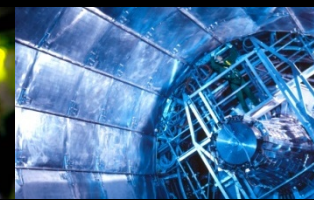
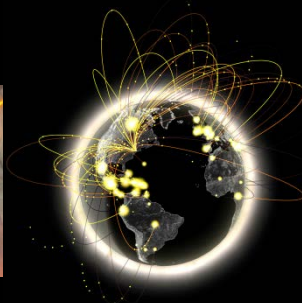
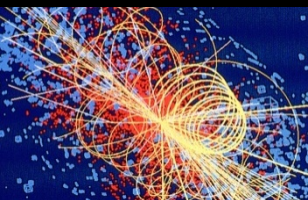
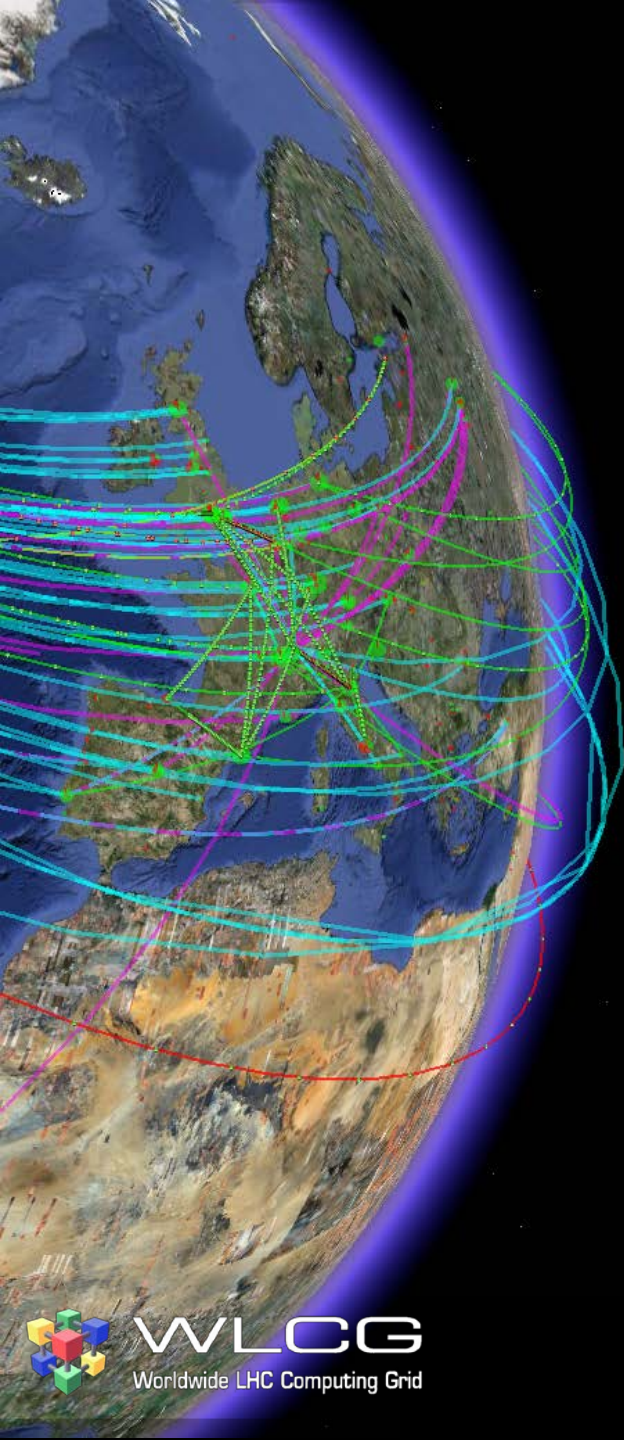


