Evolution of Computer Security Threats and Models

Vincent Brillault

(CERN Computer Security Team)

GridKa School, 2014/09/01

What is Computer Security?

- **Handling security incidents**
  - Policies
  - Investigation & forensics
  - Cooperation & coordination
- **Not (really) part of this presentation**

- **Preventing security incident**
  - Architecture/software design & implementation
  - *Hardening* of existing architecture/software
- **Against what, why, how and up to what level?**

Improving Security

- ► **Evaluate the situation (Risk assessment)**
  - ► Who are the attackers? What do they want?
  - ► What are your assets?
  - ► What are the threats?
  - ► What are the consequences?

- ► **Seal most dangerous holes & re-evaluate**

Security Continuous Integration

- **Evaluate the situation (Risk assessment)**
  - Who are the attackers? What do they want?
  - What are your assets?
  - What are the threats?
  - What are the consequences?

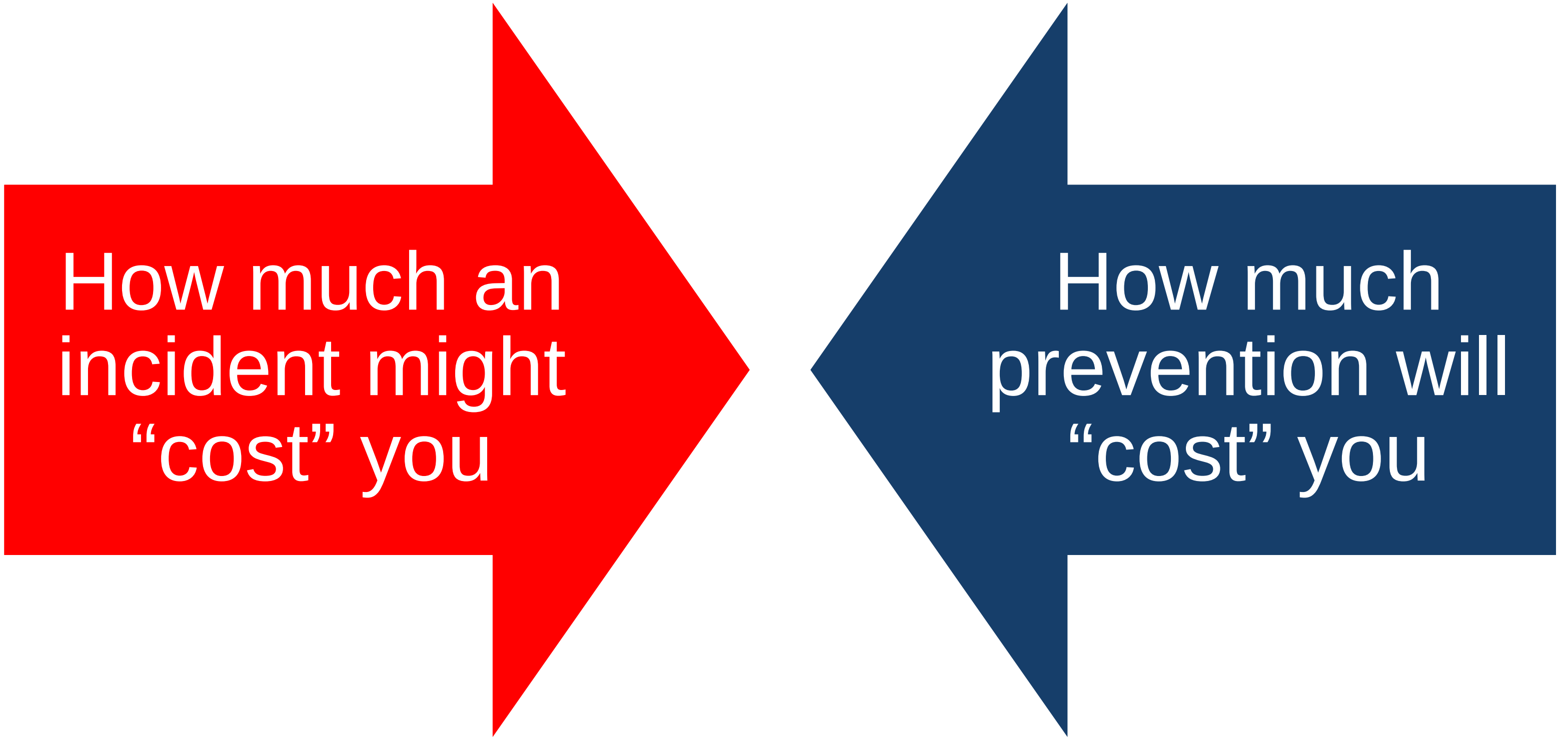
- **Seal most dangerous holes & re-evaluate**

- **Service Agility: Impact of new services/features?**

- **Follow attacker evolutions & re-evaluate:**
  - Are there new attackers?
  - Are there new attacks, new trends?

Finding the correct equilibrium

► Compromises & equilibrium:

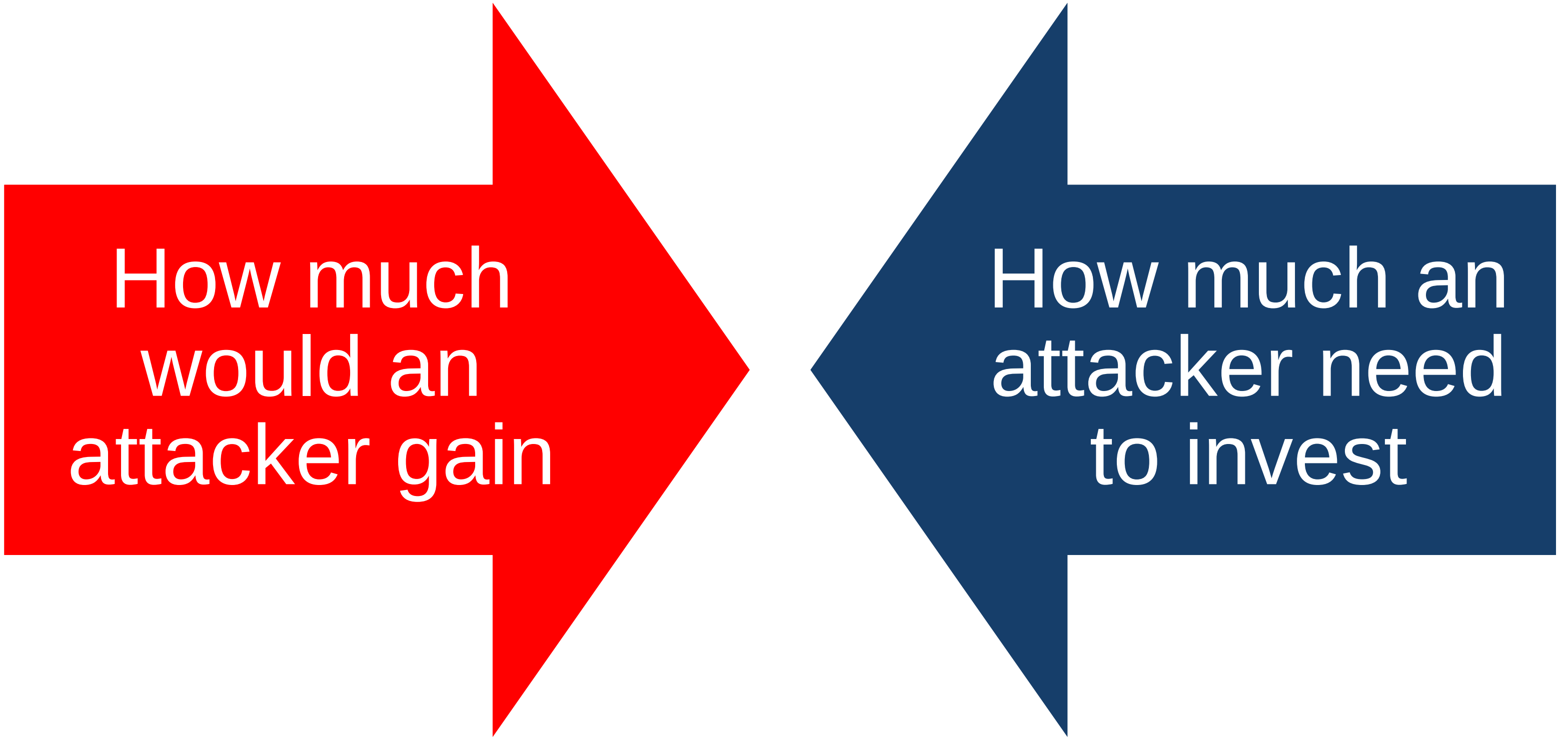


How much an incident might “cost” you

How much prevention will “cost” you

Finding the correct equilibrium

► Compromises & equilibrium:



How much would an attacker gain

How much an attacker need to invest

What are attackers after?

