

**World's Biggest Data Breach:
un'analisi «out of the box»
di Security Incidents
e Fughe di Informazioni**

**Raoul «Nobody» Chiesa
President, Security Brokers**

Chi sono

- Presidente, fondatore **Security Brokers SCpA**
- Direttore, **CyberDefcon Ltd.**
- Special Senior Advisor in tema di Cybercrime @ **UNICRI**
(United Nations Interregional Crime & Justice Research Institute)
- Former PSG Member, **ENISA** (Permanent Stakeholders Group @ European Union Network & Information Security Agency) – 2010/2012, 2013/2015
- Socio Fondatore, **CLUSIT** (Associazione Italiana per la Sicurezza Informatica)
- Comitato Direttivo, **AIP/OPSI** (Osservatorio Sicurezza & Privacy)
- Membro del board, **ISECOM** (Institute for Security and Open Methodologies)
- Membro del board, **OWASP**, Capitolo Italiano (Open Web Application Security Project)
- Cultural Attachè, **APWG** European Chapter
- Roster of Experts Member, **ITU** (International Telecommunication Union, Ginevra)
- **Sostenitore di svariate comunità in tema di InfoSec**



Chi siamo

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 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
 - **Cyber Security Strategic Consulting** (Technical, Legal, Compliance, PR, Strategy)
 - On-demand «Ninja Teams»
 - Security Incident PR Handling & Management
 - **Aspetti psicologici, sociali e comportamentali**
 - **Cybercrime Intelligence**
 - Targeted Threat Intelligence, Botnet takeovers, takedowns, Cybercriminals bounting, Cyber Intelligence Reports, interfacciamento con CERTs e LEAs/LEOs,[...]
 - **Information Warfare & Cyber War** (solo per GOV, MoD, IA)
 - 0-day ed Exploits – Digital Weapons
 - OSINT
 - Cyber Feeds

Cybercrime

→ perché parliamo di “Cybercrime”?

«Il Cybercrime è il 4° crimine economico globale»..... 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: 6-12 BLN USD\$/year

2015: (almeno) 20B USD\$/year



Key points del 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**

«Deliverables» del Cybercrime

- **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**

Esempi reali di Cybercrime

- Belgian bank Crelan loses €70 million to BEC scammers

- A possible future for IoT security

- Review: Automating Open Source Intelligence

- There's no turning back: Say goodbye to the perimeter

- The dismal state of payment data security

- Top drivers of investment in forensic data analytics

- SSH backdoor found in more Fortinet devices, exploit attempts spotted in the wild

- Magento plugs XSS holes that can lead to e-store hijacking, patch immediately!

- Versatile Linux backdoor acts as downloader, spyware

Belgian bank Crelan loses €70 million to BEC scammers

Posted on 26 January 2016.

Belgian bank Crelan has become a victim of fraudsters. According to a [statement](#) (in Dutch) published last week, the bank has lost over 70 million euros (around \$75,8 million).

The theft was perpetrated by outsiders (possibly foreigners), and was discovered during an internal audit. The bank has implemented additional security measures to prevent this from happening again.

The Belgian authorities were informed of the matter immediately, and so were the bank's risk and audit committees.

"Thanks to reserves accumulate in the past, Crelan can sustain this loss without it having consequences for the bank's clients and partners," Luc Versele, the bank's CEO, stated. "The intrinsic profitability of the bank remains intact."

They do not say so in the statement, but according to Belgian newspaper [Het Nieuwsblad](#) (in Dutch), the bank was a victim of so-called CEO fraud (or BEC scam - Business Email Compromise).

In these attacks, the fraudsters usually either manage to compromise the CEO's or another high-up manager's email account, or manage to impersonate them by creating a convincingly similar email account, and send an email to someone in the financial department, ordering a payment

Un «mondo nuovo»?

- Videoclip: Will you be ready? (Did You know? - 2011)



High Tech Criminals

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



Il ROI del Cybercrime

→ Perché il Cybercrime «ha successo»?

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%**

28



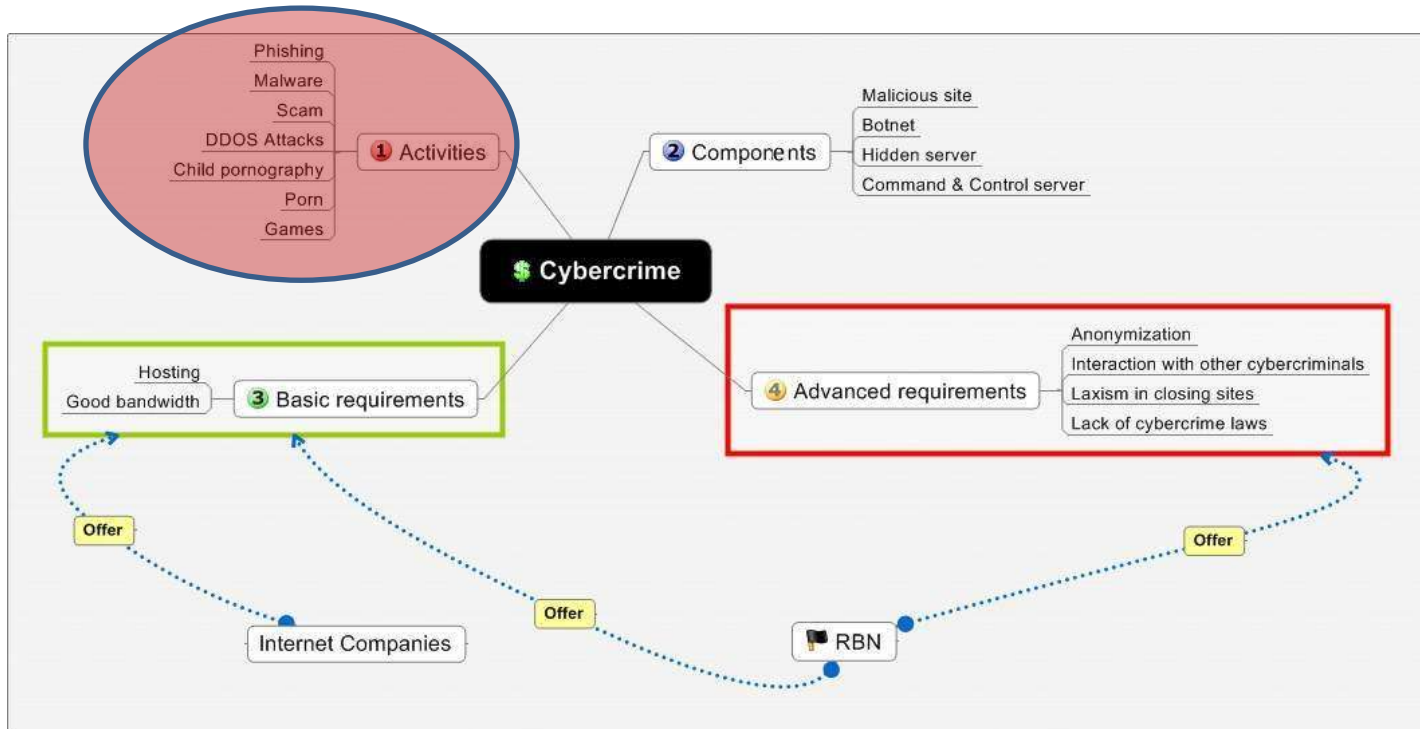
Perché tutto questo sta accadendo?

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



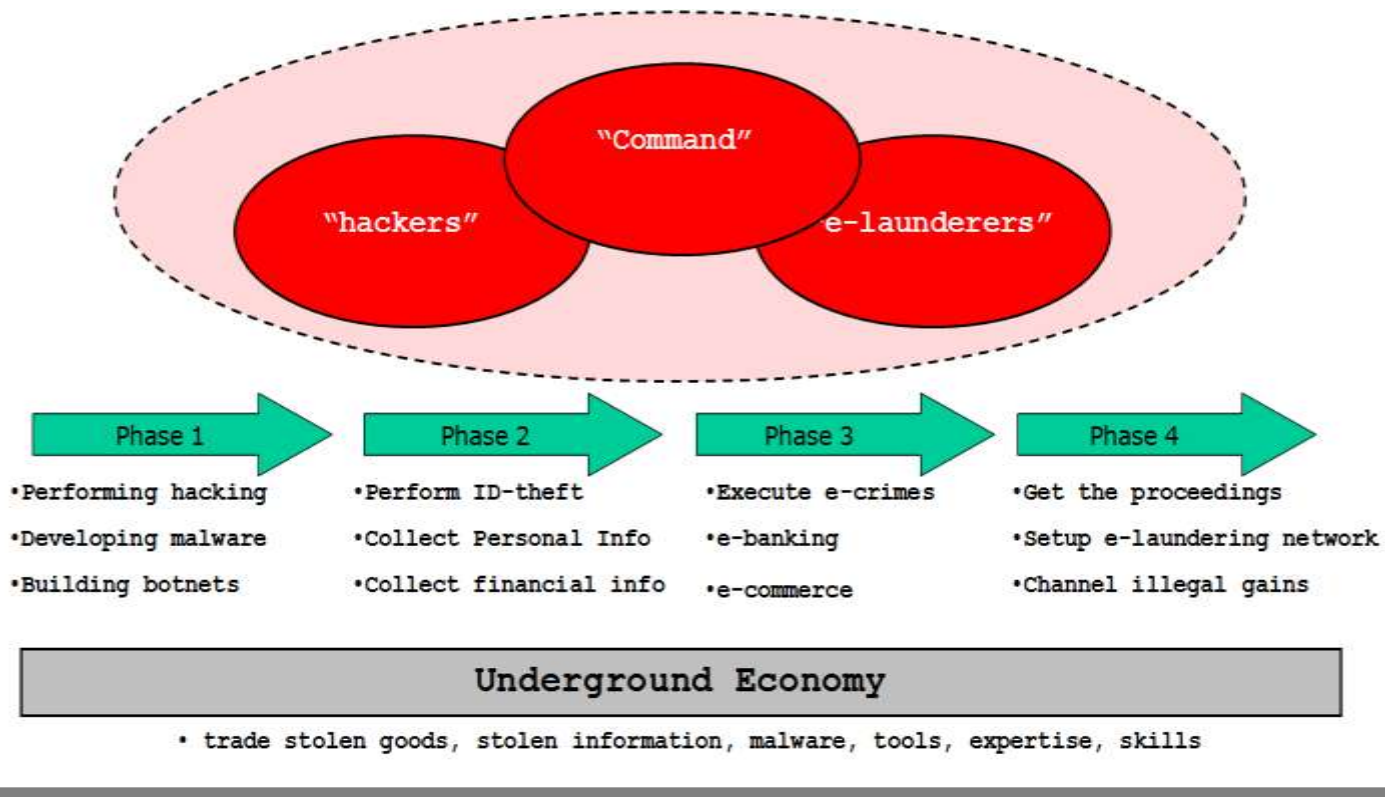
Cybercrime Business Model

→ il «Modello RBN» (Russian Business Network)



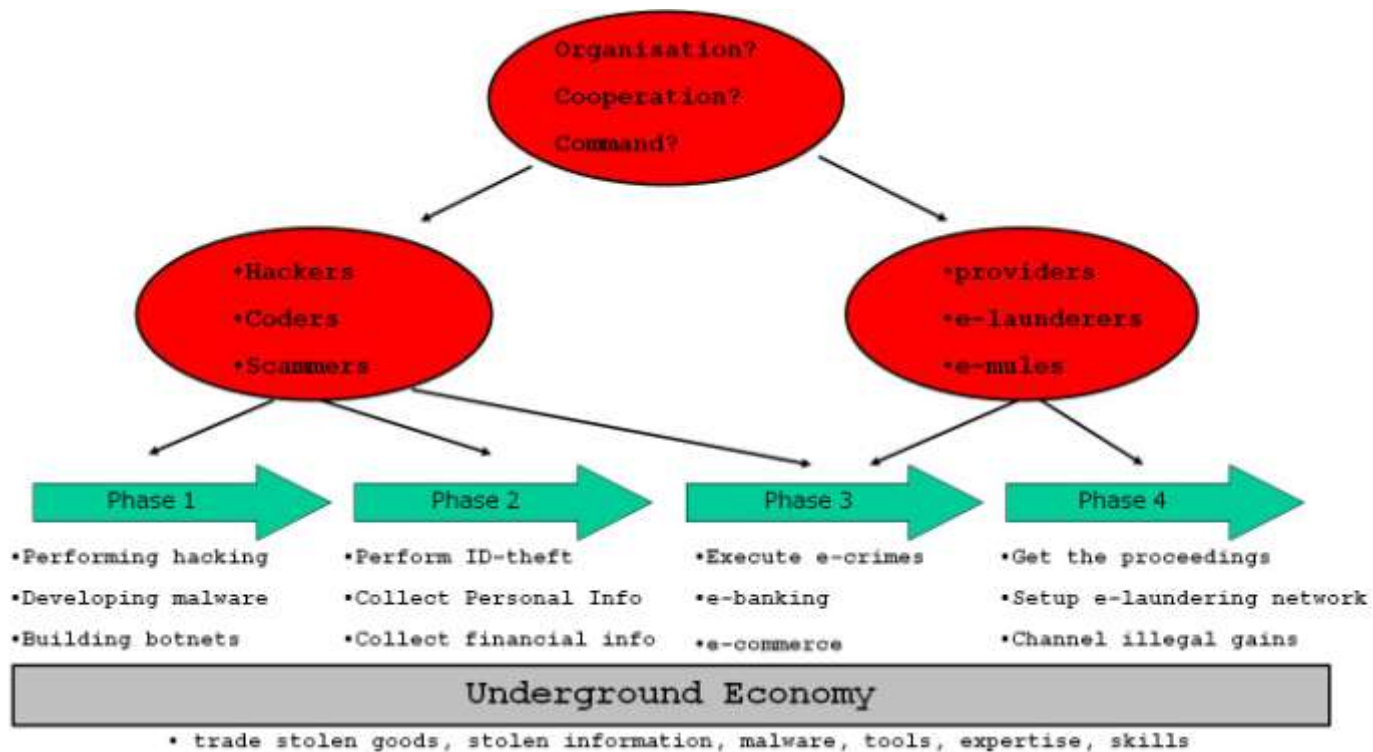
Quando il CO (crimine organizzato) incontra il Cybercrime

→ Catena del comando (e fasi operative)

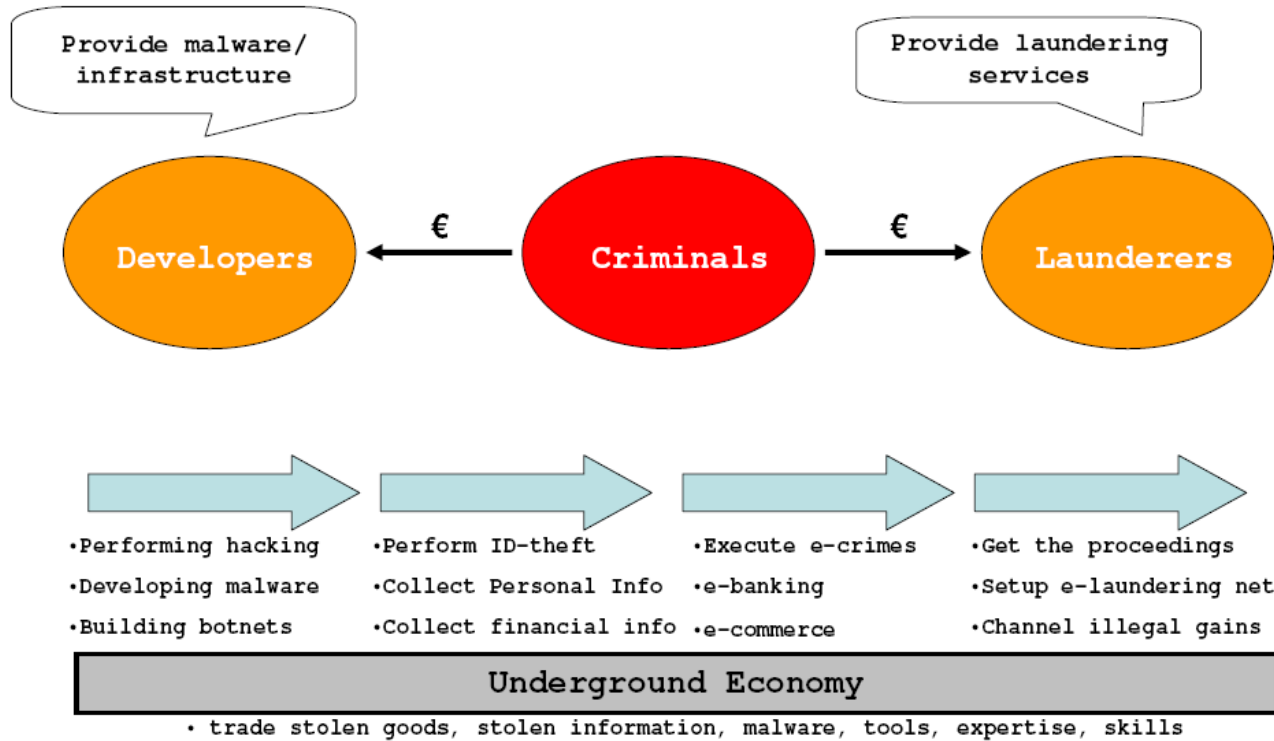


Quando il CO (crimine organizzato) incontra il Cybercrime

→ Approccio basato su «macro unità operative»



Cybercrime Business Model 2



Esempi (reali)

GATE 1: BATCH
 GATE 2: BATCH
 GATE 3: SINGLE
 GATE 4: SINGLE

Login: [Change password]
 Balance: 120 checks
 Show logo
 Logout

Limit: 119 check(s) for next 2999 second(s).