Security Update

Vincent BRILLAULT

HEPiX Spring 2014, Annecy





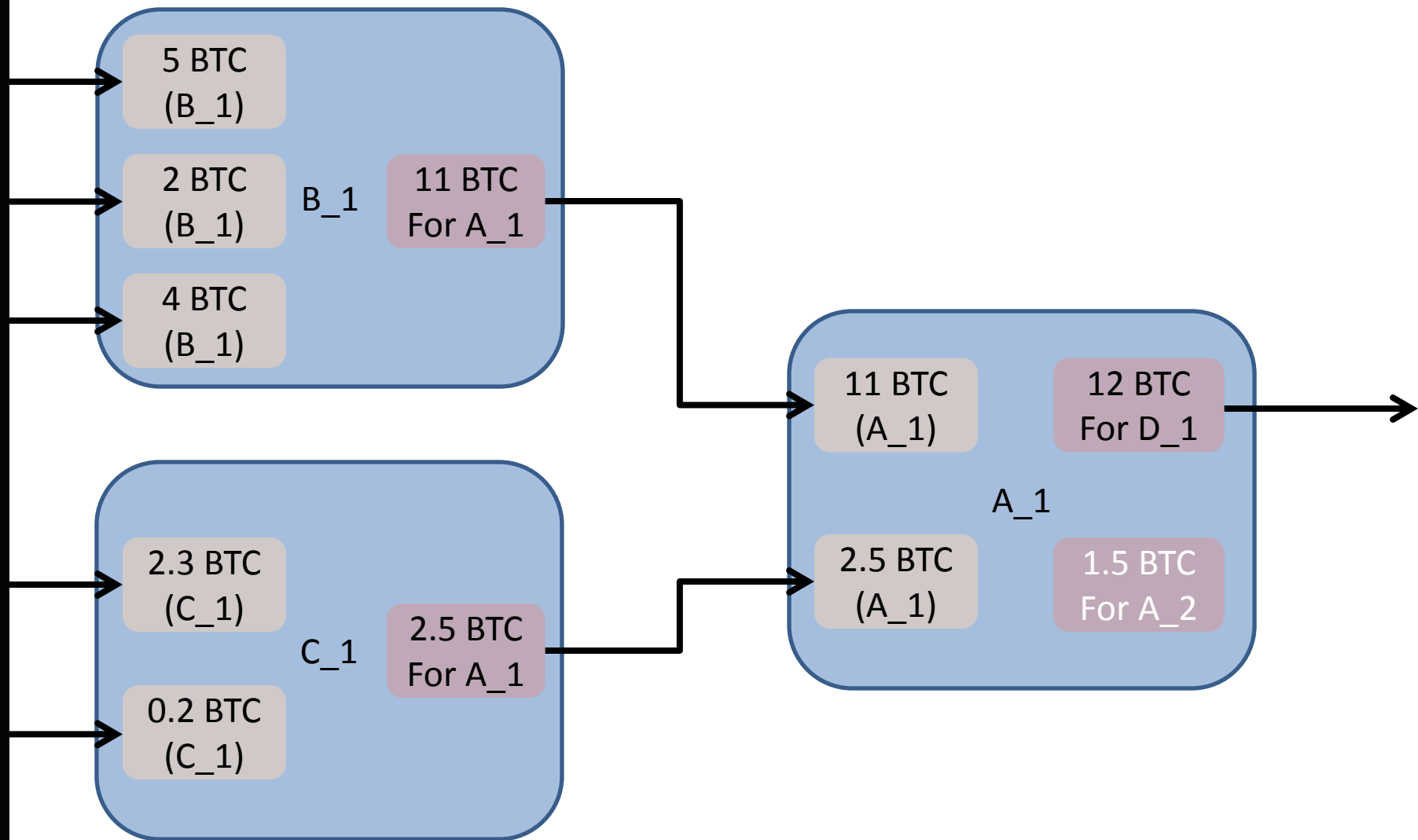
Crypto-Currencies

Crypto-Currencies



- Uncontrolled currencies
- Create an account == Generate new *address*
- *Wallet*: list of addresses & private keys
- Exchanges with *real* currencies

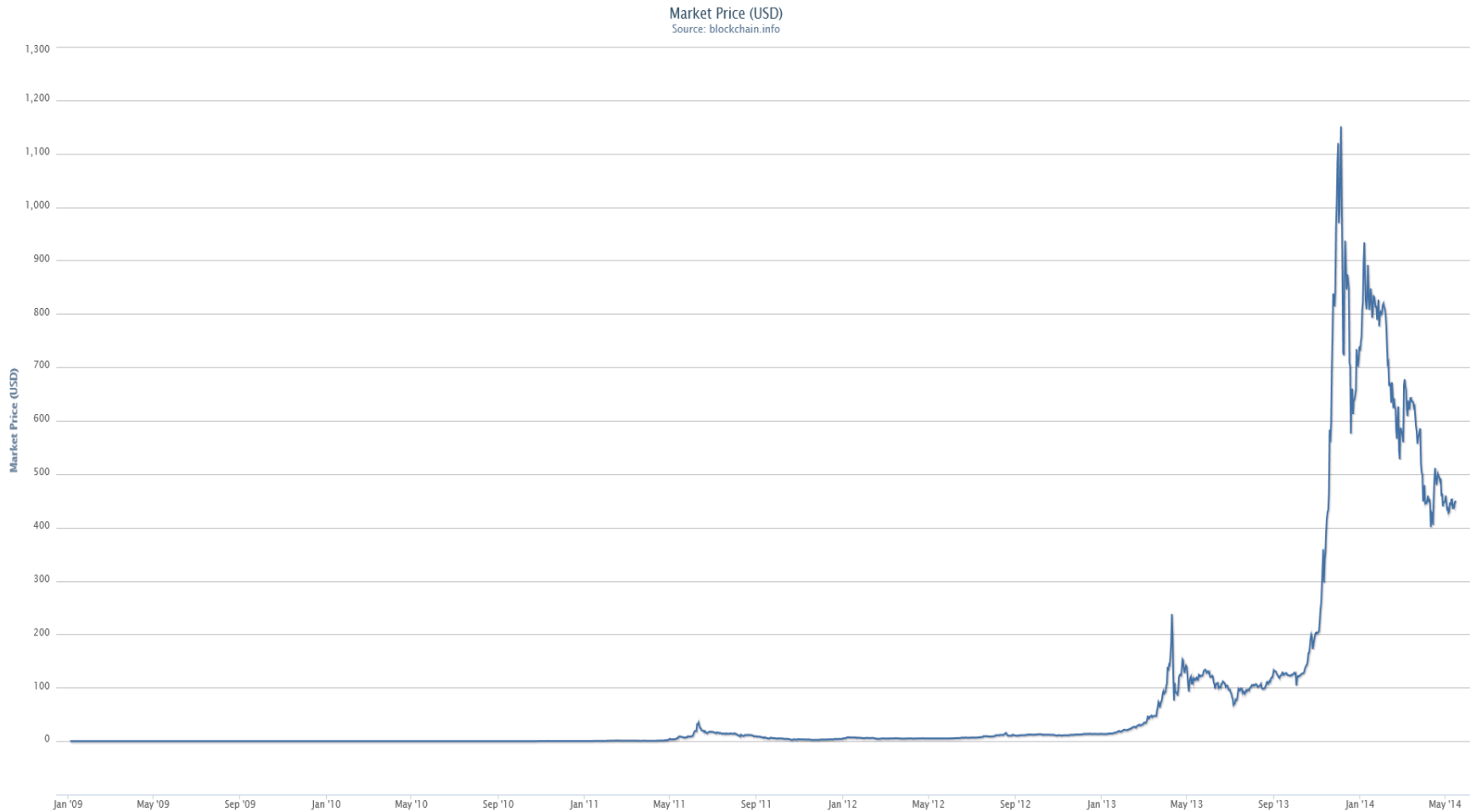
Transactions everywhere (chains)



Block Chain & Miners

- Block:
 - Contains aggregated valid transaction
 - *Proof of work*: hard computer problem
 - BTC: $\text{hash}(\text{block}) < \text{target}$
- Miners:
 - Hash blocks until someone find good one
 - Paid:
 - Per solved block
 - Per transaction (if it included a mining fee)

Exchange rates: BTC <-> USD



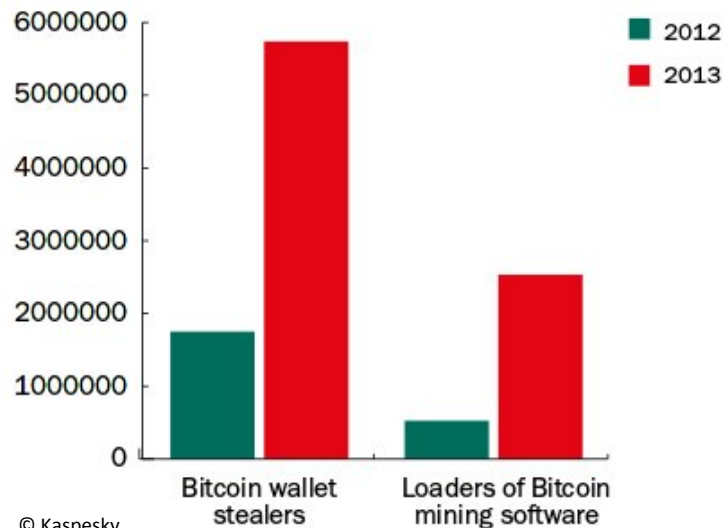
© Blockchain.org

Mining malwares

Bitcoin-mining malware reportedly found on Google Play

Fake wallpaper apps turned phones into bots for the power- and computationally intensive process of producing crypto-currency, a mobile security firm warns.