- **Bragging & Reputation**
  - Attack well known entities
  - Try to get as much exposure as possible
  - Can create noise about any “hack”, even insignificant ones
- **Difficult to prevent, damage control required**

- **Political & ideological goal (Hacktivists)**
  - Mostly anything can be a target
  - Sometime similar to standard bragging
- **Difficult to prevent, damage control required**

- **Money (professional hackers)**
- **Rational, methodic**

How to make money from hacking?

Stolen resources:

- Sell resources to other ‘business’ partners
  - Send spam (non-legitimate business offers)
  - Send phishing:
    - Malware (malicious attachments)
    - Forged forms asking for passwords
    - Links to Phishing Web pages
  - DDOS: Use distributed resources to disturb (public) services
- Host malicious content:
  - Phishing web sites (steal more credentials)
  - Malicious architecture (hide your tracks & high availability)
- Inject malicious links/ads/content to existing websites
- Mine crypto-currencies

How to make money from hacking?

- **Infected computers**
  - Ads & popups
  - Pay per install software
  - Blackmail (including Crypto-lockers)
  - Banking malware
  - Steal credentials

- **Stolen data**
  - Sell credit card numbers
  - Sell users private data (for phishing and social engineering)
  - Sell corporate data

New variable:
Crypto-currencies

Crypto-currencies

► Fully functional currencies:

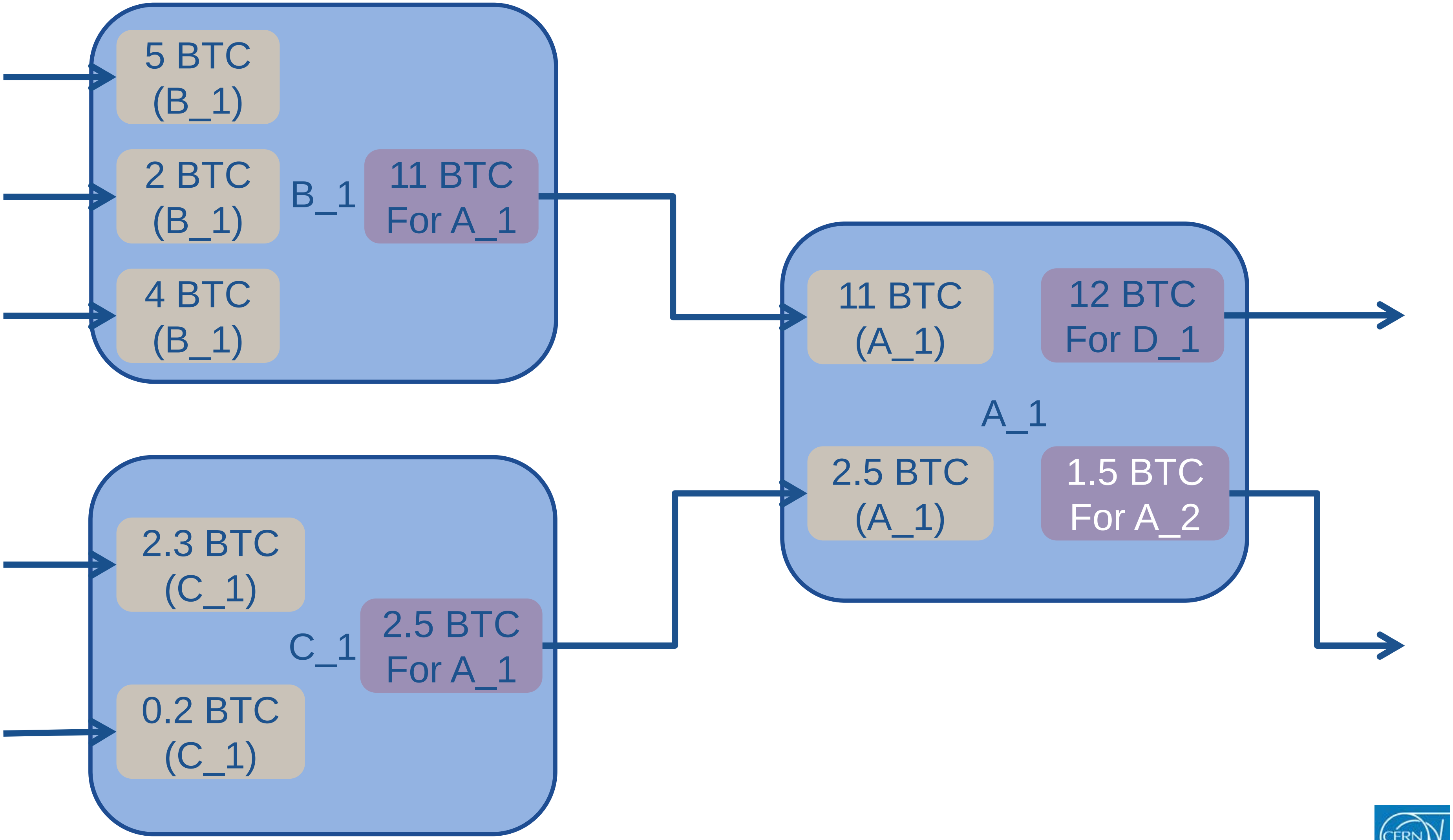
- ► Concepts of *accounts*, transactions
- ► Double-spending impossible

► No ‘banks’ required (but some exist):

- ► Accounts are auto generated:
  - ▪ Private key (used to sign transaction)
  - ▪ Address (derived from private key)
- ► Transactions are *verified* by miners

► Exchanges with *real* currencies

Transactions everywhere (chains)

