Anonymity Fails
Good shoes won’t save you this time!

http://www.olografix.org
info@olografix.org
associazione culturale telematica
metro olografix

fed.lag@protonmail.ch
last@olografix.org

AGENDA

- Case Study 1: DPR
  - Contaminazione identità
  - Sicurezza IRL
- Case Study 2: Eldo Kim
- Attacchi a correlazione
- Q&A

CUI PRODEST?

- Pentesters con interesse a migliorare sotto il profilo della “stealthiness”
- Gray Hats che vogliano segnalare falle senza essere identificati
- Interessati all’argomento dell’anonimato in generale

/* STANDARD DISCLAIMER GOES HERE */

CASE STUDY 1

Ross Ulbricht a.k.a. Dread Pirate Roberts

Silk Road

anonymous marketplace

Who, what, when, where, why

- Ross Ulbricht decide di creare una simulazione econimica, ossia un market “anonimo” basato su criptovaluta in cui vendere vari “beni”
- Silk Road va online dal 2011 al 2013
- TL;DR: Hidden Service pwnato, Ulbricht arrestato

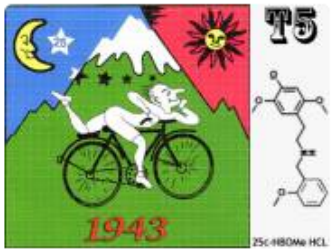
Silk Road
anonymous market

messages 0 | orders 0 | account ฿0.00

Search [ ] Go

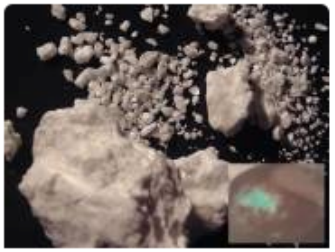
Shop by **Category**

- Drugs *8,104*
  - Cannabis *2,063*
  - Dissociatives *193*
  - Ecstasy *681*
  - Opioids *594*
  - Other *435*
  - Precursors *39*
  - Prescription *1,666*
  - Psychedelics *974*
  - Stimulants *1,039*
- Apparel *265*
- Art *118*
- Books *869*
- Collectibles *2*
- Computer equipment *40*
- Custom Orders *85*
- Digital goods *548*
- Drug paraphernalia *291*
- Electronics *79*
- Erotica *515*
- Fireworks *2*
- Food *8*
- Forgeries *75*
- Hardware *24*
- Herbs & Supplements *6*
- Home & Garden *11*
- Jewelry *96*
- Lab Supplies *73*
- Lotteries & games *77*
- Medical *54*
- Money *112*
- Musical instruments *3*
- Packaging *68*
- Services *69*
- Sporting goods *1*



1,000 x 25c-NBOMe HCL blotters (800ug)
฿9.73

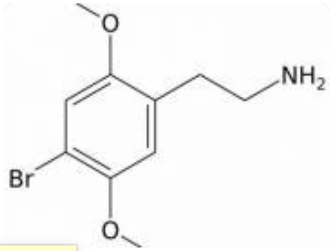
5g white russian
฿1.69



Cocaine Kokain Koks FLEX -- HIGH GRADE - 0.5
฿2.04

5g Good quality "Ali baba's Hash" from Chaouen
฿1.28

Kush
฿6.09



200mg
฿1.71

30 Xanax 1 mg {Alprazolam} tabs
฿2.53

100 x 1mg-25i-NBOMe complexed blotters
฿1.27

12ct Half Baked Brownzzz Relaxation Brownie
฿2.24

COSA È ANDATO STORTO?

- Contaminazione delle identità
- Scarsa sicurezza IRL
- Stupidità

CONTAMINAZIONE DELLE IDENTITÀ

- Nick utilizzati: frosty, altoid, DPR
- altoid posta su shroomery.org e bitcointalk.org “pubblicizzando” SR
- Sempre su bitcointalk fa riferimento all’indirizzo mail rossulbricht@gmail.com richiedendo l’aiuto di un “pro” in ambito IT che lo aiuti con una “startup rivoluzionaria”

Jump to first unread post.

altoid
Stranger
Registered: 01/28/11
Posts: 1
Last seen: 5 years, 8 months

anonymous market online? NEW 26
#13860995 - 01/28/11 12:28 AM (5 years, 8 months ago)

I came across this website called Silk Road. It's a Tor hidden service that claims to allow you to buy and sell anything online anonymously

I found it through silkroad420.wordpress.com, which, if you have a tor browser, directs you to the real site at http://tydgccykixpbu6uz.onion.

Let me know what you think...

Post Extras:

Quote from: altoid on January 29, 2011, 07:44:51 PM

What an awesome thread! You guys have a ton of great ideas. Has anyone seen Silk Road yet? It's kind of like an anonymous amazon.com. I don't think they have heroin on there, but they are selling other stuff. They basically use bitcoin and tor to broker anonymous transactions. It's at http://tydgccykixpbu6uz.onion. Those not familiar with Tor can go to silkroad420.wordpress.com for instructions on how to access the .onion site.

