Conoscete la vostra Attack Surface? L'importanza dell'Intelligence da fonti aperte per la gestione del rischio nelle organizzazioni.

Raoul Chiesa

Founding Partner, President, Security Brokers SCpA

The Innovation Group

Innovating business and organizations through ICT

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 view of **ENISA** and its **PSG** (Permanent Stakeholders Group), neither **Security Brokers**, its **Associates** and **Associated Companies,** and **Technical Partners**.
- Contents of this presentation **cannot be quoted or reproduced**.

Agenda

- Introductions
- Cybercrime
- Cyber Intelligence (fonti aperte)
- Business Risk Intelligence (BRICA)
- Live demo
- Conclusions
- Leaks…. ☹
- Reading Room!
- Contacts, Q&A

Introductions

Il relatore

- President, Founder, **Security Brokers**
- Principal, **CyberDefcon Ltd.**
- Independent Senior Advisor on Cybercrime @ **UNICRI (United Nations Interregional Crime & Justice Research Institute)**
- Former 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
- Former Member, Co-coordinator of the WG «Cyber World» @ **Italian MoD**
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- Cultural Attachè and BoD Member for **APWG.EU**
- **Supporter at various security communities**

L'azienda

Security Brokers ScpA

- Ci occupiamo di argomenti estremamente interessanti, forti del know-how frutto di **+20 anni di esperienze** e di **+30 esperti** molto noti a livello mondiale 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..), Formazione
  - **Cyber Security Strategic Consulting** (Technical, Legal, Compliance, PR, Strategy)
    - On-demand «Ninja Teams»
    - Security Incident PR Handling & Management
  - **Aspetti psicologici, sociali e comportamentali**
  - **Cyber Intelligence**
    - Cybercrime Intelligence (Banking&Finance, Oil/Gas/Energy, Transportation), Botnet takeovers, takedowns, Cybercriminals bounting, Cyber Intelligence Reports, interfacciamento con CERTs e LEAs/LEOs, servizi di OSINT e di CSINT, OSINT (Open-source Intelligence in ambito aziende pubbliche e private, GOV)
  - **Information Warfare & Cyber War** (solo per MoD / GOV / Agenzie di Intelligence)
    - 0-day ed Exploits – Digital Weapons
    - OSINT (Open-source Intelligence in ambito GOV e MIL)
    - CSINT (Closed-source Intelligence in ambito GOV e MIL)

Problemi di terminologia

No common spelling…

„Cybersecurity, Cyber-security, Cyber Security ?”

No common definitions…

Cybercrime is…?

No clear actors…

Cyber – Crime/war/terrorism ?

No common components?…

❑ Nei Paesi di lingua **non anglofona**, il problema di una corretta comprensione delle terminologie **aumenta**.

«Cyber Intelligence»?

- In linea generale, sono pochi gli addetti del settore "non security" che conoscono il reale significato della **Cyber Intelligence**: c'è "***molta confusione***".

- Innanzitutto, dobbiamo **capire cosa significa** "Intelligence".
  - Nei **Paesi anglossassoni**, il termine significa "informazione".

- La "Cyber Intelligence" quindi non è altro che la **raccolta di informazioni dal mondo Cyber**.

- Queste informazioni si chiamano, in gergo, "**feeds**".

- Principalmente esse provengono da **attente osservazioni** del mondo del **Cybercrime** (ma non solo: **Cyber Espionage rings/gangs**, **Information Warfare**).

«Cyber Intelligence»?

I feeds

❑ La Cyber Intelligence può provenire da **due distinte tipologie di fonti**:

- **Fonti Aperte** (Open Sources), quindi provenienti da attività di tipo **OSINT** (Open Source Intelligence), manuali, automatiche o "ibride" (automatizzate ma con verifiche manuali da parte di analisti)

- **Fonti Chiuse** (Closed Sources), quali l'accesso a portali non pubblici, l'infiltrazione per attività "cyber" sotto copertura, l'intercettazione di dati provenienti da diverse fonti (botnet, C&C, SIGINT, HUMINT, etc.)

- Ogni altra tipologia di fonti (i.e.: logs di Firewall, Antivirus, xIDS, IPS, etc…) **non porta alla Cyber Intelligence nè ai "feeds"**, ma si chiama semplicemente "correlazione di log".
  - Ricordate: i log sono la vostra "**miniera d'oro**"!
  - **DNS logs? CONTROLLATELI!!!!!!!!!!**

Cybercrime

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

PriceWaterhouseCoopers LLC Global Economic Crime Survey 2011

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

Various sources (UN, USDOJ, INTERPOL, 2011)

2014 Financial Turnover, estimation: 15-20 BLN USD$/year

Il crimine di oggi -> Cybercrime

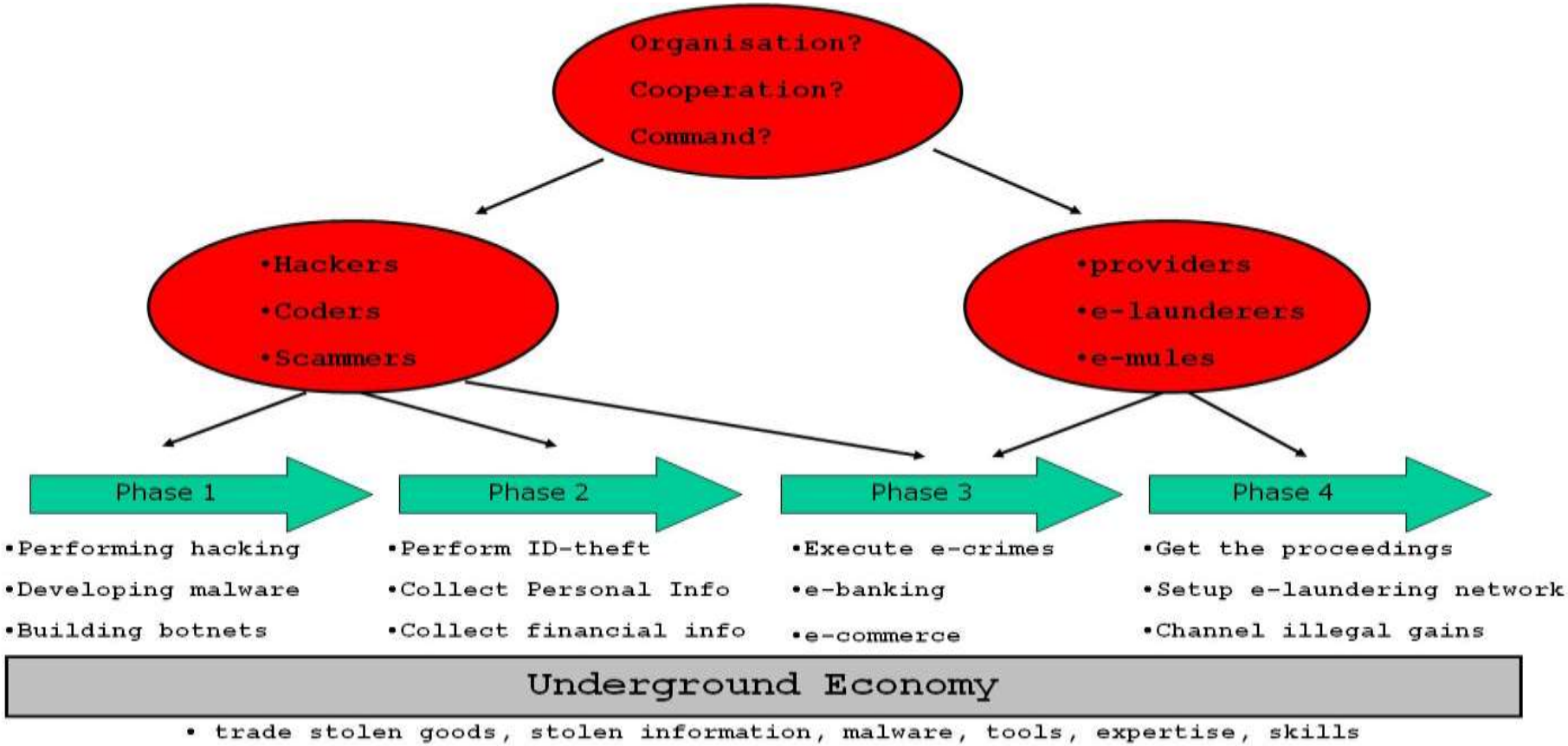
*Hai l'**informazione, information**, hai il **potere**..*

