Cybersecurity in a Global Economy

Matt Morton

CGEIT, CISSP

Do we really need cybersecurity?

Linked Globally

Walmart
TARGET
Neiman Marcus
SONY
THE HOME DEPOT
CALIFORNIA'S HOME IMPROVEMENT WAREHOUSE
JPMORGAN

OPM

Anthem

ASHLEY MADISON
Life is short. Have an affair.
Get started by telling us your relationship status:
Please Select
See Your Matches »
Over 32,430,000 anonymous members!

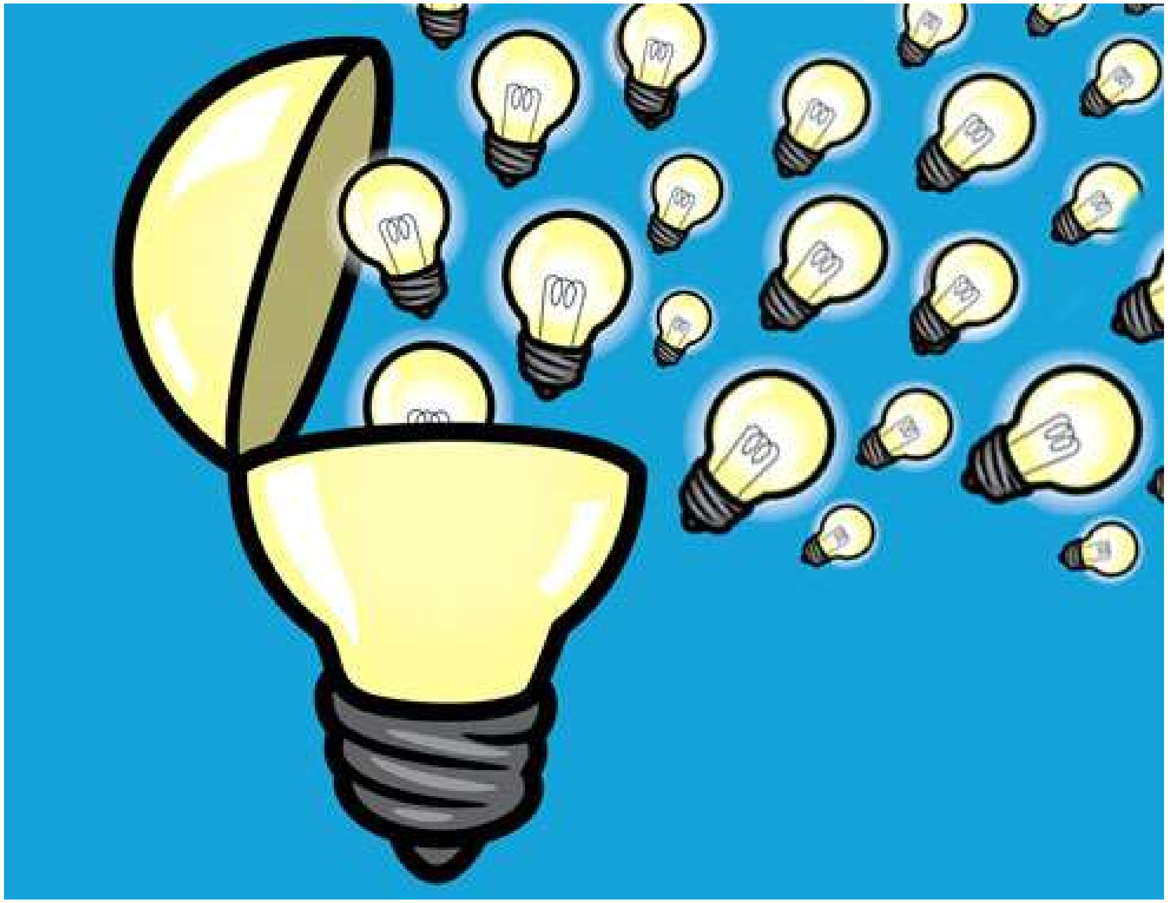
]HackingTeam[
Rely on us.

Office of Personnel Management

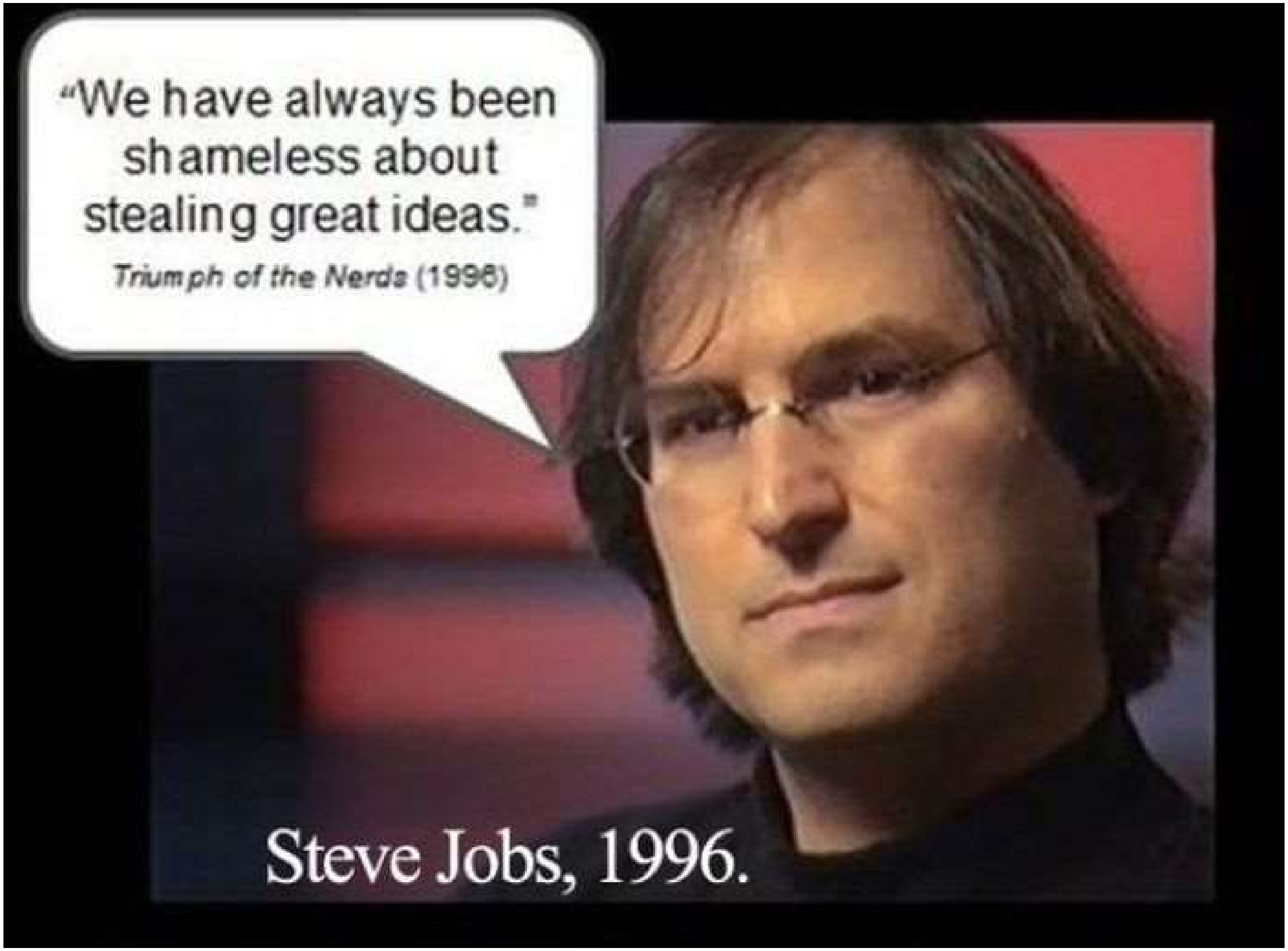
- 25 million affected
  - Security clearances
  - 2.1 million fingerprints
    - Wait - 5.6 million
- Upgrading systems since 2010
- Too little too late
- Incremental contracting
- Political favors
- Government shutdowns

New Approaches

Ideas



Stealing Ideas


"We have always been shameless about stealing great ideas."
Triumph of the Nerds (1996)
Steve Jobs, 1996.

Temüjin

- Organizing tribes
- Common goal
    - Prosperity for all
        - At least those who submit
- Controlled all commerce for 3 centuries
- From Poland to Korean coast
- Cultural impact reaches into current times
- Who is this?

Chingis (Genghis) Khan

- Dominated all of Eurasia
- Conquered Russia
    - China
    - Eastern Europe
    - Middle East
- Multiple contributions
    - Military strategy
    - Multiple cultures within one empire
    - Religious tolerance
    - Trans continental mail system
    - Paper money backed by precious metals

