HACKER: A computer hacker is any skilled computer expert that uses their technical knowledge to overcome a problem.

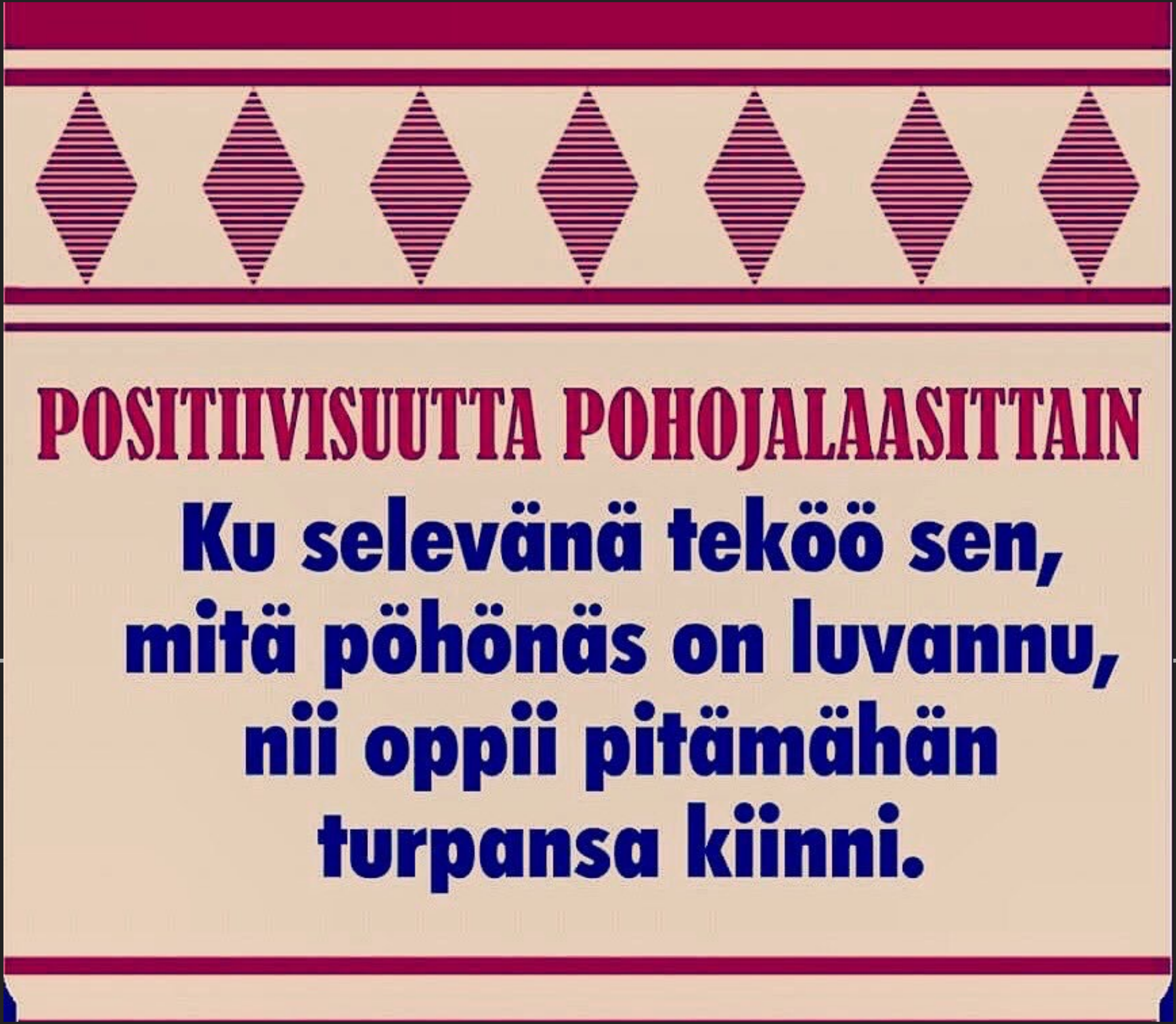
BUG BOUNTY HUNTERS EDITION

NOT ALL THOSE WHO WANDER ARE LOST

TOMI KOSKI (TK0)

- Senior Security Specialist @ NIXU
- #Hacking
- Sports
- Movies
- Handicrafts (level 1)
- @tomikoski
- haxor-profile: tk0

Each presentation needs to have a cat. Here.