// We set limit for this gate in security reasons. All u have 150 checks per each hour.

Amount: \$ [0.10 - 0.95] Cost: 1 check.

Check track
 Format: NUMBER-YYMM, for example 4610460580687572-0506
 Accept VISA, MASTERCARD, AMEX.

371273886192008-1005060664964
 371273846882003-1104070416567
 5515729000423419-100410110000745
 5515380026683600-09031011000000922
 5513210544503786-08031010229914000000
 5514257100364201-08011010000082800000
 5466160009362430-1101101092010872
 5490990229735145-07111010000091900000
 5582508618140112-100310120000651
 5544581010679844-080710129490702
 4063170000275617-120510110000536
 4060260439306068-11111010000073000000
 4045940089488312-0901101066610000517
 4035330000150674-0803101100000006520

Use 'private' proxies ONLY // If u dont like 'public' ones and if u have your 'private' ones.
 Add Bank. Type and more info by bin.

Checked: 18 pcs

CC_number	Auth_code	Auth_result	Amount	Type 1	Type 2/Region	Bank	Country	State	City
371273886192008-1005060664964	[00]	APPROVAL	4.43						
4030620070042487-091210118050249	[00]	APPROVAL	7.78	Debit	PLATINUM	Sovereign Bank	United States of America	Pennsylvania	Wyomissing
5515729000423419-100410110000745	[00]	APPROVAL	1.81		USA	BANKERS BANK, THE		GEORGIA	ATLANTA
5466160009362430-1101101092010872	[00]	APPROVAL	3.93		USA	CITIBANK SOUTH DAKOTA, N.A.		NEW YORK	NEW YORK
4024115179688193-09021011206183902041	[00]	APPROVAL	4.18	Credit	GOLD/PREM	Fia Card Services, National Association	United States of America	Delaware	Wilmington
4081810509818498-0807101124820430705	[00]	APPROVAL	8.91	Credit	SIGNATURE	Chase Bank USA, National Association	United States of America	Delaware	Newark
4071141004744429-0910101000000000600	[00]	APPROVAL	1.88	Debit	PLATINUM	Bank of America, National Association	United States of America	North Carolina	Charlotte
4036330000150674-0803101100000000600	[00]	APPROVAL	0.15	Debit	CLASSIC	New Bedford Credit Union	United States of America	Massachusetts	New Bedford
4045940089488312-0901101066610000517	[00]	APPROVAL	2.91	Debit	CLASSIC	Metro Credit Union	United States of America	Massachusetts	Chelsea
4060260439306068-11111010000073000000	[00]	APPROVAL	7.89	Debit	CLASSIC	Northern Bank & Trust Company	United States of America	Massachusetts	Woburn
4063170000275617-120510110000536	[05]	DECLINE	8.27	Debit	CLASSIC	MerriMack Valley Federal Credit Union	United States of	Massachusetts	North Andover

