



The Innovation Group

Innovating business and organizations through ICT



**CYBERSECURITY SUMMIT
2014 – ROMA**

Garantire la sicurezza delle reti e delle infrastrutture
critiche del Paese

Lectio Magistralis

HACKING, CYBERCRIME ED UNDERGROUND ECONOMY

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

20 Maggio 2014, Centro Congressi Roma Fontana di Trevi

Premessa

- L'evoluzione della cosiddetto «mondo hacker sommerso» ha generato **nuovi modelli** di criminalità informatica e **nuovi approcci**.
- Sulla base delle **nostre ricerche** e delle **nostre esperienze sul campo su questo tema**, questa presentazione analizzerà la cosiddetta "**underground economy**", partendo dal mondo del Cybercrime e dei suoi attori.

Agenda

- Presentazioni
- Terminologie
- Cybercrime
 - Attori
 - Scenari
 - Modelli di business
 - Cash-out
- Cyber Espionage
- Conclusioni
- Letture consigliate



Scenari



Scenari + Keywords

Anti-DDoS,
(di base), Sicurezza
delle applicazioni



Cyber Intelligence,
Black Ops



Fattore umano, 0days



SCADA & Sicurezza nei
Sistemi di Automazione
Industriale e IC



Cybercrime Intelligence,
Compliance



Profilo degli insider,
DLP



Basta sognare!

- Per soverchiare i tuoi avversari, **devi conoscere i tuoi nemici!**
 -negli ultimi 10 anni il concetto di «attacker» è **cambiato in modo drammatico.**
 - il concetto di “sistema di sicurezza” non esiste più (IMHO)...in verità **non è mai esistito** 😊
 - **Vulnerabilità** introdotte dai vendor
 - **0days** market
 - Attacchi **sponsorizzati dagli Stati**
 - **DDoS** powershot
 - **Cybercrime & Underground Economy**

Chi sono

- Presidente, Fondatore, **Security Brokers SCpA**
- Direttore Tecnico, **CyberDefcon Ltd.**
- Special Senior Advisor in tema di Cybercrime @ **UNICRI**
(United Nations Interregional Crime & Justice Research Institute)
- PSG Member, **ENISA** (Permanent Stakeholders Group @ European Union Network & Information Security Agency)
- Fondatore, Membro del board e membro del comitato tecnico @ **CLUSIT**
- Steering Committee, **AIP/OPSI**, Privacy & Security Observatory
- Membro, Coordinatore per l'Italia, **APWG.EU**
- Membro del board, **ISECOM**
- Membro del board, **OWASP** Italian Chapter
- **Sostenitore di numerose comunità in tema di sicurezza**



Committed to Wiping Out Internet Scams and Fraud



OWASP

The Open Web Application Security Project



L'azienda

→ Le nostre aree di competenza

Security Brokers ScpA



- Ci occupiamo di argomenti **di nicchia ed interessanti**, forti del know-how frutto di **+20 anni di esperienze** e di **+30 esperti** molto noti negli ambienti dell'**Information Security** e della **Cyber Intelligence** (ma non solo!).
- Le **principali famiglie di servizi** sono riassumibili come segue:
 - **Proactive Security**
 - con forte specializzazione su TLC & Mobile, SCADA & IA, ICN & Trasporti, Space & Air, Social Networks, e-health, [...]
 - **Post-Incident**
 - Attacker's profiling, Digital Forensics (Host, Network, Mobile, GPS, etc..), Trainings
 - **Cybersecurity Strategic Consulting** (Technical, Legal, Compliance, PR, Strategy)
 - On-demand «Ninja Teams»
 - Security Incident PR Handling & Management
 - **Aspetti psicologici, sociali e comportamentali del «Cyber»**
 - **Cybercrime Intelligence**
 - Botnet takeovers, takedowns, Cybercriminals bounting, Cyber Intelligence Reports, interfacciamento con CERTs e LEAs/LEOs,[...]
 - **Information Warfare & Cyber War** (solo per MoD)
 - 0-days brokering – Digital Weapons
 - OSINT

Disclaimer

- Le informazioni contenute in questa presentazione **non violano** alcuna proprietà intellettuale né indicano strumenti e/o informazioni che potrebbero consistere in una violazione delle leggi vigenti .
- I dati statistici presentati **sono di proprietà** del Progetto “Hackers Profiling” promosso da **UNICRI** e **ISECOM**.
- I Marchi citati appartengono ai **proprietari che li hanno registrati**.
- Le opinioni espresse sono quelle dell'autore (i) e oratore(i) e **non riflettono le opinioni** di **UNICRI** o di altri organismi e/o agenzie delle **Nazioni Unite**, né le opinioni di **ENISA** e del suo **PSG** (Permanent Stakeholders Group), né quelle di **Security Brokers**.
- I contenuti di questa presentazione possono essere **citati o riprodotti**, alla sola condizione che **la fonte sia citata**.

→ «What's this all about?»



Le terminologie

→ Prima di iniziare...

- ❑ Nel mondo dell'**InfoSec** abbiamo un *enorme* problema: **la terminologia**.
 - La quale, a sua volta - e già “sporcata”! - ha **interpretazioni** e **logiche** anche molto diverse, in funzione del **settore** in cui la si utilizza ed applica.

- ❑ Come se non bastasse, negli **ultimi anni** è scoppiata la **moda** di anteporre il prefisso “cyber” alla maggior parte dei termini.
 - **Ciò nonostante**, alcuni (grossi) dubbi persistono...persino per i madrelingua!



Ortografia non omogenea...

„Cybersecurity, Cyber-security, Cyber Security ?”

assenza di definizioni condivise...

Cybercrime é...?

Chi sono gli attori?...

Cyber – Crimine/guerra/terrorismo ?

Nei paesi non di lingua Inglese I problemi di comprensione sono aumentati esponenzialmente

Una nota di circostanza

→ Ufo Robot e Mazinga Z 😊

- ❑ In Italia abbiamo “risolto il problema” con il DPCM dello scorso gennaio 2013, dove ci siamo inventati la “sicurezza cibernetica”.
- ❑ Che a me, fa venire in mente davvero tutt’altro!



Picture credits: Daniele Dal Re

Perché?

→ Perché siamo qui?

- **2011**: anno «nero» dell'information leak: **GOVs, MILs, InfoSec, IT Industry**
 - **2012, 2013**: trend di crescita spaventoso (cfr. Rapporti CLUSIT 2012, 2013, 2014)
- Sequenza di incidenti informatici **impressionante**
- **Escalation** oltre ogni previsione
- Violazione di **target prima impensabili**
- **Effetto domino**
- Confini **sempre meno marcati** tra **Cybercrime**, Hacktivism, **Cyber Espionage**, Information Warfare e Cyber War
- Necessità di **rivedere i profili criminali** in questi ambiti
- Necessità di **attribuire il giusto peso alle dinamiche psicologiche** nelle **modalità di attacco**
- Necessità di **fare prevenzione in modo serio**
- Necessità di **gestire l'incidente** laddove accade. **Puntualmente. Professionalmente.**



Perché?

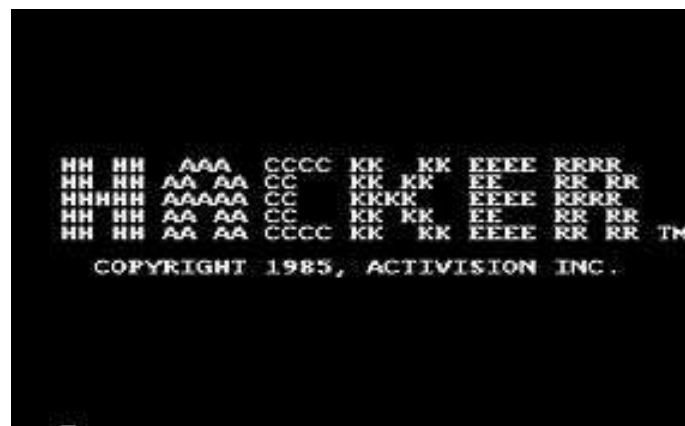
→ Le principali minacce

Sono **tre** le **minacce** principali, in ordine di **frequenza** degli incidenti (ma non di gravità, nel qual caso l'ordine è inverso):

- **Negligenza, errore umano e frodi** realizzati da **Insiders**.
- **Cyber crime transnazionale organizzato**: incassa **15Md \$** all'anno (2012) producendo danni diretti ed indiretti per quasi **400Md \$** a livello globale.
- **Cyber Espionage** e **Cyber Warfare**, da parte di soggetti state-sponsored e di mercenari.

C'era una volta...

- Sono entrato a fare parte del **meraviglioso mondo Hacker nel 1985** .
- Nel **1996**, dopo che l'operazione «trappola di ghiaccio» portò al mio arresto(domiciliari)nel 1995, **sono tornato al mondo "Underground"**.
- I miei amici Hacker mi hanno detto che avevano appena iniziato a fare i "penetration tests".
 - Non avevo idea di che cosa fossero i **WTF**.
 - Poi, ho realizzato che c'erano persone felici di **pagare** per subire **hackeraggio**
 - All'interno di **regole..era legale**.
 - Essere **pagato** per fare quello che **divertiva di più?!? Senza rischi???**
 - «Stai scherzando», LOL 😊



C'era una volta...

- Sempre in **quegli anni**, trovavamo i **bugs** :
 - Sun Solaris (we [still] love you so much)
 - HP/UX (più difficile)
 - VAX/VMS, AXP/OpenVMS (veramente pochi)
 - Linux (molti)
 - etc...
- **Nessuno ci pagava per i risultati dei nostri exploit**. Era divertente.
- Nessuno «**vendeva**» quello che trovavamo.
 - Lo tenevamo per noi, ed **occasionalmente** «scambiavamo» le nostre esperienze con altri hackers (di nostra completa fiducia).

Ai giorni nostri...

- Un **paio di cose** sono successe.
- **Lentamente il denaro è entrato** in questa attività di ricerca.
 - e, tutto il mondo è passato ad essere «always-on», «interconnesso», e **completamente dipendente** dalle IT&TLC.
- Allora, **il Cybercrime** ha visto la luce.
- **Velocemente** il denaro diventa protagonista di questa gara per le” gesta di successo”.

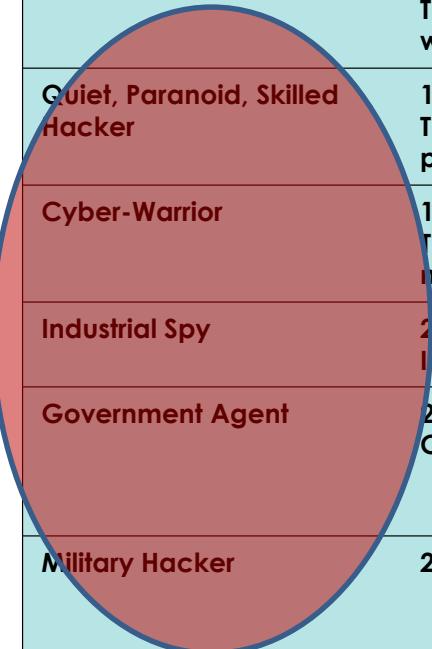
Gli attori?



unieri

advancing security, serving justice,
building peace

OFFENDER ID	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



**e, non sono
solo «hackers»**

Cybercrime

→ perché parliamo di “Cybercrime”?

«Il Cybercrime è il 4° crimine economico»..... da tecnologico è divenuto un problema di business....

**PriceWaterhouseCoopers LLC
Global Economic Crime
Survey 2014**

“2011: il fatturato dell’industria “Cybercrime” è superiore al fatturato dello spaccio di droga, traffico degli esseri umani e di armi!”

Varie fonti(ex. UN, USDOJ, INTERPOL, 2011)

Stima del fatturato 2011: 6-12 BLN USD\$/year

2013: (almeno least) 20BLN USD\$/year



High Tech Criminals

- Market model
- Different roles
- Different knowledge
- Different countries
- Age 20-30
- Well educated
- Low income
- Part timers



Fonte: ABN-AMRO & Dutch National High-Tech Crime Unit

Economical aspects for criminal organizations

Costs:

- Development of the malware on basis of the existing Zeus toolkit \$ 500
- Use of spam botnet \$ 50
- Hosting of command & control center \$ 2.000
- Use of the PC botnet for setting up sessions to Internet Banking \$ 500
- Translators for bank error pages \$ 500
- Cost of money mules in the Netherlands and Ukraine/Russia \$ 10.000

Benefits:

- 23 transactions € 116.000
- Return on investment:

750%

Cosa?

→ Che cos'è il Cybercrime?

❑ Il Cybercrime:

“utilizzo di strumenti informatici e reti di telecomunicazione per l'esecuzione di reati e crimini di diversa natura”.

❑ L'assioma alla base dell'intero modello:

“acquisire diversi insiemi di dati (informazione), tramutabili in denaro.”

❑ Punti salienti:

- **Virtuale** (modello “a piramide” ed anonimato, C&C, flessibili e scalabili, velocità di spostamento e rebuilding, utilizzo “cross” di prodotti e servizi in differenti scenari e modelli di business)
- **Transnazionale**
- Multi-mercato (**acquirenti**)
- **Diversificazione** dei prodotti e dei servizi
- **Bassa** “entry-fee”
- **ROI** (per singola operazione, quindi esponenziale se industrializzato)
- Tax & (cyber)Law **heaven**

Cosa?

→ Cybercrime nel dettaglio

L'esecuzione di crimini, mediante l'ausilio di mezzi informatici e di telecomunicazione, con lo scopo di **acquisire illegalmente informazioni** e di **tramutarle in denaro**.