Questo avviene semplicemente perché il concetto di "*informazione*" (che oggigiorno risiede su supporti digitali e viaggia in rete) può essere **immediatamente trasformato** in «qualcos'altro»":

1. **Vantaggio competitivo (geo/politico, business, relazioni personali)**
   Belgacom Hack
2. **Informazione sensibile/critica («blackmailing»/ricatto, estorsione)**
   JP Morgan
3. **Denaro (tecniche di «Cash-out», Black Market & Underground Economy)**
   Cybercrime

- Ecco perché tutti noi vogliamo «essere sicuri".
- Non è un caso se si chiama **Information Security** ☺
  - La **moda** «cyber-prefisso» è d'altr'onde una novità degli **anni recenti**.

Cybercrime: Modus Operandi (MO)



Esempio di digital underground slang (Cybercrime)

- **Carder** - Slang used to describe individuals who use stolen credit card account information to conduct fraudulent transactions.
- **Carding** - Trafficking in and fraudulent use of stolen credit card account information.
- **Cashing** - The act of obtaining money by committing fraud. This act can be committed in a variety of ways: The term can stand for cashing out Western Union wires, Postal money orders and WebMoney; using track data with PINs to obtain cash at ATMs, from PayPal accounts, or setting up a bank account with a fake ID to withdraw cash on a credit card account.
- **CC** - Slang for credit card.
- **Change of Billing (COB or COBs)** - Term used to describe the act of changing the billing address on a credit account to match that of a mail drop. This act allows the carder full takeover capability of the compromised credit card account and increases the probability that the account will not be rejected when being used for Internet transactions.
- **CVV2** - CVV2 stands for credit card security code. Visa, MasterCard, and Discover require this feature. It is a 3 digit number on the back of the card.
- **DDoS** - Acronym for Distributed Denial of Service Attack. The intent when conducting a DDOS attack is to shut down a targeted website, at least for a period of time, by flooding the network with an overflow of traffic.
- **DLs** - A slang term that stands for counterfeit or novelty driver's licenses.
- **Drop** - An intermediary used to disguise the source of a transaction (addresses, phones etc.)
- **Dumps** - Copied payment card information, at least Track 1 data, but usually Track 1 and Track 2 data.
- **Dump checking** - Using specific software or alternatively encoding track data on plastic and using a point of sale terminal to test whether the dump is approved or declined. This provides carders a higher sense of security for obtaining quality dumps fro those who offer them and also a sense of security when doing in store carding.
- **Full info(s)** - Term used to describe obtaining addresses, phone numbers, social security numbers, PIN numbers, credit history reports and so on. Full Info(s) are synonymous with carders who wish to take over the identity of a person or to sell the identity of a person.
- **Holos** - Slang for the word Holograms. Holograms are important for those who make counterfeit plastic credit cards to emulate an existing security feature.
- **ICQ** - An abbreviation for "I Seek You". ICQ is the most widely used instant messaging system for carders. Popular among Eastern Europeans in their Internet culture, it continues to be used for carding activity.
- **IRC** - An abbreviation for "Internet Relay Chat". IRC is a global system of servers through which users can conduct real-time text-based chat, exchange files, and interact in other ways.
- **IDs** - Slang for identification documents. Carders market a variety of IDs, including bills, diplomas, driver's licenses, passports, or anything that can be used as an identity document.
- **MSR (Magnetic Strip Reader**) - Device that can be used for skimming payment card information and/or encoding track information on plastic.
- Phishing - The extraction of information from a target using a hook (usually an e-mail purporting to be from a legitimate company). Phishers spam the Internet with e-mails in hopes of obtaining information that can be used for fraudulent purposes.
- **POS (Point of Sale)** - Acronym for a terminal through which credit cards are swiped in order to communicate with processors who approve or decline transactions.
- **Proxies** - Term used for proxy servers. The use of proxy servers to mask ones identity on the Internet is widely practiced amongst carders. Many vendors sell access to proxy servers, socks, http, https, and VPN (Virtual Private Networks), which aide in hiding the user's actual IP address when committing fraud or other illegal activity on the Internet.
- **Track 1/Track 2 data** - Track 1 and Track 2 data is the information stored on the magnetic stripe of a payment card that contains the account information.

Altri esempi di «slangzzz»

L33T 5P33K

- first use was to play with moderators on BBS'es and that was in age of 1kBd modems
- Very unstable really - live
- present in many languages – even google ;)
- it's not about *gangsta* talk ☺

Altri esempi di «slangzzz»

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
4	6	o	|)	3	]=	6	/-/	1	_|	|X	1	|v|	||	0	|*	(_,)	2	5	7	M	\/	\/\/	%	j	2
/\	8	<	|o	&	ph	&	[-]	!	/	|<	£	em	^/	()	|o	()	12	$	+	|_|	\/	vv	><	`/	~/
@	13	(	∂	€	)	(_+	]-[	|	]	|(	1_	]V[	//\\//	oh	|°	0_	|?	z	-|-	Y3W	\\//	'//	X	`(	%
/-\	I3	(	])	£	|=	9	)-(	eye	¿	h	|	(T)	/\/	[]	|^(o)	<|	/2	5	1	L|		\\'	)(	-/	>_
^	|3	(c)	[)	ë	(=	C-	(-)	3y3	</		|_	[V]	[\]	p	|>	9	I2	ehs	']['	µ		\^/	ecks	'/	5
aye	ß		I>	[-	I=	gee	:-:	ai	(/		lJ	nn	<\>	¤	|"	O,	|^	es	†	[_]		(n)	*	Ψ	7_
∂	P>		|>	|=-		(Y,	|~|	¡	_7		¬	//\\//\\	(\)	Ω	?	(,)	|~			_/		\V/	*	φ	
ci	|:		?			(_-	|-|	][	_)			|\/|	[]\		9	(),	1z			_\		\X/	)(	λ	
λ	!3		T)			cj	]~[	:	¿			/\/\	// []		[]Þ	¶	(r)				/_/		\\|/	ex	Ч	
Z	(3		0				)(	]				(u)	/V		|°		|2				(_)		_|_/		¥	
	/3		ß				?					(V)	¤		|7		[z						\\//\\//			
	)3		c1				)-(					(\/)	[]\[]		q		|`						_:_/			
	]3						#					/|	]\[		þ		12						(/\)			
												^^	~		¶		Я						]I[			
												/|/|			¤		|2						LL1			
												//.			|Þ		.-						UU			
												.\\					¤							Ш		
												/^^\												¶		
												/V\														
												[]\/[]														
												|^^|													

Altri esempi di «slangzzz»

Russian letters

А а	а а	a	a	Р р	р р	r	er
Б б	б б	b	be	С с	с с	s	es
В в	в в	w	we	Т т	т т	t	te
Г г	г г	g, h	ge	У у	у у	u	u
Д д	д д	d	de	Ф ф	ф ф	f	ef, fe (pot.)
Е е	е е	je, ie, e	je	Х х	х х	ch	cha
Ё ё	ё ё	jo, io	jo	Ц ц	ц ц	c	ce
Ж ж	ж ж	ż	że	Ч ч	ч ч	czi	czie
З з	з з	z	ze	Ш ш	ш ш	sz	sza
И и	и и	i, y	i	Щ щ	щ щ	ść	ścia
Й й	й й	j	j, i krátkoje	Ъ ъ	ъ ъ	-	twiórdyj znak, jer
К к	к к	k	ka	Ы ы	ы ы	y	y
Л л	л л	ł	el'	Ь ь	ь ь	-	mjákkij znak, jer'
М м	м м	m	em	Э э	э э	e	e abarótnoje
Н н	н н	n	en	Ю ю	ю ю	ju, iu	ju
О о	о о	o, -a	o	Я я	я я	ja, ia, i	ja
П п	п п	p	pe				