Let me know what you guys think

1 Other / Archival / IT pro needed for venture backed bitcoin startup on: October 11, 2011, 08:06:22 PM

Hello, sorry if there is another thread for this kind of post, but I couldn't find one. I'm looking for the best and brightest IT pro in the bitcoin community to be the lead developer in a venture backed bitcoin startup company. The ideal candidate would have at least several years of web application development experience, having built applications from the ground up. A solid understanding of oop and software architecture is a must. Experience in a start-up environment is a plus, or just being super hard working, self-motivated, and creative.

Compensation can be in the form of equity or a salary, or somewhere in-between.

If interested, please send your answers to the following questions to rossulbricht at gmail dot com

1) What are your qualifications for this position?
2) What interests you about bitcoin?

From there, we can talk about things like compensation and references and I can answer your questions as well. Thanks in advance to any interested parties. If anyone knows another good place to recruit, I am all ears.

FAIL

(ANCORA) CONTAMINAZIONE DELLE IDENTITÀ

- L’utente “ross ulbricht” posta, in una domanda su StackOverflow, porzioni di codice uguali ad alcune porzioni di codice di Silk Road.
  Pochi minuti dopo il nick viene cambiato in “frosty”

- Riferimenti alla scuola economica austriaca sul profilo G+ di Ross Ulbricht e sul profilo Silk Road di DPR.
  Altri collegamenti tra il suo profilo LinkedIn e l’attività di DPR su SR

How can I connect to a Tor hidden service using cURL in PHP?

214

288

I'm trying to connect to a Tor hidden service using the following PHP code:

```
$url = 'http://jhiwjjlqpyawmpjx.onion/'
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_PROXY, "http://127.0.0.1:9050/");
curl_setopt($ch, CURLOPT_PROXYTYPE, CURLPROXY_SOCKS5);
$output = curl_exec($ch);
$curl_error = curl_error($ch);
curl_close($ch);

print_r($output);
print_r($curl_error);
```

When I run it, I get the following error:

> Couldn't resolve host name

However, when I run the following command from my command line in Ubuntu:

```
curl -v --socks5-hostname localhost:9050 http://jhiwjjlqpyawmpjx.onion
```

I get a response as expected

The PHP cURL documentations says this:

```
--socks5-hostname
Use  the  specified  SOCKS5 proxy (and let the proxy resolve the host name).
```

I believe the reason it works from the command line is because Tor (the proxy) is resolving the .onion hostname, which it recognizes. When running the PHP code above, my guess is that cURL or PHP is trying to resolve the .onion hostname and doesn't recognize it. I've searched for a way to tell cURL/PHP to let the proxy resolve the hostname, but I can't find a way.

There is a very similar Stack Overflow question, *cURL request using socks5 proxy fails when using PHP, but it works through the command line*.

