

**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 Committee 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

«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 oggi giorno risiede su supporti digitali e viaggia in rete) può essere **immediatamente trasformato** in «qualcos'altro»:

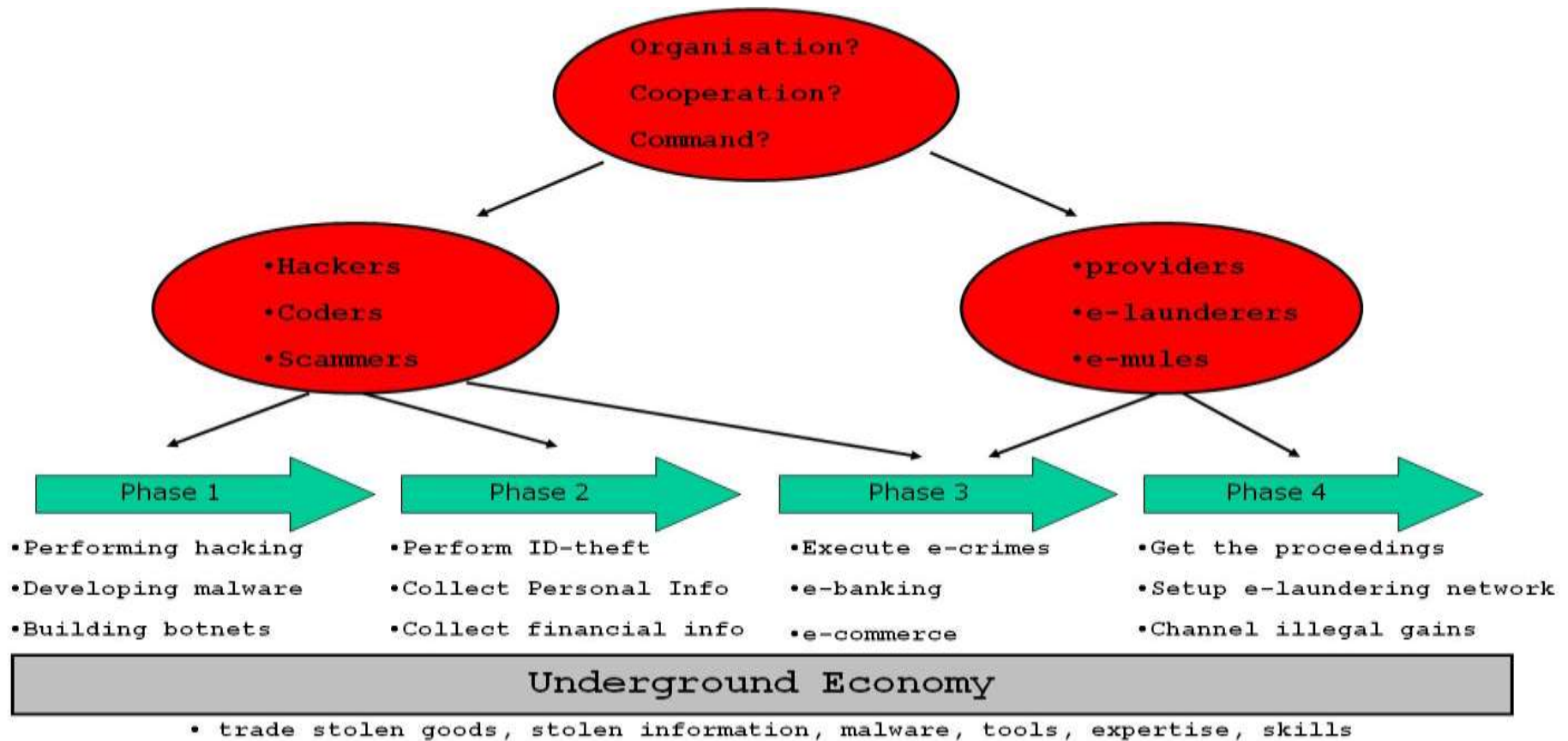
1. **Vantaggio competitivo (geo/politico, business, relazioni personali)**
Belgacom Hack
2. **Informazione sensibile/critica («blackmailing»/ricatto, estorsione)**
JP Morgan
3. **Denaro (tecniche di «Cash-out», Black Market & Underground Economy)**
Cybercrime

* 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 from 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»