Altri esempi di «slangzzz»

Examples :

- KoHTpbl Hy6bl
- Y %username% 4utbl 100 o\o, AgmuH 3a6aHb ero
- Admin cmeHu map, 3ae6aJIo
- odd noobs
- User … cheats I 100%, admin ban him
- Admin change tar, I lost it

Altri esempi di «slangzzz»

Number code introduction

- 1 = 要 to want
- 2 = 爱 to love
- 3 = 想 to miss or to want
- 4 = 死 to die *(bad luck)*
- 5 = 我 I, me
- 7 = 亲 to kiss
- 8 = 發 prosperity (good luck)
- 0 = 你 you
- Examples:
  - 514 = 我要死 I want to die
  - 56 = 无聊 bored
  - 5366 = 我想聊聊 I want to chat
  - 282 = 饿不饿 hungry?
  - 555 = 呜呜呜 refers to: the sound of crying
  - 520 = 我爱你 I love you → Chinese Valentine Day is May 20th ☺
    - And what 520-2 means?

!!! 3Q = thanks (San-Q)

Conoscere la vostra Attack Surface

Il concetto di «Attack Surface»

- La «Attack Surface» è l'insieme degli **entry points** e delle **esposizioni** che **possono portare alla violazione** dei **sistemi pubblici** e **privati** di un'organizzazione.

- Esempi:
  - Siti web
  - Sistemi di Posta Elettronica
  - Concentratori VPN
  - Dipendenti e loro presenza sui Social
  - Mobile devices
  - ISP
  - Legacy networks (PSTN, X.25, etc…)
  - Cloud
  - Fornitori, Partner
  - Documentazione sensibile (P2P…mai cercato?)
  - ……

What Do These All Have In Common?

What Did They All Have In Common?

They Didn't Even Have a Clue What Hit Them

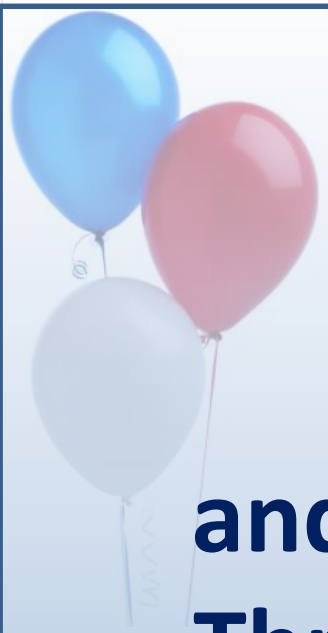
Despite Each Having Spent Millions on All The "Best" Security Products, Software & Consultants

Why Not?

Because They Didn't Know What They Didn't Know

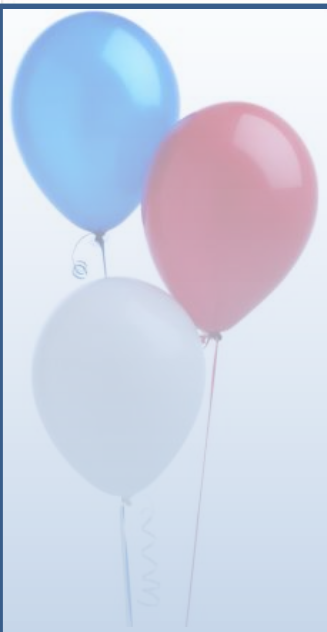
Because a Hacker only needs to Detect a Single Weak Spot where to stick the needle in.

Where You Need to Be Aware 24x7 of EVERY New possible Spot a Hacker May possibly Stick A Needle ANYWHERE in YOUR Organization ANYTIME.



So, to be able to Prevent, you need to:

Know Your Attack Surface and be Timely Alerted on Relevant Threats and Risks, Well Ahead of a Possible Attack



Business Risk Intelligence

BRI

Cyber threat Awareness

- **Know Your Attack Surface**
- **Know In Time of Attacks That MAY Happen**
- **Pro-Actively Defend Your Attack Surface**
- **Create A Cyber Security Awareness Culture**

Turning Harvested Risk Data into Actionable Intelligence

Fore-Warned is Fore-Armed

To locate and alert on **anything** that may be a risk or threat to an organization.

- **Teams of Risk Analysts**
- **Search Engines**
- **Security Networks**
- **Informal Networks**
- **Dark Sources**

- **Generic**
- **Organization Specific**

Different Crops Require Different Harvesting Methods









Some need to be harvested by hand

BRICA, 13.11 del 20 Maggio 2015

Technology

- Adobe Acrobat Reader app.Monitors().select nonDocument Javascript API Restrictions Bypass Vulnerability (ZDI-15-203)
  4 minutes ago
- TLS Protocol Flawed, HTTPS Connections Susceptible to FREAK-like Attack
  21 minutes ago
- Adobe Acrobat Reader app.Monitors select Javascript API Restrictions Bypass Vulnerability (ZDI-15-202)
  22 minutes ago
- Adobe Acrobat Reader DynamicAnnotStore enumerate Javascript API Restrictions Bypass Vulnerability (ZDI-15-201)
  24 minutes ago
- Security Advisory - Two Privilege Escalation Vulnerabilities in Huawei Mate 7 Smartphones (Huawei-SA-20150520-01-MATE7)
  34 minutes ago
- Mageia Updated phpmyadmin

Industry

- Cruise Ship from Boston Runs Aground in Bermuda
  17 minutes ago
- HEADS UP - Hackers Steal Bettys Customer Database
  23 minutes ago
- Retailers take 197 Days on Average to Identify Security Breaches
  35 minutes ago
- Tech firms send letter to Obama: no security back doors
  52 minutes ago
- Cyber attacks a growing threat for US financial system
  53 minutes ago
- HEADS UP - Airbus warns of software bug in A400M transport planes
  1 hour, 5 minutes ago
- We caught Chinese technology spies RED-HANDED claims US government
  1 hour, 18 minutes ago
- Please no non-consensual BACKDOOR SNIFFING, Mr Obama