Esempi (reali)

```
=====
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
Pasword      : 
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 (reali)

team2010
CVV MASTERS TEAM IS HERE FRESH LIVE
Global contacts:
ym: [redacted]
icq:554 [redacted]

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
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

US visa/US master \$2.5 Random

ITALY cc \$17

=====

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: \$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

=====

Esempi (reali)



WELCOME TO **GLAVMED**



A screenshot of the Canadian Pharmacy website. The top navigation bar includes links for 'Maison', 'Best-sellers', 'Tous les produits', 'FAQ', and 'Contactez-nous'. A shopping cart icon shows 'Votre panier: €0.00 (0 articles)'. A banner for 'AMAZING WEEKEND!' features a 'TIME LEFT: 01:46:29' and 'SPECIAL PRICES FOR ALL PRODUCTS'. The main content area is titled 'Liste de produit' and includes a search bar. Below the search bar, there are product listings for 'Yagara' (€30.01), 'Yashtemadhu' (€56.91), and 'Viagra + Cialis' (€66.50). A sidebar on the left lists 'Meilleures ventes' with categories like 'la Dysfonction érectile' and 'l'Amélioration de Sexe Masculin'. The bottom of the page has a green 'ORDER NOW' button and a suggestion section.

Esempi (reali)



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

\$146K USD/Week

EXTRA GIFT FOR YOU GUYS.... SURPRISE! ;)

Pavel Vrublevsky (RedEye)

GROUP IB



CEO of Chronopay,
a payment processing company

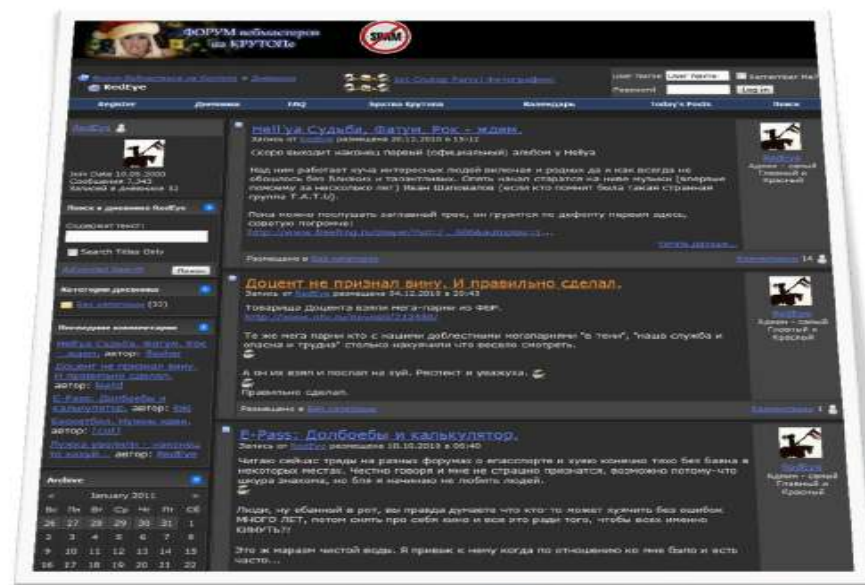


- ✓ Member of the Antispam Working Group at the Russian Ministry of Communication;
- ✓ Chairman of the Russian Committee on Electronic Commerce;
- ✓ Member of the Russian Association of Electronic Communications.

EXTRA GIFT FOR YOU GUYS.... SURPRISE! ;)

Pavel Vrublevsky (RedEye)

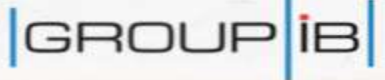
GROUP IB



Crutop.nu: the largest spammer forum

EXTRA GIFT FOR YOU GUYS.... SURPRISE! ;)

Pavel Vrublevsky (RedEye)



Pharmaceutical affiliate program:
Rx-promotion.com



EXTRA GIFT FOR YOU GUYS.... SURPRISE! ;)

DDoS Attack on Assist



ChronoPay Co-Founder Arrested



Hello there! If you are new here, you might want to [subscribe to the RSS feed](#) for updates on this topic. You may also [subscribe by email in the sidebar](#) ↗

60
tweets
TOP VOTED
retweeted

Russian authorities on Thursday arrested Pavel Vrublevsky, co-founder of ChronoPay, the country's largest processor of online payments, for allegedly hiring a hacker to attack his company's rivals.

Vrublevsky, 32, is probably best known as the co-owner of the [Rx-Promotion](#) rogue online pharmacy program. His company also consistently has been involved in credit card processing for — and in many cases [setting up companies on behalf of](#) — rogue anti-virus or "scareware" scams that use misleading PC security alerts in a bid to frighten people into purchasing worthless security software.



An undated photo of Vrublevsky.

Russian state-run news organizations [are reporting](#) that Vrublevsky was arrested on June 23. Financial Times reporter [Joe Menn](#) writes that Vrublevsky was ordered held without bail and a hearing was set for a month's time.

As I reported earlier this week, Vrublevsky [fled the country](#) after the arrest of a suspect who confessed that he was hired by Vrublevsky to launch a debilitating cyber attack against Assist, a top ChronoPay competitor. According to Russian news organizations, the ChronoPay executive wanted to sideline rival payment processing firms who were competing for a lucrative contract to process payments for Aeroflot, Russia's largest airline. Sources close to the investigation said Vrublevsky was arrested at the Sheremetievo airport outside of Moscow as he returned from a trip to the Maldives.

The arrest comes just 24 hours after authorities seized computers and servers in the United States and seven other countries this week as part of an ongoing investigation of a hacking gang that [stole \\$70 million via scareware scams](#)



Accused of organizing a DDoS attack on Assist, a payment processing company (Accused executor of the attack: Igor Artimovich)



Esempi (reali)



Esempi (reali)

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
<ol style="list-style-type: none">3 months unlimited support and virus definition base updatesOne computer licenceQuick scan. <p>Start to protect your computer with Antispyware Soft BASIC Quickly and easily!</p>	<ol style="list-style-type: none">6 months unlimited support and virus definition base updates.One computer licence.Advanced Deep Scanning. <p>Detect and stop viruses, spyware, adware, and other potentially unwanted programs before they can compromise or harm your desktops and laptops!</p>	<ol style="list-style-type: none">Lifetime warranty.Unlimited computers.Advanced Deep Scanning. <p>Buying this version, you obtain an ultimate protection. Since this day you can feel safe from Trojans, spywares, viruses, hacker attacks, adwares, keyloggers - all of them in past now. Antispyware Soft Platinum - Protection every second!</p>

Recentemente è stato incriminato un gruppo di cybercrooks autori di una campagna di Fake AV Fraud che secondo gli inquirenti ha fruttato circa **100 milioni di dollari.**

Esempi (reali)



Esempi (reali)



Perché siamo qui oggi?

Nel mese di dicembre 2015 il team di Security Brokers ha concluso un **progetto interno** il cui scopo era **analizzare i principali security incident e data breach** occorsi negli ultimi **dieci anni**, iniziando quindi dal 2004.

La lezione appresa **non è da poco**, e forse **sconvolge un po' il modus operandi e l'approccio mentale** ai quali siamo abituati oggi. Questa presentazione vuole **riassumere i punti cruciali emersi** e le **nuove logiche** che **dovremmo applicare** all'interno delle nostre organizzazioni **già nel corso di questo nuovo anno**.

I **settori di mercato** coinvolti nella ricerca sono diversi e molteplici, dal mondo **Accademico ed Universitario** all'**Energy, Banking & Finance, Gaming, Government, Healthcare, Media, Military, Retail, Tech, Telecoms, Transport e Web**.

Perché siamo qui oggi? /2

Il solo elenco sopra riportato basterebbe a **comprendere l'entità e la vastità della problematica**. Gli autori del rapporto da cui il team di lavoro ha iniziato la propria analisi hanno **distinto il "metodo di leak"** secondo i seguenti criteri: **Pubblicazione accidentale, Hacked, Insider, Computer perso/rubato, Media digitale perso/rubato, Scarsa sicurezza**.

Il team di Security Brokers ha invece voluto **effettuare un'analisi differente**, evidenziando i **macro-errori, procedurali e tecnologici**, che emergono da questa imponente mole di dati.

Durante l'intervento illustreremo anche le **soluzioni disponibili** - siano esse servizi che prodotti - e **confrontarci con i partecipanti**, informando il pubblico delle **novità "cutting-edge"** e dei **nuovi approcci per evitare di esporre** aziende ed organizzazioni ai **"rischi 2.0"**.



Cos'hanno in comune queste realtà?

**Non avevano la
minima idea di cosa li
avesse colpiti (non lo
sapevano nemmeno)**

**Nonostante avessero
speso milioni di euro
in Prodotti, Software
ed “i migliori
consulenti” ☹️**

Perché?

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.

Hackers Prefer Needling!!



Where on The Other Hand, You Need to Be Aware of EVERY New Spot a Hacker May possibly Stick A Needle ANYWHERE in YOUR Organisation ANYTIME.

**And You Need that Knowledge 24x7, With as Much Time as Possible to Take Preventive Action.
BEFORE you get hit!!**



**Si deve essere quindi coscienti
della propria **Attack Surface**,
essere “Timely Alerted” e
**comprendere i rischi e le minacce a
cui la nostra organizzazione è
esposta, ben prima che l’attacco
avvenga!****

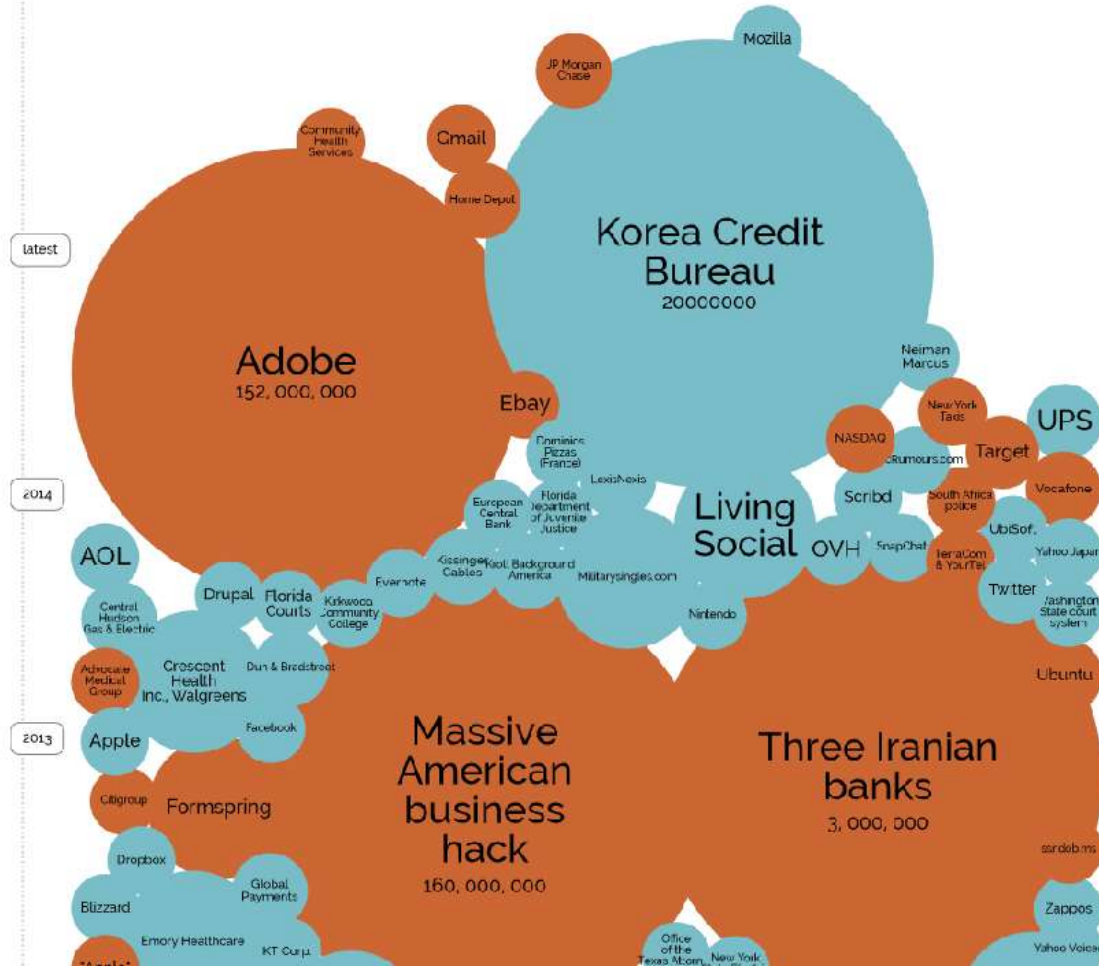
Data Breach

World's Biggest Data Breaches

Selected losses greater than 30,000 records

 interesting story

YEAR BUBBLE COLOUR YEAR METHOD OF LEAK BUBBLE SIZE NO OF RECORDS STOLEN DATA SENSITIVITY



Filter by...

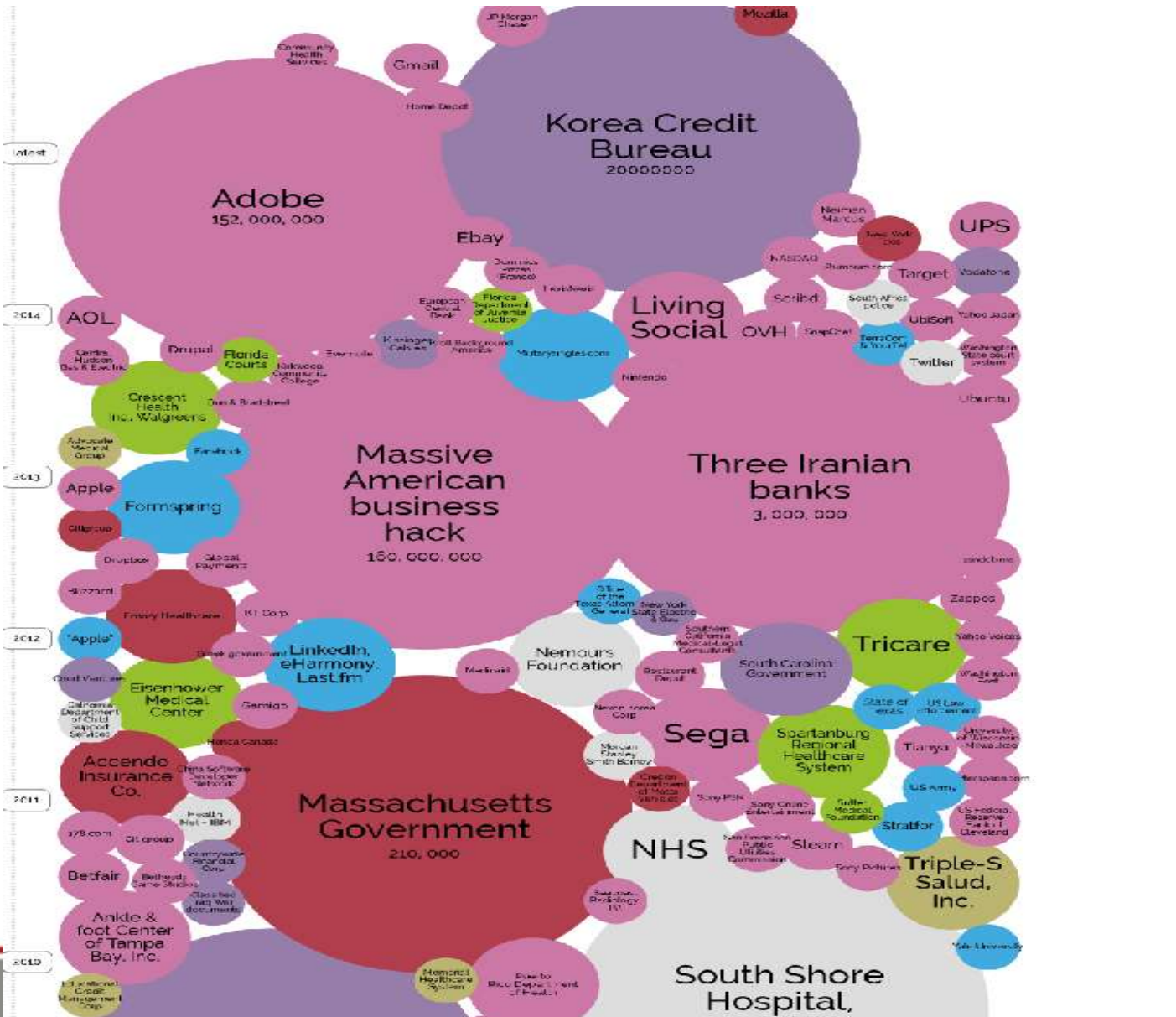
ORGANISATION

- all
- academic
- energy
- financial
- gaming
- government
- healthcare
- media
- military
- retail
- tech
- telecoms
- transport
- web

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

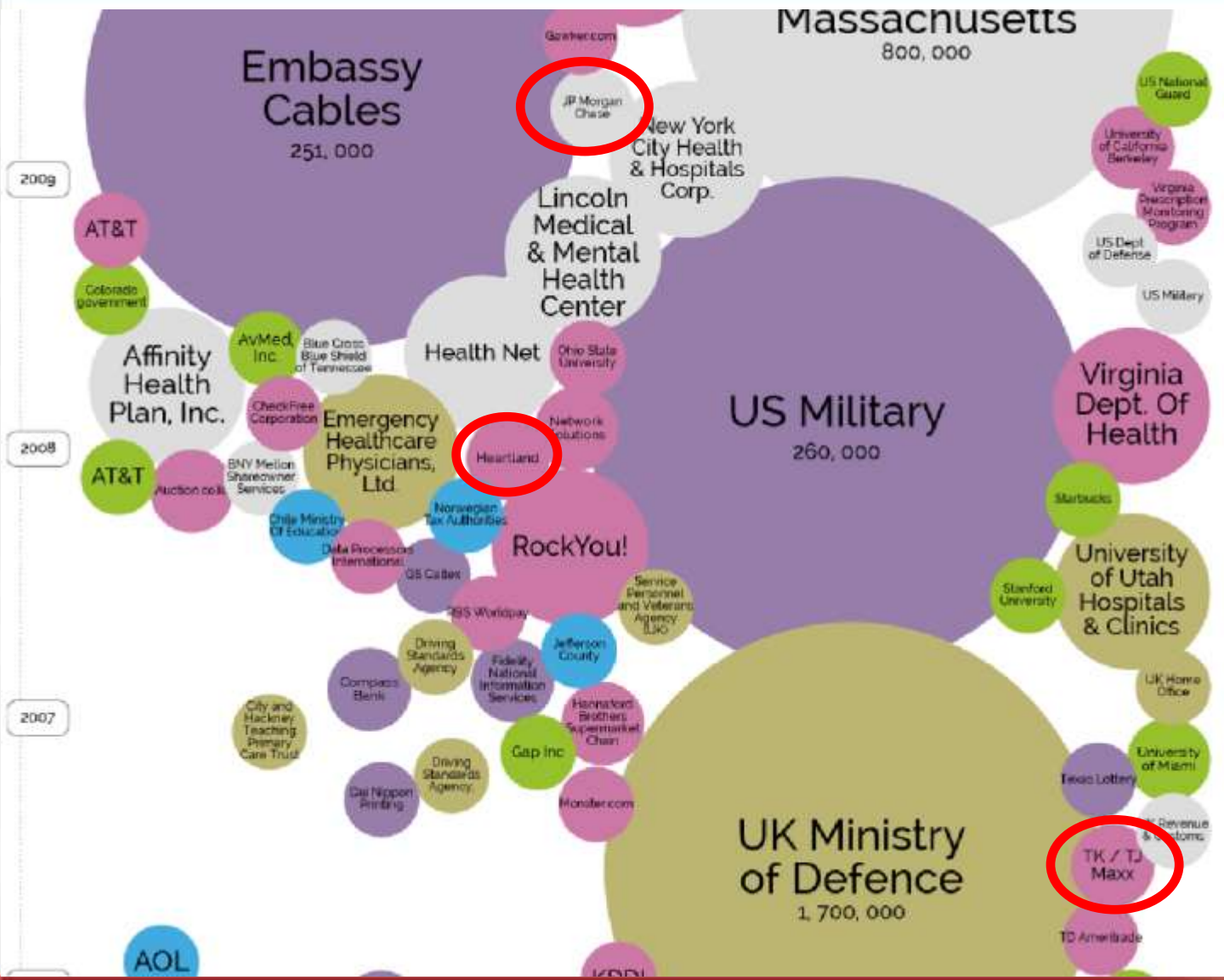
Ops... non era completa!



- Filter by...
- ORGANISATION**
- all
 - academic
 - energy
 - financial
 - gaming
 - government
 - healthcare
 - media
 - military
 - retail
 - tech
 - telecoms
 - transport
 - web
- METHOD OF LEAK**
- all
 - accidentally published
 - hacked
 - inside job
 - lost / stolen computer
 - lost / stolen media
 - poor security



Ops... non era completa!



Filter by...

ORGANISATION

- all
- academic
- energy
- financial
- gaming
- government
- healthcare
- media
- military
- retail
- tech
- telecoms
- transport
- web

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security



Ops... non era completa!



Filter by...

ORGANISATION

- all
- academic
