

Cyber Crimes



Debasis Nayak
Asian School of Cyber Laws

The Cyber Crime Terrain

- Targeting cloud computing
- Infrastructure (Stuxnet, DuQU)
- Mobile devices (Wallet fraud in Bangalore)
- Automobile access (Tracking devices)
- Credit card theft
- Phishing attacks (Mandate frauds, usual)
- Malware/Ransomware
- Medical devices
- State sponsored hacking

Cloud Computing

- Facebook
 - 80 million users + 250,000 new users per day
 - 50,000 transactions per second, 10,000+ servers
- Banking Services, Telecom, Intelligence (All big data using services)
- Such massive requirements makes it infeasible to conduct operations only from one place
- Hence, a distributed access is more practical and manageable

Security Challenges

- Attraction to hackers (high value target)
- Security of virtual OSs in the cloud
- Possibility for massive outages
- Public cloud Vs internal cloud security

Aeroplanes

- 1400 passengers in Warsaw's Chopin airport stranded
 - Hackers attacked the airline ground computer systems used to issue flight plans
- FBI has affidavit of researcher who hacked plane's computer in flight causing it to climb

Railways

- May 2016: Personal data of around 1 crore customers stolen from the IRCTC server.
- Computer-based interlocking (CBI) is a signaling system designed to prevent conflicting routes.
- CBI threats: *Safety, Economics and Reliability.*
- A hacker with access to CBI can cause physical damage by
 - changing a switch while a train is passing over it; or
 - by setting up conflicting routes.

Industrial Sector (Steel Mill)

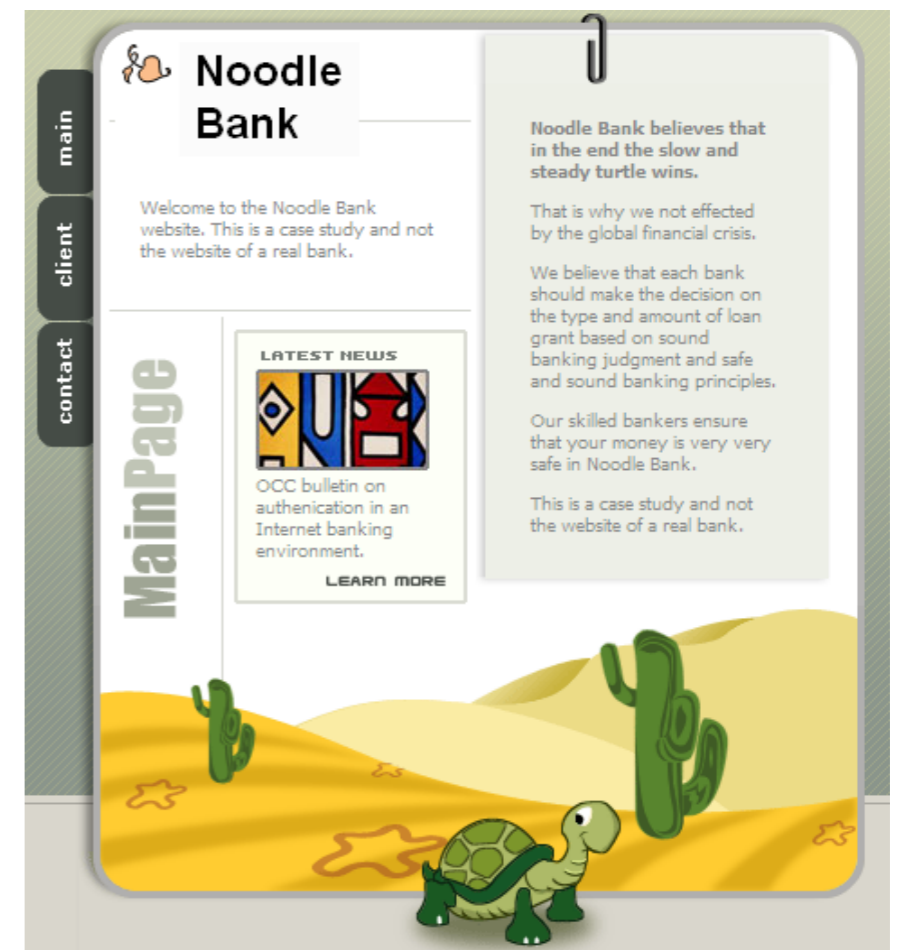
- The hackers first hacked into the office software network of the industrial site.
 - Penetrated the production management software of the steel mill.
 - Took over most of the plant's control systems.
 - Then methodically destroyed human machine interaction components.
 - Succeeded in preventing blast furnace from initiating security settings in time; caused serious damage to infrastructure

Irrigation and infrastructure

- Iranian hackers have
 - infiltrated the control system of a small dam less than 20 miles from New York City
 - carried out a dozen attacks that have infiltrated the U.S. power grid system in the last decade

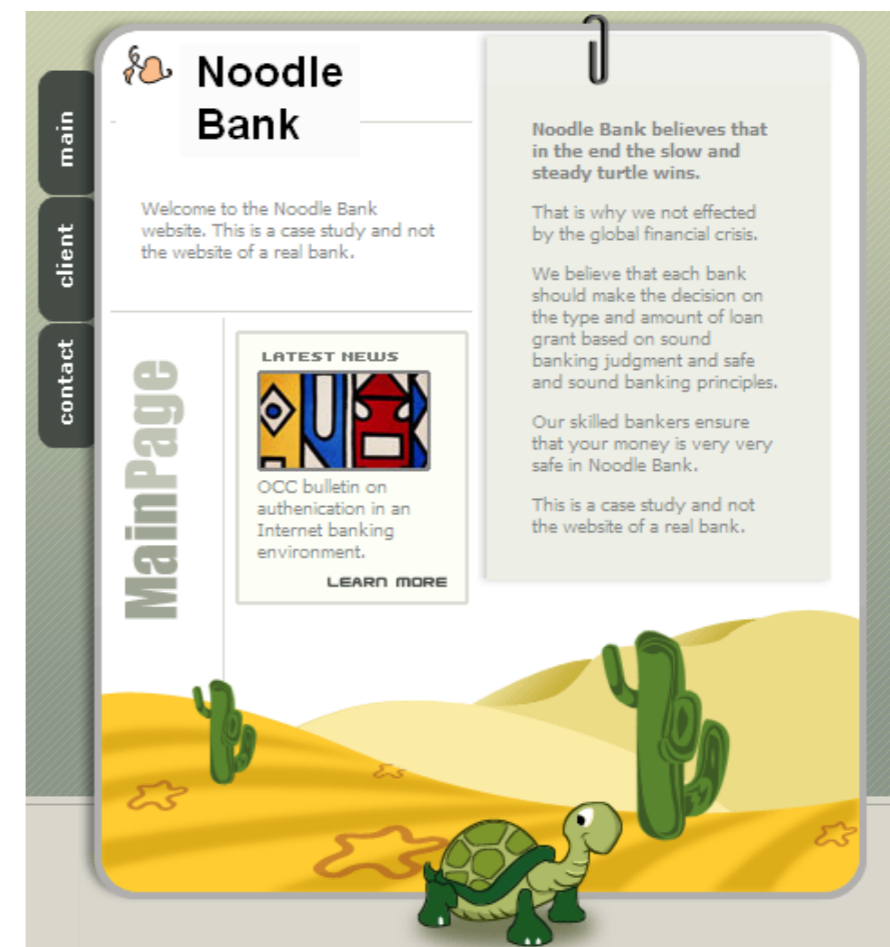
What is phishing?