Esempi:

- **Furto di Identità**
 - Personal Info
- **Furto di Credit Identity**
 - Financial Info: login bancari, CC/CVV, «fullz», etc
- **Hacking**
 - verso e-commerce, e-banking, Credit Processing Centers
- **Industrial Espionage**
- **Malware**
 - Virus, Worm, Spyware, Key Loggers, Rogue AV, Botnets, Mobile
- **Hacking su commissione**
- **Attacchi DDoS**
 - Blackmail, Hacktivism
- **Spam**
- **Counterfeiting**
 - medicinali, luxury, prodotti & servizi
- **Gambling**
 - Riciclaggio di denaro
 - Finti siti e/o non autorizzati (i.e. Italia -> da AAMS)
- **Porno generico**
 - fake sites, etc
- **Pornografia minorile / infantile**

Il crimine, nel passato («crime»)

→ Facciamo un passo indietro

**“Ogni nuova forma di tecnologia,
apre la strada a nuove forme di criminalità”.**

Il rapporto tra **tecnologia e criminalità** è stato, da sempre, caratterizzato da una sorta di “gara” tra buoni e cattivi.

Per esempio, agli inizi del ‘900, con l’avvento dell’**automobile**, i “cattivi” iniziarono a **rubarle**.

....la polizia, per contrastare il fenomeno, definì l’**adozione obbligatoria** delle targhe (car plates)...

....ed i ladri iniziarono a **rubare le targhe** delle auto (o a falsificarle).



Il crimine di oggi («cybercrime»)

→ Dalle automobili alle informazioni

Il concetto di «rapina» è stato sostituito dal furto di informazioni.

Hai l'informazione, hai il potere.

(Quantomeno, nella **politica**, nel **mondo del business**, nelle **relazioni personali...**)

Questo, semplicemente perché l'**informazione è immediatamente trasformabile** in:

- 1. Vantaggio competitivo**
- 2. Informazione sensibile/critica**
- 3. Denaro**
- 4. Ricatto**

Esempi ? (...imbarazzo della scelta ;)

- **Regione Lazio**
- **Calciopoli**
- **Scandalo Telecom Italia/SISMI**
- **Attacco Vodafone Grecia**
- **Vittorio Emanuele di Savoia**
- **Vallettopoli + Scandalo Escorts**
- **Corona**
- **McLaren/Ferrari**
- **Bisignani**

Perché tutto questo sta accadendo?

- Perché gli utenti/utilizzatori sono «stupidi» (o «ingenui», o non eruditi, non consapevoli, etc...) – Videoclip: il «Mago» belga



Money Mules

(da Striscia la Notizia)

→ Money Mules: «very normal people» ?

WANTED BY THE FBI

FEDERAL CYBER CRIME CHARGES



Ilya Karasev



Dmitry Saprunov



Lilian Adam



Marina Oprea



Kristina Izvekova



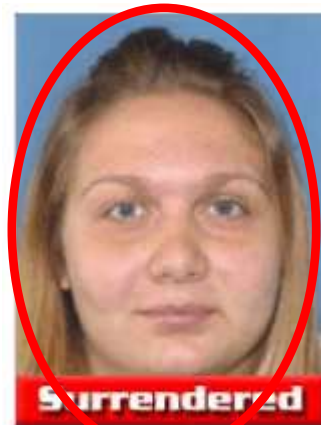
Sofya Dikova



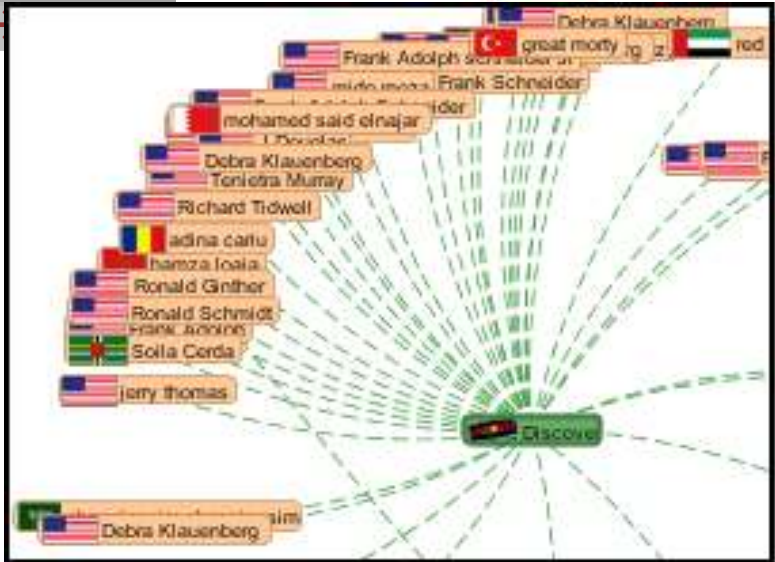
Artem Tsygankov



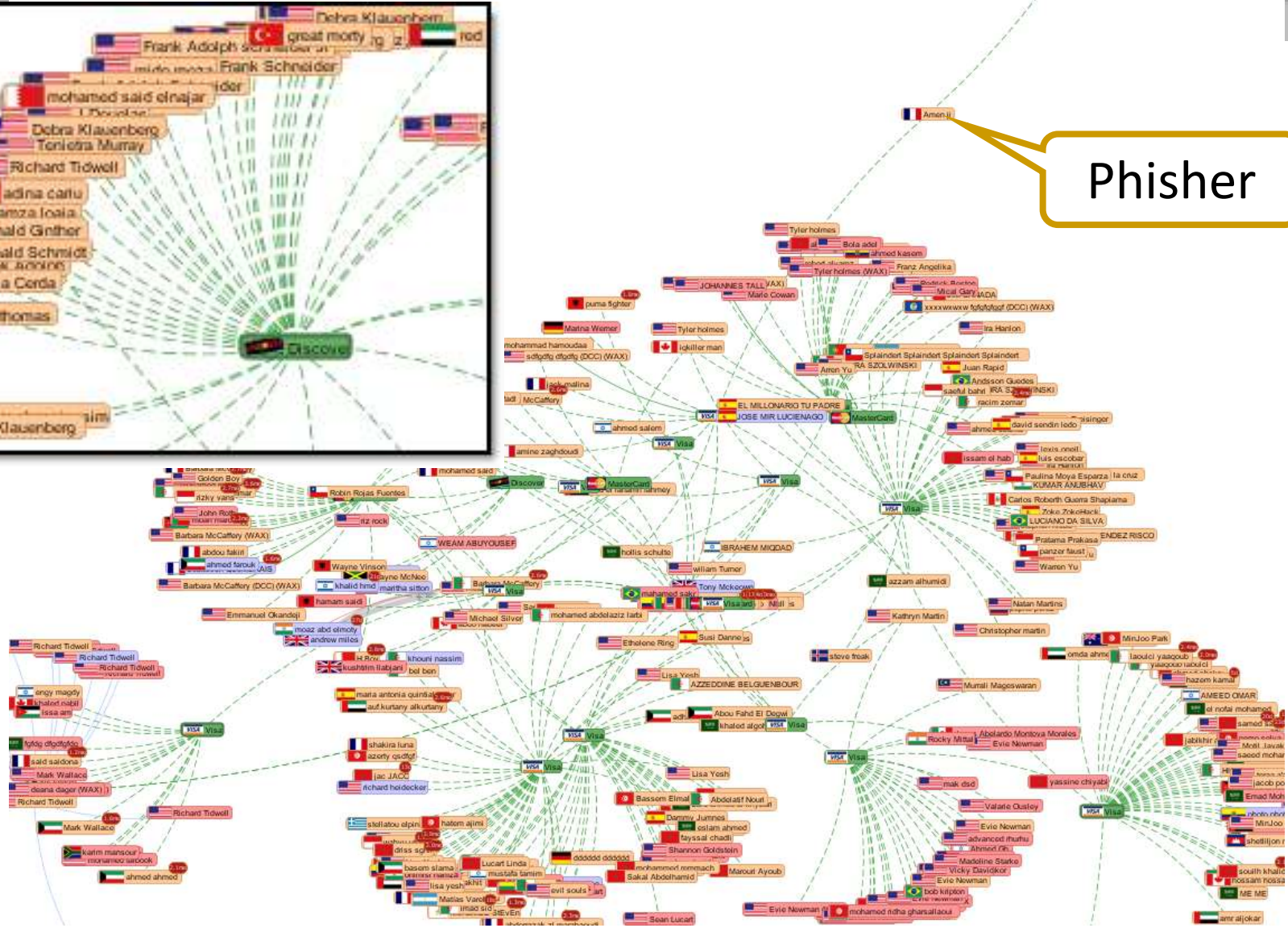
Catalina Cortac



Yulia Klepikova



Phisher



OSINT for Investigations

“Open sources can provide up to 90% of the information needed to meet most U.S. intelligence needs”

-- Deputy Director of National Intelligence, Thomas Fingar

→ Money Mules: «very normal people» ?

WANTED
BY THE FBI

facebook

29

Search

Catalina Cortac's Photos - Back in USA... :)

Photo 66 of 66 · Back to Album · Catalina's Photos · Catalina's Profile



Catalina Cortac



Lilian Adam

→NOT criminal souls: EASY to catch!!!



Criminal Persona

Money Mule



Real Persona

Yulia Klepikova



facebook

Yulia Klepikova

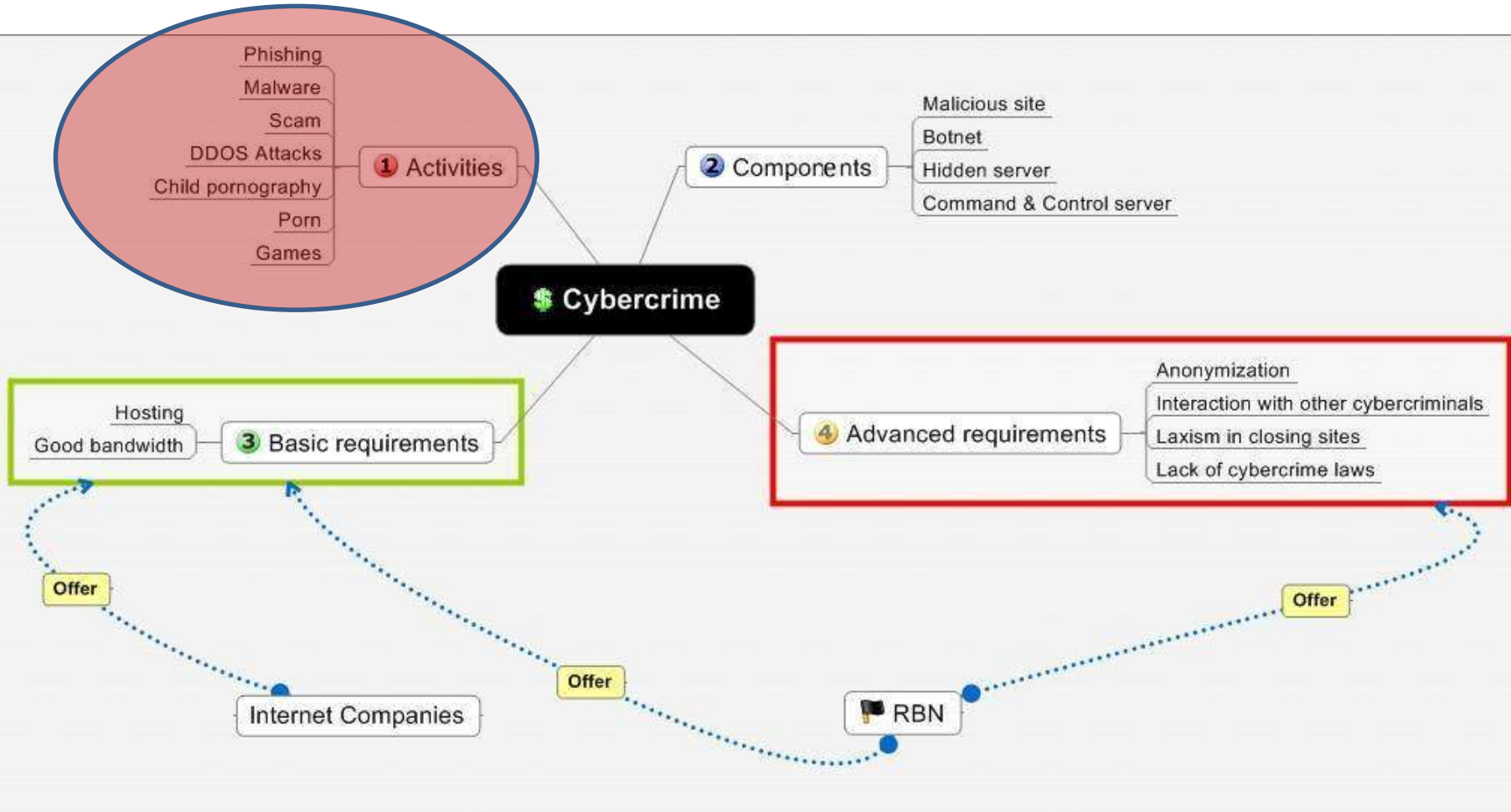
→NOT criminal souls: EASY to catch!!!



