RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

Illuminating the Deep Dark Web with drugs, exploits, and zero-days

CLE-R09

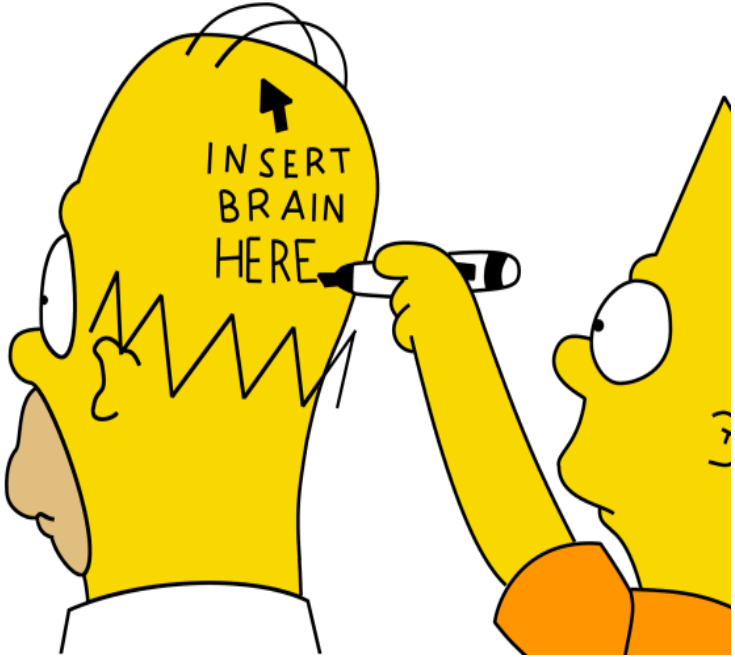
Jack Chan

Security Strategist
FortiGuard Advanced Labs, Fortinet
@FortiGuardLabs

#RSAC

WARNING

- Presentation contains real world attacker methods and demos
- Some material is not suitable to all audiences
- Use common sense and ethical guidelines
- Don’t be Homer Simpson



Who are we...

Aamir Lakhani

Researcher / Consultant
Ninja / Pirate / Hacker

FEDERAL NEWS RADIO.com 1500 AM

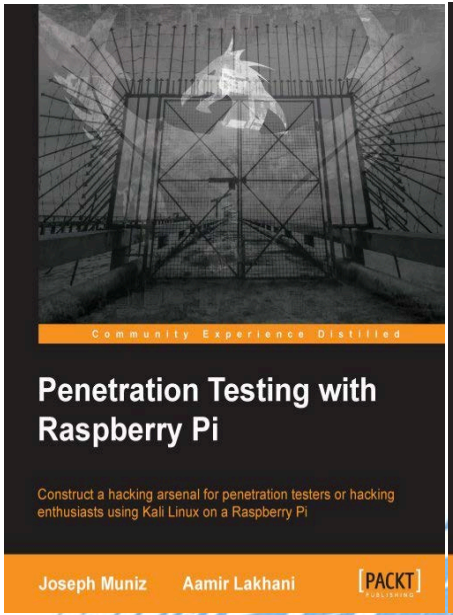
HACKERS FOR CHARITY.ORG

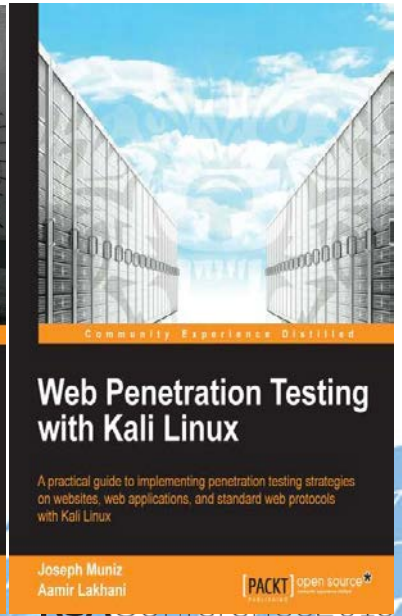
DR. CHAOS
WWW.DRCHAOS.COM

Jack Chan

Security Strategist, consultant

Time Magazine's Person of the Year 2006…





And so were...


DECEMBER 25, 2006 / JANUARY 1, 2007
www.time.com
TIME
PERSON OF THE YEAR
You.
00:00/20:06
Yes, you.
You control the Information Age.
Welcome to your world.

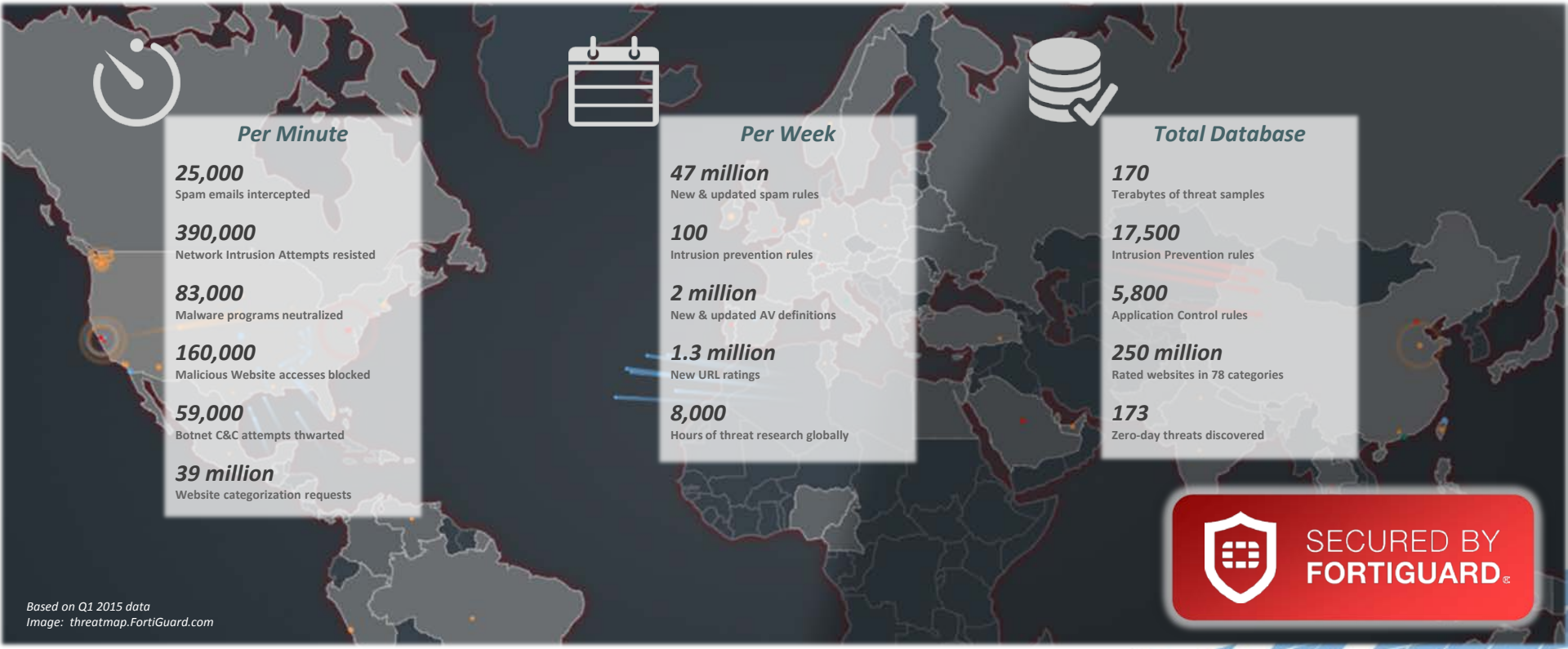
"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012

Fortinet Advantage – FortiGuard Labs Threat Research

#RSAC

The FortiGuard Minute



Based on Q1 2015 data
Image: threatmap.FortiGuard.com

Deep Web

Invisible web

Hidden web

1994

- Dr. Jill Ellsworth used the term *Invisible Web*

2001

- The first use of the specific term *Deep Web* occurred in Michael Bergman study