- Phishing involves fraudulently acquiring sensitive information (e.g. passwords, credit card details etc) by masquerading as a trusted entity.



The sites

- www.noodlebank.com (i.e NOODLEBANK.com)
- www.nood1ebank.com (i.e NOOD1EBANK.com)



The spoofed email

Inbox

Starred 

Chats 

Sent Mail

Drafts

All Mail

Spam

Trash

Contacts

[« Back to Inbox](#)

Archive

Report spam

Delete

More Actions



Urgent - Verification required

Inbox | X

★ info@noodlebank.com to me

[show details](#) 12:06 PM (9 minutes ago)

[Reply](#) | ▼

Dear Mr. Debasis Nayak,

We suspect that your online banking account number 12345678 with Noodle Bank has been compromised.

An attempt to transfer Rs 250,000 out of your account has been made. We have blocked the transfer. To verify that the transfer must be blocked, please login to your account from:

<http://www.noodlebank.com>

You need to login to your account by 12.30 pm on 27-January-2009 to cancel this transfer. If you do not do so, the transfer of Rs 250,000 out of your account will be permitted.

Regards,
Pooja Sharma,
Customer Care Executive,
Noodle Bank

The spoofing

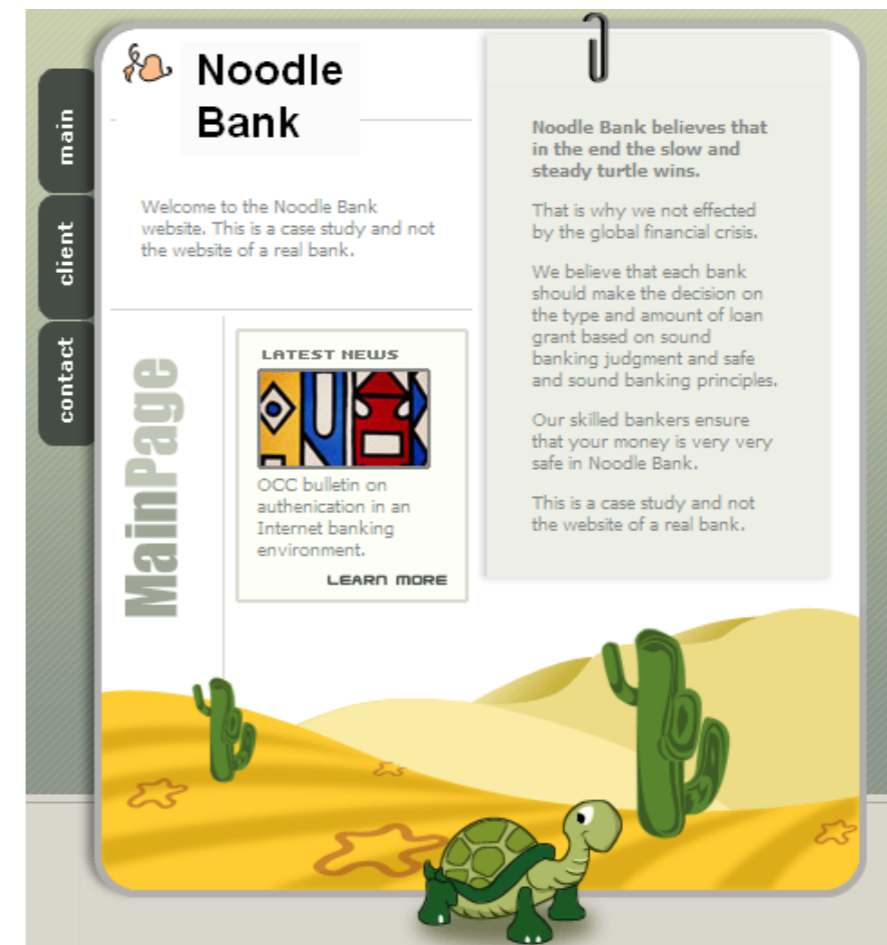
- The link appears as

www.noodlebank.com (i.e NOODLEBANK.com)

- But actually it links to

www.nood1ebank.com (i.e NOOD1EBANK.com)

The fake site



Noodle Bank

Welcome to the Noodle Bank website. This is a case study and not the website of a real bank.

Noodle Bank believes that in the end the slow and steady turtle wins.

That is why we not effected by the global financial crisis.

We believe that each bank should make the decision on the type and amount of loan grant based on sound banking judgment and safe and sound banking principles.

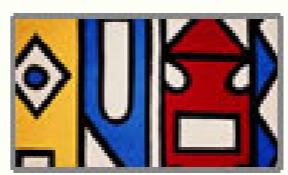
Our skilled bankers ensure that your money is very very safe in Noodle Bank.

This is a case study and not the website of a real bank.

- main
- client
- contact

MainPage

LATEST NEWS



OCC bulletin on authentication in an Internet banking environment.

LEARN MORE



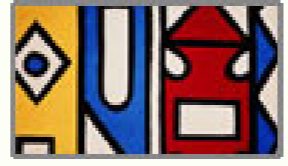
Noodle Bank

Welcome to the Noodle Bank Online Banking website.

- main
- client
- contact

MainPage

LATEST NEWS



OCC bulletin on authentication in an Internet banking environment.

[LEARN MORE](#)

Noodle Bank believes that in the end the slow and steady turtle wins.

That is why we not effected by the global financial crisis.

We have shifted our online banking system to our new secure servers. In case you have any difficulty using the new systems, please [contact us](#) for assistance.

[Click here to use our new online banking systems.](#)



client

Noodle Bank

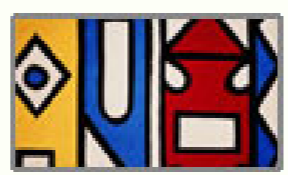
Welcome to the Noodle Bank Online Banking website.

User Name:

Password:

MainPage

LATEST NEWS



OCC bulletin on authentication in an Internet banking environment.

[LEARN MORE](#)



client

Noodle Bank

Welcome to the Noodle Bank Online Banking website.

User Name:

Password:

MainPage

LATEST NEWS



OCC bulletin on authentication in an Internet banking environment.

[LEARN MORE](#)

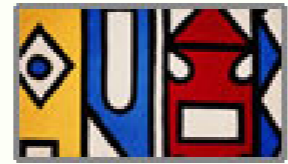


main
contact

Noodle Bank

Welcome to the Noodle Bank website. This is a case study and not the website of a real bank.

LATEST NEWS



OCC bulletin on authentication in an Internet banking environment.

