CYBERSECURITY SUMMIT
2014 – MILANO

09 aprile 2014 - Milan Marriott Hotel

The Underground Economy (with a zoom on Bitcoins)

Raoul «Nobody» Chiesa

Partner, President, **SECURITY BROKERS** SCpA
Permanent Stakeholders Group, **ENISA** (2010-2015)
Founder, Board of Directors, Technical Steering, **CLUSIT**
Board of Directors, **ISECOM**
Special Advisor on Cybercrime and Hackers Profiling, **UNICRI**
Coordinator, Cultural Attachè, **APWG** European Chapter
Board of Directors, **OWASP** Italian Chapter

Abstract

- The evolution of the so-called «hacker's underground» led to **new criminal models** and **approaches** in the **Cybercrime world**.

- This presentation will analyze the so-called "**Underground Economy**", its **players** and **scenarios**, then zooming in the **Bitcoins** - as well as different "cybercrime currencies.

- I will bring to the audience our **own experiences** on these **critical research areas**.

Anti-DDoS,
(basic) Application
Security

Cyber Intelligence,
Black Ops

Human Factor, 0days

SCADA & Industrial
Automation Security,
Defense in-depth

Cybercrime Intelligence,
Compliance

Insider's profiling, DLP

Let's stop dreaming!

- In order to «outperform your adversaries», **you must know who they are**.
  - And, over the last 10 years, the concept of «attacker» **has dramatically changed**.

- Also, the **concept** of a «secure system» doesn't exist anymore. (IMHO). Well, actually, it **never existed** ☺
  - Vulnerabilities brought-in by **vendors**
  - **0days** market
  - **State-Sponsored** attacks
  - **DDoS** powershot
  - **Cybercrime** & **Underground Economy**

- That's why this presentation **will focus on something different**, trying to walk you by new perspectives, providing **case studies** as well.

Also…

❑ In the Information Security (InfoSec) world, we have a tremendous problem: the **terminology.**

- **Each term** has different meanings, depending on the **context** and the **actor**

❑ This is not enough, tough: in the last years a **new trend** come out, which is adding the prefix "**cyber**" to **most of the terms**.

As a side note

→ LOL ☺

- In Italy, we've "solved the whole thing": in the last January 2013 DPCM (National law, "Decreto Presidenza Consiglio dei Ministri"), we do have the "**cibernetic security**" (sicurezza cibernetica)**.**
- Which to us, recalls something (much) different!

Picture credits: Daniele Dal Re

No common spelling…

„Cybersecurity, Cyber-security, Cyber Security ?”

No common definitions…

Cybercrime is…?

No clear actors…

Cyber – Crime/war/terrorism ?

No common components?…

❑ In those non English-speaking countries, problems with correctly understanding words and terms **rise up**.

Agenda

- # whoami
- The scenario(s) and the Actors
- Profiling «Hackers» (?)
- The evolution of 0days market
- Bitcoins
- Underground currencies
- Conclusions
- Resources, Q&A

Disclaimer

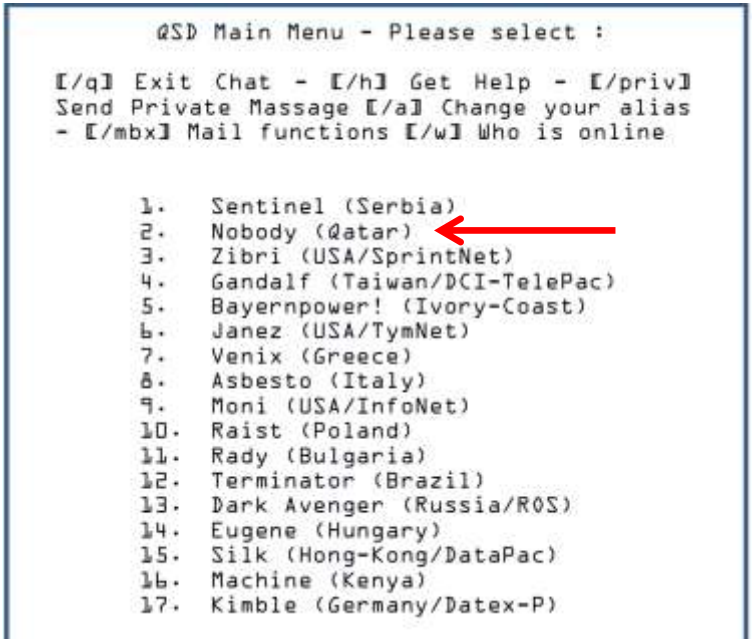
- The information contained within this presentation **do not infringe** on any intellectual property nor does it contain tools or recipe that could be in breach with known laws.
- The statistical data presented **belongs to** the Hackers Profiling Project by **UNICRI** and **ISECOM**.
- Quoted trademarks belongs to **registered owners**.
- The views expressed are those of the author(s) and speaker(s) and **do not necessary reflect** the views of **UNICRI** or others **United Nations** agencies and institutes, nor the views of **ENISA** and its **PSG** (Permanent Stakeholders Group), neither **Security Brokers** ones.
- Contents of this presentation **may be quoted or reproduced**, provided that the **source of information is acknowledged**.

The Speaker

- President, Founder, **Security Brokers SCpA**
- Principal, **CyberDefcon Ltd.**
- Independent Special Senior Advisor on Cybercrime @ **UNICRI** (United Nations Interregional Crime & Justice Research Institute)
- PSG Member, **ENISA** (Permanent Stakeholders Group @ European Union Network & Information Security Agency)
- Founder, Board of Directors and Technical Commitee Member @ **CLUSIT** (Italian Information Security Association)
- Steering Committee, **AIP/OPSI**, Privacy & Security Observatory
- Member, Co-coordinator of the WG «Cyber World» @ **Italian MoD**
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- **Supporter at various security communities**

Once upon a time…

- I joined the **wonderful world of hacking** around **1985**.
- Back in **1996**, after the operation «Ice Trap» which leaded to my (home) arrest in 1995, I **jumped back** to the underground «scene».
- My hackers friends told me they **just began doing something named** «Penetration Test».
  - I had no idea **WTF that thing was**.
  - Then I realized someone was **glad to pay you** in order to «hack» into something.
  - With **rules**, tough. **It was legal**.
  - Paid in order to do what I **mostly liked**?!? Risks-free??
  - «You must be kidding», LOL ☺



Once upon a time…

- Still on **those years**, we used to **find bugs** on our own:
  - Sun Solaris (we [still] love you so much)
  - HP/UX (harder)
  - VAX/VMS, AXP/OpenVMS (very few ones)
  - Linux (plenty of)
  - etc…
- **No one was paying us for those findings**. It was just **phun**.
- No one was «**selling**» that stuff.
  - We used to **keep 'em for us**, and **occasionally** «exchange» the exploits with some other (trusted) hackers.

Years later…

- A **couple of things** happened.
- **Money slowly got involved** in this **research-based** thing.
  - And, the whole world got «always-on», «interconnected», IT&TLC **fully-addicted**.
- Then, **Cybercrime** moved to its prime-time age.
- Money **quickly got involved** in this **exploits-race** thing.

The actors

unicri
advancing security, serving justice, building peace

- Guys, we've «evolved», somehow…
- Here's what United Nations says (Hacker's Profiling Project):

	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they act alone	SME / Specific security flaws	To give vent of their anger / attract mass-media attention
Cracker	17-30 years The destructor, burned ground	LONE	Business company	To demonstrate their power / attract mass-media attention
Ethical Hacker	15-50 years The "ethical" hacker's world	LONE / GROUP (only for fun)	Vendor / Technology	For curiosity (to learn) and altruistic purposes
Quiet, Paranoid, Skilled Hacker	16-40 years The very specialized and paranoid attacker	LONE	On necessity	For curiosity (to learn) => egoistic purposes
Cyber-Warrior	18-50 years The soldier, hacking for money	LONE	"Symbol" business company / End-User	For profit
Industrial Spy	22-45 years Industrial espionage	LONE	Business company / Corporation	For profit
Government Agent	25-45 years CIA, Mossad, FBI, etc.	LONE / GROUP	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker	25-45 years	LONE / GROUP	Government / Strategic company	Monitoring / controlling / crashing systems

SecurityBrokers
Global Cybersecurity Defense Services

And, **it's not**

just «hackers»

Cybercrime

→ Why «Cybercrime»?

«Cybercrime ranks as one of the top four economic crimes»

PriceWaterhouseCoopers LLC Global Economic Crime Survey 2011

"2011 Cybercrime financial turnover apparently scored up more than Drugs dealing, Human Trafficking and Weapons Trafficking turnovers"

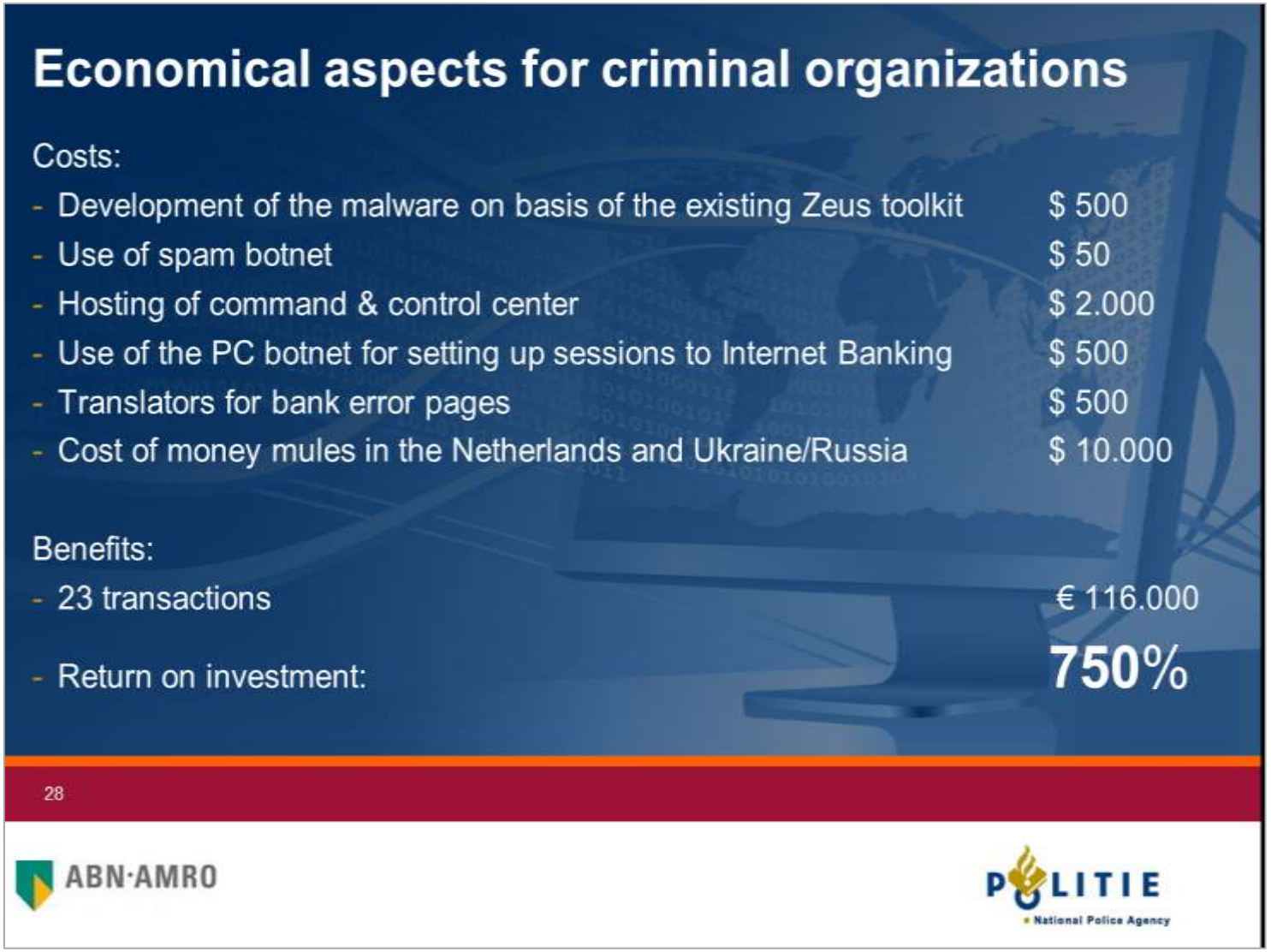
Various sources (UN, USDOJ, INTERPOL, 2011)

Financial Turnover, estimation: 6-12 BLN USD$/year

2013: (at least) 20B USD$/year

Today's scenario (cybercrime)

→ Why «Cybercrime»?