- Quando si parla di Underground Economy la nostra mente va a **piccoli criminali** localizzati in paesi dell'est Europa
- Che utilizzano **modelli «casalinghi»**
- Che **nulla hanno a che fare** con il crimine organizzato ed un'**organizzazione complessa**
- **SBAGLIATO**
- Vediamo qualche **esempio...**

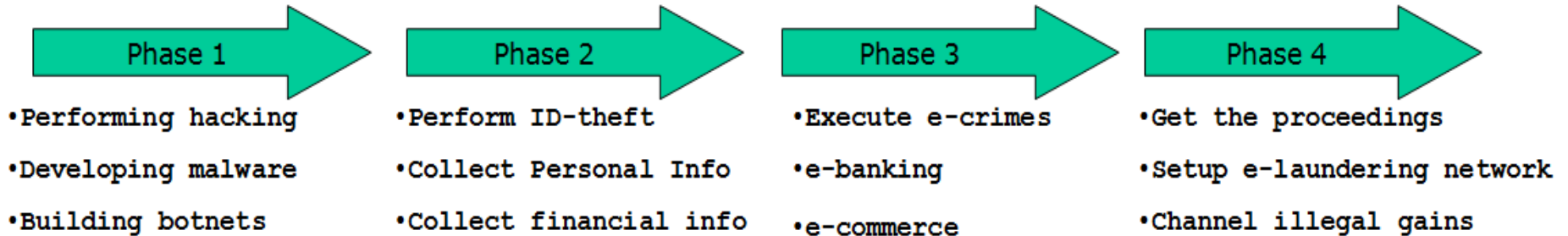
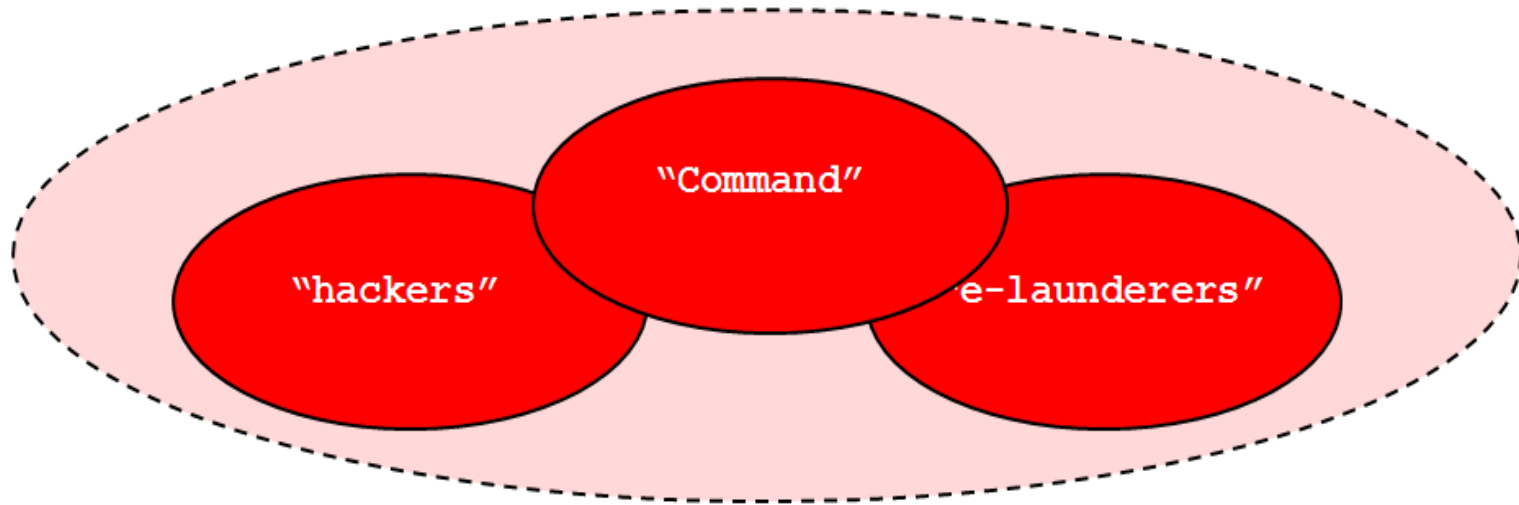
Quando il CO (crimine organizzato) incontra il Cybercrime

→ il «Modello RBN» (Russian Business Network)



Quando il CO (crimine organizzato) incontra il Cybercrime

→ Catena del comando (e fasi operative)

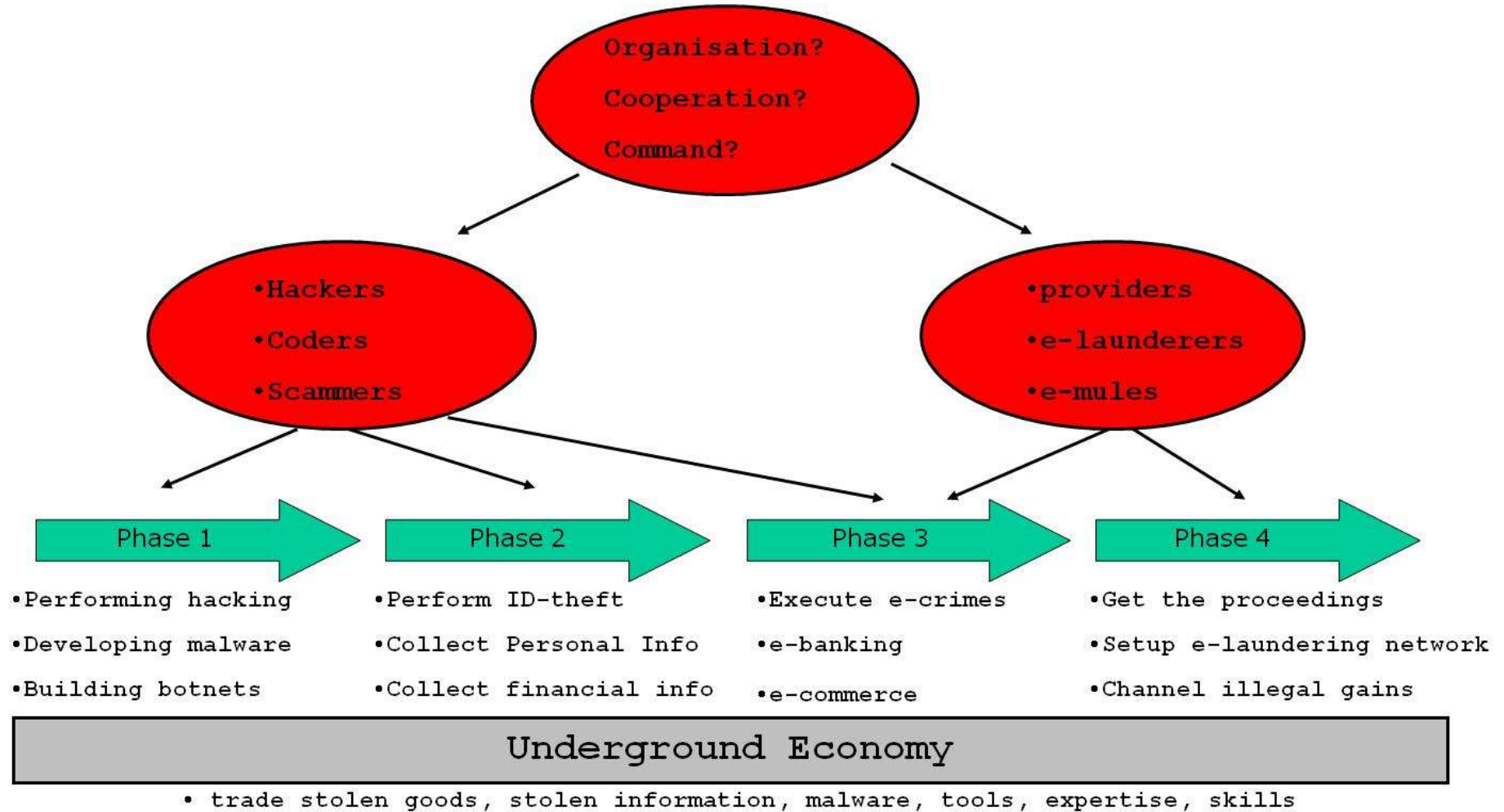


Underground Economy

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

Quando il CO (crimine organizzato) incontra il Cybercrime

→ Approccio basato su «macro unità operative»



→Esempi (veri)

```
=====
FULLZ INFO CC DEMO COMPLETE ACCOUNT INFORMATION:
=====
```

```
cvvmasters bin: -----Personal details-----
FirstName      : Stephen
Last name     : ██████████
Address       : ██████████
Address2      :
City          : Carrollton
Province      : Georgia
Postal code   : 30117
Country       : US
Phone number  : 678-████████
Date of birth : 11dd - mm08- year1982
Social Security Number : 254-██-████
Mothers maiden name : ██████████
Driver license # : ██████████
cvvmasters bin: -----Email details-----
Email          : ██████████@aol.com
Password      : ██████████
cvvmasters bin: -----Credit/Debit details-----
Name on card   : Stephen ██████████
Card number    : 435619 ██████████
Expiration date : 02-2013
CVV2          : ██████████
cvvmasters bin: -----Bank details-----
Bank Name : 435619 Bank of America, N.A. DEBIT PLATINUM USA Charlotte North Carolina NC NEW
Bank Account Number : ██████████
Bank Routing Number : ██████████
```

```
=====
1 TIME CC FREE LIVE DEMO NEW BUYERS ONLY!!
=====
```

```
We GIVE 1 CC Random FOR FREE OR TEST 1 TIME ONLY NEW CUSTOMER...THERE ARE NO MIN ORDER..YOU
```

```
ARE WELCOME TO BUY 1 OR 2 TO TEST!
PAYMENT VIA WU LR WMZ ONLY OR TRADE..
```

```
WHEN YOU READY TO BUY JUST PM US ON YAHOO msg YM: ██████████
or ██████████
```

```
ICQ: ██████████
```

```
Regards,
CvvMASTERS Team
Peace
```

Per certificare la propria credibilità vengono spesso inseriti dai dati di Carte di Credito “Demo”, ossia disponibili all’eventuale acquirente per verificare che il venditore sia in “buona fede”. Questo caso è completo di qualsiasi informazione relativa al possessore della carta (“Fullz”).

→Esempi (veri)

team2010
CVV MASTERS
Global contacts:
ym: [REDACTED]
icq:554 [REDACTED]

----- Cvv MASTERS TEAM IS HERE FRESH LIVE -----

US visa/US master \$2.5 Random
US amex/US discover \$3.5 Random
US FULLINFO CC \$25 DOB SSN MMN only Randon with Bin \$1 extra fee
MIX CC ONLY
UK CC NORMAL \$9 WITH DOB \$19 Randon with Bin \$1 extra fee
EU Visa / Master / Amex \$10
AU Visa / Master \$7
AU amex \$10
CANADA cc \$10
ITALY cc \$11
ASIA cc \$17
We offer 100% Worldwide fresh US,UK EU CCV and fullinfo cc

=====

BANK LOGINS WITH FULLZ

=====

BOA, CITI, CHASE.COM LOGIN
EMAIL+PASS
FULLS COMPLETE
BALANCE: \$5500 verified
PRICE: \$155

=====

BOA, CITI, CHASE.COM LOGIN
EMAIL+PASS
FULLS COMPLETE
BALANCE: \$25000 verified
PRICE: \$525

=====

BOA, CITI, CHASE.COM LOGIN
EMAIL+PASS
FULLS COMPLETE
BALANCE: Randon 1k....>5k
PRICE: \$125

=====

AMEX, AMERICANEXPRESS.COM LOGIN
EMAIL+PASS
FULLS COMPLETE
BALANCE: \$2000 verified
PRICE: \$120

=====

US visa/US master \$2.5 Random

ITALY cc \$17

**BOA, CITI, CHASE.COM LOGIN
EMAIL+PASS
FULLS COMPLETE
BALANCE: \$25000 verified
PRICE: \$525**

→Esempi (veri)



WELCOME TO GLAVMED



Maison | Best-sellers | Tous les produits | FAQ | Contactez-nous



Votre panier: €0.00 (0 articles)
Procédez au contrôle

Canadian Pharmacy
#1 Internet Online Drugstore



Liste de produit

VIAGRA
Pour l'ordre plus de \$300,
12 PILULES DE VIAGRA
LIBERENT
Pour d'autres ordres
4 PILULES



- Meilleures ventes
- la Dysfonction érectile
- l'Amélioration de Sexe Masculin
- Anti-Acidité
- Anti-Allergiques et l'Asthme
- Anti-Androgènes et Anti-Estrogènes

Recherche de nom: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Recherche:

Résultat de la recherche



Yagara
Notre prix: €30.01

[Plus d'information](#)

[acheter](#)



Yashimadhu
Notre prix: €56.91

Viagra + Cialis

€66.50



10 x Viagra
100 mg
10 x Cialis
20 mg

[ORDER NOW](#)

Nous vous suggérons de voir



Viagra
Notre prix: €0.78

→Esempi (veri)



7557.25	0.00	0.00	7557.25
12852.29	0.00	0.00	12852.29
21055.29	0.00	0.00	21055.29
147116.22	-591.97	0.00	146524.25

\$146.000 USD/settimana

→Esempi (veri)



→Esempi (veri)

Antispyware Soft Basic	Antispyware Soft Pro	Antispyware Soft Platinum
		
<u>3 months updates & support</u>	<u>6 months updates & support</u>	<u>Lifetime updates & support</u>
\$49.95 Buy it now	\$59.95 Buy it now	\$69.95 Buy it now
<ul style="list-style-type: none">1. 3 months unlimited support and virus definition base updates2. One computer licence3. Quick scan. <p>Start to protect your computer with Antispyware Soft BASIC Quickly and easily!</p>	<ul style="list-style-type: none">1. 6 months unlimited support and virus definition base updates2. One computer licence3. Advanced Deep Scanning <p>Detect and stop viruses and other potentially unwanted programs before they can compromise desktops and laptops</p>	<ul style="list-style-type: none">1. Lifetime warranty <p>Protect your computer from Trojans, spywares, viruses, hacker attacks, worms, and other malicious software. Now Antispyware Soft Platinum is your security</p>

Recentemente è stato incriminato un gruppo di cybercrooks autori di una campagna di frode con Falsi Antivirus che secondo gli inquirenti ha fruttato circa 100 milioni di dollari.