php curl proxy tor

share improve this question

edited Feb 26 at 18:24

Peter Mortensen

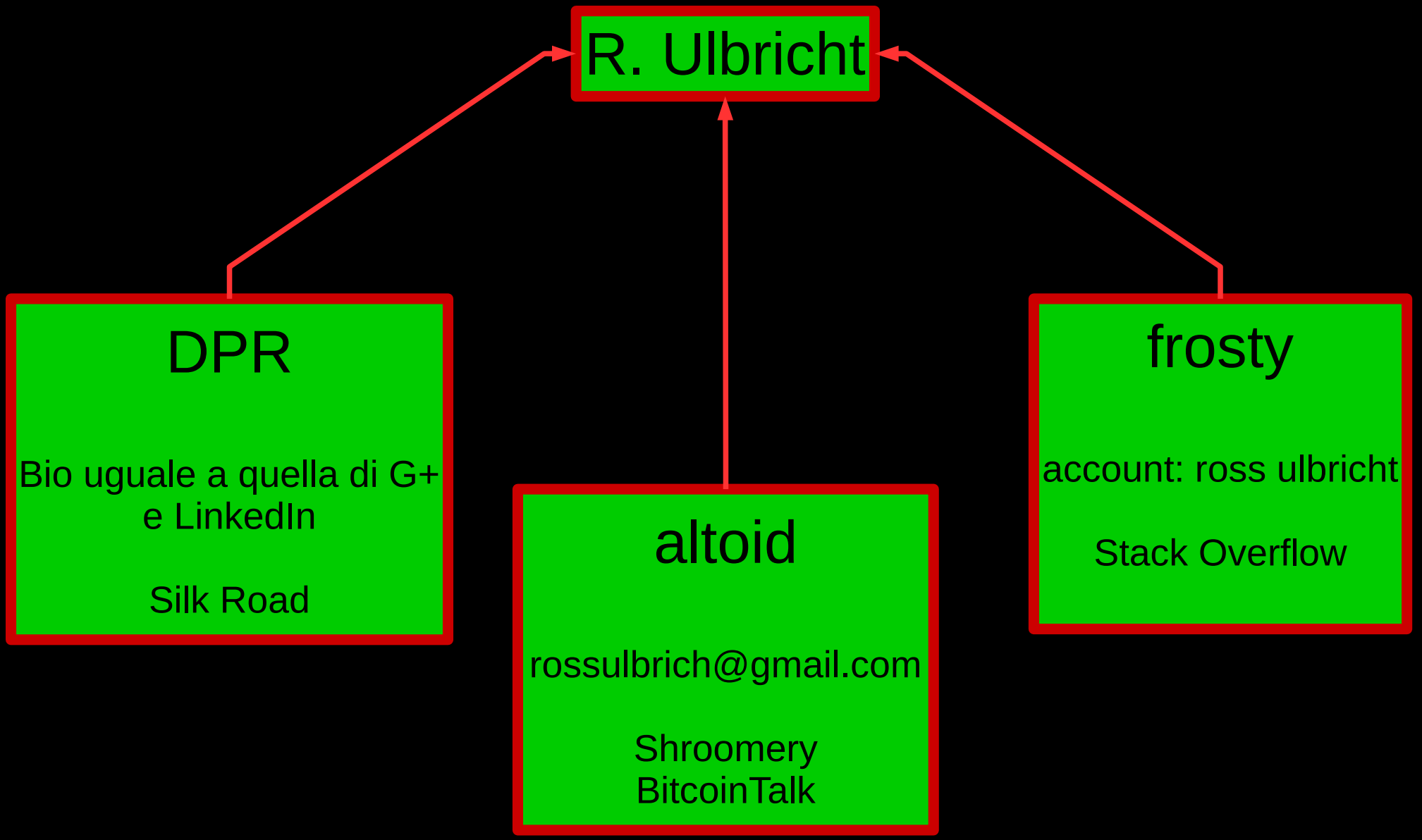
10.3k ● 13 ● 69 ● 107

asked Mar 16 '13 at 3:39

frosty

981 ● 4 ● 9 ● 9

CONTAMINAZIONE DELLE IDENTITÀ



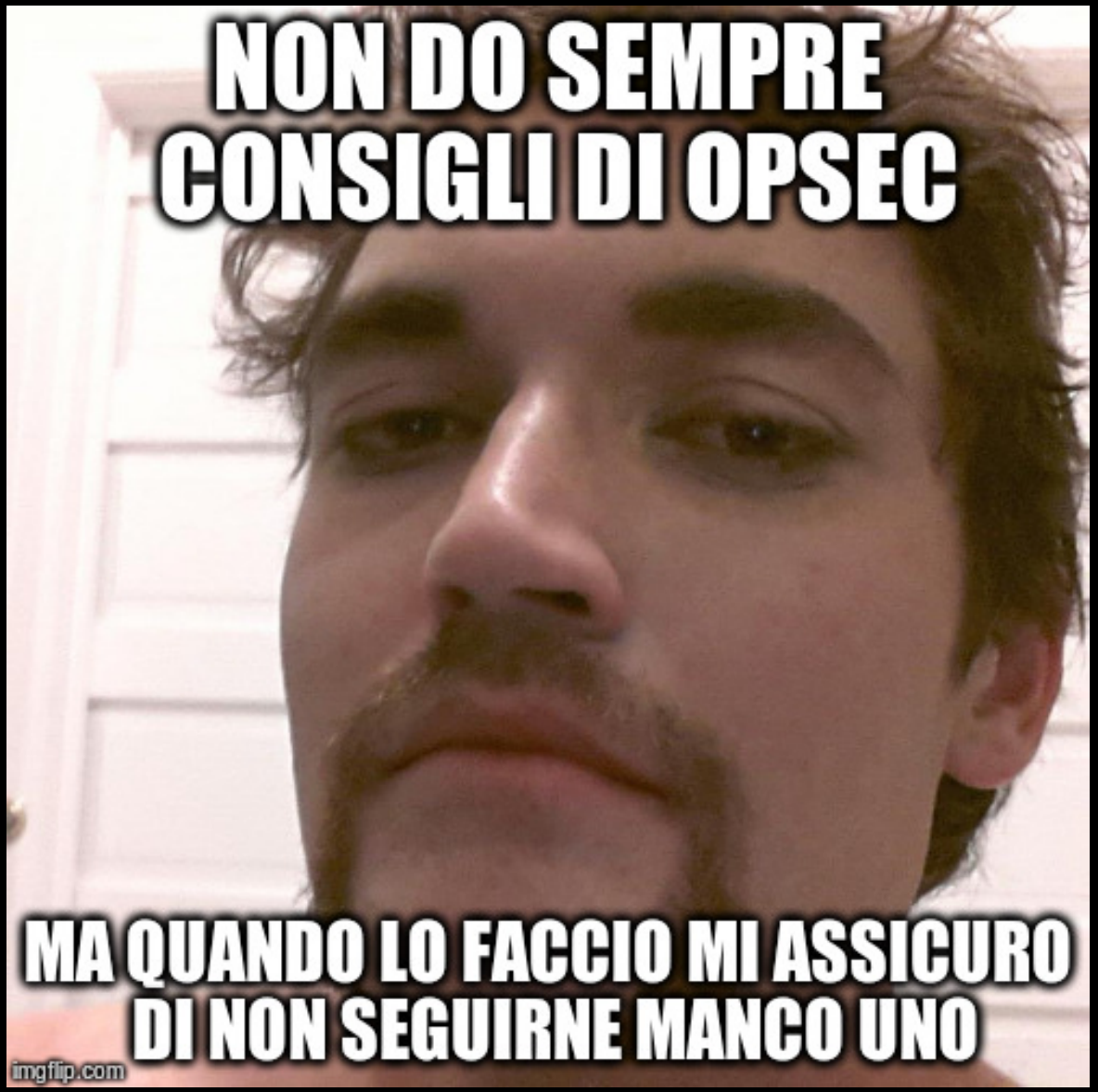
TROPPO SPECULATIVO?

