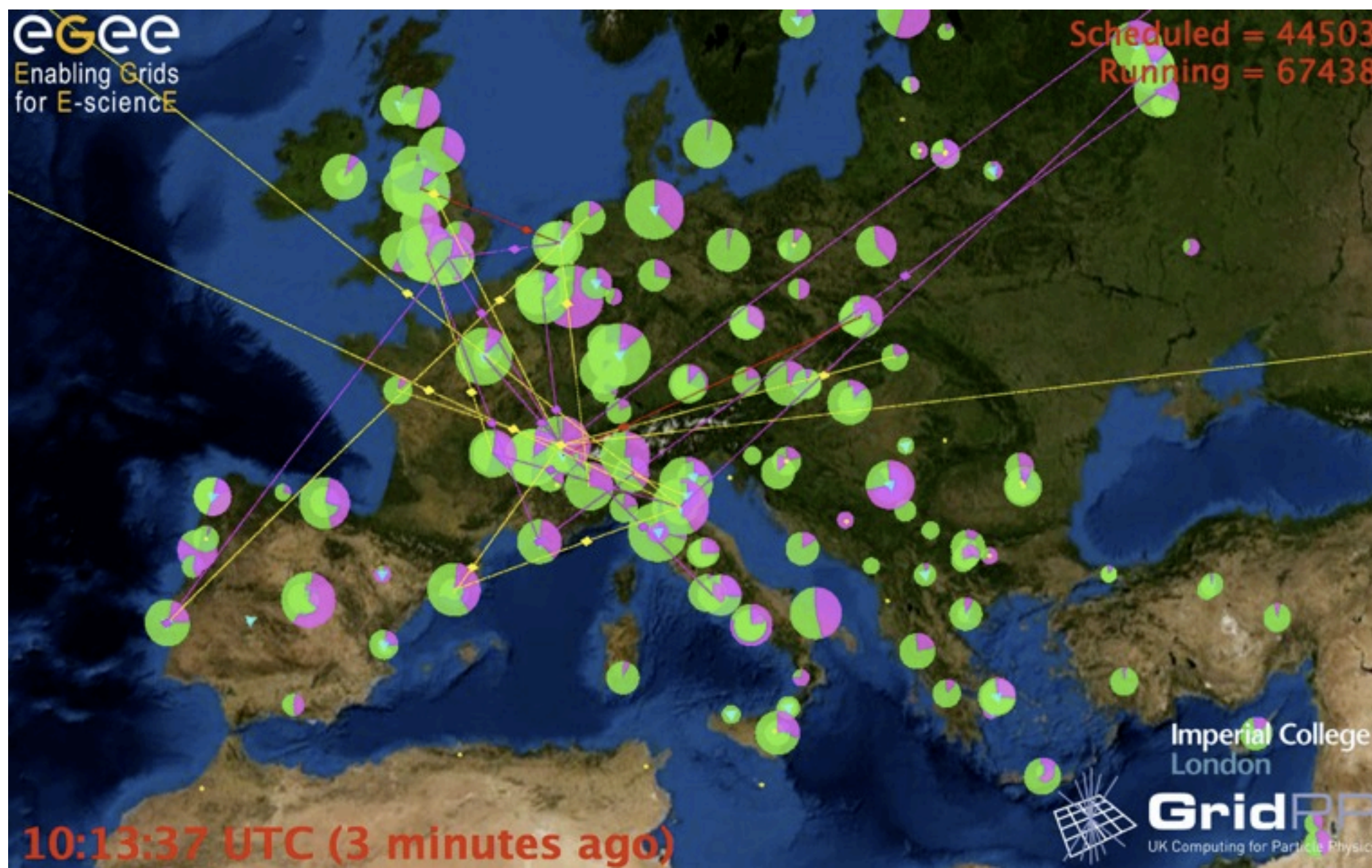


What is the impact of grid
computing?



Grids are valuable assets

- Grids are valuable to attackers
 - Large numbers of **distributed** hosts
 - **High availability**
 - **High throughput** network





Impact of grid computing over security?

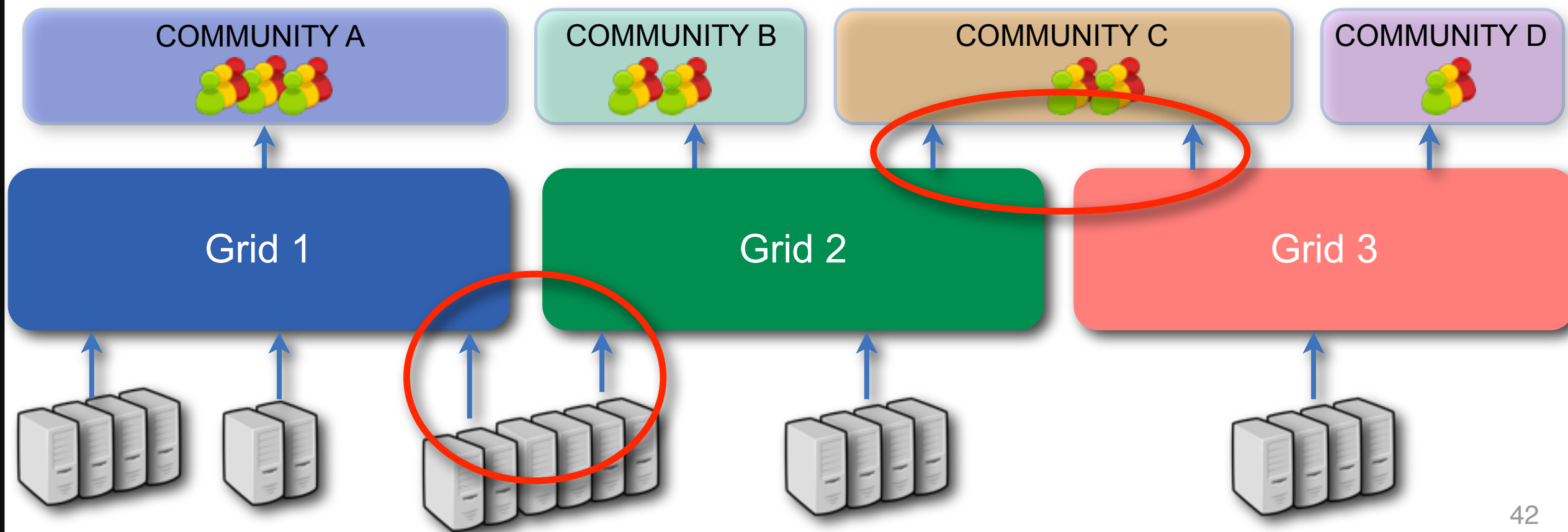
- Significant **increase in collaboration** between organizations
 - Shared users
 - Attack propagation across different sites
 - Shared resources
 - a user compromise may affect other users
 - Transparent access
 - a malicious user can transparently run malicious code across different sites

```
Terminal — ssh — ttys000 — 79x6
ssh
-bash-3.00$ id
uid=22498(rwartel) gid=2648(gr) groups=2648(gr),1096929749
-bash-3.00$
-bash-3.00$ globus-job-run lcgce02.gridpp.rl.ac.uk /usr/bin/id
uid=36346(dteam047) gid=24311(dteam)
-bash-3.00$
```




Impact of grid computing over security?