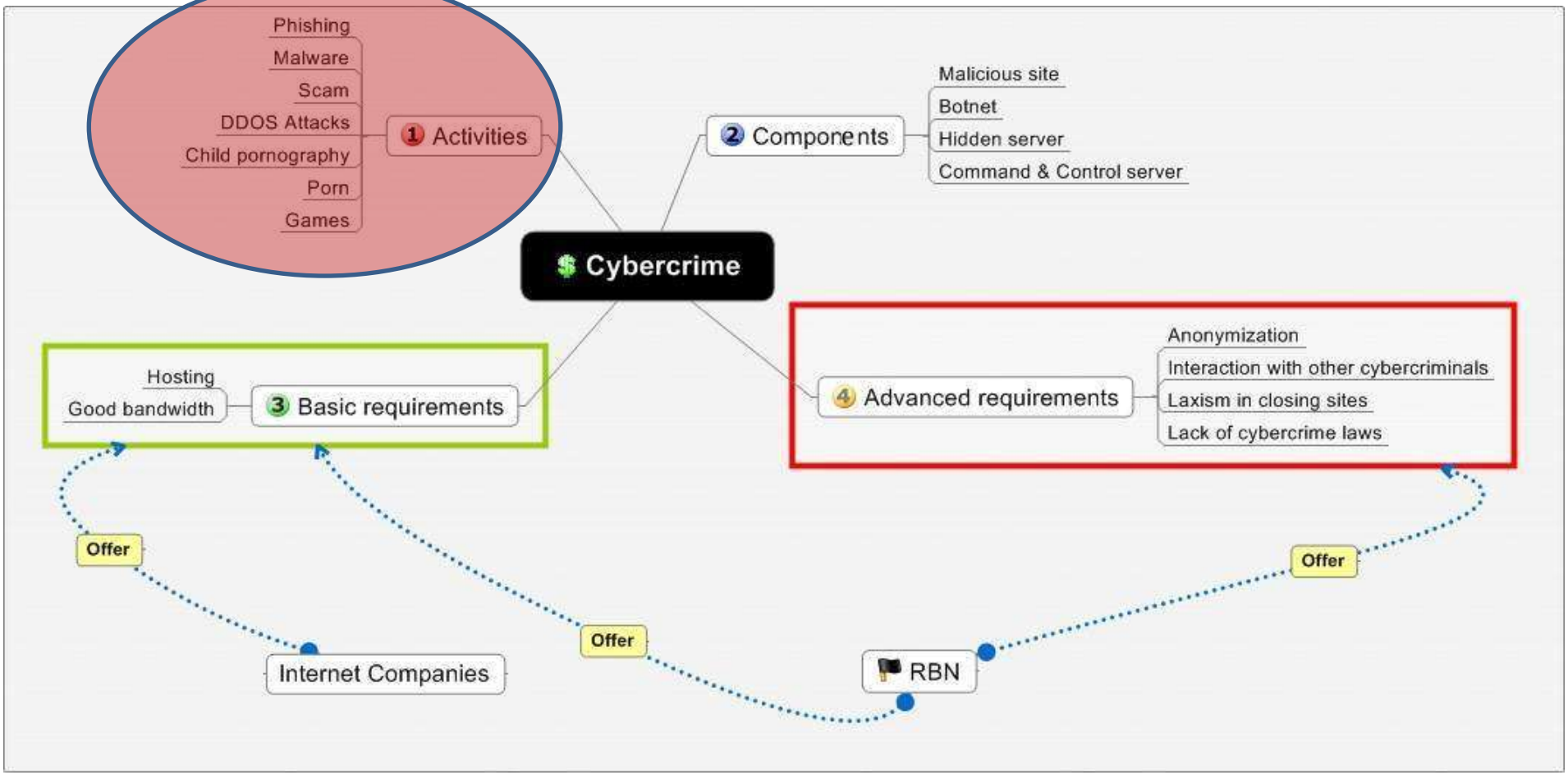


WHY IS ALL OF THIS HAPPENING?

- Because users are stupid (or «naive», uneducated, not aware, etc…)
  - Videoclip: the «wizard» from Belgium

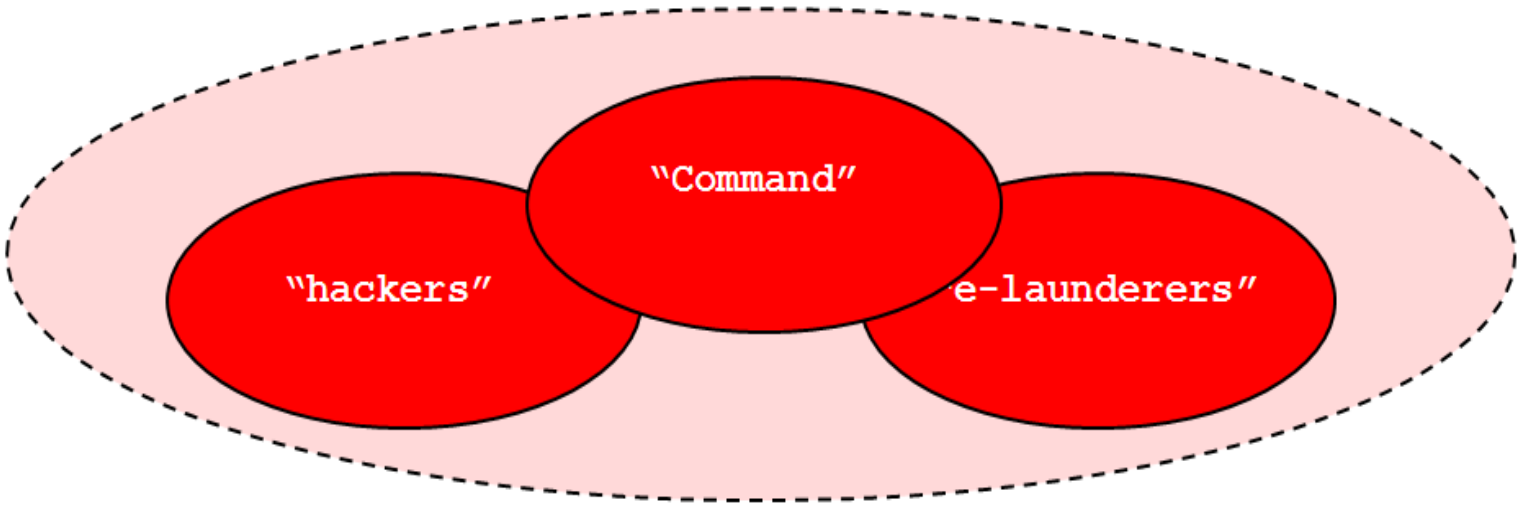
OC (organized crime) meets with Cybercrime

→ The «RBN model» (Russian Business Network)



OC (organized crime) meets with Cybercrime

→ Command chain (and operating phases)



Phase 1

- Performing hacking
- Developing malware
- Building botnets

Phase 2

- Perform ID-theft
- Collect Personal Info
- Collect financial info

Phase 3

- Execute e-crimes
- e-banking
- e-commerce

Phase 4

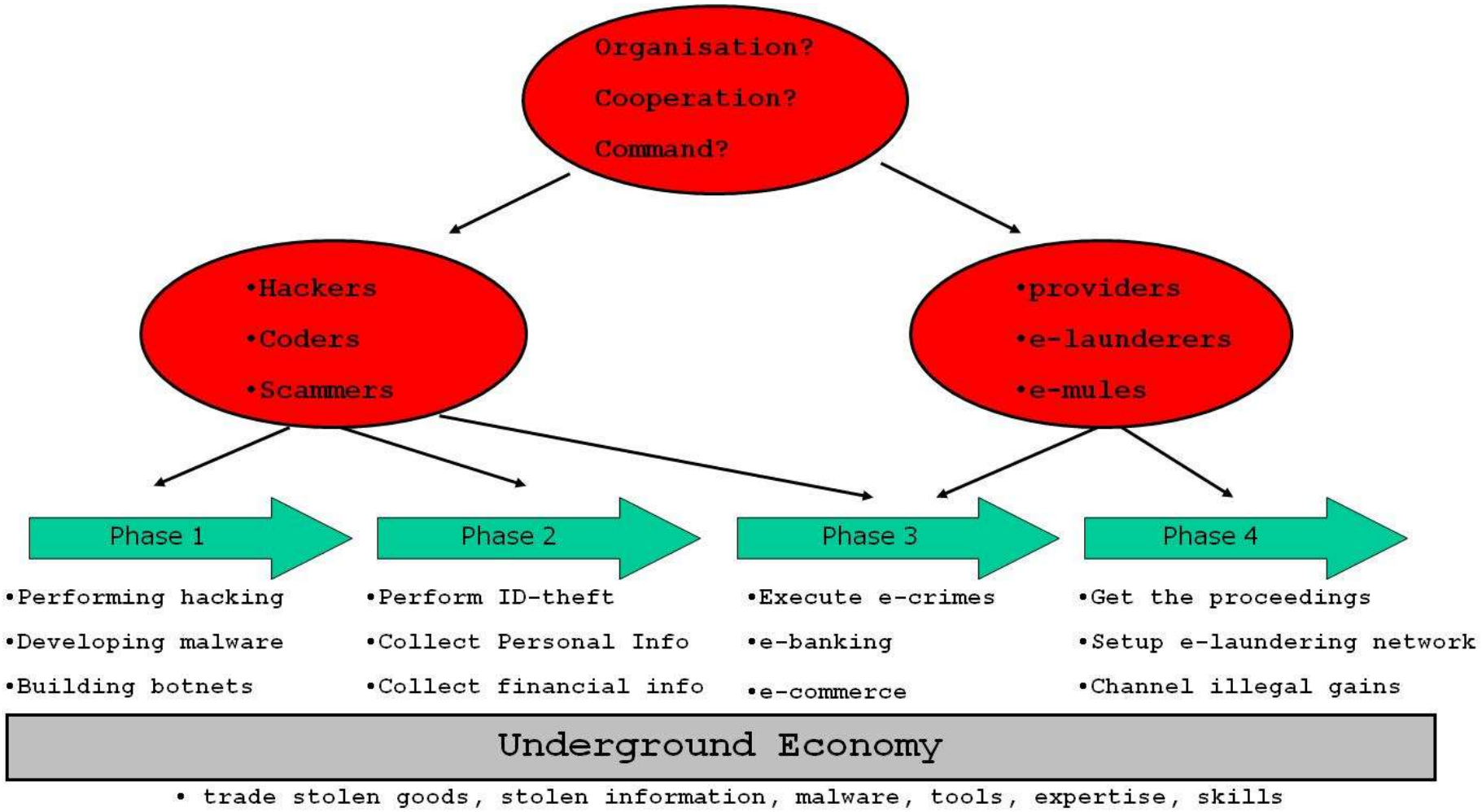
- Get the proceedings
- Setup e-laundering network
- Channel illegal gains

Underground Economy

- trade stolen goods, stolen information, malware, tools, expertise, skills

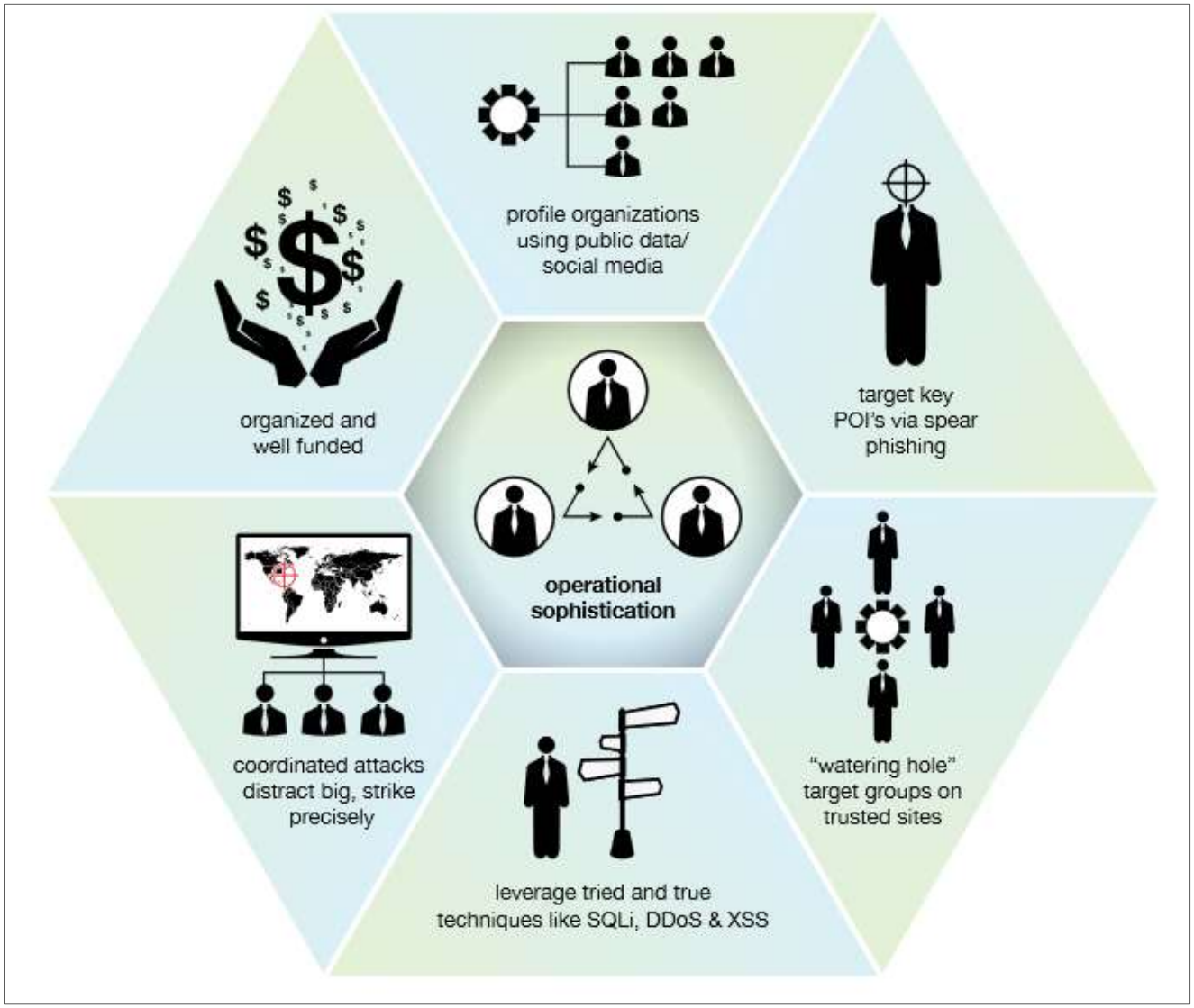
OC (organized crime) meets with Cybercrime

→ Approach by «operative macro-units»



