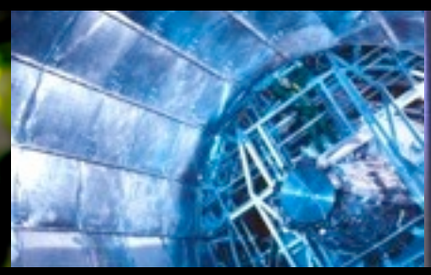
WLCG Group

Update on computer security

20th HEPIX, 24-28 Oct 2011, Vancouver



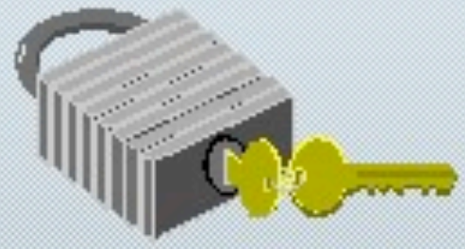





WLCG
Worldwide LHC Computing Grid

How times have changed (or not)

Secure Access to Experimental Resources



Andy Kowalski

HEPiX Jefferson Lab

October, 1997

How times have changed (or not)

Security Incident

- Thursday
  - notified by a Linux user that their PC was acting funny
  - found a hacked /bin/login and IRC software
  - called CIAC
  - checked other Linux PCs and found 4 more
  - disconnected these Linux PCs from the network

How times have changed (or not)

Security Incident

- Friday
  - found a sniffer (called pine) in /dev on a Linux PC
  - disconnected JLAB from the Internet
  - Began to inspect all multi-user systems at JLAB

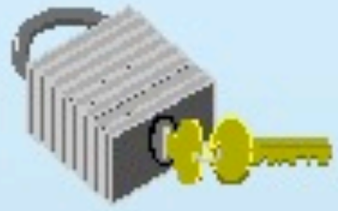
How times have changed (or not)

Security Incident

- Monday - Tuesday
  - created and passed out new passwords for everyone for every multi-user system at JLAB
  - cleaned up or reinstalled infected systems
  - had users register their IP address
  - added new filters to the firewall
- Wednesday
  - reconnected JLAB to the Internet

How times have changed (or not)