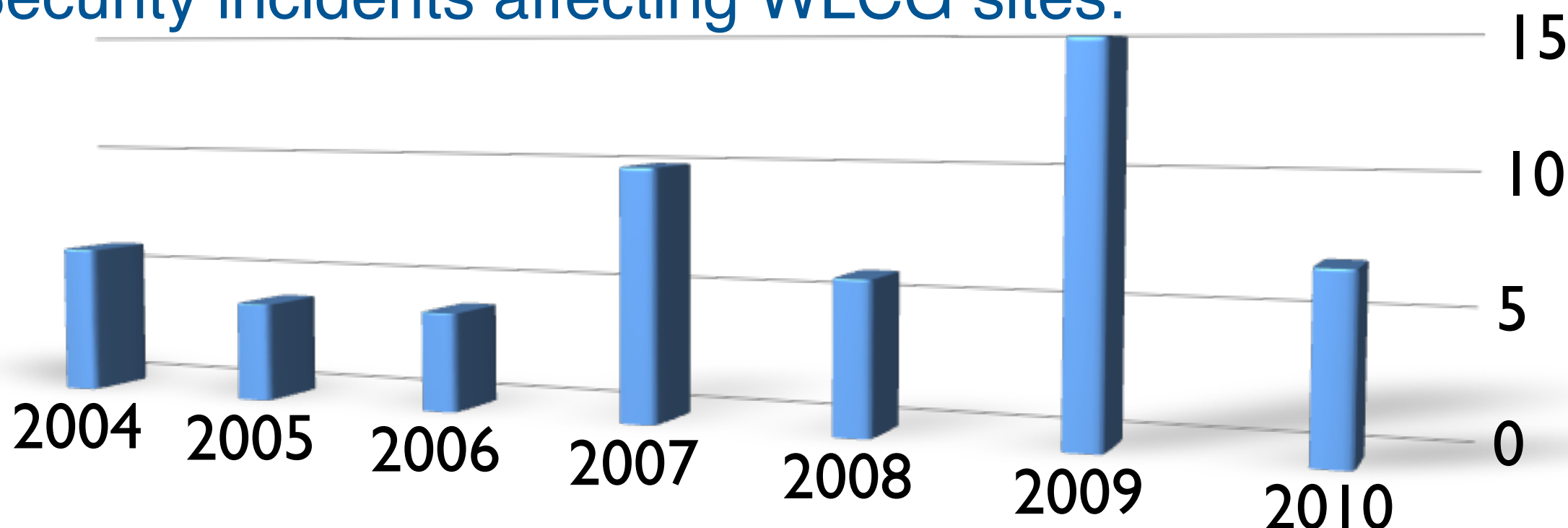
- The grid - an ideal incident propagation vector?
 - Grid resource providers may share their resources across different unrelated grids and **user communities**
 - Different grids may provide services to the same community





Impact of grid computing over security?

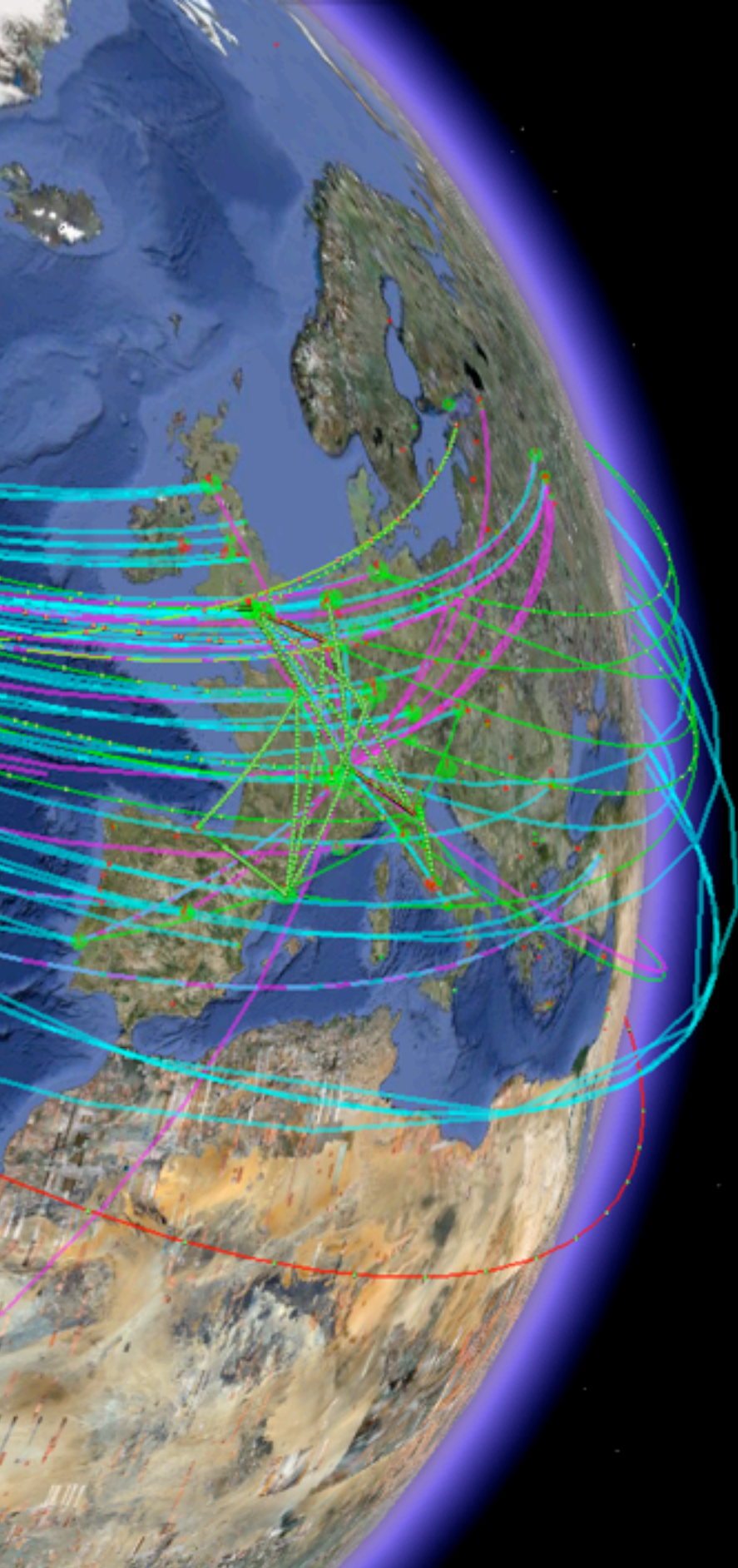
- Security incidents affecting WLCG sites:



- How many of these incidents were caused by the grid itself?