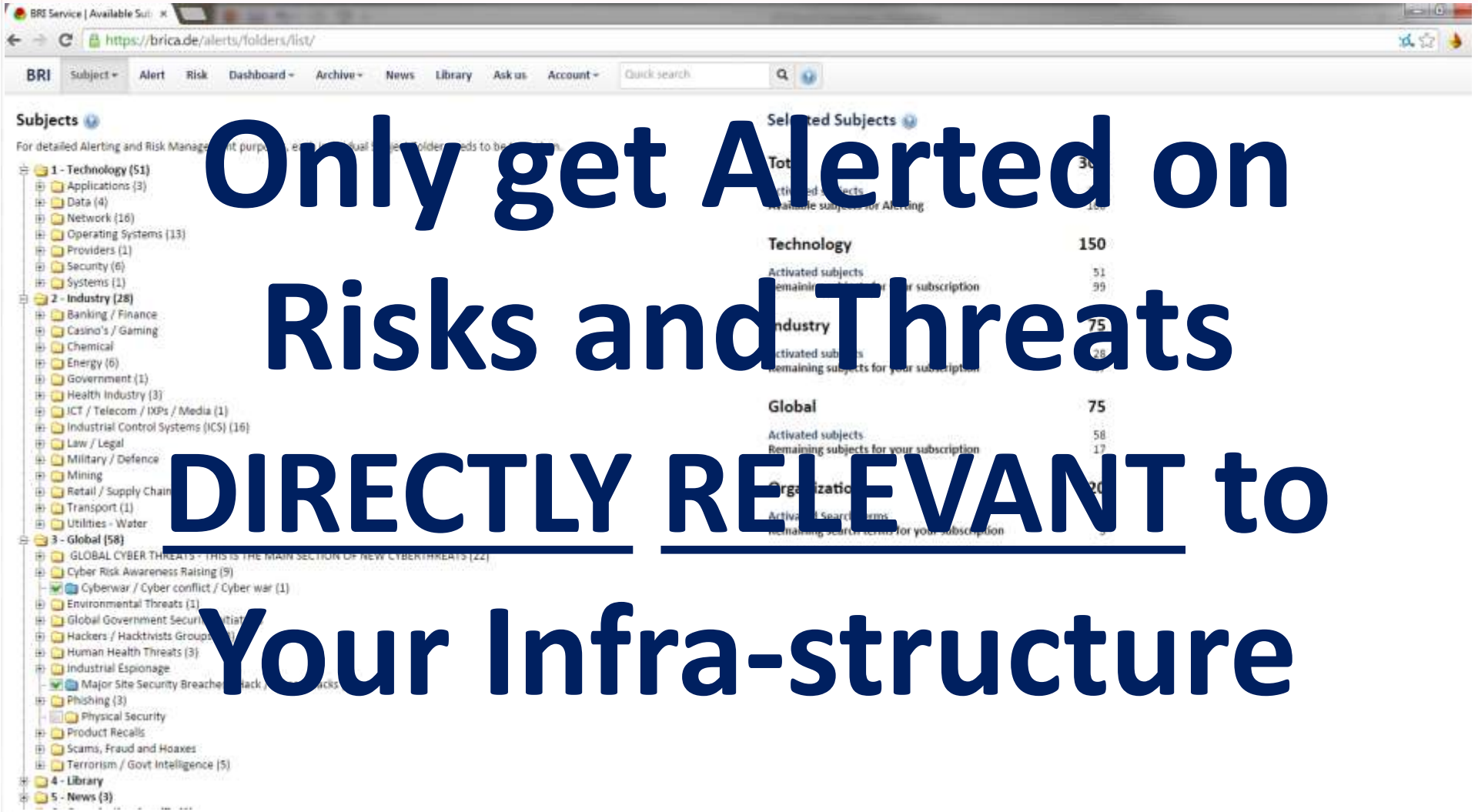
Global

- Mobile Certificates and Developer Accounts: Who is Faking It?
  5 minutes ago
- HEADS UP - Hackers Steal Bettys Customer Database
  23 minutes ago
- Italy and Spain Targeted with Ransomware
  27 minutes ago
- Email "Fax 19.05" contains trojan
  56 minutes ago
- We caught Chinese technology spies RED-HANDED claims US government
  1 hour, 18 minutes ago
- Measles outbreak feared in Australia's Queensland, 4,500 at risk
  1 hour, 43 minutes ago
- Can you afford to wait 197 days to detect a threat?
  1 hour, 47 minutes ago
- Morocco, UAE Cooperate to Deliver Aid to Help Guinea Fight Ebola
  1 hour, 50 minutes ago

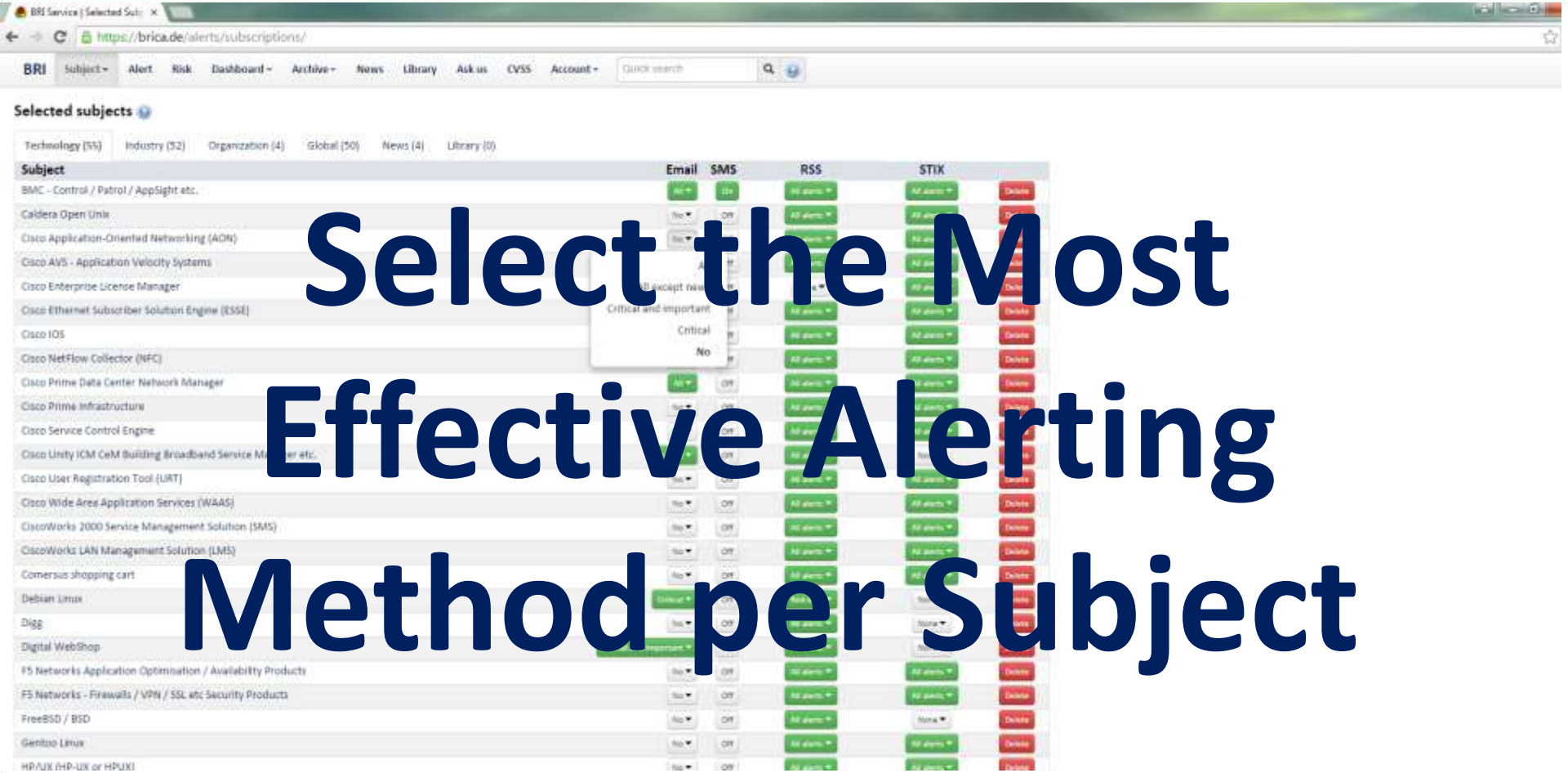
Each single raw result need checking by one or more BRI Risk analysts

BRI Risk Alert Services

- Harvesting Pods/Sensors Globally located
- 45 Risk Analysts, 4 Global Regions, 5 Shifts, 24x7
- On Average 35,000 items each 24 hrs
- Resulting in 250-600 alert items each 24 Hrs posted in database, each either Green, Yellow or Red
- Database contains some 827,000 items since Jan 2006
- Categorized in some 10,000 subjects
- Subject need to be activated first to enable alerting