LEARN MORE

Your account services have temporarily been blocked, as we suspect that your account has been compromised. An attempt to transfer Rs 250,000 to the account of Sid Kumar has been made. We have blocked the transfer.

To cancel this transfer, please click here.

To allow this transfer, please click here.



main
contact

Noodle Bank

Welcome to the Noodle Bank website. This is a case study and not the website of a real bank.

The transfer has been cancelled. Your account services will resume after 24 hours. Thank you for your cooperation. We regret the inconvenience.

LATEST NEWS



OCC bulletin on authentication in an Internet banking environment.

[LEARN MORE](#)



- Reset temperature settings on refrigerators storing blood & drugs and cause spoilage.
- Altering digital medical records.
- Restart / reboot critical equipment.
- Spoofed blood test reports.

Hospital network hacked, 4.5 million records stolen

By Jose Pagliery @Jose_Pagliery August 18, 2014: 3:25 PM ET

Recommend 30k



18th August 2014

Community Health Systems, which operates 206 US hospitals announced that hackers recently broke into its computers and stole data on 4.5 million patients.

Stuxnet

- Affects SCADA systems through USB
- Infected thousands but no damage caused
- Only affects plants having more than 33 frequency convertor drives made by
 - Ferero Paya in Iran; Vacon in Finland
- Targets frequency convertors operating between 807 – 1210 Hz (uranium enrichment)
- Destroyed over 1000 uranium enrichment centrifuges in Iran

Mobile Devices

- RuMMS
 - Family of Android Malware spread through MMS
 - “You got a photo in MMS format:
`hxxp://yyyyyyyyy.XXXX.ru/mms.apk`”
- Installed App characteristics
 - Request device administrator privileges
 - Remove icons to hide themselves from user
 - Remain running in the background

Threat actors



0.a. Send short message

0.c. Setup C2 server

0.b. Upload malware

вы получили
фотографию в формате
MMS: [http://
casamadf.████████.ru/
mms.apk](http://casamadf.████████.ru/mms.apk)

Malware
Hosting Sites

C2
Servers

1. Check
message

2. Download
malware

3. Contact C2,
upload privacy,
fetch instructions

Victim users

Android
Device

4.a. Balance
inquiry, USSD

4.b. Intercept & upload
SMS (including banks
balance reply)

4.c. SMS Worm

Banks

C2

.....

Contacts

Mobile Devices (RuMMS)

- Actions
 - Sending device information to a remote command and control server (C2)
 - Contacting the C2 server for instructions
 - Sending SMS messages to financial institutions to query account balances.
 - Uploading any incoming SMS messages (including the balance inquiry results) to the remote C2 server.
 - Sending C2-specified SMS messages to phone numbers in the victim's contacts.
 - Forward incoming phone calls to intercept voice-based two-factor authentication

Mobile Devices (Case Study)

- Bank in Karnataka
 - Customers installed Mobikwik mobile wallet
 - Linked wallet with bank's debit card to transfer funds to wallet
 - Mobikwik affiliated merchant transactions effected
 - Multiples of Rs. 49/- each per customer affecting 2000 customers
 - Total amount >80 Lakhs
 - Bank paid back all customers