Number of attacks



© Kaspersky

Infecting DVRs with Bitcoin-mining malware even easier than you suspected

It took just a day for the Internet-connected device to be under attackers' spell.

Secret Bitcoin mining code added to e-sports software sparks outrage

E-sports league made \$3,600 using the power-hungry GPUs of its users, admin admits.

Yahoo malware turned PCs into Bitcoin miners

Malicious ads served to Yahoo users were designed to transform computers into a Bitcoin mining operation, according to a security firm.

Interesting transactions



Silk Road
anonymous market

messages 1 | orders 0 | account \$0.00

Search

Go

Shop by Category

- Drugs 2,399
 - Cannabis 341
 - Dissociatives 65
 - Ecstasy 209
 - Opioids 156
 - Other 144
 - Precursors 12
 - Prescription 526
 - Psychedelics 427
 - Stimulants 273

- Apparel 114
- Art 7
- Books 743
- Collectibles 12
- Computer equipment 19
- Custom Orders 26
- Digital goods 310
- Drug paraphernalia 89
- Electronics 20
- Erotica 319
- Fireworks 2
- Food 3
- Forgeries 58
- Hardware 2
- Home & Garden 7
- Jewelry 48
- Lab Supplies 5
- Lotteries & games 29
- Medical 5



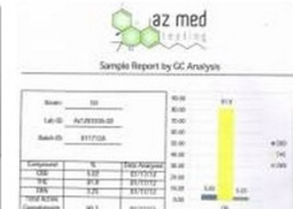
5x - 10mg Dexedrine (Pure Dextroamphetamine)
\$4.94



2 x 0,25 mg Xanax (Alprazolam)
\$1.50



Malana charas hand rubbed Indian hash 100g
\$75.83



1 Gram OG KUSH OIL 81% THC 90% TOTAL
\$4.13



14 grams (1/2 Ounce) of Nebula JWH-122
\$2.63



3.5g Crystal Meth Ice Shards
\$31.92



20 x 25mg Cialis
\$2.57



!!!...Psilocybe-Cubensis-Chocolate...!!!
\$18.15



100 x Orange Star Very high MDMA content 180mg



100x 200mg White XTC 'Speakers'



3g Methylone Crystals -\$50-Lab Grade



15mg Adderall Extended Release (1 Capsule)

Interesting transactions

CryptoLocker

Payment for private key

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)



Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

[Home Page](#)
[Getting started with Bitcoin](#)

<< Back Next >>



Why ?

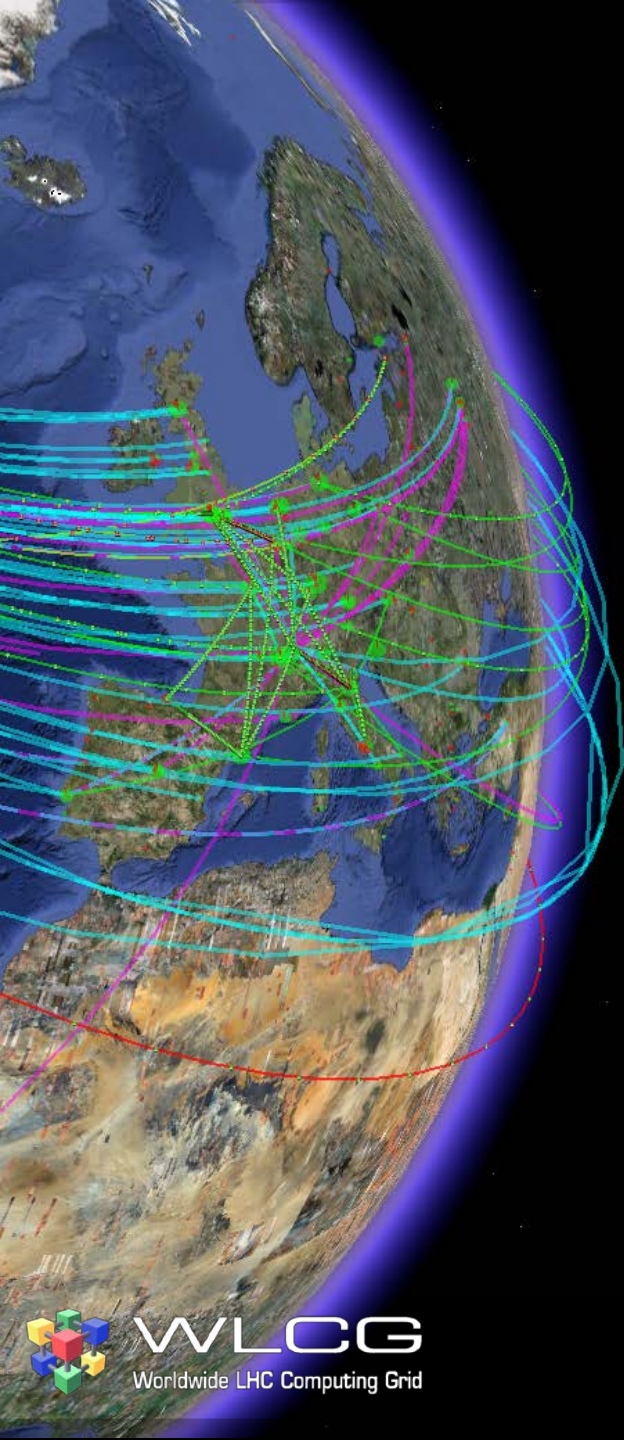
- Make money out of botnets ([CG]PU -> \$\$)
- Very low traceability:
 - No link address <-> user (except exchanges)
 - *Laundering*: create new addresses and move coins

EGI / WLCG: mining jobs

- Forbidden by VO AUPs
- Increasing number of incidents:
 - *Tests*
 - *Benchmarks*
 - Malicious jobs
- Cost:
 - CPU time
 - Forensics, investigations ...