The anonymous Internet

Daily Tor users per 100,000 Internet users

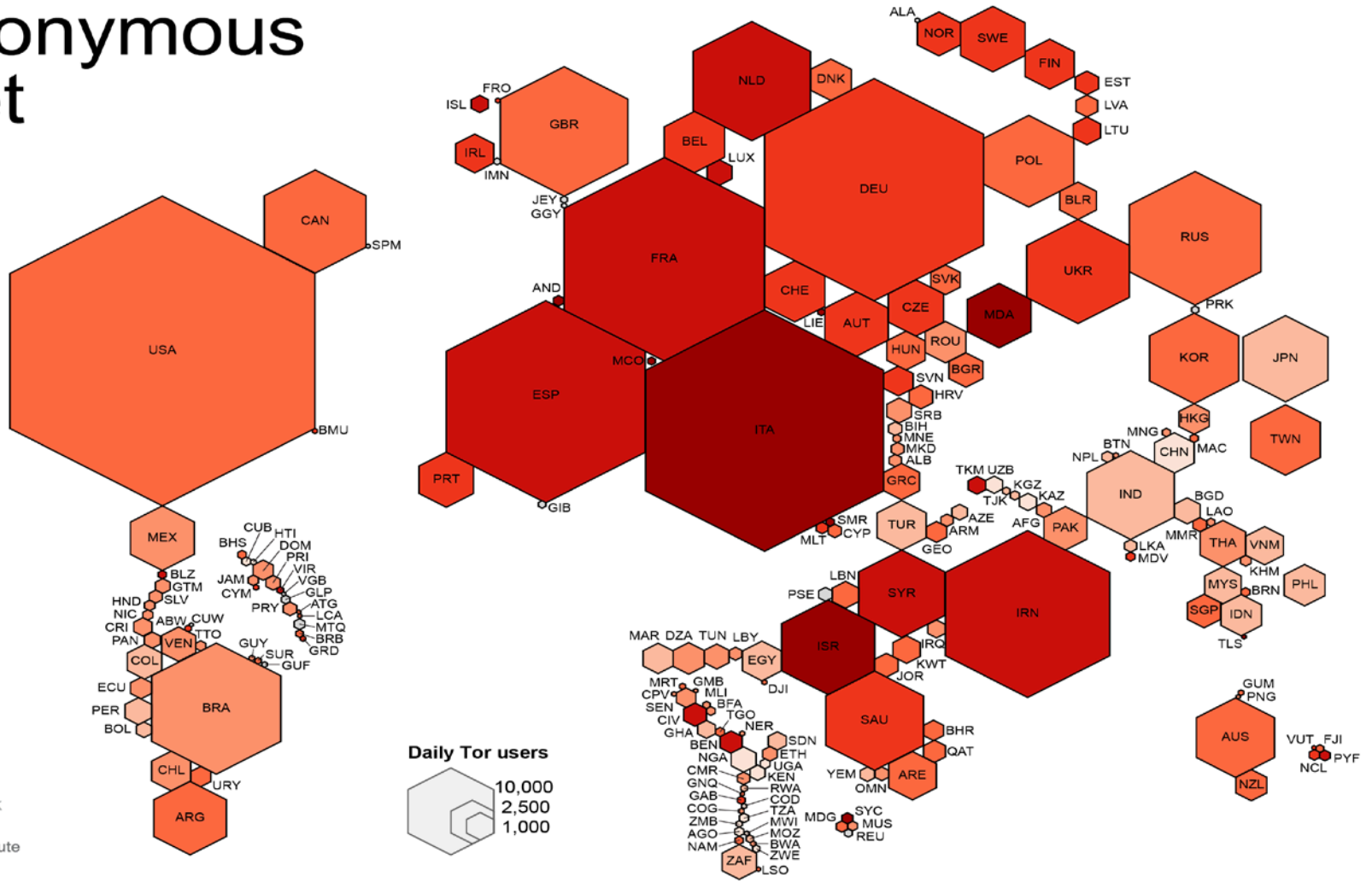
- > 200
- 100 - 200
- 50 - 100
- 25 - 50
- 10 - 25
- 5 - 10
- < 5
- no information

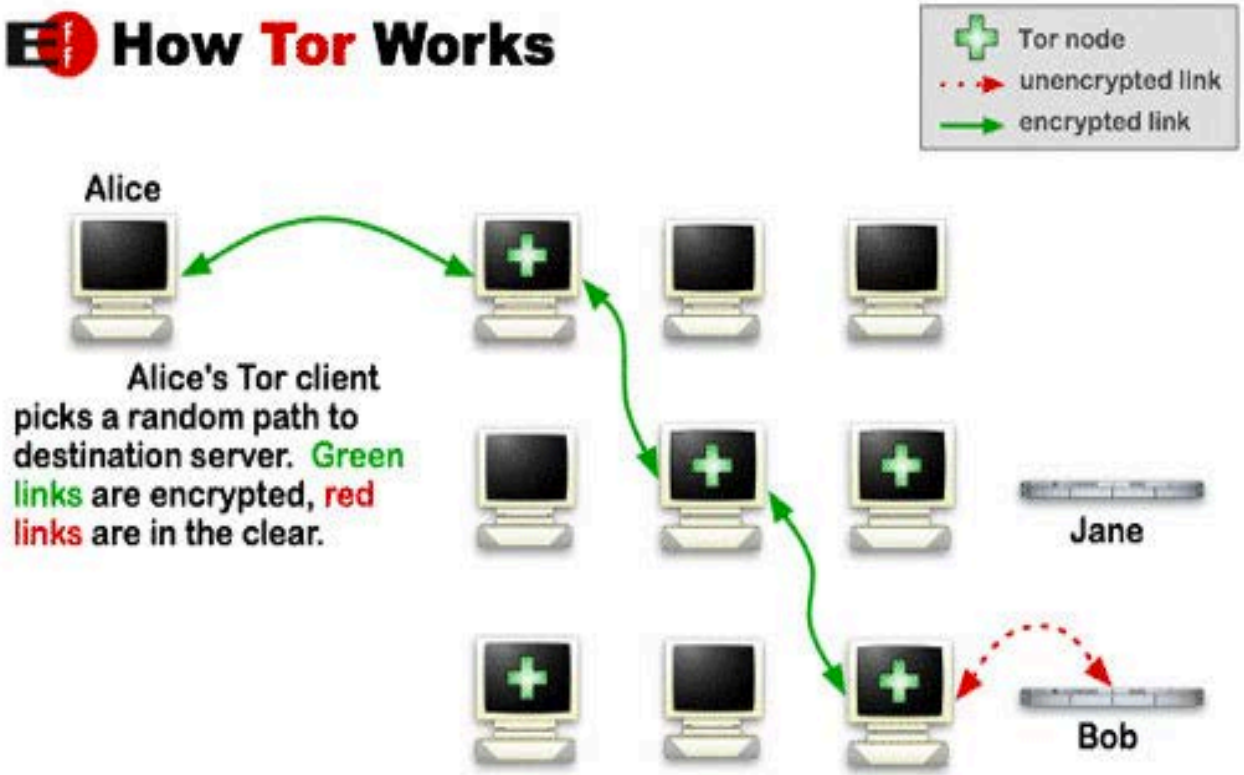
Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk

Oxford Internet Institute
University of Oxford

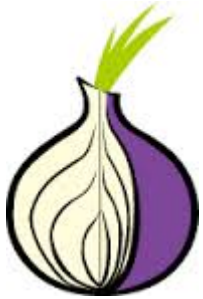




Source: TOR Project

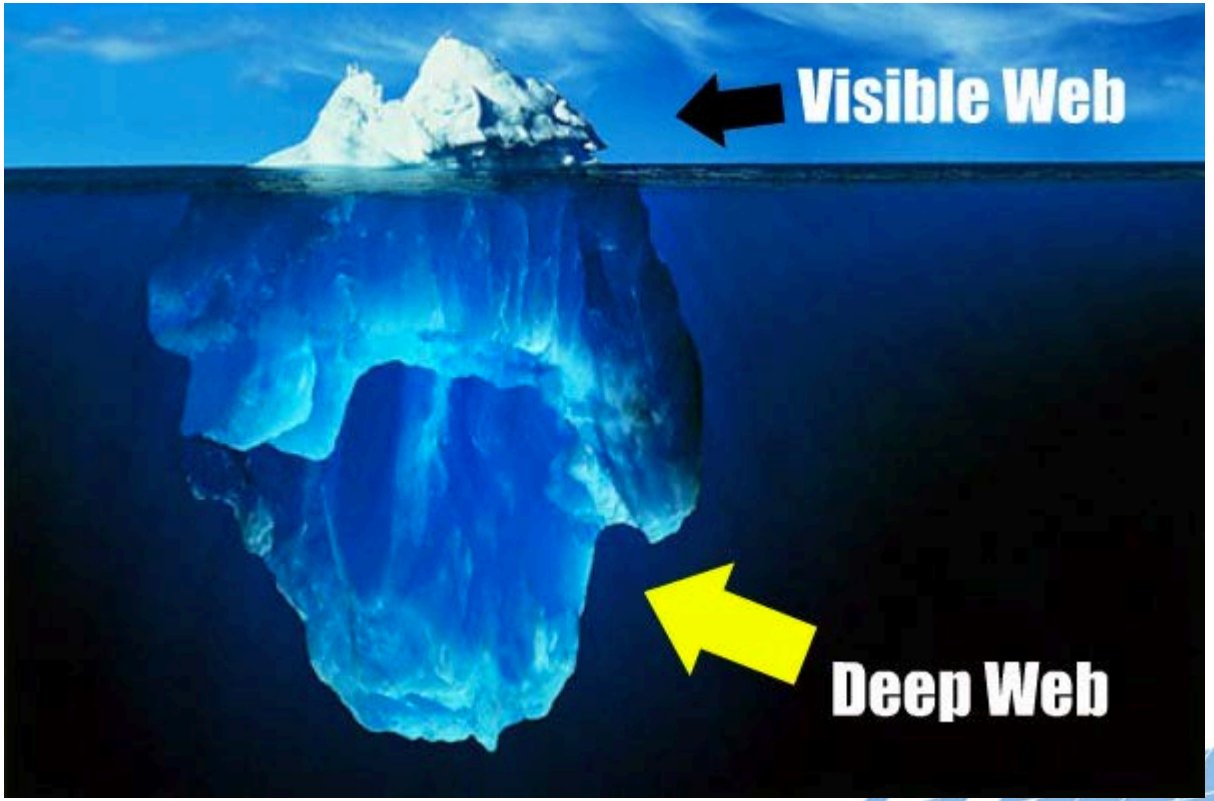
.Onion

- Works like a top-level domain
- Tor Hidden Services
- Can be hosted or Peer-to-Peer
- Can be found by search engines only if they want to be
- Must be on the TOR network or use a Web-to-TOR proxy to access
- Looks like this: http://3g2upl4pq6kufc4m.onion/ - DuckDuckGo Search
- Used for legitimate sites like Facebook and human right groups
- Used for illegal services and forums for illegal activity
- We are starting to see .onion sites with SSL – but that may actually reduce anonymity



The Deep Web

- 1000X larger?
- 7Tb observed
- More than just WWW services
- Different levels of Deep Web

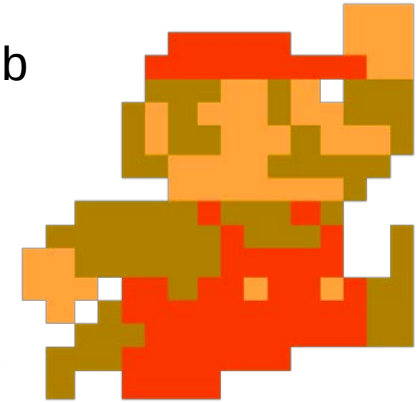


Why Search Engines Can’t find them

- Private web
- Unlinked content
- Dynamic content
- Limited-access content
- Non-HTML content
- Hidden source code

Playing the Levels

- Level 0: Common Web
- Level 1: Surface Web
  - Reddit
  - Digg
  - Temp Email Services
- Level 2: Bergie Web
  - Google locked results
  - Honeypots
  - 4Chan, Newsgroups, FTP, other services
  - Freehive, Bunny Tube, Streams



- Level 4: Charter Web
  - Hacking Groups
  - Shelling Networking
  - AI Theorist
  - Banned media
  - Activist communications
- Level 5:
  - Onion Sites
  - Illegal Material
  - Human Trafficking, Bounty Hunters, Rare Animal Trade
  - Exploits, Black Markets, Drugs

Deep Web Level 8

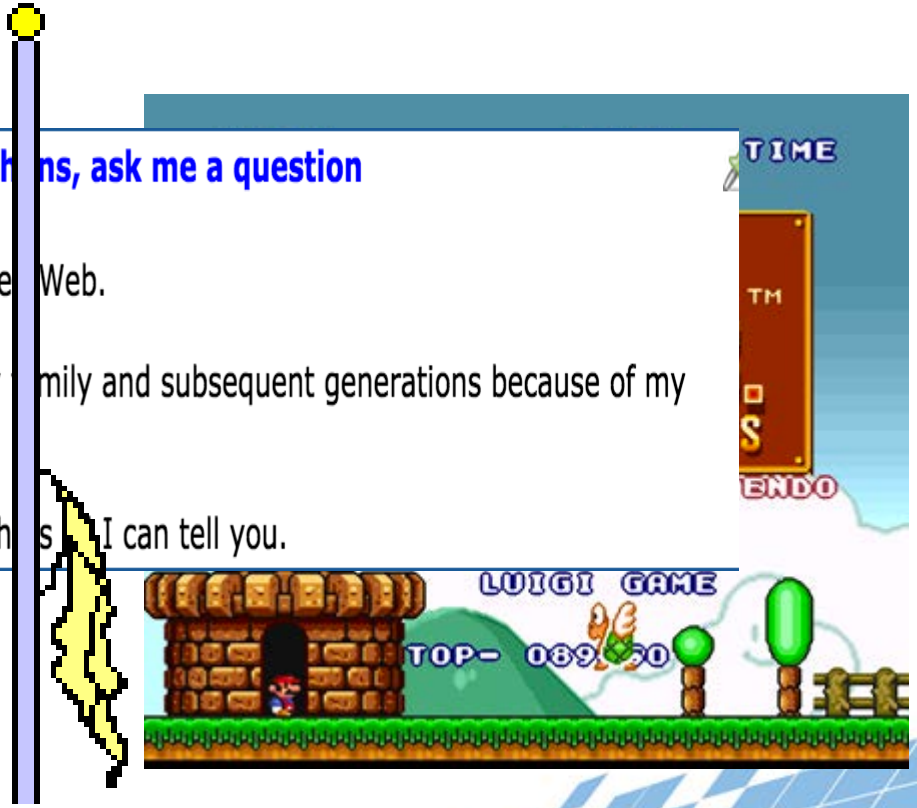
- What happened to levels 6 – 7?
- Made up, BS, Fake?

I entered the 8th Level of the Deep Web and met the Arch ns, ask me a question

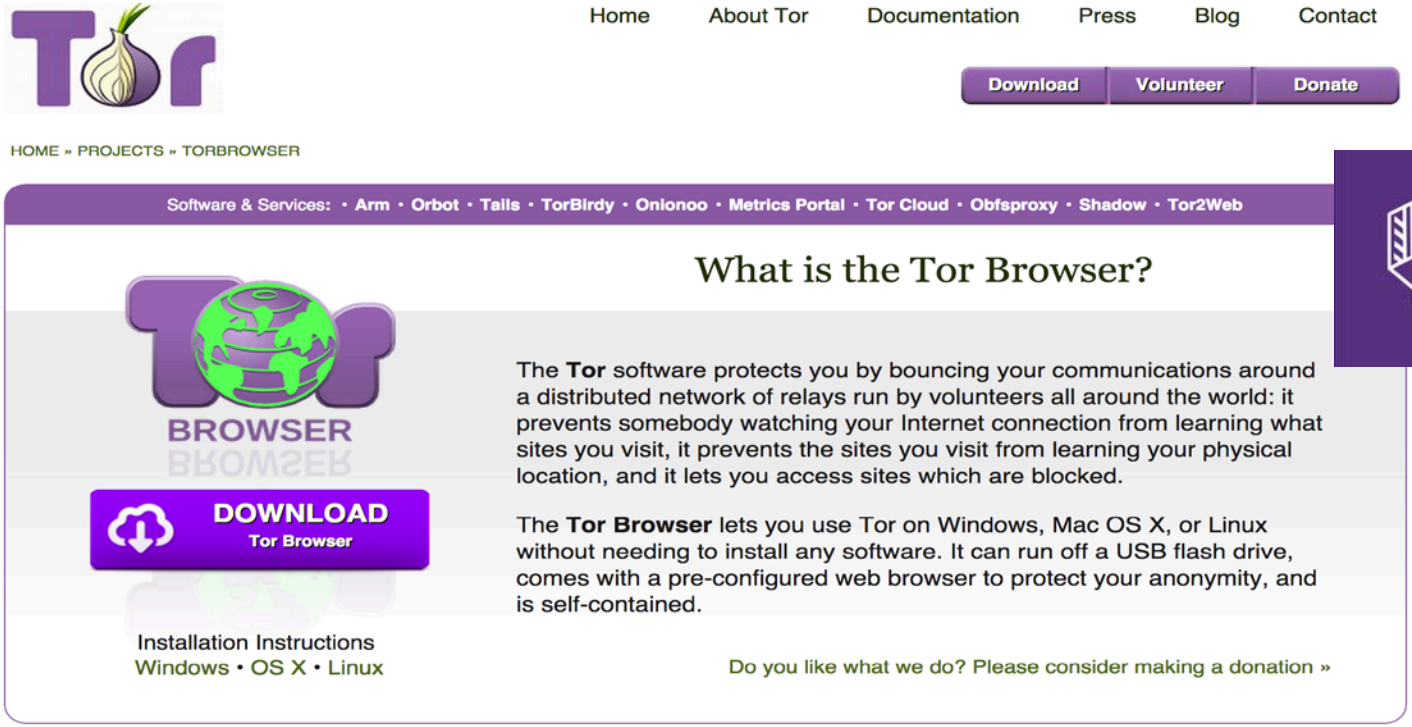
Believe it or not but I managed to enter the 8th level of the Dee Web.