Le chiavi private usate da DPR per accedere a Silk Road finivano con frosty@frosty

COSA È ANDATO STORTO?

- Contaminazione delle identità
- Scarsa sicurezza IRL
- Stupidità

SCARSA SICUREZZA IRL



SCARSA SICUREZZA IRL

- Buona la teoria, pessima la pratica
- Accorgimenti anti-forensics?
- Stesso punto di accesso, malgrado la VPN
- Colocalizzazione: accesso a mail personale dallo stesso luogo fisico in cui amministrava Silk Road

COSA È ANDATO STORTO?

- Contaminazione delle identità
- Scarsa sicurezza IRL
- Stupidità


NEW YORK STATE
DRIVER LICENSE
ID: 330 594 023 CLASS D
SCHAFFER
BENJAMIN JOHN
98 TERRACE AVE
ALBANY NY 12203
Colorado
Driver License
03-419-8351 Expires: 03-27-2016
Class: R Issued: 04-10-2013
Alberta
OPERATOR'S LICENCE
No: 874652-384
MARSHALL, Kenneth Evan
225 25 Ave NE
Calgary AB T2E 1Y1
DRIVER LICENSE CLASS E
STEPHAN AMADO JOHNSON
5132 FREMONT ST
JACKSONVILLE, FL 32210
SEX: M HGT: 6-02
SAFE DRIVER
CALIFORNIA
DL L4059385
CLASS C
END NONE
LN LAKE
FN SEAN DAVID
3250 NORTH F ST
SAN BERNARDINO,CA 92405
03271984
SEX M HAIR BRO EYES HAZ
HGT 6'-02" WGT 160 lb
DRIVING LICENCE
UK
1. ATKINSON
2. NATHANIAL LOUIS
3. GREAT BRITAIN
8. 17 WOLSELEY RD
LONDON, GREATER LONDON
Texas
USA
TX
DRIVER LICENSE
14059301
04/25/2013
Class C
Exp 03/27/2017
MOORE
WILLIAM LOUIS
634 MARY ST W
AUSTIN TX 78704
Restrictions NONE
End NONE
Hgt 6-02
Sex M
Eyes HAZ
South Carolina
DRIVER'S LICENSE
DL#: 255029482
LIGGINS, ANTHONY HAROLD
1314 COOSAW DR
CHARLESTON SC 29407
03-27-1984
Expires: 03-27-2022
Class: D
Sex: M
Weight: 160
Height: 6-02
Restrict: None
Endorse: None
Driver Licence
New South Wales, Australia
Sean Angus MCCALL

BIG FAIL

Alla richiesta di spiegazioni riguardo i documenti falsi con la sua foto sopra l’imputato risponde:

<< Non ne so niente di questa storia, sicuramente sono stati dei miei amici a farmi uno scherzo. Teoricamente chiunque può andare su siti tipo Silk Road nel Deep Web e comprare documenti falsi! >>

“È bello quando ci rendono tutto più semplice! :)”

- Agente Generico Medio dell’FBI


DAI RAGA NON VALE
LA D'URSO ERA SUI PANAMA PAPERS MA NON È IN CARCERE

BUSTED

LEZIONI APPRESE

LEZIONI APPRESE

- Compartimentalizza le identità

LEZIONI APPRESE

- Compartimentalizza le identità
- Tirati fuori dal gioco se si fa troppo grande

LEZIONI APPRESE

- Compartimentalizza le identità
- Tirati fuori dal gioco se si fa troppo grande
- Non fare pubblicità a uno dei più grossi market di scambio di droga durante un interrogatorio se sei il principale sospettato di esserne l’admin

CASE STUDY 2

Eldo Kim e l’allarme bomba ad Harvard

Who, what, when, where, why

- Studente di Harvard spaventato per un esame (e quando mai)
- Invia una mail con Guerrilla Mail fingendosi un dinamitardo che ha piazzato delle bombe ad Harvard
- Usa TOR per (tentare di) decorrelare il proprio IP da quello del mittente della mail
- Fallisce miseramente

Harvard University
@Harvard

Follow

Alert: Unconfirmed reports of explosives at four sites on campus: Science Center, Thayer, Sever, and Emerson. Evacuate those buildings now.

Reply Retweet Favorite More

846 RETWEETS

27 FAVORITES

9:14 AM - 16 Dec 13

COSA È ANDATO STORTO?

- Unico studente connesso a TOR all’interno della rete nel momento in cui viene inviata la mail
- Guerrilla Mail espone l’indirizzo IP del mittente
- Ha confessato appena i federali hanno bussato alla porta del suo dormitorio

PERSONE CON UN ESAME
NELLA DATA
IN CUI È STATA INVIATA
LA MAIL


PERSONE CON UN ESAME NELLA DATA IN CUI È STATA INVIATA LA MAIL
PERSONE CONNESSE ALLA RETE DI HARVARD


PERSONE CON UN ESAME NELLA DATA IN CUI È STATA INVIATA LA MAIL
PERSONE SU TOR NELLA RETE DI HARVARD QUELLA MATTINA
PERSONE CONNESSE ALLA RETE DI HARVARD