What can we do for the grid ?

- VOs:
 - Remind users of the AUPs
 - Make examples (temporary ban users) ?
- Sites:
 - Look for standard mining software
 - Monitor network (connection to known pools)
- Virtualization: detection by sites harder



SSL/TLS & x509

Broken SSL libraries

- Apple SSL: Wrong certificate validation

goto fail; // [Apple SSL bug test site](#)

This site will help you determine whether your computer is vulnerable to [#gotofail](#).

YOUR BROWSER IS VULNERABLE, PATCH AS SOON AS POSSIBLE!

We have examined your OS and browser version information and determined that an active vulnerability test was appropriate. Unfortunately, your browser continued loading our test image after seeing an invalid ServerKeyExchange message. An attacker able to actively intercept your network connections (this is possible on **most WiFi networks**) can freely **snoop on you**, for example when you log into your **bank account**. Please check your browser and operating system for security updates and apply them right away. [Other applications on your system](#) such as **mail, chat, financial, social networking and backup apps** are also at risk - simply switching browsers will not fully protect you.

Please see [agl's writeup](#) for a full description of the bug.

Apple has released [official iOS updates](#) that resolve this issue.

An [update is now available](#) for OS X Mavericks, please [check for the update and install it](#) right away if you're vulnerable.

Some further explanation of this site can be found in the [FAQ](#).

For more browser SSL/TLS testing check out [How's my SSL?](#) and [SSL Labs](#).

Fan mail, hate mail, bug reports, etc to gotofail@gotofail.com or @gotofailcom but requests for server source code will be ignored until everyone has had time to patch. Thanks to Jacob September for help with the stylesheet.

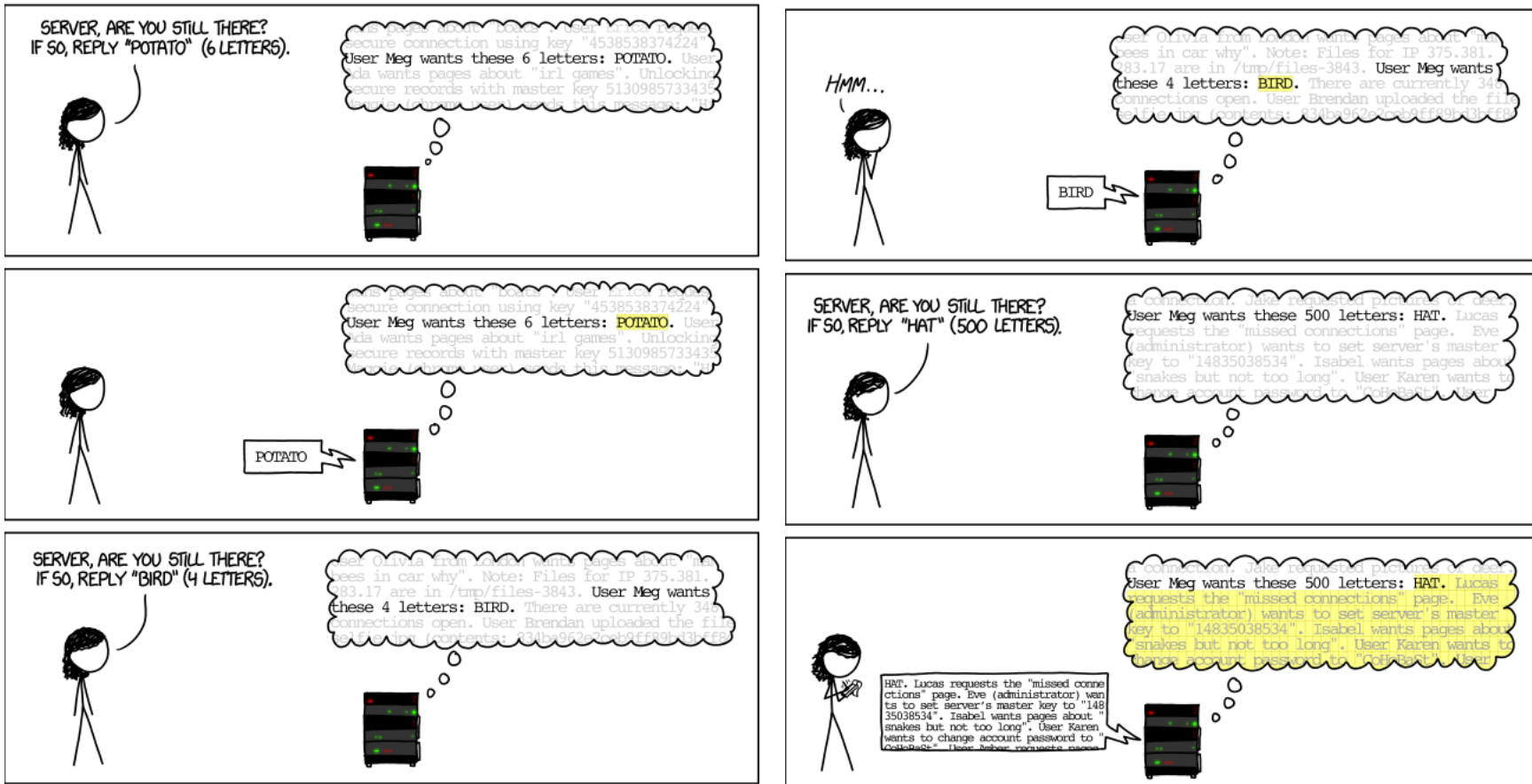
If you'd like to donate, feel free to send bitcoin to [19xUQVwyc5DDo1uoN8dXARICEfXCrkRyir](https://blockchain.info/address/19xUQVwyc5DDo1uoN8dXARICEfXCrkRyir) or [give something to EFF](#).