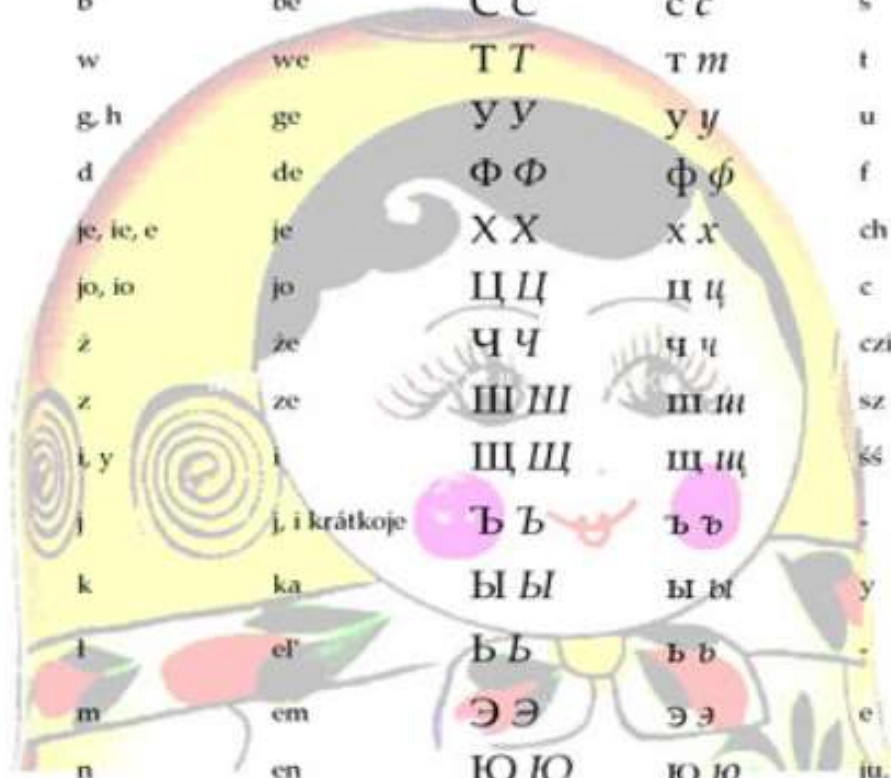
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	6	o)	3] =	6	/-/	1	_	X	1	v	\\	0	*	{_,}	2	5	7	π	\\	\\//	⊗	j	2
Λ	8	<	o	ε	ph	ε	[-]	!	/	<	ε	em	^/	()	o	()_	12	\$	+		√	vv	><	~/	~/
@	13	(ø	€)	(+_] - []	(1_]V[//\\//	oh	°	0_]?	z	- -	Y3W	\\//	'//	X	`(⊗
/\	I3	()	ε	=	9) - (eye	ε	b		(T)	/\	[]	^(o)	<	/2	\$	1	L		\\') (-/	>_
^	13	(c)	[]	ë	(=	C-	(-)	3y3	</	_	[V]	[\\]	p	>	9	I2	ehs	' ['	μ		\\^/	ecks	'/	8	
aye	8		I>	[-	I =	gee	:-:	ai	(/	lJ	nn	<\>	x	"	0,	1^	es	†	[_]		(n)	*	Ψ	7_	
ø	P>		>	= -		(v,	~	i	_7	-	//\\//\\	(\)	Ω	?	(,)	1~			\\	\\	\\V/	*	φ		
ci	!:		?			(_-	-] [_)		\\//	[]\		9	()	1z			\\	\\	\\X/) (λ		
λ	'3		T)			cj]~[:	i		/\	//	[]	[]D	ε	(r)			/	/	\\ /	ex	ϕ		
Z	(3		0) (] (]			(u)	/V	°		1'	12				(_ /		Ψ		
	/3		8			?					(V)	μ	7		[z					\\//\\//					
)3		cl) - ((\\)	[\\]	q		1'					\\: /					
	13					#					/\	[\\]	p		12					(/)					
											^^		q		8]	I[
											/ /		q		2						LL1				
											//.		q		.						UU				
											.\\		q		ε						III				
											/^^		q								q				
											/V														
											[\\]/[
											^^														



Altri esempi di «slangzzz»