Hacking behind third of London's car theft

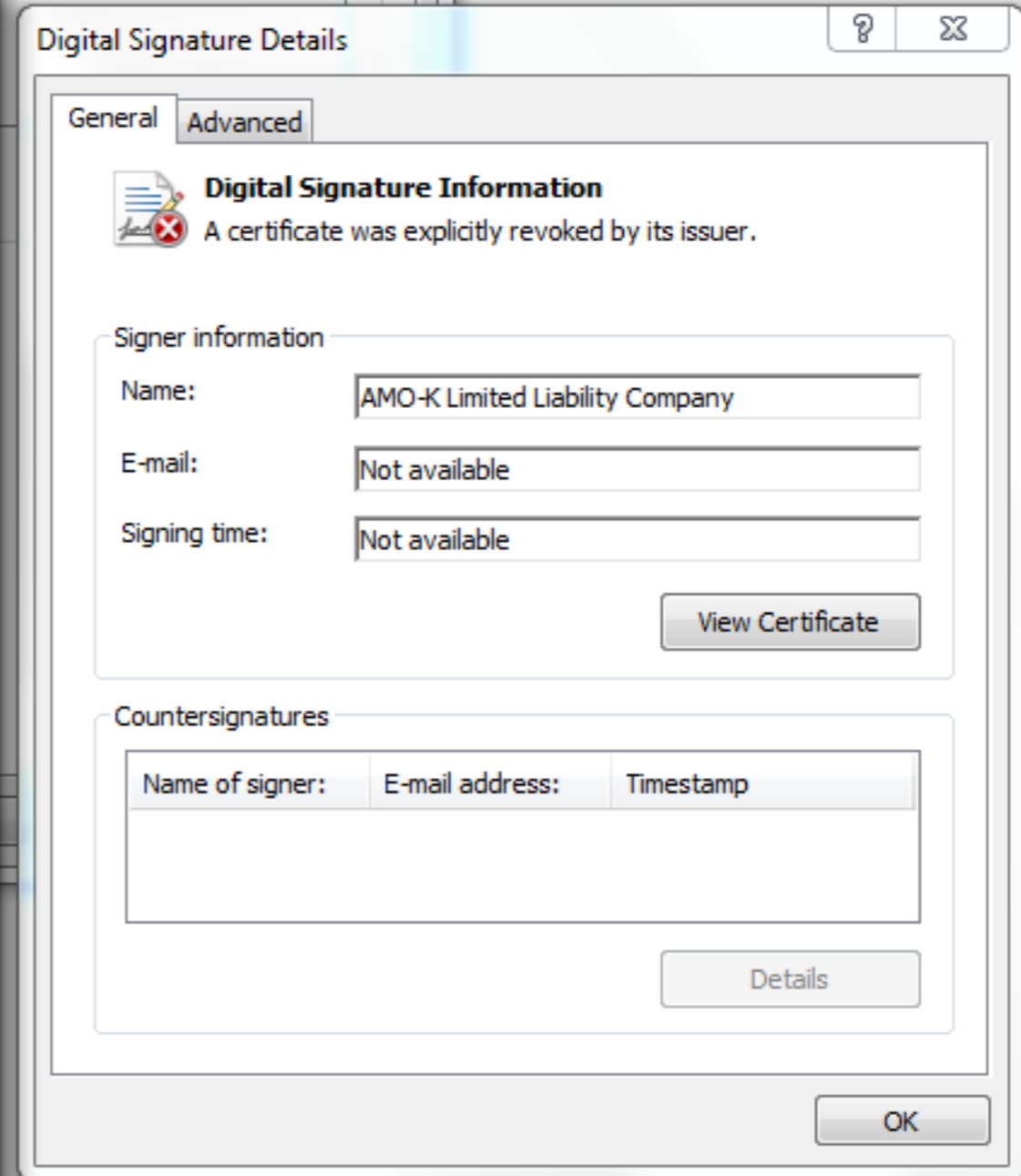
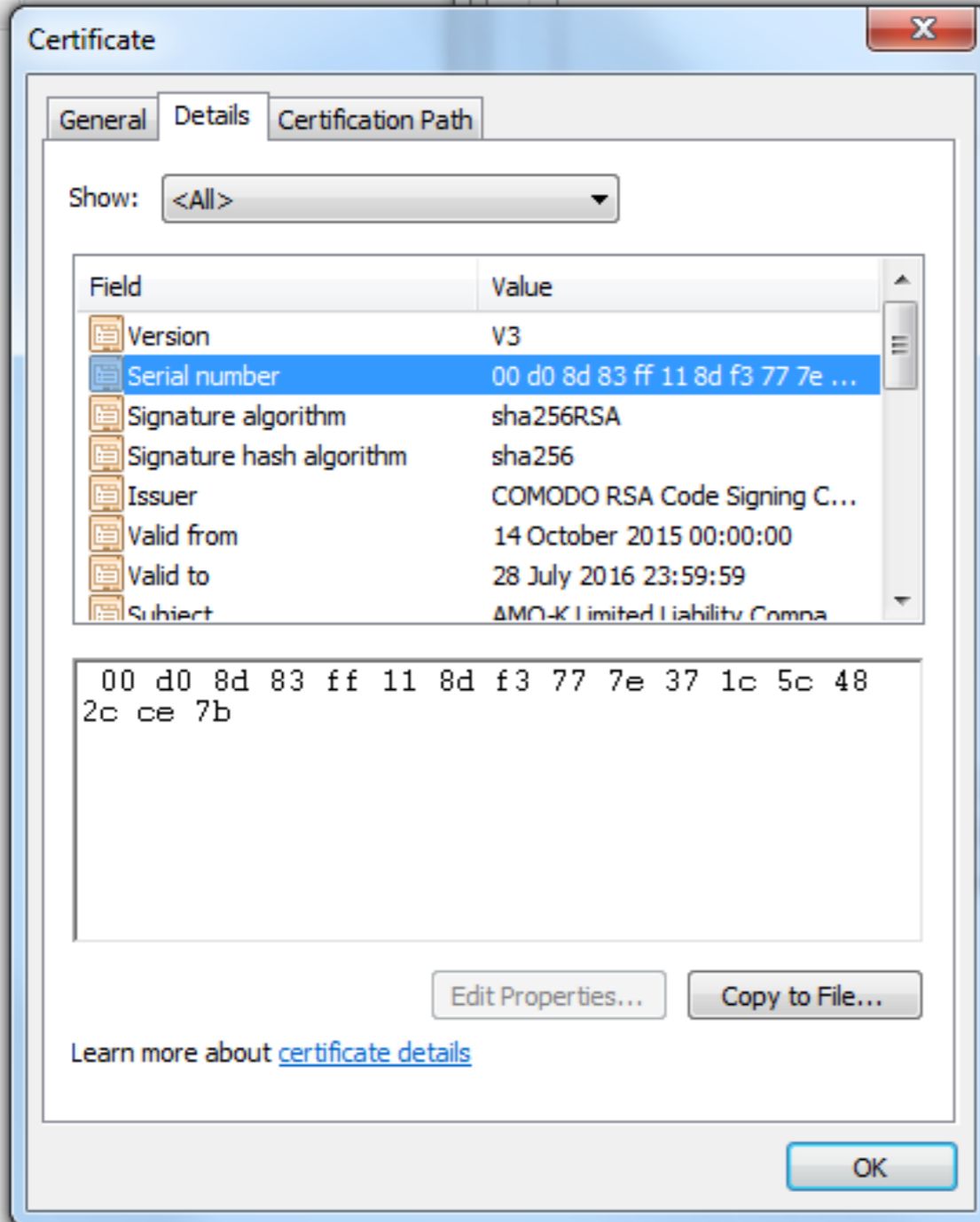
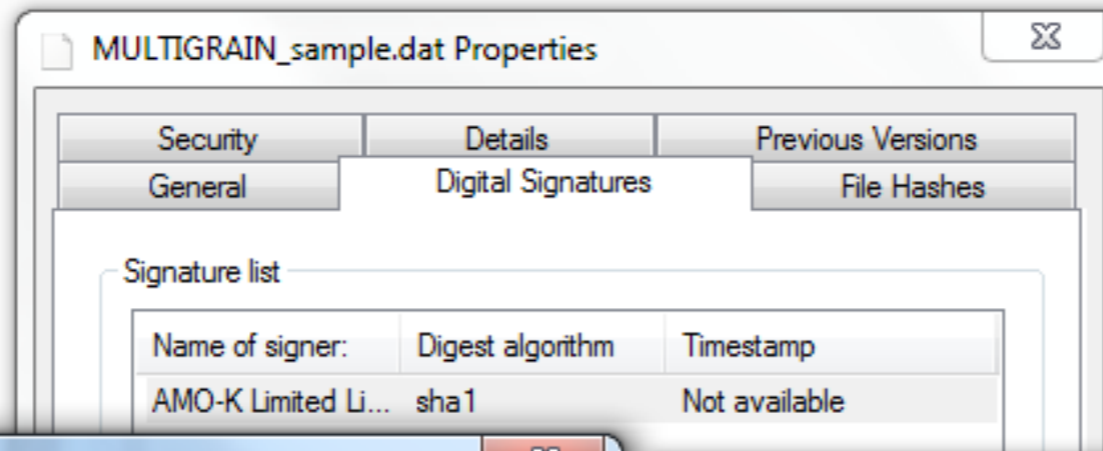
Car theft has entered the cyber age with more than one in three vehicles currently stolen in London being taken through sophisticated hacking methods, the Home Office has revealed. But experts say the issues were long predicted.

New Device Lets India's Driven Middle Class Snoop on the Chauffeur



Credit Card Theft

- PoS malware
 - MULTIGRAIN malware uses DNS to extract card data
 - Is activated only when it finds the *multi.exe* process running at PoS
 - Highly targeted, digitally signed, and exfiltrates stolen payment card data over DNS





Please Don't Rob Me

is a social experiment exploring our online behaviour. PDRM is meant to demonstrate how easy it is to find out where someone lives and if they are at home or not. The aim of this site is to educate and empower people to protect themselves better while using social media.