POSITIIVISUUTTA POHOJALAASITTAIN

Ku selevänä teköö sen,
mitä pöhönäs on luvannu,
nii oppii pitämähän
turpansa kiinni.

STORY ABOUT OSINT, BUGBOUNTIES AND PERSPECTIVE FROM HUNTER SIDE

- Open Source INTelligence
- Bug Bounties (BB)
  - How I Bug Bounty and does it actually make any sense?
- Fi(n)nish Twist
  - There are not that many Finns doing BB-stuff. Or are you? (looking at you billy_blaze!)
- Sharing my personal experiences, opinions, failures and success

OSINT (OPEN SOURCE INTELLIGENCE)

- Wikipedia quote: *"Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context"*
- (Mostly) FREE and there are LOT of different sources!
    - Search Engines (even Bing has its own perks!)
    - The Search Engines on steroids (Shodan)
    - Social Media (Twitter)
    - CrunchBase (acquisitions)
- Any (non-intrusive) way to gain MOAR information about the target

BUG BOUNTIES 1-2-3

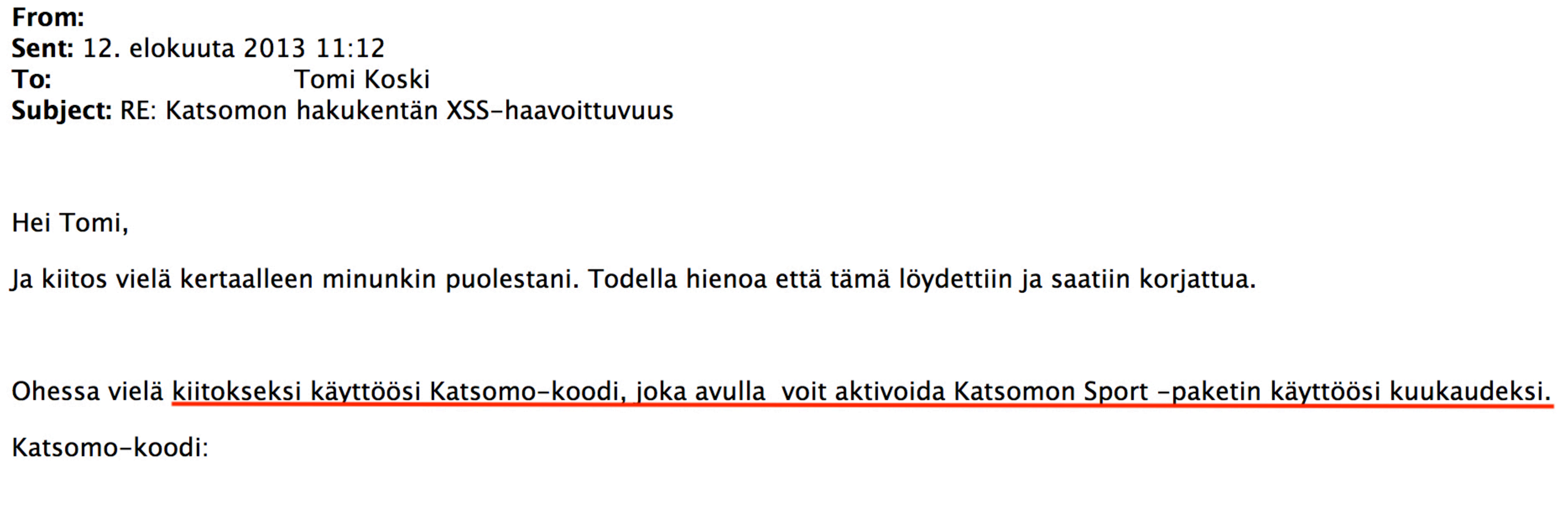
- LEGAL hacking of pre-selected target (fav for ~~> *.example)
- Mutual TRUST between researcher and program
- Simple rules/policy: Find any IN-SCOPE BUG, write quality report and profit (fame, swag, money, services, …)
- PLAY by the rules and you're fine
- HACK 'n' Learn!