Russian letters

АА	аа	a	a	РР	рр	r	er
ББ	бб	b	be	СС	сс	s	es
ВВ	вв	w	we	ТТ	тт	t	te
ГГ	гг	g, h	ge	УУ	уу	u	u
ДД	дд	d	de	ФФ	фф	f	ef, fe (pot.)
ЕЕ	ее	je, ie, e	je	ХХ	хх	ch	cha
ЁЁ	ёё	jo, io	jo	ЦЦ	цц	c	ce
ЖЖ	жж	z	ze	ЧЧ	чч	cz	chie
ЗЗ	зз	z	ze	ШШ	шш	sz	sza
ИИ	ии	i, y	i	ЩЩ	щщ	śś	śsia
ЙЙ	йй	j	j, i krátkoje	ЪЪ	ъъ	-	twiórdyj znak, jer
КК	кк	k	ka	ЫЫ	ыы	y	y
ЛЛ	лл	l	el'	ЬЬ	ьь	-	mjákkij znak, jer'
ММ	мм	m	em	ЭЭ	ээ	e	e abarótnoje
НН	нн	n	en	ЮЮ	юю	ju, iu	ju
ОО	оо	o, ~a	o	ЯЯ	яя	ja, ia, i	ja
ПП	пп	p	pe				



Altri esempi di «slangzzz»

Examples :

- KoHTpbl Hy6bl
- odd noobs
- Y %username% 4utbl 100 o\o,
AgmuH 3a6aHb ero
- User ... cheats I 100%, admin ban him
- Admin cmeHu map, 3ae6aJlo
- 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?



Each one has been
breached and their
customer data stolen
in 2014...

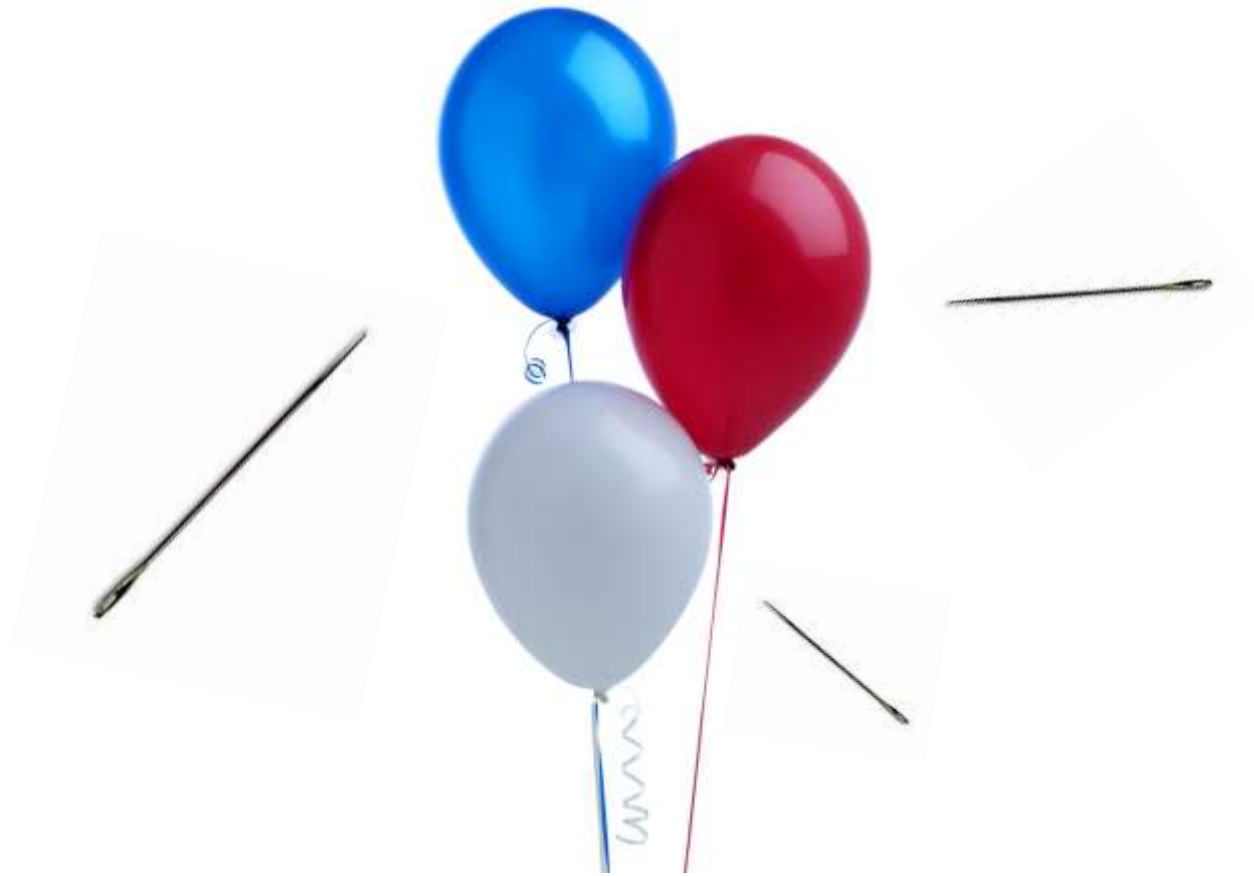
What Did They All Have In Common?