New Policies



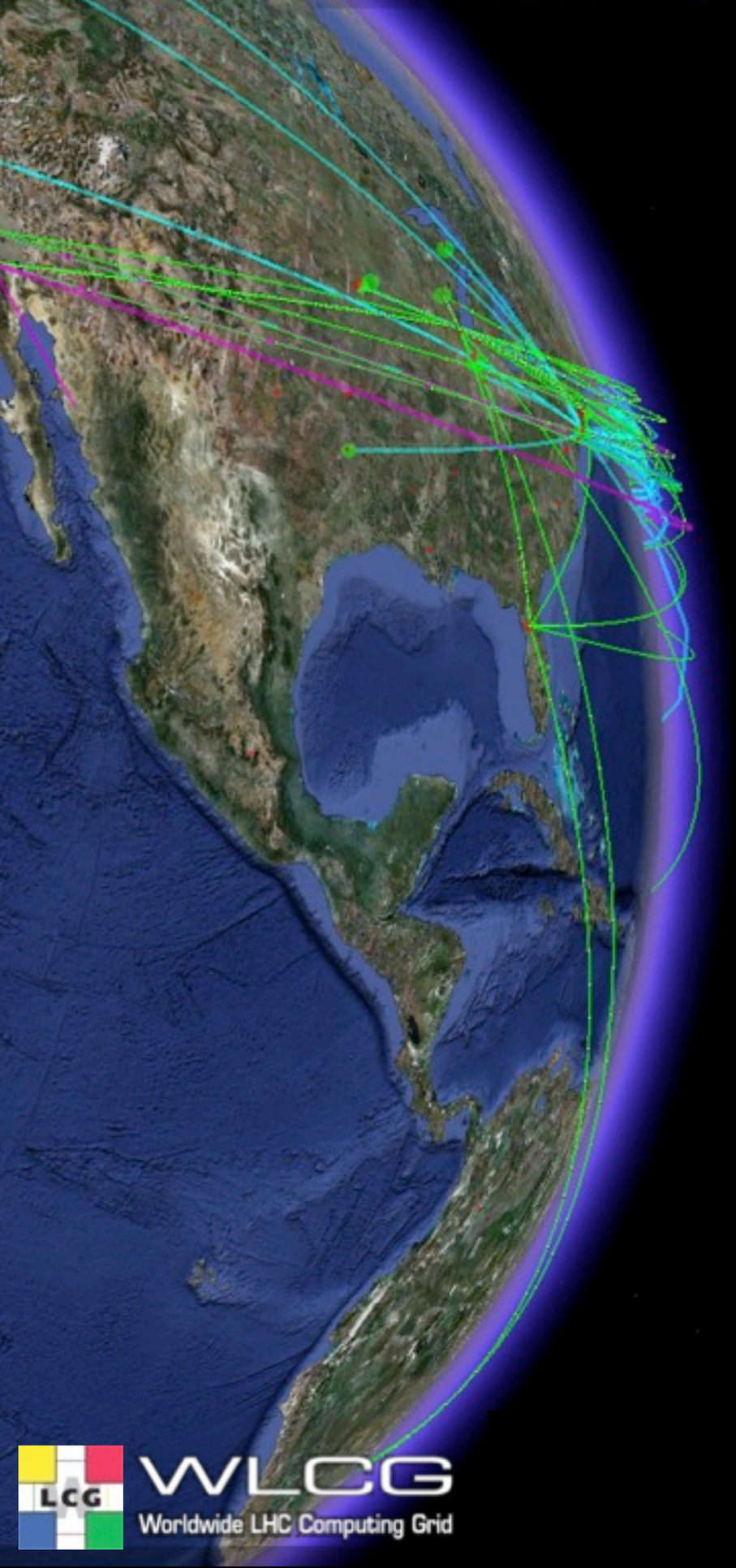
- Passwords
  - a JLAB user's password must differ from their off-site passwords
- IP addresses
  - must be registered or they will be locked down
- Access from the Internet
  - blocked by default

Major changes

- Complexity has increased
  - Schneier: complexity is the enemy of security
    - Security is constantly improving
    - But systems are getting more and more complex at a faster rate
- Attacker became professionals, motivated by profits

Products	Price
Credit card details	From $2-90
Physical credit cards (clone)	From $180 + cost of details
Card cloners	From $200-1000
Fake ATMs	From $3,500
Bank credentials	From $80-700 (with guaranteed balance)
Money laundering	From 10 to 40 percent of the total
Design and publishing of fake online stores	From $30-300 (depending on the project)

Source: Panda Labs



Security is a matter of trust

WLCG
Worldwide LHC Computing Grid

Trust is a difficult business

Trusting the root of trust

- Certificate authorities are the “root of trust”
  - SSL/TLS expected to guarantee confidentiality, integrity, authenticity, etc.
  - The security of all protocols based on TLS/SSL relies on trust

- Comodo and DigiNotar both compromised
  - Hundreds of rogue SSL certificates issued to attackers (e.g. mail.google.com, login.live.com, login.skype.com, addons.mozilla.org. etc.)
  - DigiNotar now bankrupt

- How many other certificate authorities are compromised?

DigiNotar
Internet Trust Services

COMODO
Creating Trust Online®

Trusting websites

- People now understand rogue websites can infect them
- How about legit websites?
  - Attacker apparently “sold” MySQL.com for $3000 on an underground forum

SOFTWARE / SERVICES

MySQL.com Hacked to Serve Malware

By Robert McMillan, IDG News

The website for the open-source MySQL database was hacked and used to serve malware to visitors Monday.