→Esempi (veri)



→Esempi (veri)



**SLIDE NON PRESENTE NELLA
VERSIONE PUBBLICA**

→ Business globale



**SLIDE NON PRESENTE NELLA
VERSIONE PUBBLICA**

**SLIDE NON PRESENTE NELLA
VERSIONE PUBBLICA**

**SLIDE NON PRESENTE NELLA
VERSIONE PUBBLICA**

**SLIDE NON PRESENTE NELLA
VERSIONE PUBBLICA**

Le differenze

→ Cybercrime ≠ “hackers”

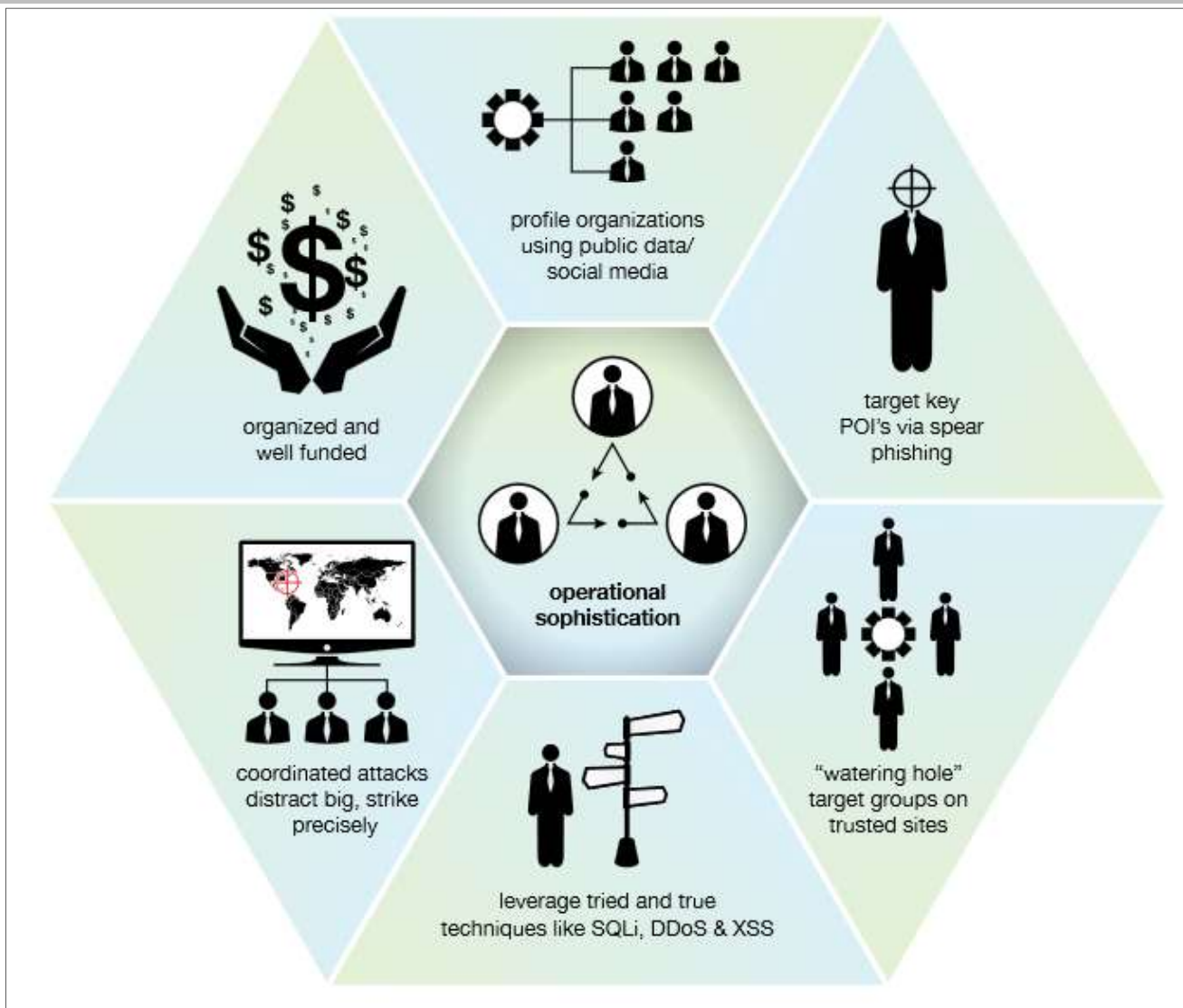
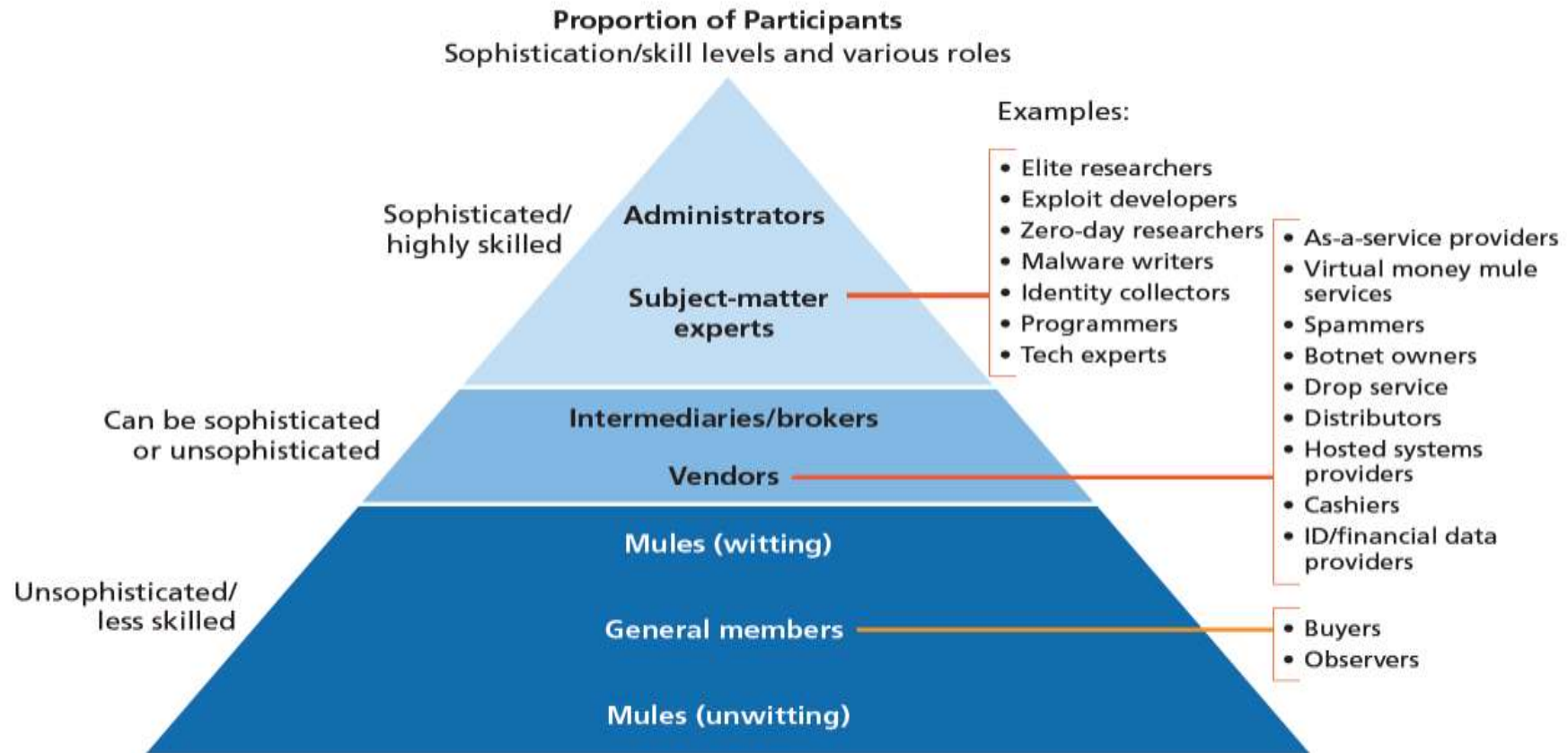


Figure 2.1
Different Levels of Participants in the Underground Market

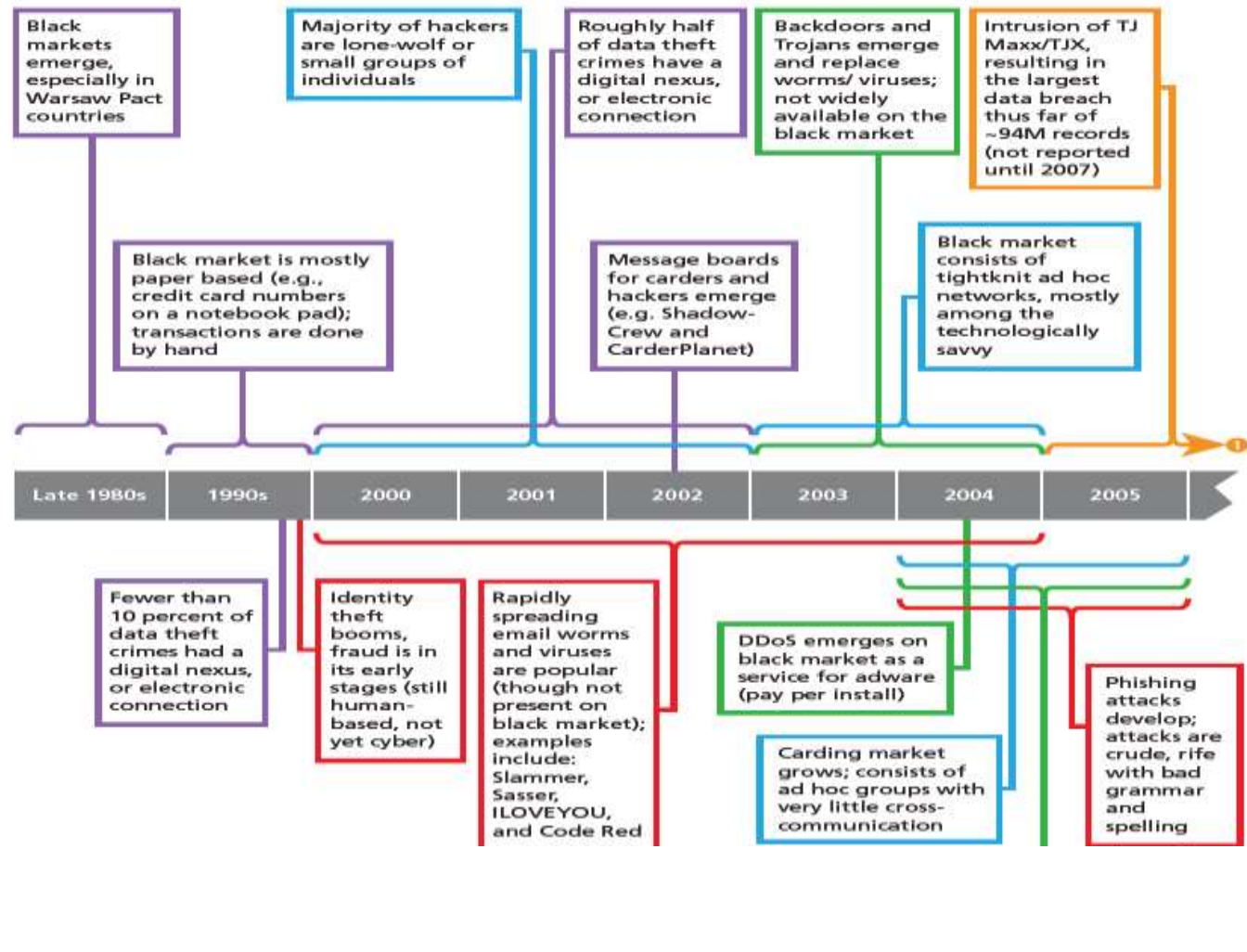


SOURCES: Drawn from interviews; Schipka, 2007; Panda Security, 2011; Fortinet, 2012; BullGuard, undated.
NOTE: Almost any participant can be a ripper; see text for discussion.