BUG BOUNTY PROGRAMS

- Coordinated platforms
  - HackerOne
  - hackr.fi 🇫🇮
  - Bugcrowd
  - ZeroCopter
  - Synack
- Company maintained
  - Swisscom
  - Microsoft
  - ATT
  - Google
  - Facebook

MY EARLY DAYS

- Started to do some random poking (mostly XSS) around summer 2013
    - Didn’t really know what to exactly do and how to test :)
    - Handpicked some random targets, mostly Finnish sites
    - Contacting any company took couple of hours too (reminder: /security.txt)
    - Got FANTASTIC help and GREAT support from one fellow hacker: Janne Ahlberg (@JanneFI / @HoaxEye)
- Most common response to my email submissions from companies:
    - …
    - Personal favourite of mine: *“If you do not stop your ACTIVITIES, actions will be taken…”*
    - Few “Thank you!’ emails and even one BOUNTY! Still very proud!



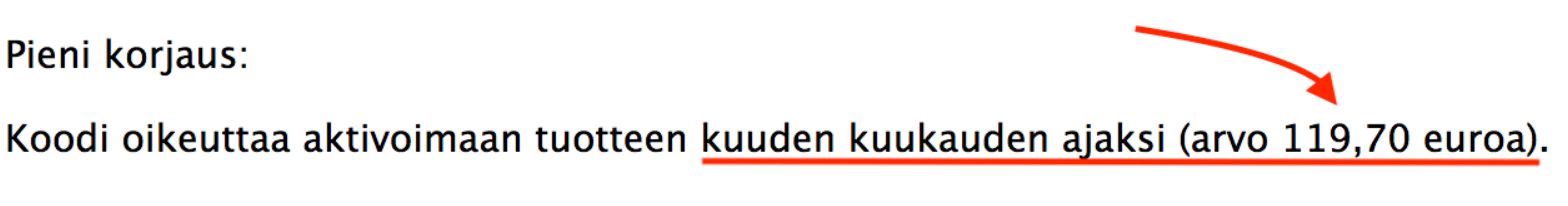
From:
Sent: 12. elokuuta 2013 11:12
To: Tomi Koski
Subject: RE: Katsomon hakukentän XSS-haavoittuvuus

Hei Tomi,

Ja kiitos vielä kertaalleen minunkin puolestani. Todella hienoa että tämä löydettiin ja saatiin korjattua.

Ohessa vielä kiitokseksi käyttöösi Katsomo-koodi, joka avulla voit aktivoida Katsomon Sport -paketin käyttöösi kuukaudeksi.

Katsomo-koodi:



Pieni korjaus:

Koodi oikeuttaa aktivoimaan tuotteen kuuden kuukauden ajaksi (arvo 119,70 euroa).

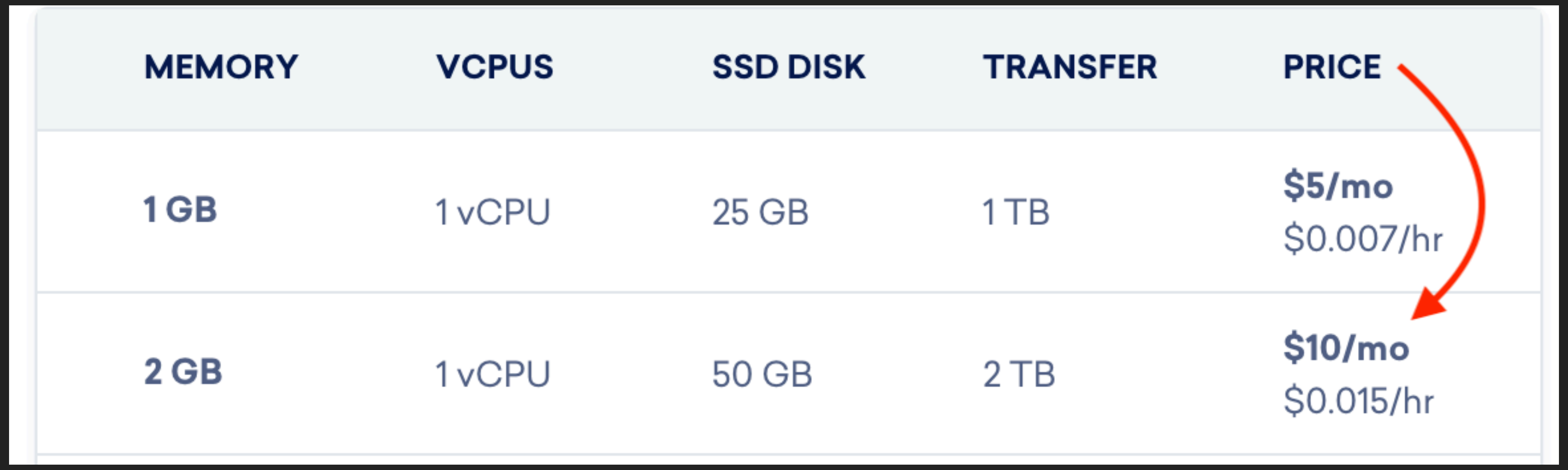
WELCOME COORDINATED DISCLOSURE PLATFORMS!