How am I still alive? Well, they said they won't touch me or my mily and subsequent generations because of my accomplishment.

You do not need superior hacking skills to enter the 8th Level th s I can tell you.

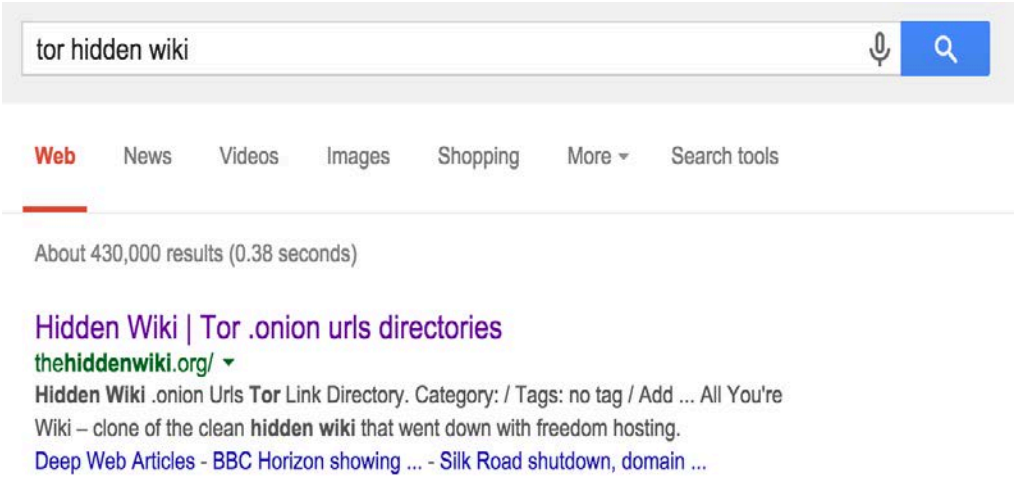


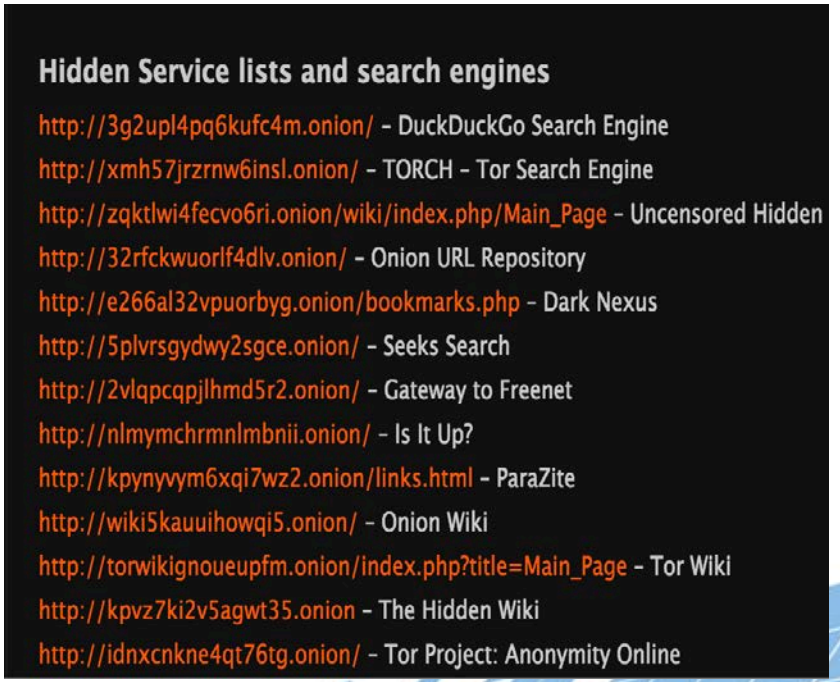
Jumping On


Home
About Tor
Documentation
Press
Blog
Contact
Download
Volunteer
Donate
HOME » PROJECTS » TORBROWSER
Software & Services: · Arm · Orbot · Tails · TorBirdy · Onionoo · Metrics Portal · Tor Cloud · Obfsproxy · Shadow · Tor2Web
What is the Tor Browser?
BROWSER
DOWNLOAD
Tor Browser
The Tor software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.
The Tor Browser lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained.
Installation Instructions
Windows • OS X • Linux
Do you like what we do? Please consider making a donation »
Tails
theamnesicincognitolivesystem

Tor Hidden Wiki – The First Place You will go to feel Dark

- Collection of hidden links and .onion sites
- How hard is it to find?





U.S. Immigration and Customs Enforcement

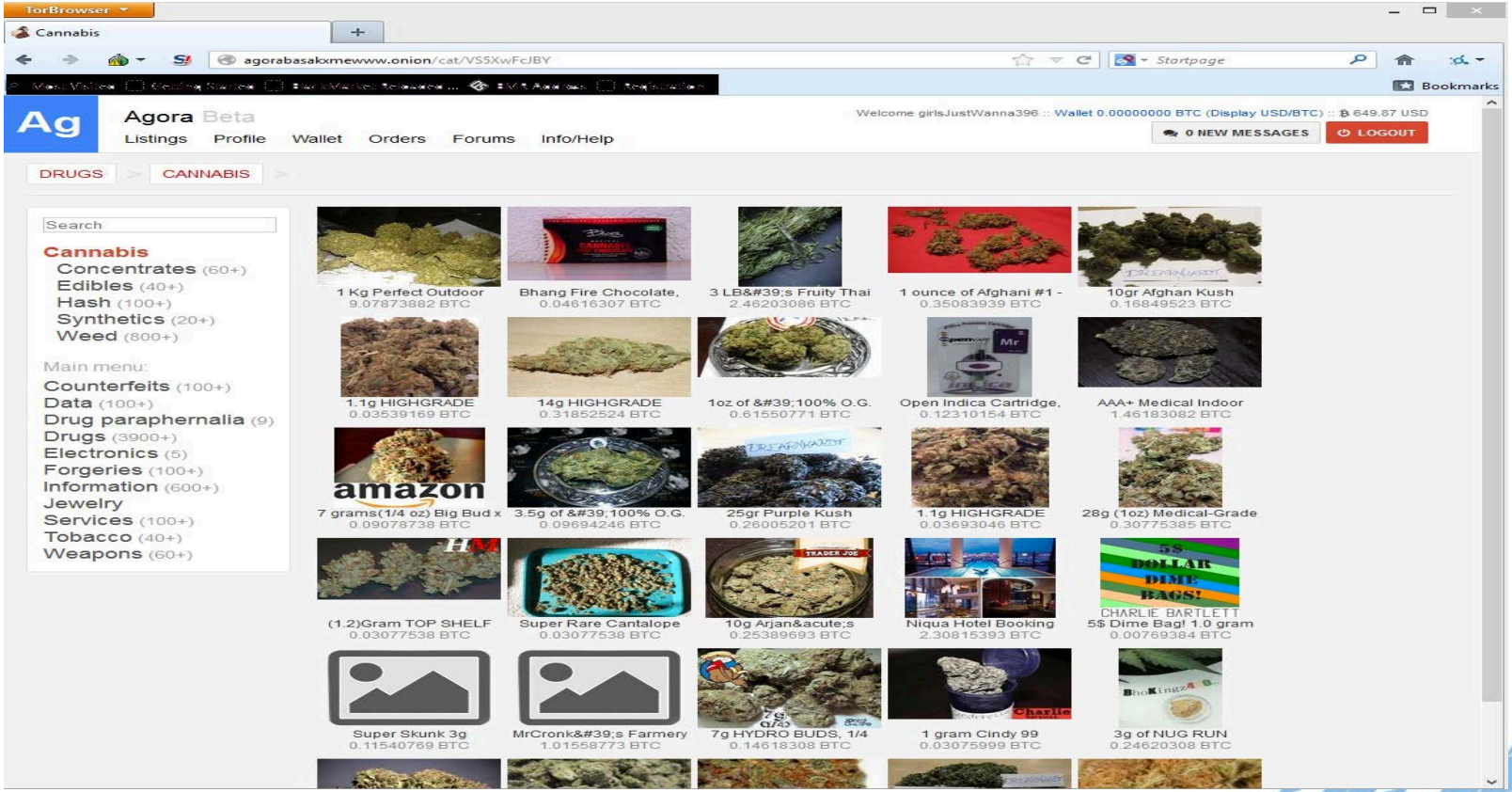
THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

- Mind-reeling amount of information
- Powerful
- Secure
- Free of surveillance
- You can get anything

Agora Market



Ag

Agora Beta

Listings Profile Wallet Orders Forums Info/Help

Welcome weiss96 :: Wallet 0.00000000 BTC :: ฿ 383.77 USD

0 NEW MESSAGES LOGOUT

#RSAC

COUNTERFEITS > ACCESSORIES >

Search

Counterfeits
- **Accessories** (60+)
- Clothing (200+)
- Electronics (20+)
- Money (60+)
- Watches (300+)

Main menu:

Counterfeits (600+)
Data (400+)
Drug paraphernalia (100+)
Drugs (12800+)
Electronics (100+)
Forgeries (200+)
Information (1400+)
Jewelry (100+)
Services (500+)
Tobacco (200+)
Weapons (100+)
Other (100+)

Louis Vuitton Eva Clutch

0.15633956 BTC
This stylish Louis Vuitton Eva Clutch comes with a golden chain wrist strap and a leather cross shoulder strap.