[ABOUT THE PROJECT](#)

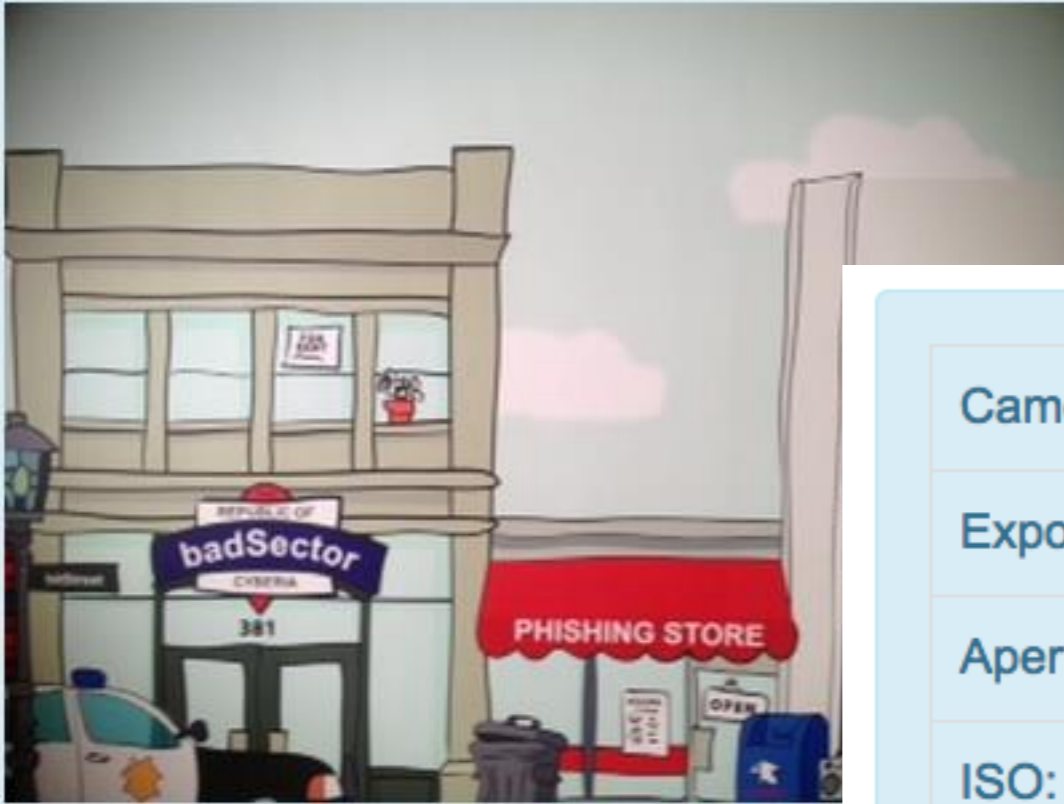
[IMAGE GALLERY](#)



Wall of careless people



This is the photo being analyzed:



This photo was taken at this location:

Longitude:

73.829

Latitude:

18.5306666667

[View this location on Google maps](#)

TV case

Camera Used:	Apple iPhone 4S
Exposure Time:	1/40
Aperture:	f/2.4
ISO:	50
Date Taken:	2014:05:30 15:43:05

Last accessed on:

25-Jul-2014

Last modified on:

30-May-2014

The Criminal Underground

1 What do criminals sell online?

2 Case 1: Silk Road

3 Case 2: Darkmarket

4 Anatomy of a Financial Cyber Crime Organization

5 Tor – the technology powering the hidden web

6 Bitcoin – the powerful virtual currency

7 Conclusions

**“ What do
criminals
sell online? ”**

What do criminals sell online?



- ✓ Narcotics & controlled substances
- ✓ Guns, ammunition, UAVs
- ✓ Stolen financial information like credit card numbers, bank account login credentials etc
- ✓ Forged documents like passports, driver's licenses etc.



Silk Road

anonymous marketplace

messages(0) | or

1 day hrs mins secs un

Shop by category:

Drugs(2788)

Cannabis(796)

Dissociatives(48)

Ecstasy(307)

Opioids(211)

Other(98)

Prescription(541)

Psychedelics(366)

Stimulants(235)

Apparel(28)

Books(286)

Computer
equipment(13)

Digital goods(219)

Drug

paraphernalia(74)

Electronics(17)

Fireworks(1)



170\$ pecunix

\$39.23



1 OZ of Jamaican Oil

\$73.91



20 Grams of MDMA
crystals

\$124.60



HYDRO 10/325
NORCO/LORATAB

\$11.75 V...

Need
your
\$0.

1oz
(Roo
\$25

Case 1: Silk Road

Online Narcotics Marketplace



Silk Road provided a platform for drug dealers around the world to sell narcotics through the Internet

- ✓ Set up in 2011 by Ross Ulbricht
- ✓ Transactions estimated to be US \$ 1.2 billion carried out in bitcoins
- ✓ Had 957,079 registered users
- ✓ Taken down in September 2013

Silk Road

Ross Ulbricht created Silk Road as an online criminal bazaar.

The site's anonymity was maintained by:

- using TOR (the onion ring network) to run the site
- using bitcoins, a virtual currency, for transactions

Ulbricht had also reportedly solicited a Silk Road user to execute a murder-for-hire of another Silk Road user who was threatening to release the identities of thousands of Silk Road users.

Silk Road was accessible through Tor on:
silkroadvb5pizr.onion



Ross Ulbricht
aka Dread Pirate Roberts

Silk Road provided an online platform for trading in:

- **Narcotics and controlled substances** (heroin, cocaine, LSD, methamphetamine). The site had 13,000 listings of controlled substances on it under various categories like Cannabis, Dissociatives, Ecstasy, Intoxicants, Opioids, Precursors, Prescription, Psychedelics, Stimulants etc.
- **Malicious software** designed for computer hacking (password stealers, key loggers, remote access tools etc.)
- **Unlawful services.** The site had 159 listings for "Services" such as hacking into Facebook, Twitter etc, tutorials for hacking ATM machines, contacts for guns and firearms, fake currency etc.
- **Pirated content.** The site had 801 listings for "digital goods" such as pirated content and hacking tools.
- **Forged documents.** The site had 169 listings for "Forgeries" such as fake driver's licenses, passports, utility bills, credit card statements, social security cards etc.



Ross Ulbricht
aka Dread Pirate Roberts

Case 2: Darkmarket

Online Carding Forum



Darkmarket facilitated the buying and selling of stolen financial information

- ✓ Set up in 2008 by Renukanth Subramaniam in London in 2008
- ✓ Had 2500 members
- ✓ Taken down in 2010

Darkmarket

Darkmarket, created by Renukanth Subramaniam in London in 2008, was an online carding forum. Its members were involved in buying and selling:

- stolen credit card data,
- login credentials, and
- equipment for carrying out financial crimes.

At its peak, Darkmarket had 2500 members from around the globe.

In a two-year operation, an undercover FBI agent with the handle *Master Splyntr* penetrated Darkmarket. 60 people were arrested. The entire operation was handled by the US Federal Bureau of Investigation along with law enforcement officials from the United Kingdom, Germany, and Turkey.

Subramaniam, who used the handle JiLsi, admitted conspiracy to defraud and was sentenced to nearly five years in prison in February 2010.

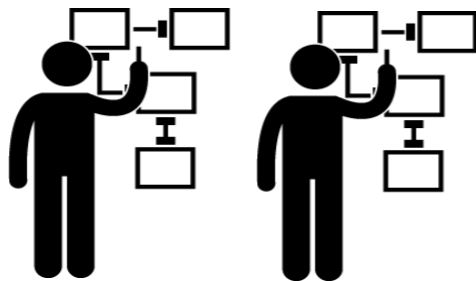


Renukanth Subramaniam
aka JiLsi

Darkmarket Organizational Chart



→ **ADMIN**
The Admin ran the escrow service and controlled membership.