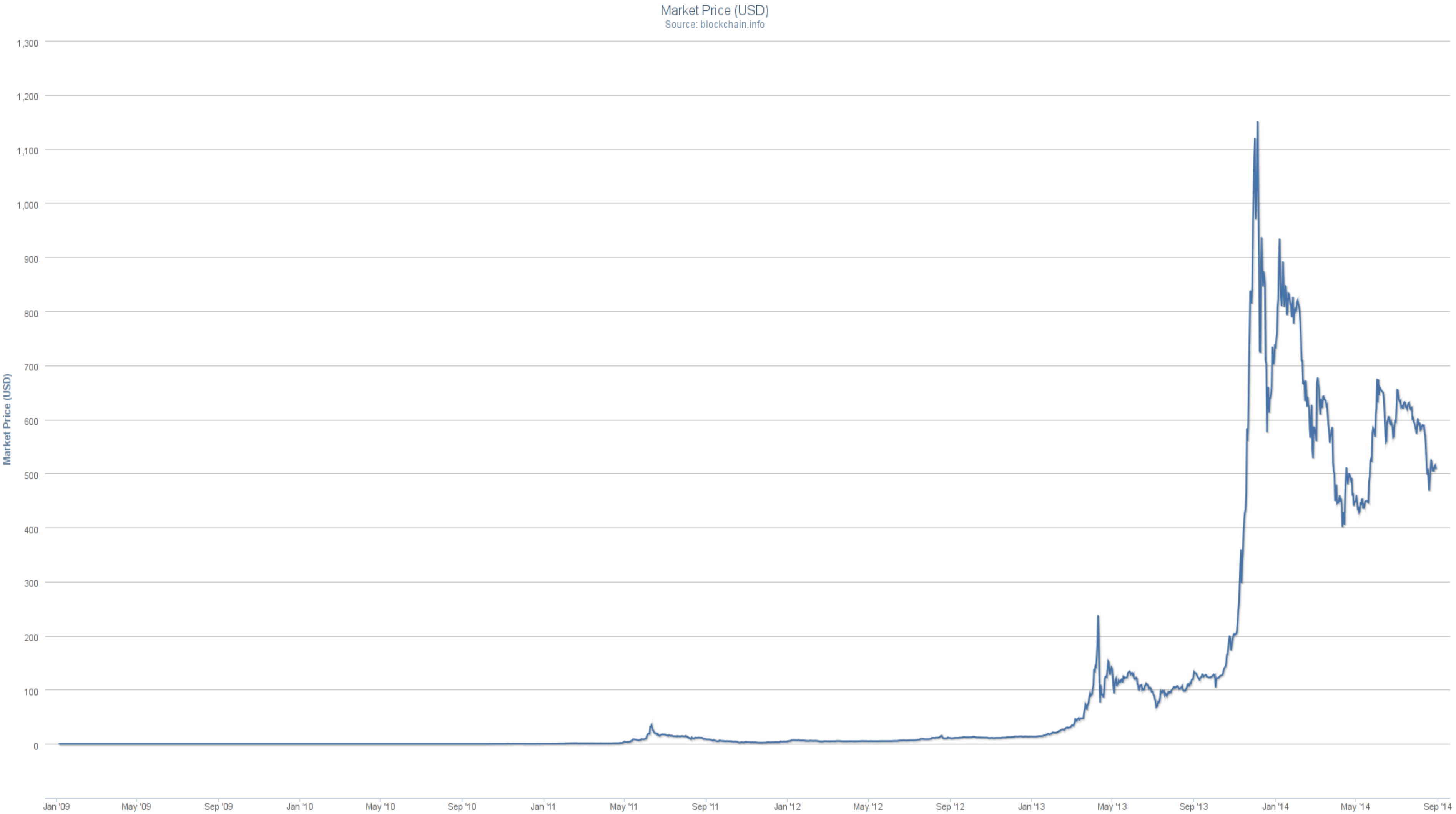


Block Chain & Miners

- **Block:**
  - Contains aggregated valid transaction
  - *Proof of work*: hard computing problem
    - BTC: hash(block) < target

- **Miners:**
  - Hash blocks until someone find good one
  - Paid:
    - Per solved block
    - Per transaction (if it included a mining fee)

Change rate (BTC-USD) explosion



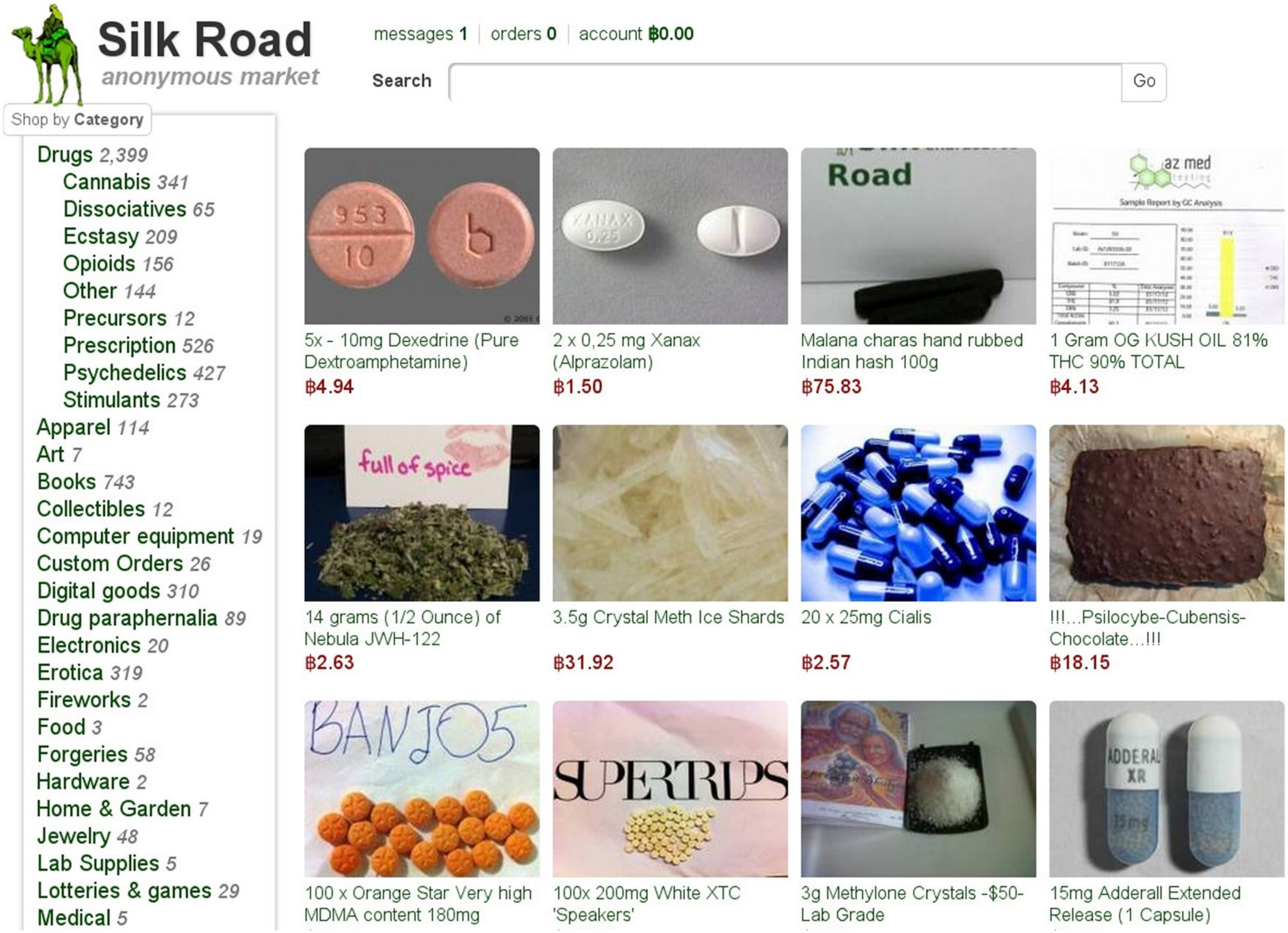
Crypto-currencies: Security implications

- **Easy and *reliable* way to make money from [CG]PU**

- **Very low traceability:**
  - No link address <-> user (except currency exchanges)
  - *Laundering*: create new addresses and move coins