The real ones go for $775. You can own this identical version for just $60.
Brought to you by:
MagicHat 4.82/5, 300~500 deals

From: USA
To: Worldwide

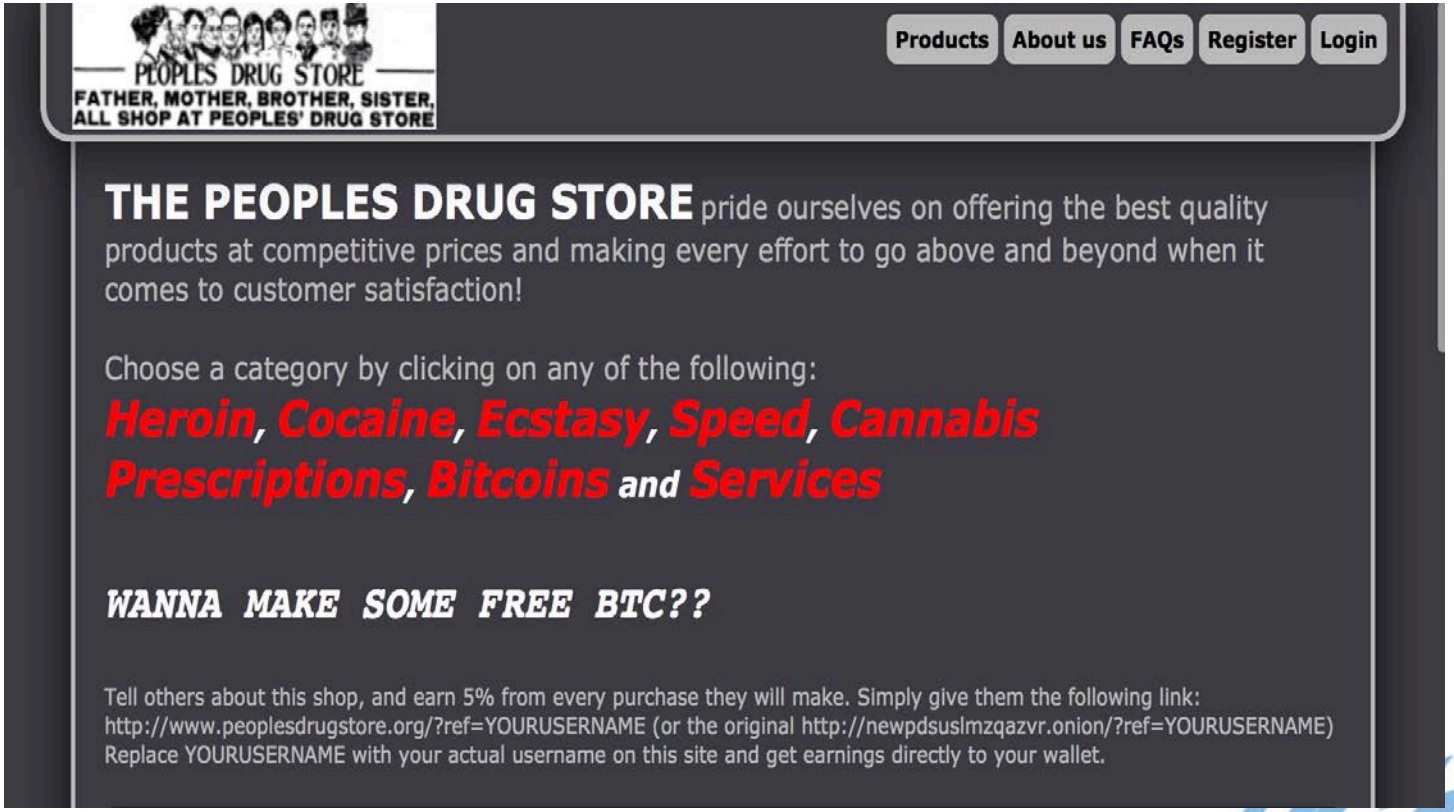
0.15633956 BTC

BUY...

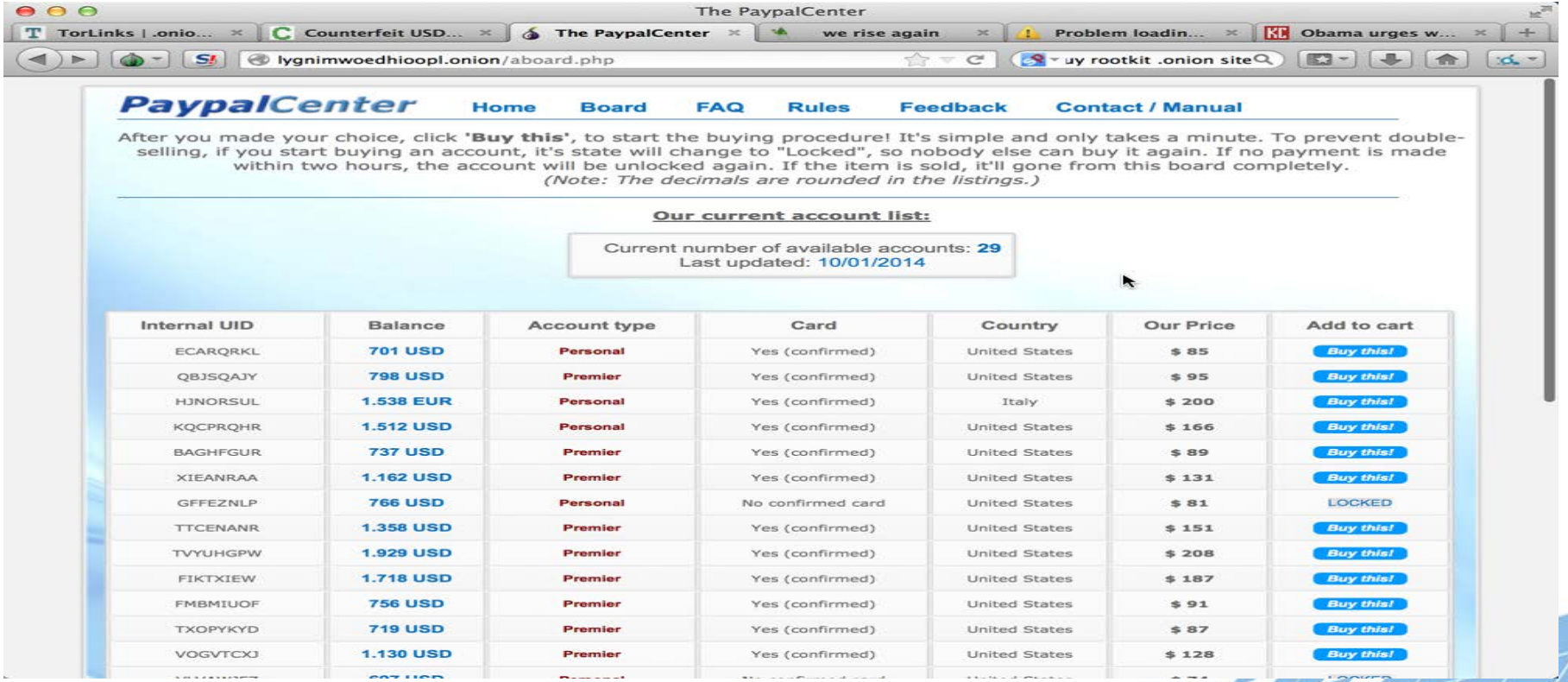
Feedbacks:

5/5	Terrific Vendor. Awesome product! Can't wait to order more :) Thanks MagicHat!	38 days ago	anon ~5/5, 6~10 deals
5/5		84 days ago	anon ~5/5, 10~15 deals
5/5	Looks just as good as my real LV. Great product...looking for more LV	122 days	anon ~2/5, 3~5