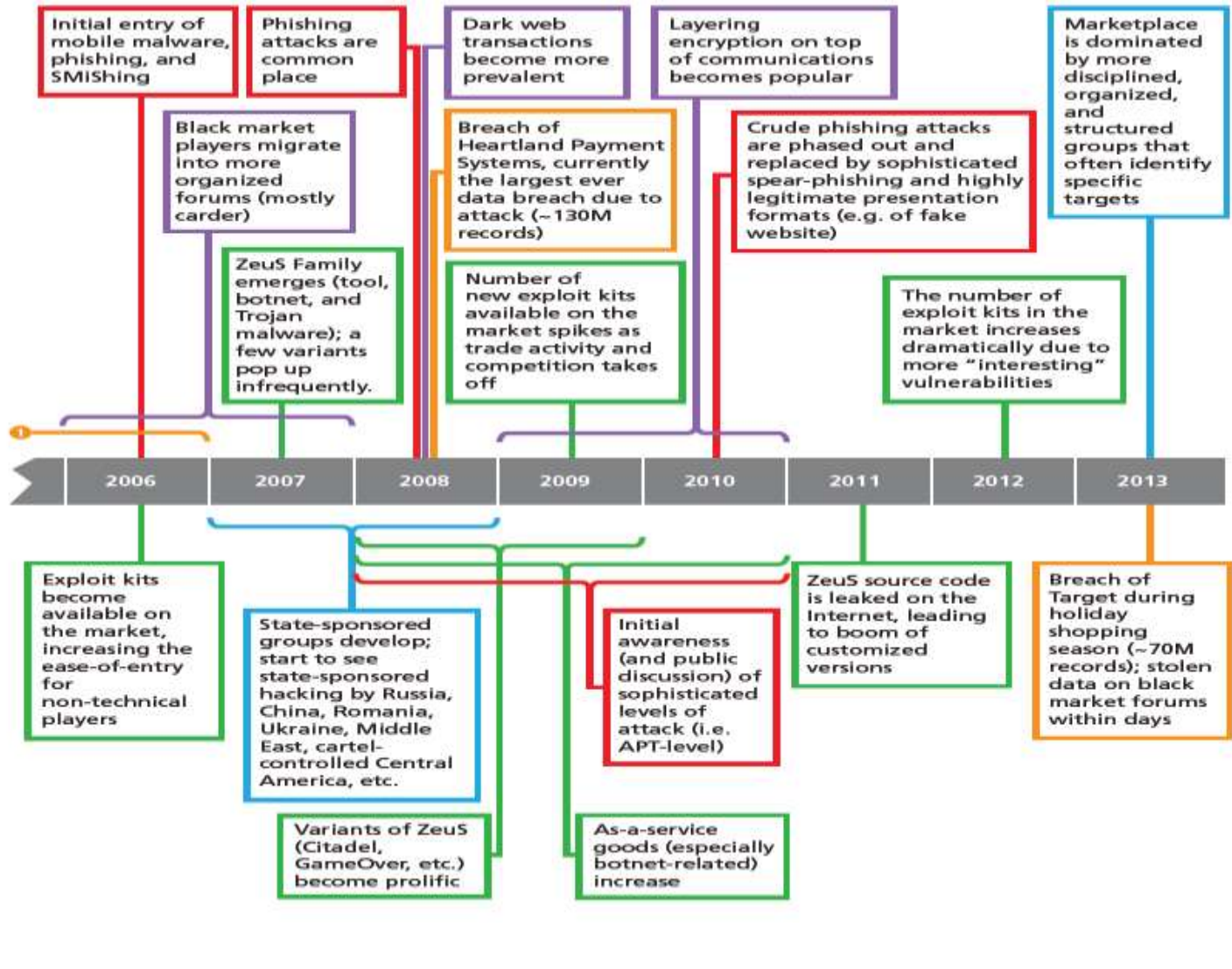
RAND RR610-2.1

...evoluzione del fenomeno fino ai giorni nostri (2013)

Figure 6.1
Black Market Timeline



...evoluzione del fenomeno fino ai giorni nostri (2013)



Videoclip time!



CYBER ESPIONAGE

* *spionaggio*

→ Il Cybercrime

- Parliamo di un ecosistema che è **spesso sottovalutato**: nella maggioranza dei casi è **il punto di partenza o il transito** verso altri ecosistemi:
 - Spionaggio “classico” che utilizza gli skill ed il know-how propri del cybercrime odierno
 - Guerra dell’Informazione
 - Black Ops
 - **Cyber Espionage (industriale, governativo, militare)**
 - Hacktivismo
 - Cyber Milizie (private)
 - Underground Economy e Mercati Neri
 - Crimine organizzato
 - Carders
 - Botnet owners
 - 0days
 - Malware factories (APTs, code-writing outsourcing)
 - Lupi solitari
 - “cyber”-mercenari , Web sommerso, etc

CYBER ESPIONAGE

→ Operation Nitro, Operation Red Dragon

- Lo spionaggio industriale e commerciale ha raggiunto nell'anno 2011 **livelli senza precedenti**.
 - Sono venute alla luce **attività continuative di intelligence ai danni di importanti industrie**, principalmente occidentali, realizzate tramite **sofisticate intrusioni** da parte di team di **specialisti di altissimo livello**.
- Le così dette "Operation Nitro" ed "Operation Night Dragon" hanno interessato **numerose multinazionali del settore chimico, energetico ed oil & gas**.
- Mediante **attacchi mirati** di tipo *spear phishing* gli aggressori hanno preso il controllo dei pc portatili di alcuni dipendenti, potendo in tal modo utilizzare le **legittime connessioni VPN delle vittime** per connettersi in remoto agli applicativi ed ai server aziendali interni, **assumendone il controllo** tramite malware e/o monitorandone le attività.
- Questo genere di attacchi *stealth*, che si **protraggono per mesi** (in alcuni casi anni) prima di essere scoperti, sono particolarmente insidiosi e difficili da evitare, tanto che nessuna organizzazione oggi può dirsi al riparo da essi.

→ Il Cyber Espionage

- ❑ La **complessità** e i **costi** infrastrutturali ed operativi dello spionaggio (in senso ampio) nel corso degli anni sono **scesi drasticamente**, complice (causa) la rivoluzione informatica e la c.d. “Società Digitale”.
- ❑ Nella maggior parte dei casi, l’**informazione** risiede (anche, o solo) su **supporti digitali** e **viaggia in rete**.
- ❑ Un **primo effetto** è il **totale annullamento** del concetto di “furto” (proprio del crimine) e la **conseguente centralità** del concetto di “copia” (proprio del mondo dello spionaggio):
 - ciò che “è sempre lì”, evidentemente “è al sicuro”;
 - aumento del tempo necessario alla scoperta;
 - diminuzione del tempo necessario allo smercio e conseguente cash-out.
- ❑ Purtroppo gli incidenti (pubblici) toccano **sia il mondo civile che quello militare**:
 - insider (motivazioni politiche, etiche, religiose, fama e mass media, corruzione, ricatto, ignoranza);
 - contractor (fornitori esterni, consulenti, accessi VPN e RAS, etc..);
 - “competitor” (civile e militare) sia *State-Sponsored* che *Independent*.

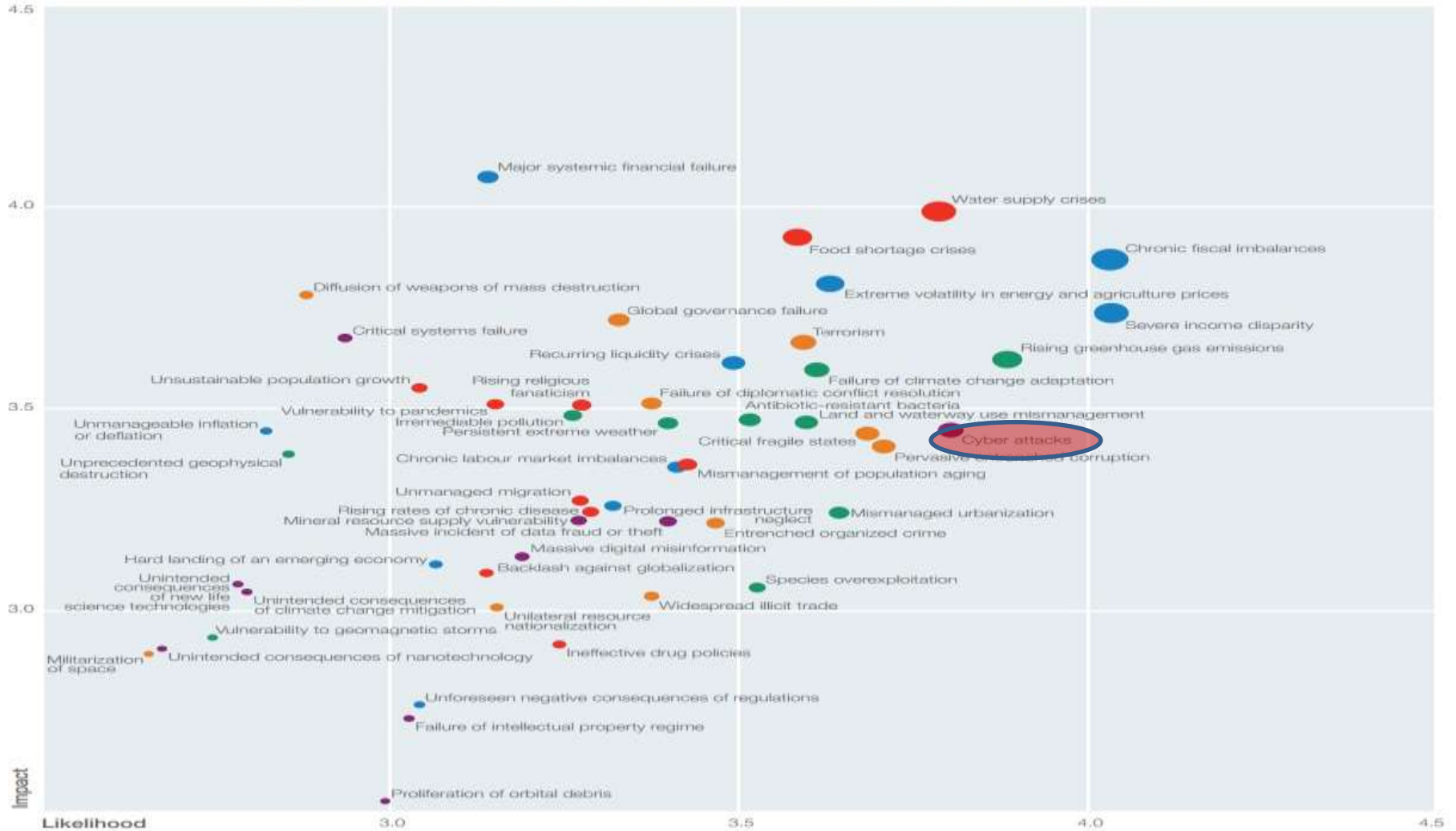
→ RAT e rischi tecnologici dal WEF

Vittima	Attaccante	Tecniche usate
Multinazionali del settore Chimico ed Oil & Gas	Ignoto (Chinese espionage?)	Spear Phishing, Social Engineering, exploit varie vulnerabilità, Malware (RAT)

- I Global Risks Report 2012 e 2013 del World Economic Forum, analizzando le **50 principali minacce globali** e classificandole per **impatto e probabilità**, nella sezione "**Rischi tecnologici**" pone al secondo posto, dopo il cybercrime, la possibilità di *critical system failure*, ovvero di **incidenti ad infrastrutture critiche** in grado di scatenare, per **effetto domino**, **impatti negativi a cascata su tutto il sistema socio-economico**.
- I **sistemi informatici deputati al controllo dell'automazione in ambito industriale** sono una delle principali fonti di rischio in un'ottica di critical system failure: pur essendo pensati per offrire le massime garanzie in termini di continuità e di sicurezza operativa, **storicamente non sono stati progettati tenendo in considerazione la possibilità di attacchi informatici**.