- **Publicly verifiable transactions with no middleman**

Bitcoin explosion: *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

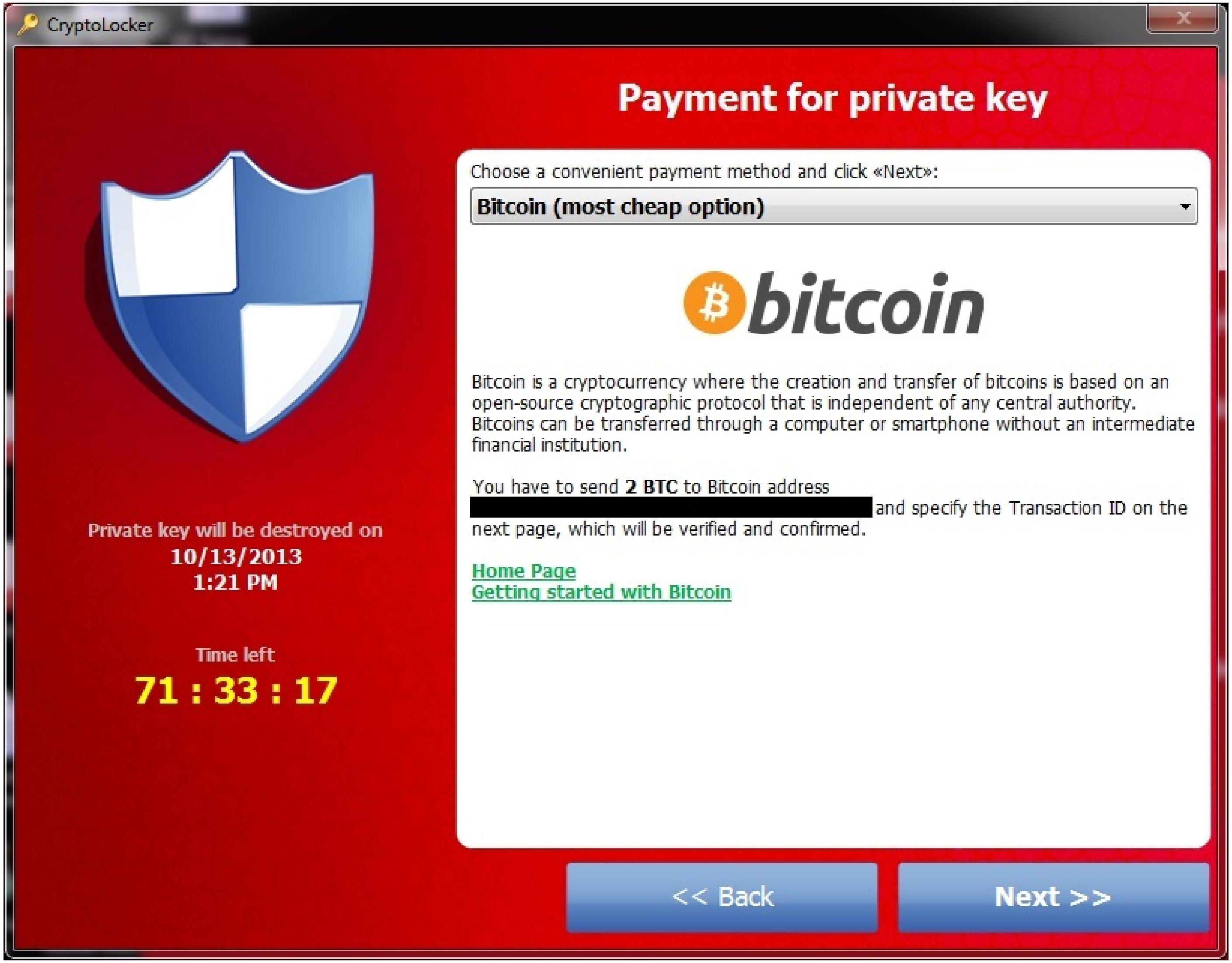
100 x Orange Star Very high MDMA content 180mg

100x 200mg White XTC 'Speakers'

3g Methylone Crystals -$50- Lab Grade

15mg Adderall Extended Release (1 Capsule)

Bitcoin explosion: *interesting* transactions



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.

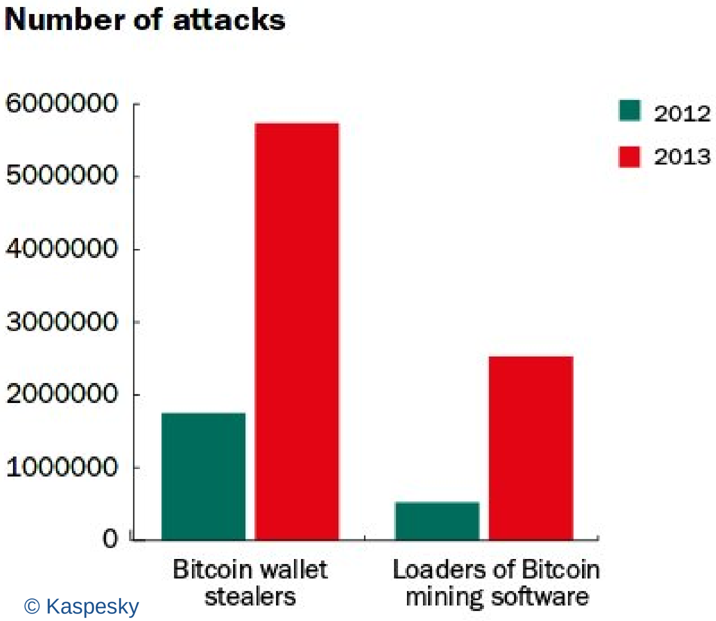
You have to send **2 BTC** to Bitcoin address [redacted] and specify the Transaction ID on the next page, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

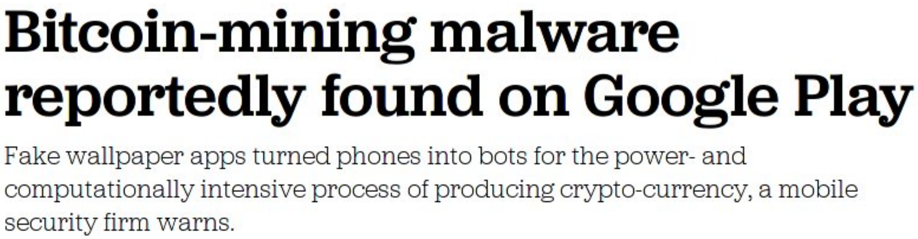
Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 33 : 17

Bitcoin explosion: malware boom

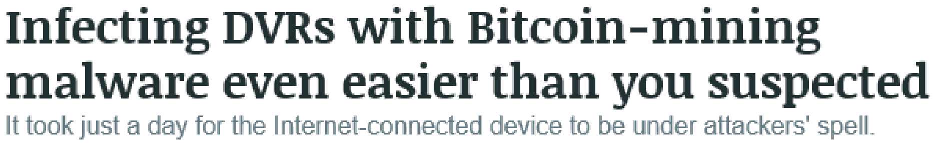


© Kaspesky



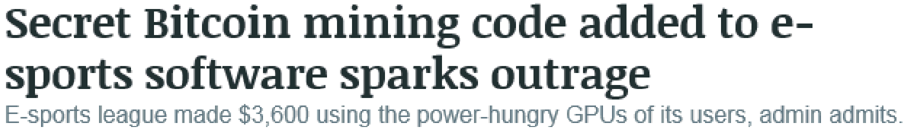
Bitcoin-mining malware reportedly found on Google Play

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



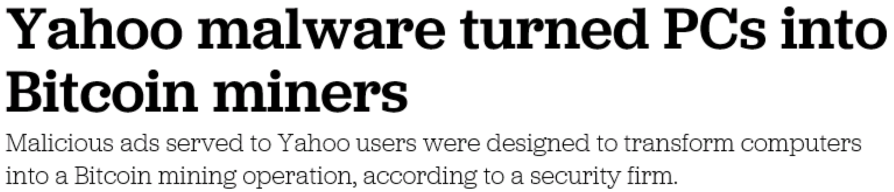
Infecting DVRs with Bitcoin-mining malware even easier than you suspected

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.

Crypto-currency: Security Impact

► Not really a standard threat

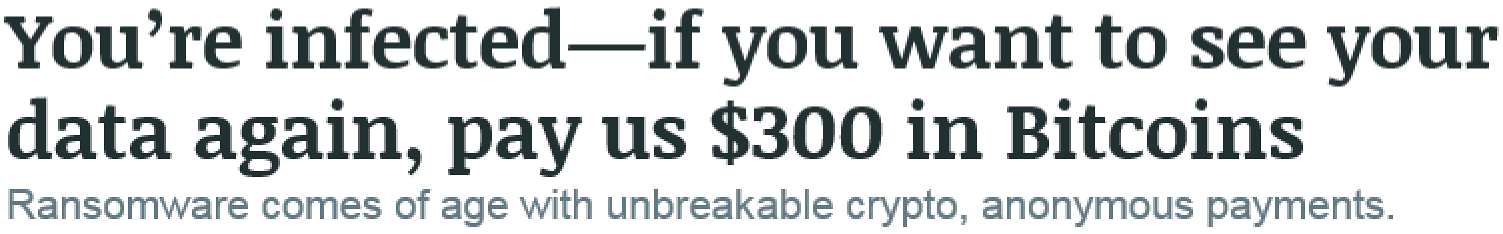
- ► Small disruption (consuming resources)
- ► No real impact on system integrity
- ► Interesting way of detecting a compromise: 100% CPU

► BUT: insider threat

- ► What prevent users to mine crypto-currencies?
- ► What are the consequences of mining?

New threat:
Crypto-lockers

What is Cryptolocker?



You’re infected—if you want to see your data again, pay us $300 in Bitcoins

Ransomware comes of age with unbreakable crypto, anonymous payments.