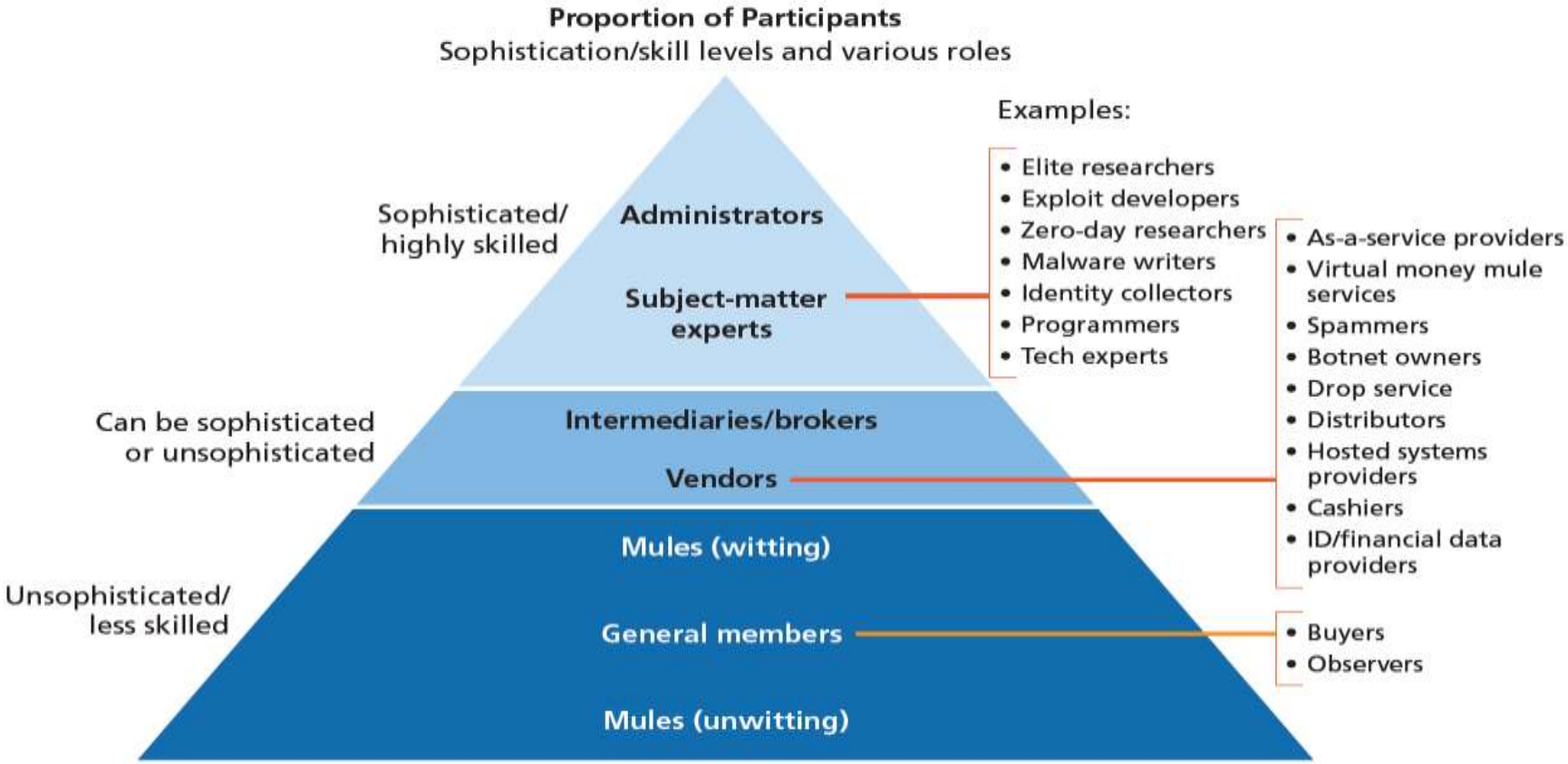
Differences

→ Cybercrime ≠ "hackers"



…That was RBN. Now things evolved ☹

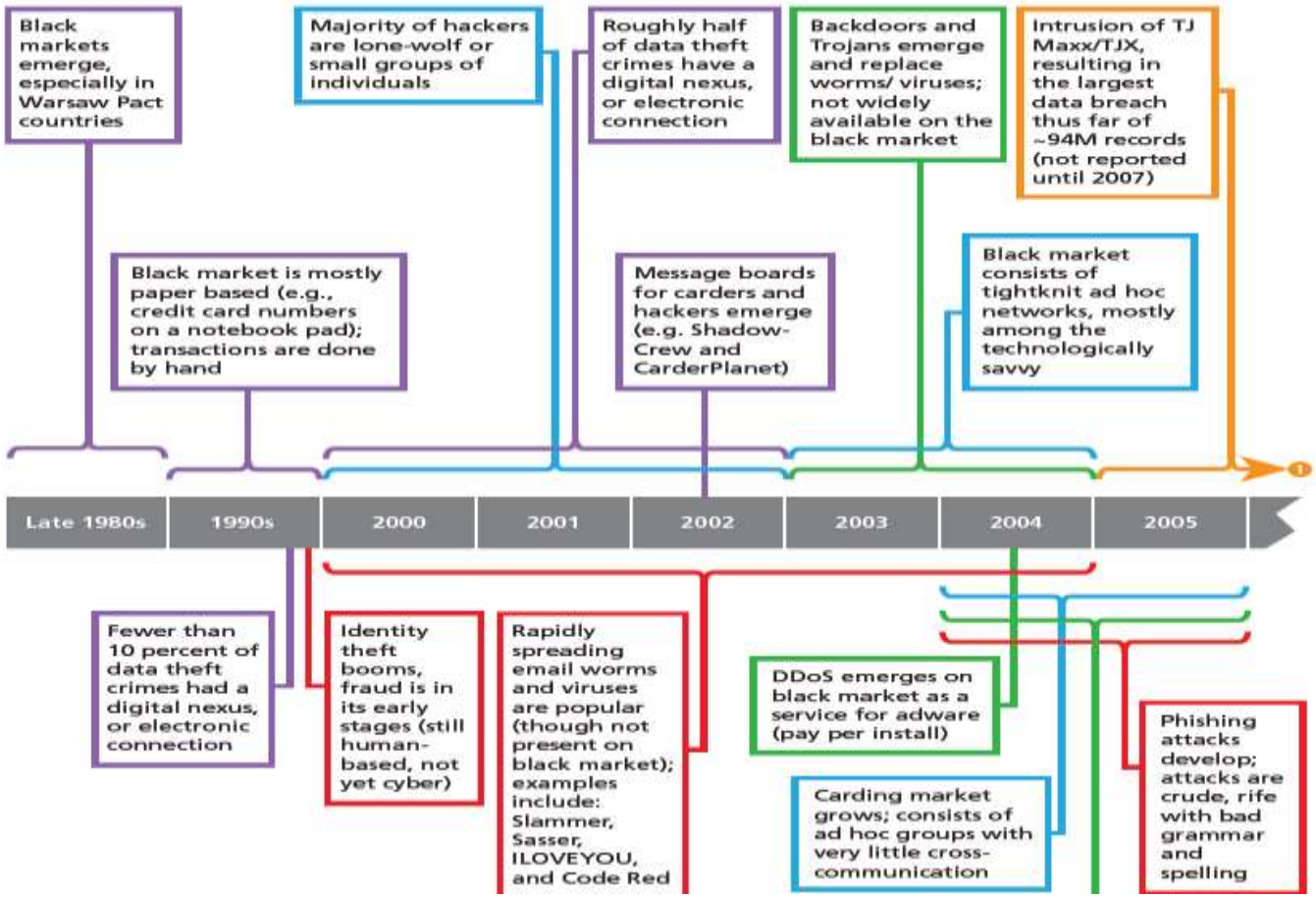
Figure 2.1
Different Levels of Participants in the Underground Market



SOURCES: Drawn from interviews; Schipka, 2007; Panda Security, 2011; Fortinet, 2012; BullGuard, undated.
NOTE: Almost any participant can be a ripper; see text for discussion.
RAND *RR610-2.1*

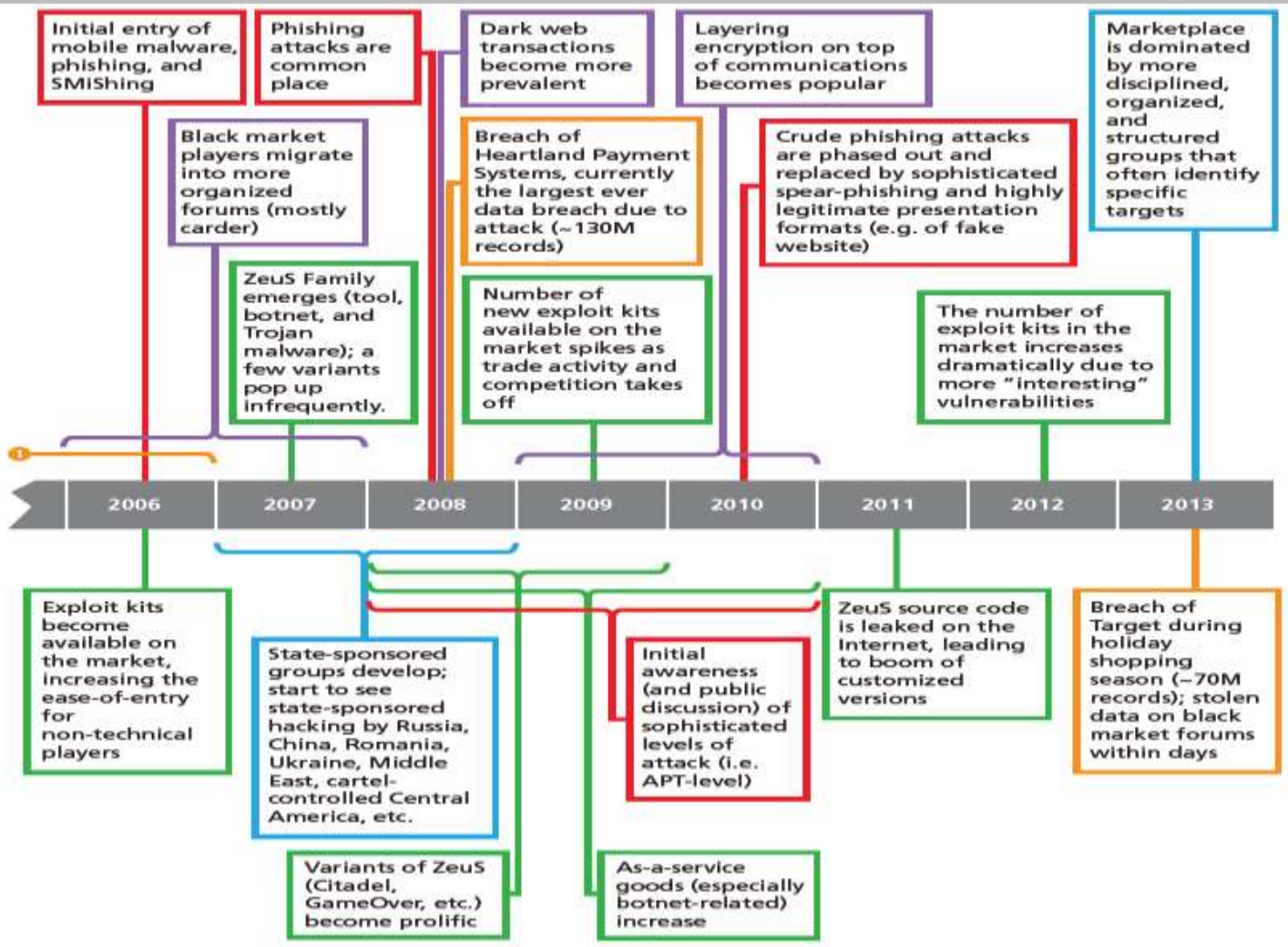
…Let's take a look from the beginning 'till now (2013)

Figure 6.1
Black Market Timeline



RAND *RR610-6.1a*

…Let's take a look from the beginning 'till now (2013)



RAND *RR610-6.1a*

Videoclip time!

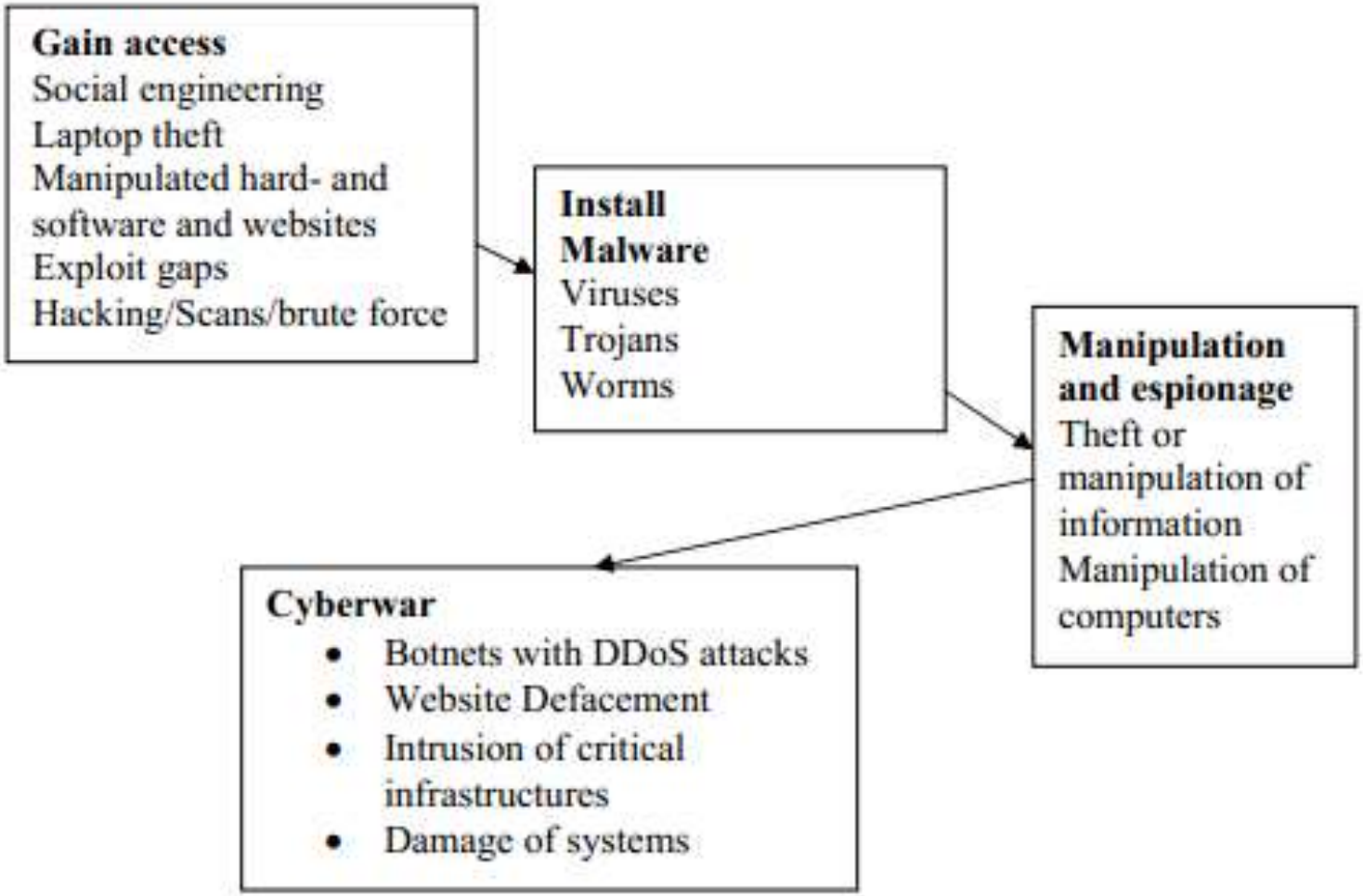
* ESPIONAGE

→ Zooming in

- We are speaking about an ecosystem **which is very often underevaluated**: most of times, it is the **starting** or **transit point** towards different ecosystems:
  - Information Warfare
  - Black Ops
  - **Industrial Espionage**
  - Hacktivism
  - (private) Cyber Armies
  - Underground Economy and Black Markets
    - Organized Crime
    - Carders
    - Botnet owners
    - 0days
    - Malware factories (APTs, code-writing outsourcing)
    - Lonely wolves
    - “cyber”-mercenaries, Deep Web, etc