- GNUTLS: Wrong certificate validation
Goto Apple: GnuTLS falls foul of
SSL certificate verification issues

Summary: *An audit conducted by Red Hat has turned up an SSL certificate verification vulnerability in all versions of GnuTLS.*

HeartBleed: What ?

HOW THE HEARTBLEED BUG WORKS:



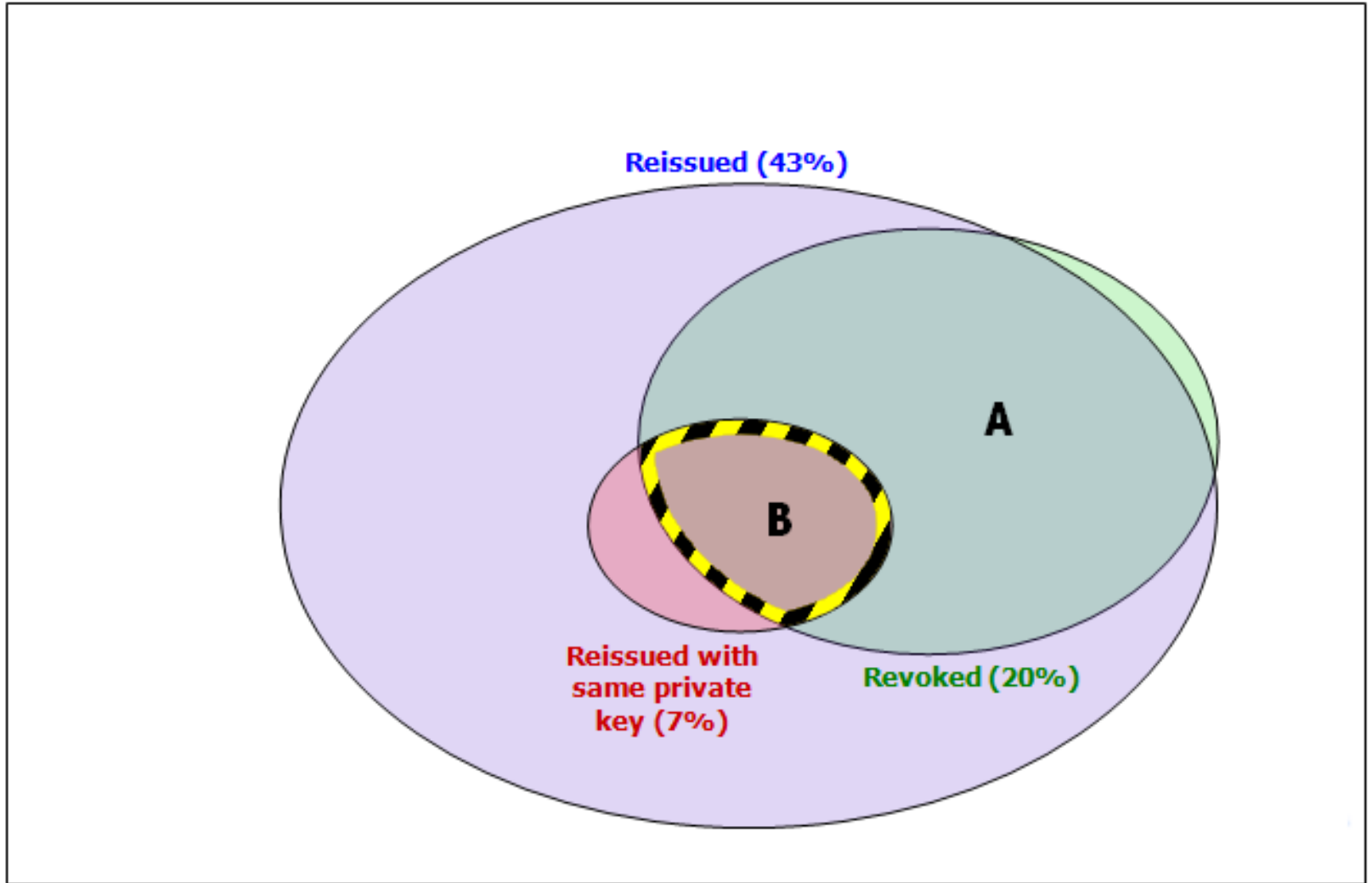
© XKCD

HeartBleed

- Reason:
 - No input sanitization!
 - Openssl maintained by 6 peoples (1 paid)
- Costs:
 - All password changed
 - Certificates revoked & rekeyed

HeartBleed: “fixed”

All websites affected by the Heartbleed bug



HeartBleed: Lesson Learned

Core Infrastructure Initiative

The Core Infrastructure Initiative is a multi-million dollar project housed at The Linux Foundation to fund open source projects that are in the critical path for core computing functions. Inspired by the Heartbleed OpenSSL crisis, The Initiative's funds will be administered by the Linux Foundation and a steering group comprised of backers of the project as well as key open source developers and other industry stakeholders.



The steering group will work with an advisory board of esteemed open source developers to identify and fund open source projects in need. Support from the initiative can include funding for fellowships for key developers to work full time on the open source project, security audits, computing and test infrastructure, travel, face-to-face meeting coordination and other support. Early supporters include:



Grid impact

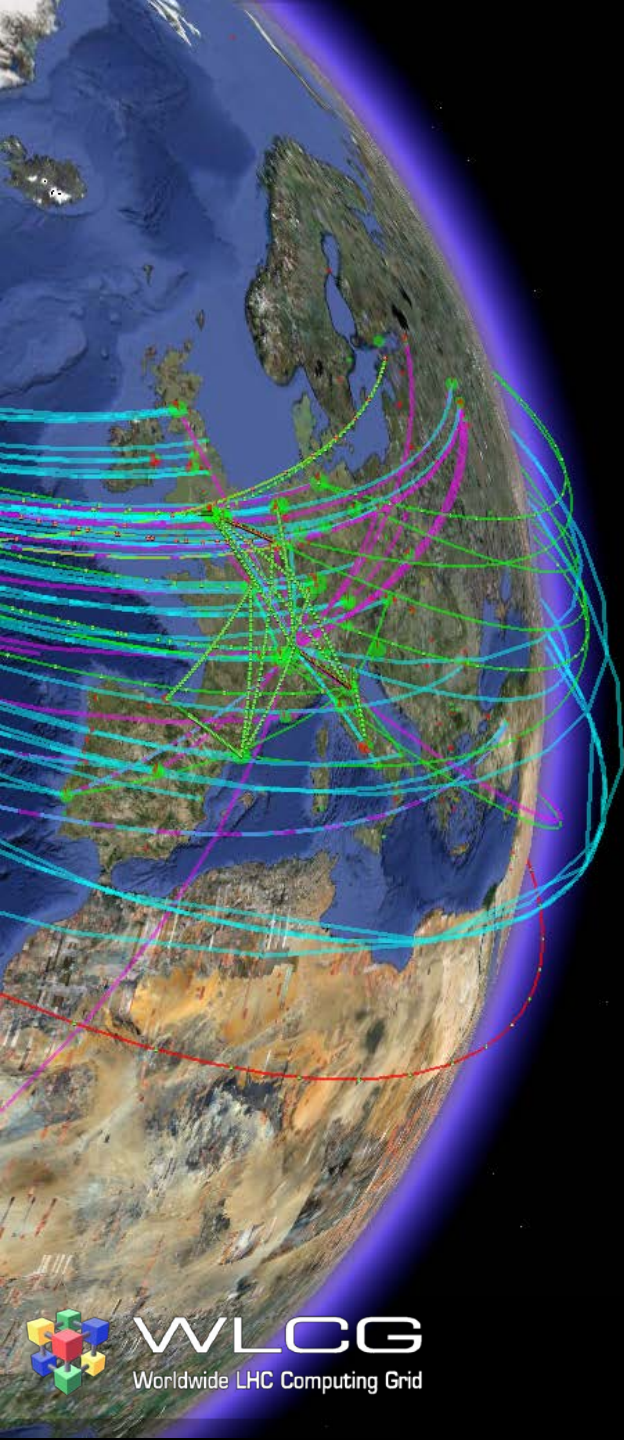
- Lots of services *protected* by old versions
- Most vulnerable (web)sites fixed promptly
 - Thanks!
- Client certificates can't be leaked on servers
- Still pending: clients vulnerability:
 - Hard to detect
 - Hard to abuse (require MITM)

X509 Validation

TABLE V: Semantic discrepancies in certificate validation (incorrect answers in **bold**)

Problem	Certificates triggering the problem occur in the original corpus	OpenSSL	PolarSSL	GnuTLS	CyaSSL	MatrixSSL	NSS	OpenJDK, Bouncy Castle	Browsers
Untrusted version 1 intermediate CA certificate	No	reject	reject	accept	reject	accept	reject	reject	reject
Untrusted version 2 intermediate CA certificate	No	reject	reject	reject	reject	accept	reject	reject	reject
Version 1 certificate with valid basic constraints	No	accept	reject	accept	accept	accept	reject	reject	Firefox: reject Opera, Chrome: accept
Intermediate CA not authorized to issue further intermediate CA certificates, but followed in the chain by an intermediate CA certificate	No	reject	reject	reject	reject	accept	reject	reject	reject
... followed by a leaf CA certificate	No	reject	reject	accept	reject	accept	reject	reject	reject
Intermediate CA not authorized to issue certificates for server's hostname	No	reject	reject	accept	accept	accept	reject	reject	reject
Certificate not yet valid	Yes	reject	accept	reject	reject	reject	reject	reject	reject
Certificate expired in its timezone	Yes	reject	accept	reject	reject	accept	reject	reject	reject
CA certificate not authorized for signing other certificates	No	reject	reject	accept	accept	accept	reject	reject	reject
Server certificate not authorized for use in SSL/TLS handshake	Yes	reject	accept	accept	accept	accept	reject	reject	reject
Server certificate not authorized for server authentication	Yes	reject	accept	accept	accept	accept	reject	reject	reject
Certificate with unknown critical extension	No	reject	reject	accept	accept	accept	reject	reject	reject
Certificate with malformed extension value	No	accept	reject	accept	accept	accept	reject	reject	reject
Certificate with the same issuer and subject and a valid chain of trust	No	reject	reject	accept	reject	accept	reject	reject	reject
Issuer name does not match AKI	No	reject	accept	accept	accept	accept	reject	reject	reject
Issuer serial number does not match AKI	No	reject	accept	reject	accept	accept	reject	reject	reject

Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations Chad Brubaker and Suman Jana



Windigo

Windigo

- Large scale malicious operation
 - Targeting mainly servers
 - Without using 0-days or vulnerability (mostly)
- Two parts:
 - Botnet building
 - Botnet exploitation (making money)

Botnet building: Ebury

- Ebury already presented during last HEPiXs
- Two versions:
 - Malicious SSHD binary (old version)
 - Malicious libkeyutil library (loaded for sshd)
- Malicious activity:
 - Backdoor based on magic ssh version string
 - Credential Exfiltration

Ebury Exfiltration

- Credentials exfiltrated:
 - Password from compromised servers
 - Password to compromised servers
 - Private ssh keys from compromised servers
- Exfiltration:
 - Encoded *DNS* query: passwords & username
 - Shared memory: private keys & passwords