PERSONE CON UN ESAME NELLA DATA IN CUI È STATA INVI LA MAIL

PERSONE SU TOR NELLA RETE DI HARVARD QUELLA MATTINA

RSONE CONNESSE ALLA RETE DI HARVARD

LEZIONI APPRESE

- Usa sempre e solo wi-fi pubbliche non nominative e non monitorate, cambiandole periodicamente (ok, facciamo finta di niente sul “non monitorate”)

LEZIONI APPRESE

- Usa sempre e solo wi-fi pubbliche non nominative e non monitorate, cambiandole periodicamente (ok, facciamo finta di niente sul “non monitorate”)
- Possibilmente metti un bridge fra te e il nodo di entrata

LEZIONI APPRESE

- Usa sempre e solo wi-fi pubbliche non nominative e non monitorate, cambiandole periodicamente (ok, facciamo finta di niente sul “non monitorate”)
- Possibilmente metti un bridge fra te e il nodo di entrata
- Usa servizi mail che non espongano l’IP del mittente

LEZIONI APPRESE

- Usa sempre e solo wi-fi pubbliche non nominative e non monitorate, cambiandole periodicamente (ok, facciamo finta di niente sul “non monitorate”)
- Possibilmente metti un bridge fra te e il nodo di entrata
- Usa servizi mail che non espongano l’IP del mittente
- NEGA ANCHE L’EVIDENZA!!!!!!

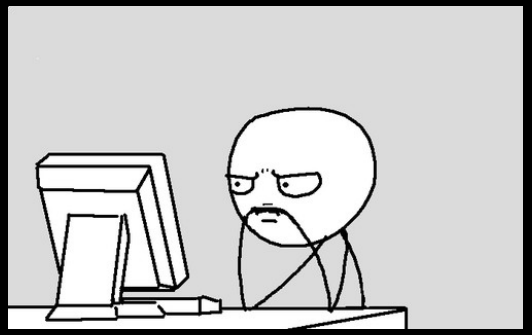
ATTACCHI A CORRELAZIONE

- Time based
- Packet based

TIME BASED

- Verifica la correlazione fra il periodo di tempo in cui un sospetto è connesso a TOR e il periodo in cui l’attività illecita è stata eseguita
- Relativamente facile da eseguire
- Non richiede particolari risorse