- **No infection method by itself (run by something else)**

- **Impressive blackmail:**
  - Use proper cryptography to encrypt all interesting files
  - Increase pressure: threat to delete private key

- **‘Standard’ business: only few reports of non-decryption**

- **Enormous results: > 40’000 BTC**

Cryptolocker prevention

- **Do backups:**
  - Backups on an external system (e.g. tape backups)
  - Off line backups

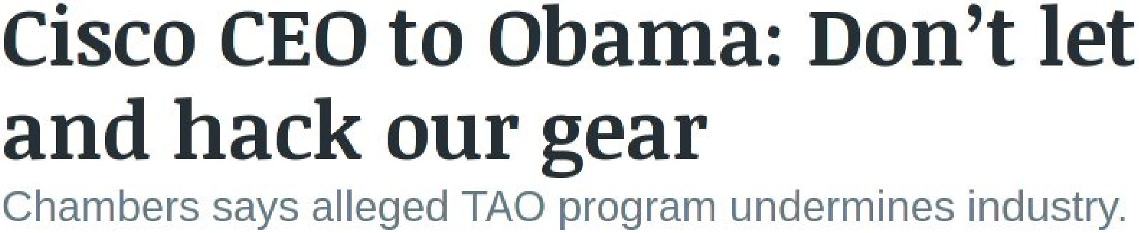
- **Follow the ‘Least Privilege Principle’:**
  - Give ‘Read only’ accesses when possible (e.g. websites)
  - Remove outdated permissions

- **Never pay**
  - Paying increase the incentive to make malware
  - There is no proof they will give you data back or won’t re-attack you
  - Crypto-locker case: private key database discovered!

New *Attackers*: Nations

Hardware interception

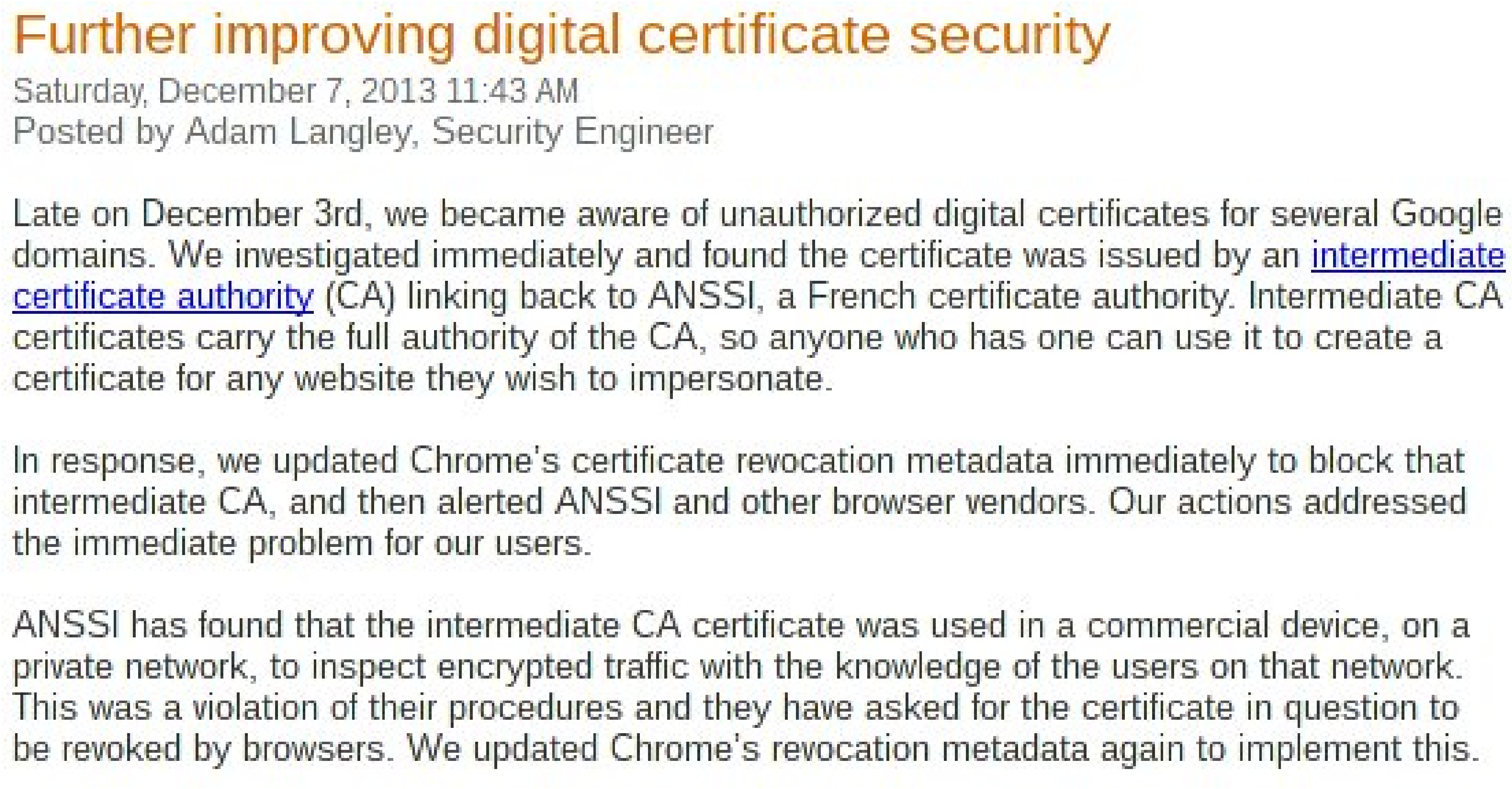
(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon



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.

Nations: Security Threats?

- **Lot of reports of mass surveillance programs**
  - Data interception
  - Hardware backdoors
  - …

- **Examples of malwares used by law enforcement**

- **From our point of view:**
  - Able to spend *unlimited* resources
  - Goal/potential damage unclear

- **Nothing special to do**

Why Computer Security is broken: SSL/TLS example

What is SSL/TLS?

► Communication layer ensuring:

- ► Confidentiality: nobody can read the exchanged data
- ► Authenticity: you know who you are talking to
- ► Integrity: nobody can change your messages

► Used almost everywhere:

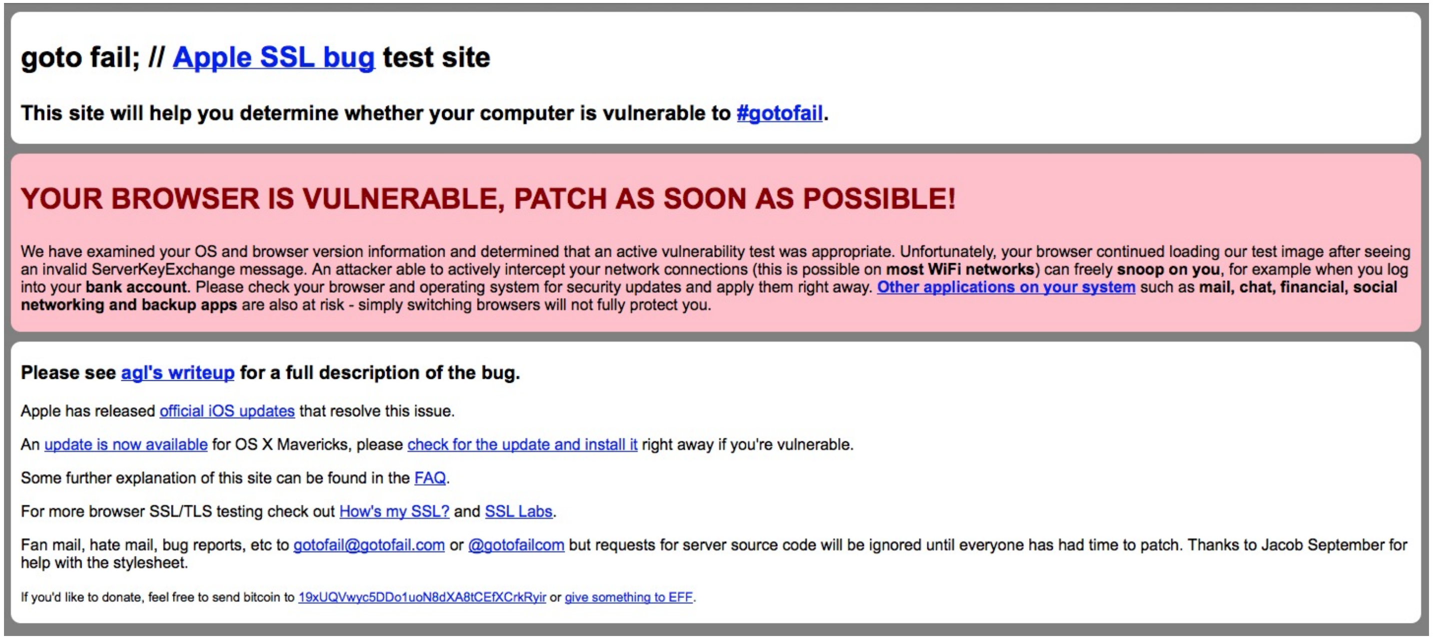
- ► ‘s’ in HTTPs, SMTPs, IMAPs…
- ► Implemented in Linux, Windows, Mac OS

► History:

- ► SSL, SSL v2, SSL v3
- ► TLS1.0, TLS1.1, TLS1.2, (TLS 1.3)

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.