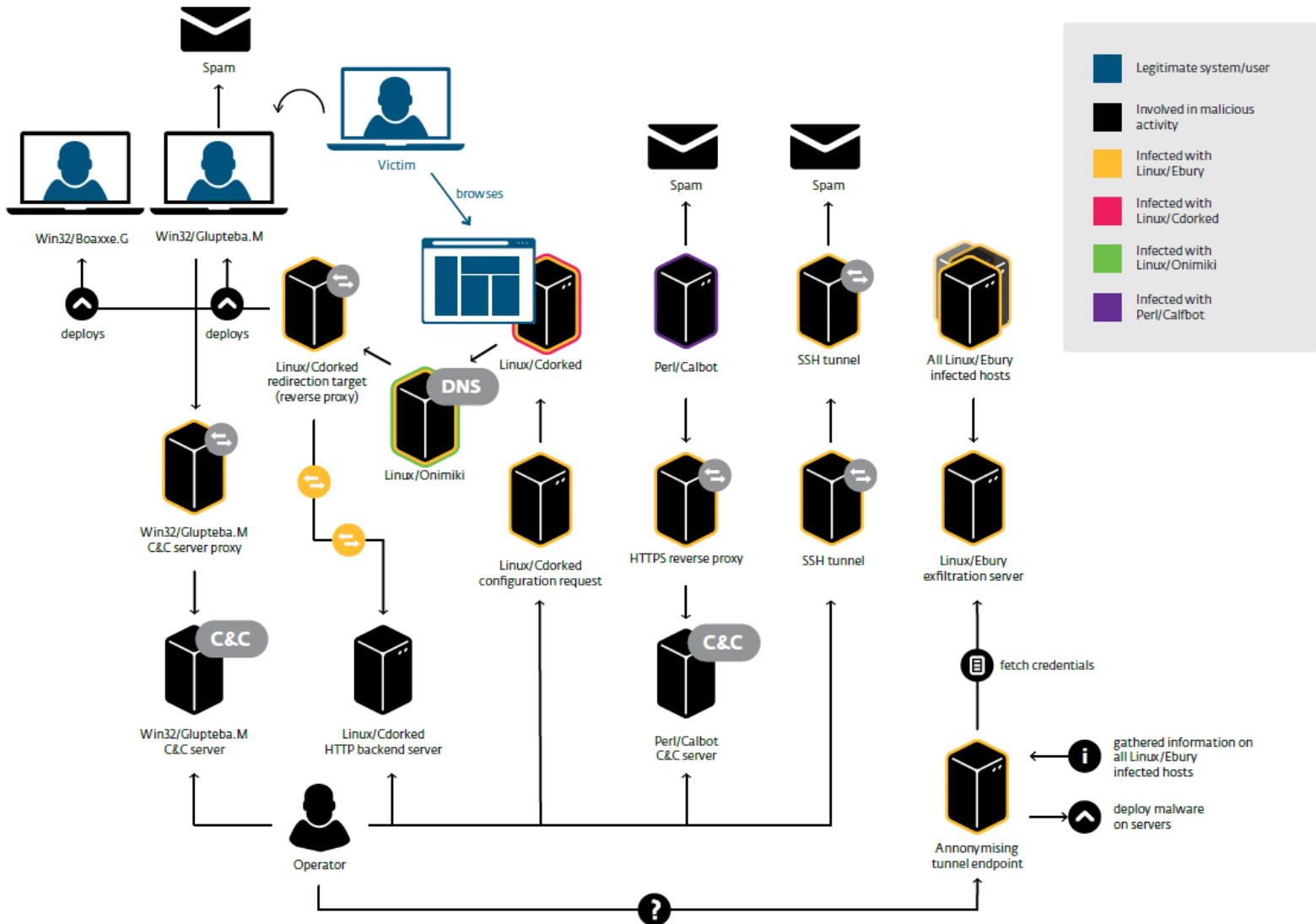
Ebury Exfiltration

- *DNS* queries:
 - Domain Generation Algorithm: identify server
 - Protections:
 - Redundancy (old): compare 2 requests
 - Signature (new): Sign exfiltration IP with private key
- Shared memory
 - Every credential is stored to memory
 - Backdoor ('cat') used to fetch them
 - Easily identifiable (0666 & big): recently *fixed*

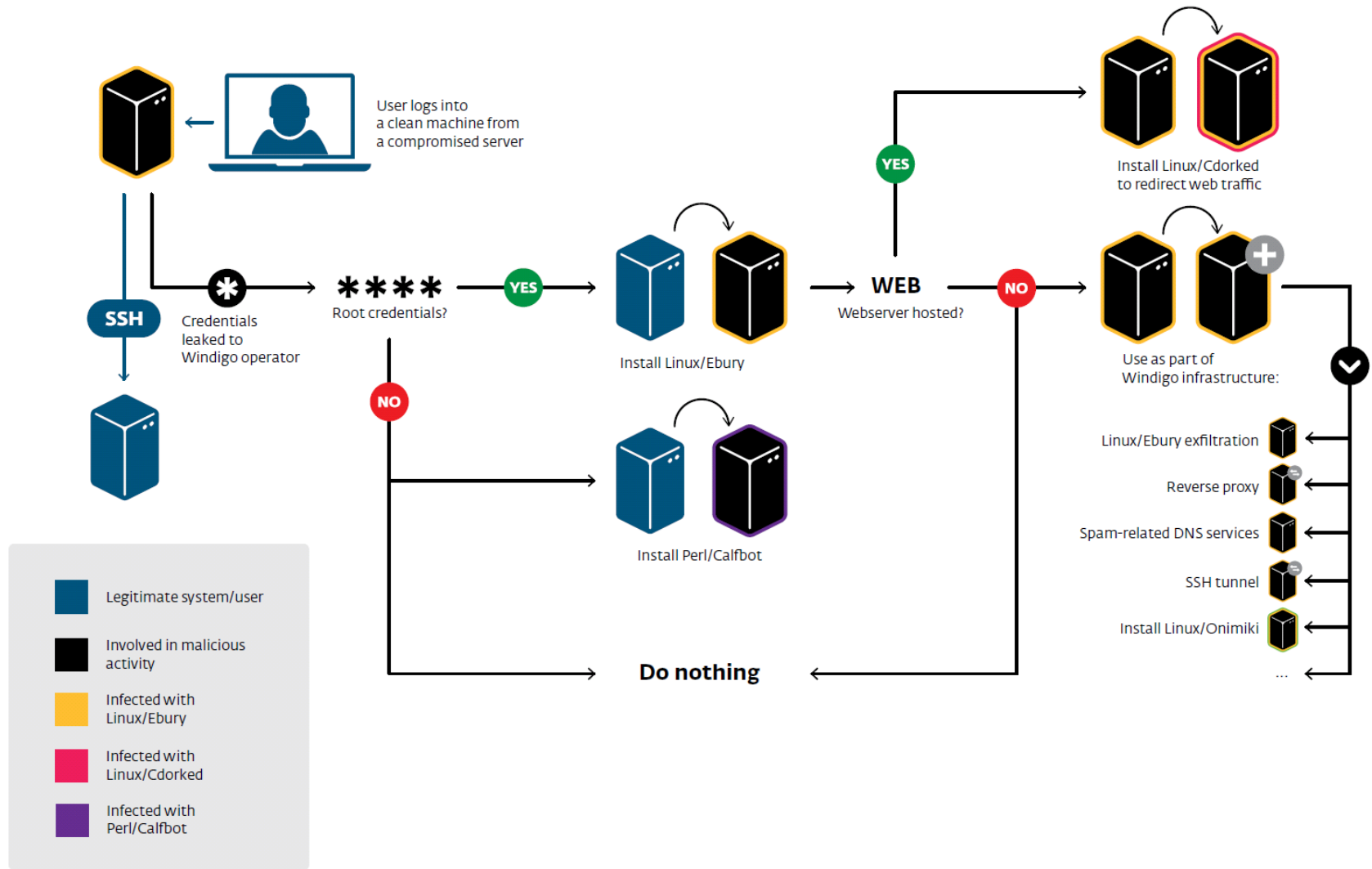
Botnet exploitation

- Send spam from the backdoor
- Perl/Calfbot: send spam from servers
- Linux/Cdorked:
 - Redirect users to malicious websites
 - Infects clients & sent spam
- Activity dissimulation (proxy)