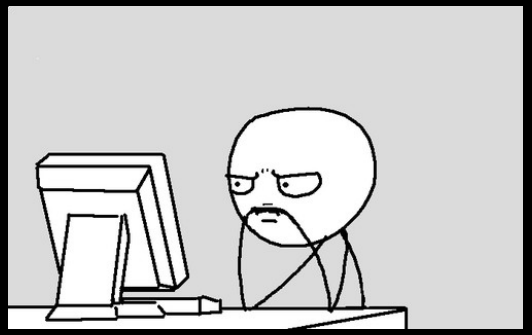
JH



TOR

SUP_G

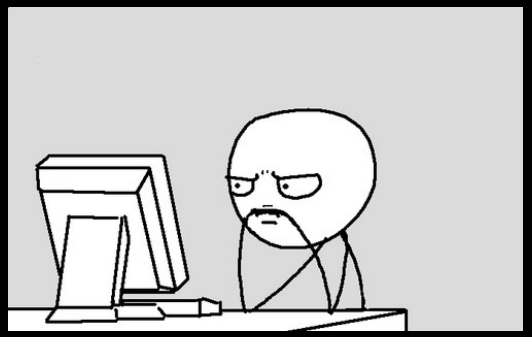
JH



TOR

SUP_G

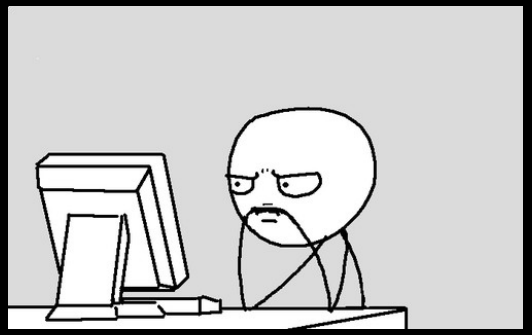
JH



TOR

SUP_G

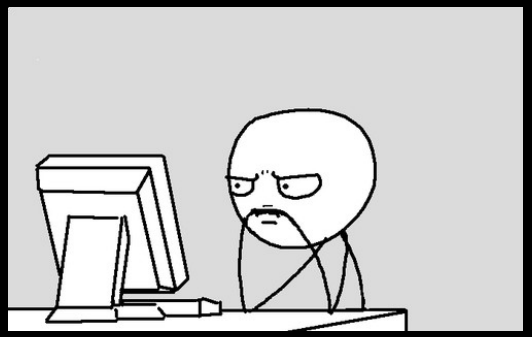
JH



TOR

SUP_G

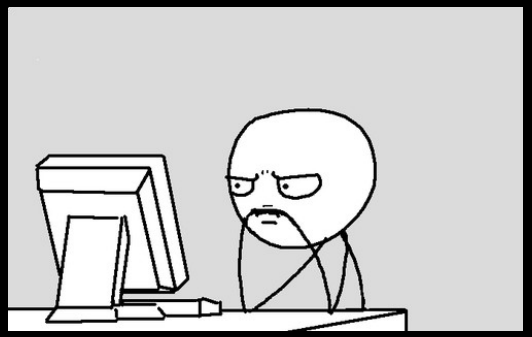
JH



TOR

SUP_G

JH

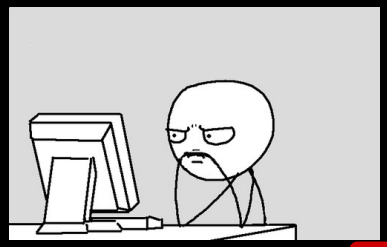


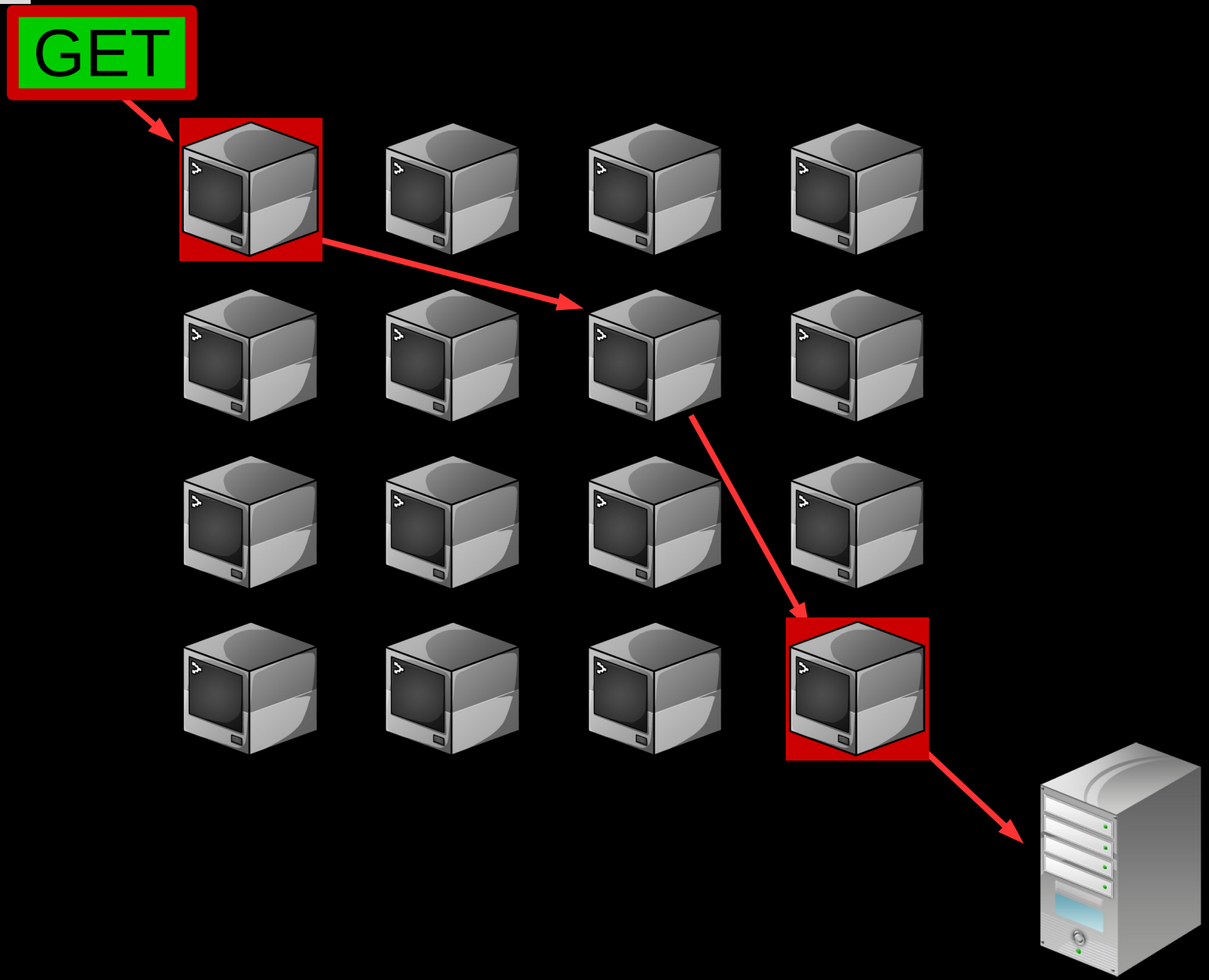
TOR