SIMILAR ARTICLES:

Hacker Collective Anonymous Strikes at Child Porn Sites

LastPass, Online Password Manager, May Have Been Hacked

Porn Site Users Beware: LulzSec Posts Your E-mail Address

What if Google's Hack Attack

Security vendor Armorize noticed the problem at around 5 a.m. Pacific Time Monday. Hackers had installed JavaScript code that threw a variety of known browse those with out-of-date br Adobe Flash, Reader or have been quietly infecte

Hacked BBC streaming websites serve up malware

Driveby exploit on 6Music and 1Xtra

By **Dan Goodin in San Francisco** • **Get more from this author**

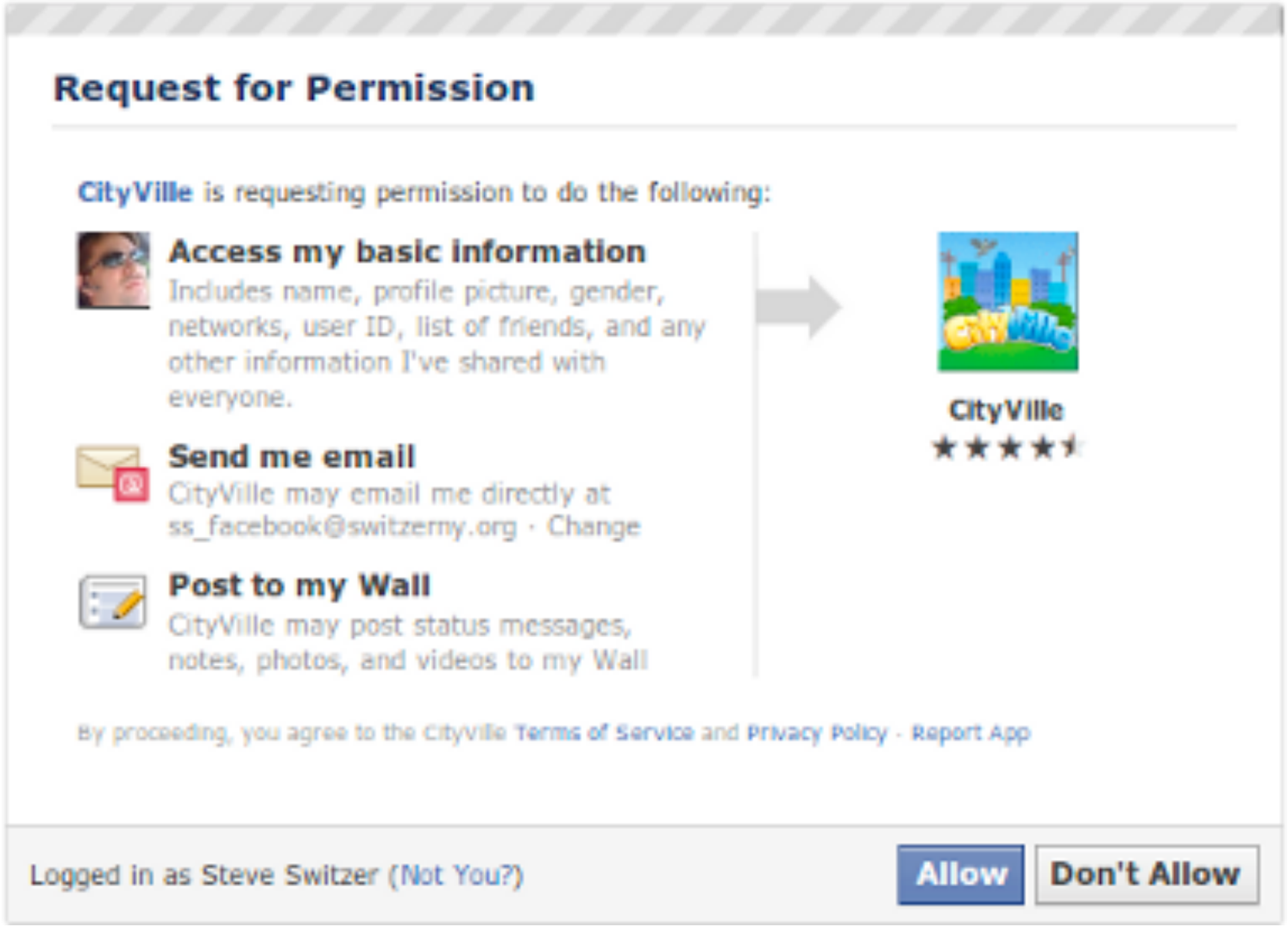
Posted in Security, 15th February 2011 19:18 GMT

Streaming sites operated by the BBC were hacked on Tuesday so they silently served visitors with malware, researchers from security firm Websense said.