Botnet exploitation



Botnet propagation

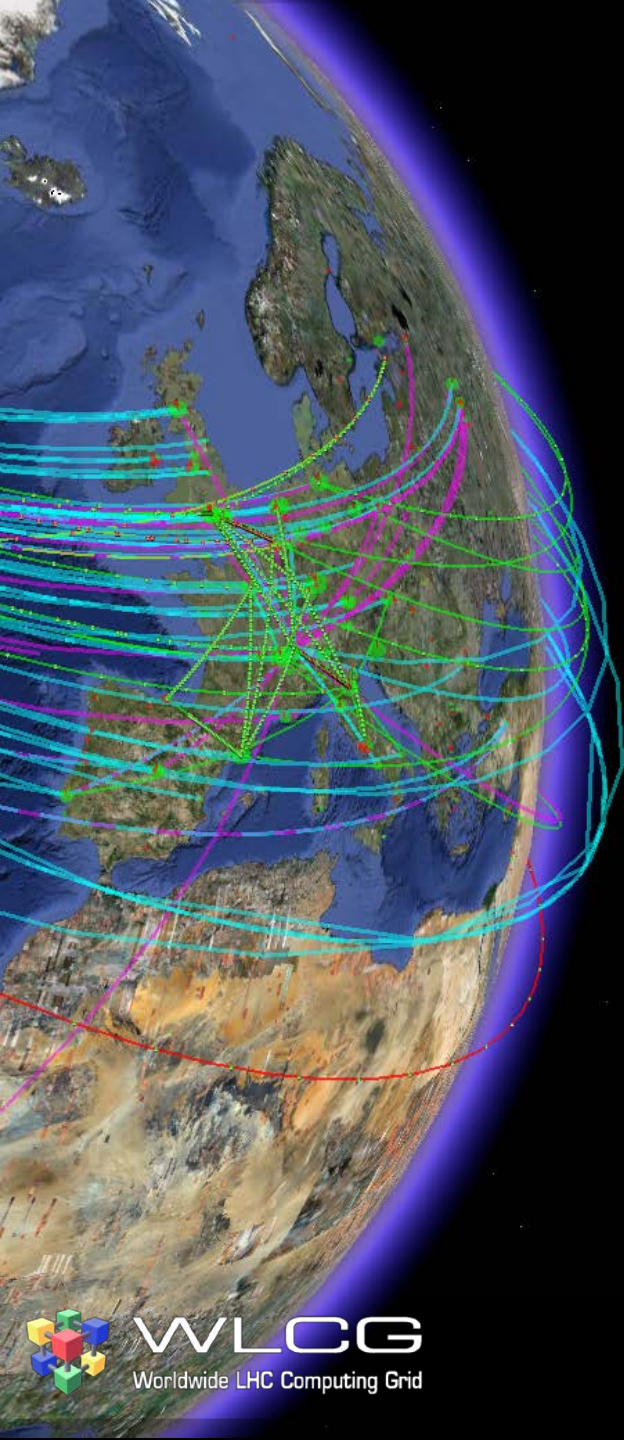


Grid ?

- No infection so far in EGI !
- Stay careful: could easily propagate

Protection/Detection

- Protection:
 - Kerberos authentication not targeted
 - 2 factor authentication
- Detection:
 - rpm -Va (at least keyutils-libs & openssh-server)
 - <https://github.com/eset/malware-ioc>



New threat

Surveillance

- Theoretical physics is not protected: international center in Italy targeted!

NSA Revelations: ICTP, Honduran Resort, Telecoms & More. [Edward Snowden](#) revelations to the French newspaper “**Le Monde**” break the wall of silence and inaction of the government on the Italian scandal erupted following the revelations of **Edward Snowden**.

The Parisian newspaper [has revealed a new espionage operation](#) of the communications made by the **National Security Agency (NSA)** to the detriment of the International Centre for Theoretical Physics in Trieste: **the ICTP**, one of the most prestigious scientific institutes in the world dedicated to the Pakistani physicist and Nobel laureate Abdus Salam.

Despite its truly international character, the ICTP in Trieste is in all respects an Italian research center and owes its existence and its operations to finance the government, which, however, is silent on the case. A silence now constant since the beginning of the scandal that Datagate, such as “L’Espresso” has written for months, also cover Italy, as evidenced by [the top secret documents Snowden inspected by our newspaper](#) and files that the American journalist **Glenn Greenwald** [has shared with L’Espresso](#) on programs of mass surveillance of the NSA who have also targeted our country.

© usnewsghost.wordpress.com

Hardware interception



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

Cisco CEO to Obama: Don't let NSA intercept and hack our gear

Chambers says alleged TAO program undermines industry.



Man In The Middle



Further improving digital certificate security

Saturday, December 7, 2013 11:43 AM

Posted by Adam Langley, Security Engineer

Late on December 3rd, we became aware of unauthorized digital certificates for several Google domains. We investigated immediately and found the certificate was issued by an [intermediate certificate authority](#) (CA) linking back to ANSSI, a French certificate authority. Intermediate CA certificates carry the full authority of the CA, so anyone who has one can use it to create a certificate for any website they wish to impersonate.

In response, we updated Chrome's certificate revocation metadata immediately to block that intermediate CA, and then alerted ANSSI and other browser vendors. Our actions addressed the immediate problem for our users.

ANSSI has found that the intermediate CA certificate was used in a commercial device, on a private network, to inspect encrypted traffic with the knowledge of the users on that network. This was a violation of their procedures and they have asked for the certificate in question to be revoked by browsers. We updated Chrome's revocation metadata again to implement this.

Questions ?