http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf

Figure 2: Global Risks Landscape 2012



Source: World Economic Forum

Figure 38: Technological Risks

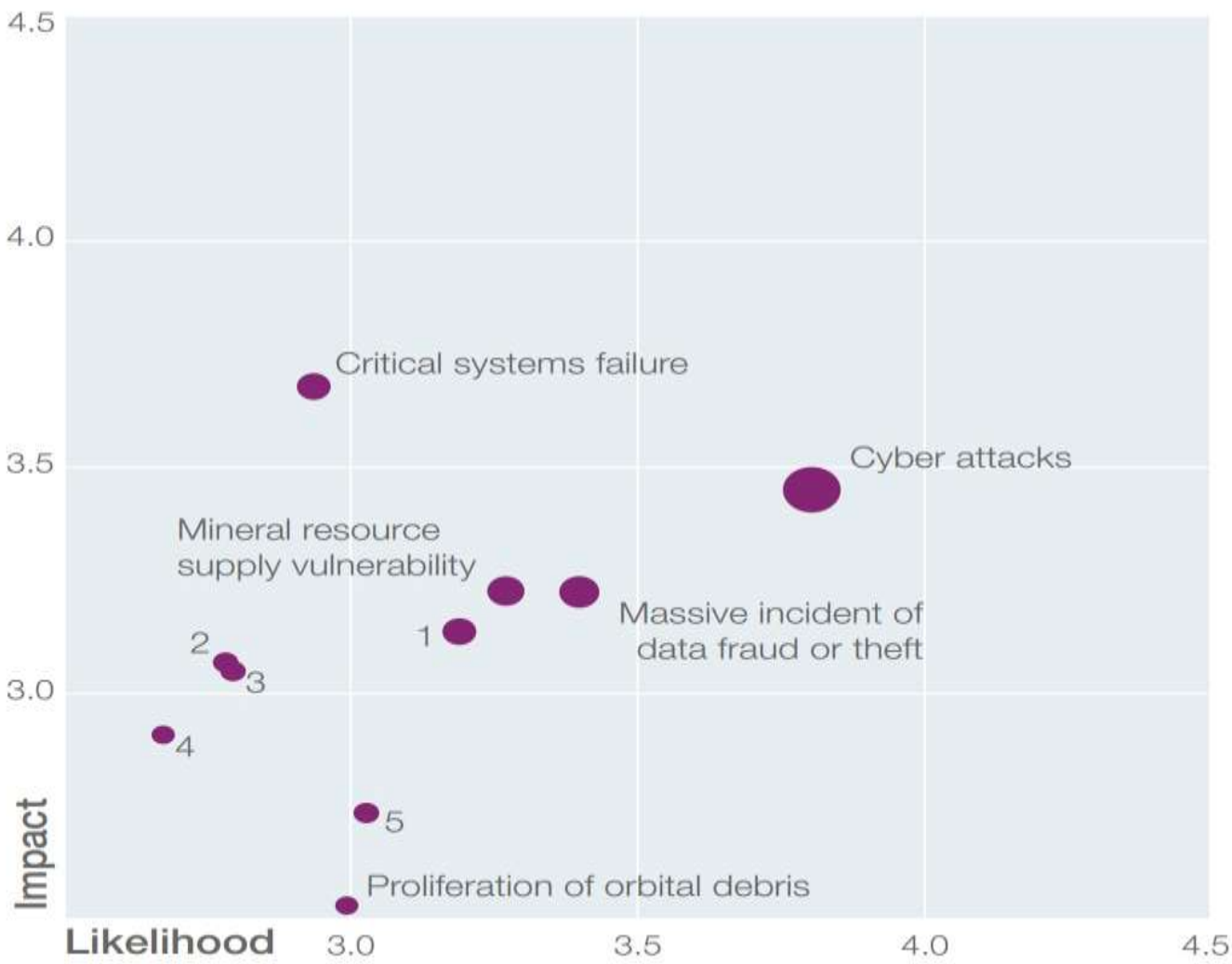
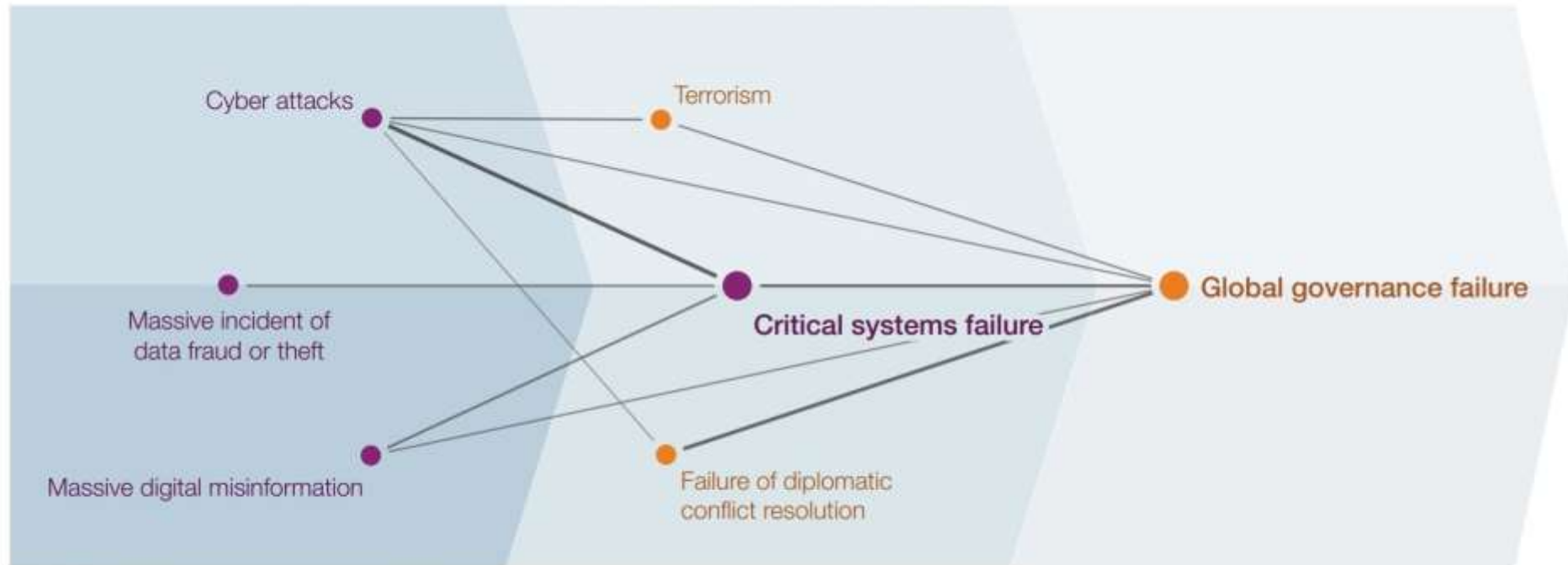


Figure 17: The Dark Side of Connectivity Constellation



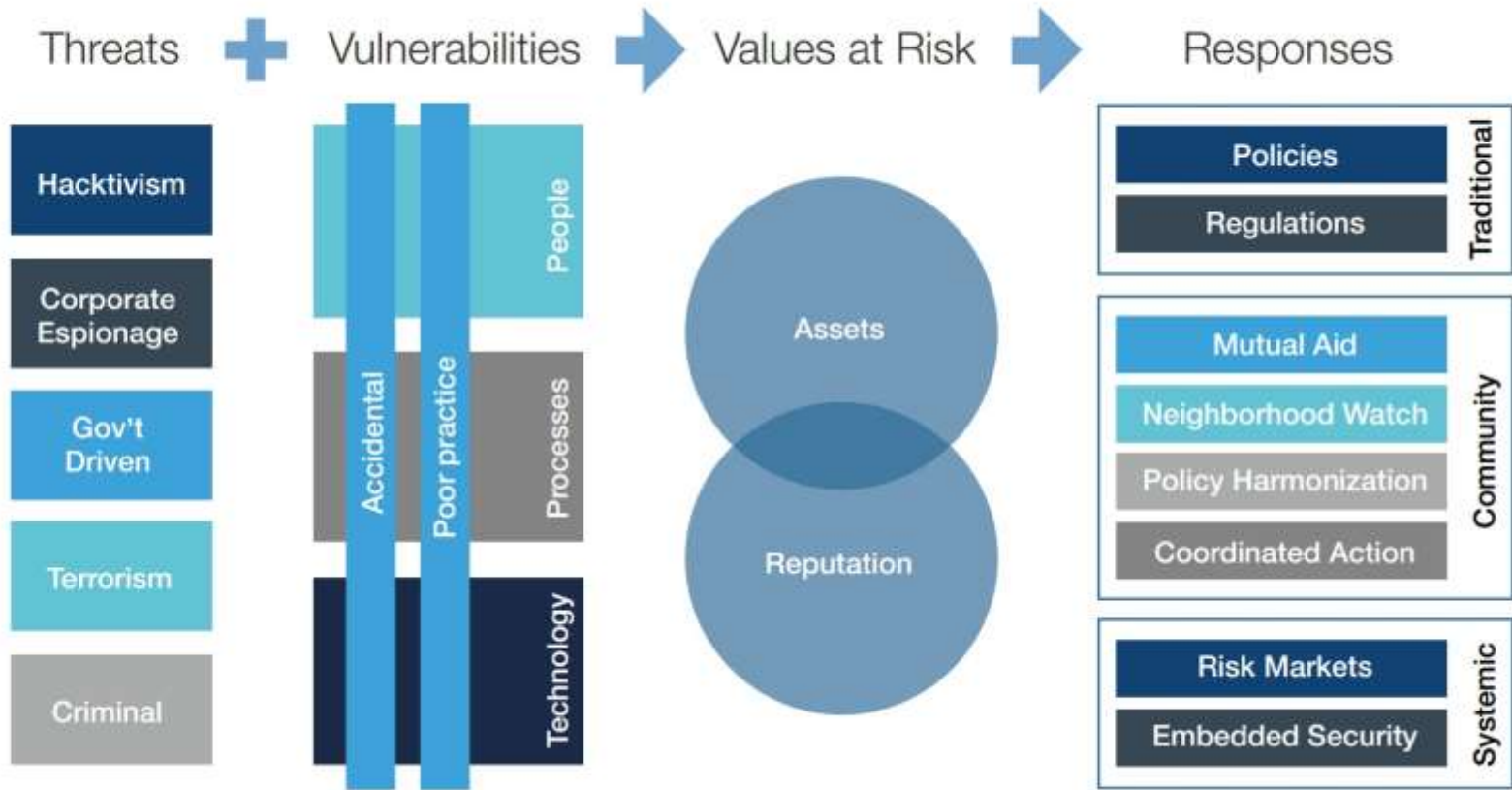
Origin Risk
Increasing capabilities for cyber crime and attacks.

Pathways
Balance-of-power tips as new actors can wage effective interference and disrupt commerce.

Manifestation
The traditional system of global governance is undermined.

Source: World Economic Forum

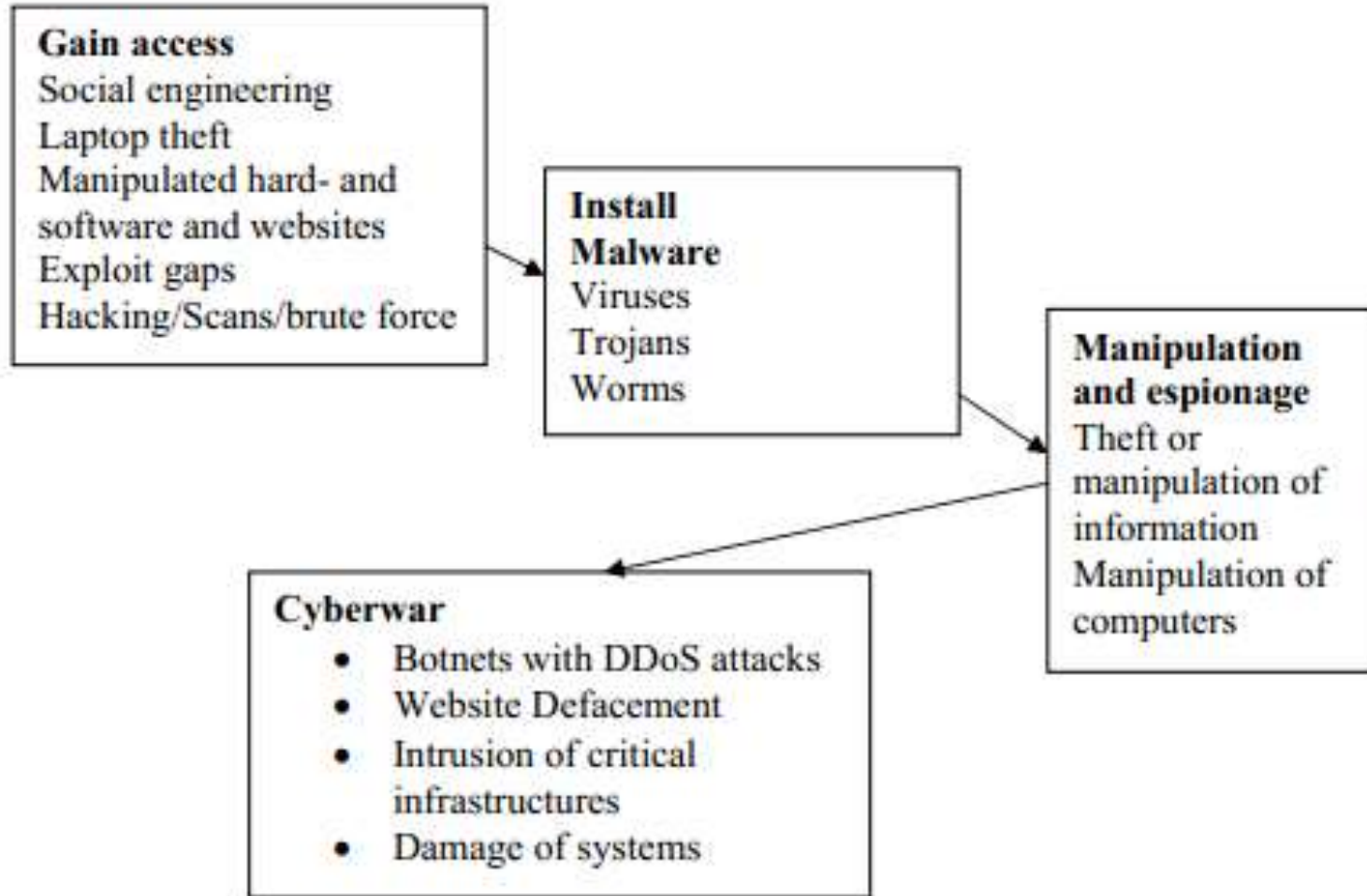
Figure 41: Framework for Cyber Threats and Responses



Source: World Economic Forum

Cyber * (espionage, crime, war)

→ Come possiamo costatare, non ci sono poi così tante differenze con l'appoggio degli hackers