NONE

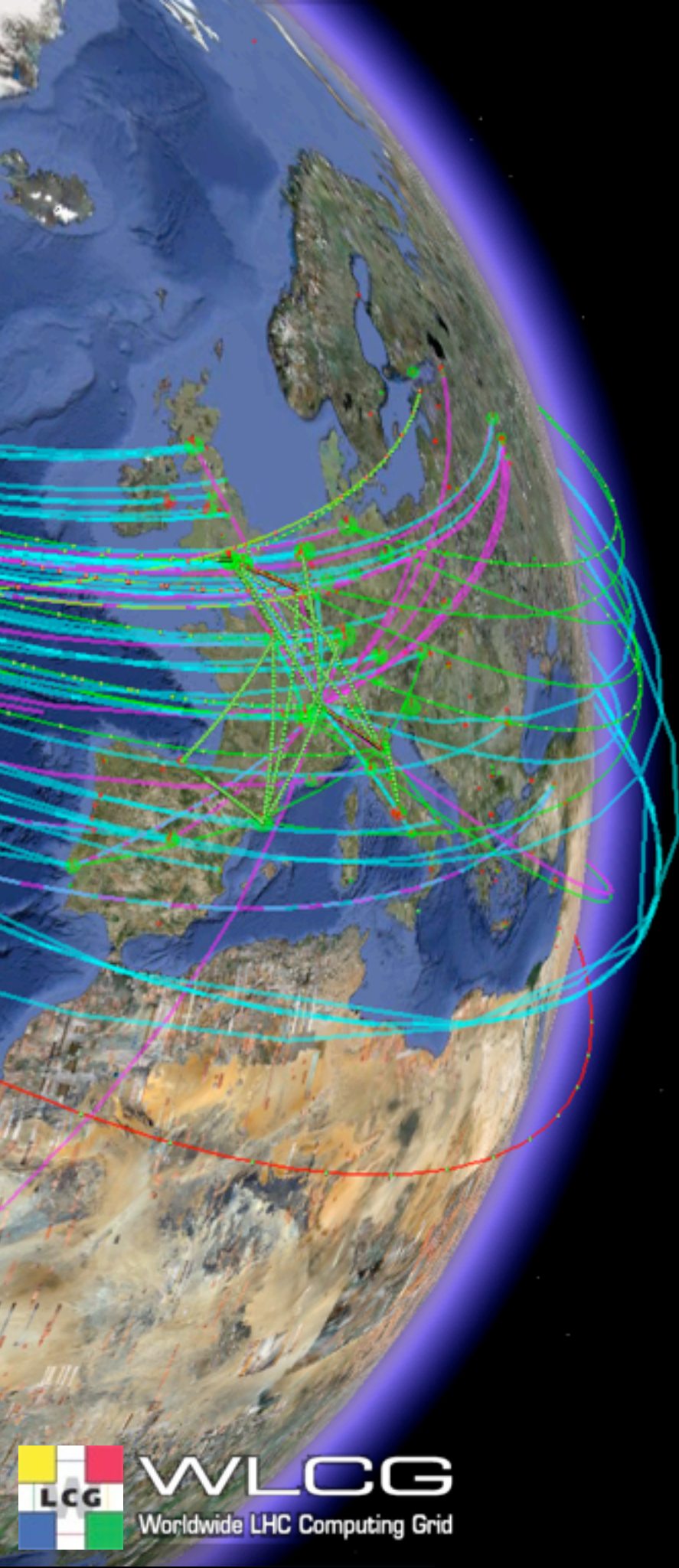
- All these incidents were **standard site security issues**
- However, the grid sites:
 - Could share information to **detect and prevent these incidents**
 - Could work together to **help the unexperienced sites**
 - Could collaborate to **resolve these incidents**
- The grid helped re-enforcing academic security**



What are the most common
causes of grid security
incidents?

Main causes of security incidents

- Compromised user accounts at other sites (SSH)
- Vulnerable Web applications
- Failure to apply security patches
- Weak passwords in some cases → **Training**