Crime is Thriving

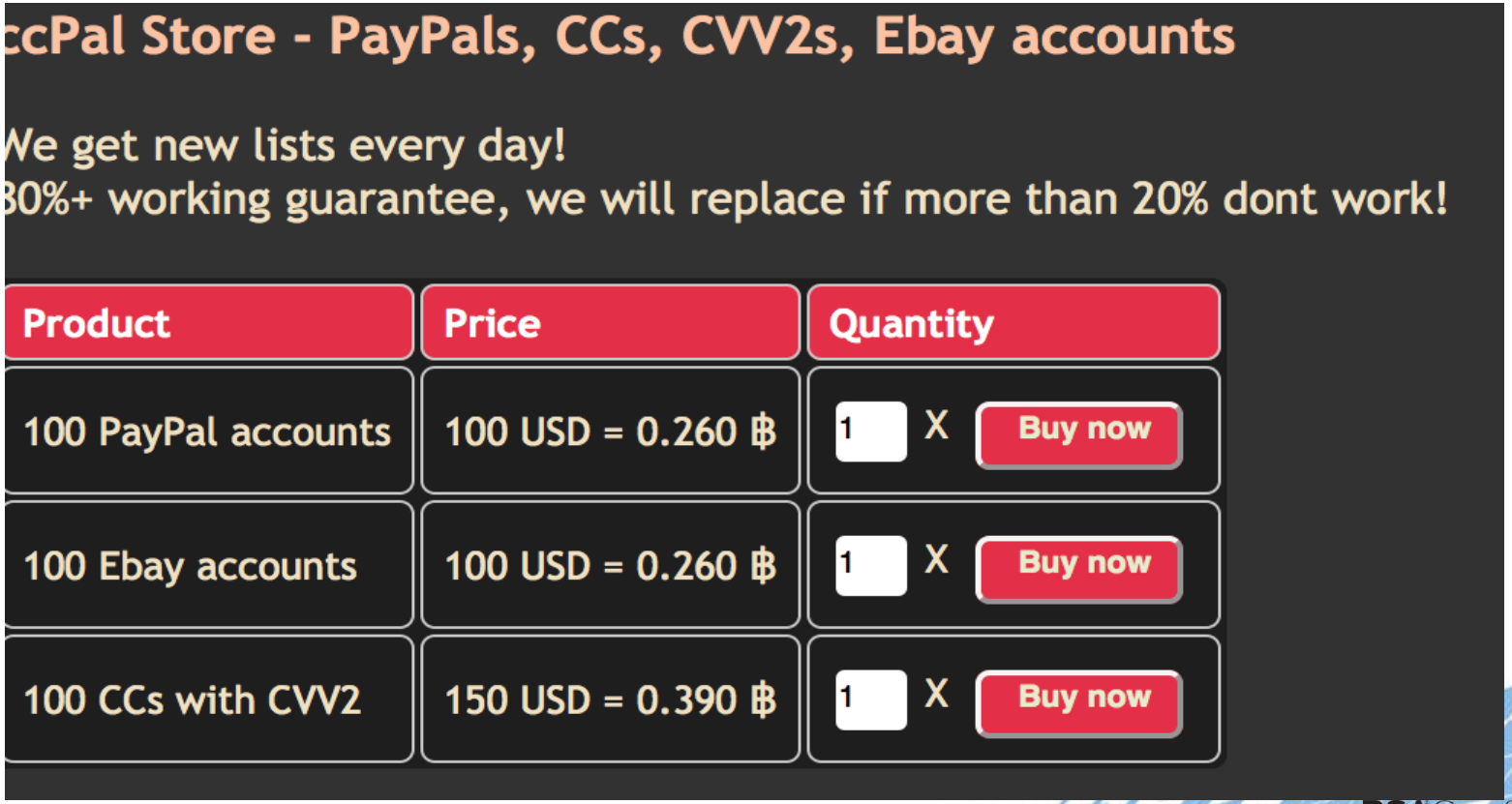


The Real Secret of PayPal



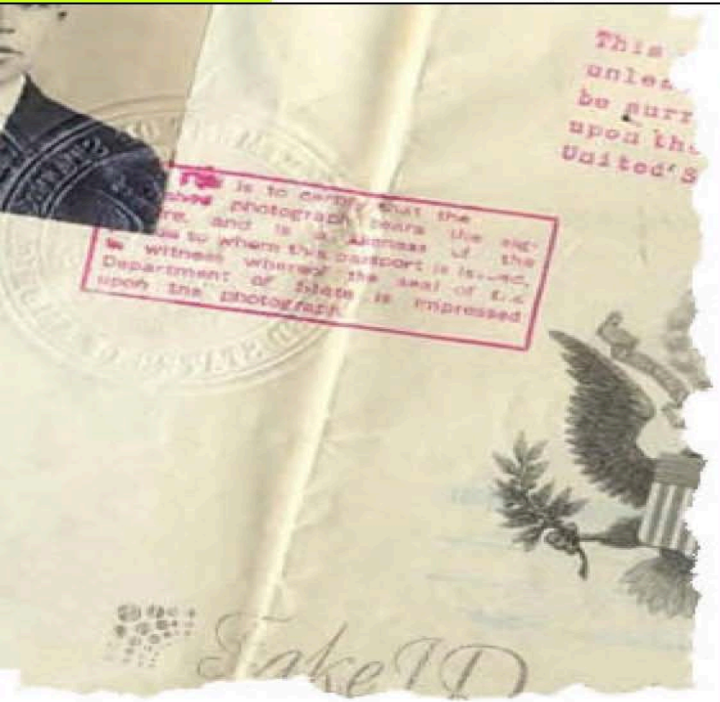
Internal UID	Balance	Account type	Card	Country	Our Price	Add to cart
ECARQRKL	701 USD	Personal	Yes (confirmed)	United States	$ 85	Buy this!
QBJSQAJY	798 USD	Premier	Yes (confirmed)	United States	$ 95	Buy this!
HJNORSUL	1.538 EUR	Personal	Yes (confirmed)	Italy	$ 200	Buy this!
KQCPRQHR	1.512 USD	Personal	Yes (confirmed)	United States	$ 166	Buy this!
BAGHFGUR	737 USD	Premier	Yes (confirmed)	United States	$ 89	Buy this!
XIEANRAA	1.162 USD	Premier	Yes (confirmed)	United States	$ 131	Buy this!
GFFEZNLP	766 USD	Personal	No confirmed card	United States	$ 81	LOCKED
TTCENANR	1.358 USD	Premier	Yes (confirmed)	United States	$ 151	Buy this!
TVYUHGPW	1.929 USD	Premier	Yes (confirmed)	United States	$ 208	Buy this!
FIKTXIEW	1.718 USD	Premier	Yes (confirmed)	United States	$ 187	Buy this!
FMBMIUOF	756 USD	Premier	Yes (confirmed)	United States	$ 91	Buy this!
TXOPYKYD	719 USD	Premier	Yes (confirmed)	United States	$ 87	Buy this!
VOGVTCXJ	1.130 USD	Premier	Yes (confirmed)	United States	$ 128	Buy this!

Cyber Crime Sales



FakeID®

Main | News | Services | Samples | faq | **Order** | Contacts



Welcome

Welcome to **Fake Documents Service**- the unique producer of quality fake documents. We offer only original high-quality fake passports, driver's licenses, ID cards, stamps and other products for following countries: Australia, Belgium, Brazil, Canada, Finland, France, Germany, Italy, Netherlands, UK, USA and some others.

If you want to learn more about what kinds of documents can be found in our website please visit the sections "Services" and "Samples". You can find more details about ordering procedure and additional details visiting the sections "FAQ" and "Order".

Login | Register | FAQs | Products

50 USD BILLS

Our notes are produced of cotton based paper. They pass the pen test without problems. UVI is incorporated, so they pass the UV test as well. They have all necessery security features to be spent at most retailers. Free shipping in the US.

Product	Price	Quantity
25 x 50 USD BILLS	600 USD = 1.343 ฿	1 X Buy now
100 x 50 USD BILLS	2000 USD = 4.475 ฿	1 X Buy now

Special K


Exposed – Kim Kardashian
exposed36mq3ns23.onion/Kim_Kardashian.html
Click here to view Kim's Credit Report
Kimberly Noel Kardashian
SSN: [redacted]23
DOB: 10/21/1980
Address: 25[redacted]ow Rd
Hidden Hills, CA 91302
Previous Addresses:
18056 Lake Encino Dr Encino, CA 91316
19254 Romar St Northridge, CA 91324
19254 Romar St Canoga Park, CA 91304
118 S CLARK DR APT 206 WEST HOLLYWOOD, CA 90048
5210 PREMIERE HILLS CIR APT 230 WOODLAND HILLS, CA 91364
Return to Exposed Homepage
Find: hacker
Next
Previous
Highlight all
Match case
Reached end of page, continued from top

Credit Cards!