Only get Alerted on Risks and Threats DIRECTLY RELEVANT to Your Infra-structure

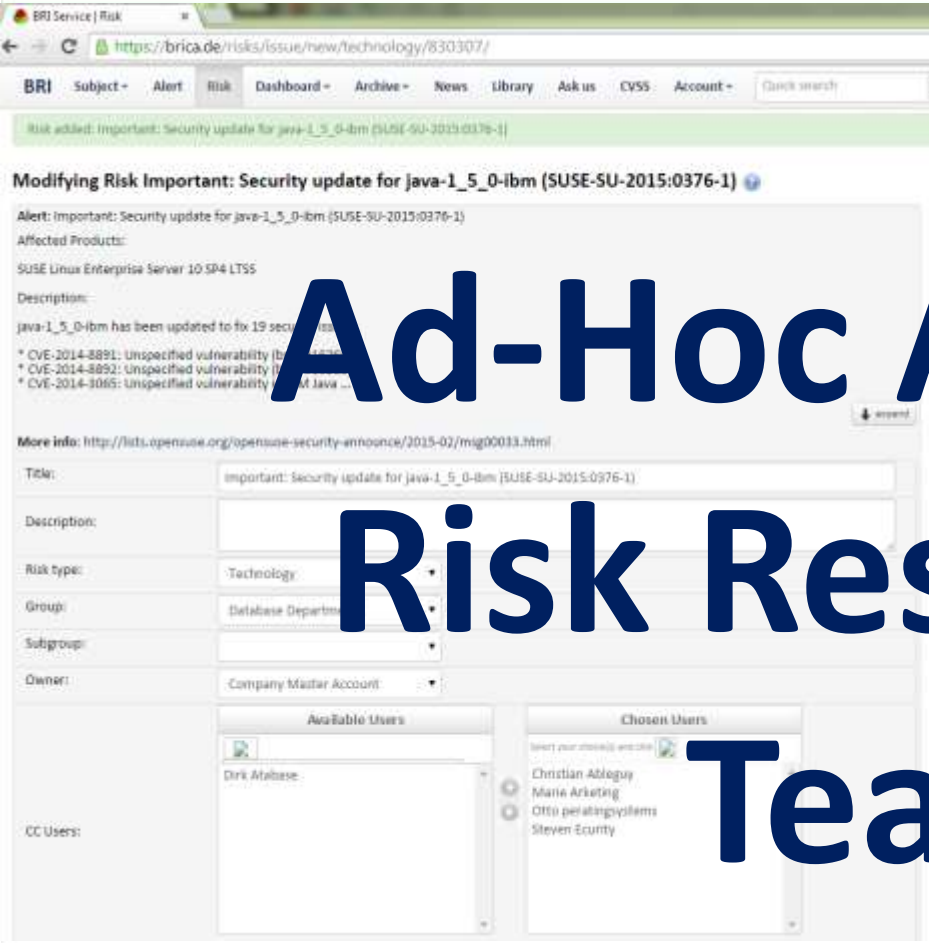


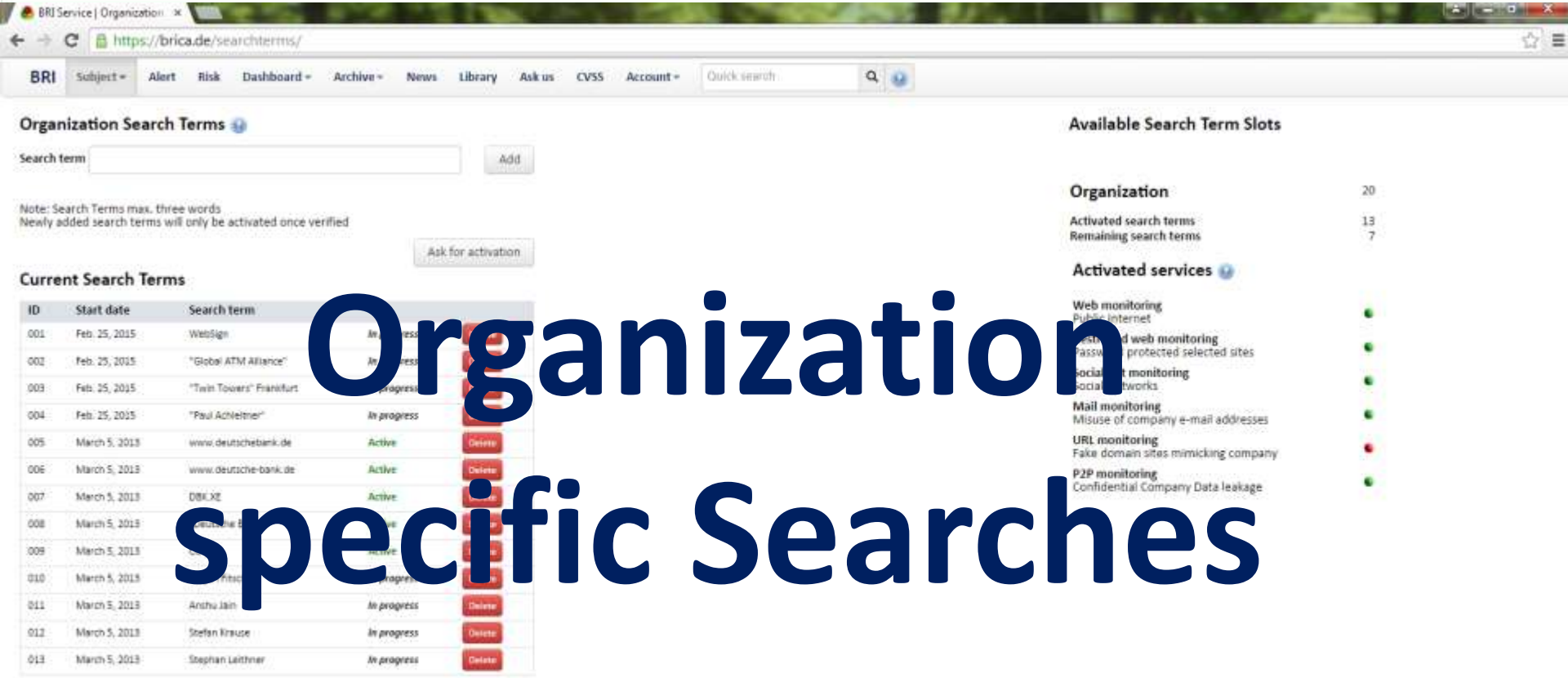
Select the Most Effective Alerting Method per Subject