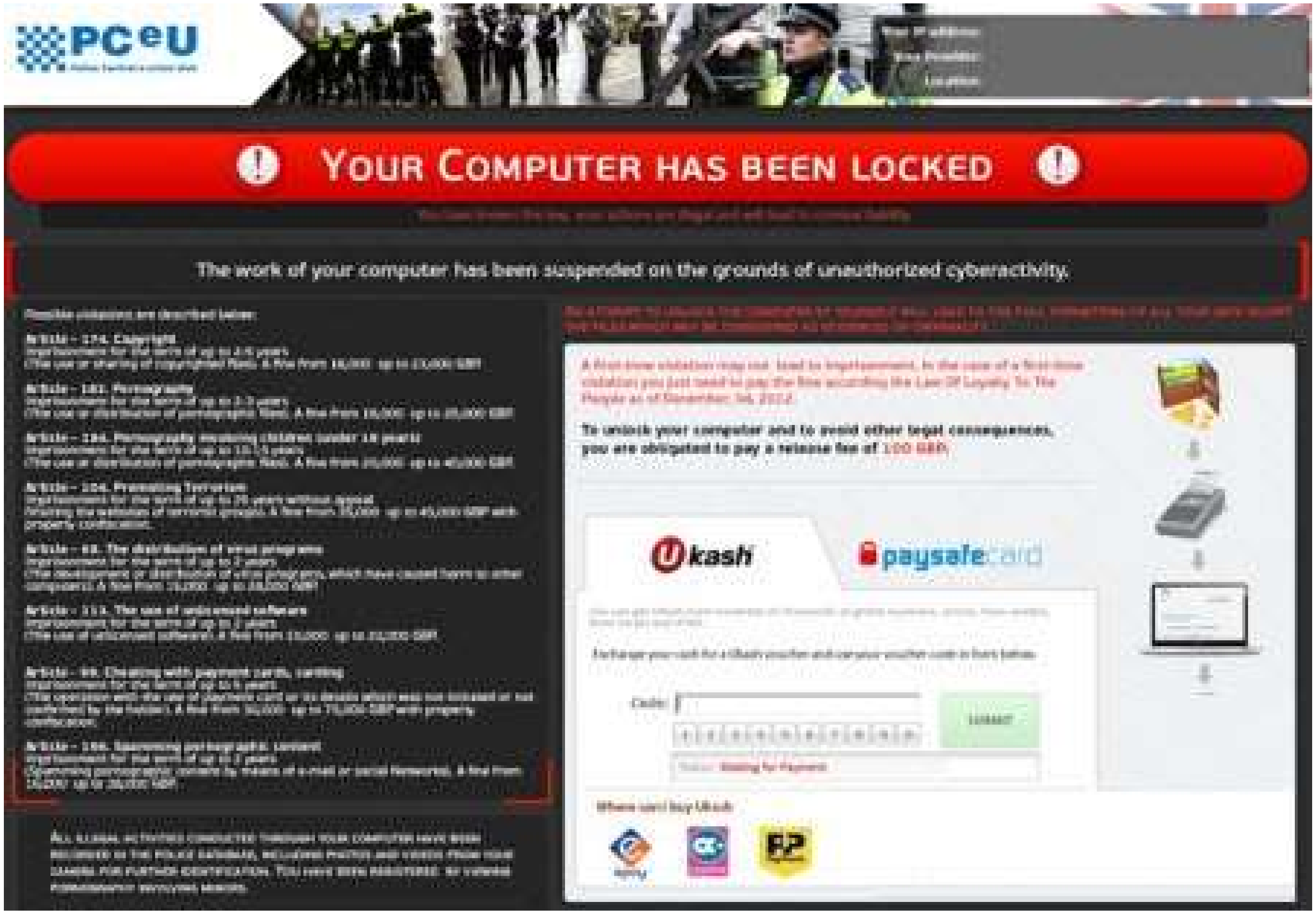
Mongolian Global Economy

- Controlled all commerce well into 14th century
- Encouraged safe, fast communication throughout empire
- No real desire to manage countries
- Control of mail riders
  - Ability to intercept
  - Read messages
- Seeing a pattern?

What’s different today?

- Similar battle today in dealing with Mongolian strategy
- Multiple tribes or groups on the Internet
- Freedom of expression on Internet
- Continued attempts to extract tribute

Ransomware



YOUR COMPUTER HAS BEEN LOCKED

You have broken the law, your actions are illegal and will lead to criminal liability

The work of your computer has been suspended on the grounds of unauthorized cyberactivity.

Possible violations are described below:

Article - 174. Copyright
Imprisonment for the term of up to 2-5 years
(The use or sharing of copyrighted files). A fine from 18,000 up to 23,000 GBP

Article - 183. Pornography
Imprisonment for the term of up to 2-3 years
(The use or distribution of pornographic files). A fine from 18,000 up to 20,000 GBP

Article - 184. Pornography involving children (under 18 years)
Imprisonment for the term of up to 10-15 years
(The use or distribution of pornographic files). A fine from 20,000 up to 40,000 GBP

Article - 104. Promoting Terrorism
Imprisonment for the term of up to 25 years without appeal
(Visiting the websites of terrorist groups). A fine from 35,000 up to 45,000 GBP with property confiscation.

Article - 68. The distribution of virus programs
Imprisonment for the term of up to 2 years
(The development or distribution of virus programs, which have caused harm to other computers). A fine from 15,000 up to 28,000 GBP

Article - 113. The use of unlicensed software
Imprisonment for the term of up to 2 years
(The use of unlicensed software). A fine from 15,000 up to 20,000 GBP

Article - 99. Cheating with payment cards, carding
Imprisonment for the term of up to 5 years
(The operation with the use of payment card or its details which was not initiated or not confirmed by the holder). A fine from 30,000 up to 70,000 GBP with property confiscation.

Article - 198. Spamming pornographic content
Imprisonment for the term of up to 2 years
(Spamming pornographic content by means of e-mail or Social Networks). A fine from 15,000 up to 28,000 GBP

ALL ILLEGAL ACTIVITIES CONDUCTED THROUGH YOUR COMPUTER HAVE BEEN RECORDED IN THE POLICE DATABASE, INCLUDING PHOTOS AND VIDEOS FROM YOUR CAMERA FOR FURTHER IDENTIFICATION. YOU HAVE BEEN REGISTERED BY VIEWING PORNOGRAPHY INVOLVING MINORS.

AN ATTEMPT TO UNLOCK THE COMPUTER BY YOURSELF WILL LEAD TO THE FULL FORMATTING OF ALL YOUR DATA AS WELL AS THE FILES WHICH WILL BE CONSIDERED AS EVIDENCE OF CRIMINALITY.

A first-time violation may not lead to imprisonment. In the case of a first-time violation you just need to pay the fine according the Law Of Loyalty To The People as of December 14, 2012.

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of 100 GBP.

[illegible]

Exchange your cash for a Ukash voucher and enter your voucher code in form below.

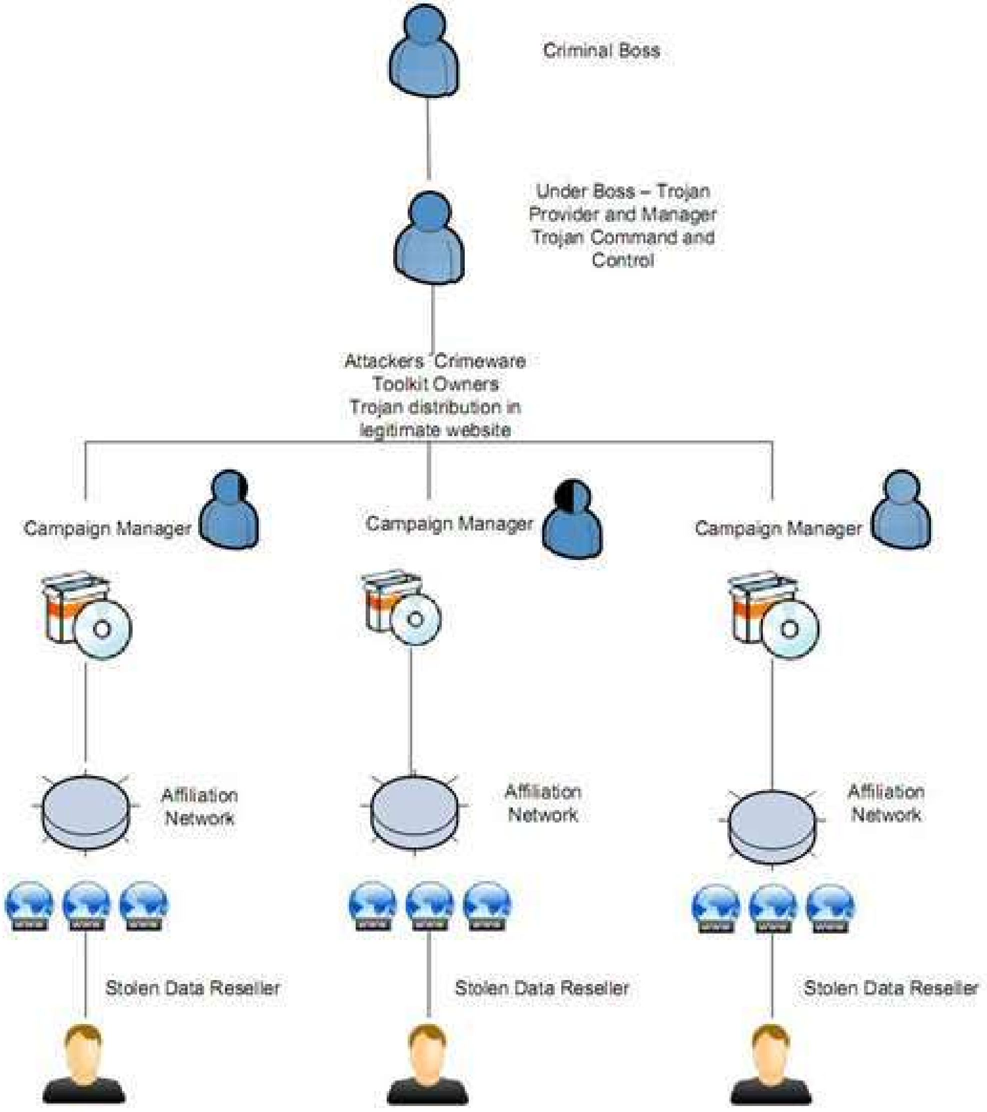
Code:

Status: Waiting for Payment

Where can I buy Ukash

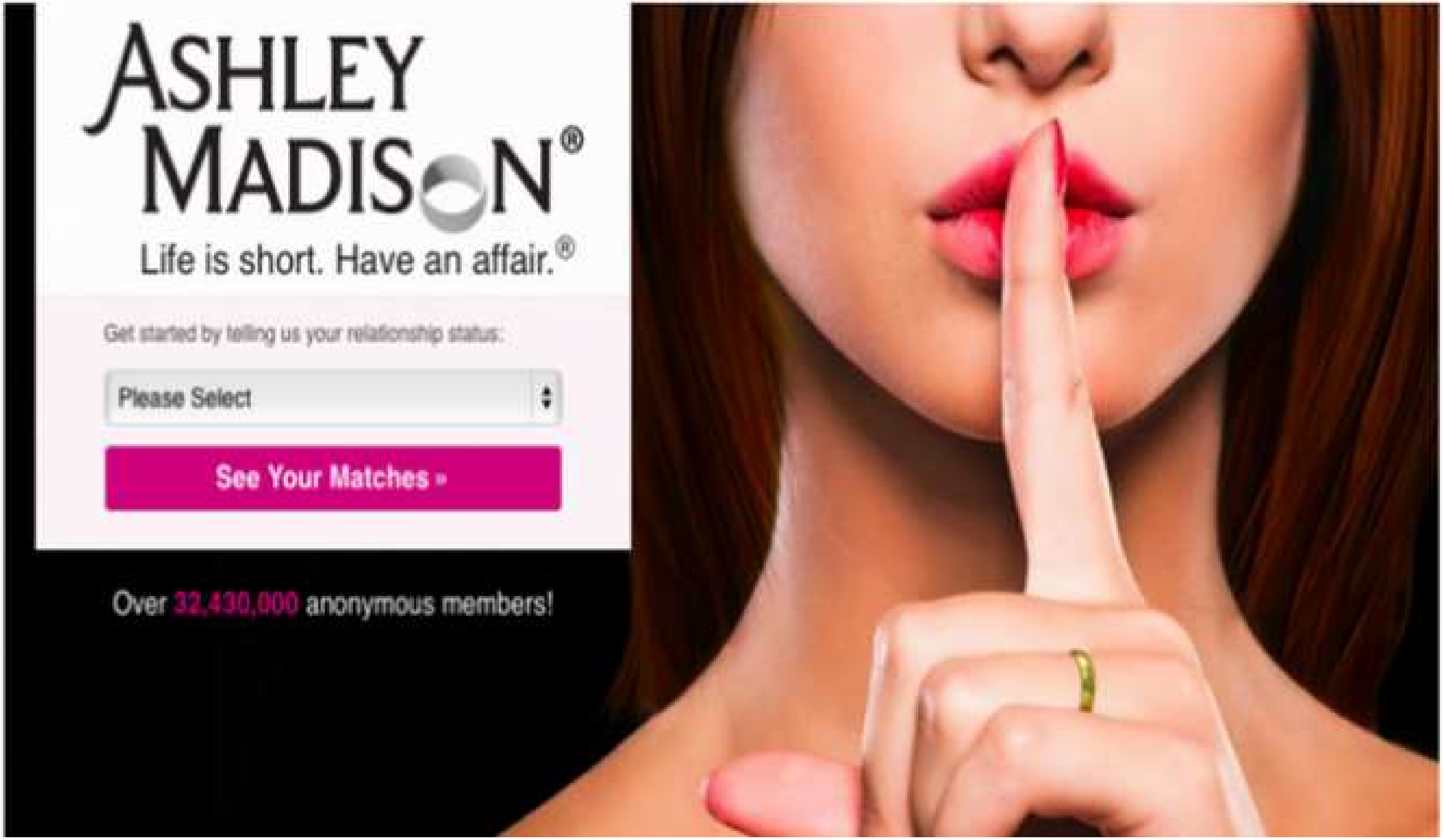
Phishing

Cybercrime Hierarchy



Coalescing Groups

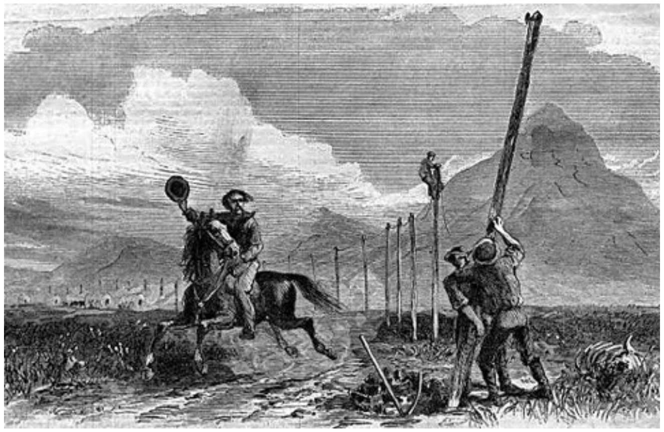
Interconnected



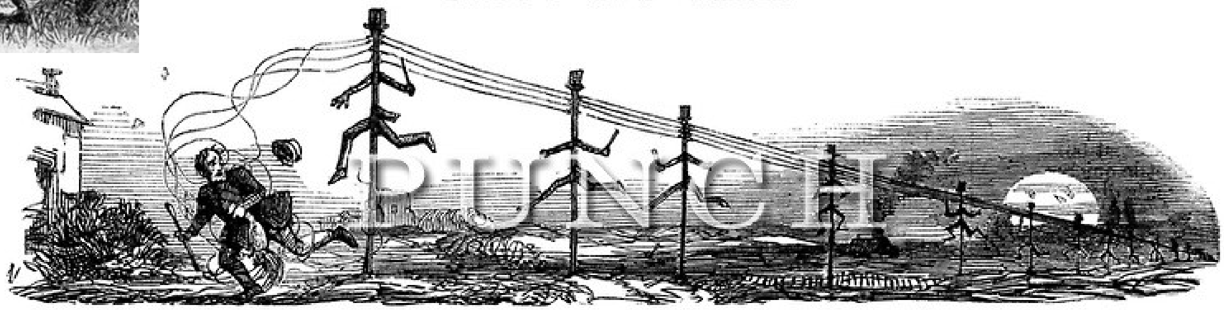
Get started by telling us your relationship status:

Over 32,430,000 anonymous members!

Hacking the Telegraph



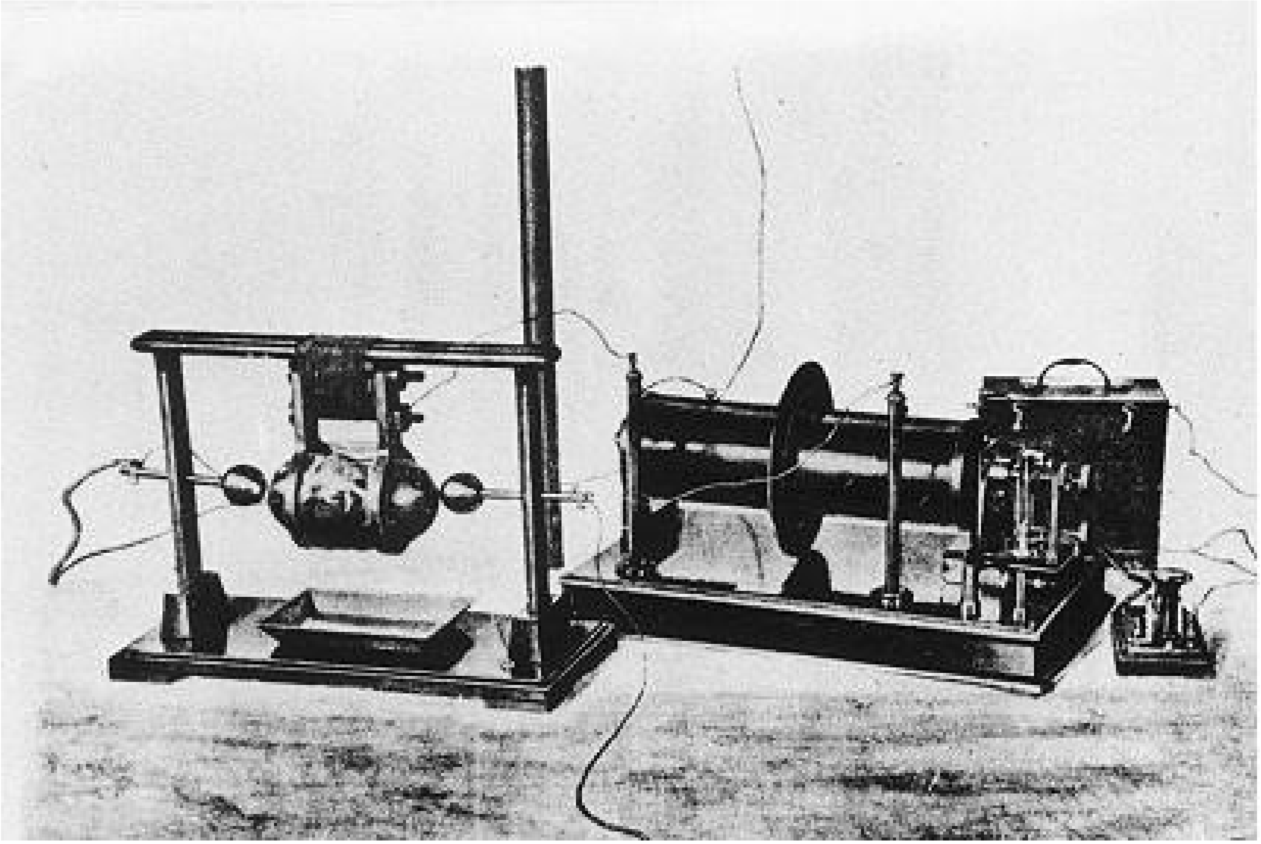
SWIFT AND SURE.



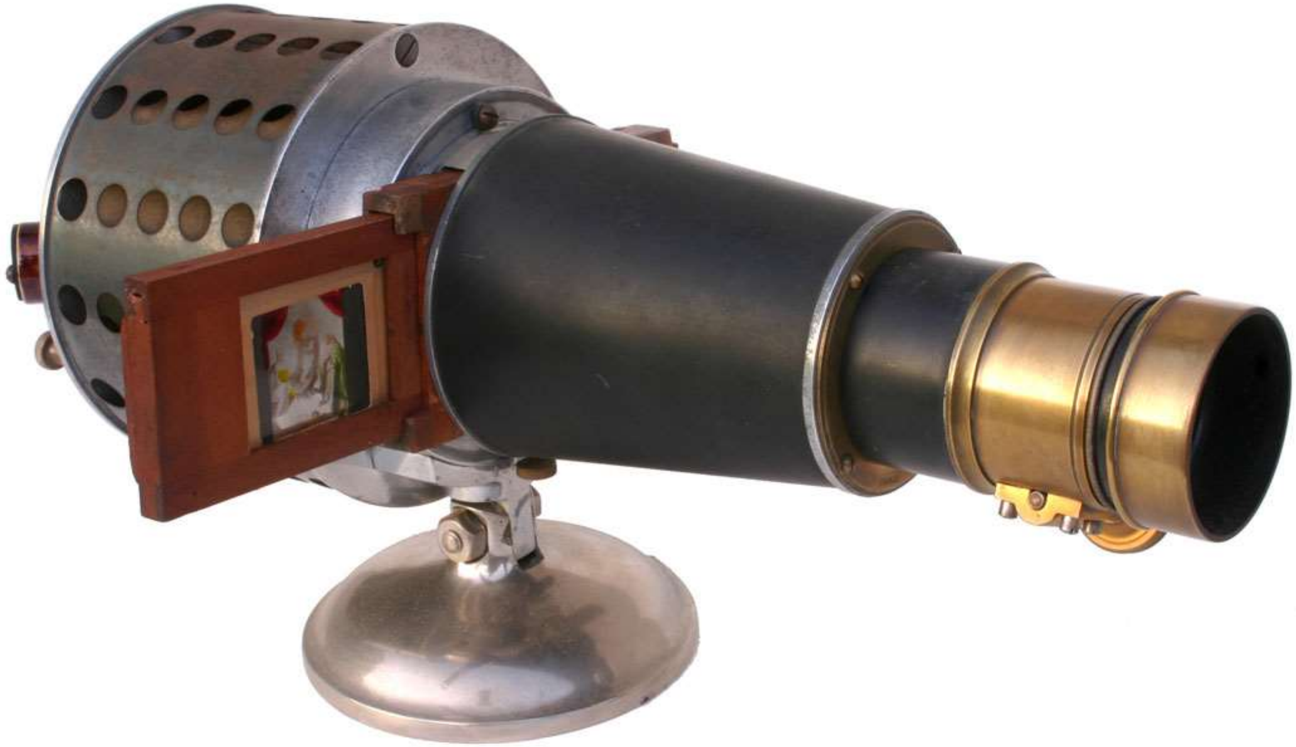
A VISION VERY LIKE REALITY.