- 2016: Registered to HackerOne and BugCrowd like all the cool kids!
- …Time flies, almost nothing really happens…
- Few $100-150 bounties received for good efforts I suppose :)
- 2017: Started to dive into available programs on platforms and did my first (and worst) submissions
- Decided to make some personal goals for next season 2017-2018:
  - GOAL #1: Pay personal BURP license for a year (~400EUR)
  - GOAL #2: Buy new bling-bling computer (too many $$$/EUR)
  - TAXES <3 (see GOAL #1 and GOAL #2)

TIME YOU ENJOY WASTING IS NOT WASTED TIME?

- Got sucked in bad but yet-another “i got no time for this”, internal timing issue
- Estimated (and effective) BB-testing time ~0-3 hours per day
- Too much bounty’ing around the night makes me waaaay too zombie
- Only MANUAL testing? /facepalm
- Haven’t quit my day job (and not planning to)
- Occasionally testing killed my home internet of shopping (*living-room screams*)
- PRO-TIP: Don’t kill all the fun by overdoing IT [ba-dum-tsssss]

(SEMI)AUTOMATION TO THE RESCUE!



MEMORY	VCPUS	SSD DISK	TRANSFER	PRICE
1 GB	1 vCPU	25 GB	1 TB	$5/mo $0.007/hr
2 GB	1 vCPU	50 GB	2 TB	$10/mo $0.015/hr

- EPIC SERVER-FARM…? I use single Linux box for $10/month
- My treasure chest for bunch of scripts for different phases:
  1. Gathering (enumeration)
  2. Scanning (ports)
  3. Fuzzing / Peeking URLs (find)
  4. Results / Reporting (still manual labor mostly) :|
- Even during this talk, my teany-weany server is knocking ports and causing EPIC mayhem!
- Box can SERVE files (js/html), do DNS extractions and act as an callback for example, you feel me?!
- ~~> Demo target: *.example.com

TOOLS OF MY CHOICE: GATHERING

- DNS enumeration / brute-forcing
  - Subfinder / amass
  - dnssearch
  - knockpy
  - RESULTS:
    example.com
    www.example.com
    hidden.example.com