- energy
- financial
- gaming
- government
- healthcare
- media
- military
- retail
- tech
- telecoms
- transport
- web

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

E la notizia di questi ultimi giorni

T H R E A T W A T C H

\$ \$ \$
FINANCIAL SERVICES

[Tweet](#)
[Share](#)
[Share](#)
[+1](#)

[Print](#)
[Email](#)

CYBERCRIMINALS POCKETED UP TO \$1 BILLION BY IMPERSONATING BANK OFFICERS

CREDENTIAL-STEALING MALWARE; CYBER ESPIONAGE; NETWORK INTRUSION; SOCIAL ENGINEERING; SPEARPHISHING; UNAUTHORIZED USE OF SYSTEM ADMINISTRATOR PRIVILEGES; USER ACCOUNTS COMPROMISED

Hackers wriggled spyware into bank computers to observe how employees ran the business, so they could make their fraudulent transactions look like normal operations.

The malicious software recorded every move of employees who process daily transfers and conduct bookkeeping. For months, the malware sent back video feeds and images to the criminal group, which comprised Russians, Chinese and Europeans.

Without detection, the crooks turned on various cash machines, and

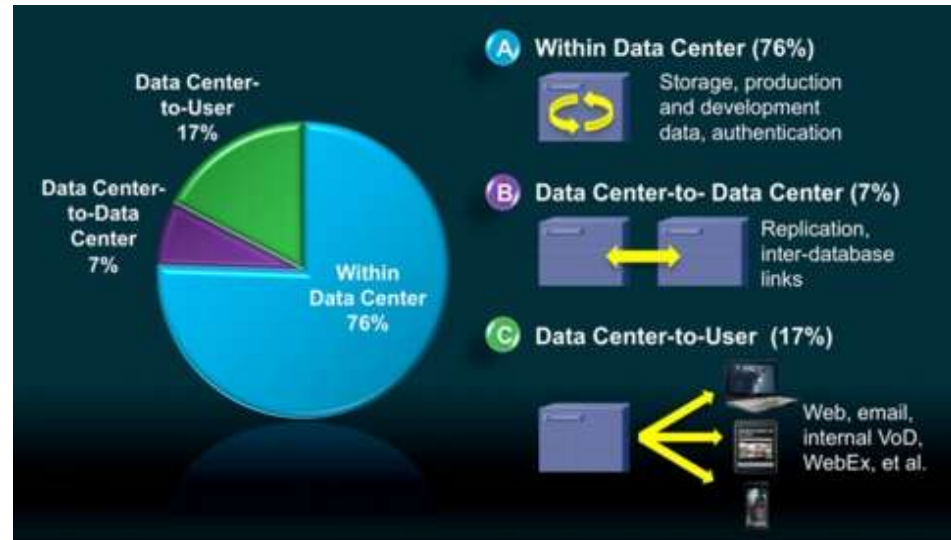
L'analisi

- * I «world's biggest data breaches» sono stati **così tanti**, dal 2004 ad oggi, che comunque **non stanno tutti su una pagina** 😞
- * I dettagli qui:
 - * <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- * Parliamo di una **escalation senza fine**
- * **Nessuno ne è indenne. Non più**
 - * Inoltre, **dipendiamo oramai troppo dal M2M**
- * **Informazioni = Potere**. Tramutabile in **denaro**, velocemente
 - * Il **danno conseguente** a queste violazioni è spesso **incalcolabile**
 - * Danno **Operativo**, di **Business**, di **Immagine**, **Economico** (**risarcimenti ai clienti, multe dalle Authority**).

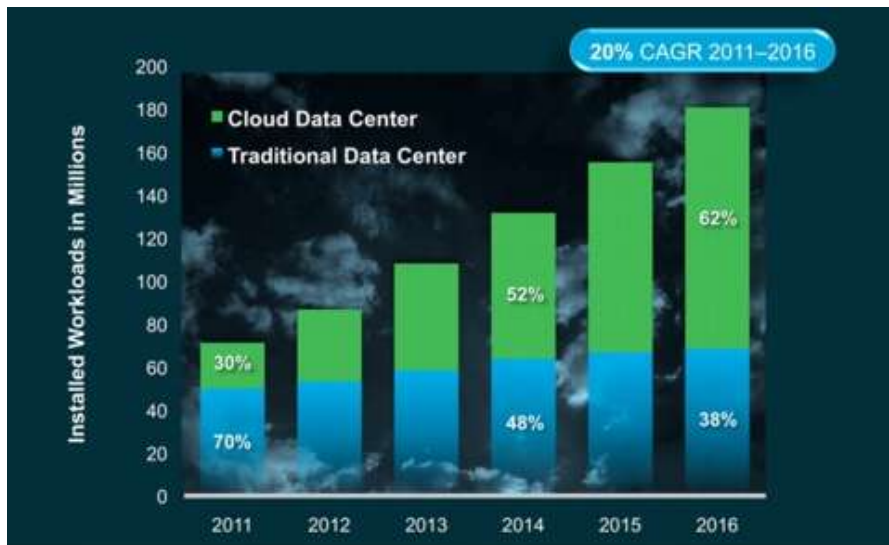
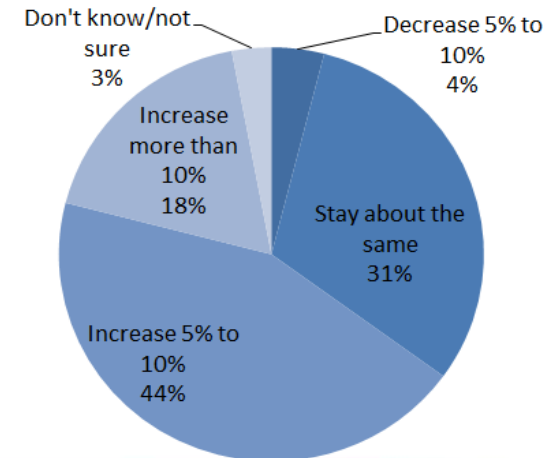
M2M, Cloud e connessioni «automatiche»

L'83% del traffico nei Data Center è M2M

I servizi Cloud portano maggiore automazione M2M



Business and operational process automation drives most machine-to-machine transactions. How do you expect your organization's machine-to-machine (M2M) transactions and processes will change in the next 12 months?



L'analisi /2

Con il mio team ho analizzato tutti questi data breach.

Le principali motivazioni del successo degli attaccanti sono riassumibili così:

- Carenze nell'esecuzione professionale delle Verifiche di Sicurezza (penetration test, ethical hacking, compliance check)
- Mancanza di segregazione delle rete dati interne
- **Assenza di una corretta gestione e centralizzazione delle connessioni SSH, interne ed esterne**
- **Assenza di strumenti per prevenire il Data Leak (DLP) su connessioni cifrate (tunnelling via SSH, exfiltration over SSL)**
- **Mancanza di corrette fonti di Cyber Intelligence (open e closed)**
- Mancanza di awareness interna sui dipendenti
- Assenza o totale carenza di strumenti, metodologie e formazione di Digital Forensics

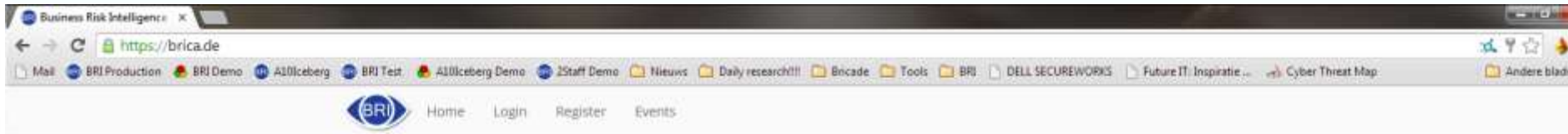
Cybercrime Intelligence (fonti aperte)

FORE-WARNED IS FORE-ARMED

An average soccer player runs to where the ball is.

A great soccer player runs to where the ball is going to be when he gets there.

Cybercrime Intelligence (fonti aperte)



BRI

BRI is a Global Threat Intelligence, Risk Awareness and Early Warning Service, alerting you on any new risk potentially affecting your infrastructure, assets, staff, board, confidential data, and your organizations' reputation.

Providing you with that precious awareness, knowledge and extra time to safeguard against and respond effectively to new threats your organization may be faced with.

Business Risk Intelligence & Cyberthreat Awareness

Your complete one-stop resource for Relevant, Focused, Timely and Actionable Risk Intelligence.

Business Risk Intelligence allows you to assume a more strategic position in the war against cybercrime. This allows you to better understand the threatscape, including attack trends and threat exposure. Resulting in recognizing attacks before they are happening in real-time and identifying new threats the moment they emerge.

Login to your Account

Email address

Password

Remember me

Note: both fields are case-sensitive.

Register

For more information, fill out this form and we'll contact you as soon as possible.

Name

Position

Organization name

Address

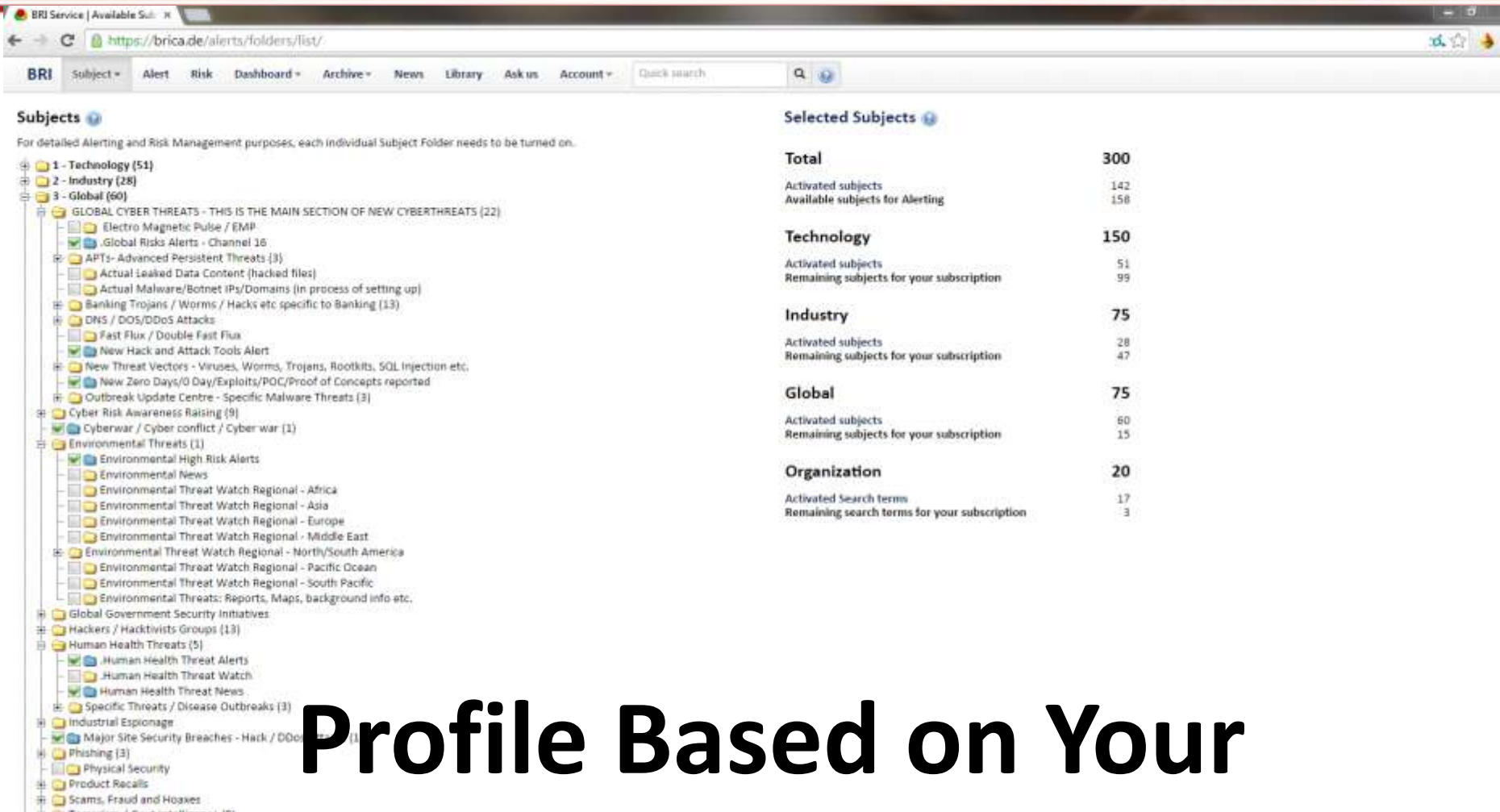
City

Cybercrime Intelligence (fonti aperte)

The screenshot displays the BRI Service website interface. At the top, there's a navigation bar with options like 'Subject', 'Alert', 'Risk', 'Dashboard', 'Archive', 'News', 'Library', 'Ask us', and 'Account'. Below this is a search bar and a 'Quick search' button. The main content area is titled 'Latest Generic Subjects And Updates' and shows 789,899 alerts available. The alerts are organized into three columns: Technology, Industry, and Global. Each alert includes a title, a brief description, and a timestamp indicating when it was posted. For example, in the Technology column, there's an alert about 'Malvertising Payload Targets Home Routers' posted 12 minutes ago. In the Industry column, there's an alert about 'U.S. Government Probes Medical Devices for Possible Cyber Flaws' posted 1 hour, 47 minutes ago. In the Global column, there's an alert about 'Liberia Says 4,465 Ebola Cases Have Been Recorded in the Country' posted 10 hours ago. On the right side of the page, there's an 'Updates' section with a mission statement, a 'FORE-WARNED IS FORE-ARMED' warning, and a list of 'New BRI Features' including changes to folder structures and the addition of new risk subject folders.

Be Warned on Relevant Threats, Emerging Issues

Cybercrime Intelligence (fonti aperte)



The screenshot displays the BRI Service web interface. On the left, a tree view shows a hierarchy of folders under 'Subjects'. The main section is 'GLOBAL CYBER THREATS - THIS IS THE MAIN SECTION OF NEW CYBERTHREATS (22)', which includes sub-folders like 'Electro Magnetic Pulse / EMP', 'Global Risks Alerts - Channel 16', 'APTs- Advanced Persistent Threats (3)', 'Actual Leaked Data Content (hacked files)', 'Actual Malware/Botnet IPs/Domains (In process of setting up)', 'Banking Trojans / Worms / Hacks etc specific to Banking (13)', 'DNS / DOS/DDoS Attacks', 'Fast Flux / Double Fast Flux', 'New Hack and Attack Tools Alert', 'New Threat Vectors - Viruses, Worms, Trojans, Rootkits, SQL Injection etc.', 'New Zero Days/0 Day/Exploits/POC/Proof of Concepts reported', 'Outbreak Update Centre - Specific Malware Threats (3)', 'Cyber Risk Awareness Raising (9)', 'Cyberwar / Cyber conflict / Cyber war (1)', and 'Environmental Threats (1)'. Other folders include 'Environmental High Risk Alerts', 'Environmental News', 'Environmental Threat Watch Regional - Africa', 'Environmental Threat Watch Regional - Asia', 'Environmental Threat Watch Regional - Europe', 'Environmental Threat Watch Regional - Middle East', 'Environmental Threat Watch Regional - North/South America', 'Environmental Threat Watch Regional - Pacific Ocean', 'Environmental Threat Watch Regional - South Pacific', 'Environmental Threats: Reports, Maps, background info etc.', 'Global Government Security Initiatives', 'Hackers / Hacktivists Groups (13)', 'Human Health Threats (5)', 'Human Health Threat Alerts', 'Human Health Threat Watch', 'Human Health Threat News', 'Specific Threats / Disease Outbreaks (3)', 'Industrial Espionage', 'Major Site Security Breaches - Hack / DDoS (1)', 'Phishing (3)', 'Physical Security', 'Product Recalls', and 'Scams, Fraud and Hoaxes'.

On the right, a 'Selected Subjects' summary table provides the following data:

Category	Total
Total	300
Activated subjects	142
Available subjects for Alerting	158
Technology	150
Activated subjects	51
Remaining subjects for your subscription	99
Industry	75
Activated subjects	28
Remaining subjects for your subscription	47
Global	75
Activated subjects	60
Remaining subjects for your subscription	15
Organization	20
Activated Search terms	17
Remaining search terms for your subscription	3

Profile Based on Your Infra-Structure and Industry

Cybercrime Intelligence (fonti aperte)

Subjects

For detailed Alerting and Risk Management purposes, each individual Subject Folder needs to be turned on.

- 1 - Technology (51)
- 2 - Industry (28)
- 3 - Global (60)
 - GLOBAL CYBER THREATS - THIS IS THE MAIN SECTION OF NEW CYBERTHREATS (22)
 - Cyber Risk Awareness Raising (9)
 - Cyberwar / Cyber conflict / Cyber war (1)
 - Environmental Threats (1)
 - Environmental High Risk Alerts
 - Environmental News
 - Environmental Threat Watch Regional - Africa
 - Environmental Threat Watch Regional - Asia
 - Environmental Threat Watch Regional - Europe
 - Environmental Threat Watch Regional - Middle East
 - Environmental Threat Watch Regional - North/South America
 - Environmental Threat Watch Regional - Pacific Ocean
 - Environmental Threat Watch Regional - South Pacific
 - Environmental Threats: Reports, Maps, background info etc.
 - Global Government Security Initiatives
 - Global Government Initiatives APEC
 - Global Government Initiatives EU / Europe