→ **MODERATORS**
They monitored the forum and arbitrated disputes.



→ **REVIEWERS**
They assessed the quality of the stolen financial information.



→ **HACKERS / DATA THIEVES**
These were the vendors permitted to sell to members. Categories – Trial and Reviewed.



→ **MEMBERS**
These were the fraudsters who bought and misused stolen financial information.

Underground Economy

- Expensive email spam (using a customer database): \$50-\$500 (£31-£310) per one million emails
- SMS spam: \$3-\$150 (£1.86-£93) per 100-100,000 messages
- Bots for a botnet: \$200 (£124) for 2,000 bots

Underground Economy

- DDoS botnet: \$700 (£433)
- Windows rootkit (for installing malicious drivers): \$292 (£180)
- Hacking a Facebook or Twitter account: \$130 (£80)

Underground Economy

- Hacking a Gmail account: \$162 (£100)
- Hacking a corporate mailbox: \$500 (£310)
- Scans of legitimate passports: \$5 (£3.10) each
- Traffic: \$7-\$15 (£4.33-£9.29) per 1,000 visitors for the most valuable traffic (from the US and EU)

**“ Bitcoin –
the virtual currency
that powers the
underground digital
economy ”**

What are bitcoins?

- Bitcoins are an anonymous, decentralized form of electronic currency existing entirely on the Internet. They are generated and controlled automatically through computer peer-to-peer networks.
- The Bitcoin scheme is a large scale global payment system in which all the transactions are publicly accessible, but quite anonymous.
- Bitcoins are like "cash" in cyberspace - anonymous.
- Bitcoins are not issued by any Government, bank or company. They are not issued or backed by any central body. This is unlike currencies (e.g. Rupees, Dollars, Euro) which are backed by Governments.
- Bitcoins work on public key cryptography and digital signatures.



What is bitcoin? (contd.)

- Bitcoin keys do not have to be registered anywhere in advance, as they are only used when required for a transaction.
- Transacting parties do not need to know each other's identity. This is analogous to walking into a shop and paying cash to buy something. The shop owner does not need to know your identity.



Sample bitcoin transaction

Pooja wants to send 1 bitcoin to Rohit

Step 1: Rohit sends his bitcoin address to Pooja.

e.g. 1PC9aZC4hNX2rmmrt7uHTfYAS3hRbph4UN

Step 2: Pooja adds Rohit's address and the amount of bitcoins to transfer to a "transaction" message.

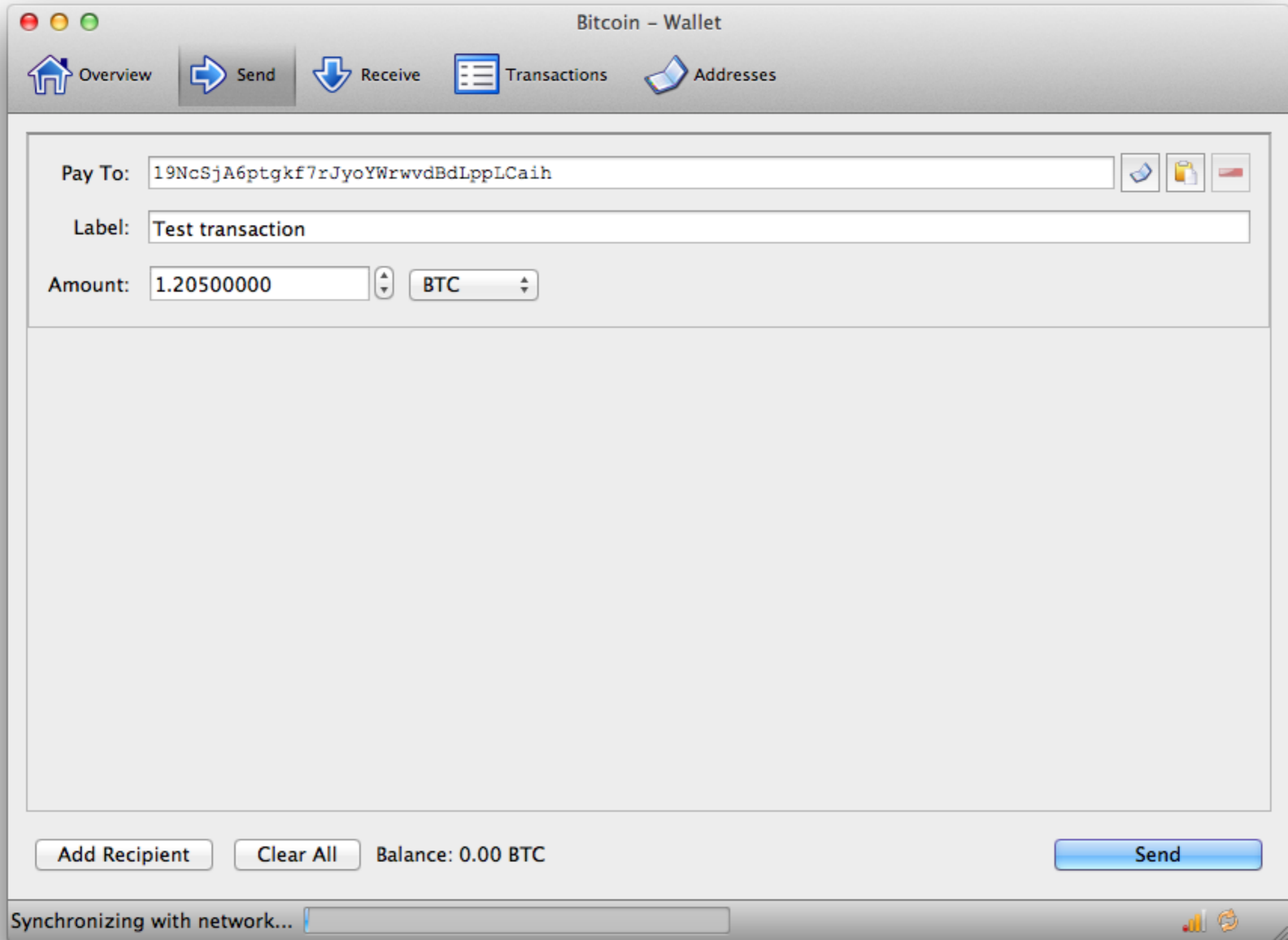
Step 3: Pooja signs the "transaction" message with her private key, and announces her public key for signature verification.