Main causes of security incidents

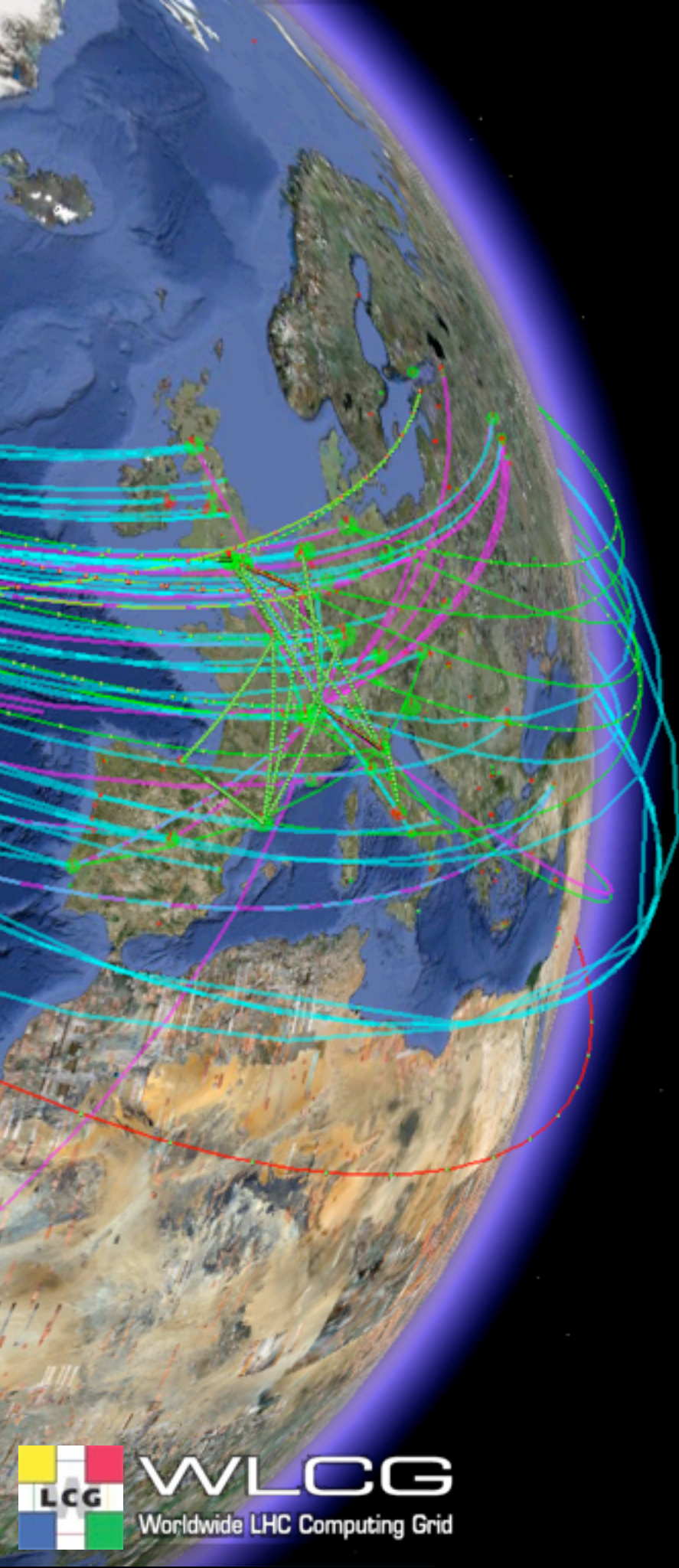
- Compromised user accounts at other sites (SSH)
- Vulnerable Web applications
- Failure to apply security patches

Training:

- Secure coding
- Check all user input by design

Apply security patches

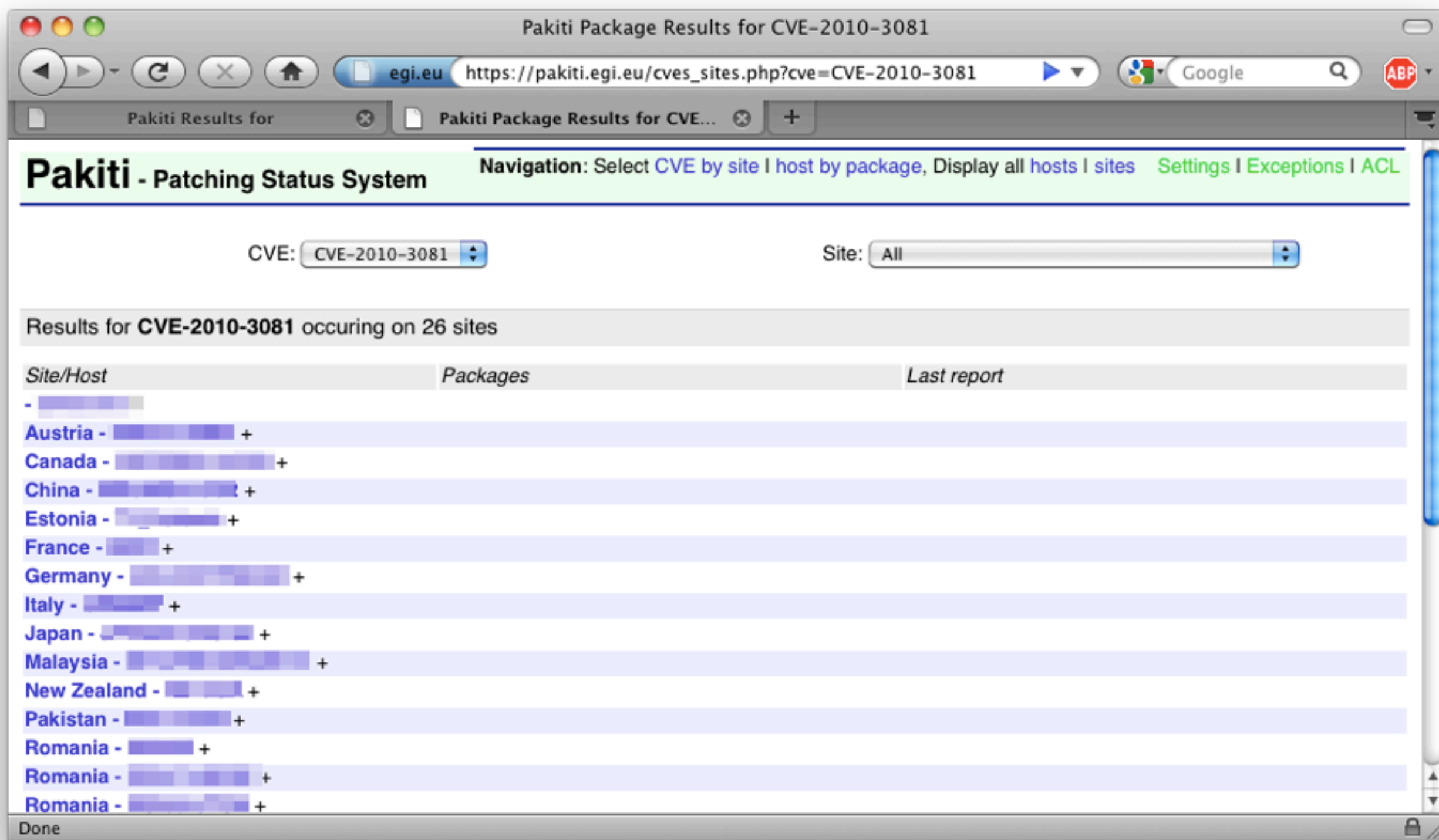
- Avoid modifying source code yourself
- Use upstream RPMs when possible instead





Security patching (1/3)

- Advanced monitoring of the sites with Pakiti
 - Sites affected by critical vulnerabilities are the main target
 - They can be suspended after 7 days (after appropriate warnings)





Security patching (2/3)

Pakiti Results for Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://[redacted]/hosts.php

Pakiti - Patching Status System Navigation: Select hosts by CVE | package, Display all hosts | domains Settings

Show: **vulnerable** | unpatched | **all** | not reporting Order by: tag | host | time | kernel | os Select tag: all

Tag: [redacted]