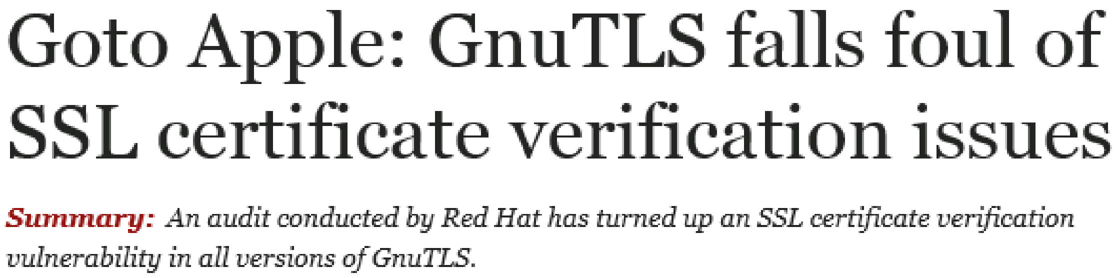
Some further explanation of this site can be found in the FAQ.

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 19xUQVwyc5DDo1uoN8dXA8tCEfXCrkRyir or give something to EFF.

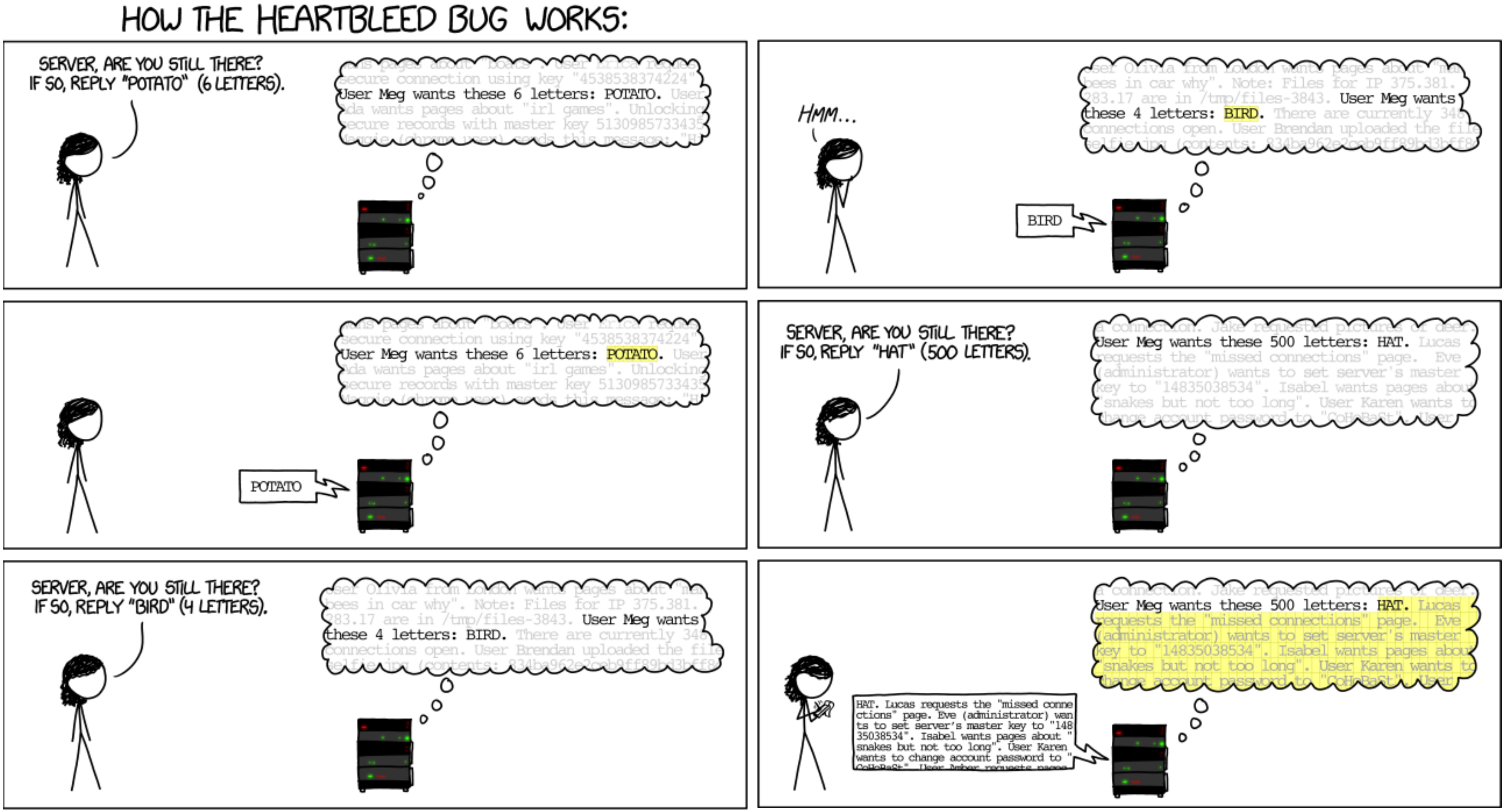
► GNUTLS: Wrong certificate validation



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 (OpenSSL)


HOW THE HEARTBLEED BUG WORKS:
SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).
ants pages about "boats". User Erica requests secure connection using key "4538538374224". User Meg wants these 6 letters: POTATO. User Ada wants pages about "irl games". Unlocking secure records with master key 5130985733435. Maggie (chrome user) sends this message: "H
HMM...
User Olivia from London wants pages about "ma bees in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 348 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
BIRD
ants pages about "boats". User Erica requests secure connection using key "4538538374224". User Meg wants these 6 letters: POTATO. User Ada wants pages about "irl games". Unlocking secure records with master key 5130985733435. Maggie (chrome user) sends this message: "H
POTATO
SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).
User Olivia from London wants pages about "ma bees in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 348 connections open. User Brendan uploaded the file selfie.jpg (contents: 834ba962e2ceb9ff89bd3bff8
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User Amber requests pages