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.

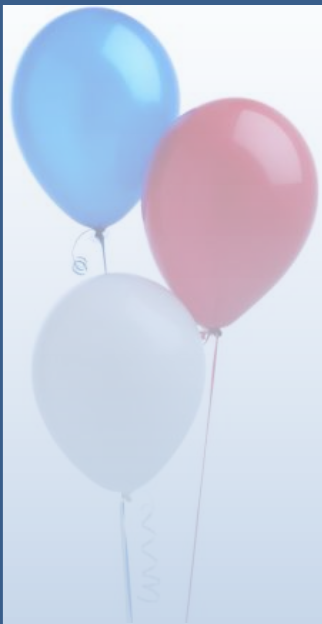


Where You Need to Be Aware 24x7 of EVERY New possible Spot a Hacker May possibly Stick A Needle ANYWHERE in YOUR Organization ANYTIME.



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



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

Subject Category	Total	Activated	Remaining
Technology	150	51	99
Industry	75	28	47
Global	75	58	17
Organization	20	1	19



Selected subjects

Technology (55) Industry (32) Organization (4) Global (50) News (4) Library (0)

Subject	Email	SMS	RSS	STIX	
BMC - Control / Patrol / AppSight etc.	All alerts	ON	All alerts	All alerts	Delete
Caiera Open Unix	No	ON	All alerts	All alerts	Delete
Cisco Application-Oriented Networking (AON)	No	ON	All alerts	All alerts	Delete
Cisco AVS - Application Velocity Systems	All except news	ON	All alerts	All alerts	Delete
Cisco Enterprise License Manager	All except news	ON	All alerts	All alerts	Delete
Cisco Ethernet Subscriber Solution Engine (ESSE)	All except news	ON	All alerts	All alerts	Delete
Cisco IOS	All except news	ON	All alerts	All alerts	Delete
Cisco NetFlow Collector (NFC)	All except news	ON	All alerts	All alerts	Delete
Cisco Prime Data Center Network Manager	All except news	ON	All alerts	All alerts	Delete
Cisco Prime Infrastructure	All except news	ON	All alerts	All alerts	Delete
Cisco Service Control Engine	All except news	ON	All alerts	All alerts	Delete
Cisco Unity ICM CeM Building Broadband Service Manager etc.	All except news	ON	All alerts	All alerts	Delete
Cisco User Registration Tool (URT)	All except news	ON	All alerts	All alerts	Delete
Cisco Wide Area Application Services (WAAS)	All except news	ON	All alerts	All alerts	Delete
CiscoWorks 2000 Service Management Solution (SMS)	All except news	ON	All alerts	All alerts	Delete
CiscoWorks LAN Management Solution (LMS)	All except news	ON	All alerts	All alerts	Delete
Comersus shopping cart	All except news	ON	All alerts	All alerts	Delete
Debian Linux	All except news	ON	All alerts	All alerts	Delete
Digg	All except news	ON	All alerts	All alerts	Delete
Digital WebShop	All except news	ON	All alerts	All alerts	Delete
F5 Networks Application Optimization / Availability Products	All except news	ON	All alerts	All alerts	Delete
F5 Networks - Firewalls / VPN / SSL etc Security Products	All except news	ON	All alerts	All alerts	Delete
FreeBSD / BSD	All except news	ON	All alerts	All alerts	Delete
Gentoo Linux	All except news	ON	All alerts	All alerts	Delete
HP/UX (HP-UX or HPUX)	All except news	ON	All alerts	All alerts	Delete