* ESPIONAGE

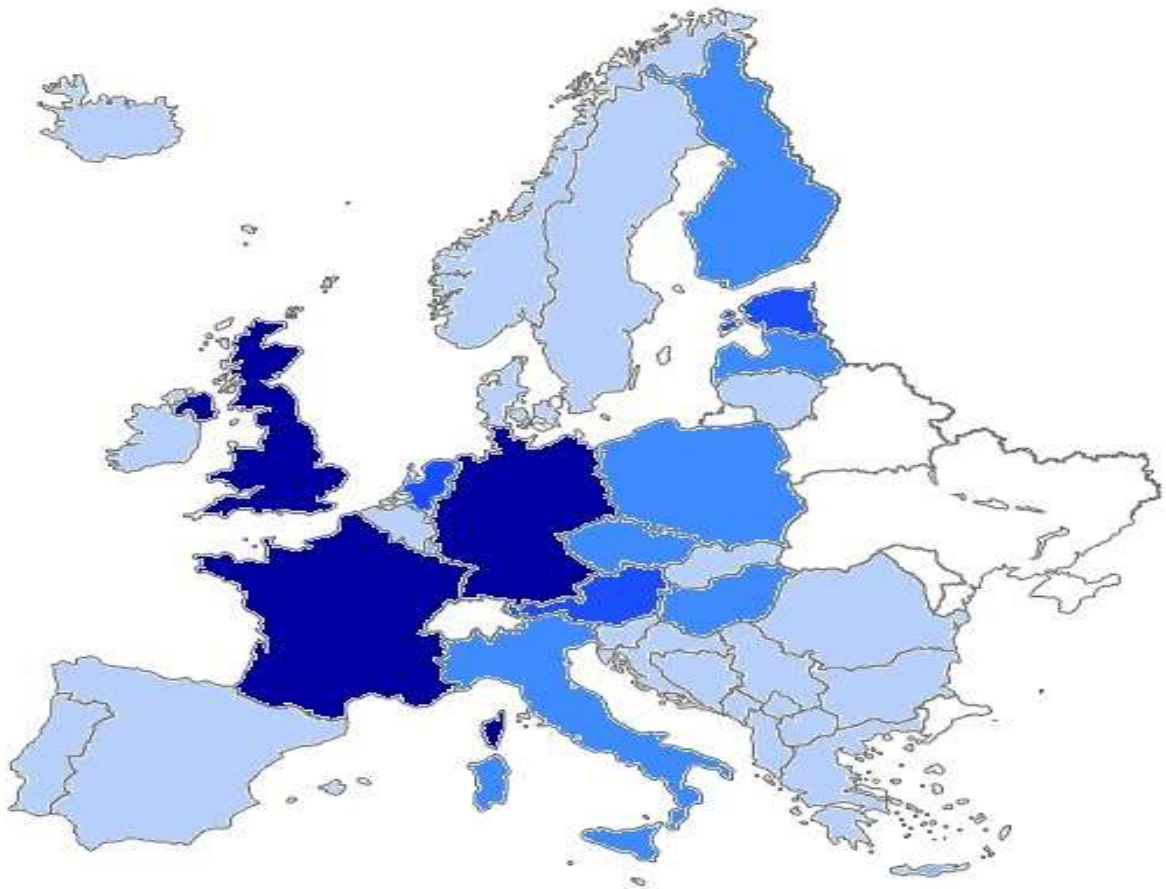
→ As we can see, not so many differences with the hacking approach



Source: Saalbach: «**Cyberwar** Methods & Practice»

EU

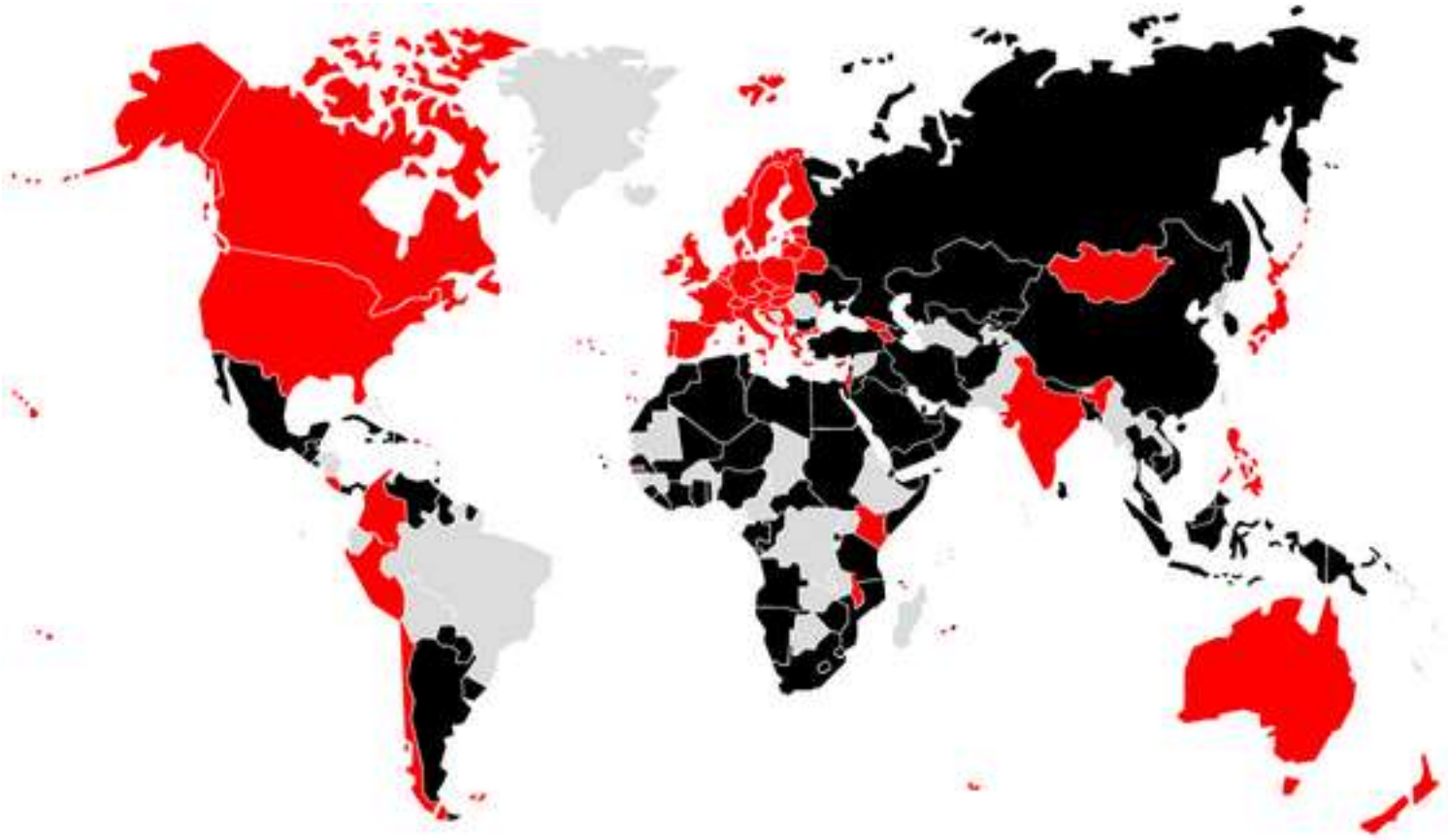
→ Geopolitical Shift: 2013 - Map of Cyber Defense evolving Member States (partial)



Source: Flavia Zappa,
Security Brokers, 2013

World

→ Geopolitical shift : 2013 - Map of ITU Dubai General Assembly December (red=not signed; black=signed)



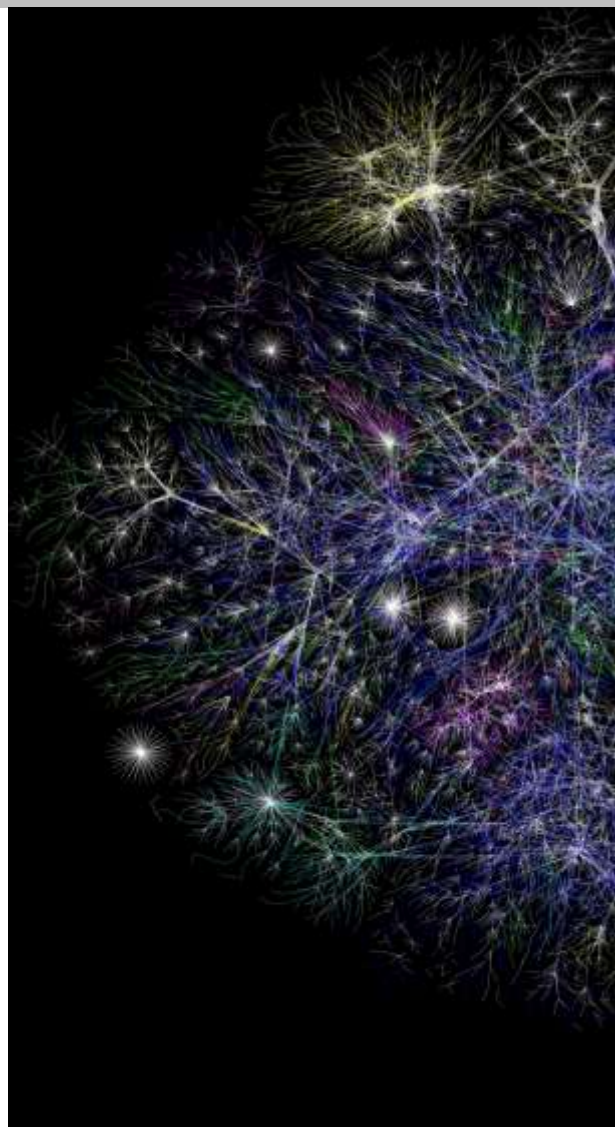
Source: Flavia Zappa,
Security Brokers, 2013

WHAT'S HAPPENING AROUND?

- **Cybercrime and Information Warfare** have a **very wide spectrum of action** and use **intrusion techniques** which are nowadays, somehow, available to a **growing amount of Actors**, which use them in order to **accomplish different goals**, with **approaches and intensity which may deeply vary**.