Step 4: Pooja broadcasts the transaction on the Bitcoin network for all to see. (See www.blockchain.info)

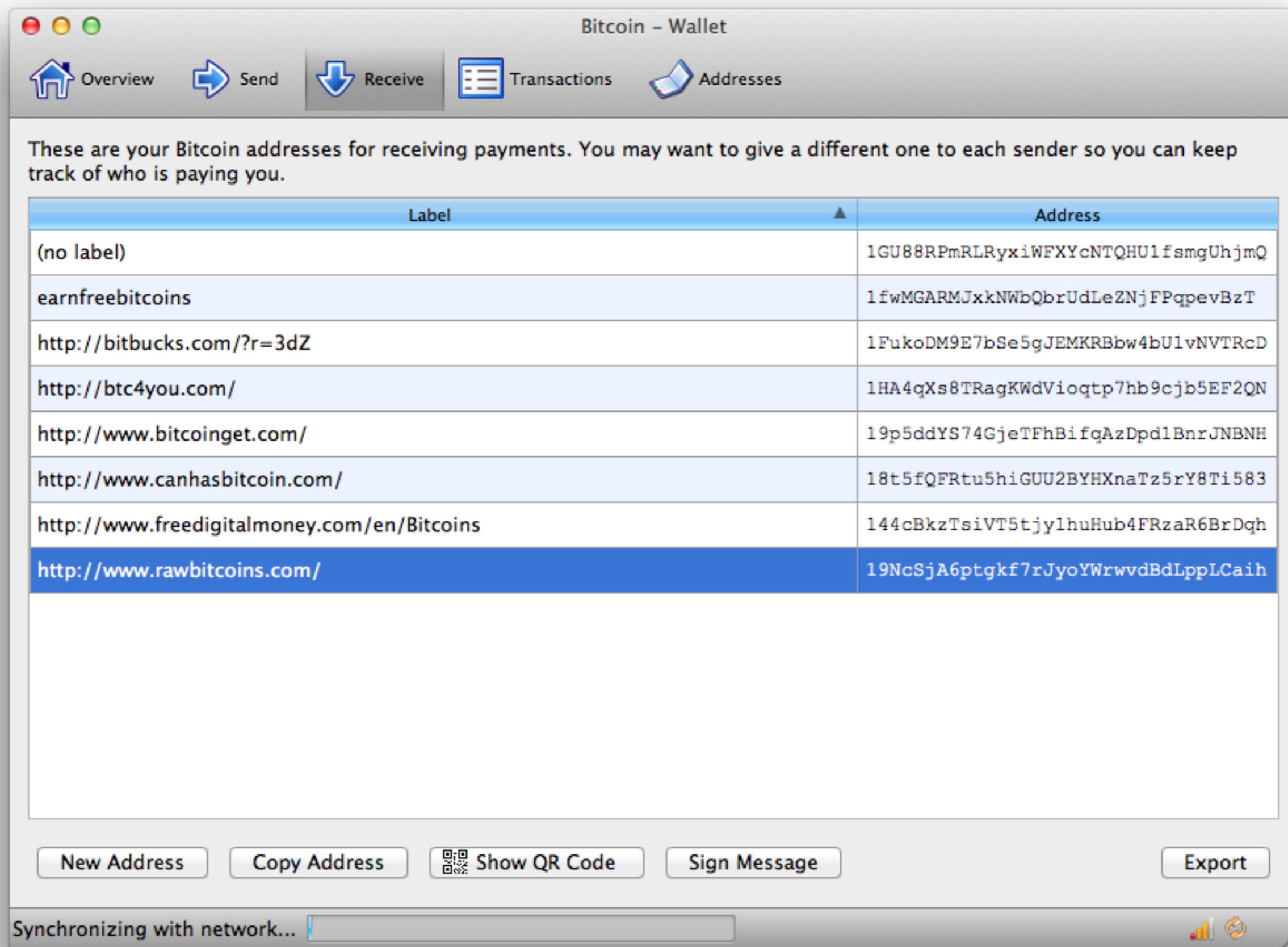
Steps 1 and 2 require human action. Steps 3 and 4 are done by the Bitcoin client software.



Making a bitcoin payment



A bitcoin wallet showing multiple bitcoin addresses



The screenshot shows a Bitcoin wallet window titled "Bitcoin - Wallet". The interface includes a navigation bar with buttons for "Overview", "Send", "Receive", "Transactions", and "Addresses". Below the navigation bar, a message states: "These are your Bitcoin addresses for receiving payments. You may want to give a different one to each sender so you can keep track of who is paying you." A table lists several addresses, with the last one highlighted in blue. At the bottom, there are buttons for "New Address", "Copy Address", "Show QR Code", "Sign Message", and "Export". A status bar at the very bottom indicates "Synchronizing with network..." with a progress indicator.

Label	Address
(no label)	1GU88RpmRLRyxiWFXycNTQHU1fsmgUhjmQ
earnfreebitcoins	1fwMGARMJxkNWbQbrUdLeZNjFPqpevBzT
http://bitbucks.com/?r=3dZ	1FukoDM9E7bSe5gJEMKRBbw4bU1vNVTRcD
http://btc4you.com/	1HA4qXs8TRagKWdVioqtp7hb9cjb5EF2QN
http://www.bitcoinget.com/	19p5ddYS74GjeTFhBifqAzDpd1BnrJNBH
http://www.canhasbitcoin.com/	18t5fQFRtu5hiGUU2BYHXnaTz5rY8Ti583
http://www.freedigitalmoney.com/en/Bitcoins	144cBkzTsiVT5tjy1huHub4FRzaR6BrDqh
http://www.rawbitcoins.com/	19NcSjA6ptgkf7rJyoYWrwvdbdLppLCaih

Blockchain showing all bitcoin transactions ever made

Bitcoin Block Explorer - Blockchain.info

blockchain.info

Home Charts Stats Markets Developers Wallet

Search

Home

Most recently mined blocks in the bitcoin block chain

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
268039	4 minutes	171	2,143.79 BTC	GHash.IO	97.73
268038	11 minutes	211	3,118.89 BTC	GHash.IO	131.88
268037	19 minutes	356	3,637.52 BTC	GHash.IO	188.56
268036	31 minutes	225	5,911.22 BTC	BTC Guild	212.58
268035	39 minutes	367	5,053.39 BTC	Slush	183.54
268034	53 minutes	23	215.71 BTC	Eligius	12.32
268033	54 minutes	88	4,142.36 BTC	BTC Guild	32.50

[More...](#)


Latest Transactions

8f2c5c3ab87f010e333036682...	< 1 minute	0.40068002 BTC
bdec99cf7fd24c930da6ce79d...	< 1 minute	5.76306798 BTC
7c694a774f5176c28cb106e9b...	< 1 minute	2.54014145 BTC

Search

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address..

Address / Firstbits / ip / SHA hash



About & Contact: [About Us](#) - Status: [Ok \(334 Nodes Connected\)](#) - Advanced: [Enable](#) - Currency:

How Silk Road used bitcoins

- Every Silk Road user had one or more bitcoin addresses associated with his Silk Road account.
- These addresses were stored on wallets maintained on servers controlled by Silk Road.
- A user had to first send bit coins to an address associated with his Silk Road account.
- The user could then make a purchase on Silk Road. This amount was held in escrow till the transaction was completed.
- Once the transaction was complete, the bit coins would be transferred to the vendor's Silk Road bitcoin address. From here the vendor could transfer the bit coins to an external bitcoin address and convert them to real currency.
- Silk Road charged a commission between 8 - 15% for each transaction.
- Silk Road used a special technique to send payments through a “complex semi-random series of dummy transactions” to further anonymize the transactions.