Select the Most Effective Alerting Method per Subject



Only Act on Relevant Threats Minimise White noise

The screenshot shows a web browser window with the URL <https://brica.de/alerts/>. The page has a navigation menu with items: BRI, Subject, Alert, Risk, Dashboard, Archive, News, Library, Ask us, Account, and a search bar. The main content is divided into three sections: 'Your incoming alerts', 'My Technology Alerts (224)', 'My Industry Alerts (47)', and 'My Global Alerts (162)'. Each section contains a list of alerts with details such as title, severity, and time ago. For example, under 'My Technology Alerts', there are alerts like 'Re-Release - Security Advisory-Information Leakage Vulnerability' and 'Moderate Security update for openstack-dashboard'. Under 'My Industry Alerts', there are alerts like 'Hacking Smart Electricity Meters To Cut Power Bills' and 'Sandworm to Blacken: The SCADA Connection'. Under 'My Global Alerts', there are alerts like 'Heads-Up - Hackers strike defense companies' and 'Virgin Media Customers Targeted in Phishing Scam'. Each alert entry includes a 'Connect to risk' button, a 'Not applicable' button, and a 'New risk' button.

Ad-Hoc Assigned Risk Resolution Teams

The screenshot shows a web browser window with the URL <https://brica.de/risks/issue/new/technology/830307/>. The page title is "Modifying Risk Important: Security update for java-1_5_0-ibm (SUSE-SU-2015:0376-1)". The main content area displays the following information:

- Alert:** Important: Security update for java-1_5_0-ibm (SUSE-SU-2015:0376-1)
- Affected Products:** SUSE Linux Enterprise Server 10 SP4 LTSS
- Description:** java-1_5_0-ibm has been updated to fix 19 security issues.
 - * CVE-2014-8891: Unspecified vulnerability (Buffer overflow) in Java ...
 - * CVE-2014-8892: Unspecified vulnerability (Denial of Service) in Java ...
 - * CVE-2014-3085: Unspecified vulnerability (Denial of Service) in Java ...
- More info:** <http://lists.opensuse.org/opensuse-security-announce/2015-02/msg00033.html>
- Title:** Important: Security update for java-1_5_0-ibm (SUSE-SU-2015:0376-1)
- Description:** (Empty text box)
- Risk type:** Technology
- Group:** Database Department
- Subgroup:** (Empty dropdown)
- Owner:** Company Master Account
- CC Users:** A list of users is shown, including Dirk Altbese, Christian Altbegy, Marie Arkelrig, Otto perlatingsvilems, and Steven Ecurty.

BRI Service | Organization x
 https://brica.de/searchterms/

BRI Subject = Alert Risk Dashboard = Archive = News Library Ask us CVSS Account = Quick search

Organization Search Terms

Search term Add

Note: Search Terms max. three words
 Newly added search terms will only be activated once verified

Ask for activation

Current Search Terms

ID	Start date	Search term	Status	Action
001	Feb. 25, 2015	WebSign	In progress	Delete
002	Feb. 25, 2015	"Global ATM Alliance"	In progress	Delete
003	Feb. 25, 2015	"Twin Towers" Frankfurt	In progress	Delete
004	Feb. 25, 2015	"Paul Achleitner"	In progress	Delete
005	March 5, 2015	www.deutschebank.de	Active	Delete
006	March 5, 2015	www.deutsche-bank.de	Active	Delete
007	March 5, 2015	DBK.XE	Active	Delete
008	March 5, 2015	deutschebank.com	Active	Delete
009	March 5, 2015	deutschebank.com	Active	Delete
010	March 5, 2015	deutschebank.com	In progress	Delete
011	March 5, 2015	Anshu Jain	In progress	Delete
012	March 5, 2015	Stefan Krause	In progress	Delete
013	March 5, 2015	Stephan Leitner	In progress	Delete