© XKCD

Costs

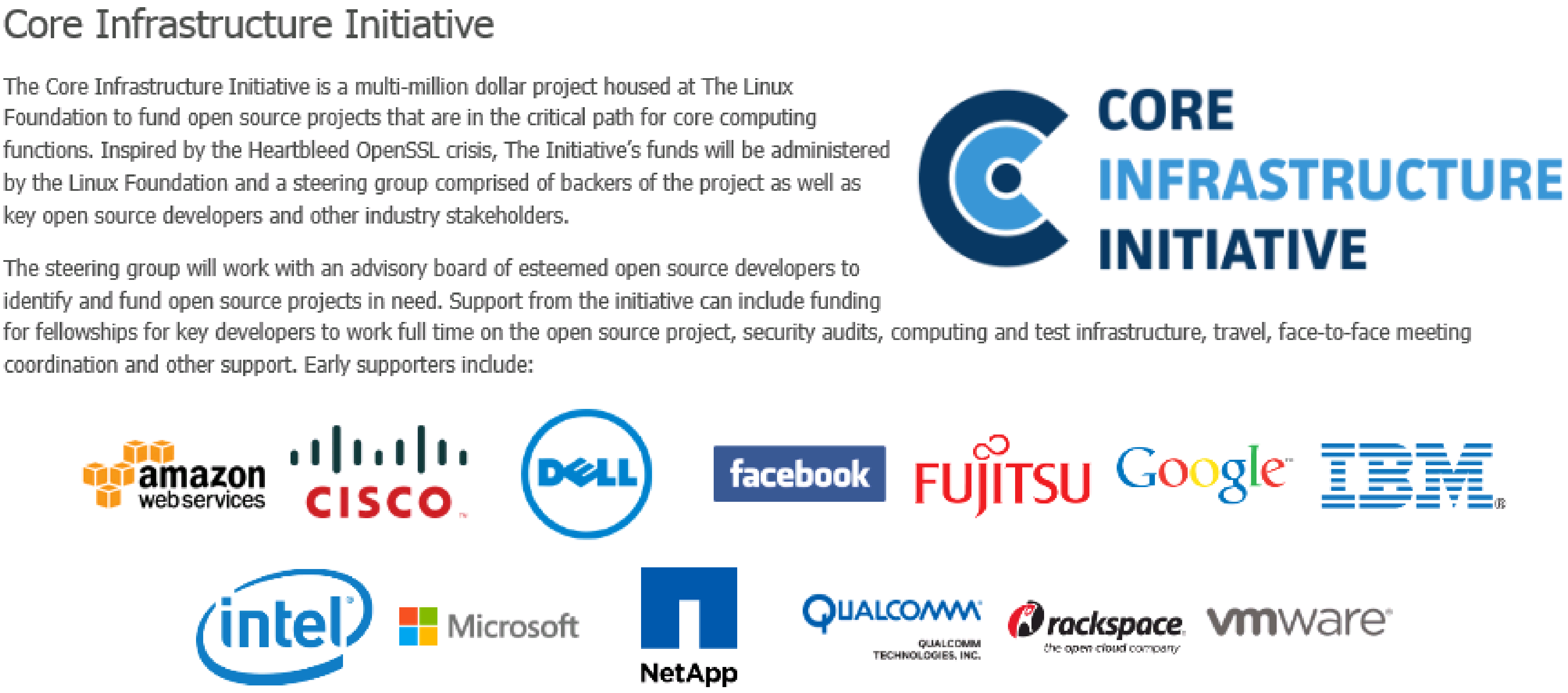
- **Apple & GNUTLS: Man In The Middle:**
  - Someone could intercept and modify protected data
  - Mainly a client issue, not a server issue

- **Heartbleed: Stealing data from servers (& clients)**
  - Stealing users passwords
  - Stealing server privates keys
- **Long term impact unknown:**
  - Stolen passwords & keys could still be valid
  - Recent discovery of (old) attacks using Heartbleed

Reasons for failures

- **Apple: basic programming issue**
- **GNUTLS: wrong return value**
- **Heartbleed:**
  - Basic input validation missing
  - OpenSSL maintained by few peoples
- **Bad quality code everywhere?**
  - Software has no guaranty: if it breaks, bad luck…
  - Programmers not responsible: only expected to patch quickly!

Heartbleed: Lesson learned?



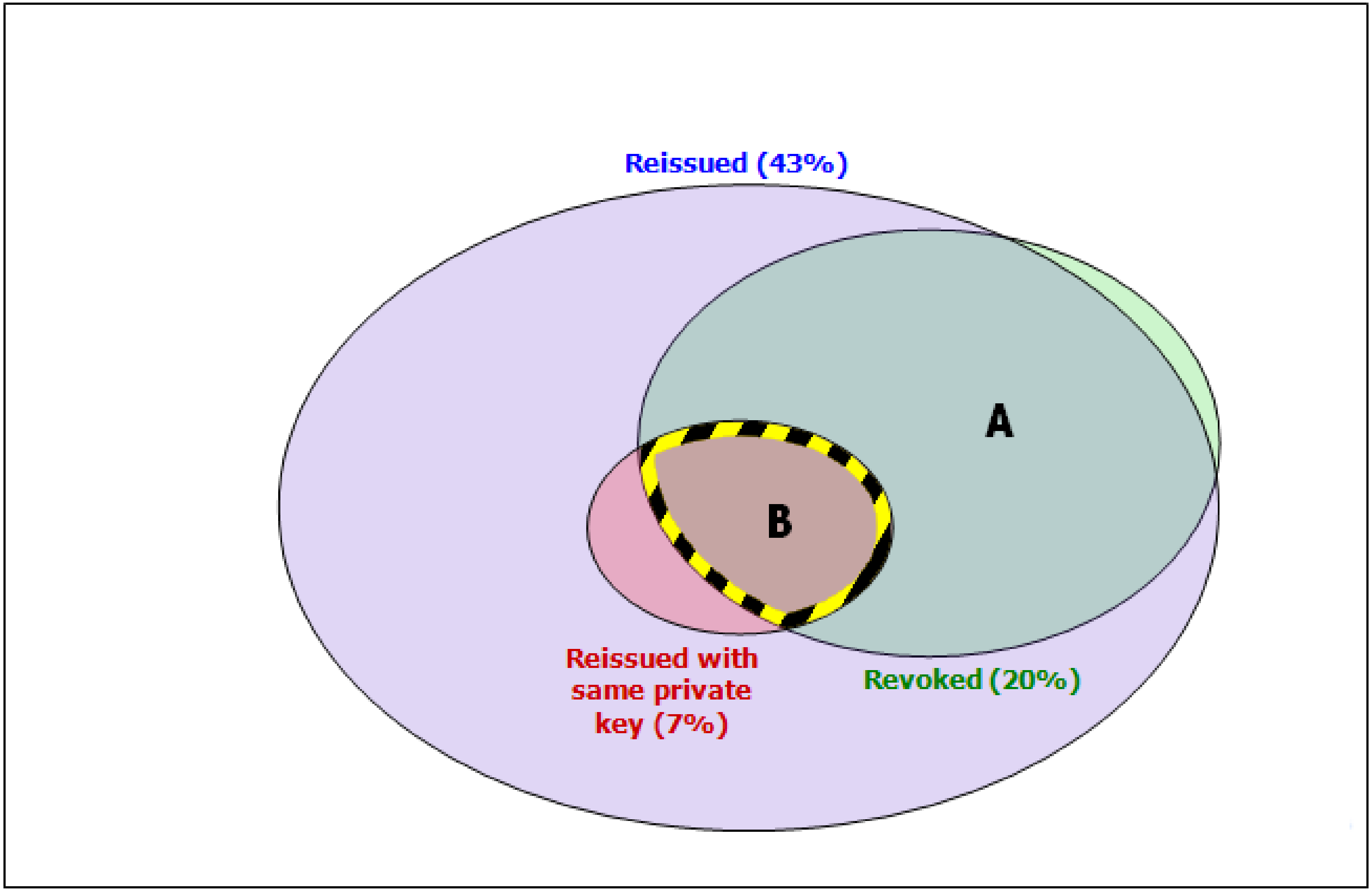
Core Infrastructure Initiative

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:

Heartbleed: fixed? (1 month later)

All websites affected by the Heartbleed bug



THANKS FOR COMING!

QUESTIONS?

Good old method: credential theft, Windigo

What is Windigo?