TOOLS OF MY CHOICE: SCANNING

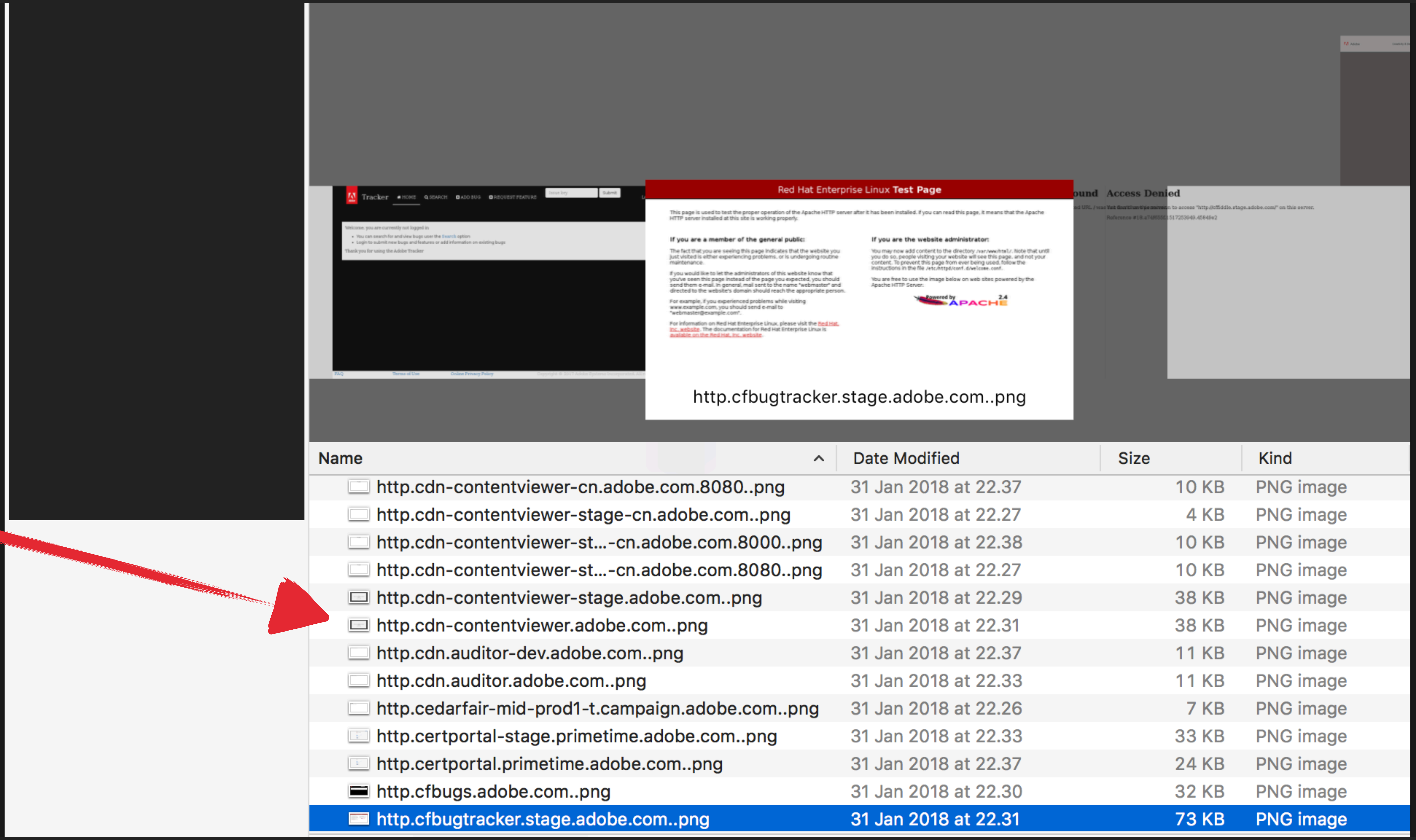
- Port scanning
  - NMAP
  - masscan
  - aquatone
  - RESULTS:
    http://example.com:80
    https://www.example.com:4443
    http://hidden.example.com:15432

TOOLS OF MY CHOICE: FUZZING

- Fuzzing, Crawling, Spidering
  - WFUZZ
  - Python / cURL
  - RESULTS:
    http://example.com:80/.bash_history
    https://www.example.com:4443/typo3/phpmyadmin/scripts/setup.php
    http://hidden.example.com:15432/admin/db/backup01.tgz

TOOLS OF MY CHOICE: PEEKING

- Photograph all URLs for easy picking ("URLie")
  - EyeWitness
  - RESULTS:



Red Hat Enterprise Linux Test Page
Tracker
Access Denied
http.cfbugtracker.stage.adobe.com..png

Name	Date Modified	Size	Kind
http.cdn-contentviewer-cn.adobe.com.8080..png	31 Jan 2018 at 22.37	10 KB	PNG image
http.cdn-contentviewer-stage-cn.adobe.com..png	31 Jan 2018 at 22.27	4 KB	PNG image
http.cdn-contentviewer-st...-cn.adobe.com.8000..png	31 Jan 2018 at 22.38	10 KB	PNG image
http.cdn-contentviewer-st...-cn.adobe.com.8080..png	31 Jan 2018 at 22.27	10 KB	PNG image
http.cdn-contentviewer-stage.adobe.com..png	31 Jan 2018 at 22.29	38 KB	PNG image
http.cdn-contentviewer.adobe.com..png	31 Jan 2018 at 22.31	38 KB	PNG image
http.cdn.auditor-dev.adobe.com..png	31 Jan 2018 at 22.37	11 KB	PNG image
http.cdn.auditor.adobe.com..png	31 Jan 2018 at 22.33	11 KB	PNG image
http.cedarfair-mid-prod1-t.campaign.adobe.com..png	31 Jan 2018 at 22.26	7 KB	PNG image
http.certportal-stage.primetime.adobe.com..png	31 Jan 2018 at 22.33	33 KB	PNG image
http.certportal.primetime.adobe.com..png	31 Jan 2018 at 22.37	24 KB	PNG image
http.cfbugs.adobe.com..png	31 Jan 2018 at 22.30	32 KB	PNG image
http.cfbugtracker.stage.adobe.com..png	31 Jan 2018 at 22.31	73 KB	PNG image