Available Search Term Slots

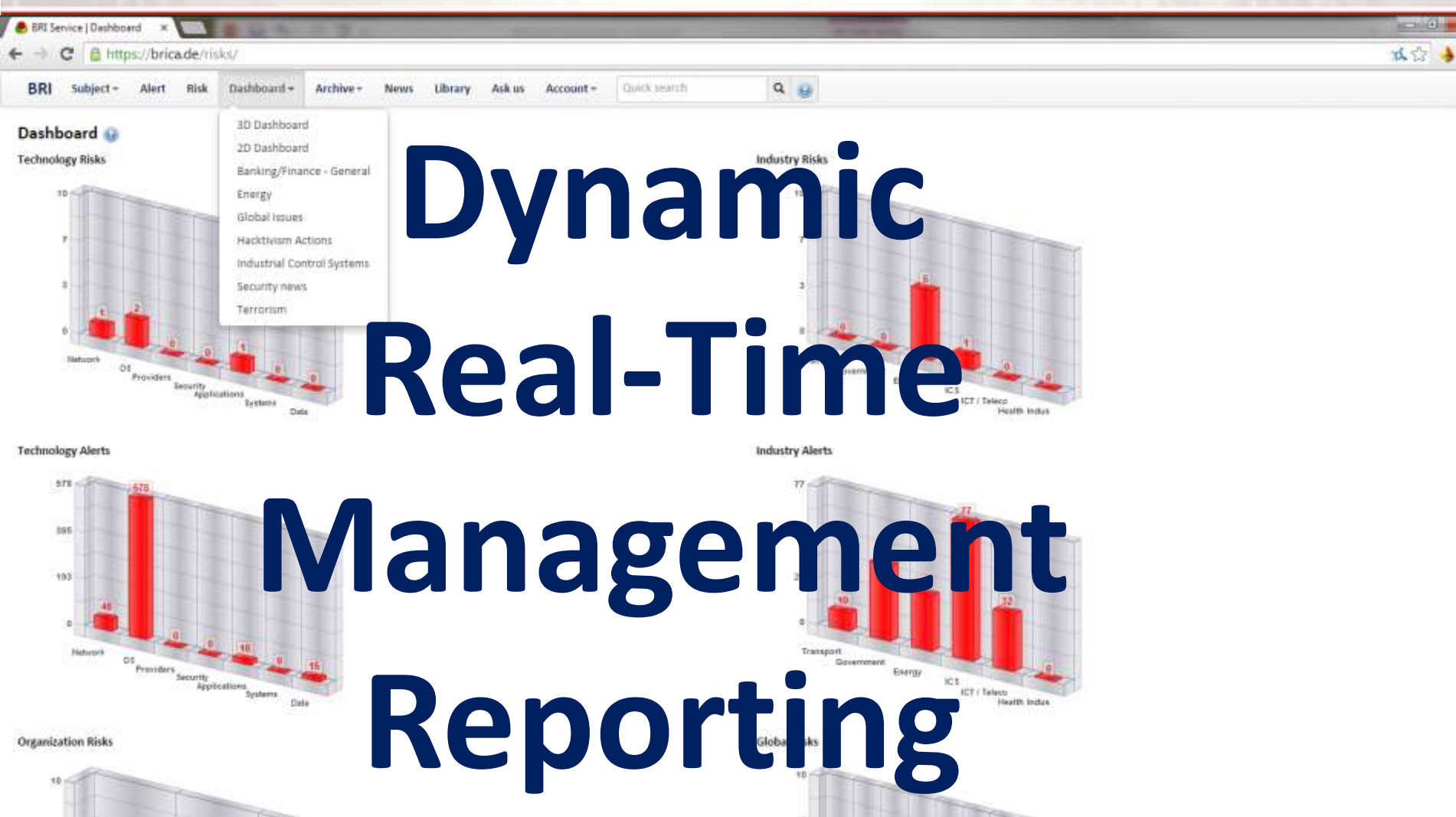
Organization 20

Activated search terms 13
 Remaining search terms 7

Activated services

- Web monitoring: Public internet (Active)
- Web monitoring: Password protected selected sites (Active)
- Social network monitoring: Social networks (Active)
- Mail monitoring: Misuse of company e-mail addresses (Active)
- URL monitoring: Fake domain sites mimicking company (Warning)
- P2P monitoring: Confidential Company Data leakage (Active)

Organization specific Searches



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

search

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](#)



**INCREASE UPTIME. STOP OUTAGES. AND GET
A GOOD NIGHT'S SLEEP. TRY PAGERDUTY
FREE.**



```
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



CODESHIP IS FAST AND SECURE. GET 5 PRIVATE PROJECTS AND 100 BUILDS PER MONTH FOR FREE.

```
1.
2. 888 888      d88888      888  Y8P
3. 8888888888888888      d88P888      888
4. 888 888      d88P 888 888888b. 888888 888 .d8888b .d88b. .d8888b
5. 888 888      d88P 888 888 "88b 888 888 88K      d8P Y8b d88P"
6. 8888888888888888      d88P 888 888 888 888 888 "Y8888b. 888888888 888
7. 888 888      d88888888888 888 888 Y88b. 888      X88 Y8b.      Y88b.
8. 888 888      d88P      888 888 888 "Y888 888 888888P' "Y8888 "Y8888P
9.
10. Twitter.com/LulzsecItaly || Twitter.com/Anonitaly || antisec@in.com
11.
12.
13. 'Giorno a voi
14. Questa è una prerelease, parte di una serie di dump che rilasceremo per rivelare
15. alcuni fra i più importanti rapporti e segreti nelle Agenzie di law Enforcement Informatiche, e le loro pratiche illegali e amorali.
16. Queste release saranno pubblicate e tweettate da tutta la community LulzSec & Anonymous nella campagna #AntiSec.
17. 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