Coming Soon

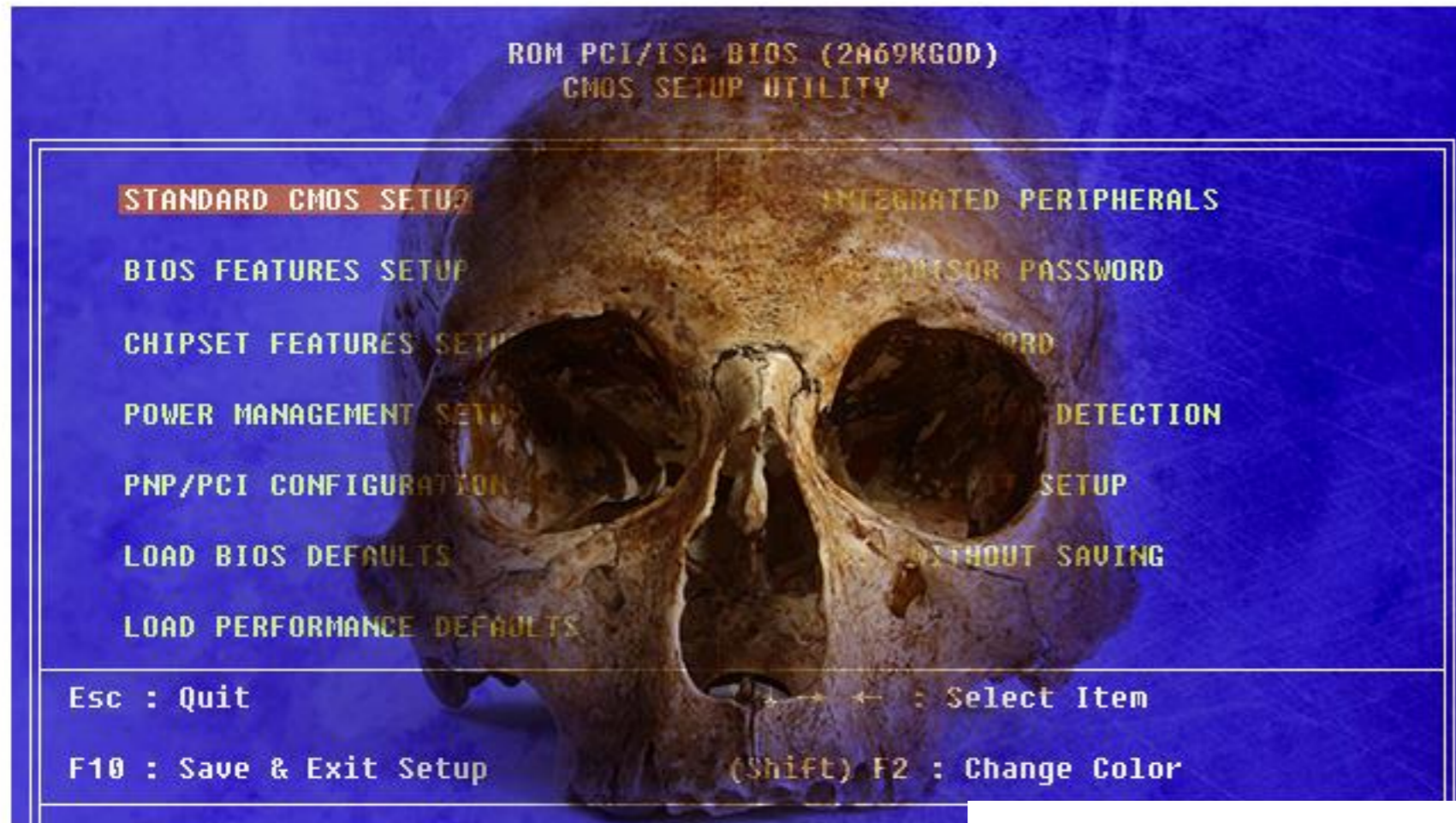
To a computer near you

Meet “badBIOS,” the mysterious Mac and PC malware that jumps airgaps

Like a super strain of bacteria, the rootkit plaguing Dragos Ruiu is omnipotent.

by Dan Goodin - Oct 31 2013, 7:37pm IST

BLACK HAT HACKING 621



Aurich Lawson / Thinkstock

Researchers prove PC viruses can spread via microphones

When the so-called “badBIOS” virus was found in October, transmitting itself by audio broadcasts at inaudible frequencies, it seemed incredible - and now we have proof-of-concept.

How 3-D Printed Guns Evolved Into Serious Weapons in Just One Year

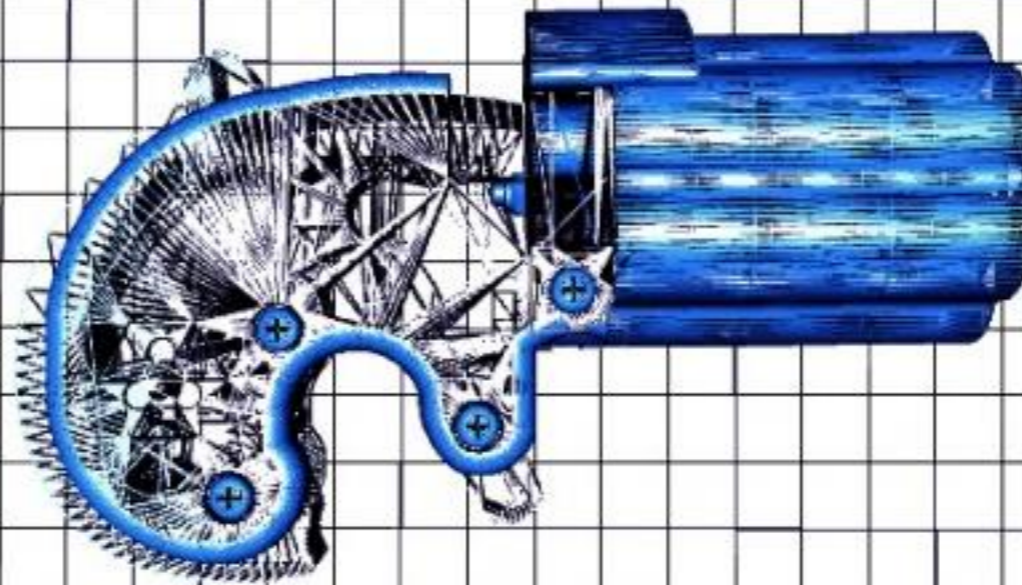
BY ANDY GREENBERG 05.15.14 | 6:30 AM | PERMALINK

[f Share](#) 2.5k

[g+1](#) 268

[in Share](#)

[Pin it](#) 5



The Repringer, a tiny, 3D-printable revolver that fires .22 calibre ammunition. Image: FOSSCAD

Law, Investigation, Awareness

- Sections 65 to 74, IT Act, 2000
 - Major amendments made in 2008
- Amendments made to the Indian Evidence Act
 - 65B, 88A , 45A, etc.
- Amendments to Bankers' Books Evidence Act
- Amendments to CrPC