BONUS: POKING AROUND

- BURP (Pro) testing with extensions
- Random tools, clever stuff based on interest/type of the target
    - Common Crawl Index Server
        - curl -sX GET “http://index.commoncrawl.org/CC-MAIN-2018-34-index?url=*.example.com&output=json" | jq -r .url | sort -u
    - Nikto, WPScan, Python+BeautifulSoup, meg, LinkFinder, PayloadsAllTheThings, Own custom “tools”, …
- RESULTS: AWESOME RESULTS! :)

${SEARCH_ENGINE} DORKING

- inurl:status JMXInvokerServlet (JBOSS java deserialisation RCE)
- site:s3.amazonaws.com (file buckets)
- inurl:/index.cfm (Coldfusion)
- site:example.com ext:atom | ext:scm | ext:stm | ext:sxw | ext:psw | ext:pps | ext:csv | ext:ini | ext:properties | ext:nfo | ext:bak | ext:swf | ext:old | ext:swp | ext:git | ext:svn | ext:py | ext:pyc | ext:am | ext:ac | ext:xhtml | ext:do | ext:cfm | ext:log | ext:cfg (Juicy stuff)

- DDG and BING! ip:104.40.211.35 (all domains behind an IP)

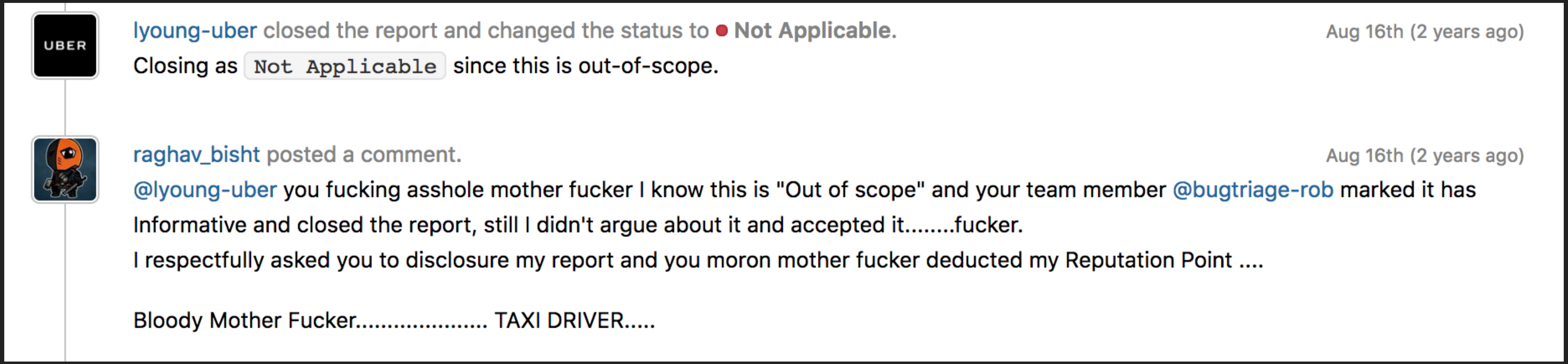
TARGETS FOR EVERYBODY!

- Lots of targets, lots of hackers
- Believe or not, these super-secret techniques from previous slides actually has worked for me!
- ~~Old~~ LEGACY services will get new features (regression tests)
- Modern DevOps-pipelines are so cool - open Jenkins instance with RCE is even cooler!
- Look into all (even old'ish) programs – found an RCE after 414 resolved bugs

0X10> ALMOST THERE...

THINGS TO KEEP IN MIND

- AUTOMATE!
- Prefer targets with large scope, *.example.com
- Quality of submissions (reports) will have an impact to final result (bounty)
- When you find something, first try to chain more bugs for better results and then submit
- Take a break occasionally (i'm kind of having one now!) :)
- Play nice.



lyoung-uber closed the report and changed the status to ● Not Applicable. Aug 16th (2 years ago)