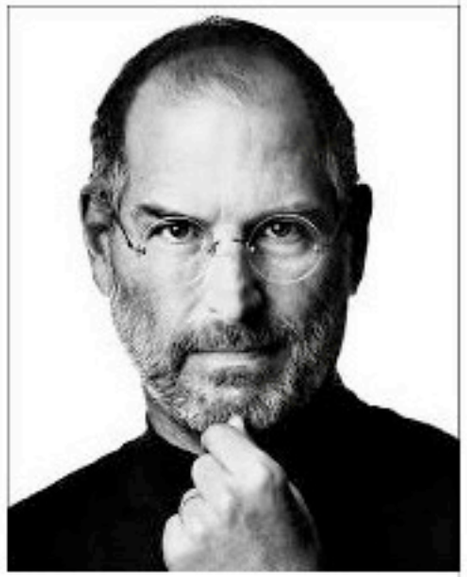
An iframe tag on the BBC's 6 Music and 1Xtra websites injected an exploit that was housed on a website with an address ending in cc, a top level domain for the Cocos Islands. The

Trusting social networks

- Goal: trick victims into clicking a malicious link
- Any major event in the news is a good opportunity
- Social networks a perfect opportunity
  - A toolkit to build a malicious Facebook App cost for a little as $ 25



Trusting “official” (fan) pages?



R.I.P. Steve Jobs Me gusta

Sitio web

Muro — R.I.P. Steve Jobs · Todos (Más recientes)

Compartir: Publicación Foto

Escribe algo....

R.I.P. Steve Jobs
In memory of Steve, a company is giving out 50 ipads tonight. R.I.P. Steve Jobs
http://bit.ly/restinpeace-steve-jobs
· Comentar · Traducir · Compartir · Hace 6 horas

A 1.175 personas les gusta esto.

Ver los 521 comentarios — Ver los 47 contenidos compartidos

Escribe un comentario...

R.I.P. Steve Jobs
R.I.P. Steve Jobs
Me gusta · Comentar · Traducir · Compartir · Hace 9 horas

A 2.624 personas les gusta esto.

Ver los 609 comentarios — Ver los 144 contenidos compartidos

Escribe un comentario...

ACTIVIDAD RECIENTE

R.I.P. Steve Jobs cambió la siguiente información: Información.

R.I.P. Steve Jobs se ha unido a Facebook. · Me gusta · Comentar

- Muro
- Información
- Actividad de tus amigos
- Fotos

Información

R.I.P. Steve Jobs Official Page

A
80.167
personas les gusta esto.

Crear una página
Agregar a los favoritos de mi página
Suscríbete a través de RSS
Reportar página
Compartir

- Out of 80 000 fans, 25 669 clicked on the link!

Trusting “official” (fan) pages?

Trusting the media

foxnewspolitics
@foxnewspolitics Washington, D.C.

Follow

Tweets | Favorites | Following | Followers | Lists

foxnewspolitics foxnewspolitics
We wish @joebiden the best of luck as our new President of the United States. In such a time of madness, there's light at the end of tunnel
6 hours ago

foxnewspolitics foxnewspolitics
BREAKING NEWS: President @BarackObama assassinated, 2 gunshot wounds have proved too much. It's a sad 4th for #america. #obamadead RIP
6 hours ago

foxnewspolitics foxnewspolitics
#ObamaDead, it's a sad 4th of July. RT to support the late president's family, and RIP. The shooter will be found
6 hours ago

foxnewspolitics foxnewspolitics
@BarackObama shot twice at a Ross' restaurant in Iowa while campaigning. RIP Obama, best regards to the Obama family.
6 hours ago

foxnewspolitics foxnewspolitics

Tweets | Favorites | Following | Followers | Lists

NBCNews NBC News
NBCNEWS hacked by The Script Kiddies. Follow them @s_kiddies!
5 minutes ago