ALL **CREDIT CARD** PIN CODES IN THE WORLD LEAKED ...
pastebin.com/2qbRKh3R

Sep 10, 2012 ... ALL **CREDIT CARD** PIN CODES IN THE WORLD LEAKED. 0000 0001 0002 0003 0004 0005 0006 0007 0008 0009. 0010 0011 0012 0013 ...

[2015] **Credit card** - Pastebin.com
pastebin.com/xB5aGiKf

Jan 30, 2015 ... BANK BUKOPIN | Indonesia(ID) | VISA | CLASSIC | **CREDIT CARD** | LO:120 LA:- 5 [ResellerPanel]Live=> | 4211670101485875|07/2017|844 ...

Credit Card DUMP [Working] - Pastebin.com
pastebin.com/0sJTUkf7

Feb 10, 2015 ... Want a free **creditcard**? Dump below of working cards as of 10/02/2015. 4427919903011599 0817 257. 4427910007028860 1115 553.

#OpUSA 10000 **credit card** leak - Pastebin.com
pastebin.com/8QB5018R

May 7, 2013 ... **Credit card**: American Express, 373276618282003. Expiration date: 8 2007. Cardholders Name: Nicole George. **Credit card** verification ...

[C++] USA **Credit Card** LeakeD By XhàckerTN - Pastebin.com
pastebin.com/Ay39ejx9

Sep 8, 2013 ... USA **Credit Card** LeakeD By XhàckerTN. (13:34 GMT). XhàckerTN Facebook Page : https://www.facebook.com/Xhackertnofficial. XhàckerTN ...

credit card leaked hacked - Pastebin.com
pastebin.com/KMPwvdLs

Oct 16, 2013 ... City : Hayden Lake. State : ID. Zip Code : 83835. Contry : United States. Payment Type : Visa. Debit or **credit card** number :

Cybercrime Marketing

Message Board – Download RATs and Malware

Mr. TwoFaces 2014-11-25 16:01 (edited by Mr. TwoFaces 2014-12-04 17:39)

Member

Offline

Registered: 2014-11-25
Posts: 17
User Karma: 10

Collection of Cracked Paid RATs

I'd like to present to you my list of cracked paid RATs sorted by coding language.
Please PM me if any download link isn't working, I will provide a new one for you.

Format:

Language

Name (Thread Design)
Download Link

Thank you hackb0t for providing .onion links

VB.NET (.NET 2.0)

Proton RAT (http://i.imgur.com/Mq5hVKb.png)
http://sh.st/uBM0r

Diamond RAT (http://i.cubeupload.com/AfyMG2.png)
http://4zjgf5i7dkafxpdm.onion/index.php ... &q=838

LuxNET (http://i7.minus.com/ibiXfLEOy381VW.jpg)
http://4zjgf5i7dkafxpdm.onion/index.php ... &q=839

Nanocore (https://i.imgur.com/R1xLbyf.png)
http://4zjgf5i7dkafxpdm.onion/index.php ... &q=840

Plasma RAT v1.5.1(http://i.imgur.com/O75WJNg.png)
http://ge.tt/7D7PV6x1/v/0

PHP

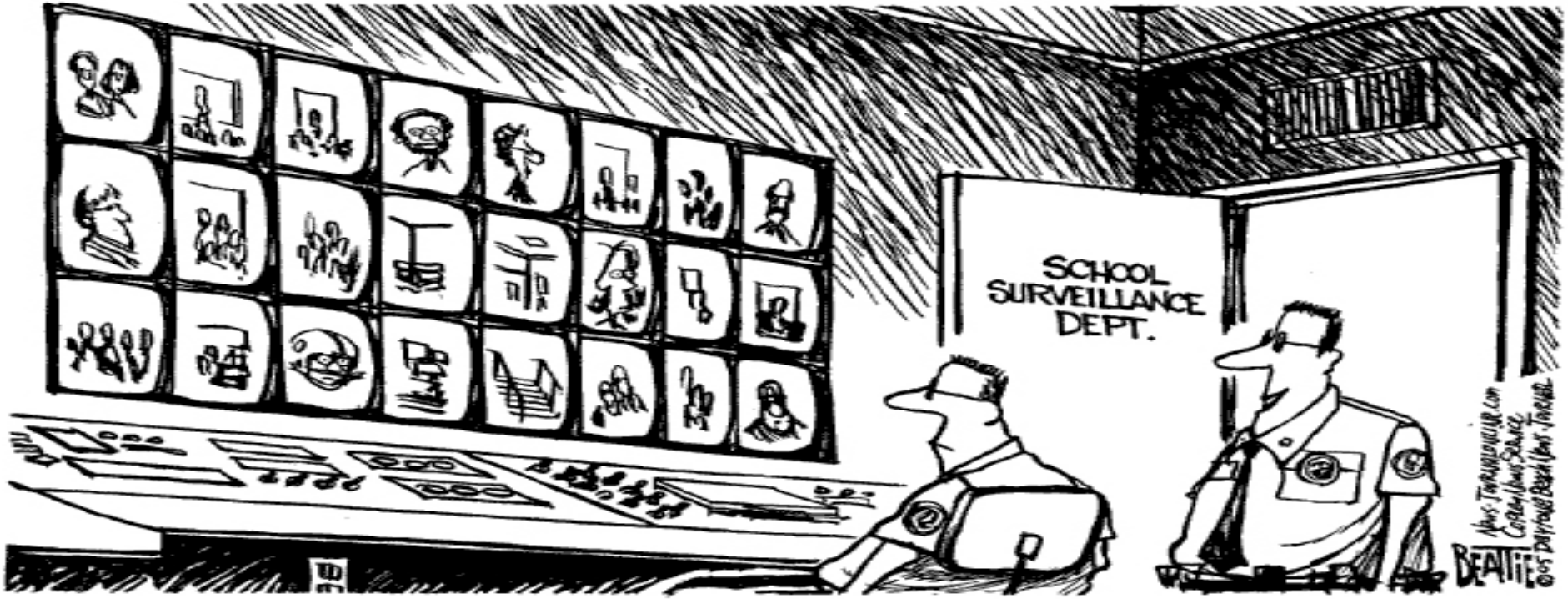
KazyBot (http://i.imgur.com/rnETeTb.png)
http://4zjgf5i7dkafxpdm.onion/index.php ... &q=845

Casting some light

Stopping TOR

- Application Protocols
- SSL Intercept
- IP Reputation-Based Filtering
- Sandbox Solutions
- DLP Solutions

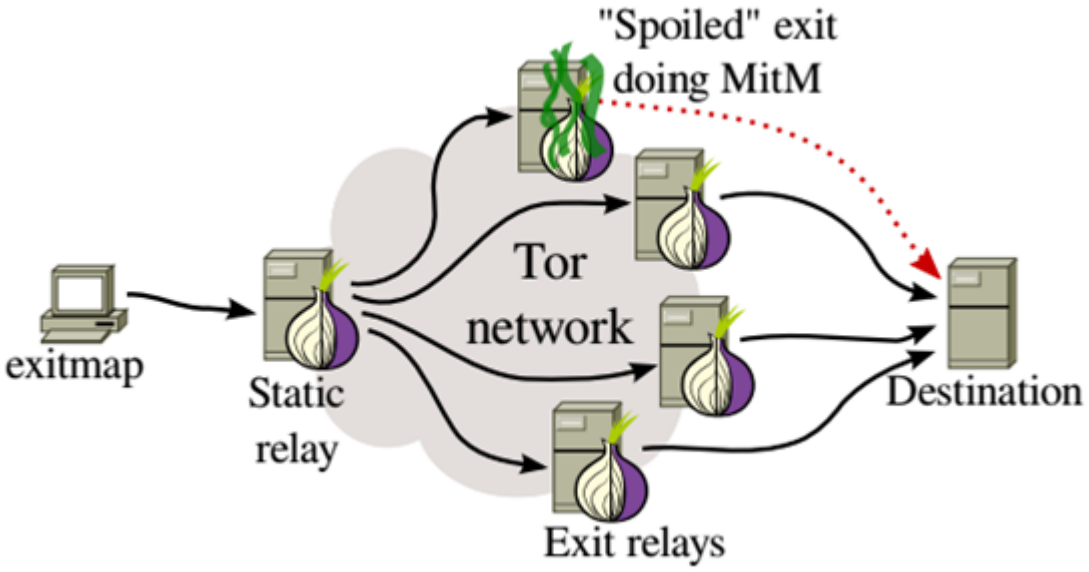
Policies that make sense



"Oh, look . . . they're reading '1984' in Ms. Smith's English class."