SINCE justice took to tracking crime by the aid of the Electric Telegraph, she can no longer be described in the words of HORACE as "*Pede pœna claudo.*" No wonder the murderer is nervous, when he is, literally, very often " hung upon wires."

Hacking Wireless Telegraph

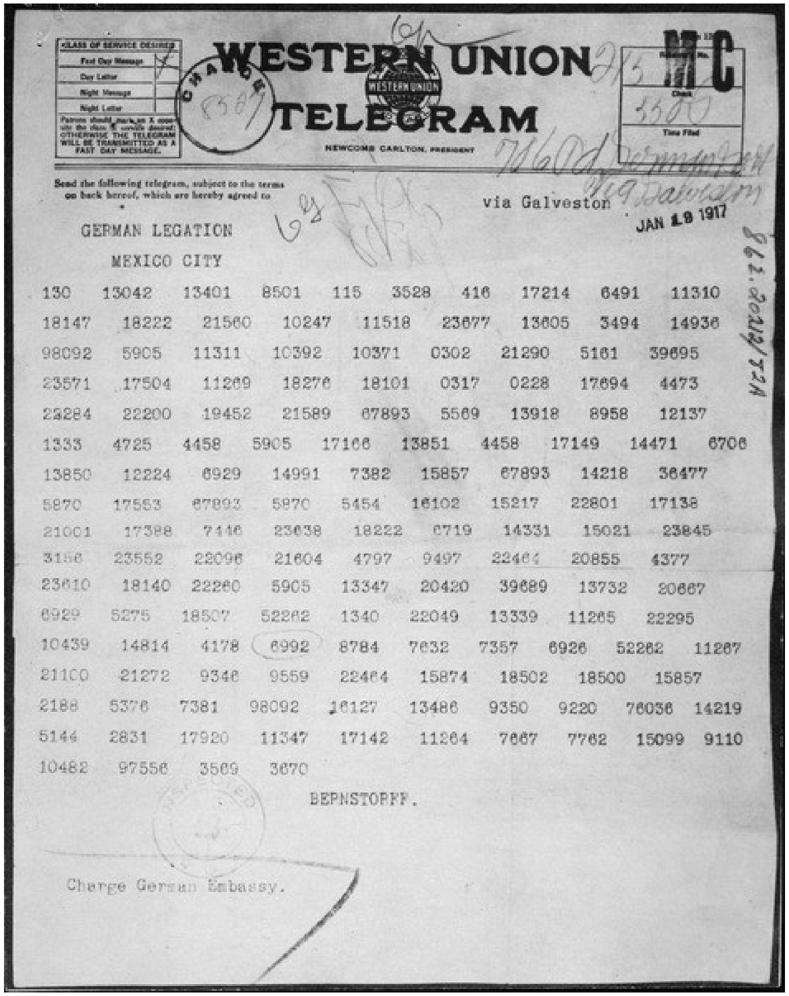


Projector hacked by Maskelyne



Zimmerman Telegram

- Sent by Germans in 1917 to Mexico
- Sent from German Embassy in US
- Intercepted by British Intelligence
- Decrypted and shared with U.S.



CLASS OF SERVICE DESIRED
Fast Day Message ☒
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

CHARGE 8389

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Check 3380

Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

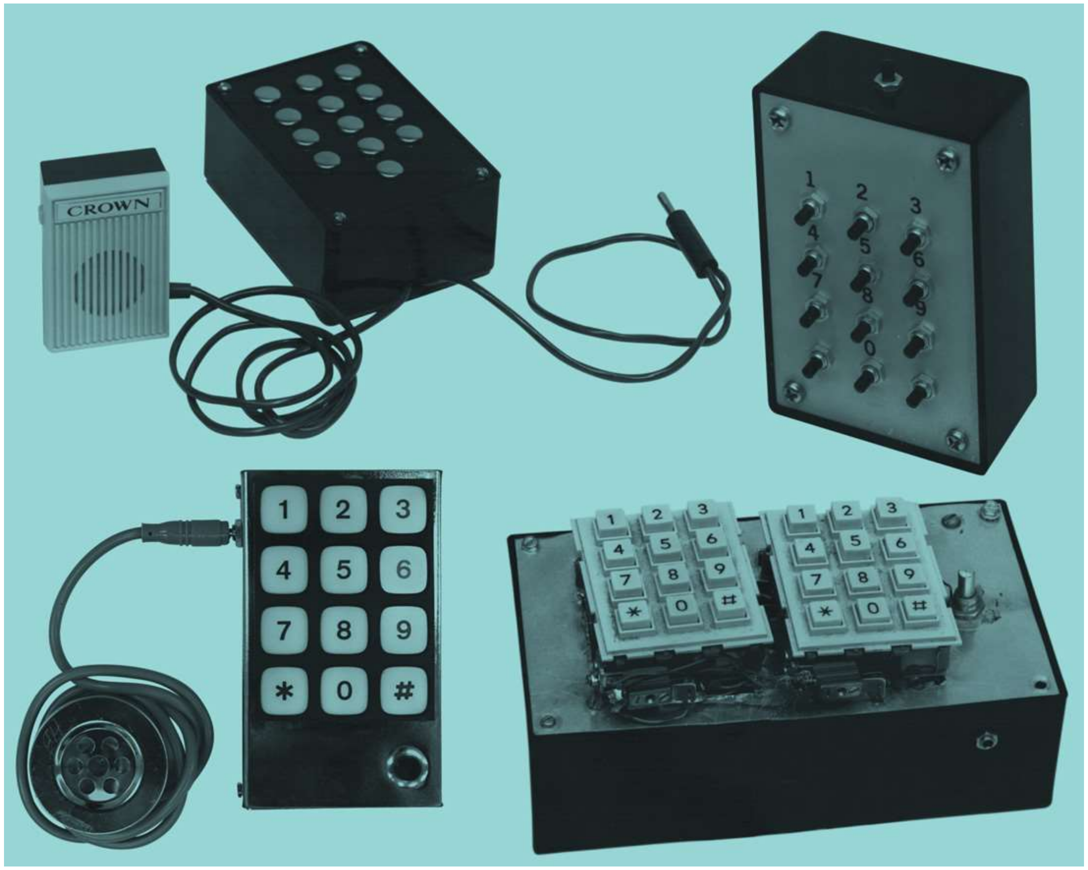
```
130    13042  13401  8501   115    3528   416    17214  6491   11310
18147  18222  21560  10247  11518  23677  13605  3494   14936
98092  5905   11311  10392  10371  0302   21290  5161   39695
23571  17504  11269  18276  18101  0317   0228   17694  4473
22284  22200  19452  21589  67893  5569   13918  8958   12137
1333   4725   4458   5905   17166  13851  4458   17149  14471  6706
13850  12224  6929   14991  7382   15857  67893  14218  36477
5870   17553  67893  5870   5454   16102  15217  22801  17138
21001  17388  7446   23638  18222  6719   14331  15021  23845
3156   23552  22096  21604  4797   9497   22464  20855  4377
23610  18140  22260  5905   13347  20420  39689  13732  20667
6929   5275   18507  52262  1340   22049  13339  11265  22295
10439  14814  4178   6992   8784   7632   7357   6926   52262  11267
21100  21272  9346   9559   22464  15874  18502  18500  15857
2188   5376   7381   98092  16127  13486  9350   9220   76036  14219
5144   2831   17920  11347  17142  11264  7667   7762   15099  9110
10482  97556  3569   3670
```

BEPNSTORFF.

Charge German Embassy.