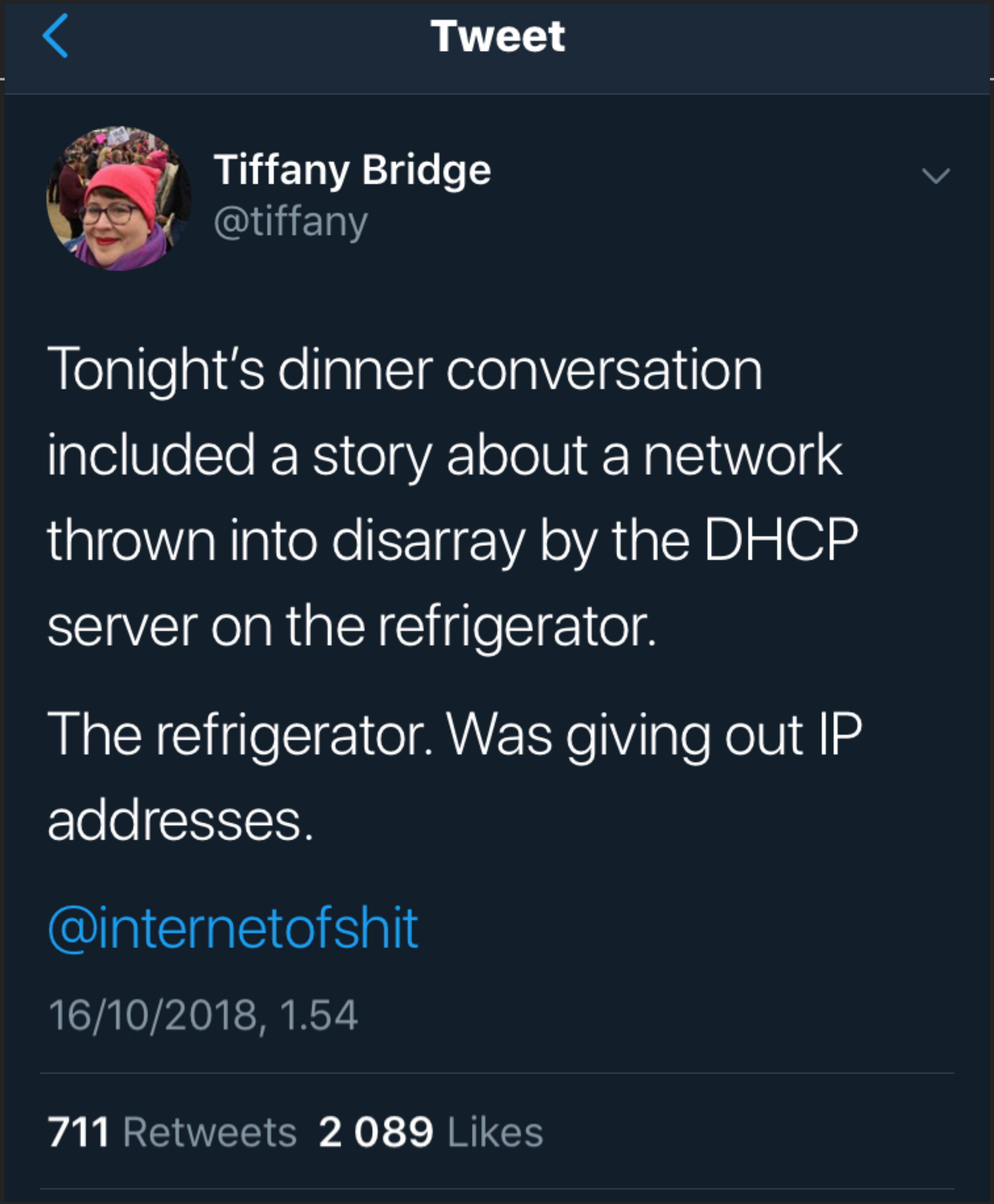
Closing as `Not Applicable` since this is out-of-scope.

raghav_bisht posted a comment. Aug 16th (2 years ago)

@lyoung-uber you fucking asshole mother fucker I know this is "Out of scope" and your team member @bugtriage-rob marked it has Informative and closed the report, still I didn't argue about it and accepted it........fucker.

I respectfully asked you to disclosure my report and you moron mother fucker deducted my Reputation Point ....

Bloody Mother Fucker..................... TAXI DRIVER.....