Only Act on Relevant Threats

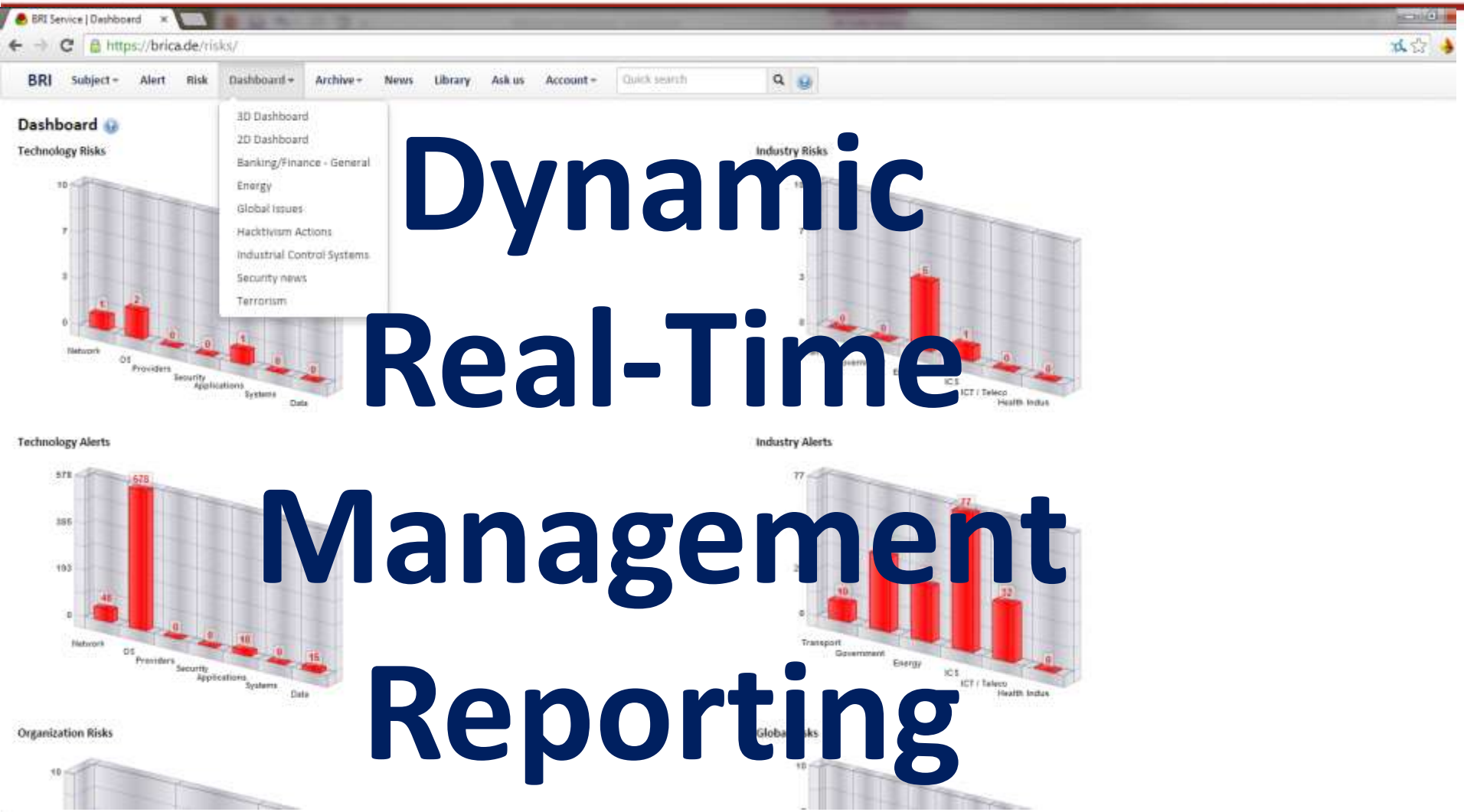
Minimise White noise

Ad-Hoc Assigned Risk Resolution Teams

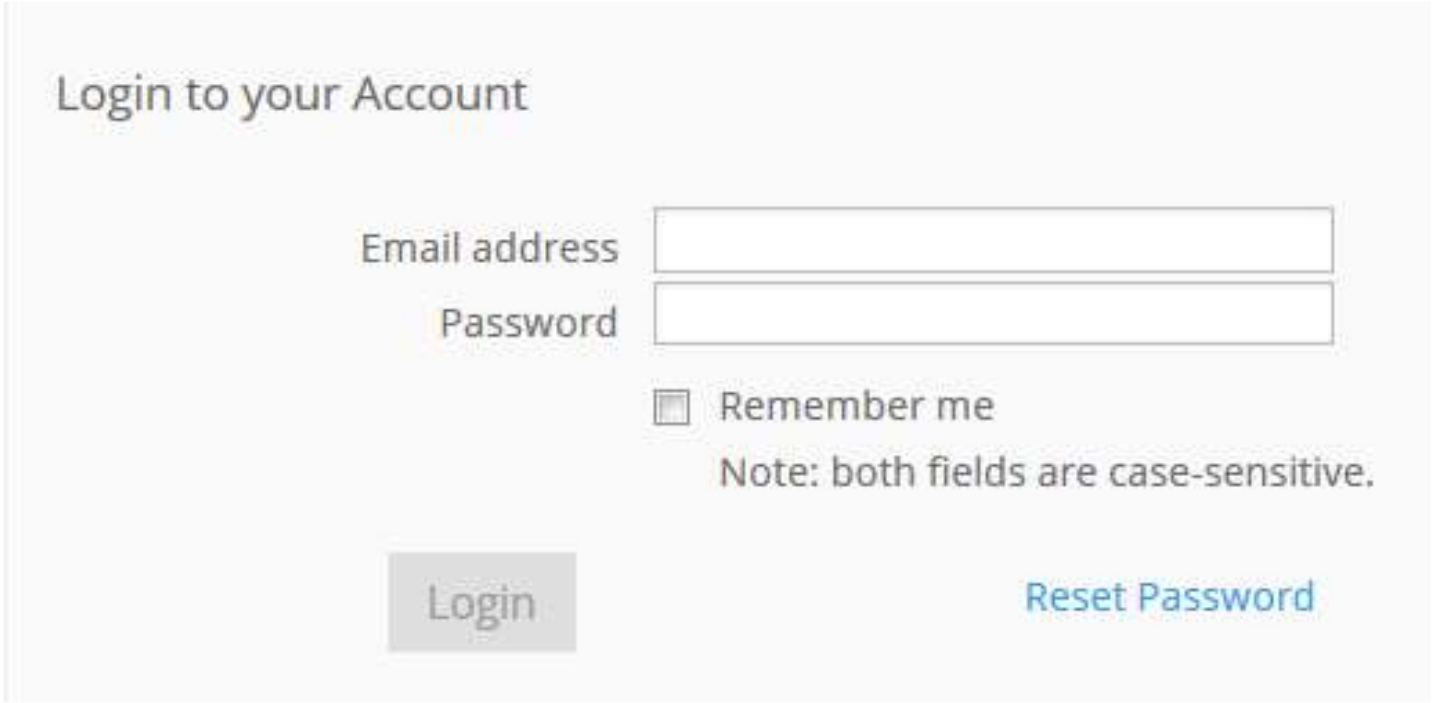




Organization specific Searches


BRI Service | Dashboard
https://brica.de/risks/
BRI
Subject
Alert
Risk
Dashboard
Archive
News
Library
Ask us
Account
Quick search
Dashboard
3D Dashboard
2D Dashboard
Banking/Finance - General
Energy
Global Issues
Hacktivism Actions
Industrial Control Systems
Security news
Terrorism
Technology Risks
Industry Risks
Technology Alerts
Industry Alerts
Organization Risks
Dynamic
Real-Time
Management
Reporting

Live Demo


Login to your Account
Email address
Password
Remember me
Note: both fields are case-sensitive.
Login
Reset Password

Conclusioni

Conclusioni

- L'utilizzo di **più portali di informazioni aperte**, svariati e differenti l'uno dall'altro, risulta **altamente dispersivo**:
  - Time-consuming
  - Approccio «manuale»
  - Mancanza di centralizzazione dei dati
  - Troppi Google dorks…
- Sento sempre parlare di «**Big Data Analytics**»…..
  - Ma **ci vanno i dati** da «far frullare»!
- Non è accettabile (ed è davvero **pericoloso ed imbarazzante**) venire a conoscenza dei propri leaks da:
  - Stampa e media
  - Pastebin &co
  - Clienti
  - Competitor
  - Vostro figlio ☹

Spare leaks

PASTEBIN | #1 paste tool since 2002 create new paste

PASTEBIN Follow @pastebin Mi piace 201

create new paste trending pastes sign up | login | my

** Pastebin PRO Accounts Spring Special ** Get 40% discount for a limited time only! Click Here to check it out ;-) Want more features

Untitled

BY: A GUEST ON JUL 30TH, 2011 | SYNTAX: NONE | SIZE: 18.94 KB | VIEWS: 3,897 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

8 11


```
1. vitrociset.it DATA LEAKED LOLZ!!
2.
3. 62      Administrator    admin    Admin@localhost.com      f393e68f8e256a962c2985c1c334fb10:jS2b9jrHueIAakuvj4NZBhL5XndAWTXN       Super
   Administrator     0       1       25       2009-02-13 10:53:33      2011-07-28 10:37:28
4.         admin_language=
5. language=
6. editor=
7. helpsite=
8. timezone=0
9.
```