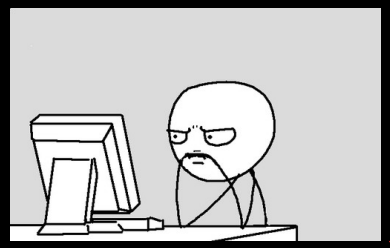
SUP_G

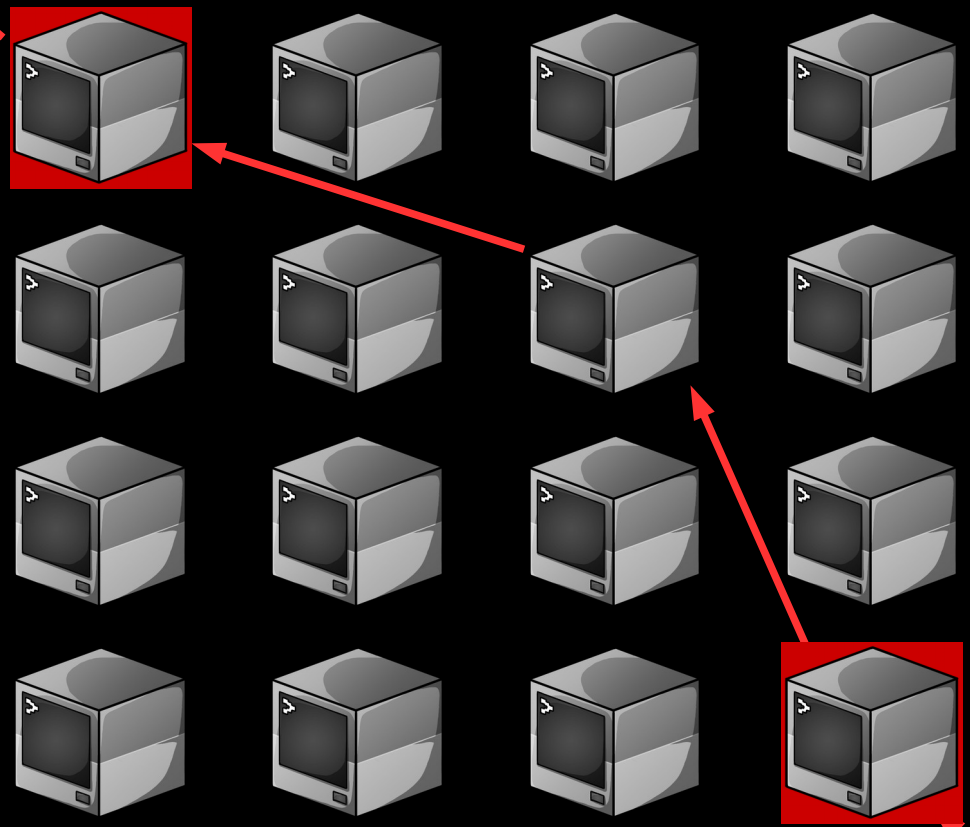
PACKET BASED

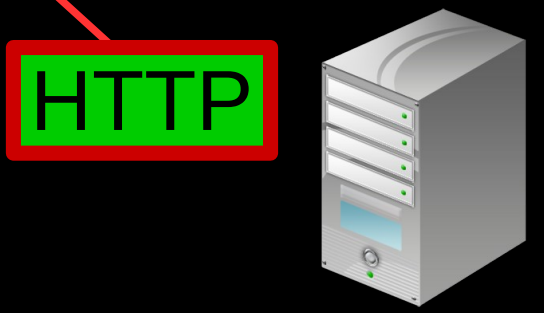
- Analizza il traffico su vaste porzioni della rete correlando i metadati dei singoli pacchetti in entrata e in uscita
- Difficile da eseguire
- Richiede ingenti investimenti da parte dell'attaccante
  (ogni riferimento a TLAs americane ~~non~~ è casuale)