- **All of the above is launched against any kind of targets:** Critical Infrastructures, Governative Systems, Military Systems, Private Companies of any kind, Banks, Medias, Interest Groups, Private Citizens….
  - National States
  - IC / LEAs
  - Organized Cybercrime
  - Hacktivists
  - Industrial Spies
  - Terrorists
  - Corporations
  - Cyber Mercenaries

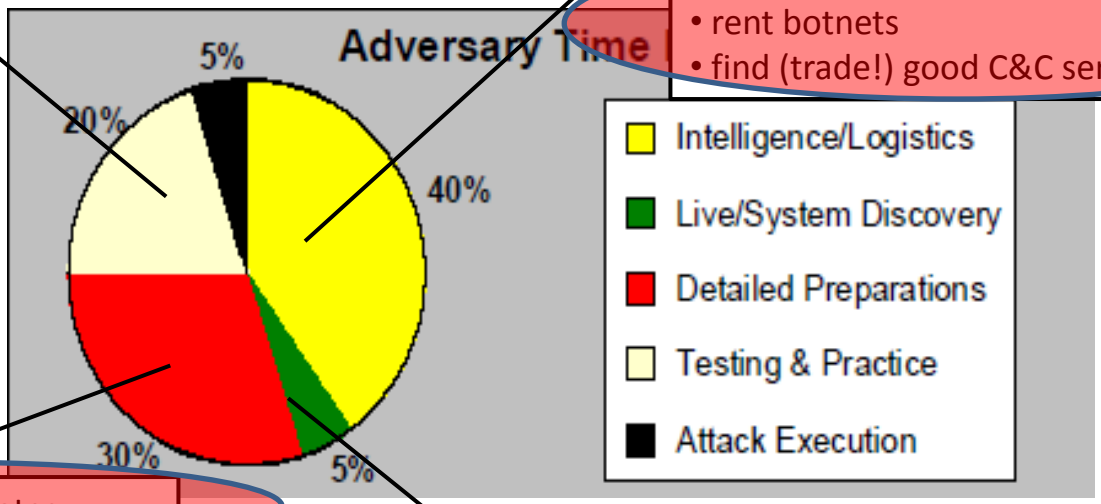
Everyone against everybody



Making Cyber "something"…

- equipment to mimic target network
- dummy run on similar network
- sandbox zerodays

- „dummy list" of „ID-10T" for phishing
- background info on organisation (orgchart etc.)
- Primer for sector-specific social-engineering
- proxy servers
- banking arrangements
- purchase attack-kits
- rent botnets
- find (trade!) good C&C server



- purchase 0-days / certificates
- purchase skill-set
- bespoke payload / search terms

- Purchase L2/L3 system data

Alexander Klimburg 2012

The pricing debate

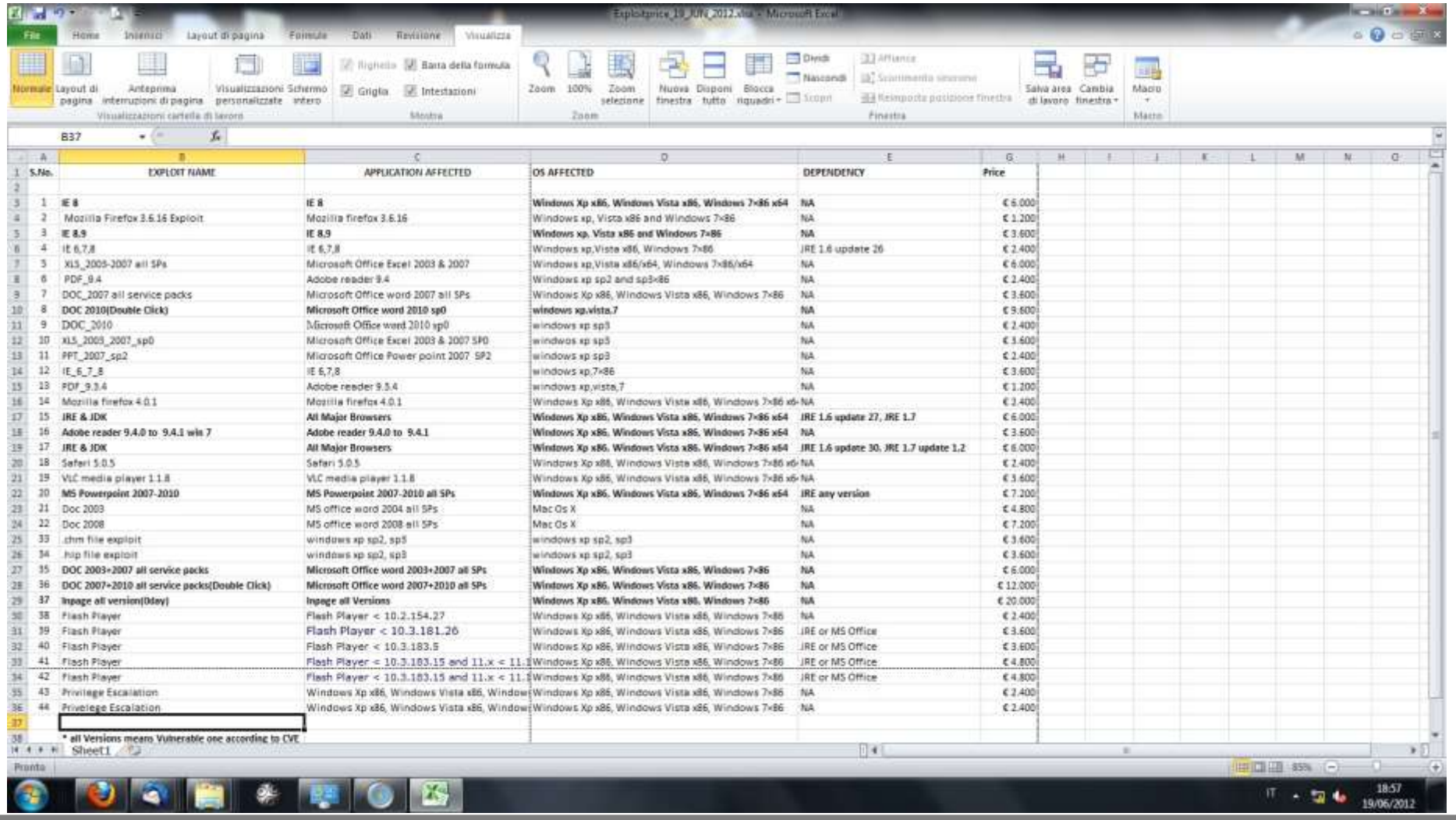
- I think all of you remember this:

ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
IOS	$100,000-$250,000

Source: Forbes, "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits", 2012, in http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits

The pricing debate

- What about this? (CHEAP but LAME, India's ones)



S.No.	EXPLOIT NAME	APPLICATION AFFECTED	OS AFFECTED	DEPENDENCY	Price
1	**IE 8**	**IE 8**	**Windows Xp x86, Windows Vista x86, Windows 7×86 x64**	**NA**	€ 6.000
2	Mozilla Firefox 3.6.16 Exploit	Mozilla firefox 3.6.16	Windows xp, Vista x86 and Windows 7×86	NA	€ 1.200
3	**IE 8.9**	**IE 8.9**	**Windows xp, Vista x86 and Windows 7×86**	**NA**	€ 3.600
4	IE 6,7,8	IE 6,7,8	Windows xp,Vista x86, Windows 7×86	JRE 1.6 update 26	€ 2.400
5	XLS_2003-2007 all SPs	Microsoft Office Excel 2003 & 2007	Windows xp,Vista x86/x64, Windows 7×86/x64	NA	€ 6.000
6	PDF_9.4	Adobe reader 9.4	Windows xp sp2 and sp3×86	NA	€ 2.400
7	DOC_2007 all service packs	Microsoft Office word 2007 all SPs	Windows Xp x86, Windows Vista x86, Windows 7×86	NA	€ 3.600
8	**DOC 2010(Double Click)**	**Microsoft Office word 2010 sp0**	**windows xp,vista,7**	**NA**	€ 9.600
9	DOC_2010	Microsoft Office word 2010 sp0	windows xp sp3	NA	€ 2.400
10	XLS_2003_2007_sp0	Microsoft Office Excel 2003 & 2007 SP0	windows xp sp3	NA	€ 3.600
11	PPT_2007_sp2	Microsoft Office Power point 2007 SP2	windows xp sp3	NA	€ 2.400
12	IE_6_7_8	IE 6,7,8	windows xp,7×86	NA	€ 3.600
13	PDF_9.3.4	Adobe reader 9.3.4	windows xp,vista,7	NA	€ 1.200
14	Mozilla firefox 4.0.1	Mozilla firefox 4.0.1	Windows Xp x86, Windows Vista x86, Windows 7×86 x6	NA	€ 2.400
15	**JRE & JDK**	**All Major Browsers**	**Windows Xp x86, Windows Vista x86, Windows 7×86 x64**	**JRE 1.6 update 27, JRE 1.7**	€ 6.000
16	**Adobe reader 9.4.0 to 9.4.1 win 7**	**Adobe reader 9.4.0 to 9.4.1**	**Windows Xp x86, Windows Vista x86, Windows 7×86 x64**	**NA**	€ 3.600
17	**JRE & JDK**	**All Major Browsers**	**Windows Xp x86, Windows Vista x86, Windows 7×86 x64**	**JRE 1.6 update 30, JRE 1.7 update 1,2**	€ 6.000
18	Safari 5.0.5	Safari 5.0.5	Windows Xp x86, Windows Vista x86, Windows 7×86 x6	NA	€ 2.400
19	VLC media player 1.1.8	VLC media player 1.1.8	Windows Xp x86, Windows Vista x86, Windows 7×86 x6	NA	€ 3.600
20	**MS Powerpoint 2007-2010**	**MS Powerpoint 2007-2010 all SPs**	**Windows Xp x86, Windows Vista x86, Windows 7×86 x64**	**JRE any version**	€ 7.200
21	Doc 2003	MS office word 2004 all SPs	Mac Os X	NA	€ 4.800
22	Doc 2008	MS office word 2008 all SPs	Mac Os X	NA	€ 7.200
33	.chm file exploit	windows xp sp2, sp3	windows xp sp2, sp3	NA	€ 3.600
34	.hlp file exploit	windows xp sp2, sp3	windows xp sp2, sp3	NA	€ 3.600
35	**DOC 2003+2007 all service packs**	**Microsoft Office word 2003+2007 all SPs**	**Windows Xp x86, Windows Vista x86, Windows 7×86**	**NA**	€ 6.000
36	**DOC 2007+2010 all service packs(Double Click)**	**Microsoft Office word 2007+2010 all SPs**	**Windows Xp x86, Windows Vista x86, Windows 7×86**	**NA**	€ 12.000
37	**Inpage all version(0day)**	**Inpage all Versions**	**Windows Xp x86, Windows Vista x86, Windows 7×86**	**NA**	€ 20.000
38	Flash Player	Flash Player < 10.2.154.27	Windows Xp x86, Windows Vista x86, Windows 7×86	NA	€ 2.400
39	Flash Player	Flash Player < 10.3.181.26	Windows Xp x86, Windows Vista x86, Windows 7×86	JRE or MS Office	€ 3.600
40	Flash Player	Flash Player < 10.3.183.5	Windows Xp x86, Windows Vista x86, Windows 7×86	JRE or MS Office	€ 3.600
41	Flash Player	Flash Player < 10.3.183.15 and 11.x < 11.1	Windows Xp x86, Windows Vista x86, Windows 7×86	JRE or MS Office	€ 4.800
42	Flash Player	Flash Player < 10.3.183.15 and 11.x < 11.1	Windows Xp x86, Windows Vista x86, Windows 7×86	JRE or MS Office	€ 4.800
43	Privilege Escalation	Windows Xp x86, Windows Vista x86, Window	Windows Xp x86, Windows Vista x86, Windows 7×86	NA	€ 2.400
44	Privilege Escalation	Windows Xp x86, Windows Vista x86, Window	Windows Xp x86, Windows Vista x86, Windows 7×86	NA	€ 2.400

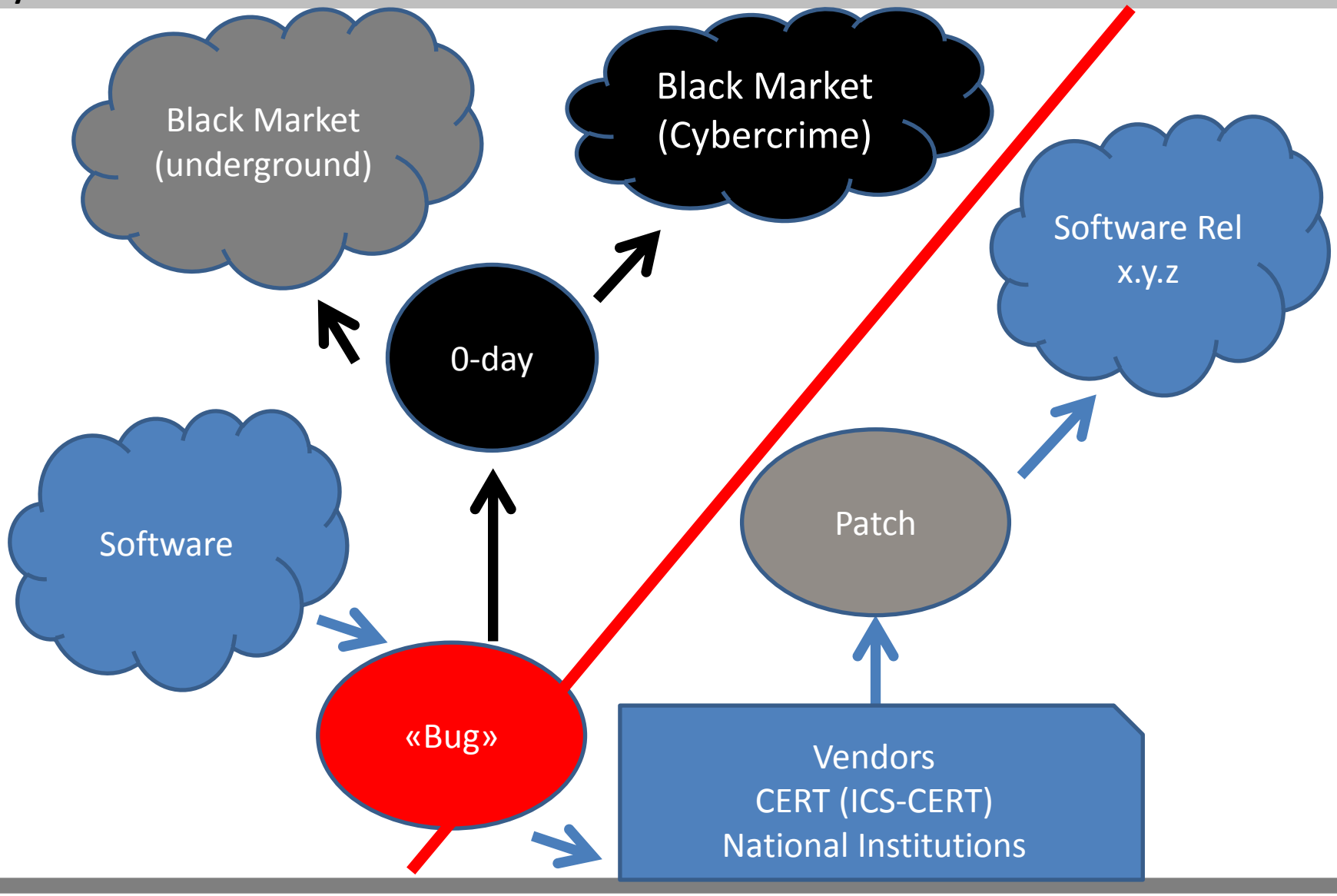
* all Versions means Vulnerable one according to CVE

Where’s the truth?