862.20212/72A

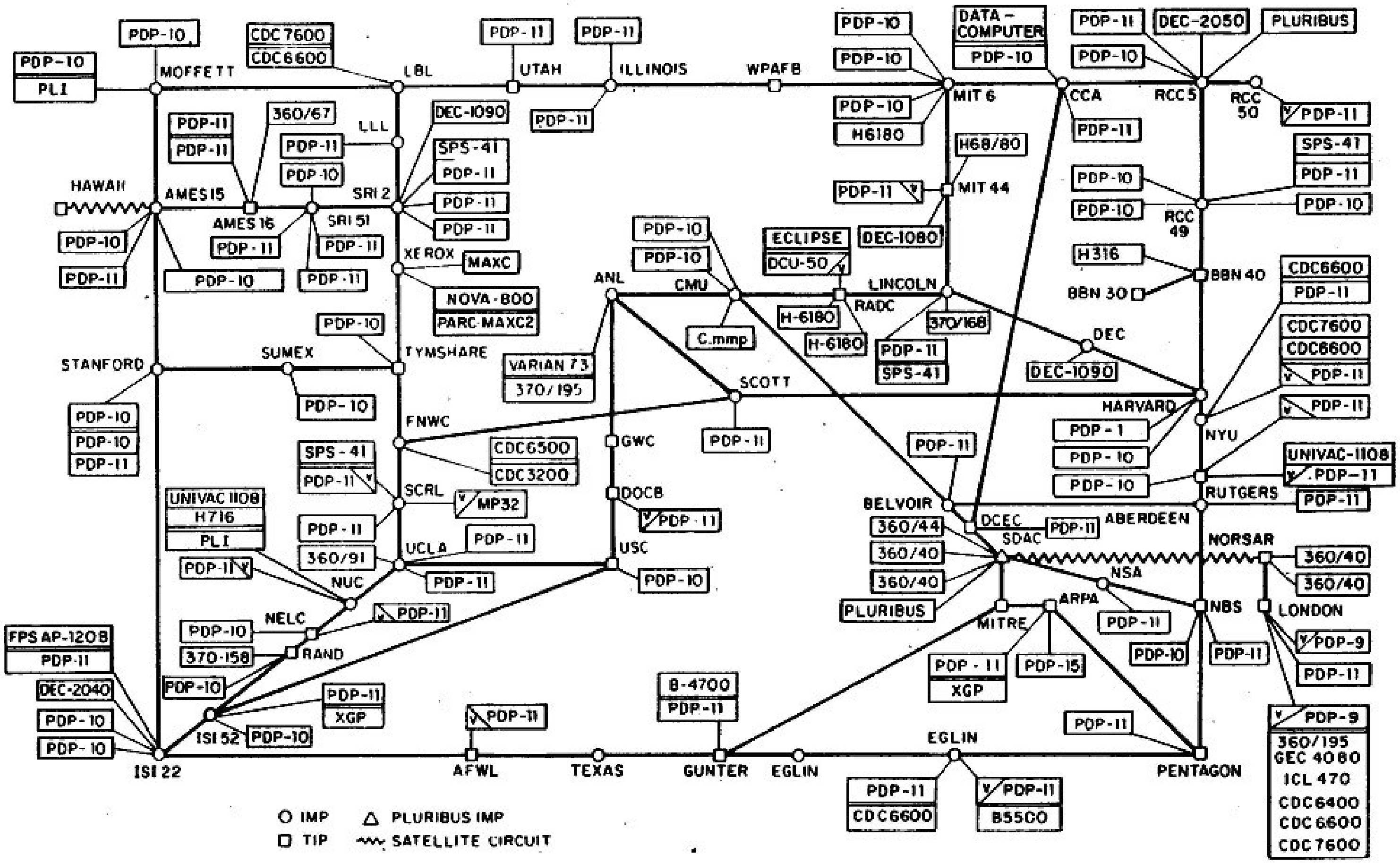
Phone Phreaking



Arpanet Computer

Arpanet

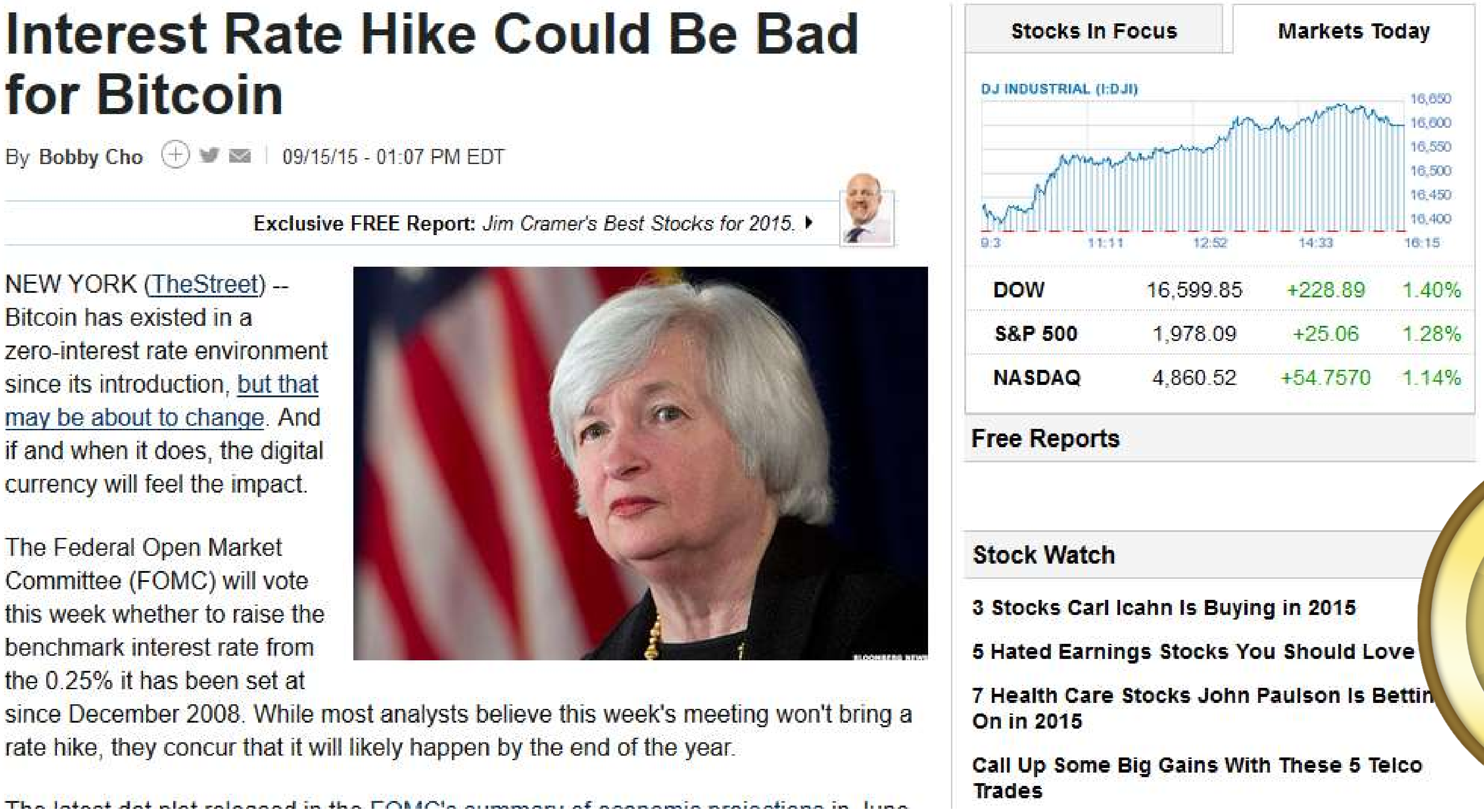
ARPANET LOGICAL MAP, MARCH 1977



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

Bitcoin



Interest Rate Hike Could Be Bad for Bitcoin

By **Bobby Cho** | 09/15/15 - 01:07 PM EDT

Exclusive FREE Report: *Jim Cramer's Best Stocks for 2015.*

NEW YORK (TheStreet) -- Bitcoin has existed in a zero-interest rate environment since its introduction, but that may be about to change. And if and when it does, the digital currency will feel the impact.

The Federal Open Market Committee (FOMC) will vote this week whether to raise the benchmark interest rate from the 0.25% it has been set at since December 2008. While most analysts believe this week's meeting won't bring a rate hike, they concur that it will likely happen by the end of the year.

The latest dot plot released in the FOMC's summary of economic projections in June

Stocks In Focus | Markets Today

DOW	16,599.85	+228.89	1.40%
S&P 500	1,978.09	+25.06	1.28%
NASDAQ	4,860.52	+54.7570	1.14%

Free Reports

Stock Watch

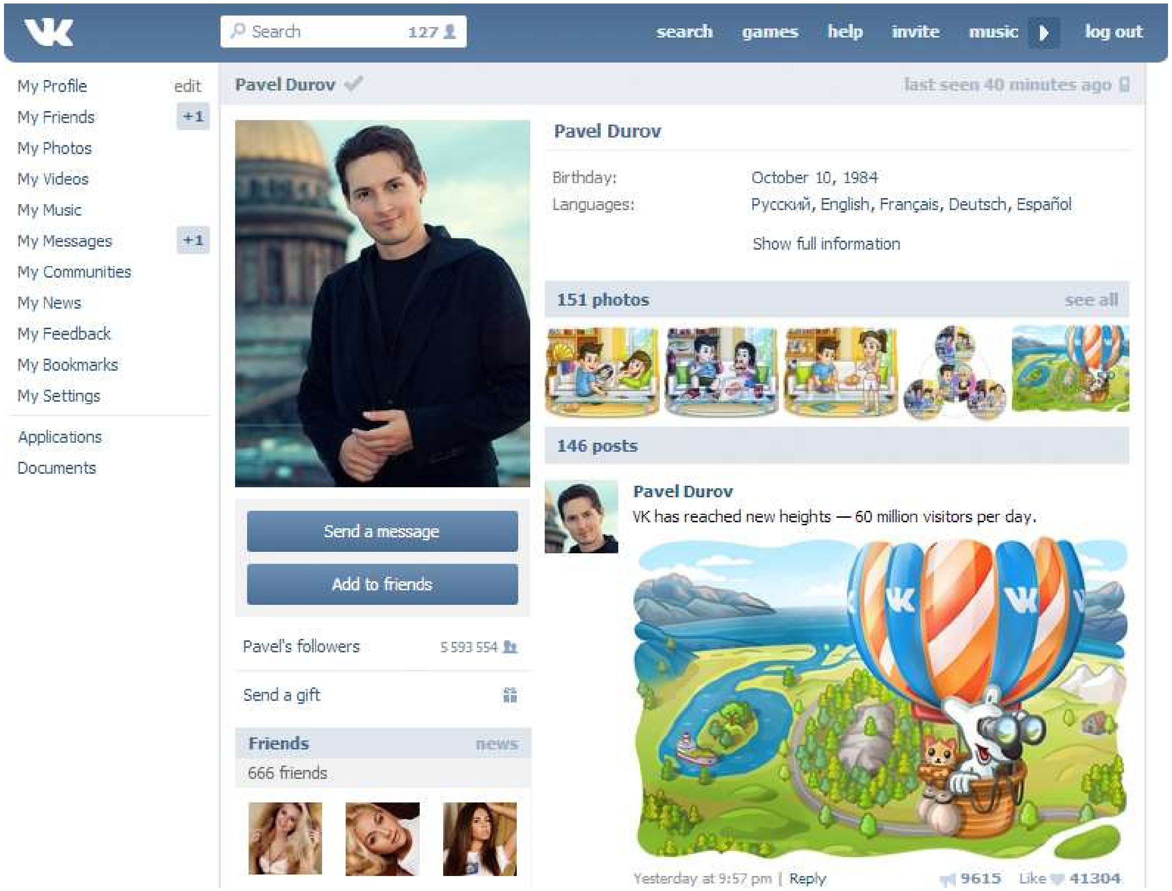
3 Stocks Carl Icahn Is Buying in 2015

5 Hated Earnings Stocks You Should Love

7 Health Care Stocks John Paulson Is Bettin On in 2015

Call Up Some Big Gains With These 5 Telco Trades

VKontatkte



Search 127

search games help invite music log out

My Profile edit
My Friends +1
My Photos
My Videos
My Music
My Messages +1
My Communities
My News
My Feedback
My Bookmarks
My Settings