Security	Other	CVEs	Hostname	OS	Current kernel	Last report	Ops
0	0	0	[redacted]	Scientific Linux 4.8	2.6.9-89.0.16.EL	28.11.09 04:09	X

Tag: [redacted]

Security	Other	CVEs	Hostname	OS	Current kernel	Last report	Ops
0	0	0	[redacted]	Scientific Linux CERN SLC release 5.4 (Boron)	2.6.18-164.6.1.el5PAE	28.11.09 04:12	X

Tag: **Pakiti client**

Security	Other	CVEs	Hostname	OS	Current kernel	Last report	Ops
0	0	0	([redacted]) IP: [redacted]	CentOS release 5.4 (Final)	2.6.24-24-generic	25.11.09 21:15	X
3	0	2	[redacted]	Scientific Linux SL 5.4	2.6.18-164.6.1.el5	25.11.09 21:21	X
0	0	0	[redacted]	Scientific Linux SL release 5.4 (Boron)	2.6.18-164.6.1.el5	27.11.09 13:28	X
0	0	0	[redacted]	Scientific Linux SL release 5.4 (Boron)	2.6.18-164.6.1.el5	27.11.09 21:39	X
0	0	0	[redacted]	Scientific Linux SL 4.6	2.6.9-89.0.16.ELxenU	25.11.09 21:20	X
0	0	0	[redacted]	Scientific Linux SL 5.3	2.6.18-164.6.1.el5	25.11.09 21:21	X
0	0	6	[redacted]	Scientific Linux CERN SLC release 5.4 (Boron)	2.6.18-164.6.1.el5	28.11.09 21:21	X
0	0	368	[redacted]	Scientific Linux SL release 4.5 (Beryllium)	2.6.9-89.0.16.ELsmp	29.11.09 05:21	X
0	0	190	[redacted]	Scientific Linux SL release 4.7 (Beryllium)	2.6.9-89.0.16.ELsmp	28.11.09 05:21	X



Security patching (3/3)

Pakiti Package Results for CVE-2009-4536 for cern.ch

cern.ch <https://pakiti.cern.ch/cves.php?selcve=&seldomain=&cv> Google

Pakiti Package Results for CVE-20...

Pakiti - Patching Status System

Navigation: Select hosts by [CVE](#) | [package](#), Display all [hosts](#) | [domains](#) [Settings](#)

CVE: Domain:

[Click to get anonymous link to this page \(lifetime of the link is 1 week\)](#)

Selected CVE: **CVE-2009-4536**

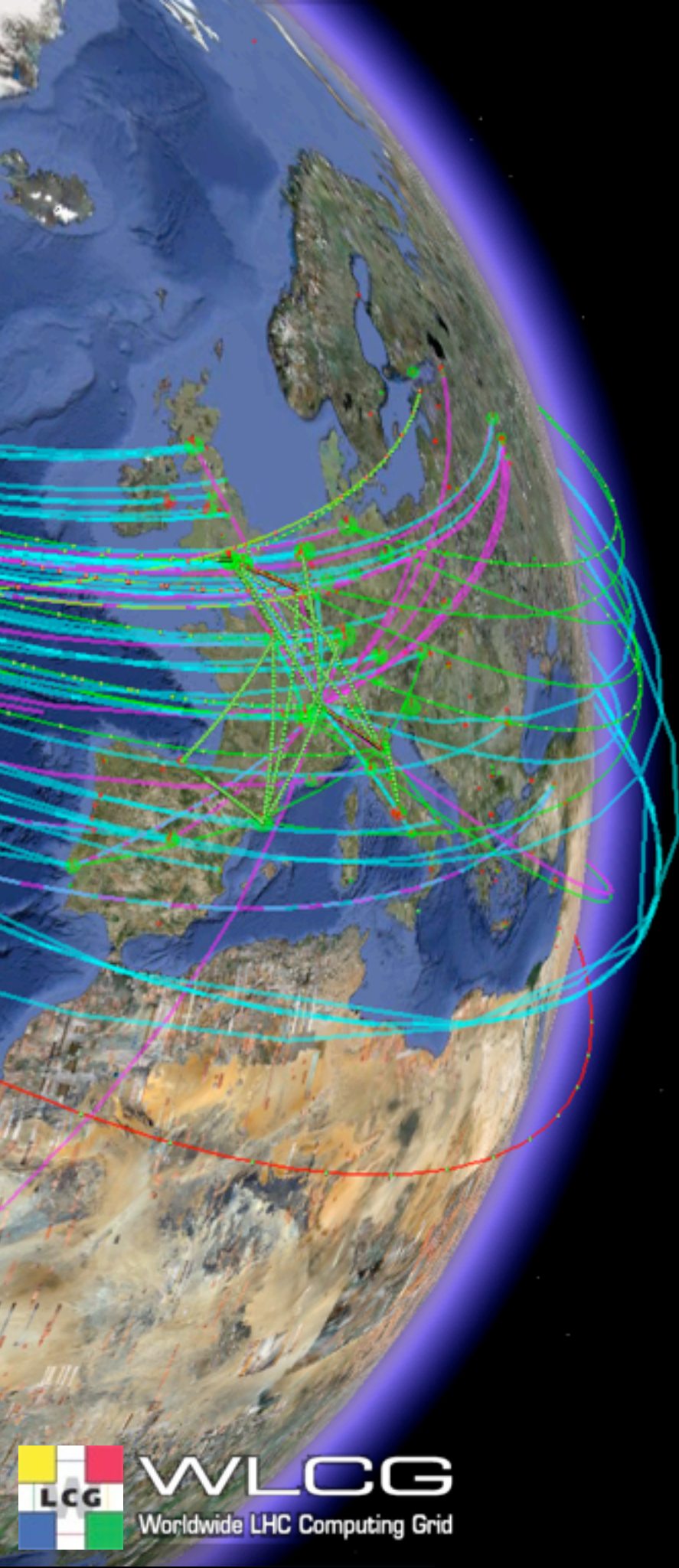
Domain/Host	Packages	Last report
cern.ch +		
5.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	16 February 2010 17:28
5.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	17 February 2010 17:14
1.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	17 February 2010 05:27
3.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	16 February 2010 17:57
4.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	16 February 2010 21:24
1.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	16 February 2010 13:16
2.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	17 February 2010 09:14
0.cern.ch	kernel-smp (0:2.6.9-89.0.16.EL.cern)	17 February 2010 05:47

Done

<http://pakiti.sourceforge.net>

Main causes of security incidents

- Compromised user accounts at other sites (SSH)