What’s the right approach with «pricing»?

Getting the big picture

→ 0-day Markets



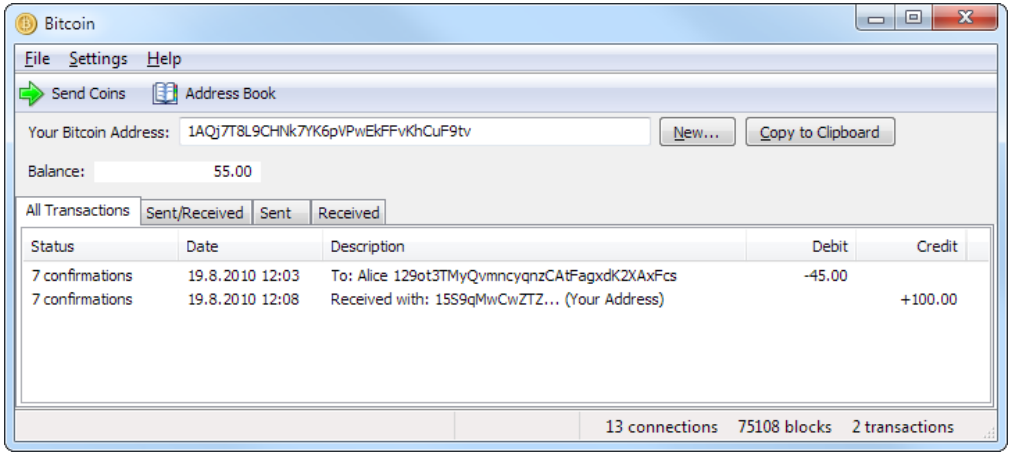
A different (more serious?) approach

Public Knowledge of the vulnerability	Buyer's typology IS = IT Security companies INT = Intelligence Agencies for Governmental use (National Security protection) MIL = MoD/related actors for warfare use OC = Cybercrime	0-day Exploit code + PoC Cost: Min/Max
Y	IS	10K – 50K USD
Y	INT	30K – 150K USD
Y	MIL	50K – 200K USD
Y	OC	5K – 80K USD
N	ALL	X2 – X10

A different (more serious?) approach

Public Knowledge of the vulnerability	Vulnerability relays on: Operating System (OS) Major General Applications (MGA) SCADA-Industrial Automation (SCADA)	Buyer's typology IS = IT Security companies INT = Intelligence Agencies for Governmental use (National Security protection) MIL = MoD/related actors for warfare use OC = Cybercrime	0-day Exploit code + PoC Cost: Min/Max
Y	OS	OC	40K – 100K
Y	MGA	INT	100K – 300K
Y	SCADA	MIL	100K – 300K
N	OS	MIL	300K – 600K
N	SCADA	MIL	400K – 1M

On Bitcoins



On Bitcoins

- **A peer-to-peer digital currency that is pseudo-anonymous.**
- **The identity of the individual is disguised, but his/her transactions are open to the public. It is anonymous to the extent that it is difficult to relate a digital identity to an actual person.**
- **Bitcoins have huge implications on money laundering.**
- **Various government institutions around the world are starting to view it as an area requiring regulation.**

On Bitcoins

- **Bitcoins are created through a process of ‘mining’, in which users who provide their computing power, verify and record payments into a public ledger in exchange for transaction fees in newly minted bitcoins.**

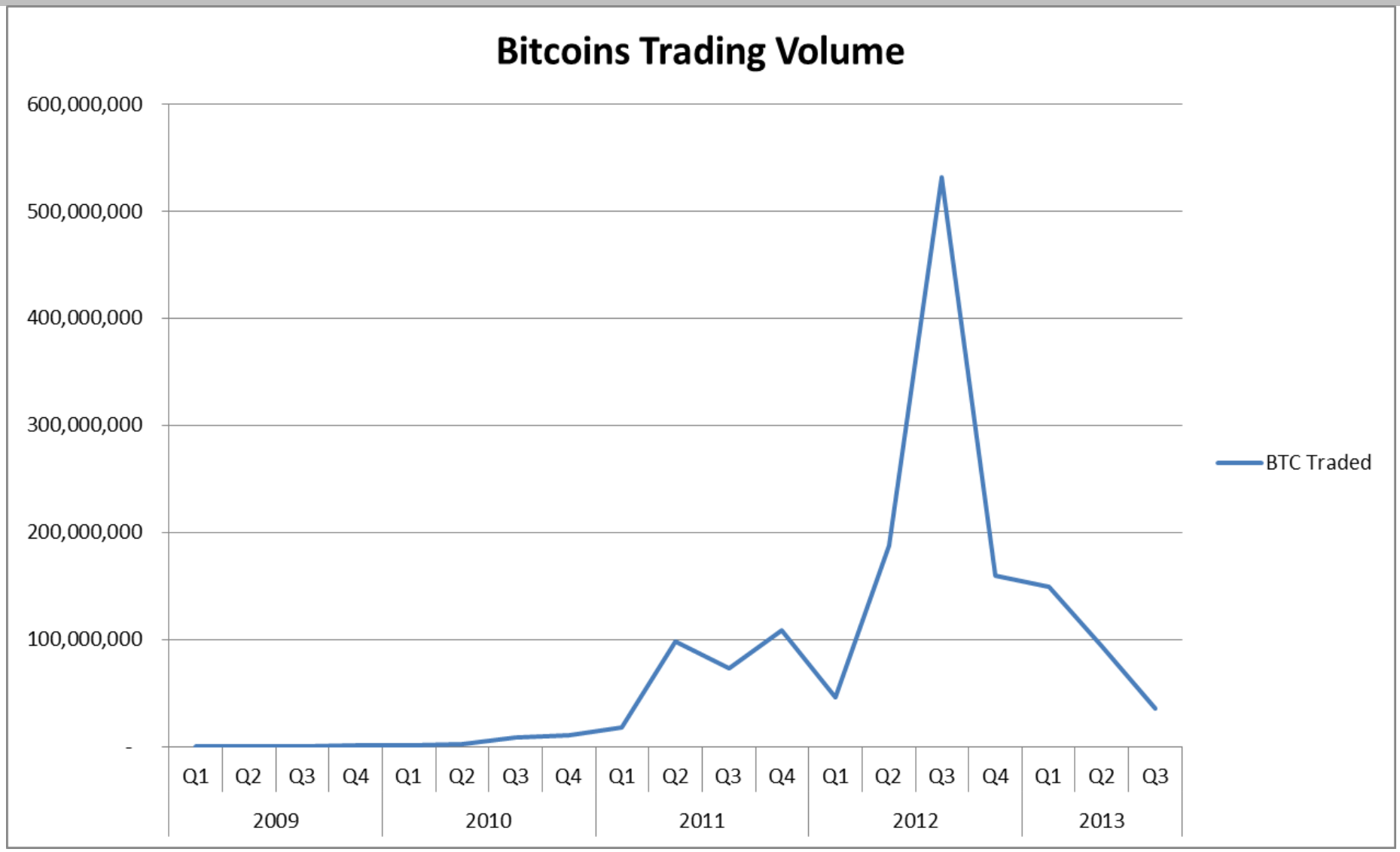
- **This process is akin to a central bank printing new money, but is less centralised.**

On Bitcoins: why is it important to business?

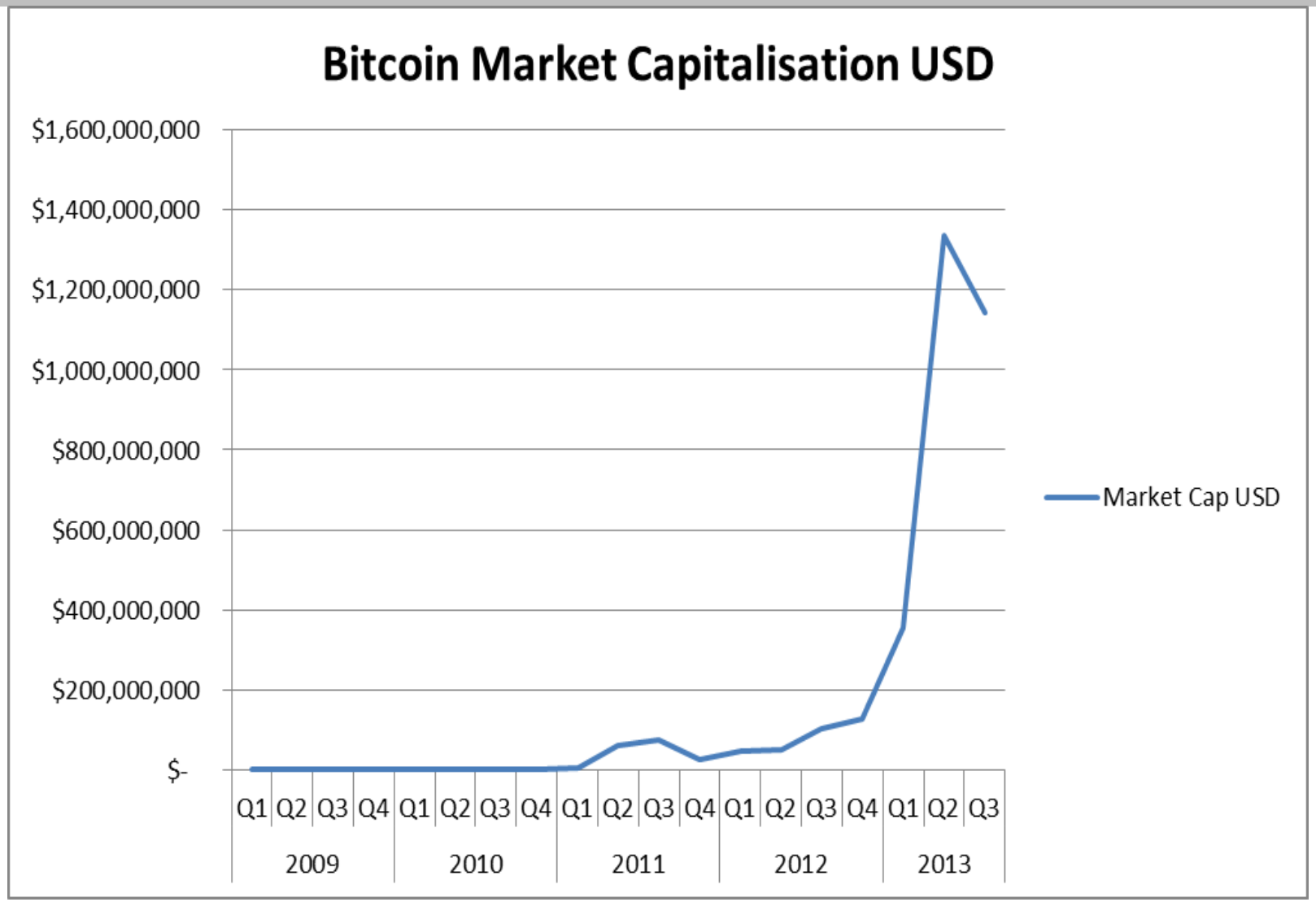
- **Botnets steal your computing power to either:**
  1) 'Mine' more bitcoins. Similar to SETI, but more nefarious.
  2) Conduct various cyber crimes

- **If your networks are insecure, you are indirectly facilitating cyber criminals.**