 - Global Government Initiatives DECD
 - Global Government Initiatives Other Countries/Economies
 - Global Government Initiatives UK
 - Global Government Initiatives UN
 - Global Initiatives - Global Impact
 - Global Intel / Government Initiatives USA
 - Government Encryption / PKI Initiatives
 - Hackers / Hacktivists Groups (13)
 - Human Health Threats (5)
 - Industrial Espionage
 - Industrial Espionage - Background Information and Reports
 - Industrial Espionage Alerts
 - Industrial Espionage News
 - Major Site Security Breaches - Hack / DDoS Attacks (1)
 - Phishing (3)
 - Physical Security
 - Product Recalls
 - Product Recall Alerts - Electronic and Business
 - Product Recall Alerts - General and Consumer
 - Scam/Fraud/News News
 - Scam/Fraud/News Alerts

Selected Subjects

Total	300
Activated subjects	142
Available subjects for Alerting	158
Technology	150
Activated subjects	51
Remaining subjects for your subscription	99
Industry	75
Activated subjects	28
Remaining subjects for your subscription	47
Global	75
Activated subjects	80
Remaining subjects for your subscription	15
Organization	20
Activated Search terms	17
Remaining search terms for your subscription	3

Intelligence on:
**Anything that May Negatively Affect the
Organization, People, Products,
Reputation & Shareholders**

BRICA: dati per decidere. In tempo

BRICA: dati per decidere. In tempo

BRICA Service | Awareness D...
https://brica.de/alerts/awareness/?alert_type=all

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

Latest Generic Subjects And Updates
785,904 alerts available.

Technology

- Android NFC hack allow users to have free rides in public transportation 38 minutes ago
- Malvertising Payload Targets Home Routers 1 hour, 9 minutes ago
- Android Ransomware Koler Self-Replicates via SMS, Targets Users in the US 1 hour, 23 minutes ago
- Android malware mutations on the rise 1 hour, 30 minutes ago
- Heads-Up - Koler 'Police' Ransomware Gets its Worm On 1 hour, 35 minutes ago
- China attacks lead Apple to alert users on iCloud threats 2 hours, 1 minute ago
- Mac Threats on the Rise: Five Tips to Stay Safe 2 hours, 30 minutes ago
- NOT OK GOOGLE: Android Images can conceal code 2 hours, 25 minutes ago
- 'Pieces of iPad' Giveaway Facebook Scam 2 hours, 27 minutes ago
- Clever Droptop Phishing Scam 2 hours, 41 minutes ago
- Memory leak in sanjaveinamekup (FreeBSD-SA-14:22.name) 2 hours, 42 minutes ago
- Koler worm spreads via SMS, holds users for ransom 2 hours, 44 minutes ago
- Owning Emmental - This operation is at compromising bank accounts 2 hours, 55 minutes ago
- 60% of Android attacks use financial malware 2 hours, 55 minutes ago
- BlackArch Linux 14.0 - New addition to Arch Linux for penetration testing 2 hours, 55 minutes ago
- CallStalk Hacker Breaches 19 HostGator Servers Amid Hong Kong Protests 2 hours, 57 minutes ago

Industry

- Apple grapple: Congress kills FBI's Cupertino crypto kybosh plan 6 minutes ago
- The Top Five NERC CIP Audit Fails 10 minutes ago
- ICO in Drone Camera Privacy Warning 27 minutes ago
- Is your phone line a '6-figure liability waiting to happen'? 1 hour, 18 minutes ago
- Laser hit plane with 118 passengers 1 hour, 29 minutes ago
- Android malware mutations on the rise 1 hour, 30 minutes ago
- Iranian citizens want access to the Windows Store but there is one little problem 1 hour, 53 minutes ago
- China attacks lead Apple to alert users on iCloud threats 2 hours, 1 minute ago
- Forex-Rigging Fines Could Hit \$41 Billion Globally: Citi 2 hours, 34 minutes ago
- U.S. Government Probes Medical Flaws 2 hours, 44 minutes ago
- U.S. Government Probes Medical Flaws 2 hours, 44 minutes ago
- China says it's hard to resume cyber talks 2 hours, 50 minutes ago
- The myth of Russian humiliation 2 hours, 52 minutes ago
- Owning Emmental - This operation is at compromising bank accounts 2 hours, 55 minutes ago
- 60% of Android attacks use financial malware 2 hours, 55 minutes ago
- The underworld of finance: Welcome to shadow banking 2 hours, 57 minutes ago

Global

- Android NFC hack allow users to have free rides in public transportation 38 minutes ago
- Malvertising Payload Targets Home Routers 1 hour, 9 minutes ago
- Is your phone line a '6-figure liability waiting to happen'? 1 hour, 18 minutes ago
- Android Ransomware Koler Self-Replicates via SMS, Targets Users in the US 1 hour, 23 minutes ago
- Android malware mutations on the rise 1 hour, 30 minutes ago
- Heads-Up - Koler 'Police' Ransomware Gets its Worm On 1 hour, 35 minutes ago
- Ebola outbreak can be contained within 6 months 1 hour, 59 minutes ago
- China attacks lead Apple to alert users on iCloud threats 2 hours, 1 minute ago
- Chinese APT groups targeting Australian lawyers 2 hours, 8 minutes ago
- 90% of Ebola investigations report caused by WHO officials 2 hours, 4 minutes ago
- Woman suffers facial Ebola track in Republic of the Congo 2 hours, 6 minutes ago
- Ebola in Belem, Brazil, But Not in a World of 7 Billion 22 minutes ago
- IT OK GOOGLE: Android Images can conceal code 15 minutes ago
- 'Pieces of iPad' Giveaway Facebook Scam 2 hours, 27 minutes ago
- Clever Droptop Phishing Scam 2 hours, 29 minutes ago
- Clash DropBox Phishing Scam 2 hours, 29 minutes ago
- Rocky warns of UAV threats 2 hours, 30 minutes ago
- 7 killed in Baghdad twin car bombings

Updates

Our Mission is Contributing to Creating a Truly Safe Internet for Everyone on this Planet

FORE-WARNED IS FORE-ARMED

Early Warning Actionable Risk Intelligence, enabling Pro-Active Risk Management. The best security practices start with looking for trouble, instead of waiting for trouble to find you.

New BRI Features

- Changes to folders structures - Moved folder - Banking Trojans / Worms / Hacks etc specific to Banking to: GLOBAL CYBER THREATS - THIS IS THE MAIN SECTION OF NEW CYBERTHREATS
- eBay and Amazon folders moved to Retail Breaches Parent (Industry-Retail Section)
- Function Enhancements - Main Page - Now shows as Default only the latest RED items. For checking other latest Yellow and/or Green, click on top-right.
- STIX Feed - You can now exactly specify what alert intel you want to pass through using your Stix feed. In the Menu Subjects-Selected you can specify what subjects can generate a Stix entry, and for what Criticality.
- New Risk Alert folders added - Most recent one first
- Supply chain compromise
- Western OSX Trojan
- Centreon - Systems Management Suite
- Chinese Origin attacking
- Pyw - Supply chain system
- Supply chain compromise in Tin-Tin Toy
- Clash DropBox Phishing Scam
- Clash DropBox Phishing Scam
- Clash DropBox Phishing Scam
- Android - New Android malware launching Nov 5th, threatening to target about a large org...

Green
Yellow
Red

- Nice To Know
- Need To Know
- Must Know Now!

BRICA: dati per decidere. In tempo

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

Selected subjects Technology (51) Industry (28) Organization (3) Global (60) News (2) Library (0)

Subject	Email	SMS	RSS	STIX	
BMC - Control / Patrol / AppSight etc.	All	On	All alerts	All alerts	Delete
Caldera Open Unix	No	Off	All alerts	All alerts	Delete
Checkpoint - Firewall-1, NG etc.	No	Off	Red and yellow only	None	Delete
Cisco Application-Oriented Networking (AON)	No	Off	All alerts	All alerts	Delete
Cisco AVS - Application Velocity Systems	No	Off	All alerts	All alerts	Delete
Cisco Enterprise License Manager	No	Off	None	All alerts	Delete
Cisco Ethernet Subscriber Solution Engine (ESSE)	No	Off	All alerts	All alerts	Delete
Cisco NetFlow Collector (NFC)	No	Off	All alerts	All alerts	Delete
Cisco Pix	Critical and important	On	All alerts	Red only	Delete
Cisco Prime Data Center Network Manager	All	Off	All alerts	All alerts	Delete
Cisco Service Control Engine	No	Off	All alerts	All alerts	Delete
Cisco Unity ICM CeM Building Broadband Service Manager etc.	Critical	Off	All alerts	None	Delete
Cisco User Registration Tool (URT)	No	Off	All alerts	All alerts	Delete
Cisco Wide Area Application Services (WAAS)	No	Off	All alerts	All alerts	Delete
CiscoWorks 2000 Service Management Solution (SMS)	No	Off	All alerts	All alerts	Delete
CiscoWorks LAN Management Solution (LMS)	No	Off	All alerts	All alerts	Delete
Comersus shopping cart	No	Off	All alerts	All alerts	Delete
Debian	Critical	Off	Red and yellow only	None	Delete
Digipix	No	Off	All alerts	All alerts	Delete
Digipix WebS	No	Off	All alerts	All alerts	Delete
FS Networks Application Optimisation / Availability Products	All except news	Off	All alerts	All alerts	Delete
FreeBSD / BSD	Critical and important	Off	All alerts	None	Delete
Gentoo Linux	Critical	Off	All alerts	All alerts	Delete
HP (HP-UNIX/HPV)	All	Off	All alerts	All alerts	Delete
IBM Lotus	All	Off	All alerts	All alerts	Delete
Juice	All	Off	All alerts	All alerts	Delete
Mandriva	No	Off	All alerts	Red and yellow only	Delete

**Alerts Method Selectable:
Email, SMS, RSS, XML, Stix**



BRICA: dati per decidere. In tempo