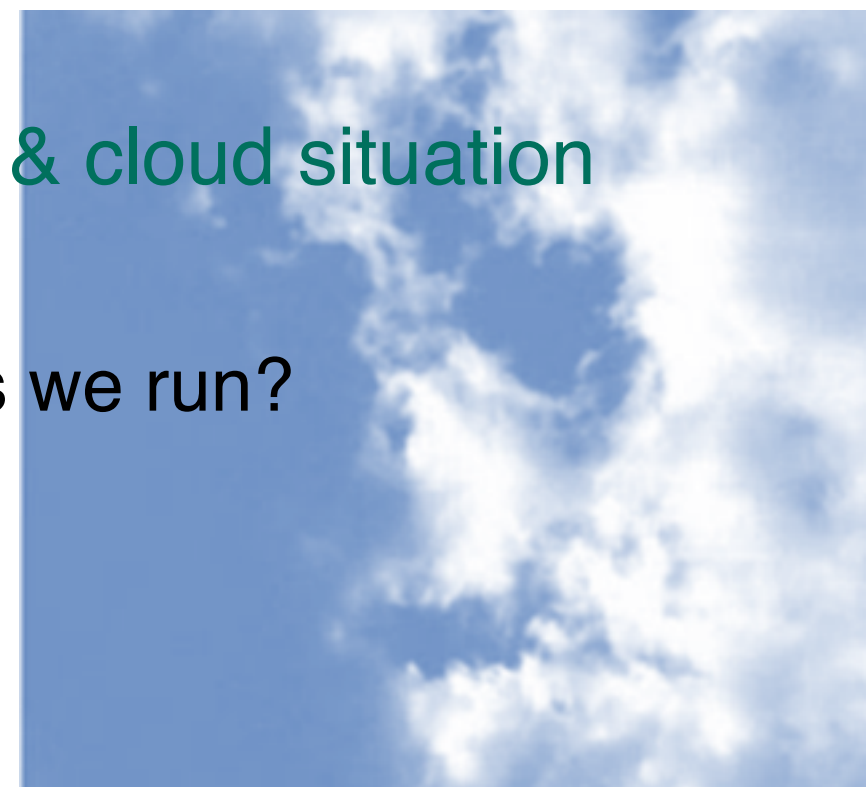
Compromised accounts

- Difficult to manage:
 - Your security depends on the security of your partners
 - Probably no authority over your partners
- Essential to **share information** and expertise
 - Closely **collaborate** to resolve incidents
- Adopting **common security policies** helps a lot
- For all grid infrastructure developers/designers/architects:
 - **Assuming the security perimeter is limited to x509 is wrong!**



Compromised accounts

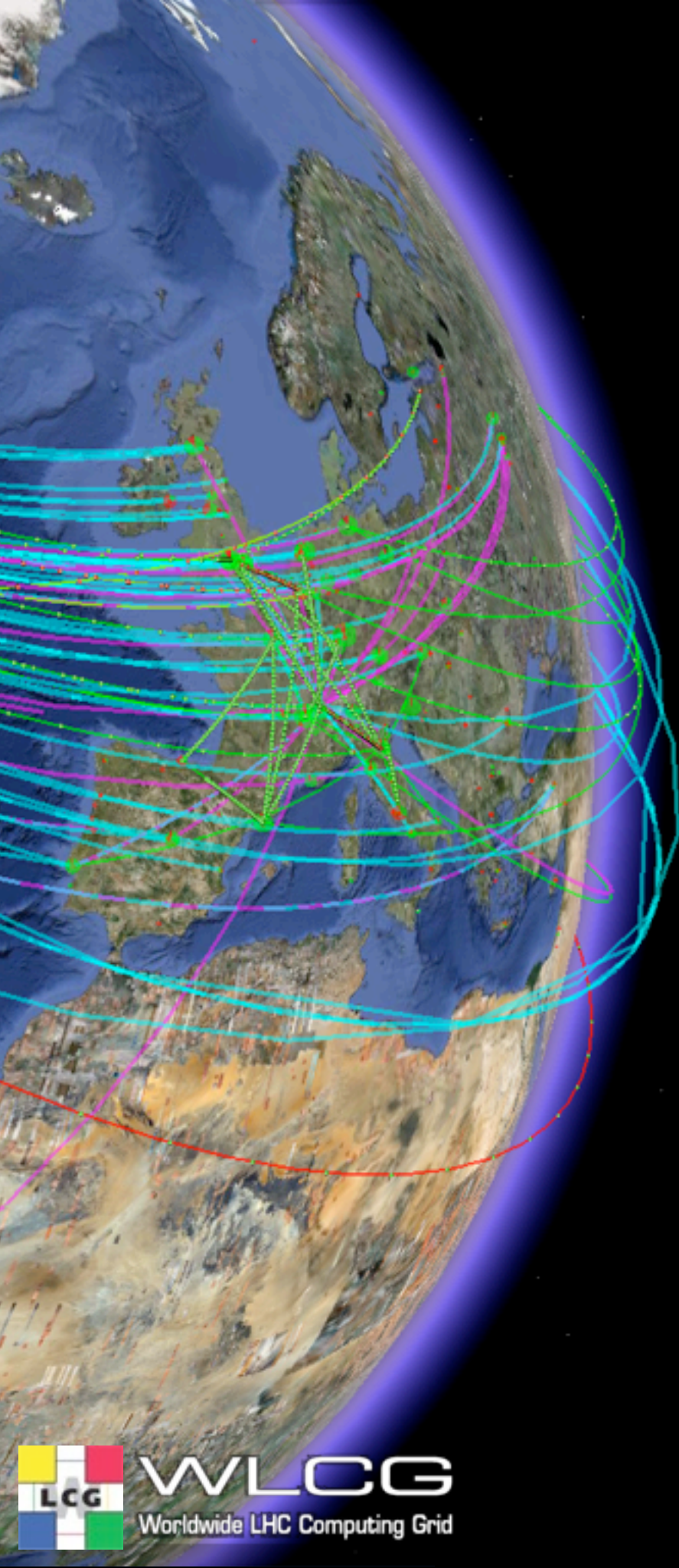
- A few things done at CERN in 2010:
 - Improved segregation between clusters (adm <-> general usage)
 - Prevent LKM to be loaded (CAP_SYS_MODULE)
 - Better mapping/traceability of users activity
 - Including a LKM to match network traffic with a PID (and local user).
 - Advanced kernel level root kit detection
 - Reinstallation made easier
 - Public root exploits result in reinstallation of the main front-end
 - Carefully monitoring the virtualization & cloud situation
 - Can we have enough traceability?
 - Can we perform forensics on the VMs we run?