Applications
Documents

Pavel Durov

last seen 40 minutes ago

Send a message

Add to friends

Pavel's followers 5 593 554

Send a gift

Friends news

666 friends

Pavel Durov

Birthday:	October 10, 1984
Languages:	Русский, English, Français, Deutsch, Español

Show full information

151 photos see all

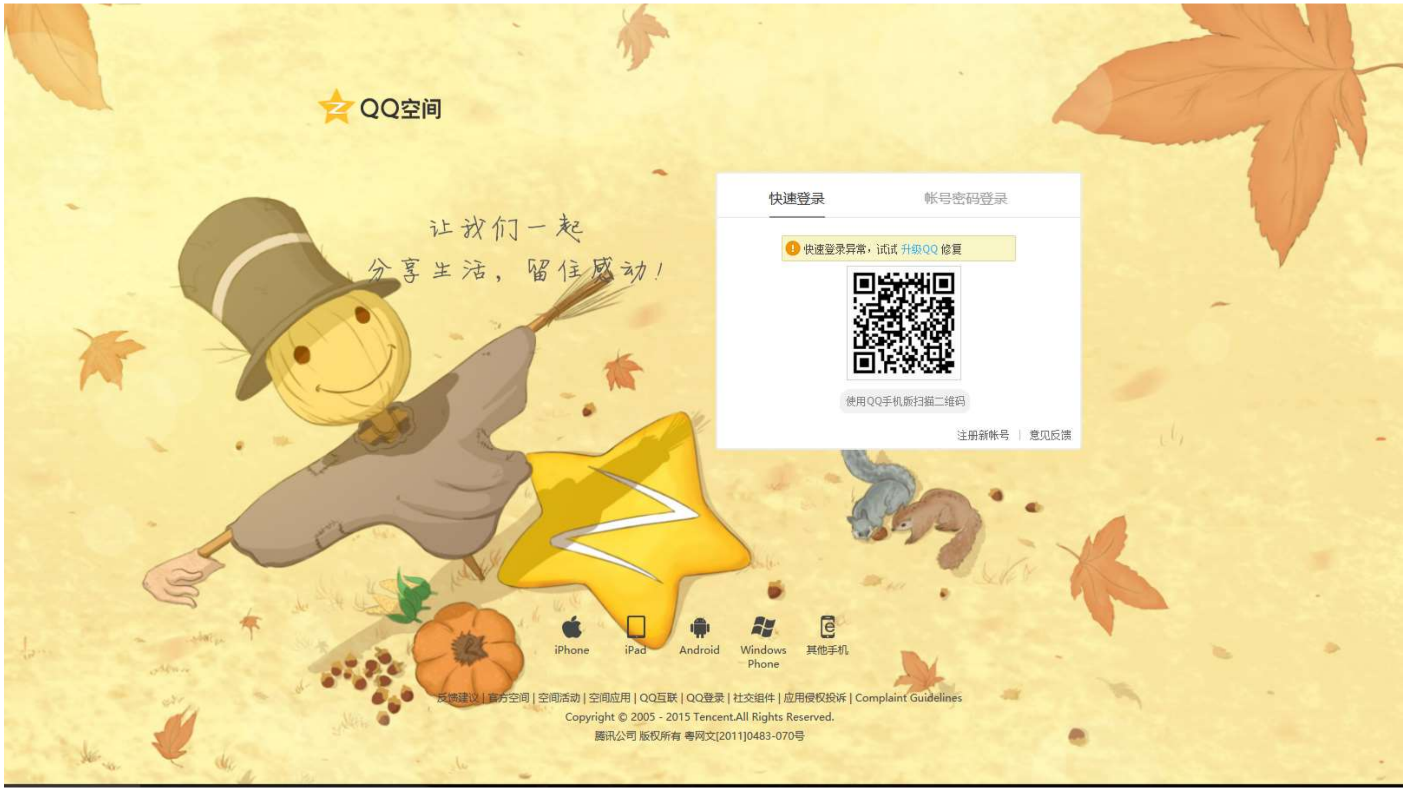
146 posts

Pavel Durov

VK has reached new heights — 60 million visitors per day.

Yesterday at 9:57 pm | Reply 9615 Like 41304

Qzone



快速登录异常，试试 升级QQ 修复

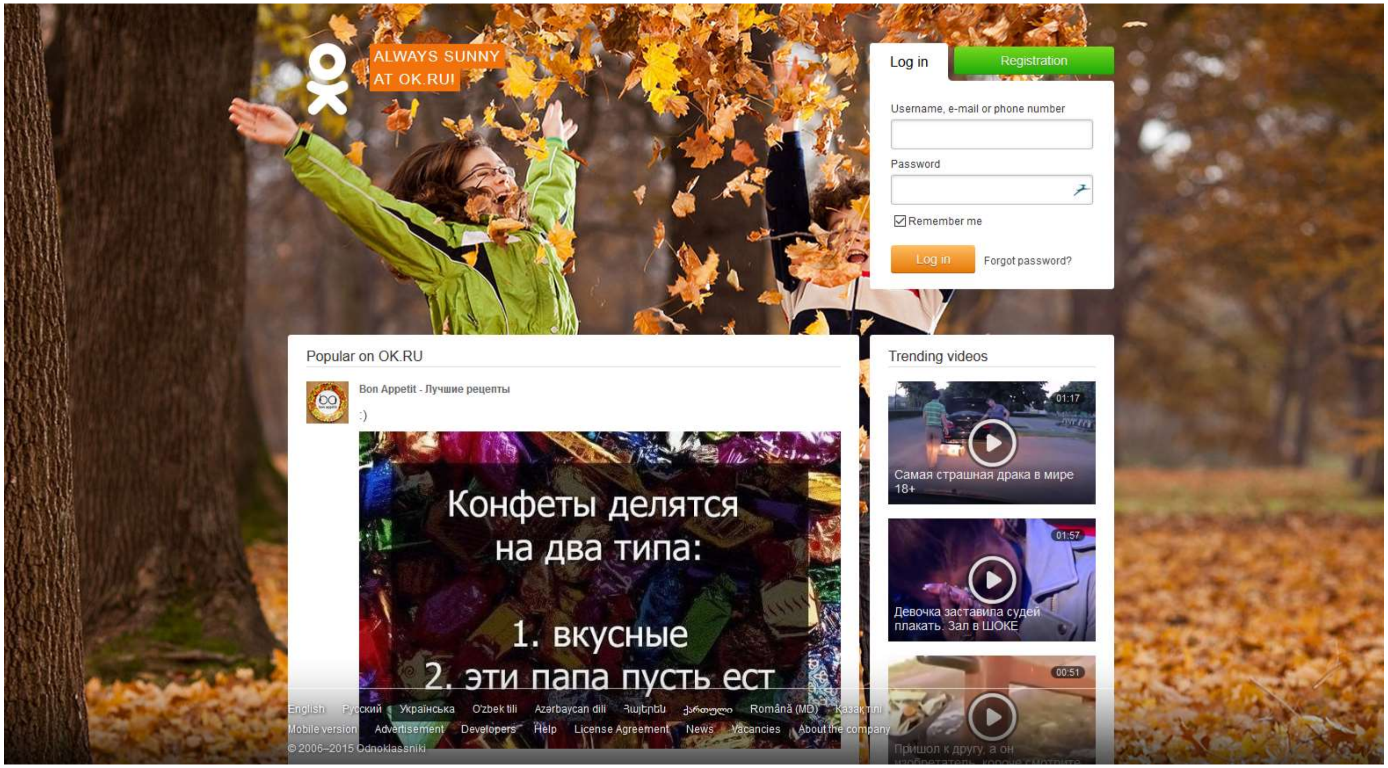
使用QQ手机版扫描二维码

反馈建议 | 官方空间 | 空间活动 | 空间应用 | QQ互联 | QQ登录 | 社交组件 | 应用侵权投诉 | Complaint Guidelines

Copyright © 2005 - 2015 Tencent.All Rights Reserved.

腾讯公司 版权所有 粤网文[2011]0483-070号

Odnoklassni



Bon Appetit - Лучшие рецепты

:)

Конфеты делятся на два типа:

1. вкусные

2. эти папа пусть ест

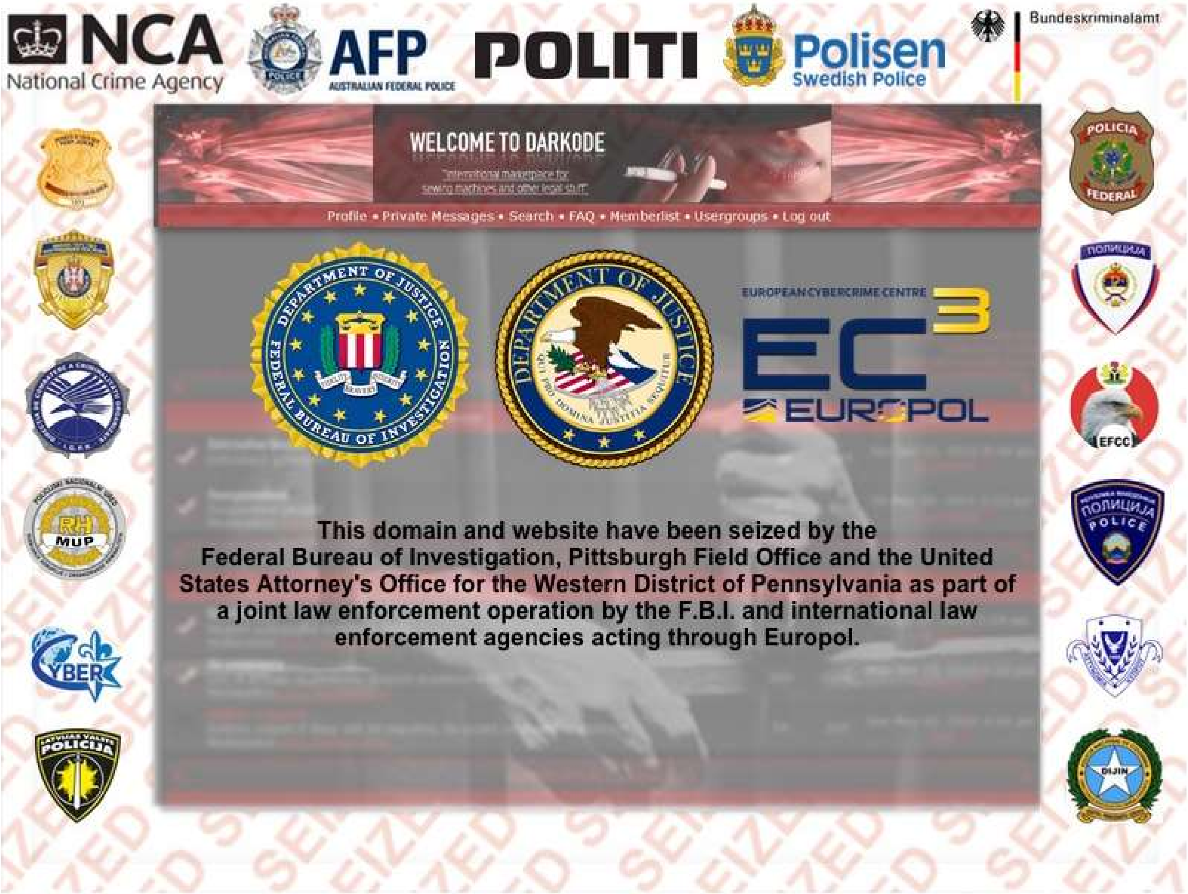
Самая страшная драка в мире 18+

Девочка заставила судей плакать. Зал в ШОКЕ

Пришол к другу, а он изобретатель, короче смотрите

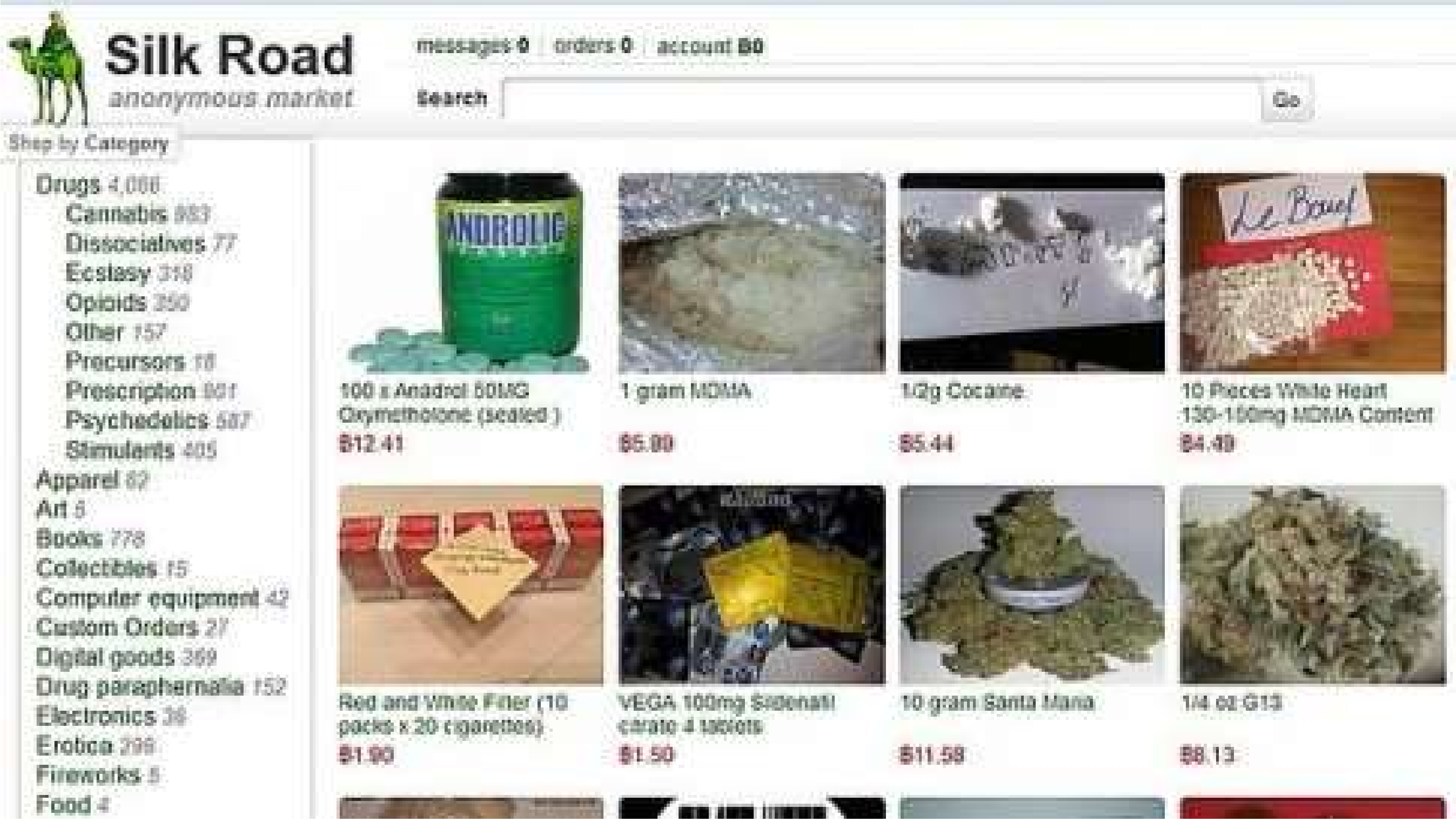
© 2006–2015 Odnoklassniki

Darkode


NCA
National Crime Agency
AFP
AUSTRALIAN FEDERAL POLICE
POLITI
Polisen
Swedish Police
Bundeskriminalamt
WELCOME TO DARKODE
"international marketplace for sewing machines and other legal stuff"
Profile • Private Messages • Search • FAQ • Memberlist • Usergroups • Log out
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL
POLICIA FEDERAL
ПОЛИЦИЈА
EFCC
ПОЛИЦИЈА POLICE
DIJIN
MUP
CYBER
POLICIJA

This domain and website have been seized by the Federal Bureau of Investigation, Pittsburgh Field Office and the United States Attorney's Office for the Western District of Pennsylvania as part of a joint law enforcement operation by the F.B.I. and international law enforcement agencies acting through Europol.

Silk Road



Silk Road
anonymous market

messages 0 | orders 0 | account ฿0

Search [ ] Go

Shop by Category

- Drugs 4,088
  - Cannabis 883
  - Dissociatives 77
  - Ecstasy 318
  - Opioids 350
  - Other 157
  - Precursors 18
  - Prescription 801
  - Psychedelics 587
  - Stimulants 405
- Apparel 62
- Art 5
- Books 778
- Collectibles 15
- Computer equipment 42
- Custom Orders 27
- Digital goods 369
- Drug paraphernalia 152
- Electronics 38
- Erotica 298
- Fireworks 5
- Food 4

100 x Anadrol 50MG Oxymetholone (sealed)
฿12.41

1 gram MDMA
฿5.89

1/2g Cocaine
฿5.44

10 Pieces White Heart 130-150mg MDMA Content
฿4.49

Red and White Filter (10 packs x 20 cigarettes)
฿1.90

VEGA 100mg Sildenafil citrate 4 tablets
฿1.50

10 gram Santa Maria
฿11.58

1/4 oz G13
฿8.13

APT1

Lizard Squad

Chelsea Manning

Snowden

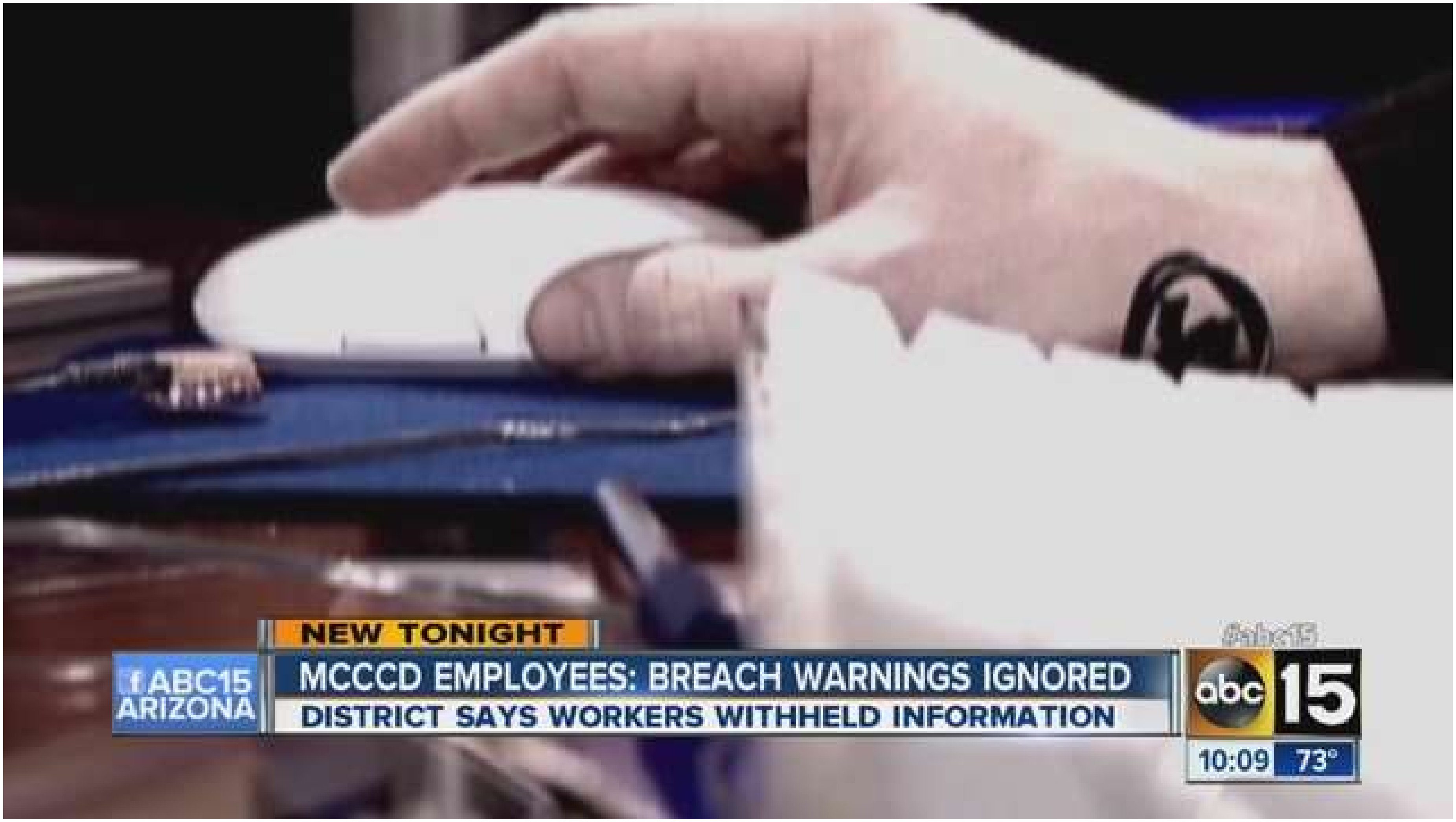
2014

- 312 breaches
  - Up from 253 in 2013
- 1.1 million identities exposed on average
- Top three sectors
  - Healthcare
  - Retail
  - Higher education

Yikes!