NBCNews NBC News
This is not a joke, Ground Zero has just been attacked. W attempting to get reporters on the scene. #groundzeroat
6 minutes ago

NBCNews NBC News
Flight 4782 is not responding, suspected hijacking. One hit Ground Zero site at 5:47. #groundzeroattacked
9 minutes ago

by USATODAY

Script_kiddiez_ The Script Kiddies
Just hacked @usatoday
5 minutes ago Favorite Retweet Reply

USATODAY USA TODAY Top News
Follow @Script_kiddiez_ for more hacks in the future, inc vote now at on.fb.me/ouunmj
7 minutes ago

USATODAY USA TODAY Top News
Fox News, Wal-mart, Unilevel, Pfizer, NBC and now USA T Vote now! on.fb.me/ouunmj
8 minutes ago

Trusting operating systems

- Several major intrusions in the recent years
  - Debian, Fedora, etc.
- Kernel.org, Linux.com, Linux Foundation, etc.
  - Severe root compromise on multiple hosts
    - “via a compromised user credential”
  - People worried about the software being mirrored - wrong!
  - Real issue: signing keys owned by local users (448 users)
    - Stealth buffer overflow in a carefully chosen location?
      - –> Private root exploit for the next few years!
    - Experience showed that community code review often fails

WLCG Worldwide LHC Computing Grid

Trusting authorities

- German government using keylogger
  - Capture data from Firefox, Skype, MSN Messenger, ICQ etc.
  - Can take screenshot, record audio (incl. Skype)
  - Allegedly installed onto the computer as it passed through customs control at Munich Airport.

Several German states admit to use of controversial spy software

A hacker group says Berlin may have software to spy on citizens

A number of other German states have followed Bavaria in confirming the use of a controversial software program to spy on people through their computers. The German justice minister has demanded an investigation.

Several additional German states have admitted to deploying spyware in order to investigate serious criminal offenses, according to regional media sources.

The interior ministers of the states of Baden-Württemberg, Brandenburg, Schleswig-Holstein and Lower Saxony said that regional police had used the software within the parameters of the law. In Lower Saxony, the software has been in use for two years, according to the public broadcaster NDR.

Trust is a difficult business

- It is a difficult business, even military infrastructures struggle

Malware compromises USAF Predator drone computer systems

by Graham Cluley on October 10, 2011 | 13 Comments

FILED UNDER: Malware

According to a Wired report, malware has infected the control systems used by the United States Air Force to fly Predator and Reaper drones, logging keypresses as the unmanned aircraft are flown remotely in Afghanistan, Libya, Pakistan and other conflict zones.

The malware intrusion is said to have been detected by the Department of Defense's own Host Based Security System (HBSS), but attempts to permanently remove the infection from one of America's most important weapons systems have proven unsuccessful.