The screenshot shows the BRICA Alerts Dashboard interface. At the top, there's a navigation bar with 'BRI', 'Subject', 'Alert', 'Risk', 'Dashboard', 'Archive', 'News', 'Library', 'Ask us', and 'Account'. A search bar is also present. The main content is divided into three sections: 'Your incoming alerts', 'My Technology Alerts (256)', 'My Industry Alerts (655)', and 'My Global Alerts (1797)'. Each section contains a list of alerts with details like title, time ago, and action buttons (Connect to risk, Not applicable, New risk). The 'Your incoming alerts' section is partially obscured by a large text overlay.

Relevant Alerts to the BRI-Risk Management Module

BRICA: dati per decidere. In tempo

Modifying Risk Memory leak in sandboxed namei lookup (FreeBSD-SA-14:22.namei)

Alert: Memory leak in sandboxed namei lookup (FreeBSD-SA-14:22.namei)

Affects:
FreeBSD 9.1 and later.

Problem Description
The namei facility will leak a small amount of kernel memory every time a sandboxed process looks up a nonexistent path name.

III. Impact
A remote attacker ...

[expand](#)

More info: <http://www.freebsd.org/security/advisories/FreeBSD-SA-14%3A22.namei.asc>

Title: Memory leak in sandboxed namei lookup (FreeBSD-SA-14:22.namei)

Description: Check this out, make sure that we are safe!!! Report back this afternoon before 16.00 please

Risk type: Technology

Group:

Subgroup:

Owner: Company Master Account

CC Users:

Available Users	Chosen Users
<input type="text"/> Christian Ableguy Dirk Atabas Marie Ark Mark Etim Support Nathan E... Nelle Etw... Randal Iskofficer	Select your choices and click Otto peratingsystems Steven Ecurity

[Choose all](#) [Clear all](#)

Severity:

Planned completion date:

**Communicated and
Managed to Completion**

Cybercrime Intelligence (da fonti chiuse): mondo Finance, Large Corporate, e PMI

Powered by

IntelCrawler

Evoluzione del «perimetro»

- * Nel mondo dell'Information Security si chiama «**evoluzione del perimetro**».
- * E' la **conseguenza dell'evoluzione tecnologica e dell'impatto della c.d. «Digital Society»** sul mondo del business:
 - * BYOL (Bring Your Own Laptop)
 - * BYOD (Bring Your Own Device)
 - * Remote Working
 - * Remote Co-Working
 - * Social Networks
 - * Cloud
 - *

E-banking (botnet)

SLIDE NON DISPONIBILE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

E-banking (remote view via C&C)

SLIDE NON DISPONIBILE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

E-banking (remote view via C&C)

SLIDE NON DISPONIBILE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

Cards, POS, NFC

SLIDE NON DISPONIBILE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

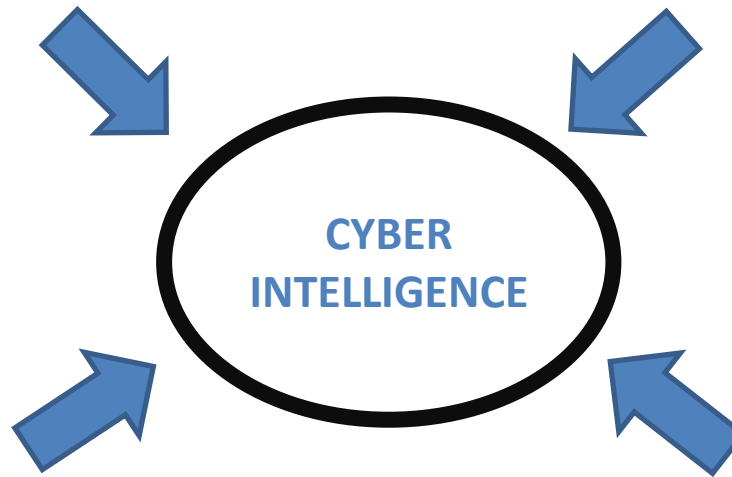
Cards, POS, NFC

SLIDE NON DISPONIBILE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

Operative Cyber Intelligence

Cybercrime Intelligence – Una Piattaforma di Intelligence che ha raggiunto ed ha accesso ad oltre **1 milione di “nicks”, 50 milioni di posts, e centinaia di milioni di cyber prints.**

Malware Intelligence – Il Virtual Sandboxing Environment offre l'opportunità di analizzare campioni di malware ed i correlati “cyber prints”, e **confrontarli con altri database e fonti.**



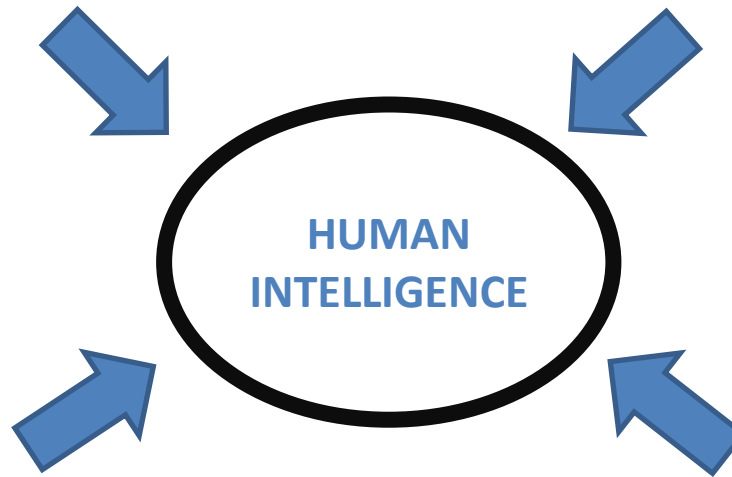
Network Intelligence – Nel corso degli anni abbiamo scansato ed analizzato l'**intera classe di IPv4** per monitoraggio di spam, reverse search, malware ed exploits sources per mitigare il rischio e prevenire le minacce.

Threat Intelligence – I nostri clienti ricevono **notifiche e alert di Intelligence quotidianamente** dai nostri Centri e forniamo **risposte tempestive alle richieste personalizzate.**

Operative Human Intelligence

Strong Know-how – Profonda conoscenza e penetrazione nel **mondo Asiatico** ed **Arabo** per ricercare, valutare, analizzare, fare merging ed interpretare **Intelligence da multiple e diversificate fonti**.

Malware Intelligence – Permette di essere la **risorsa chiave nelle prime fasi** di un potenziale **crimine informatico** o di una **campagna di attacco mirato**. Capacità di iniziare le operazioni in **pochissimi secondi**.

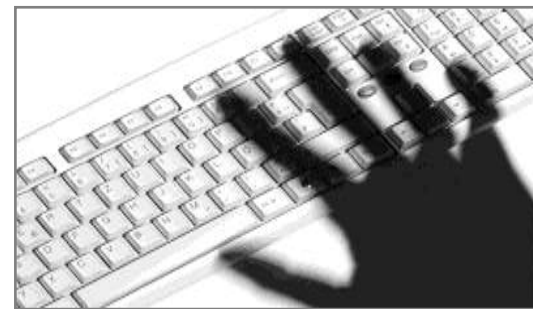


Underground Intelligence – Cyber Intelligence, Threat Intelligence e varie tattiche di infiltrazione, insieme alle **tecnologie di Context-Aware Intelligence** creano in modo efficace una **Agenzia Privata di Intelligence** per i nostri clienti.

Fast relocation – Immediato e veloce **trasferimento delle informazioni** sul posto dell'incidente in modo che il cliente possa effettuare **controlli di sorveglianza** ed **assistenza tecnica** da eseguire fisicamente (on-site).

Operative Signal Intelligence

- * SIGINT capabilities **proprietarie ed autonome**.
- * Aggregiamo **flussi di dati** raccolti tramite le nostre stazioni SIGINT posizionate in **differenti parti del mondo**, combinandoli con le **analisi operative** e le informazioni di **Botnet Intelligence**.
- * Approfondita esperienza nelle **intercettazioni satellitari (VSAT)** e **valutazione della sicurezza delle telecomunicazioni** per scopi di Intelligence.



Powered by

IntelCrawler

Cyber Intelligence (da fonti chiuse): what you get?

Powered by

IntelCrawler

Mercato Finance: deliverables

* Anti Money Laundering Intelligence feed

Monitoraggio di migliaia di organizzazioni ed individui coinvolti in attività fraudolente e riciclaggio di denaro in tutto il mondo.

Avere accesso ai feed mette in sicurezza il vostro business e previene i rischi da attività di riciclaggio (Money Mules per il mercato Banking, Gambling, Pharmacy, etc).



* Triple «C» feed

Feed sulle liste di Carte di Credito Compromesse che vengono «scovate» nei Black Market e nel Digital Underground e pronte ad essere utilizzate in modo fraudolento.



* POS feed

Feed sui POS o reti POS compromessi, informando sul numero approssimativo di Carte di Credito compromesse, geo-localizzazione grafica e gli Indirizzi IP dei terminali infettati, siano essi POS, Totem, etc.

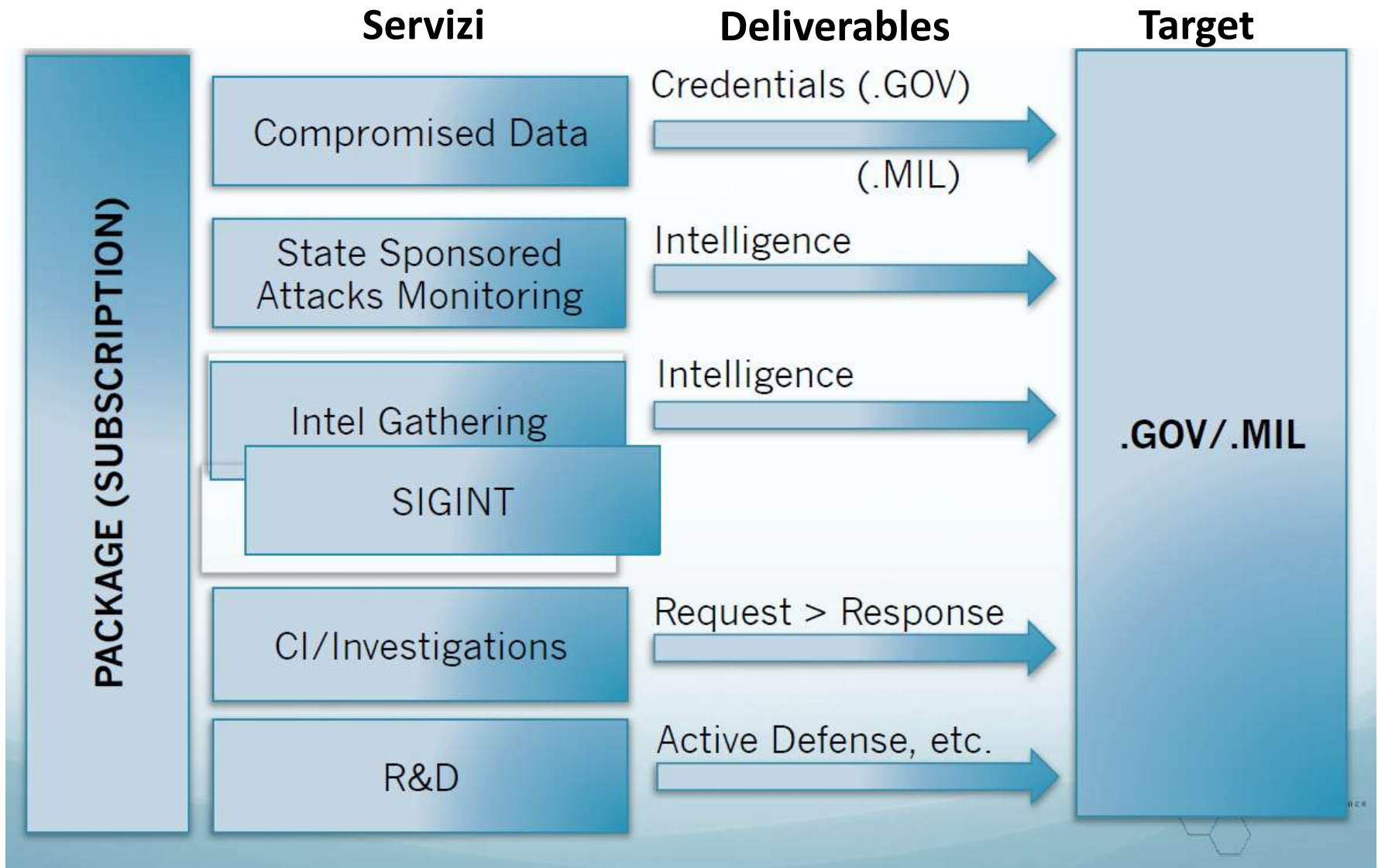


Powered by

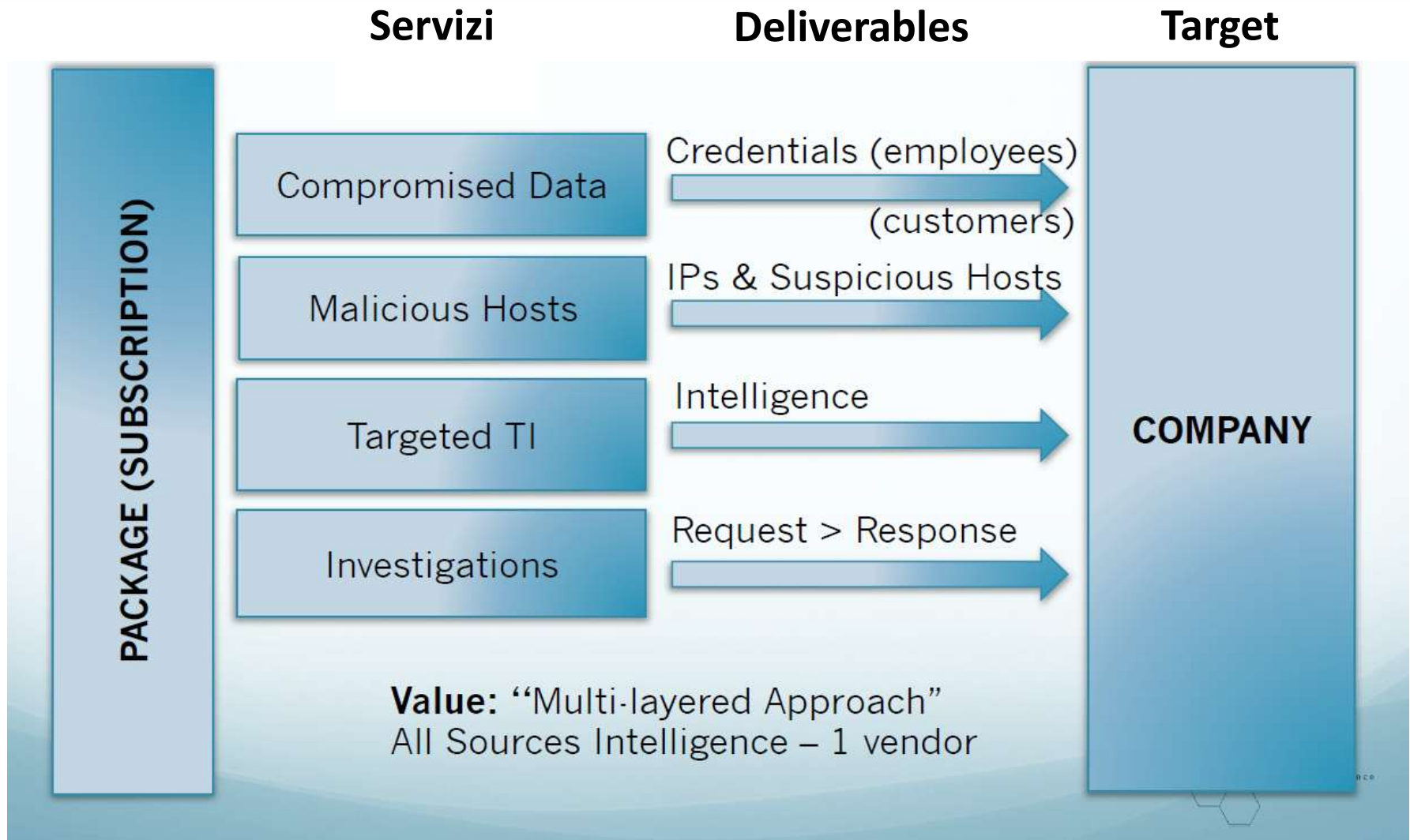
IntelCrawler



Difesa e Governo



Altri mercati verticali



Andiamo on-line a “toccare con mano”...

Contacts, Q&A

* **Raoul Chiesa**

rc [at] security-brokers [dot] com

* Ing. **Selene Giupponi** (Digital Forensics Unit)

sg [at] security-brokers [dot] com

* Ing. **Mauro Salvau** (Cyber Intelligence & Prodotti SSH)

ms [at] security-brokers [dot] com

DOMANDE?



EXTRA MATERIAL



Encryption: The Next Advanced Cyber-Weapon

Copyright 2014 SSH Communications Security

TorinoIN - 16 Febbraio 2016



Chi è «SSH Secure Communications»

- * E' l'azienda che ha **creato il protocollo Secure Shell (SSH)**
- * **Contributori leader** negli standard aperti (open standards):
 - * Leading authors di 5 RFCs
 - * Influencers verso 98 RFCs
 - * Autori delle Best Current Practices per Secure Shell identity Management presso l'IETF (Internet Engineering Task Force)
- * Oltre **3,000 clienti in tutto il mondo**, incluse 7 delle aziende presenti in Fortune 10
- * Insieme a loro, proponiamo un **approccio platform-based** di Secure Shell per lo Sviluppo, la Gestione, il Monitoring e la Data Loss Prevention



In Business Since 1995

Alcuni Clienti SSH

Energy & Utilities



Government



Financial



Retail



Healthcare



Secure Shell - utilizzo

- * **Secure login** ai sistemi remoti (sostituisce il Telnet)
- * **Secure File Transfer** (sostituisce FTP)
- * **Secure Command Execution** su sistemi remoti (sostituisce rsh)
- * **Secure Backup & Copy**
- * **Secure tunneling** di applicazioni TCP insicure e già esistenti
- * **Application proxy e VPN**

Le «gold questions»

1. Sapete *quali* utenti hanno accesso *a che cosa* sulle **vostre reti encrypted**?
2. Potete identificare le **relazioni di trust** (*key pairs*) in essere presso la vostra struttura?
3. Le vostre **procedure di creazione** delle chiavi sono **centralizzate e controllate**?
4. **Rimuovete** le chiavi?
5. Effettuate la **rotazione** delle chiavi?
6. Siete in grado di fornire un **compliance report**?

Encryption: a double-edged sword

Used for good:

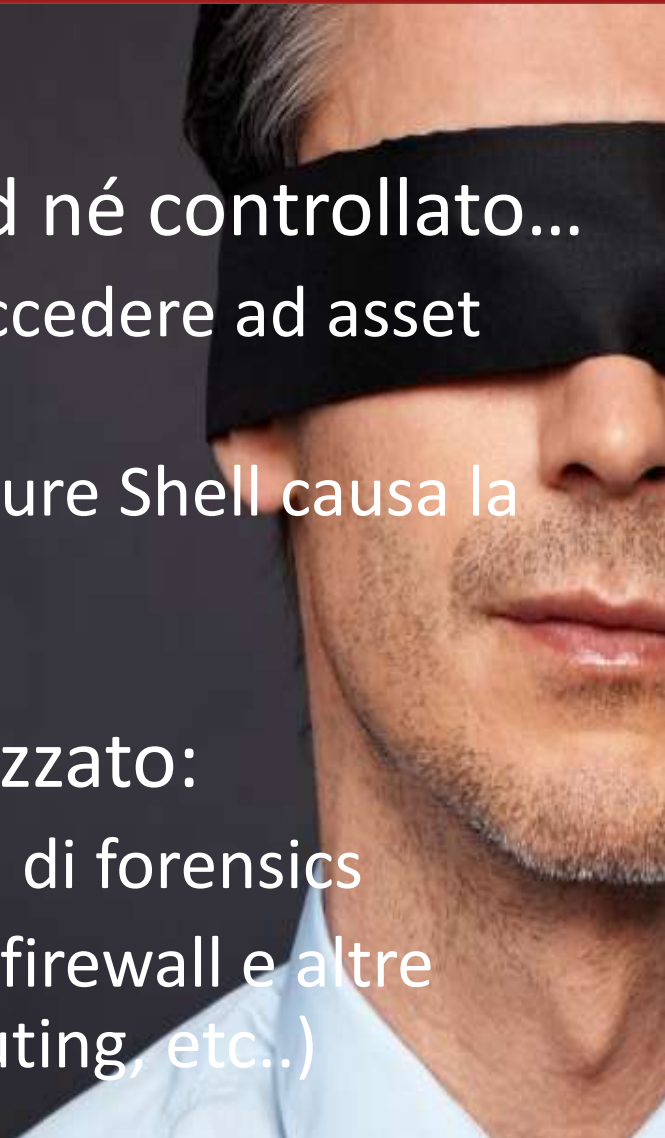
- * Prevenzione degli attacchi Man-in-the-Middle
- * Lo strumento preferito per l'amministrazione remota
- * Securizza le comunicazioni point-to-point
- * Securizza le connessioni M2M automatizzate



Encryption: a double-edged sword

Used for bad:

- * Quando l'accesso non è managed né controllato...
 - * Permette ai malicious insiders di accedere ad asset informativi critici
 - * La perdita o il furto delle chiavi Secure Shell causa la compromissione delle identità
- * Quando l'accesso non è monitorizzato:
 - * «Accieca» le security ops ed i team di forensics
 - * Permette agli attacker di aggirare i firewall e altre politiche di restrizione (accessi, routing, etc..)

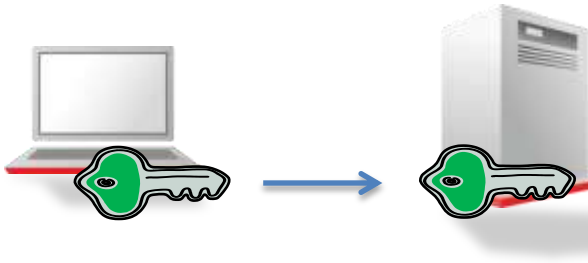


Perché «SSH» è una security issue?

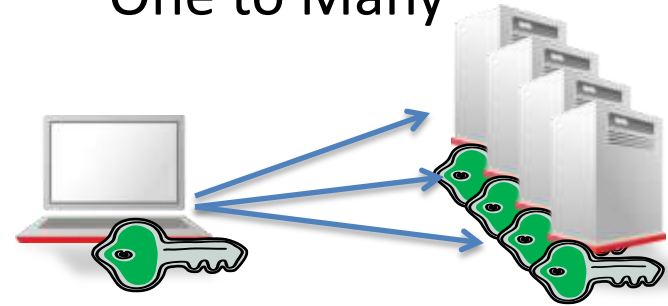
- * Storicamente, la Security e gli Audit **non hanno mai posto troppa attenzione** alle connessioni Secure Shell.
 - * L'**errore psicologico**: “Secure Shell fornisce login sicuri e traffico cifrato = controlli migliori = non c'è bisogno di ulteriori verifiche”;
 - * **Nessuna o poca attenzione** sulle implicazioni nell'identità e nell'Access Management delle *User Keys* di Secure Shell.