Compromised accounts

- SSH authentication is an issue:
 - Passwords+Keys: sniffed/copied and re-used by attackers
 - The vast majority of Linux incidents at CERN results from compromised account at other sites
- Evaluating multi-factor authentication
 - Disappointed by many existing solutions
 - Financial or service cost
 - Lack of documentation/support, or simply little security benefit
 - Did not fit the environment (“just have to patch your SSH client”)
 - Pilot Yubikey service in progress:
 - <https://twiki.cern.ch/twiki/bin/view/Main/Yubikeys>
 - A few caveats, but seems to be a good trade-off overall



How to be best prepared?



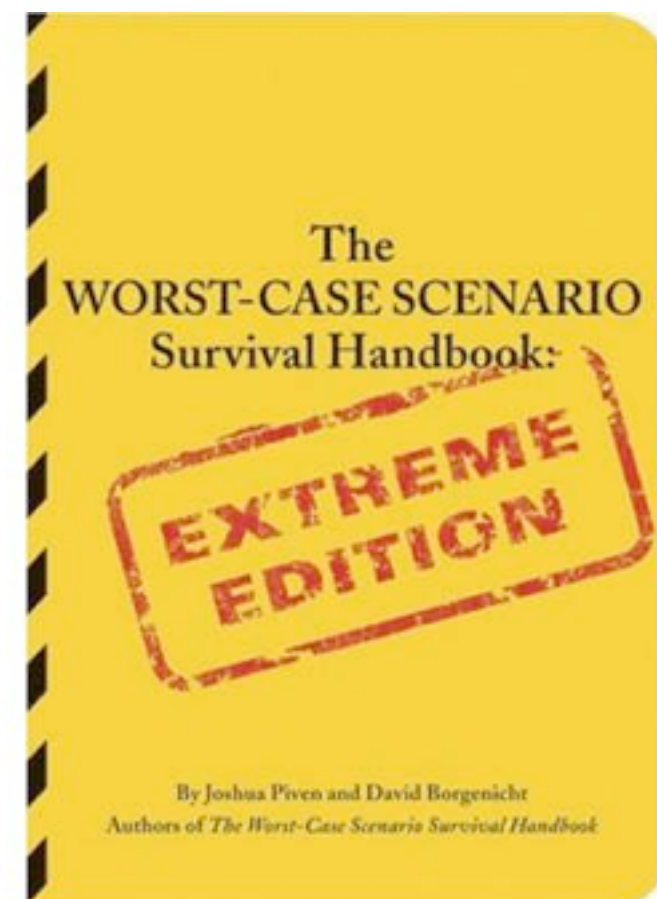
Identify the threats

- Identify the threats
 - Gather service (and security?) experts around a table
 - Identify your assets (= what you are trying to protect)
 - Brainstorm on possible threats against these assets
 - Think evil
 - How would YOU work around existing security systems?
 - What malicious events could severely affect your services?
 - Keywords: internet, exploit, service availability, trust, source code, dependency, vulnerability, confidentiality, privacy, press, partners, student, reputation, availability, illegal, warez, profit, backdoor, software lifecycle



Google™
UK

is it dangerous to		Advanced Search
		Preferences
		Language Tools
is it dangerous to reheat rice	15,000 results	
is it dangerous to swallow chewing gum	51,800 results	
is it dangerous to drink too much water	431,000 results	
is it dangerous to fly when pregnant	1,830,000 results	
is it dangerous to have a laptop on your lap	34,800 results	
is it dangerous to fly while pregnant	1,680,000 results	
is it dangerous to holiday in egypt	1,350,000 results	le.com
is it dangerous to inhale helium	20,000 results	
is it dangerous to wake a sleep walker	880,000 results	
is it dangerous to drink blood	395,000 results	
	close	





Organise threats into risk

- Organise threats into risk
 - Assign a likelihood and impact for each threat
 - How bad would it be if it happened (1 -> 4)?
 - How likely is this threat to actually happen (1 -> 4)?

<div>Impact</div> <div>Likelihood</div>	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

- Service and security expert can help





Manage the risks

- Manage the risks

- Order the risks based on the scores. The most important risks are on top.

Score	Impact	Likelihood	Risk
16	4	4	Remote exploitation of an unpatched operating system security vulnerability
16	4	4	Developers introduce a local root escalation vulnerability on software the team provides
8	2	4	A malicious host within the LAN is trying to access the main service database
8	4	2	Developers leak critical passwords to the public CVS repository
...
4	1	4	A summer student turned out to be evil
2	2	1	Privileged users run malicious code

- Highlighting the most important risks is essential





Define mitigation techniques

- Define mitigation techniques
 - Always try to make smart trade-offs: what is lost versus what is gained
 - Recommendations needs to be effective, but also efficient. It has to be worth it.

Score	Impact	Likelihood	Risk	Mitigation
16	4	4	Remote exploitation of an unpatched operating system security vulnerability	Apply security patches on a regular basis
16	4	4	Developers introduce a local root escalation vulnerability on software the team provides	Review CVS commits for component X & Y
8	2	4	A malicious host within the LAN is trying to access the main service database	Protect the database with password authentication
8	4	2	Developers leak critical passwords to the public CVS repository	Block off-site access to the CVS repository
...	
4	1	4	A summer student turned out to be evil	NONE - Accept the risk?
2	2	1	Privileged users run malicious code	NONE - Accept the risk?

- If a risk cannot be managed or accepted: escalate to the management
 - The risk is then accepted or rejected





Additional considerations

- Document
 - The risk assessment process you go through and its regular revisions
 - The main risks, including mitigation/recommendations
 - A process for to ensure the mitigation/recommendations are implemented/work
- Important to periodically review the situation and update the recommendations
 - Dynamic/changing environment