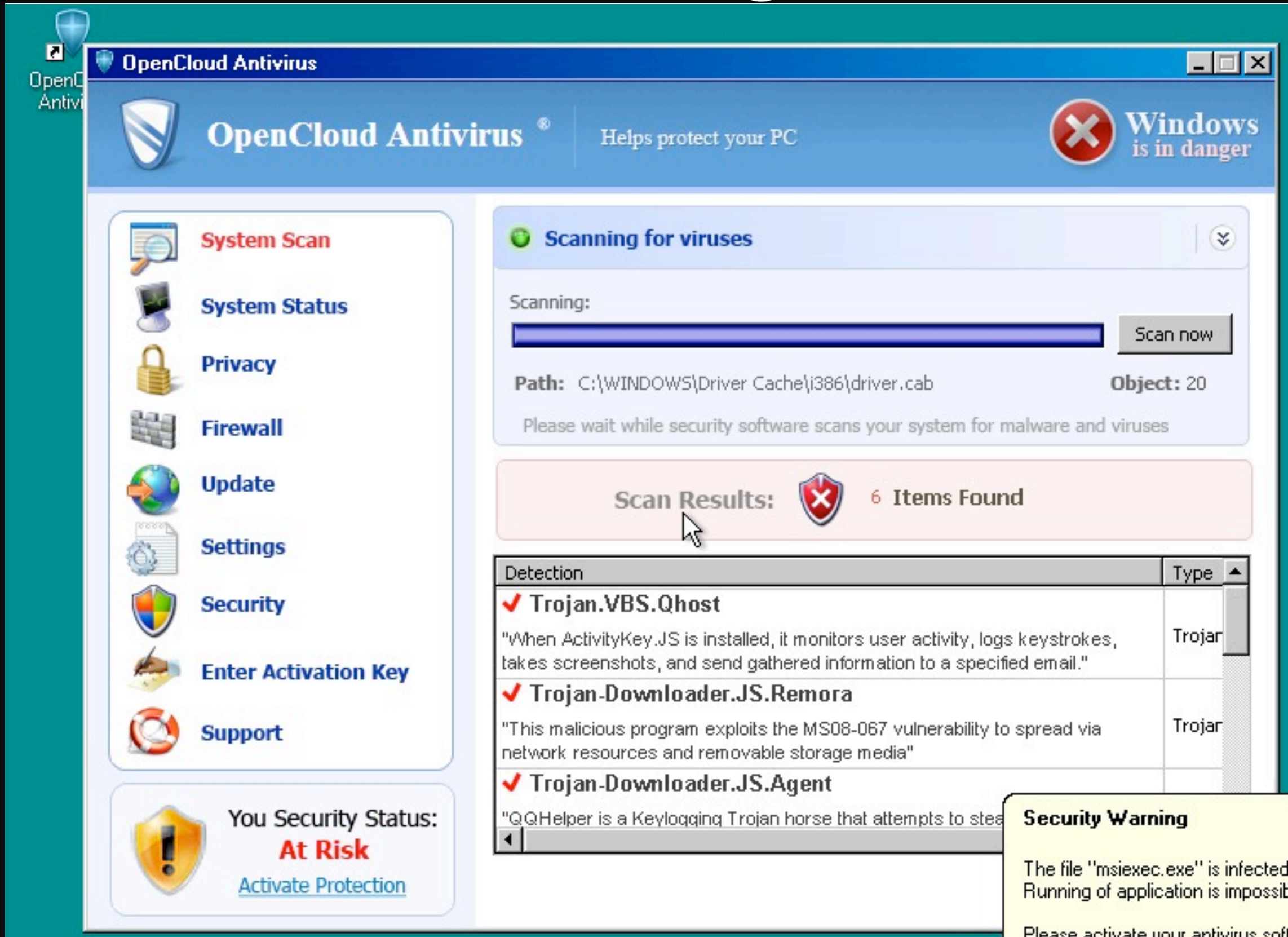
"The network defenders at the 24th Air Force learned of the virus by reading about it in [the news]" (http://cern.ch/go/7Tdd)

Mobile phone security

- Mobile phones & apps are increasingly becoming a target
  - iOS and Android in particular
  - Contain a lot of valuable information (marketable)
    - Personal & corporate data (mails, photos, contacts, docs, etc.)
    - Credentials, accounts
    - Great potential for malware (record audio, video, location)
  - Operating systems & browsers not as mature as desktop versions
  - Malicious apps are a good infection vector
  - Much more difficult to patch, and takes more time
  - "Production malware" already in the wild, improves quickly