Tiffany Bridge
@tiffany

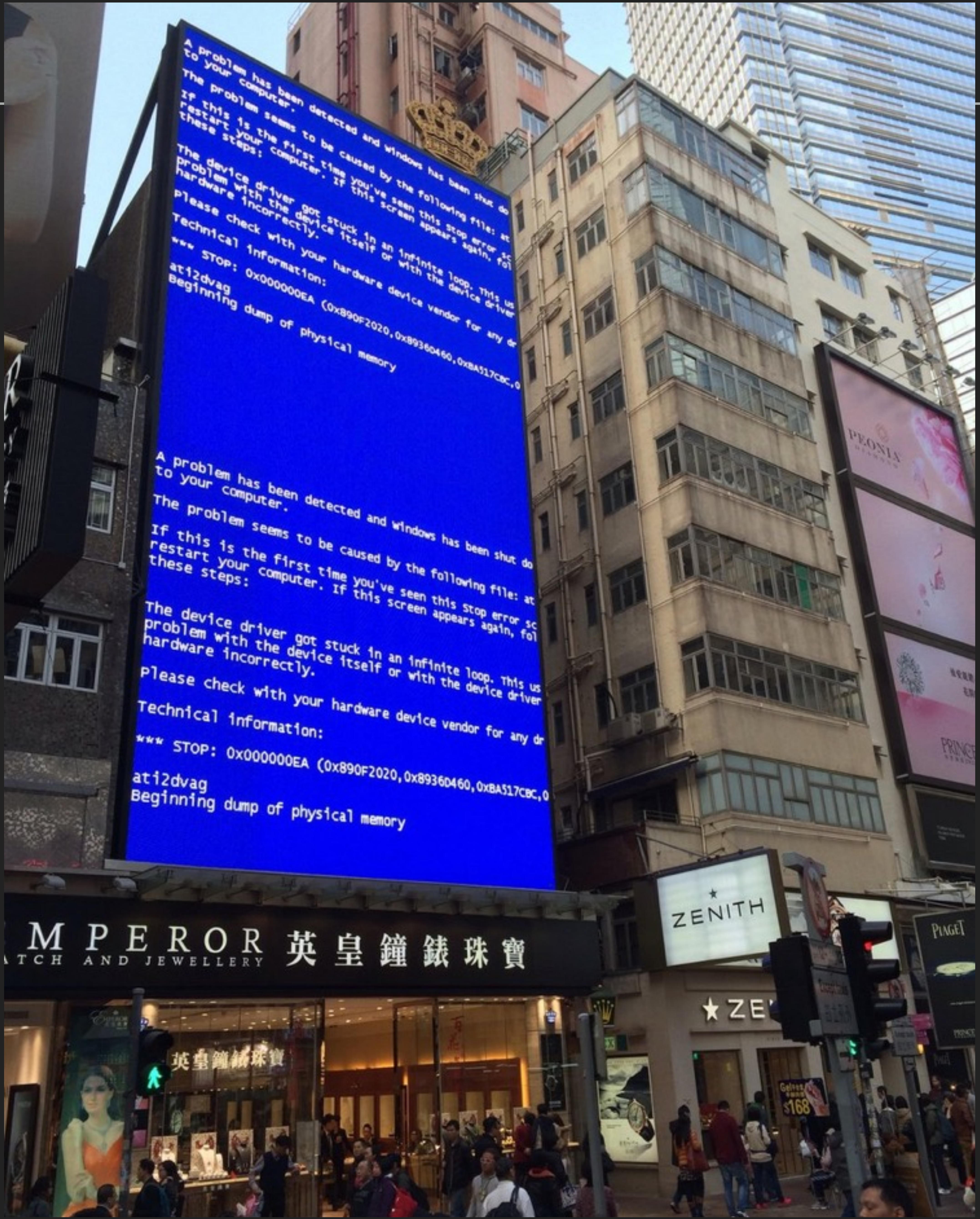
Tonight's dinner conversation included a story about a network thrown into disarray by the DHCP server on the refrigerator.

The refrigerator. Was giving out IP addresses.

@internetofshit

16/10/2018, 1.54

711 Retweets 2 089 Likes



A problem has been detected and windows has been shut do
to your computer.
The problem seems to be caused by the following file: at
If this is the first time you've seen this stop error sc
restart your computer. If this screen appears again, fol
these steps:
The device driver got stuck in an infinite loop. This us
problem with the device itself or with the device driver
hardware incorrectly.
Please check with your hardware device vendor for any dr
Technical information:
*** STOP: 0x000000EA (0x890F2020,0x89360460,0xBA517C8C,0
ati2dvag
Beginning dump of physical memory
MPEROR
TCH AND JEWELLERY
英皇鐘錶珠寶
ZENITH
ZE
PIAGET

THANK YOU!

QUESTIONS?

NO?

IT'S OKAY.

WE'LL CHAT LATER…

~~~

@TOMIKOSKI
~~~