Drawings

- 17 2011 QD-KSCTN-CD - Phan cong...
- 874-PRO-11-Letter of Intent- Provis...
- Berkoben
- GEMBN - Marine Inspection 14 April...
- PTSC-GS TDI Brooks MMSA 2288701
- Relazione_PTSC_VN093
- Vung May 2288701
- TBCCDV vo 39 TBCCDV-TM 2011
- Transmittal_send Data to PAC
- 20110728 1st Meeting Invitation
- To Orogenic
- Q4109800298 Commercial
- 1124
- FUGRO SURVEY-MV FUGRO GEMBN...
- GPYH-0284-VNM-PTSC - Rev 0 Anal...
- PTSC G&S Vibrocuer
- Richiesta Mancenzione ordinaria
- foglio firmato A2.5
- CAPER ESR and Ethical Review
- DOW_CAPER_VF_20110415
- GRANT Agreement_CAPER 20110415
- TLP_AMBER_JWWN_Charter_V0.7_Clean
- TLP_AMBER_Minutes_JWWN_Spring_Meeting_MAR_29-30_2011
- TLP_AMBER_Minutes_JWWN_Spring_Meeting_MAR_29-30_2011
- ICSA-11-103-01
- SonicOS_5.6.0.10_Release_Notes
- SonicOS_5.8.0.2_Release_Notes
- NCCCK_Fishing_Advisory
- ICSA-11-091-01A
- ICSA-11-096-01
- ICS-CERT_Monthly_Monitor_April2011
- CS III JWWN After Action Report 20101221 v00
- CI_ES_SVI_K_4_001_Gestione segnalazione eventi da IC - Conceptual Design_rev 1x
- Meeting Procedures Annex
- Meeting Procedures Annex
- Membership Management Annex
- Membership Management Annex
- JWWN_Draft_Charter_3_Mar_2011_(clean)
- JWWN_Draft_Charter_3_Mar_2011_(clean)
- JWWN_Draft_Charter_3_Mar_2011_changes
- JWWN_Draft_Charter_3_Mar_2011_changes
- CBP Directory Issue 25
- CBP Directory Issue 25
- Fung - Cofee training
- 4 Section III-Scope Of Work 2D_Rev1...
- J7-TBCCDV
- 1064 Lich cong tac tuan cua BGD
- comment_FEP Soox VSP Draft1_cdt
- MMSA_Order_2288701_1(mb-signed)
- Relazione_MONRE_VN012
- TBCCDV So 36 - 2011
- STN letter No.18 - PP - DEV-11
- TBCCDV vo 38 TBCCDV-TM 2011
- To Fugro 120711 Ref 452PGS
- KokKeong
- 917-55F-11
- Invoice Packing
- SCM_246-11 LOA to PTSC G&S (fax...
- 0284-SV-6X-PLN-05
- DPR 15-19
- 03 GeophysicalGeotechnical_Exhibit...
- 5.Section IV-Procedures 2D_Rev1- sy...
- 446 PGS
- 1075 2011 - Chtrinh binh chon nhan...
- DPR 070711 to 100711
- Proposed Route to Diamond_1
- Relazione_PTSC_VN090
- The tentative schedule of Geophysic...
- Doi ten va Con dau
- 11.7.2011.Consortium Agreement PT...
- Shipping Confirmation
- P2457 - DTS PTSC Nam Con Son 2
- AAE Boomer System
- Quotation_PTSC_Lo B,6 May
- 41 TMA&PTKD TB 2011
- Cong van LPK
- To PCVL 190711 ref.467 PGS
- dpr_NEARSHORE SURVEY RUNLINE...
- 16 2011 QD-KSCTN-CD - Dieu chinh...
- 493 Lich cong tac cua CT HDQT va ...
- App D Proposed Survey Schedule
- Fax Ref. 449.PGS to CLJOC
- Proposed Route to Diamond_2
- Relazione_PTSC_VN092
- The tentative schedule of Geotechni...
- Su Tu Nau GEOPHYSICAL SERVICES...
- cover
- Invoice Packing List_Temporary Im...
- 27.06.11 - Quotation to Talismans
- AAE Squid 2000 Sparker
- CLJOC-2011-55F-T169 - EX-HBIT B C...
- OROGENIC
- GPYH-0284-VNM-PTSC - Rev 0 Site...
- 18 7 2011 Revised Proposal
- Invitation to JWWN Spring Meeting MAR 29-30 2011
- Agenda_JWWN_Spring_Meeting_MAR_29-30_2011
- Logistic_information_JWWN_Spring_Meeting_MAR_29-30_2011-1
- CAPER_Consortium Agreement_V20110910
- G&L BCC_lettersDGPS
- G&L BCC_rispostaPAD
- Richiesta account Polcom
- Anticipo Missione
- Richiesta congedo ordinario
- Richiesta CS - Malattia
- Richiesta congedo per malattia del figlio
- Richiesta congedo straordinario per gravi motivi
- Richiesta congedo parentale
- Dichiarazione coniuge per congedo parentale
- Richiesta permessi mensili
- Richiesta permesso breve
- Attività fuori ufficio
- Richiesta cambio turno - recupero riposo
- Richiesta intervento tecnico
- 2009 Standard Catalog of World Coins 1901-2000 (36 Edition)
- CS_SIA-SSB_Ministero_Interno_PS_280211
- CI_ES_COP_P_4_001_Piano della configurazione
- CI_ES_COP_K_4_001_Modalita' di esecuzione dei servizi e delle attivita'
- amended-foia-redlined
- Invitation to JWWN Spring Meeting MAR 29-30 2011
- esercizio leaflet
- Form per adesione progetto
- Disciplinare CNAIPIC
- All_L
- All_L
- Convenzione_Banca_d'Italia
- strategic-concept-2010-eng
- Nato_-_Cyber_defence.Messaggio_M.A.E.
- Lettera_Banca_d'Italia_a_CTIDC_novembre_2010
- Good practice organizing a conference call
- Convenzione_ATM
- CBP Directory Issue 25
- Disciplinare_CNAIPIC
- ECB
- ECB
- mechanicswithfaq
- mechanicswithfaq
- magIT
- magIT
- evalformplayer
- evalformplayer
- PON_-_Obiettivi_Operativi_2007-2013_7
- information-package-for-players
- nota DIS 25102010
- appuntamento capo ps 08102010
- information-package-for-players
- CBP Directory Issue 25
- Convenzione Vedafone 2010
- Convenzione Ferrovie dello Stato 2010
- Convenzione RAI 2010