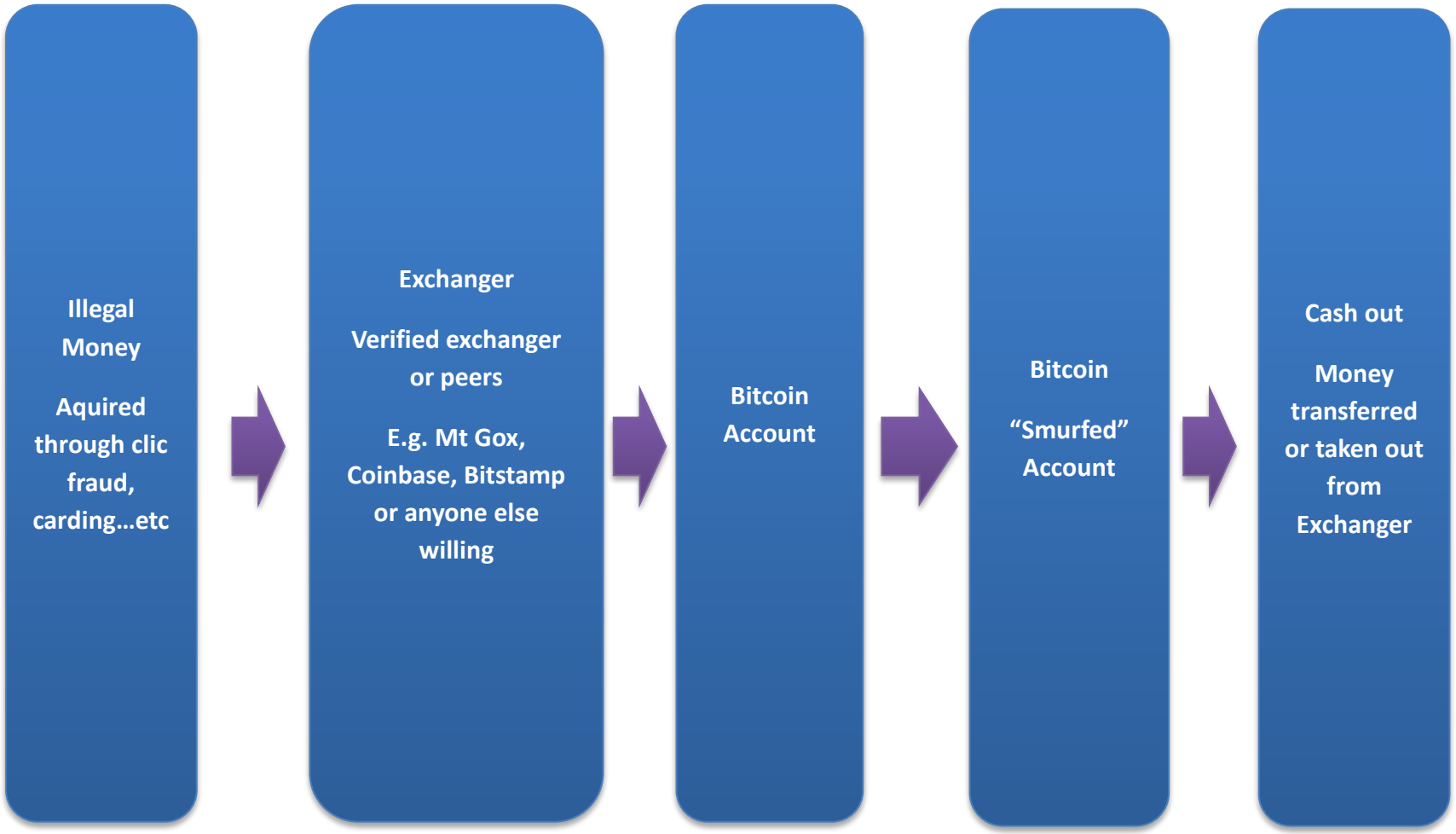
On Bitcoins



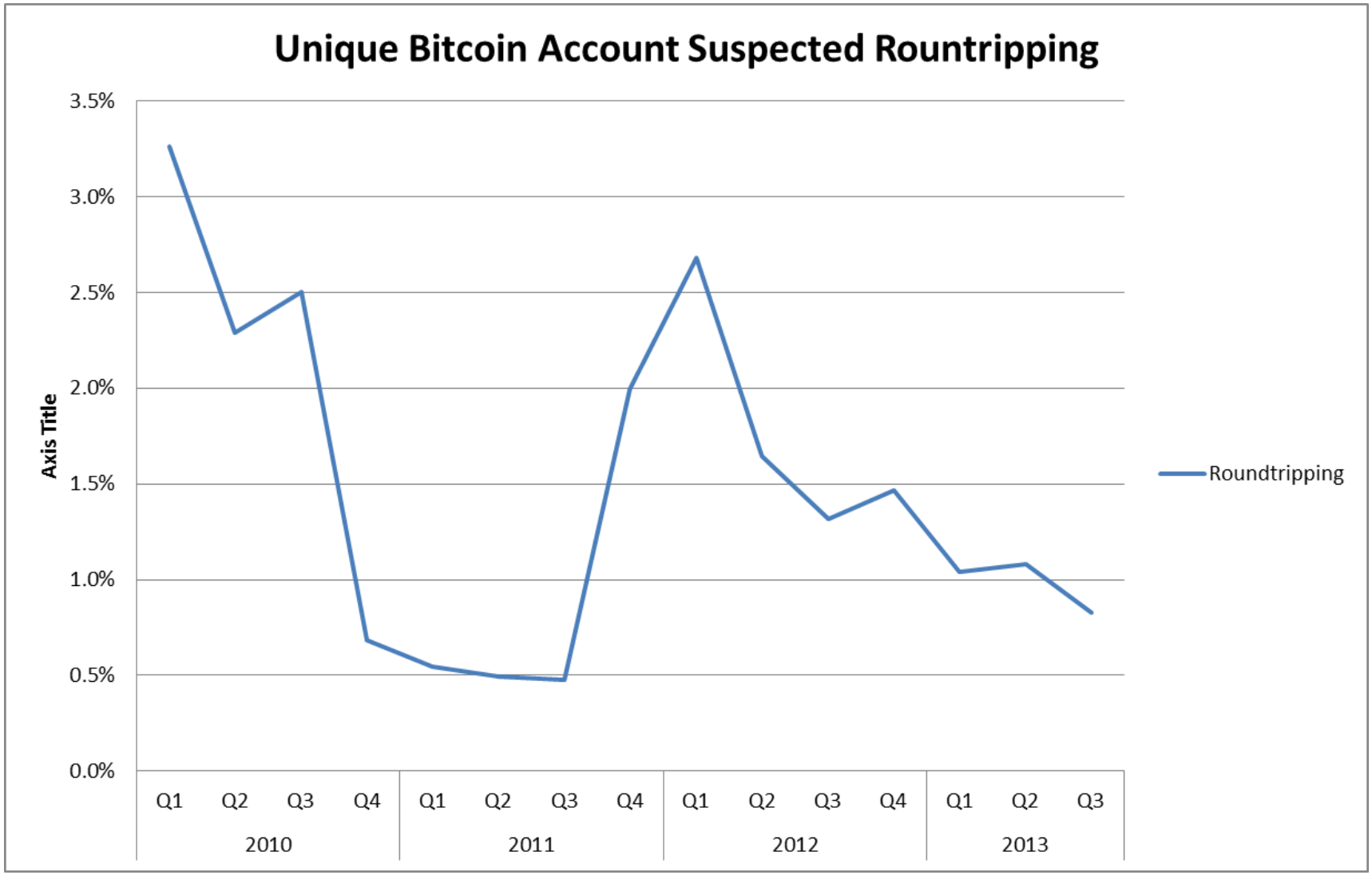
On Bitcoins



Round-tripping with Bitcoins



Round-tripping with Bitcoins



Round-tripping with Bitcoins

Year	Qtr	% RT	USD
2010	Q1	3.3%	$ -
	Q2	2.3%	$ -
	Q3	2.5%	$ 440
	Q4	0.7%	$ 1,643
2011	Q1	0.5%	$ 3,198
	Q2	0.5%	$ 24,707
	Q3	0.5%	$ 38,701
	Q4	2.0%	$ 186,743
2012	Q1	2.7%	$ 564,852
	Q2	1.6%	$ 280,848
	Q3	1.3%	$ 501,184
	Q4	1.5%	$ 809,282
2013	Q1	1.0%	$ 1,627,240
	Q2	1.1%	$ 4,126,558
	Q3	0.8%	$ 2,230,083

Summary on Bitcoins

- **While Bitcoins can be used legitimately, they are used by cyber criminals to launder money.**
- **An unsecured network can be used by the same cyber criminals, thereby indirectly increasing their gains.**
- **More regulation is required in the area.**
- **We would like to use international credit card fraud data to further examine to extent to which Bitcoins are related to fraud.**
- **The data has been difficult to obtain so far.**

HOW DO YOU PAY CYBERCRIME SERVICES/PRODUCTS?

- **CASH (F2F)**
- **Offshore bank accounts**
- **Underground currencies (digital)**
  - **NOTE: it's not just about Bitcoin!**

HAWALA

You probably know about “HAWALA”

Hawala (also known as hundi) is an informal value transfer system based on the performance and honour of a huge network of money brokers

Learning from terrorism financial approach

Many of electronic payment systems are following the HAWALA principle
And built on the top of similar infrastructure

Now backed by digital inftastructure

No traces in banking network

Money disappear in one place, pop up in another

Underground Curriences

Lets look at some examples

There is more than one way to transfer money

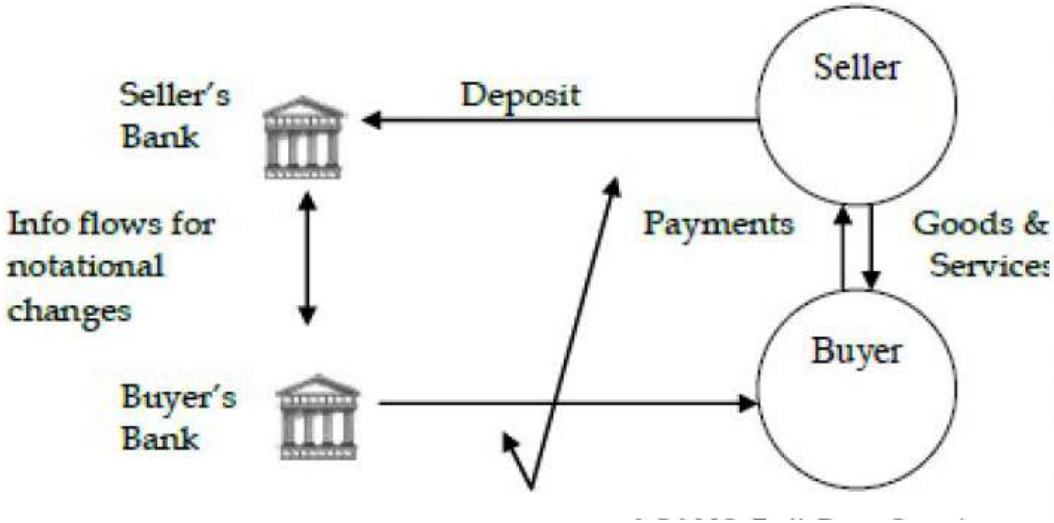
Underground Curriences

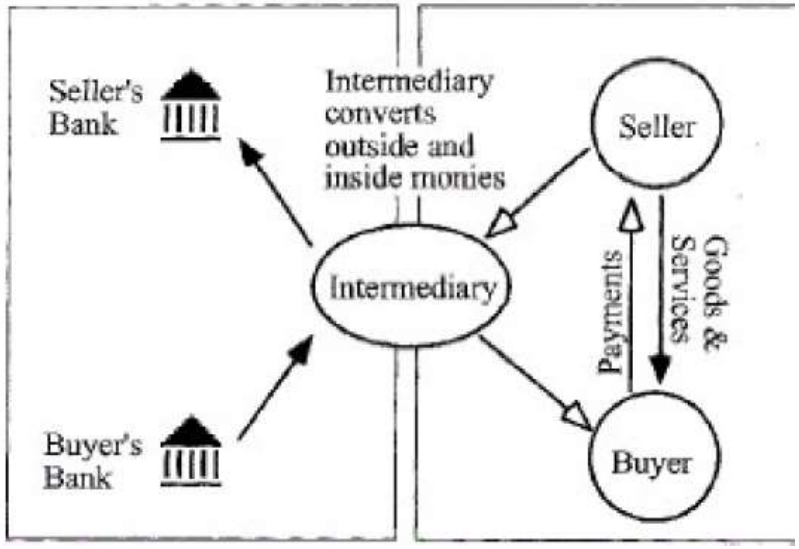
Of course you know paypal and other "white" payment electronic systems. They are simple, and uninteresting

Figure 4: Electronic cash system (Charalampos, 2004)

Underground Curriences

- Controlled by regulatory acts. (http://www.ffiec.gov/PDF/EFS.pdf)
- Similar to conventional payment systems (not much space for anonymized fraud :-))





Underground Curriences

Getting to know "Underground" money systems

- WMZ - web money - one wmz = one USD
- Drop - money mule
- CC - creditcards
- Abuse resistant - Safe to host any kind of fraudulent service
- Partnerka - partnership program

WMR – эквивалент RUB
WMZ – эквивалент USD
WME – эквивалент EUR
WMU – эквивалент UAH
WMB – эквивалент BYR
WMY – эквивалент UZS
WMG – эквивалент 1GG

Underground Curriences

There are many:

- Web Money (WMZ)
- Yandex Money
- LR (liberty reserve
- Epassporte (dead!)

Where is webmoney office in Thailand?

Webmoney Gate Czech	Прага	Чехия
Webmoney в Брянске	Брянск	Россия
WebMoney Club	Орел	Россия
WmPerm.RU	Пермь	Россия
wmTrader.BIZ	ОМСК	Россия
WMCashing	Санкт-Петербург	Россия
WebMoney центр в Великобритании	Нортхэмптон	Великобритания
oWMT.ru - Генеральный дилер Webmoney Transfer	ОМСК	Россия
Webmoney.kg	Бишкек	Кыргызстан
WMT-Tula, сервис WebMoney в г. Тула	Тула	Россия
Moscow Transfer	Москва	Россия
WMZ.lv	Рига	Латвия
Webmoney Israel	Хадера	Израиль
WebMoney Exchange Point, Pattaya, Thailand	Патайя	Тайланд
Финансовый цен		
Ростовский обме		
Webmoney24	Санкт-Петербург	Россия
Обменный пункт Webmoney в Екатеринбурге	Екатеринбург	Россия
E-money - электронные деньги в Кыргызстане	Бишкек	Кыргызстан

Pataya!! Where gangsters are ;-)

Underground Curriences

Credit card “dumps” websites, work only with “trusted” systems. Why?