- * **Se non propriamente gestite**, le *User Keys* di Secure Shell possono **danneggiare significativamente i controlli di accesso** ai sistemi informativi dell'azienda ed introdurre **rischi di sicurezza notevoli**, che **non possono essere sottovalutati**.
- * Alcuni degli scenari nelle prossime slide vi aiuteranno a **comprendere la drammaticità** di quanto sopra.

Le chiavi creano *Relazioni di Trust*

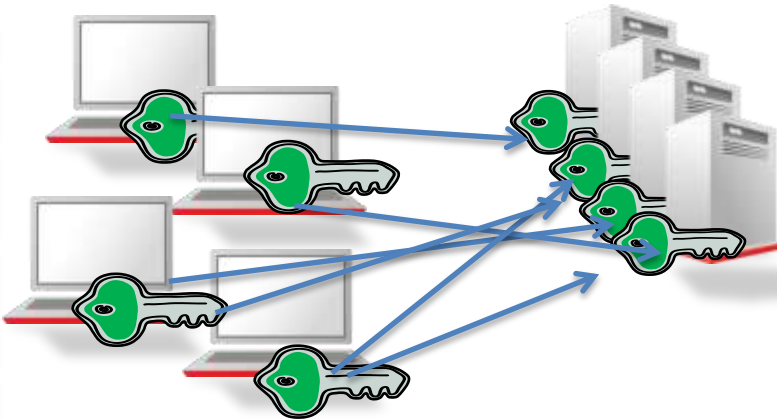
One to One



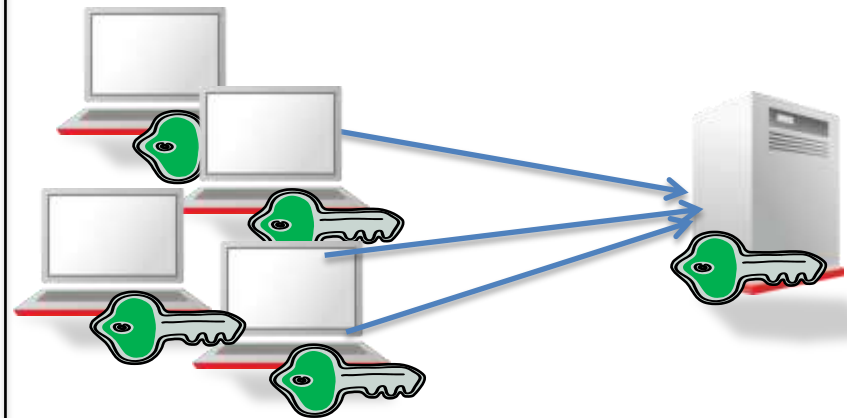
One to Many



Many to Many

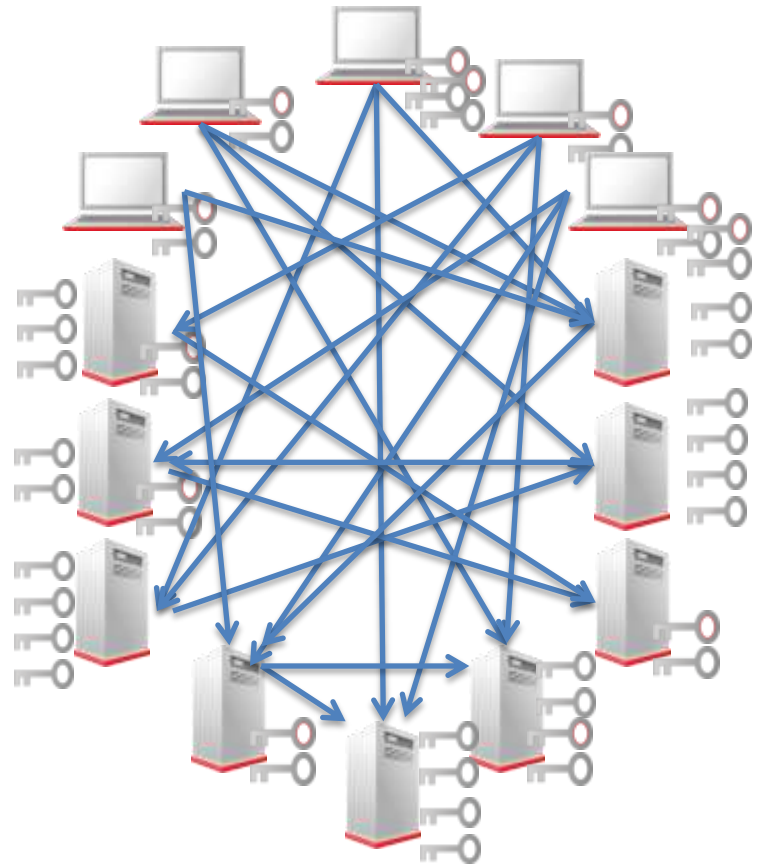


Many to One

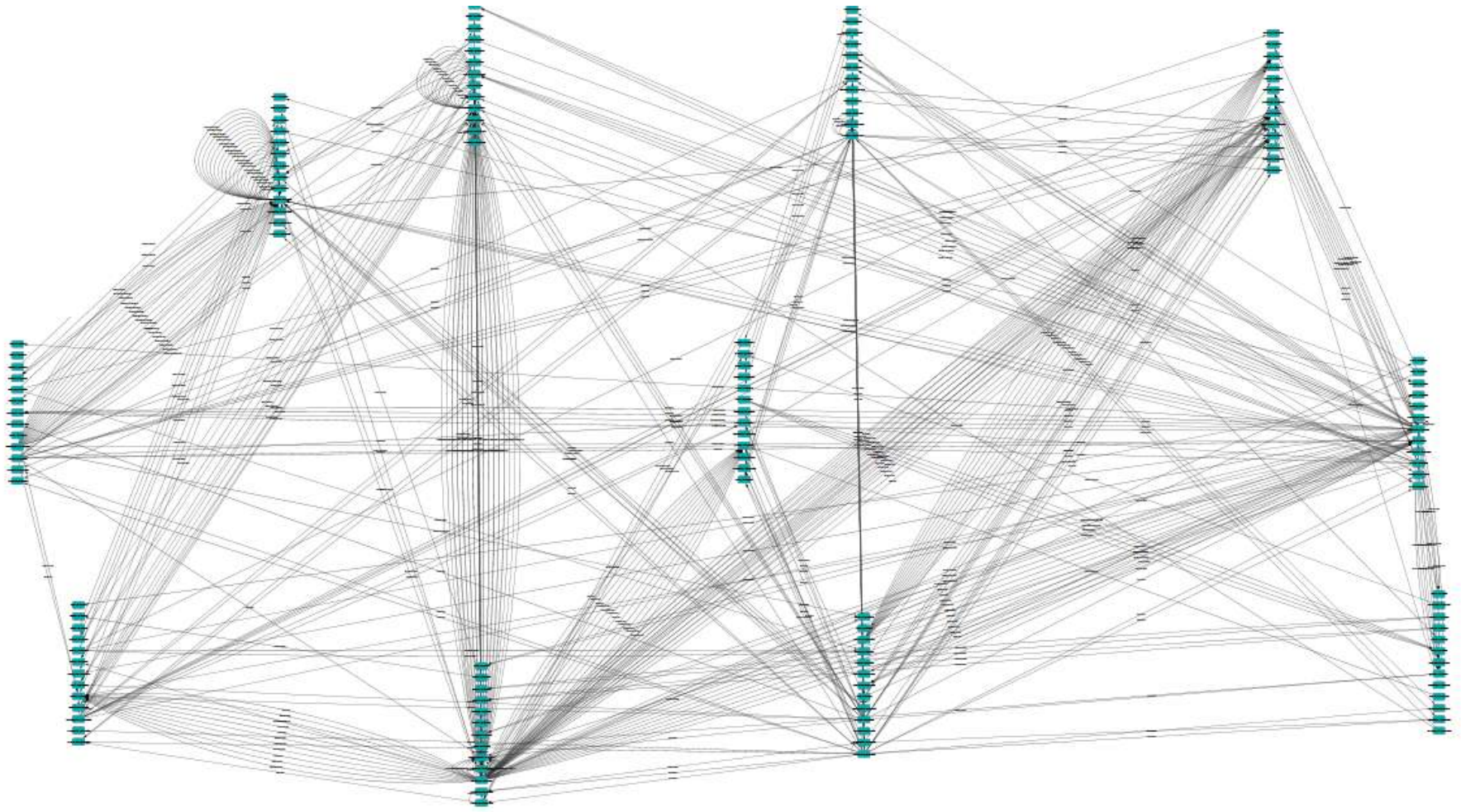


Situazioni tipiche a livello Enterprise

- * **Nessuna visibilità** su *chi accede a quali server Secure Shell*, siano essi *Utenti Privilegiati* o **Account di Applicazioni**.
- * **Nessun** strumento o metodo per **rimuovere le chiavi**.
- * **Nessun** strumento o metodo per **restringere o ruotare le Private Keys**.
- * **Errori nei setup manuali** e nella **manutenzione**.

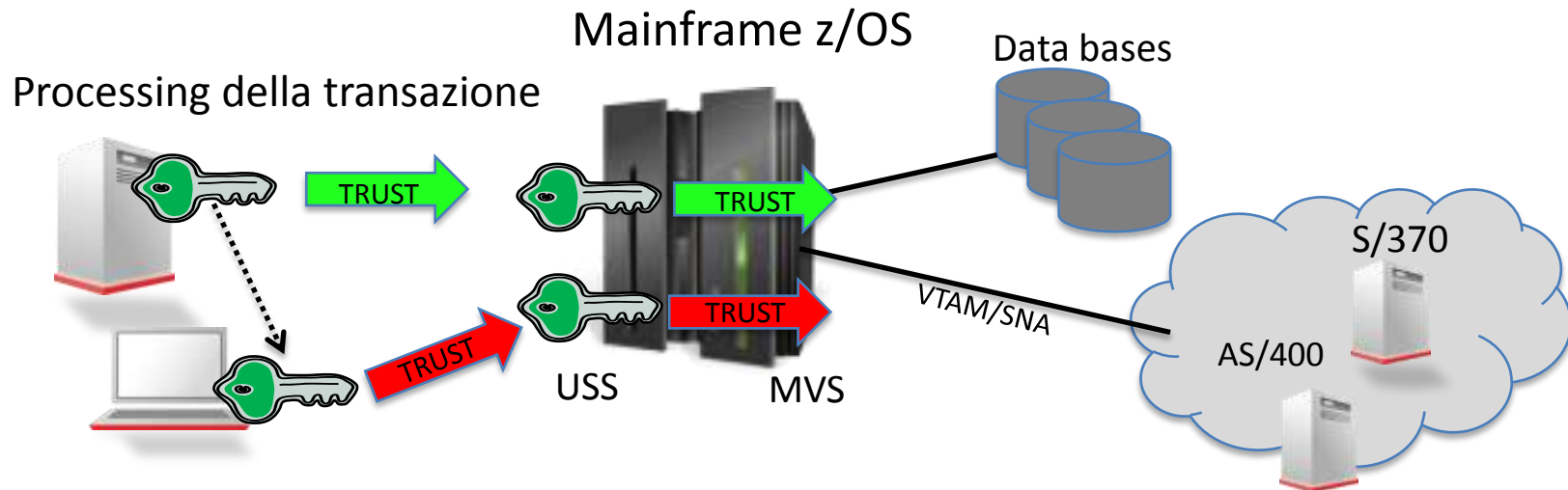


Ciò che (probabilmente) avete in casa...



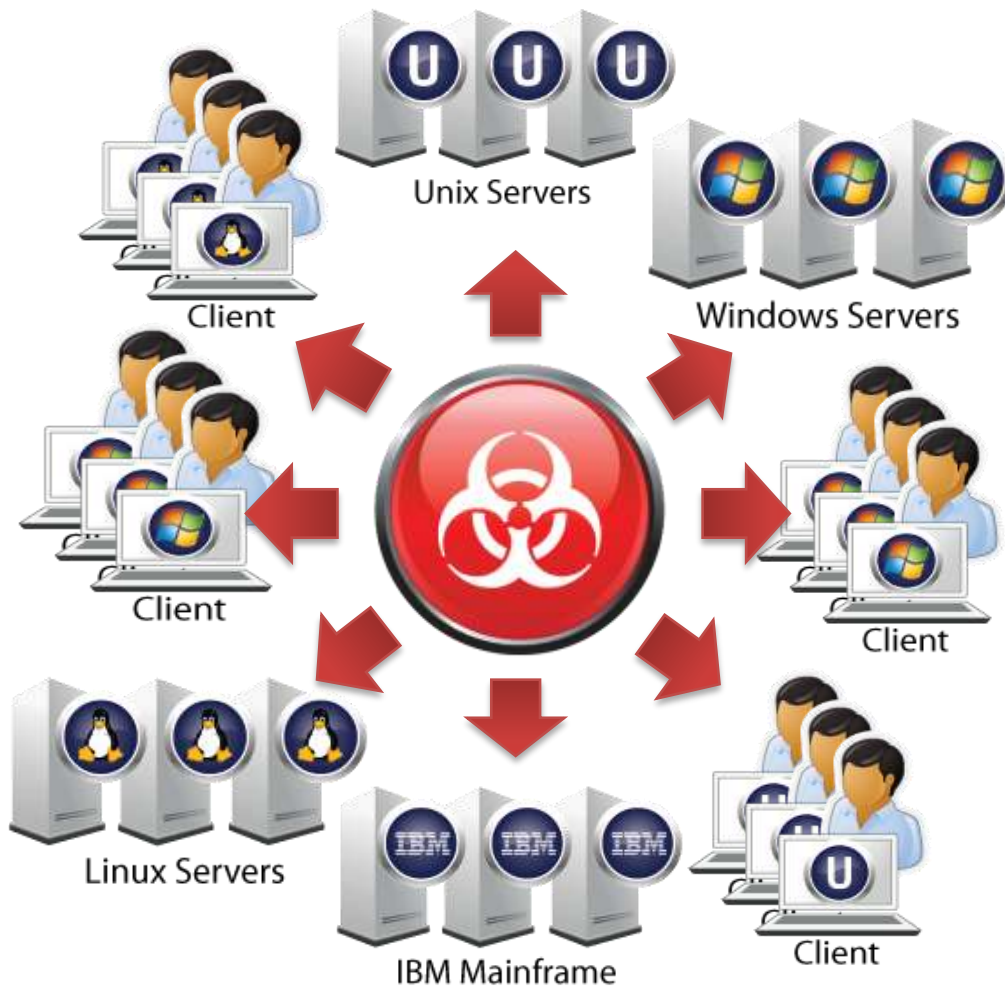
Visualizzazione delle trust relationships su 100 hosts SSH in uno dei network di un nostro Cliente.

Backdoors nei Mainframe



- La *Public Key* abilita l'accesso automatico per il processing della transazione nell'ambiente dei mainframe IBM.
- La copia della *Public Key* viene spostata su un'altra directory utente directory in USS.
- La *Public Key* permette al detentore remote della *Private Key* di loggarsi come quell'utente sull'USS e di accedere al MVS, senza passare dal RACF.

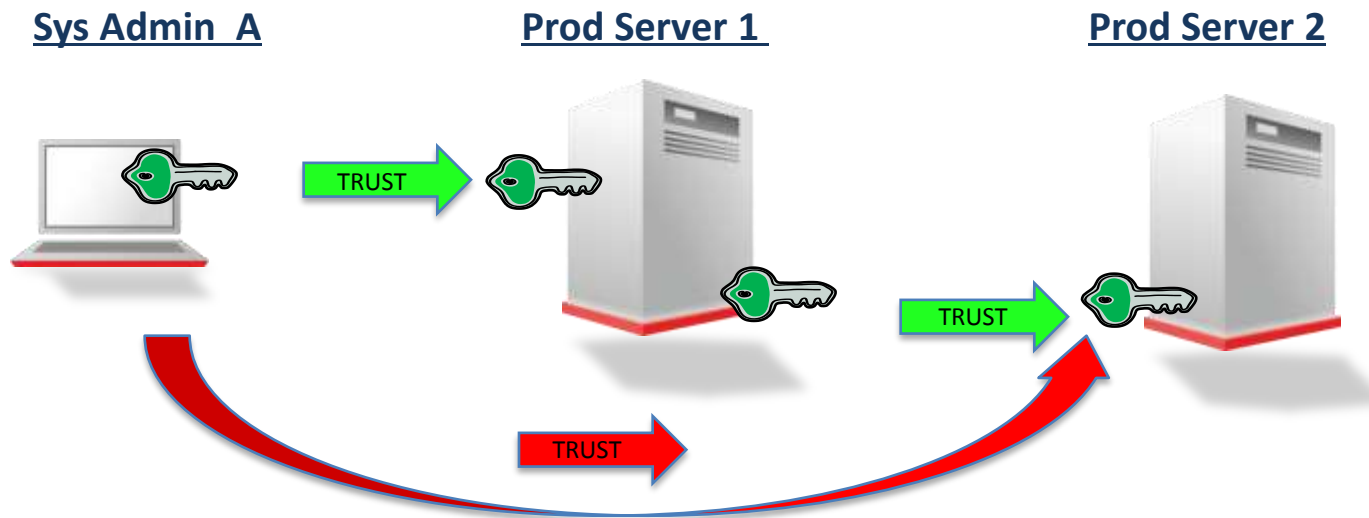
Minaccia da Malware o Cyber Weapon



- La maggior parte delle aziende ha in media **da 8 a più di 100** chiavi SSH, configurate per garantire l'**accesso sicuro** ad ogni server Unix, Linux e Mainframe.
- Queste chiavi spesso offrono **accessi e diritti amministrativi** di tipo "elevato".
- L'insieme di accessi key-based è così denso **da rendere altamente plausibili** scenari nei quali **un attacco si può diffondere praticamente a tutti i server dell'azienda**.
- I **rischi aumentano sostanzialmente** se il malware utilizza anche altri vettori di attacco per scalare a "root" (massimo livello di amministrazione) dopo aver violato il server "entry point".

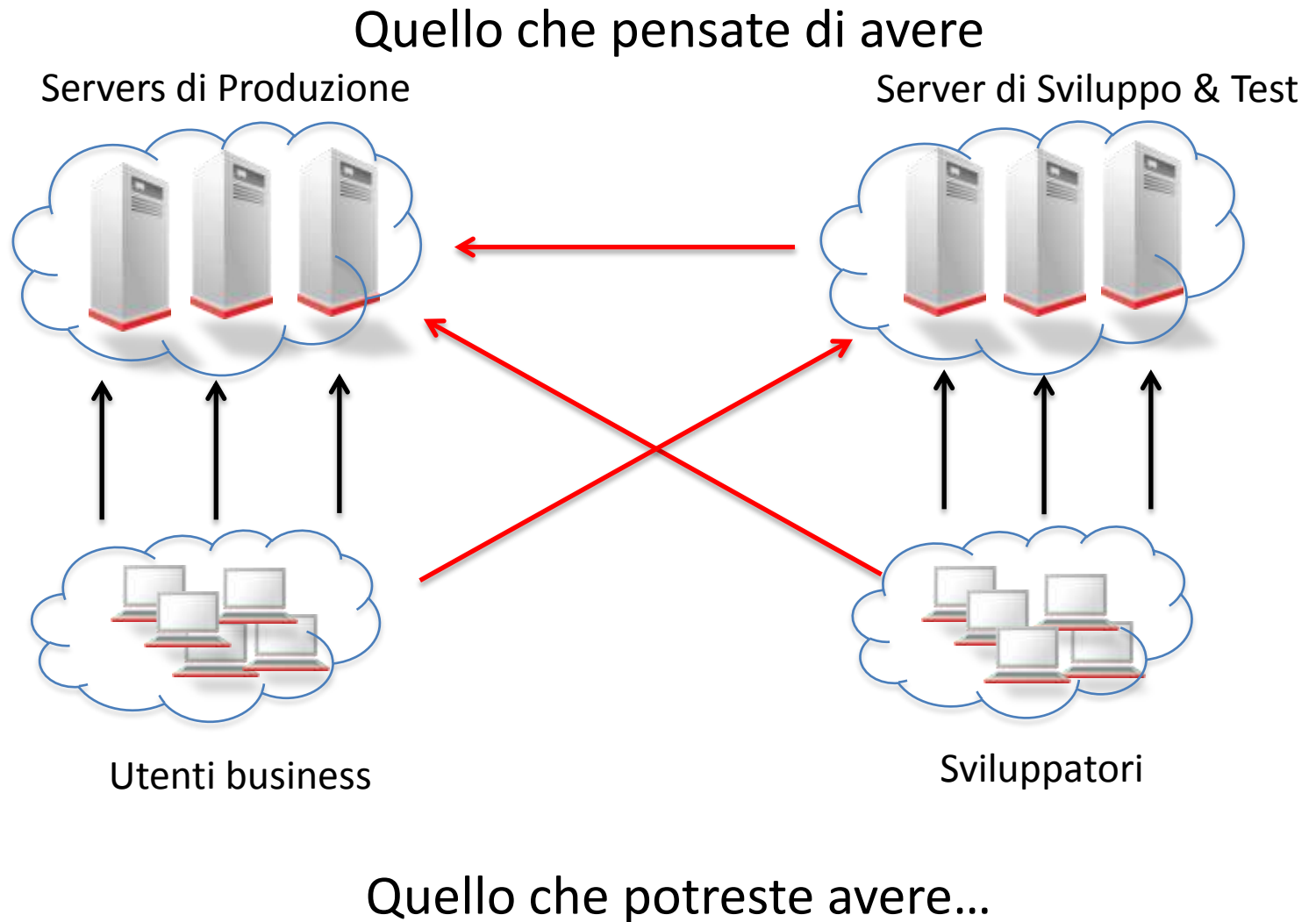
«Transitive Trust»

Transitive Trust

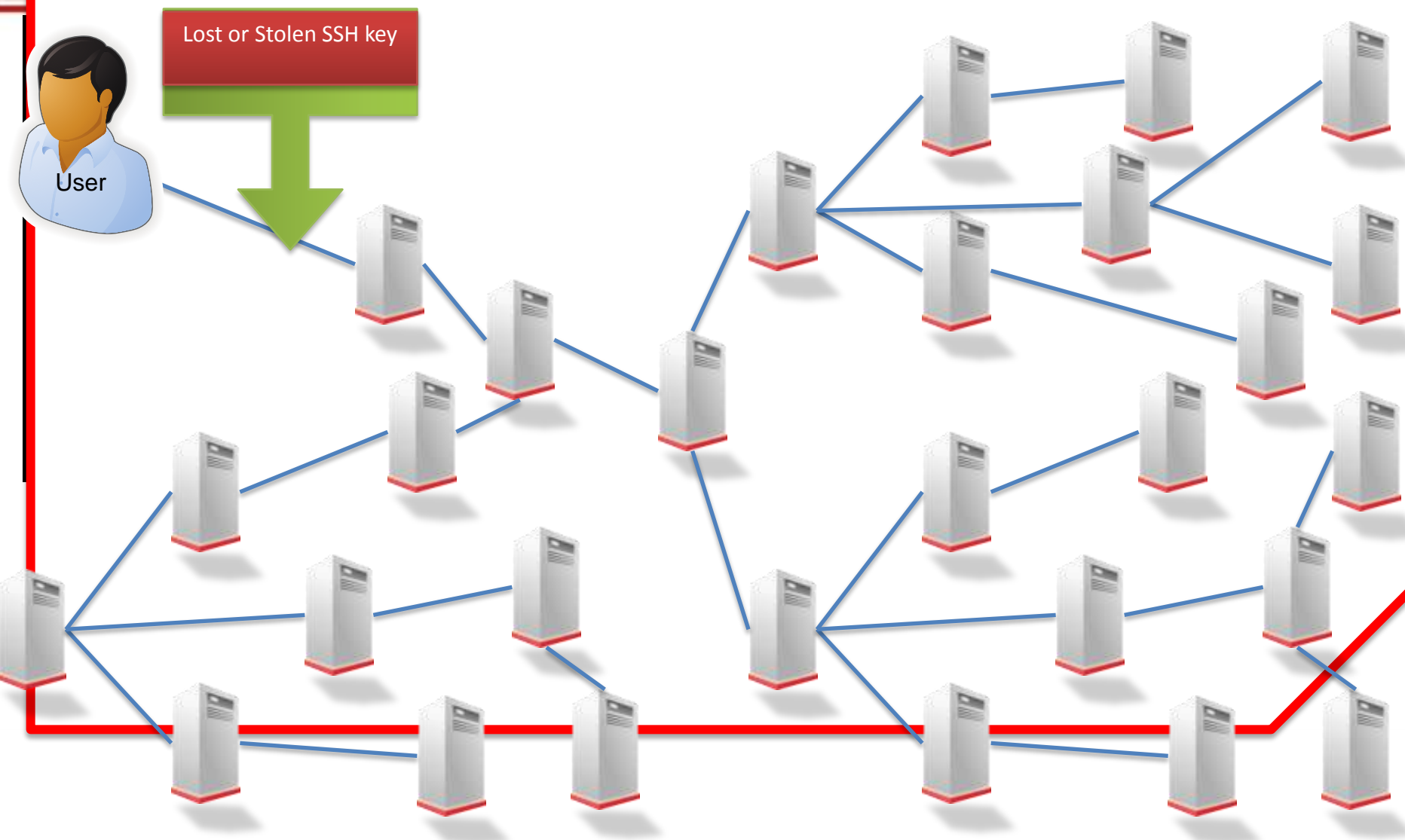


- Sys Admin A is authorized to login as root to Prod Server 1 but not Prod Server 2
- Prod Server 1 is authorized to initiate sftp secure file transfers on Prod Server 2
- Sys Admin A can initiate sftp file transfers on Prod Server 2 by logging in Prod Server 1

Segregation of Duties

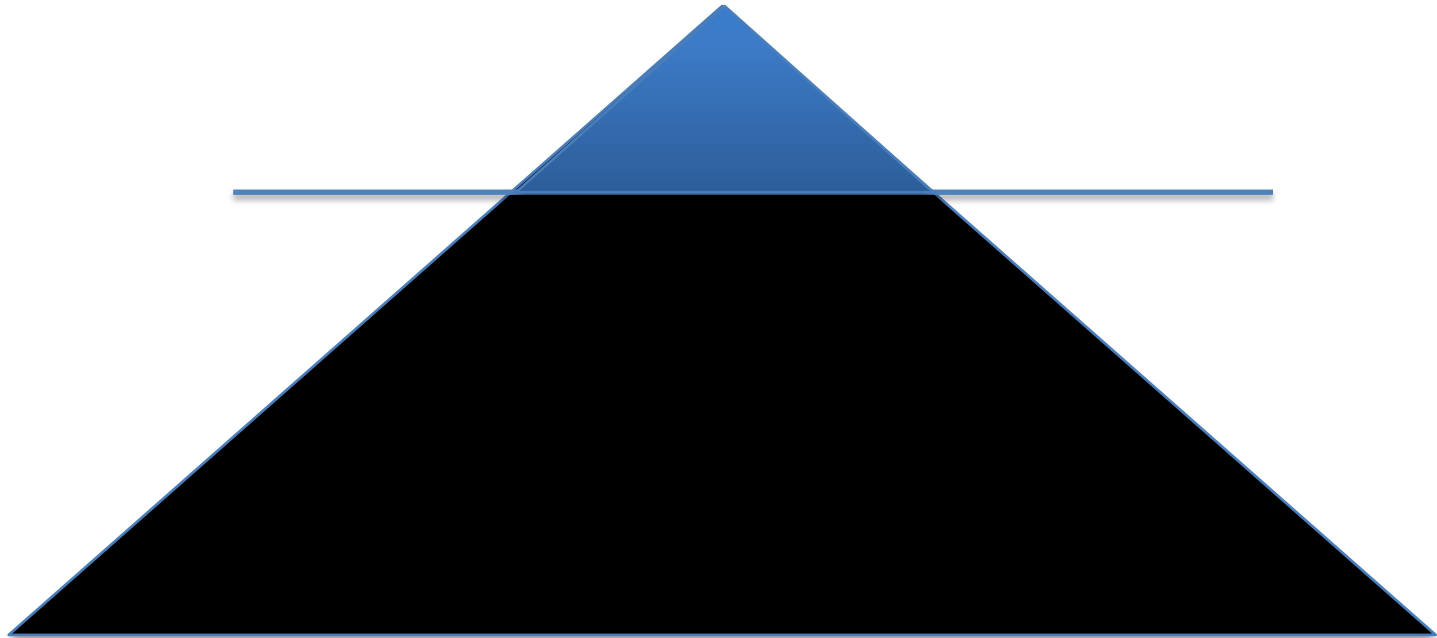


Transitive Trust Can Propagate



La punta dell'iceberg

End Users Identities (sull'Active Directory)



Secure Shell Identities

Nelle grandi realtà le **Secure Shell Identities** possono superare le **identità dei singoli utenti** con un **fattore pari a 100**

**OK, ho una slide più
«graficamente accattivante» ;)**

Dangerous Gaps In Your Security Architecture: “I Thought We Had This Covered?”

20% Interactive (Human) users
of Identities

- * Most organizations **lack sufficient access controls, continuous monitoring, DLP or forensics capabilities** in M2M networks
- * In many cases, **M2M authentications vastly outnumber interactive authentication**
- * M2M connections **can be hijacked by interactive users**
- * M2M connections **often carry high value payloads** such as credit card numbers and personally identifiable information
- * M2M encrypted communications are **rarely monitored** and the encryption used to protect the **data blinds ops & forensics**

80%
of Identities

La slide precedente

La slide precedente si riferisce ad un **case study** reale.

Mostra infatti la situazione da noi rilevata presso un **primario istituto bancario**, che ha causato il **fallimento di un audit SOX** (Separation of Duties) ed un **audit MAS** (Monetary Authority of Singapore).

E' stato infatti rilevato come, durante i **test di compliance**, nello spostare dei file immagine dall'area di **Sviluppo** a quella di **Produzione** (o applicando il percorso inverso), fosse **possibile copiare altresì i file delle *Authorized Keys***, creando così **backdoors sui sistemi in Produzione**.

Questo scenario è purtroppo **alquanto tipico**, e l'**impatto** in termini di **business** (economici, di immagine ed operativi) in seguito alle **mancate compliance** è estremamente **alto**.

Problematiche di Compliance

- Normativa 231/01 per la Responsabilità degli Amministratori di Sistema (IT)
- Normativa 196 Privacy (IT)
- PCI-DSS
 - 3.5 *“Protect encryption keys used for encryption of cardholder data against disclosure and misuse.”*
 - 3.6 *“Fully document and implement all key management processes and procedures.”*
 - 4.1 *(Credit Cards data in transit, even if only through open networks)*
- SOX (INTL)
- GLBA (INTL)
- FFIEC (INTL)
- NIST, FISMA, NERC (INTL)
- COBIT, IT Governance Framework (INTL)
 - DS5.8 - *Cryptographic Key Management*
 - Certification practices, key visibility, creation, storage, distribution and revoke*
 - Supports SOX and other external audits*
 - Often referenced on internal security policies*
- ISO 27001/13 A.10.1.2 Key Management (INTL)
- HIPAA (INTL)
- MAS - Monetary Authority of Singapore (SG)



Current & Emerging Compliance Standards

Compliance Requirement	Status	Potential Audit Finding
Monetary Authority of Singapore	Updated to include specific language concerning keys	Yes
NIST-FISMA	C2.2.x & expected update to include specific requirements around SSH key authentication	Yes
PCI	Access control requirements extended to Secure Shell and other methods of authentication (see SSH website for video)	Yes
SOX	DS 5.8 – Access control and key management requirements	Yes
NERC	R5 – Account management	Yes
HIPAA	4.x information access management	Yes

Unmanaged Secure Shell: i rischi

I rischi nell'Identity e nell'Access Management

Gli **Amministratori di Sistema** che **lasciano l'azienda** hanno **ancora accesso** ai sistemi **critici**

Nessuna salvaguardia per **prevenire** l'utilizzo di **copie non autorizzate** delle *Private Keys*

Relazioni di trust delle chiavi, **non più necessarie**, sono **ancora attive** sui sistemi host

Assenza di **rotazione delle chiavi**

Escalation inaspettate o non previste di **accessi non autorizzati**

Mancanza di visibilità delle relazioni di trust tra gli **ambienti di test e di sviluppo** (host, applicazioni)

Mancanza di visibilità delle relazioni di trust dei **confini organizzativi**

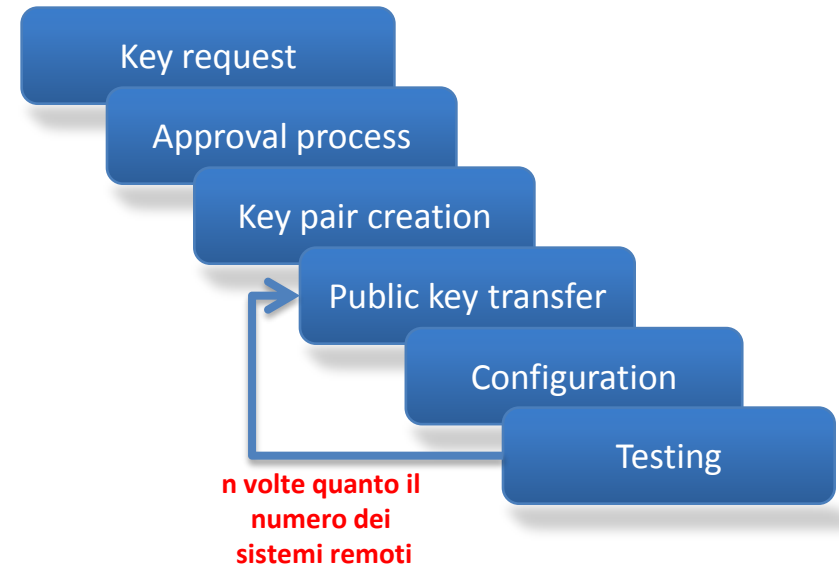
Troppi **singoli individui autorizzati** a creare **relazioni permanenti di trust** tra gli host e le applicazioni

Errori nei processi manuali di creazione delle relazioni di trust

Assenza di **auditing e reporting**

Unmanaged Secure Shell: problematiche sui costi

- * **Processo manuale complesso** per la creazione di nuove chiavi e relazioni di fiducia
- * Ancora più complesso in termini di tempo il **processo di rotazione e rimozione delle chiavi** (time-consuming)
- * Più dinamici sono gli ambienti, più key operations sono necessarie (**cloud / grid computing**)
- * I costi possono arrivare a diversi **milioni/anno**



Numero di sistemi SSH systems nell'ambiente	20000
Numero di setup per nuove chiavi all'anno	10000
Tempo medio per il setup (cad.)	15 min
Media di sistemi per ogni setup	10
Numero di operazioni di key removal per server	2
Tempo richiesto per singola operazione	30 min
Numero di altre key operations per server	4
Tempo richiesto per singola operazione	15 min
Costo orario stimato del security admin	\$ 59
Stima del costo operative all'anno	\$3 835 000



Does it Really Happen?

In the real world...

Real-Life Examples

Former Hostgator employee arrested, charged with rooting 2,700 servers

Prosecutors: Backdoor and digital key gave him near unfettered access.

by Dan Goodin - Apr 19 2013, 7:51pm FLEET

BLACK HAT INTERNET CRIME



theguardian

News Sport Comment Culture Business Money Life & style

News Technology Software

GitHub users warned over security risk

Search tool on programming site turns up SSH keys, which could allow attackers to hack sites or alter programs silently

COMPUTERWORLD

Write Papers Webcasts News

Topics

News

In Depth

Reviews

Blog

Opinion

Security

Application Security Cybercrime and Hacking Cyberwarfare

Malware and Vulnerabilities Mobile Security Privacy

Home > Security

News

Hackers break into two FreeBSD Project servers using stolen SSH keys

Users who installed third-party software packages distributed by FreeBSD.org are advised to reinstall their machines

SECURITY ANALYST SUMMIT 2014

9-13 FEB 2014 HARD ROCK HOTEL, PUNTA CANA, DOMINICAN REPUBLIC

threat post

CATEGORIES

FEATURED

PODCASTS

VIDEOS

Twitter Facebook LinkedIn YouTube

Welcome > Blog Home > Government > New 'Mask' APT Campaign Called Most Sophisticated Yet