« 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/.../ministro-difesa-hacked.html>



Plus in social di Facebook

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 trasformare 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_MailInviat-905be267

Salva come Excel

Powered by Zoho

	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 ZOHIO

A1	fx	ID	ID_iscrizione	Nome	Cognome	Categoria	PaganteCongresso
1		ID	ID iscrizione	Nome	Coqnome	Cateqoria	PaqanteCongresso
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 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 / 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 WikiLeaks, 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.



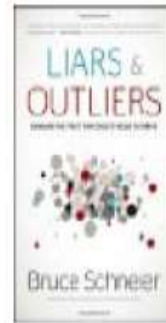
Shadow Government: Surveillance, Secret Wars, and a Global Security State in a Single-Superpower World
Engelhardt, Tom, Greenwald, Glenn; Paperback
Sold by Amazon Export Sales, Inc.



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

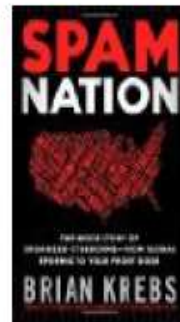
Sold by Amazon Export Sales, Inc.



We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency

Olson, Parmy; Paperback

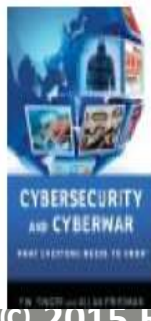
Sold by Amazon Export Sales, Inc.



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 Anonymity
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.



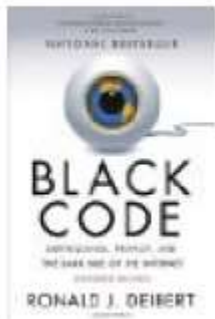
Kill Chain: The Rise of the High-Tech Assassins
Cockburn, Andrew; Hardcover
Sold by Amazon Export Sales, Inc.



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?