- Average cost of breach
  - $217 per record
- Average organizational cost
  - $6.53 million
- Higher Education average cost
  - $300 per record
  - 150,000 identities
    - $45 million in direct and indirect costs

What happens to those that deal poorly?


NEW TONIGHT
ABC15 ARIZONA
MCCCD EMPLOYEES: BREACH WARNINGS IGNORED
DISTRICT SAYS WORKERS WITHHELD INFORMATION
#abc15
abc 15
10:09
73°

Maricopa

- Multiple breaches
- Board refused to fix issues
  - Political battles
- 2 class action lawsuits
  - Average compensatory damage request
    - <u>$3000 per claimant</u>
  - 2.5 million identities
  - Maximum claim of $15 billion dollars
  - There is a cap
- 2 FTC complaints

Do we care?

- 76% of citizens surveyed said they felt stress as a result of being notified
- 57% of consumers said they would discontinue or be less likely to continue a relationship with a company that lost their info
- On average 6% “churn” rate
- Do we follow through with these sentiments?

11 Worst Breaches of all time

- Heartland Payment Systems, 2008-2009: 130 million records compromised
- Target Stores, 2013: 110 million records compromised
- Sony online entertainment services, 2011: 102 million records compromised
- National Archive and Records Administration, 2008: 76 million records compromised
- Anthem, 2015: 69 million to 80 million records compromised
- Epsilon, 2011: 60 million to 250 million records compromised
- Home Depot, 2014: 56 million payment cards compromised
- Evernote, 2013: More than 50 million records compromised
- Living Social, 2013: More than 50 million records compromised
- TJX Companies Inc., 2006-2007: At least 46 million records compromised
- LastPass – 2013, 2015 – multiple computer password hashes lost

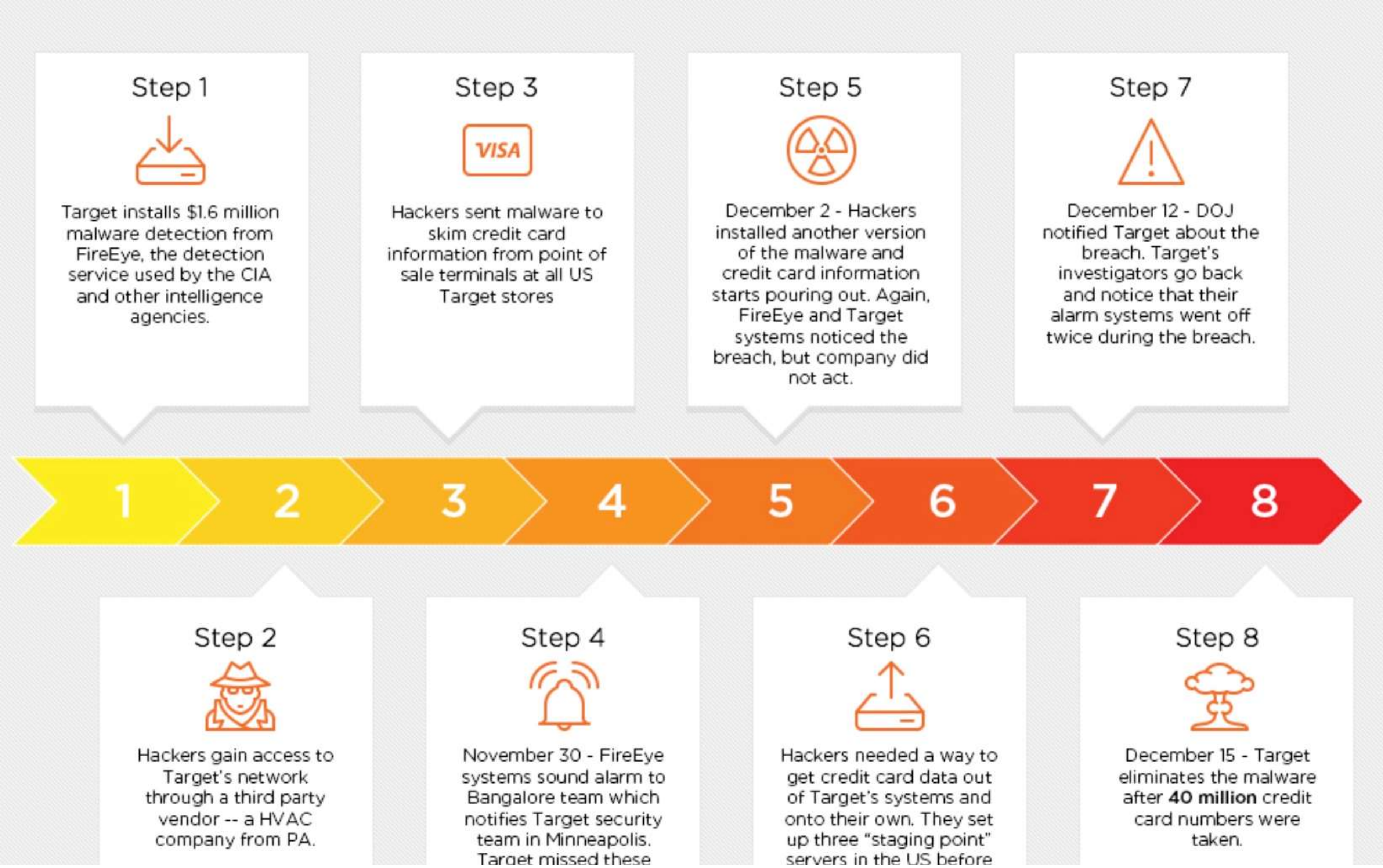
Sony Pictures

Hacked By #GOP
y warned you, and this is just a beginning.
till our request be met.
tained a yo r inte al da includi our s crets an top secre
If you don't obey s, e'll se data show low to e worl
Determine what ill y u d till ove the
Data Link :
HACKED
SONY
PICTURES

Sony Pictures

- Perpetrated by Lizard Squad (as GOP)
- May have been hired by North Korea (Schneir)
- Paid fired Sony system administrators for inside information
- FBI investigation continues
- Will cost Sony 35 million to repair holes
- Although no bottom line impact it remains to be seen if the brand damage will prevent talent from working on Sony pictures.
- Began with phishing attack to iPhones

Target



Step 1

Target installs $1.6 million malware detection from FireEye, the detection service used by the CIA and other intelligence agencies.

Step 2

Hackers gain access to Target's network through a third party vendor -- a HVAC company from PA.

Step 3

Hackers sent malware to skim credit card information from point of sale terminals at all US Target stores

Step 4

November 30 - FireEye systems sound alarm to Bangalore team which notifies Target security team in Minneapolis. Target missed these

Step 5

December 2 - Hackers installed another version of the malware and credit card information starts pouring out. Again, FireEye and Target systems noticed the breach, but company did not act.

Step 6

Hackers needed a way to get credit card data out of Target's systems and onto their own. They set up three "staging point" servers in the US before

Step 7

December 12 - DOJ notified Target about the breach. Target's investigators go back and notice that their alarm systems went off twice during the breach.

Step 8

December 15 - Target eliminates the malware after **40 million** credit card numbers were taken.

Target

- Began as an intrusion from a third party vendor system to work on their HVAC system
- Compromised the POS terminal at all of their stores
- Target systems detected intrusion within an hour of it occurring
- Team in India notified the team in Minneapolis
- more than 2 weeks before they were actually responding to it but by then it was too late.

Damage

- 40 million credit and debit cards numbers
- 46% drop in profit in the 4th quarter of 2013
- Cost to bank and credit unions to reissue cards - 200 million dollars
- 100 million to upgrade all terminals
- Class action lawsuit - 10 million
- Total cost in excess of 1 billion dollars
- Now Target has laid off 13 percent of its workforce in the 1st quarter of 2015

Wait . . .

- 46% drop in profit
- Stock price drops to 1/2 of its original trading price (it has since rebounded)
- CEO - gone
- CIO - gone as well as a large amount of mid level managers
- And now laying off 13% of its workforce?
- Probably not their business objectives

Root Cause?

- Definition of business value
- My definition
  - Balance of governance and growth
- Profits only mindset
  - Leaving support activities unfunded or understaffed
- Government and non-profits
  - Value is being defined as cost reduction only
  - Not in the quality of services

BUMMER
quickmeme.com

What can you do?

- Don’t use personal information when it’s not necessary.
- Keep a list of who has your data
- Use secure passwords
- Encryption is good ☺
- Make sure and lock down your WiFi
- Ask questions of those who want your personal info

What can you do?

- When in doubt throw it out - Data Privacy Day – Jan 28th
- Report any problems/concerns to www.ic3.gov
- Backup your important data
- Be careful using public hotspots - limit what you do on those sites
- Strong passwords
- Use a good Antivirus solution - many are available for free
- Phishing

What can we all do?

- Talk to your local representatives
- Talk with your business
- Be an advocate in the community
- Participate in Cyber Security Awareness Month Oct

Education

- Cyber security literacy in elementary school through college
- All empowered leads to more difficult to fool

Board Visibility

- Take Cyber Threat seriously
- All boards
  - Profit
  - Non-profit
  - Educational
- Recognize the cost of assuming risk

Law Enforcement Support

- Need tools to do their job
- They DO NOT need shortcuts that sacrifice our privacy

Collaboration

- Threat is shared
- Bad guys exploit our
  - own selfish self interests
  - Siloes
  - Bureaucracy
- Cost should be shared
- Information needs to be able to assist without creating jeopardy

Mongol Success

- City states were isolated and didn't work together
  - Fewer numbers
  - Less resources
- Mongols in Eastern Europe
- Keys to winning

Finally

- Collaboration is key
- Transparency
- Amplify the effect of our resources
- Develop sharing methods
- Secrecy can be used against us
- Trust across all sectors

Questions?

- Thank You!