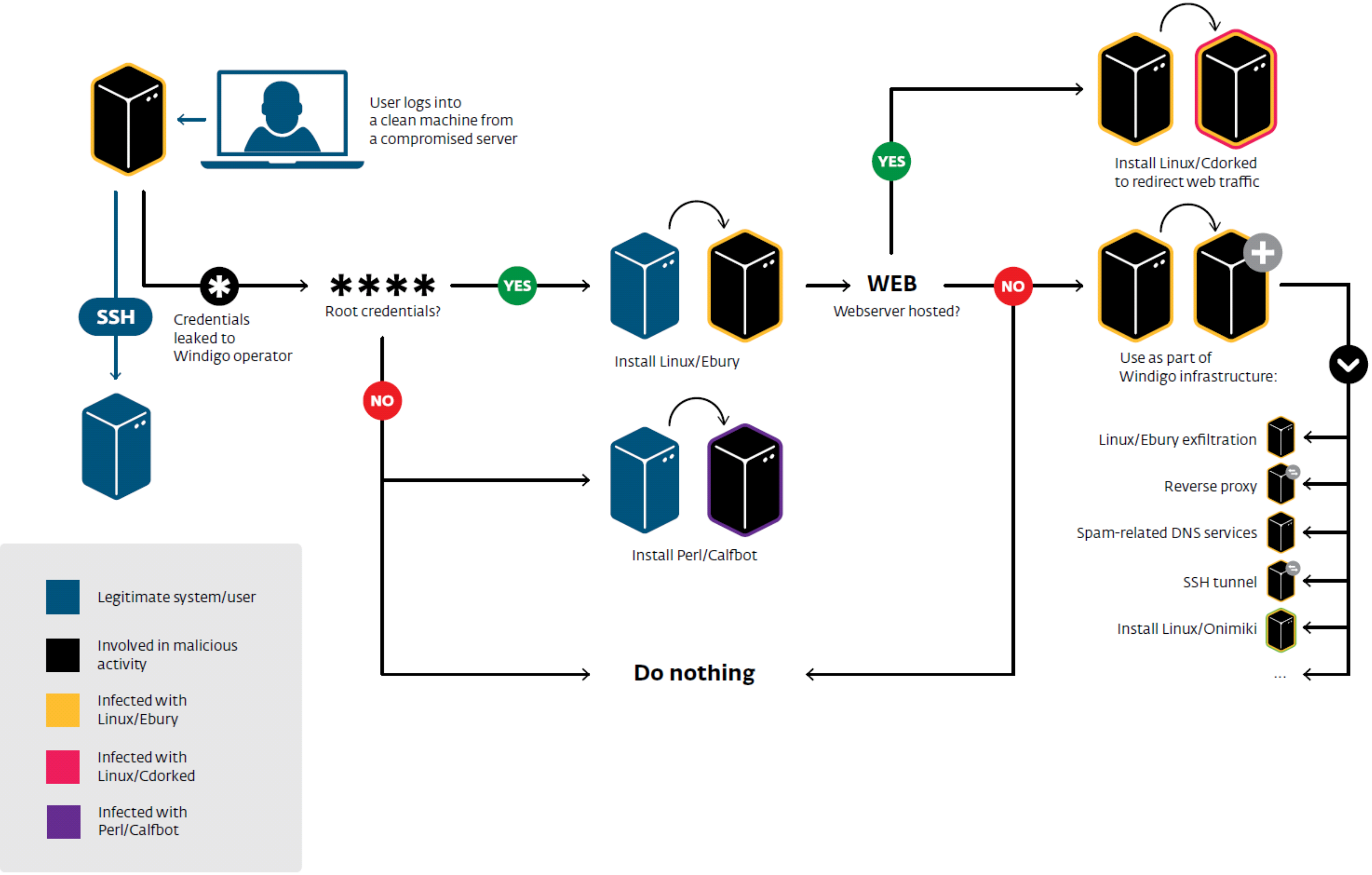
▶ Large scale malicious operation

- ▶ Targeting mainly servers
- ▶ Without using 0-days or vulnerability (mostly)

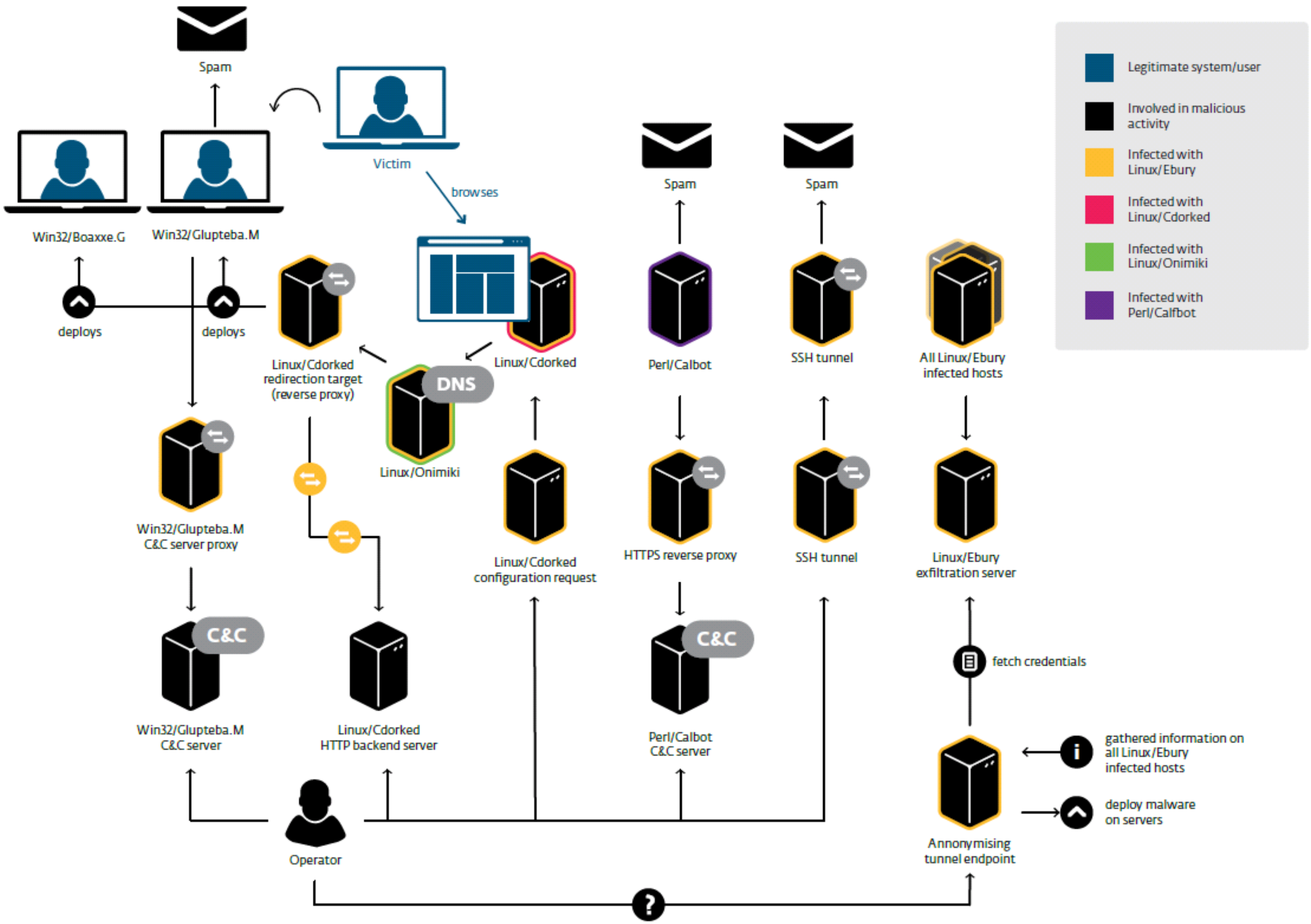
▶ Botnet building: Ebury

- ▶ Openssh Backdoor
- ▶ Stealing credential used for Openssh:
  - Password
  - SSH private keys
- ▶ Credential exfiltration:
  - Pushed to malicious servers (pseudo DNS queries)
  - Pulled by operators (stored locally)

How does Windigo grow?



Making money out of Windigo?


Spam
Victim
browses
Win32/Boaxxe.G
Win32/Glupteba.M
deploys
deploys
Linux/Cdorked redirection target (reverse proxy)
Linux/Cdorked
DNS
Linux/Onimiki
Spam
Spam
Perl/Calbot
SSH tunnel
All Linux/Ebury infected hosts
Win32/Glupteba.M C&C server proxy
Linux/Cdorked configuration request
HTTPS reverse proxy
SSH tunnel
Linux/Ebury exfiltration server
C&C
Win32/Glupteba.M C&C server
Linux/Cdorked HTTP backend server
C&C
Perl/Calbot C&C server
fetch credentials
gathered information on all Linux/Ebury infected hosts
deploy malware on servers
Operator
Annonymising tunnel endpoint
?
Legitimate system/user
Involved in malicious activity
Infected with Linux/Ebury
Infected with Linux/Cdorked
Infected with Linux/Onimiki
Infected with Perl/Calbot