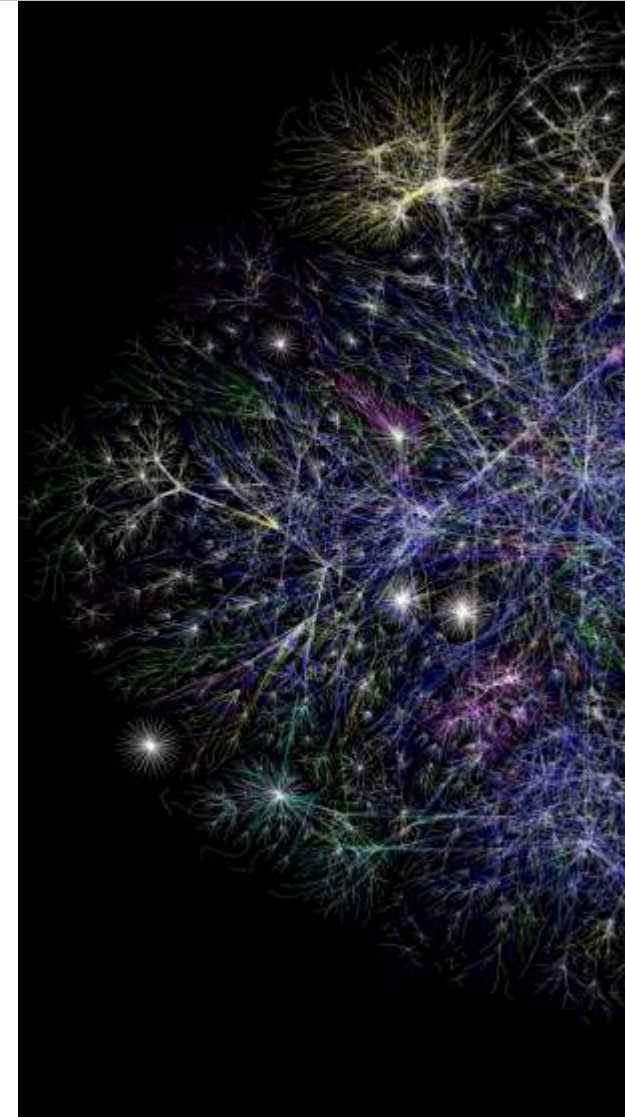


Source: Saalbach «Cyberwar Methods & Practice»

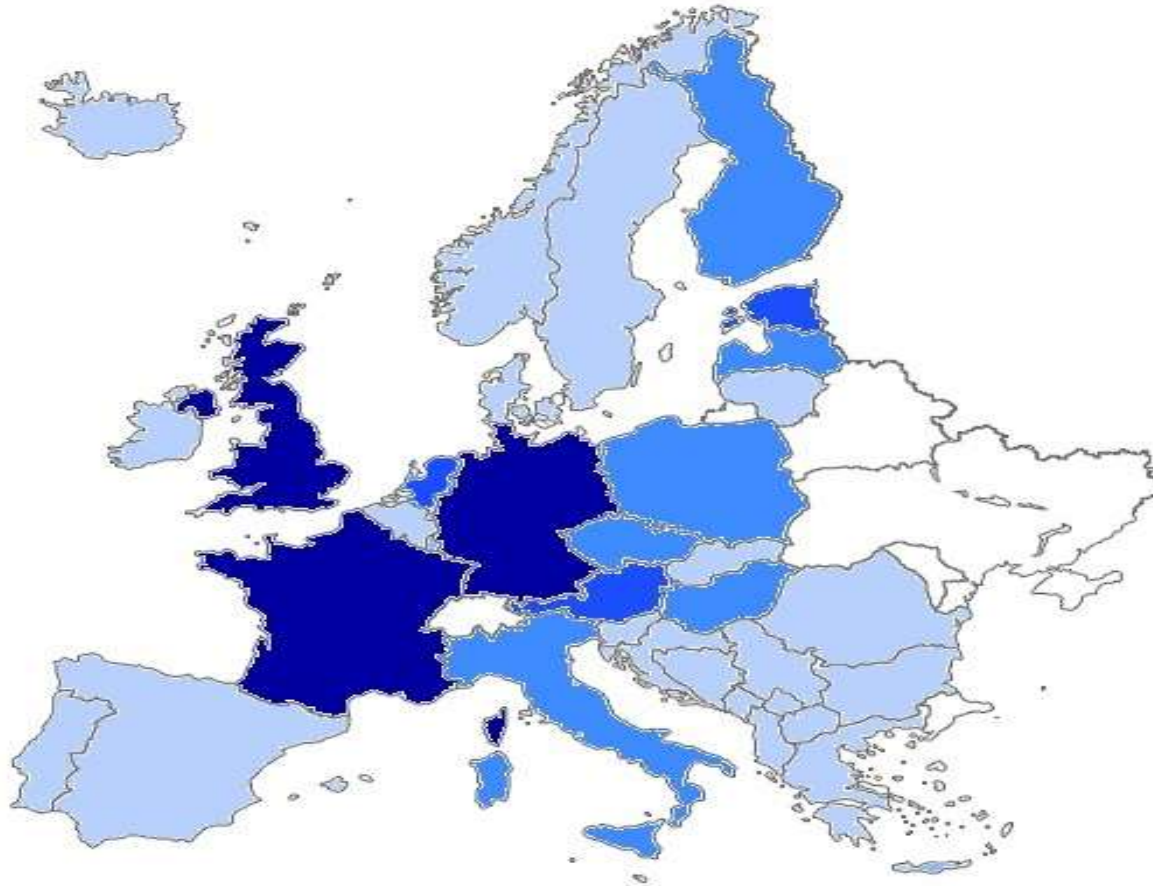
Che cosa sta accadendo?

- **Cybercrime e la guerra dell'informazione** hanno un **ampio spettro di azione e utilizzano tecniche di intrusione** che sono oggi, in qualche modo, a disposizione di una quantità **crescente di attori**, che li utilizzano per **realizzare obiettivi diversi**, con **approcci e intensità che possono variare profondamente**.
- **Quanto sopra è lanciato contro ogni tipo di target:** Infrastrutture Critiche, sistemi di governo , sistemi militari, aziende private di ogni genere, banche, Media, Gruppi di interesse, privati cittadini
 - Stati
 - IC / LEAs
 - Cyber crimine organizzato
 - Hacktivismo
 - Spie industriali
 - Terroristi
 - Corporazioni
 - Cyber Mercenari

Tutti contro tutti



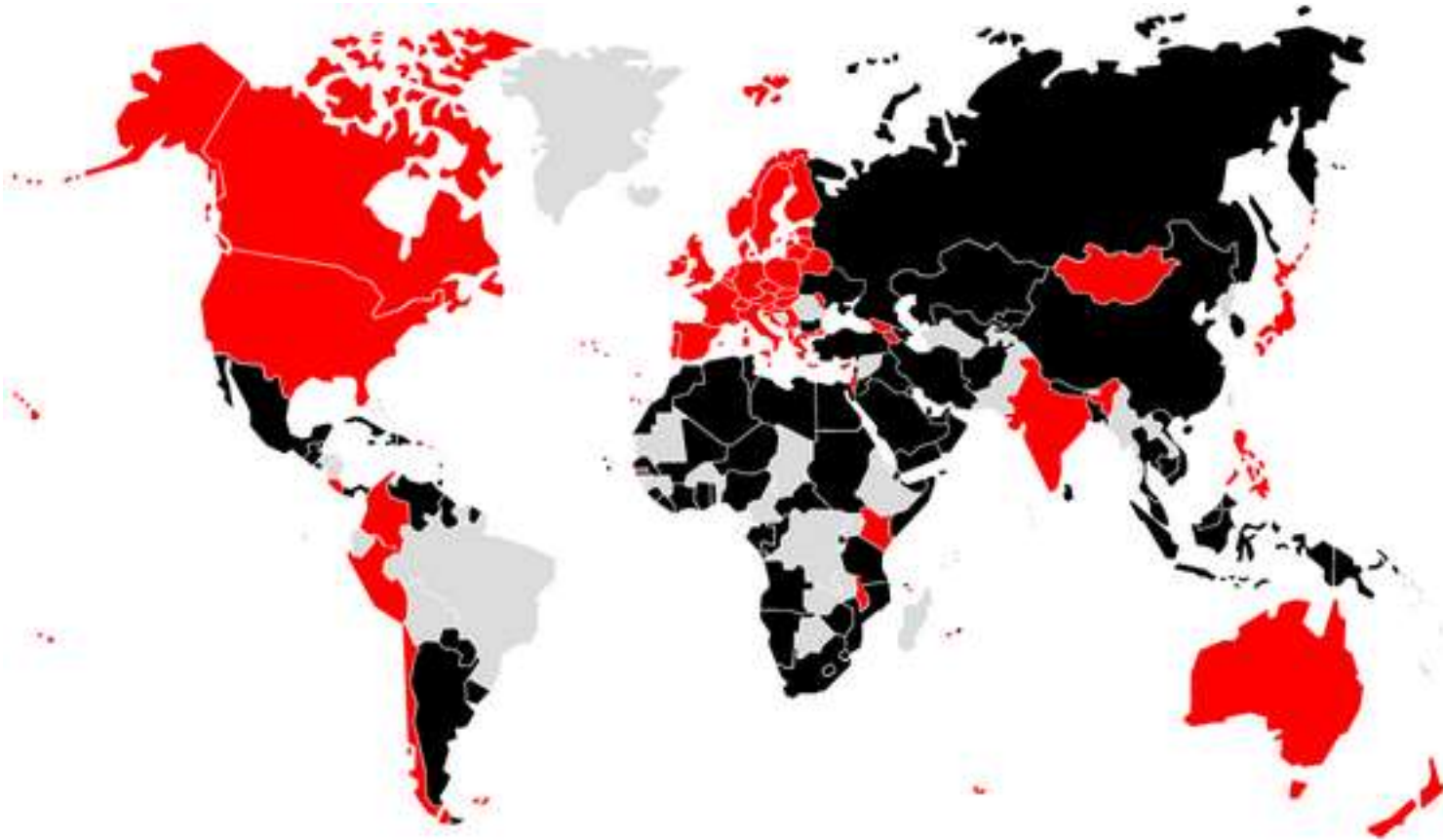
→ Cambiamento Geopolitico: 2013 – Mappa della evoluzioni della Cyber difesa negli stati membri (parziale)



Source: Flavia Zappa,
Security Brokers, 2013

Mondo

→ Cambiamento Geopolitico : 2013 - ITU Dubai Assembleia Generale Dicembre (red=not signed; black=signed)

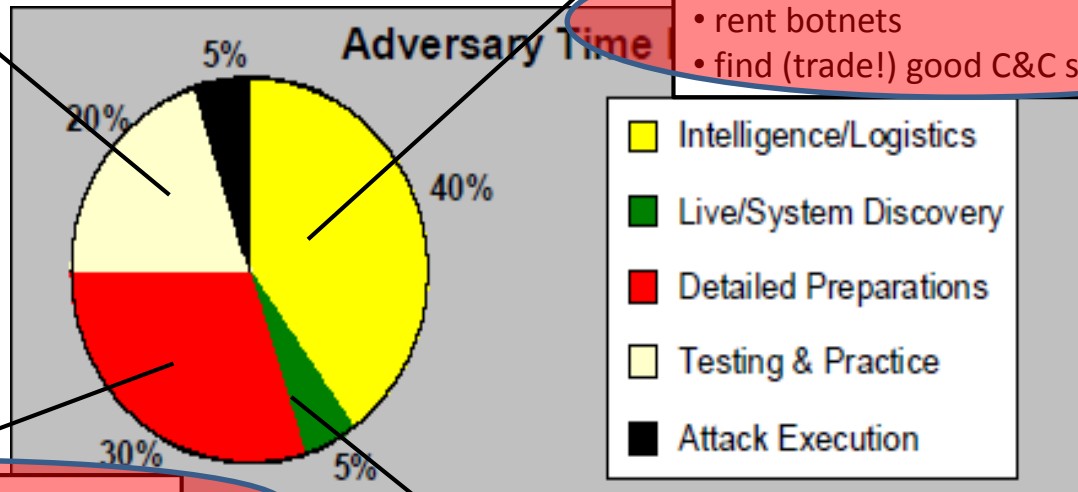


Source: Flavia Zappa,
Security Brokers, 2013

Fare Cyber "qualcosa"...

- 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

La discussione sui prezzi

- Penso vi ricordiate di questo listino:

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>

La discussione sui prezzi

- Che ne dite di questo? (a buon mercato ma «cheap quality», quelli degli indiani)