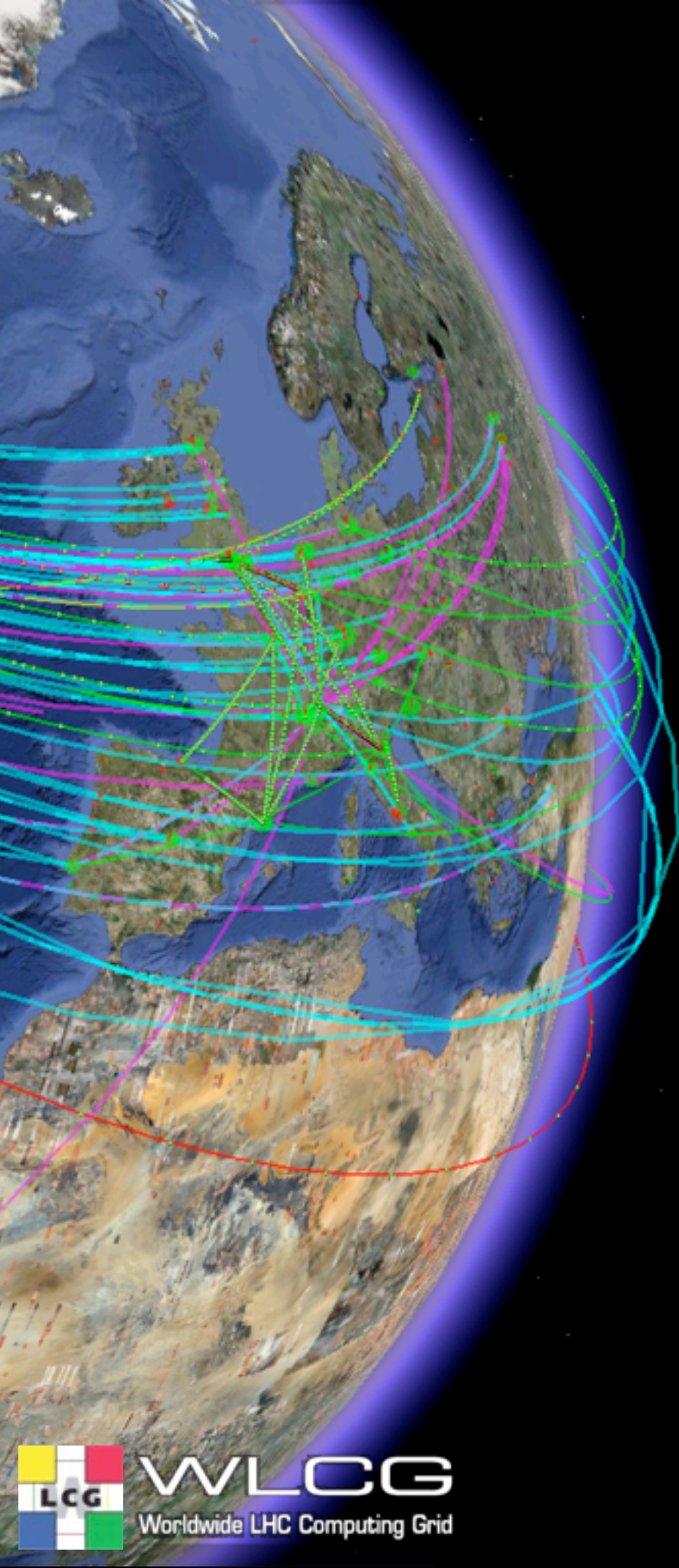




Final word of advice

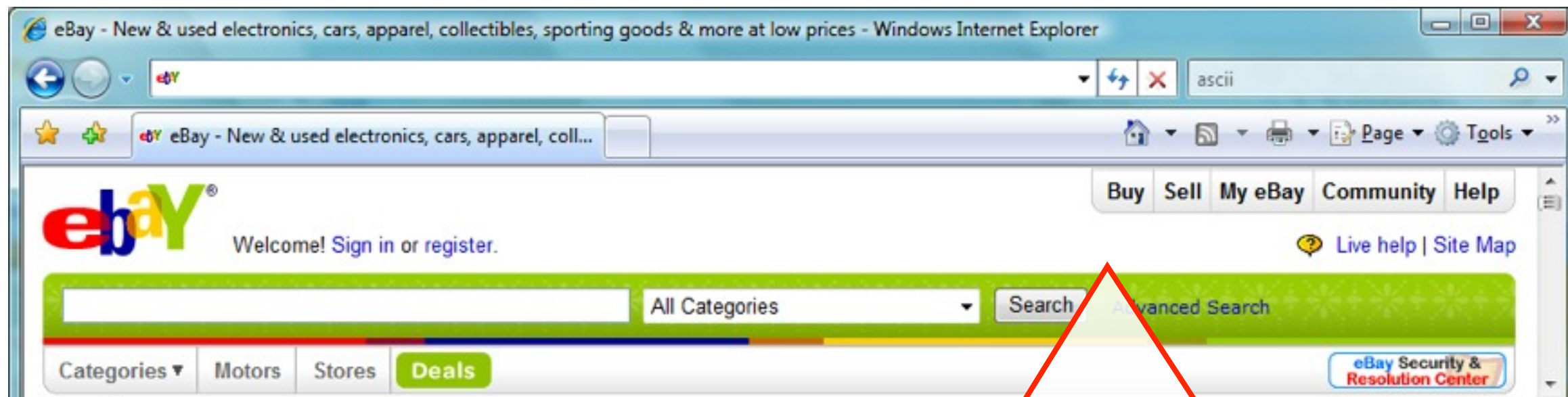
- Common pitfalls (quoting Bruce Schneier)
 - “People exaggerate spectacular but rare risks and downplay common risks.”
 - “People underestimate risks they willingly take and overestimate risks in situations they can’t control. When people voluntarily take a risk, they tend to underestimate it. When they have no choice but to take the risk, they tend to overestimate it.”
- Additional notes
 - The more complex a system is, the harder it is to improve its security
 - Do not underestimate skills/knowledge of attackers (<http://www.defcon.org/>, <http://www.phrack.com/>, etc.)
 - Know your enemy. Ex:
 - Using AJAX? What are the common security hacks?
 - Webmaster of a public portal? Have you heard about <http://zone-h.org/>?
 - Ask your security team for data/statistics/past experience/advice/recommendations
 - This helps making decisions (ex: to assess impact/likelihood)

Summary





Quizz



Which URL leads you to www.ebay.com ?

- ▶ <http://www.ebay.com/cgi-bin/login?ds=1%204324@%31%33%37%2e%31%33%38%2e%31%33%37%2e%31%37%37/p?uh3f223d>
- ▶ <http://www.ebay.com/ws/eBayISAPI.dll?SignIn>
- ▶ http://scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&co_partnerid=2&usage=0&ru=http%3A%2F%2Fwww.ebay.com&raflid=0&encRaflid=default
- ▶ <http://secure-ebay.com>



Soon or later...

- Each site/grid has been or will be affected by a security incident
- Part of **normal operations**, just need to ensure
 - It is “**cheap**” to deal with
 - The overall infrastructure is not affected
- It is essential to prepare for this event to reduce its:
 - **Impact** (appropriate & timely response, etc.)
 - **Likelihood** (prevention, service hardening, etc.)
- Share information
- Report incidents
- A grid is as **strong** as its **weakest** site!