Spare leaks

CNAIPIC #Antisec #Opitaly

BY: LULZSECITALY ON JUL 25TH, 2011 | SYNTAX: NONE | SIZE: 4.04 KB | VIEWS: 22,099 | EXPIRES: NEVER

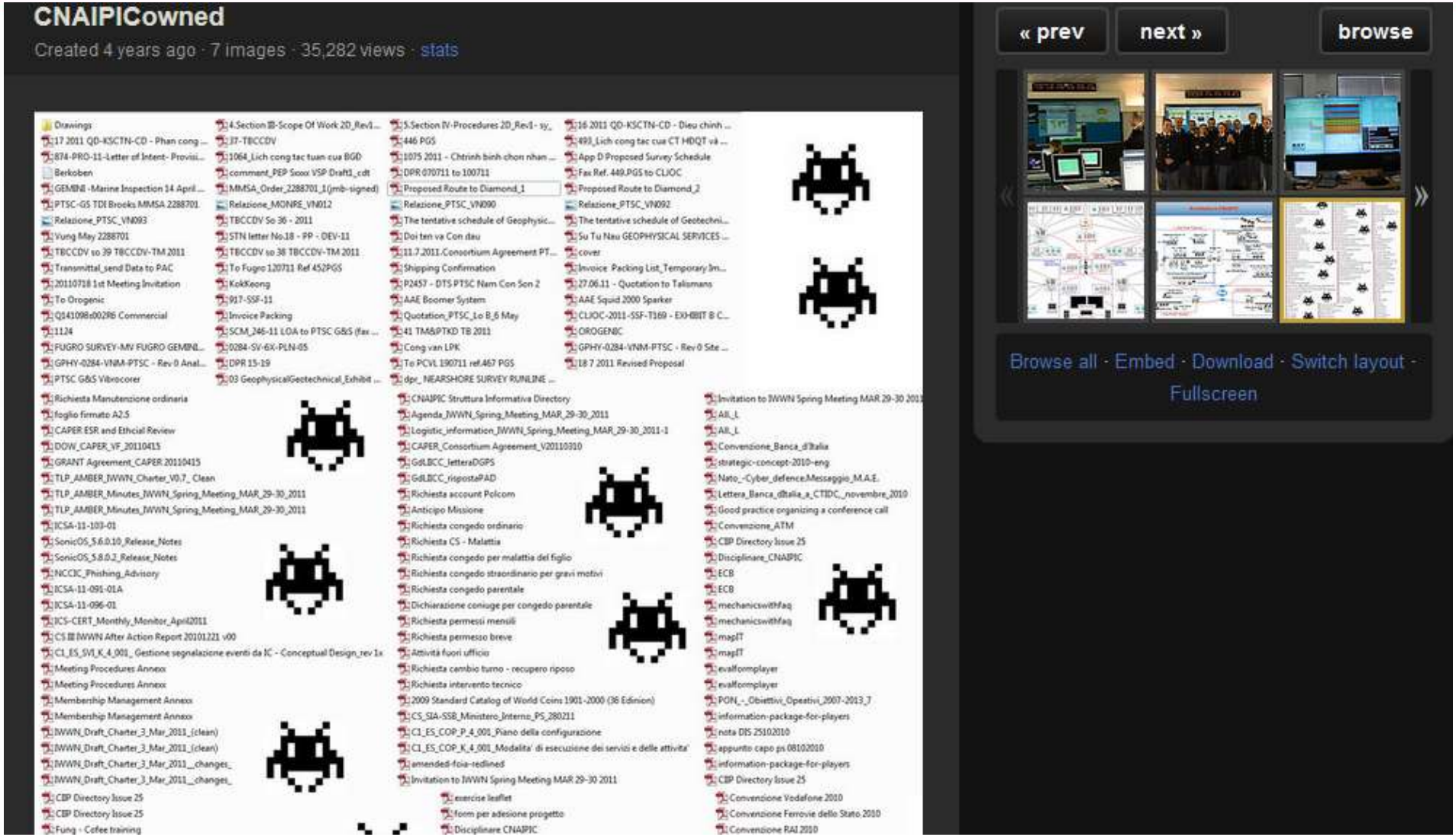
DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT


```
  888  888         d88888          888    Y8P
888888888888      d88P888          888
  888  888       d88P 888 88888b.  888888 888 .d8888b   .d88b.   .d8888b
  888  888      d88P  888 888 "88b 888    888 88K      d8P  Y8b d88P"
888888888888   d88P   888 888  888 888    888 "Y8888b. 88888888 888
  888  888    d8888888888 888  888 Y88b.  888      X88 Y8b.     Y88b.
  888  888   d88P     888 888  888  "Y888 888  88888P'  "Y8888   "Y8888P

Twitter.com/LulzsecItaly || Twitter.com/Anonitaly || antisec@in.com


'Giorno a voi
Questa è una prerelease,parte di una serie di dump che rilasceremo per rivelare
alcuni fra i più importanti rapporti e segreti nelle Agenzie di law Enforcement Informatiche,e le loro pratiche illegali e amorali.
Queste release saranno pubblicate e tweettate da tutta la community LulzSec & Anonymous nella campagna #AntiSec.
Oggi abbiamo ottenuto l'accesso al vaso di Pandora delle agenzie anticrimine Italiane e crediamo che questo sia l'nizio di una nuova
```

Spare leaks


CNAIPICowned
Created 4 years ago · 7 images · 35,282 views · stats
« prev
next »
browse
Browse all · Embed · Download · Switch layout · Fullscreen

Spare leaks

Il blog di Anonymous Italia

Home page | Darknet | WebChat | Contatti | Come raggiungerci

lunedì 18 maggio 2015

Ministero della Difesa - You have been Hacked!

OperationPayBack

Trovaci su Facebook

Operation Payback ITA

Mi piace 19.778

Operation Payback ITA

18 maggio alle ore 22.58

Ministero della Difesa - You have been Hacked!
+ di 1700 account privati sono stati trafugati dal sito web della difesa
http://anon-news.blogspot.com/.../ministero-difesa-hacked.html

Spare leaks

Cittadini del mondo: annunciamo che una lista di dati personali di eserciti e governanti di tutto il mondo è caduta nelle nostre mani.

Alcuni lavorano per grandi industrie belliche come **Selex**, **Mdba**,**Thales Group**, altri operano presso i vari ministeri d'europa come ad esempio quello della difesa spagnolo che con i suoi uomini spara ai profughi africani che cercano di entrare in Europa, altri ancora si occupano di **Cyber Defence**, come i signori dell' HackingTeam che vendono ai governi software per spiare i propri cittadini, come evidenziato da Wikileaks.

Aguzzini degli eserciti e delle polizie di tutto il mondo, politicanti sfruttatori: il vostro sogno è quello di traformare il pianeta in una gigantesca caserma dove gli esseri umani ignoranti sfruttati e impauriti devono lottare per guadagnare ciò che a stento basta a sostentarli.

Tutto ciò è aberrante e Anonymous non si stancherà mai di combatterlo.

Usurpatori e gendarmi: vogliamo che i rivoluzionari e le rivoluzionarie di tutto il mondo conoscano la vostra identità e si oppongano a voi come meglio credono, perciò abbiamo deciso di diffondere questi dati con l' intento di generare la più ferma opposizione possibile, contro il potere omicida degli Stati e delle industrie belliche che voi sostenete.