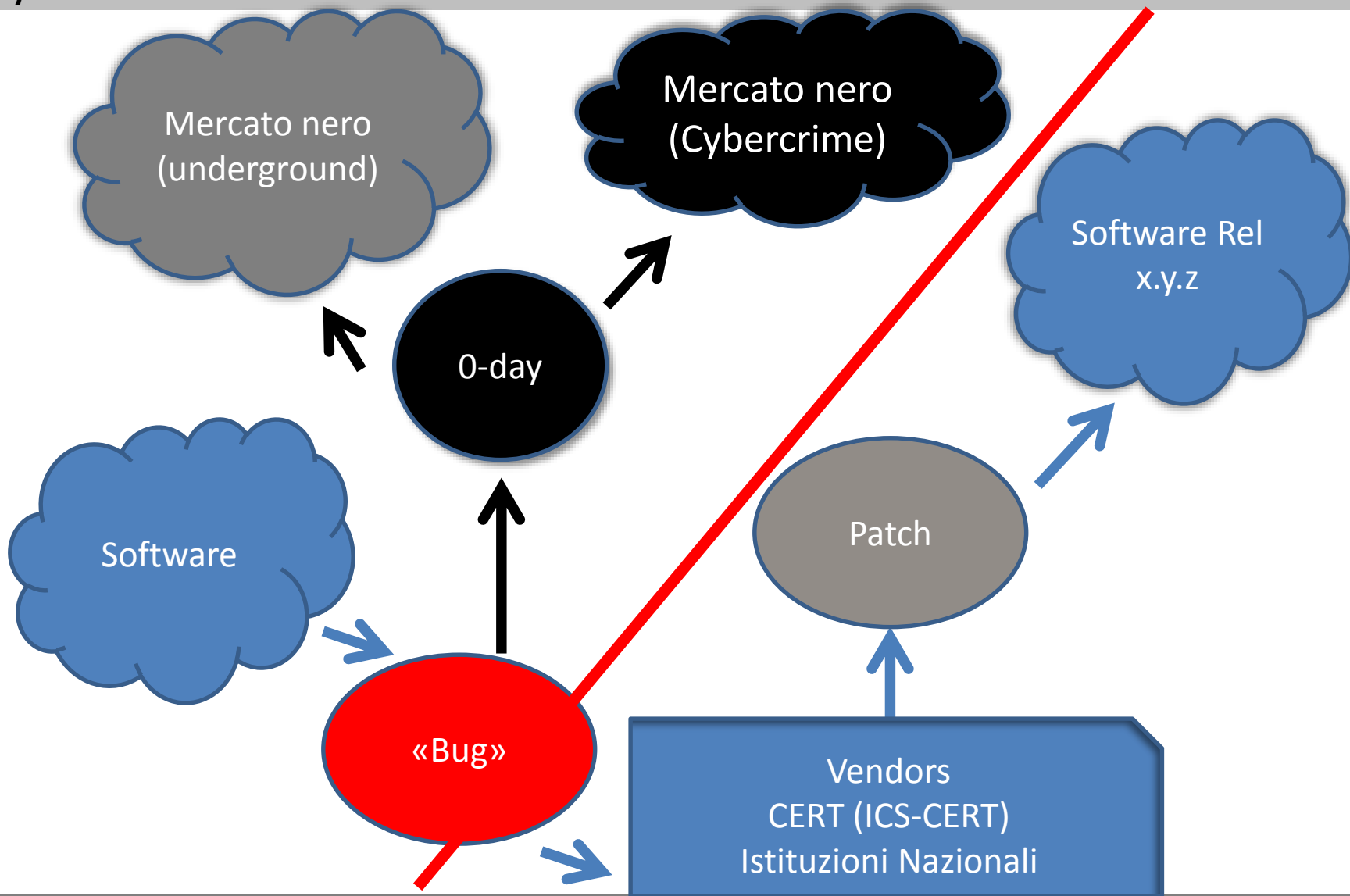
S.No.	EXPLOIT NAME	APPLICATION AFFECTED	OS AFFECTED	DEPENDENCY	Price
1	IE 8	IE 8	Windows Xp x86, Windows Vista x86, Windows 7x86 x64	NA	€ 6.000
2	Mozilla Firefox 3.5.16 Exploit	Mozilla firefox 3.5.16	Windows xp, Vista x86 and Windows 7x86	NA	€ 1.200
3	IE 8.9	IE 8.9	Windows xp, Vista x86 and Windows 7x86	NA	€ 3.600
4	IE 6,7,8	IE 6,7,8	Windows xp, Vista x86, Windows 7x86	JRE 1.6 update 26	€ 2.400
5	XLS_2003-2007 all SPs	Microsoft Office Excel 2003 & 2007	Windows xp, Vista x86/x64, Windows 7x86/x64	NA	€ 6.000
6	PDF_9.4	Adobe reader 9.4	Windows xp sp2 and sp3x86	NA	€ 2.400
7	DOC_2007 all service packs	Microsoft Office word 2007 all SPs	Windows Xp x86, Windows Vista x86, Windows 7x86	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,7x86	NA	€ 3.600
13	PDF_3.3.4	Adobe reader 3.3.4	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 7x86 x64	NA	€ 3.400
15	JRE & JDK	All Major Browsers	Windows Xp x86, Windows Vista x86, Windows 7x86 x64	JRE 1.6 update 27, JRE 1.7	€ 6.000
16	Adobe reader 9.4.0 to 9.4.1 via 7	Adobe reader 9.4.0 to 9.4.1	Windows Xp x86, Windows Vista x86, Windows 7x86 x64	NA	€ 3.500
17	JRE & JDK	All Major Browsers	Windows Xp x86, Windows Vista x86, Windows 7x86 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 7x86 x64	NA	€ 2.400
19	VLC media player 1.1.8	VLC media player 1.1.8	Windows Xp x86, Windows Vista x86, Windows 7x86 x64	NA	€ 3.600
20	MS Powerpoint 2007-2010	MS Powerpoint 2007-2010 all SPs	Windows Xp x86, Windows Vista x86, Windows 7x86 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
23	.chm file exploit	windows xp sp2, sp3	windows xp sp2, sp3	NA	€ 3.600
24	hip file exploit	windows xp sp2, sp3	windows xp sp2, sp3	NA	€ 3.600
25	DOC 2003+2007 all service packs	Microsoft Office word 2003+2007 all SPs	Windows Xp x86, Windows Vista x86, Windows 7x86	NA	€ 6.000
26	DOC 2007+2010 all service packs(Double Click)	Microsoft Office word 2007+2010 all SPs	Windows Xp x86, Windows Vista x86, Windows 7x86	NA	€ 12.000
27	Impage all version(DDay)	Impage all Versions	Windows Xp x86, Windows Vista x86, Windows 7x86	NA	€ 20.000
28	Flash Player	Flash Player < 10.2.154.27	Windows Xp x86, Windows Vista x86, Windows 7x86	NA	€ 2.400
29	Flash Player	Flash Player < 10.3.181.20	Windows Xp x86, Windows Vista x86, Windows 7x86	JRE or MS Office	€ 3.600
30	Flash Player	Flash Player < 10.3.183.5	Windows Xp x86, Windows Vista x86, Windows 7x86	JRE or MS Office	€ 3.600
31	Flash Player	Flash Player < 10.3.183.15 and 11.x < 11.2	Windows Xp x86, Windows Vista x86, Windows 7x86	JRE or MS Office	€ 4.800
32	Flash Player	Flash Player < 10.3.183.15 and 11.x < 11.2	Windows Xp x86, Windows Vista x86, Windows 7x86	JRE or MS Office	€ 4.800
33	Privilege Escalation	Windows Xp x86, Windows Vista x86, Windows 7x86	Windows Xp x86, Windows Vista x86, Windows 7x86	NA	€ 2.400
34	Privilege Escalation	Windows Xp x86, Windows Vista x86, Windows 7x86	Windows Xp x86, Windows Vista x86, Windows 7x86	NA	€ 2.400

Dov'è la verità?

**Qual è l'approccio corretto in
tema di «prezzi»?**

Realtà oltre il mito

→ 0-day Market



Un approccio differente (più serio?)

Conoscenza Pubblica della vulnerabilità	Tipo di acquirente = SI società di sicurezza IT INT = Agenzie di Intelligence per uso governativo (Protezione sicurezza nazionale) MIL = MoD /attori correlait per uso di guerra CO = 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	CO	5K – 80K USD
N	ALL	X2 – X10

Un approccio differente (più serio?)

Conoscenza Pubblica della vulnerabilit	Vulnerabilità risiede su: Sistema Operativo (SO) Le principali applicazioni generali (MGA) SCADA- Automazione industriale (SCADA)	Tipo di acquirente = SI società di sicurezza IT INT = Agenzie di Intelligence per uso governativo (Protezione sicurezza nazionale) MIL = MoD /attori correlait per uso di guerra CO = Cybercrime	0-day Exploit code + PoC Cost: Min/Max
Y	SO	CO	40K – 100K
Y	MGA	INT	100K – 300K
Y	SCADA	MIL	100K – 300K
N	SO	MIL	300K – 600K
N	SCADA	MIL	400K – 1M

ma come vengono pagati i prodotti/servizi di Cybercrime?

- **Contanti (F2F)**
- **Conti bancari Offshore**
- **Valute underground(digitali)**
 - **NOTA: non si tratta solo di Bitcoins!**

Valute "underground"

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

The screenshot shows the website "Magnetic Money" with a dropdown menu open for selecting an exchange point. The menu lists various services and currencies, with "LiqPay (USD)" selected. The main page displays exchange rates for USD and EUR, a search bar for the best rate, and a table of exchange points with columns for "Обменник", "Отда", "Резерв", "BL", and "Отзывы".

Обменники

Обменник	Отда
Speed-Exchange	1 WM
cash4wm	1 WM

Курсы обмена валют ЦБ РФ 25.11.2010

Доллар	USD	↑	31.2929
Евро	EUR	↓	41.9168

Таблица обменных пунктов:

Обменник	Резерв	BL	Отзывы
Speed-Exchange	10.55	-	2 / 0
cash4wm	606.85	1368	5 / 0

Интернет-банкинг:

- Альфа Банк
- Телебанк ВТБ24
- Промсвязьбанк
- Приват 24 (USD)
- Приват 24 (UAH)
- Visa/MasterCard (USD)
- Visa/MasterCard (RUR)
- Visa/MasterCard (UAH)
- Visa/MasterCard (EUR)
- Wire Transfer (RUR)
- Wire Transfer (USD)

Valute "underground"

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

PRIVATE COLLIDER SYSTEM
ONE WAY TO BUY



SSN LOOKUP ONLINE!
PRICE \$4!!!

Checker [Online](#) Accept: [V](#)
[MC](#) [Amex](#) [Discover](#)
 [PYC](#)  [ENG](#)

Collider Menu	COLLIDER INSTRUCTION TO USE	Account
<ul style="list-style-type: none">BUY CCBUY DUMPSCC Order HistoryBUY ACCOUNTSACC ORDER HISTORYAccount checker[Online] SSN LookupsFull CC CheckBatch DUMP/CC ChekingChecker HistoryProxy SocksDOB/MMN USA CaliforniaTicket SystemBillingPayment HistoryPrices	<p>Short Service Description</p> <p>After registration on service you could search for CC you need for free. When you found what you need to buy you should fund your account. To fund it you should enter amount in \$ you need to add to your account and click Pay By WM Button.</p> <p>We have 2 type of DB's in our service and 3 types of Valid rate</p> <p>OWN BASE - our own database (not resellers) AGENT DB - bases of our agents that were given for reselling (resellers)</p> <p>Base Valid Rate Types</p> <p>Good Valid ratio of this db = from 50% * Advantage – lot of cards, countries and bins</p> <p>Fresh Valid ratio of this db = Excellent * Advantage – Excellent valid ratio</p> <p>Deep - bases of our agents that were given for reselling</p>	<p>Account: mirza Balance: 0.00 cr. Properties Log off</p> <p>Payments</p> <p><input type="text" value="25"/></p> <p>WM Temporary OFFLINE. Plea use LR</p> <p>LR Merchant (LR PAYMENT 10% fee) Funding Credits - Manual</p> <p>Calculator</p> <p>1\$ = 5 cr</p>

Conclusioni (full version)

- ❑ Che si parli o meno di «APT», gli attacchi si sono **evoluti** nel corso degli ultimi **3-4 anni**, puntando sul **fattore umano** quando si tratta di **spionaggio mirato**, beneficiando dalla:
 - Ignoranza delle vittime(mancanza di istruzione, di formazione di base , di sensibilizzazione alla sicurezza , simulazioni);
 - Esposizione e visibilità sulle reti sociali delle società e dei suoi dipendenti;
 - appaltatori e fornitori;
 - BYOD (Bring your Own Device: smartphone, tablet);
 - “lavoro a distanza”;
 - La mancanza di dialogo e di scambio d’informazioni con gli altri operatori del mercato (anche con i competitor!);
 - Mancanza di procedure (approvato, ready-to-go, testato) per la gestione degli incidenti,, **Informativa Forense e in generale “PR della gestione della sicurezza”**.
- ❑ La “soluzione”? Non esiste la panacea che risolve tutti i mali. Ma, il buon senso, l’educazione del personale, e l’essere pronti alla gestione di questi incidenti
 - ✓ Parlare con il **management, ottenere che le autorizzazioni siano approvate**
 - ✓ **Sensibilizzazione** al problema sicurezza a **tutti i livelli aziendali**
 - ✓ **Corsi di formazione ad hoc**(Idipartimento IT, sviluppatori software, dipartimento sicurezza, Blue Team) e **simulazioni pratiche**(almeno) annuali (2-3 /anno=ottimale)
 - ✓ **Cruciale: lavorare con i colleghi di differenti dipartimenti**, come ad esempio quello legale, risorse umane , Marketing, Vendite!!

Conclusioni (bignamino)

→ Cosa fare?

Rivedere i propri modelli ed approcci (nuove minacce, nuovi scenari)

- **Gestione del rischio “2.0” e politiche di Gestione Crisi (cyber)**
 - **Applicazioni Web (S-SDLC)**
 - **App aziendali (dati privacy)**
 - **Presenza sui Social Network (politiche di sicurezza)**
 - **Contratti Anti-DDoS (esternalizzare il rischio)**
- **Verifiche di sicurezza (basta “low budget” → low quality!)**
 - **Utilizzo di metodologie di penetration testing e compliance! (OSSTMM ISO/IEC 27001, PCI-DSS, OWASP)**
- **Dialogare (IT, Sicurezza, Comunicazione e Marketing: tutti insieme)**
- **Simulazioni di crisi “cyber” (cosa facciamo se succede che....?)**
- **Procedure e team di Digital Forensics (prima, non “dopo”!)**
- **Cybercrime Intelligence (“sapere, oggi”)**
- **IPv6 (la “nuova internet”)**

Ringraziamenti

- Dr. Roberto Masiero, D.ssa Simona Macellari
 - per il supporto organizzativo

- Fyodor Yarochkin
 - Per la sezione relativa alle valute Underground

Lecture /1

The Kingpin: la storia della più grande rapina digitale del secolo, Kevin Poulsen, 2013, Hoepli

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 Own a Continent, (an Identity), (a Shadow) (V.A.), Syngress Publishing, 2004, 2006, 2007

Stealing the Network: How to Own 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

Lecture /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

Contatti, Q&A

- ...dubbi? Perplexità? Curiosità?

- rc [at] security-brokers [dot] com

- Pub key: http://www.security-brokers.com/keys/rc_pub.asc

Grazie per la vostra attenzione!

Domande?