AlertPay, SMS, LiqPay

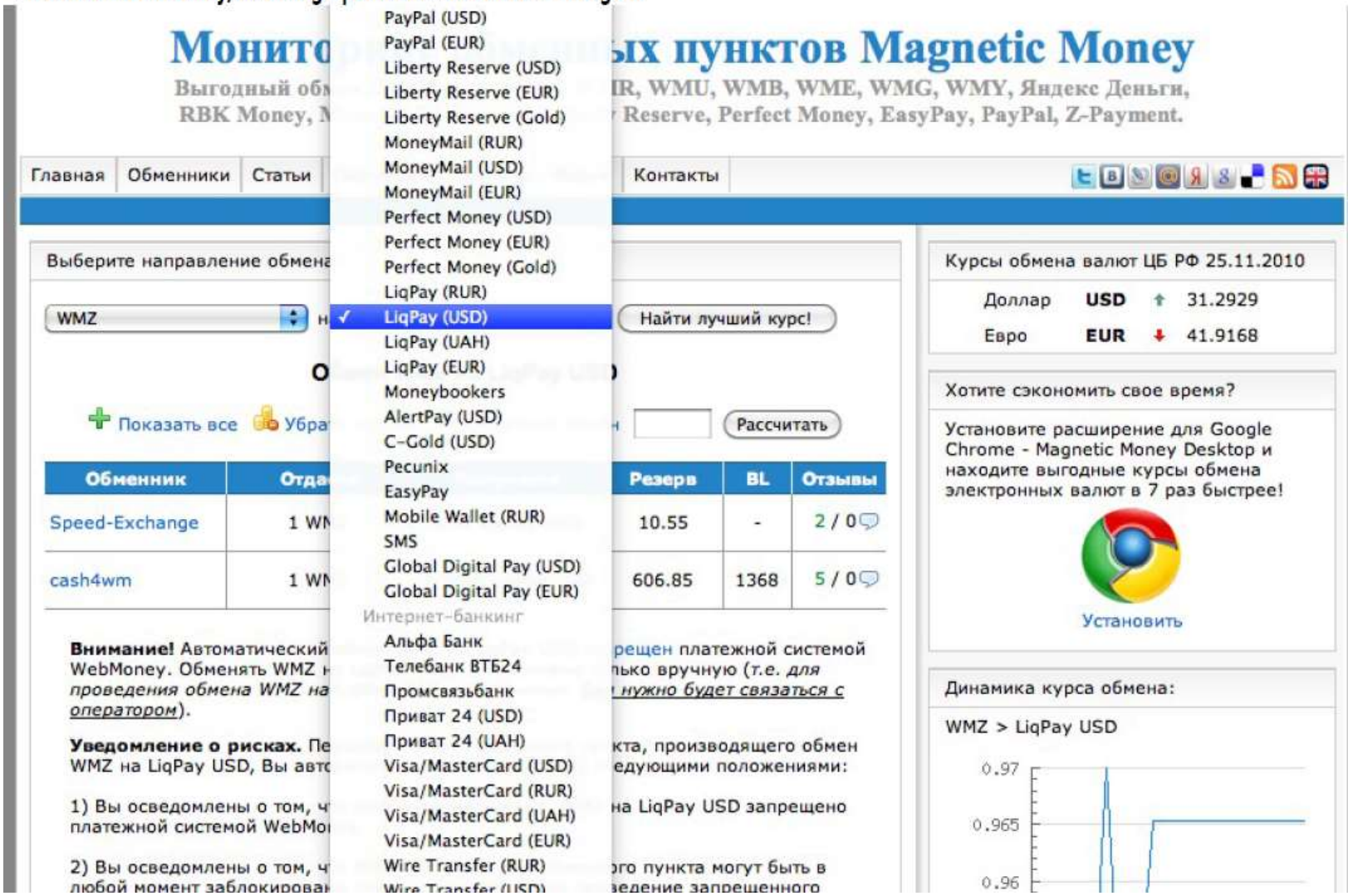
Underground Curriences

They feature "awesome" geographical locations

Liberty Reserve – largest payment processor and money transfer ... +1 -
www.libertyreserve.com/ - 頁庫存檔
Oldest, safest and most popular payment processor operating in Costa Rica and serving millions all around a world. Store your funds privately in gold, Euro or ...

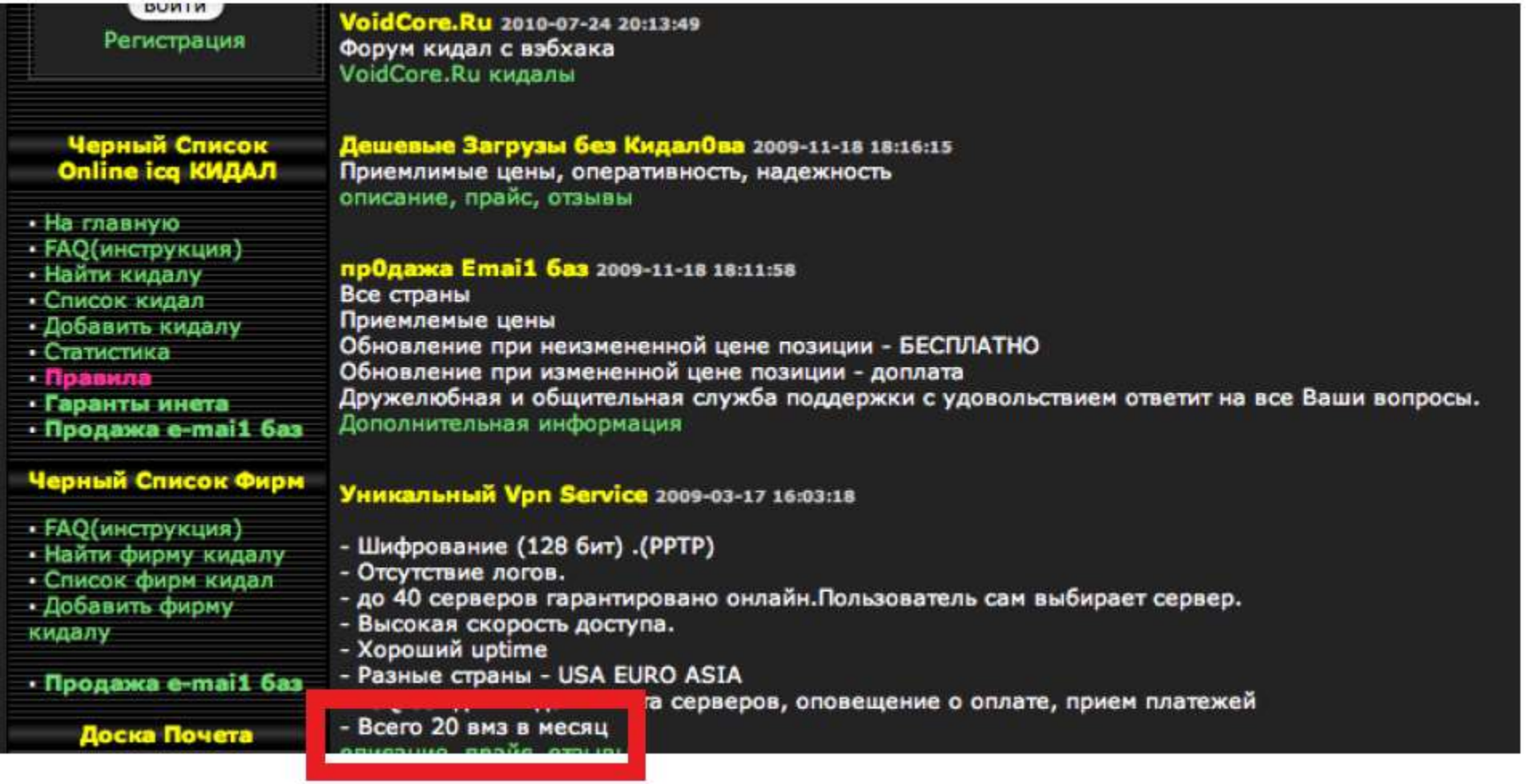
Underground Curriences

As with real currency, exchange points exist. Percent charged:



Underground Curriences

WMZ - widely used on black markets



Underground Curriences

Credit cards: easily available and covertable into non-traceable currency

41:50:Wesley Maxwell::756 Post Drive::Whiteman AFB:Missouri:65305:United States:Wesley Maxwell:5471691100
02:34:Andrew Martin::840 21st Ave North::south saint paul:Minnesota:55075-1314:United States:Andrew Martin:40
00:56:Eric Wentorf::3510 Haven Ave::Racine:Wisconsin:53405:United States:Eric Wentorf:4356874055603252:030
18:19:Luz Owens::521 Southbridge Creek Drive::Jacksonville:Florida:32259:United States:Luz Owens:549099329
16:59:Luz Owens::521 Southbridge Creek Drive::Jacksonville:Florida:32259:United States:Luz Owens:549099329
50:31:Allan Gonzalez Muniz::420 Declaration Ave::Billings:Montana:59105:United States:Allan Gonzalez Muniz:44
13:46:Jamie Kozak::w3804 Hemlock Drive:54555:Phillips:Wisconsin:54555:United States:Jamie Kozak:601100611
42:55:Leslie Oster , III::2604 N. E. 1st Ave.::Ocala:Florida:34470:United States:Leslie Oster , III:5111220002016789
52:34:Ronald Gieseke:Arachnid, Inc.:6212 Material Ave.::Love's Park:Illinois:61132:United States:Ronald Gieseke:
20:57:Travis Jones::250 Meadow Lane::Secaucus:New Jersey:07094:United States:Travis Jones:44821501416198
55:50:Allan Papworth::3570 Corey Rd::Malabar:Florida:32950:United States:Allan Papworth:5466160047269145:0
42:48:Grigoriy Ter-Oganov:E.T.G.:100 Morain st. #302::Kennewick:Washington:99336:United States:Grigoriy

Underground Curriences

Such data is also on sale (note LR -> Liberty Reserve payment system)

Bad guys hacking bad guys

BUSINESS INSIDER AUSTRALIA

Tech | Money & Markets | Briefing | Ideas | Executive Life

RECENTLY ON GIZMODO

Blow Corn Starch To Breath Fire Like A Dragon

RECENTLY ON GIZMO

Breakfast Wrap: Tue Stories

TECH

Millions Have Been Stolen In Bitcoins After Major Online Marketplace Silk Road Was Hacked

DYLAN LOVE | FEB 14 2014, 1:02 PM | 10

There's not much to see on Silk Road right now:

Silk Road
anonymous market

Silk Road is regrouping for 24-48hrs after suffering a major attack.

Urgent Announcement

The anonymous marketplace for illegal drugs has been hacked. Defcon, a pseudonymous administrator for the site, shares the following details:

> Nobody is in danger, no information has been leaked, and server access was never obtained by the attacker.

Conclusions

- ❑ Despite being or not APTs, attacks evolved over the last **3-4 years**, focusing on the **human factor** when dealing with **targeted espionage**, getting benefits from:
  - Ignorance of the victims (lack of education, basic training, security awareness, simulations);
  - Exposure and visibility on the Social Networks of the companies and its employees;
  - contractors and external suppliers;
  - BYOL (Bring your own device: smartphones, tablets;
  - "remote working";
  - Lack of dialogue and information exchange with other market players (even competitors!);
  - Lack of procedures (approved, ready-to-go, tested) for Incident Handling, **Digital Forensics** e **overall** the "PR Security Management".

- ❑ The "solution"? There is not a panacea which "fixes everything". But, **good sense**, **personnel education** and **being ready** to manage such incidents.
  - ✓ Speaking with the **management, getting the authorizations approved**
  - ✓ Security **Awareness to all of the company's levels**
  - ✓ **Specific trainings** (IT department, software developers, Security department, Blue Team) and **practical simulations** (at least) yearly (2-3 /year=better)
  - ✓ The <u>most important thing</u>: **work along with colleagues** from **different departments**, such as Legal, Human Resources, Marketing, Sales!!

Acknowledgements

- Dr George Li, BSc (Syd), BCom (Syd, Hons. I), PhD (Syd)
- Antonio Guerrero, PG Dip Management, MGSM, MBA (2014), MGSM
  - All the section on Bitcoins

- Fyodor Yarochkin
  - all the section on Underground Currencies

Reading room/1

The Kingpin, Kevin Poulsen, 2012

Fatal System Error: the Hunt for the new Crime Lords who are bringing down the Internet, Joseph Menn, Public Affairs, 2010

Profiling Hackers: the Science of Criminal Profiling as applied to the world of hacking, Raoul Chiesa, Stefania Ducci, Silvio Ciappi, CRC Press/Taylor & Francis Group, 2009

H.P.P. Questionnaires 2005-2010

Stealing the Network: How to 0wn a Continent, (an Identity), **(a Shadow)** (V.A.), Syngress Publishing, 2004, 2006, 2007

Stealing the Network: How to 0wn the Box, (V.A.), Syngress Publishing, 2003

Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier, Suelette Dreyfus, Random House Australia, 1997

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Clifford Stoll, DoubleDay (1989), Pocket (2000)

Masters of Deception: the Gang that Ruled Cyberspace, Michelle Stalalla & Joshua Quinttner, Harpercollins, 1995

Kevin Poulsen, Serial Hacker, Jonathan Littman, Little & Brown, 1997

Takedown, John Markoff and Tsutomu Shimomura, Sperling & Kupfler, (Hyperion Books), 1996

The Fugitive Game: online with Kevin Mitnick, Jonathan Littman, Little & Brown, 1997

The Art of Deception, Kevin D. Mitnick & William L. Simon, Wiley, 2002

The Art of Intrusion, Kevin D. Mitnick & William L. Simon, Wiley, 2004

@ Large: the Strange Case of the World's Biggest Internet Invasion, Charles Mann & David Freedman, Touchstone, 1998

Reading room/2

The Estonia attack: Battling Botnets and online Mobs, Gadi Evron, 2008 (white paper)

Who is "n3td3v"?, by Hacker Factor Solutions, 2006 (white paper)

Mafiaboy: How I cracked the Internet and Why it's still broken, Michael Calce with Craig Silverman, 2008

The Hacker Diaries: Confessions of Teenage Hackers, Dan Verton, McGraw-Hill Osborne Media, 2002

Cyberpunk: Outlaws and Hackers on the Computer Frontier, Katie Hafner, Simon & Schuster, 1995

Cyber Adversary Characterization: auditing the hacker mind, Tom Parker, Syngress, 2004

Inside the SPAM Cartel: trade secrets from the Dark Side, by Spammer X, Syngress, 2004

Hacker Cracker, Ejovu Nuwere with David Chanoff, Harper Collins, 2002

Compendio di criminologia, Ponti G., Raffaello Cortina, 1991

Criminalità da computer, Tiedemann K., in Trattato di criminologia, medicina criminologica e psichiatria forense, vol.X, Il cambiamento delle forme di criminalità e devianza, Ferracuti F. (a cura di), Giuffrè, 1988

United Nations Manual on the Prevention and Control of Computer-related Crime, in International Review of Criminal Policy – Nos. 43 and 44

Criminal Profiling: dall'analisi della scena del delitto al profilo psicologico del criminale, Massimo Picozzi, Angelo Zappalà, McGraw Hill, 2001

Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques, Turvey B., Knowledge Solutions Library, January, 1998

Malicious Hackers: a framework for Analysis and Case Study, Laura J. Kleen, Captain, USAF, US Air Force Institute of Technology

Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology, Täterpro

Contacts, Q&A

- **Need** anything, got **doubts**, wanna **ask me smth**?
  - rc [at] security-brokers [dot] com
  - Pub key: http://www.security-brokers.com/keys/rc_pub.asc

Thanks for your attention!

QUESTIONS?