We are Anonymous
We are legion
We do not forgive
We do not forget
Expect us

+ di 1700 account privati sono stati trafugati dal sito

Spare leaks

v_MailInviate-905be267 Salva come Excel Powered by ZOHO

A1 fx A

	A	B
1	A	DA
2	aldo.semeraro@esercito.difesa.it	idgs.presidency.ue@smd.difes
3	alessandro.durso@am.difesa.it	idgs.presidency.ue@smd.difes
4	alfredo.deflorio@marina.difesa.it	idgs.presidency.ue@smd.difes
5	andrea.berdacchini@esercito.difesa.it	suadsezformav2@comfordot.es
6	andrea.lanzilli@aeronautica.difesa.it	idgs.presidency.ue@smd.difes
7	andrea.martellotti@esercito.difesa.it	suadsezformav2@comfordot.es
8	angelo.affinito@aeronautica.difesa.it	idgs.presidency.ue@smd.difes
9	angelovito.tosto@esercito.difesa.it	suadsezformav2@comfordot.es
10	annalisa.pelo@gmail.com	idgs.presidency.ue@smd.difes
11	antomars2001@yahoo.it	idgs.presidency.ue@smd.difes
12	antonio.bal65@gmail.com	suadsezformav2@comfordot.es
13	antonio.balzano@esercito.difesa.it	suadsezformav2@comfordot.es
14	antonio.castelluccio@aeronautica.difesa.it	idgs.presidency.ue@smd.difes
15	antonio.decandia@persociv.difesa.it	suadsezformav2@comfordot.es
16	antonio.dibranco@esercito.difesa.it	suadsezformav2@comfordot.es

Sheet1

Spare leaks + veloce analisi di scenario

v_lista_nominativi_iscritti — Salva come Excel — Powered by ZOHO

A1 | fx | ID ID_iscrizione Nome Cognome Categoria PaganteCongresso

	A
1	ID ID_iscrizione Nome Cognome Categoria PaganteCongresso
2	219 1000 eleonora d'ortenzi Attendee Ospiti COMFORDOT EI
3	220 1001 alice di silvio Attendee Ospiti COMFORDOT EI
4	221 1002 matteo fasano Attendee Ospiti COMFORDOT EI
5	222 1003 maritza genao Attendee Ospiti COMFORDOT EI
6	223 1004 Manuel ACCETTURA Attendee Ospiti COMFORDOT EI
7	226 1007 giovanni malizia Attendee Ospiti COMFORDOT EI
8	117 1008 Martin GULDEMOND Attendee Attendee
9	227 1009 Luca MESSERSI' Operating Personnel Ospiti COMFORDOT EI
10	228 1010 Benito Vitolo Operating Personnel Ospiti COMFORDOT EI
11	147 1011 STEFANO SPRO' Organization Personnel RAMDIFE STAFF
12	229 1012 CESARE FINOCCHI Operating Personnel Ospiti COMFORDOT EI
13	230 1013 GERARDO CAPASSO Operating Personnel Ospiti COMFORDOT EI
14	231 1014 Alberto PUGLIA Operating Personnel Ospiti COMFORDOT EI
15	232 1015 ANTONIO DE CANDIA Operating Personnel Ospiti COMFORDOT EI
16	233 1016 PASQUALE SCAFETTA Operating Personnel Ospiti COMFORDOT EI

Sheet1

Reading room /1

Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door, Brian Krebs, 2015

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

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 / of Intrusion, Kevin D. Mitnick & William L. Simon, Wiley, 2002/2004

@ 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

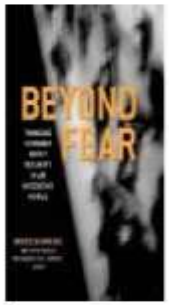
Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques, Turvey B., Knowledge Solutions Library, January, 1998

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

Il mio ultimo ordine su Amazon ☺

Information Doesn't Want to Be Free: Laws for the Internet Age
Doctorow, Cory,Palmer, Amanda,Gaiman, Neil; Hardcover
Sold by Amazon Export Sales, Inc.



Beyond Fear: Thinking Sensibly About Security in an Uncertain World.
Schneier, Bruce; Hardcover
Sold by Amazon Export Sales, Inc.

@War: The Rise of the Military-Internet Complex
Harris, Shane; Hardcover
Sold by Amazon Export Sales, Inc.

Worm: The First Digital World War
Bowden, Mark; Paperback
Sold by Amazon Export Sales, Inc.

Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It
Goodman, Marc; Hardcover
Sold by Amazon Export Sales, Inc.

This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information
Greenberg, Andy; Hardcover
Sold by Amazon Export Sales, Inc.

Il mio ultimo ordine su Amazon ☺

Lords of Secrecy: The National Security Elite and America's Stealth Warfare
Horton, Scott; Hardcover
Sold by Amazon Export Sales, Inc.

Cyber War: The Next Threat to National Security and What to Do About It
Clarke, Richard A.,Knake, Robert; Paperback
Sold by Amazon Export Sales, Inc.

Shadow Government: Surveillance, Secret Wars, and a Global Security State in a Single-Superpower World
Engelhardt, Tom,Greenwald, Glenn; Paperback
Sold by Amazon Export Sales, Inc.

No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State
Greenwald, Glenn; Hardcover
Sold by Amazon Export Sales, Inc.

DarkMarket: How Hackers Became the New Mafia
Glenny, Misha; Paperback
Sold by Amazon Export Sales, Inc.

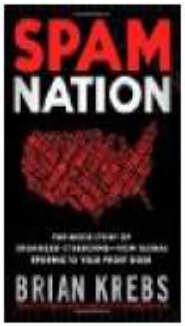
Liars and Outliers: Enabling the Trust that Society Needs to Thrive
Schneier, Bruce; Hardcover
Sold by Amazon Export Sales, Inc.

Il mio ultimo ordine su Amazon ☺

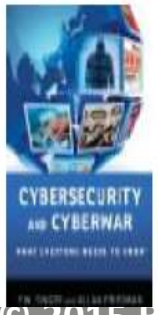
McMafia: A Journey Through the Global Criminal Underworld
Glenny, Misha; Paperback
Sold by Amazon Export Sales, Inc.

Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon
Zetter, Kim; Hardcover
Sold by Amazon Export Sales, Inc.

We Are Anonymous: Inside the Hacker World of LulzSec Anonymous, and the Global Cyber Insurgency
Olson, Parmy; Paperback
Sold by Amazon Export Sales, Inc.



Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door
Krebs, Brian; Hardcover
Sold by Amazon Export Sales, Inc.



Cybersecurity and Cyberwar: What Everyone Needs to Know®
Singer, P.W.,Friedman, Allan; Paperback
Sold by Amazon Export Sales, Inc.

The Snowden Files: The Inside Story of the World's Most Wanted Man
Harding, Luke; Paperback
Sold by Amazon Export Sales, Inc.

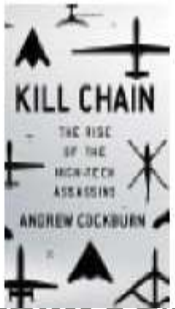
Il mio ultimo ordine su Amazon ☺

The Black Box Society: The Secret Algorithms That Control Money and Information
Pasquale, Frank; Hardcover
Sold by Amazon Export Sales, Inc.

Secrets and Lies: Digital Security in a Networked World
Schneier, Bruce; Paperback
Sold by Amazon Export Sales, Inc.

Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous
Coleman, Gabriella; Hardcover
Sold by Amazon Export Sales, Inc.

This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers
Greenberg, Andy; Paperback
Sold by Amazon Export Sales, Inc.

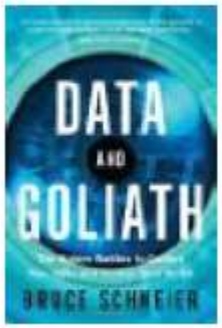


Kill Chain: The Rise of the High-Tech Assassins
Cockburn, Andrew; Hardcover
Sold by Amazon Export Sales, Inc.

The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet
Sauter, Molly,Zuckerman, Ethan; Paperback
Sold by Amazon Export Sales, Inc.

Il mio ultimo ordine su Amazon ☺

Black Code: Surveillance, Privacy, and the Dark Side of the Internet
Deibert, Ronald J.; Paperback
Sold by Amazon Export Sales, Inc.



Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World
Schneier, Bruce; Hardcover
Sold by Amazon Export Sales, Inc.

Contacts, Q&A

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

Thanks for your attention!

QUESTIONS?