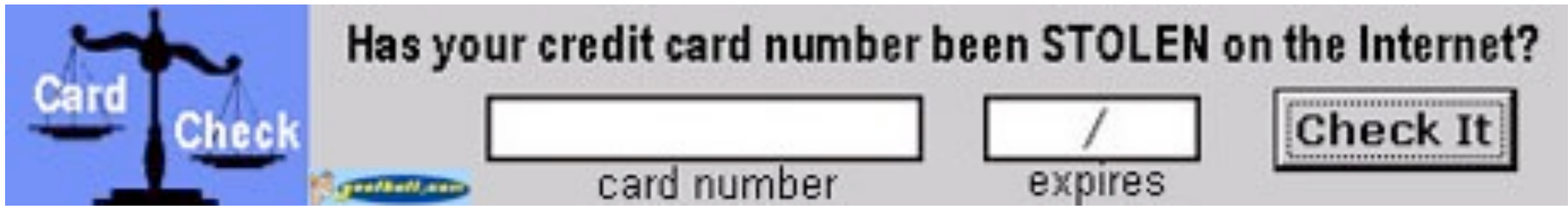
- Android/Jmsonez.A - a calendar app that sends SMS texts to a premium rate number.
- Android/Smsmecap.A – a fake comedy app that sends SMS texts to everyone in the user's address book.
- Android/DroidKungFu – malware that is capable of installing its own software and updates.
- Android/DrdDreamLite – capable of sending data back to the attacker.

Cloud is good



Recent HEP incidents

- Attackers traditionally after your IP & bandwidth
  - DSL hosts easier to compromise and highly distributed
  - Your site is not very attractive
- New malicious use case surfaced: Bitcoin mining
  - Lots of CPU/GPU power needed
  - Your site is very attractive
  - Recent incident affecting several academic sites: attacker possibly earned several thousand dollars
  - # of incidents will likely be indexed on the Bitcoin currency value

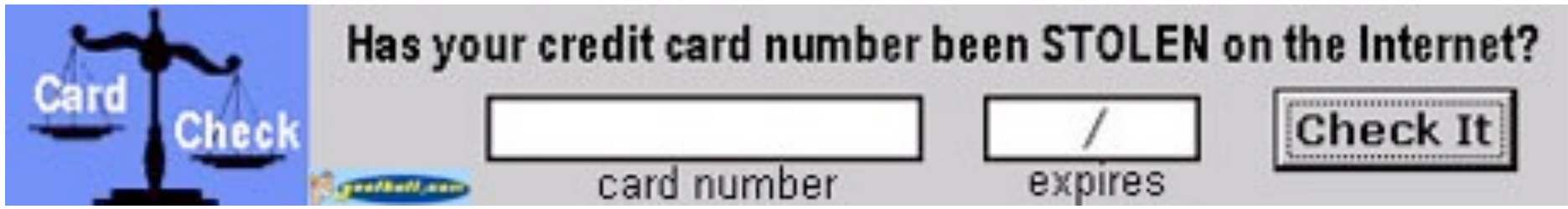


Recent HEP incidents

- Stolen SSH accounts remain the primary infection vector
  - EGI TF: “11 of 12 incidents are due to defeating ssh authentication.”
  - Part of normal operations, business as usual
  - No major root escalation
  - Multi-factor authentication deployment in progress at several sites

- Insecure JMX console config (JBOSS) particularly targeted
  - Good idea to scan/check your site

- Identity federation will change the current incident response landscape



Identity Federation

- Identity Federation workshop in June at CERN
  - Minutes: http://cern.ch/go/F8jZ
  - "The goal is to explore the requirements for federated identity management across the different disciplines, compare the functionality, operational constraints and state of deployment of current technologies, and formulate a roadmap for how we could establish such a service in the future."

- 2nd workshop in Oxford, 2-3 Nov 2011:
  - http://indico.cern.ch/conferenceDisplay.py?confId=157486
  - Registration still open!