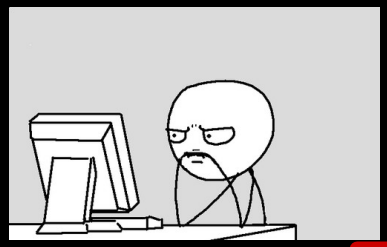

GET

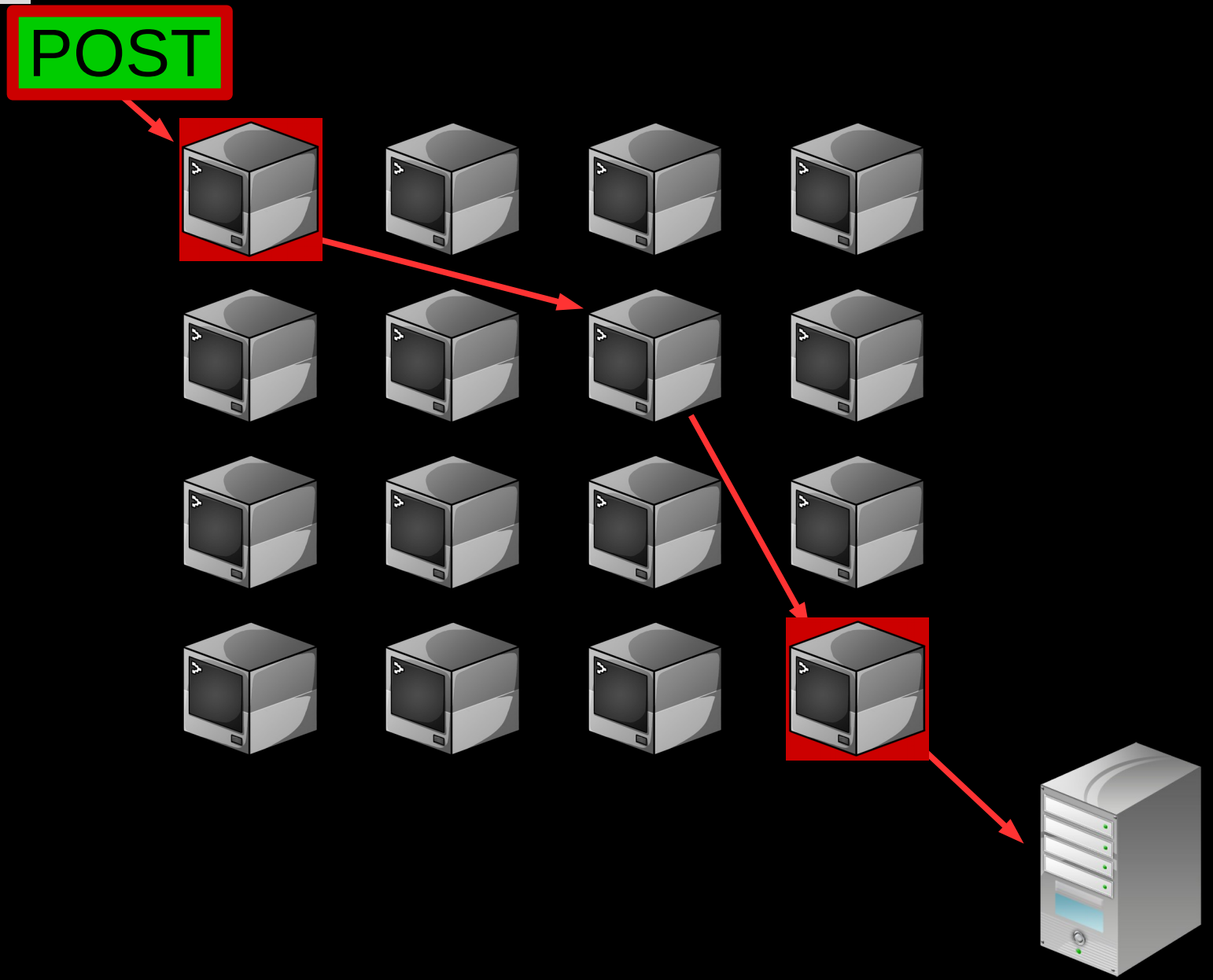


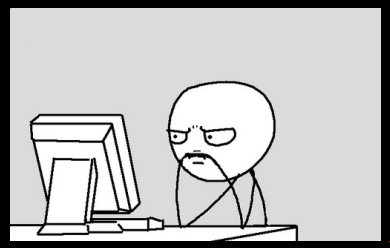


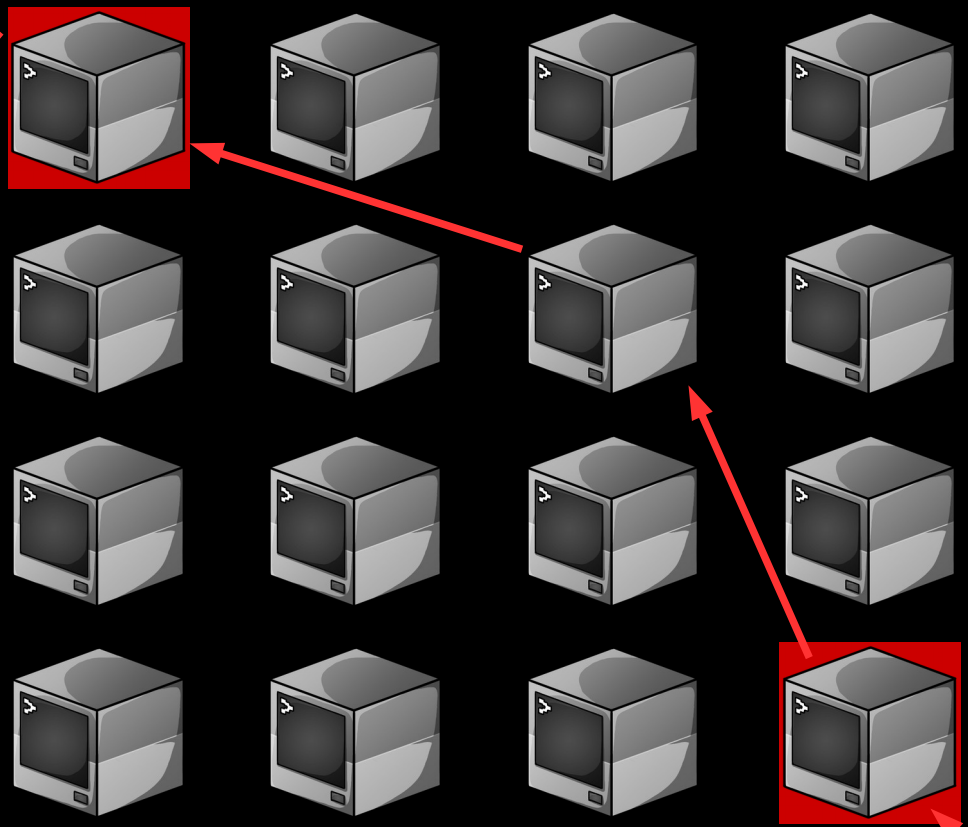


HTTP




POST




HTTP

CONTROMISURE

- Usare TOR consistentemente e non solo per “operazioni”
- Variare più volte il percorso dei pacchetti
- Non accedere direttamente a TOR (Bridge? Proxy? VPN over TOR? VPN over TOR over VPN? VPN over TOR over… avete capito!)

DOMANDE?