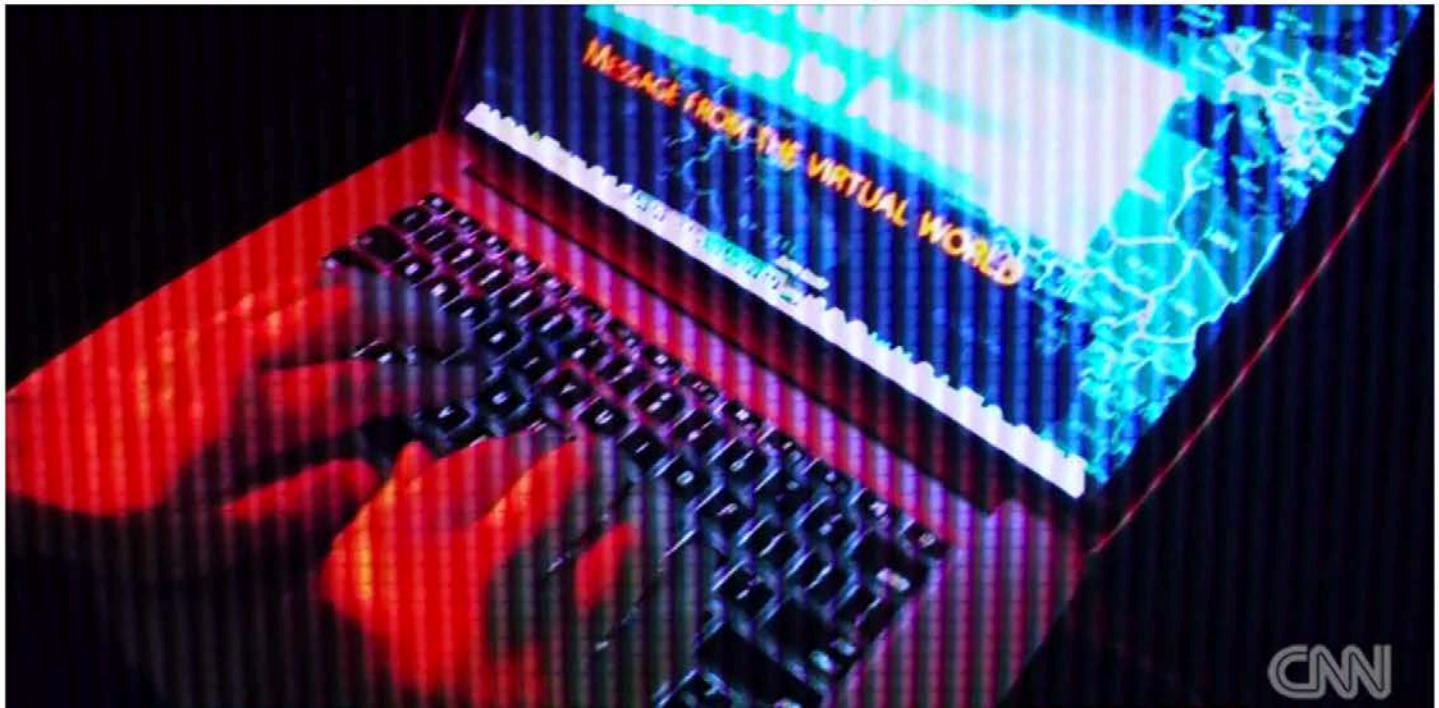
“Spoiled” exit Nodes and being anonymous

- Exit nodes doing MitM
- Controlling both entry and exit nodes
- Using NON-Tor Services



Pentagon hunts for ISIS on the secret Internet

By **Barbara Starr** and **Jamie Crawford**, CNN
Updated 6:08 PM ET, Tue May 12, 2015



ISIS: Full coverage


How ISIS controls l
from birth to foosb


ISIS loses quarter o
territory in Iraq - 3 t
to know

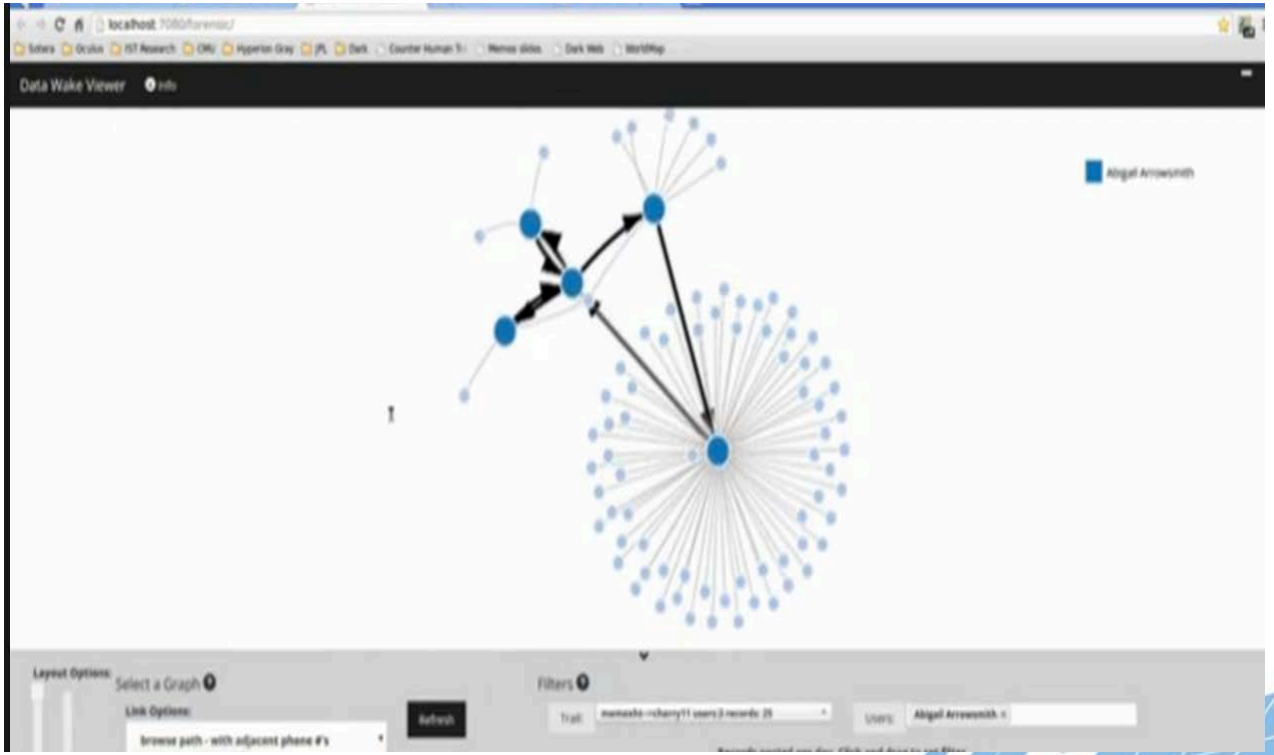

The Americans link
ISIS


ISIS releases some
Christian hostages
why?


Who's doing what

MEMEX Deep Web Search Engine

- Deep Web Crawlers
- Indexers
- Threat Intelligence
- US Gov’t Program



Want to play a game?

- Use a different system to test. Don’t use VMs. Use Live CDs or USBs
- Use a VPN on top of TOR (I like Private Internet Service – others? Tweet me @aamirlakhani)
- Don’t connect back to your network
- Spend time building a offline image.
- Listen, surf, and don’t participate
- Almost all newbie’s will get scammed, hacked, or in some sort of illegal trouble (e.g .onion Twitter)

Apply Knowledge to Real World

Educate + Learn = Apply

DarkNET can be a valuable tool for security professionals

How to Apply what I learned

- Darknet is a valuable tool for researchers to gauge the state of their cyber security program :
  - Users need to be aware of the dark and dangerous groups of attackers.
  - Reputation and Unified Threat Management Systems can help mitigate risks.
  - Researchers need to understand traffic is not anonymous. Controlling entry and exit nodes may be able to reveal true identity of users. ISPs and law enforcement may monitor TOR and other protocols.
  - Threat Intelligence can be gained by monitoring “chatter” on your employees and your organizations.

Reputation Filtering

‘Blastware’ Beware

Recent destructive malware in the wild

- Disk Wipers
  - Overwrites hard-drive and MBR
  - Triggered by logic bomb/timer
  - South Korea, March 2013
    - 3 banks, 2 media companies
    - 50,000 systems
- Ransomware
  - Encrypts data
  - Leaves hard drive intact
  - Forensics unhampered

New 2014 FortiGuard Labs discovery: DorkBot

- Erases hard drive if analysis is detected
- New variations likely to destroy other targets

Shout Out

- RSA and RSA Asia
- Fortinet and FortiGuard Labs
- Singapore
- TOR Project
- Google Image Search (or this presentation would have no pictures)

www.FortiGuard.com

Thank You

Thank you

Thank You

- Jack Chan
- Fortinet Blog: blog.fortinet.com
- FortiGuard Research: www.fortiguard.com
- Twitter: @FortiGuardLabs