Identity Federation - Main challenges

- Trust framework: provide accreditation for non-x509 identity providers (IGTF)
- Attributes management and release
- Policies and procedures
  - Trust between federations essential
- Incident response - significant impact
  - Identity providers will have a key role
    - New responsibilities
- Risks to be managed
  - Phishing against end users
  - Malicious identity providers
  - Malicious service providers
- Token translation services important for grids

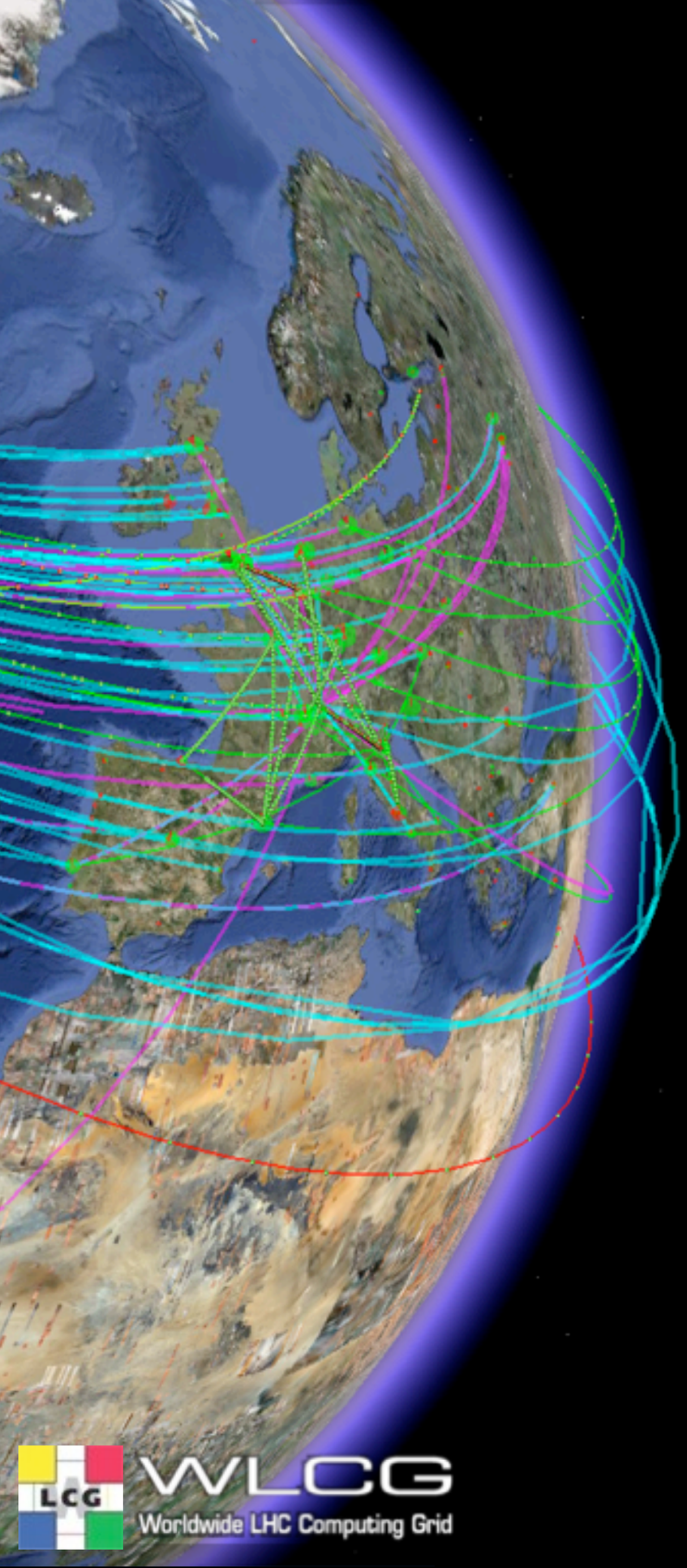
"It's a baby. Federal regulations prohibit our mentioning it's race, age, or gender."

WLCG - Technical Evolution Group

- Different "technical evolution groups" formed in WLCG
  - To reassess the implementation of the grid infrastructures that we use in the light of the experience with LHC data, and technology evolution, but never forgetting the important successes and lessons, and ensuring that any evolution does not disrupt our successful operation.

- One group focuses on security, in particular:
  - Conduct a risk analysis/assessment
  - Review the security model, including AAI on the worker nodes
  - Review the security model, including AAI on the storage systems

- Work has just started
  - https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG



Questions & Discussion

WLCG
Worldwide LHC Computing Grid