```
... Proxy Server ... Proxy Enabled ...
... configuration ... Unknown ... Installed
... No ... system32 ... Files
... C:\SID\{...} \procServer32 ...
... GetSystemReport v1.0 ...
... New Config
... updated for all users ...
... TEMP5_URL_AUX ... New URL_AUX_WAIT ...
... Original URL_AUX ...
```

NEW 'MASK' APT CAMPAIGN CALLED MOST SOPHISTICATED YET

Malicious Insiders: Exploiting Encrypted Networks

- * Edward Snowden case: Attack vector still unknown, however recent high level statements show that keys were probably used to execute the attack
 - * **U.S. National Security Agency (NSA) director Keith Alexander** told the House Permanent Select Committee on Intelligence that Snowden was **able to gain access to NSA files that he should not have had access to by fabricating digital keys**
- * A former Host Gator employee uses an SSH key to gain free access to 2,700 servers, potentially putting thousands of their customers' websites at risk

Former Hostgator employee arrested, charged with rooting 2,700 servers

Prosecutors: Backdoor and digital key gave him near unfettered access.

by Dan Goodin - Apr 19 2013, 7:51pm FLEET

BLACK HAT INTERNET CRIME 63



External Threats: Accessing Critical Systems



* FreeBSD

- * Potential threat: Software downloads from a trusted source could contain a virus or Trojan

* Apache



The Apache Software Foundation

- * Potential threat: Integrity of copies of the hugely popular Apache Web server distributed through the Apache.org site

External Threats: Targeted & Advanced Malware Attacks

- * While investigating the breach of a large internet hosting provider, **Symantec** researchers discovered a new backdoor, dubbed “**Fokirtor**,” that targets the Linux operating system and is capable of stealing login credentials from Secure Shell (SSH) connections.
- * With Fokirtor, attackers could have accessed the encryption key that secured the unnamed organization’s internal communications.
- * Ultimately the malware could allow an attacker to execute commands of their choosing and even collect data from individual SSH connections, like the connecting hostname, IP address, port and SSH key used to authenticate users.

External Threats: Attacking Point-on-Sale Environments

Visa Security Alert: Remote Access Vulnerabilities—Most Frequent Attack Method Used by Intruders (2011)

- * Insecure remote access continues to be **the most frequent attack method** used by intruders to gain access to a **merchant's point-of-sale (POS) environment**
- * There are a variety of remote access solutions available, ranging from command-line based (SSH, Telnet) to visually driven packages
- * **Remote management applications come with an inherent level of risk, creating a virtual "back-door" for unauthorized access;** therefore, these applications must be configured in a manner that complies with the Payment Card Industry Data Security Standard (PCI DSS).
- * The **exploitation of improperly configured remote management software tools is the method of attack most frequently used by hackers** against POS payment systems.

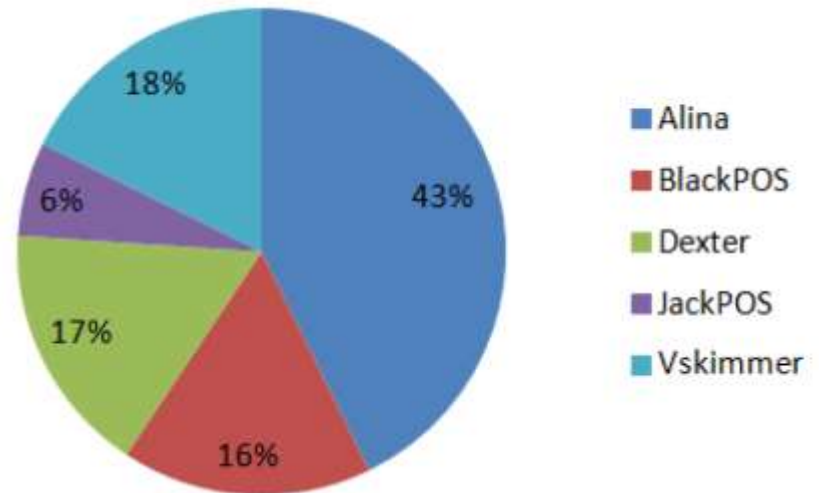
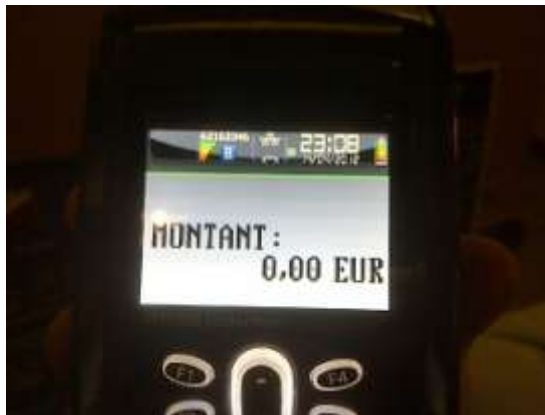
POS (in)security

Data Leakage

~~POS Device Tampering~~

POS Device Infection

Traffic Analysis



POS (in)security

“Kartoxa/BlackPOS” & Target Breach

Binary Analysis (March 2013)

C&C Detection

```
mmemset(&v57, 0xCCu, 0x380u);  
v88 = 0;  
sub_403190(&v87, lpMultiByteStr);  
v89 = 0;  
v86 = 0;  
buff_curr_pos = buffer;  
bufend = buffer + bytes_read - 1;  
v83 = strstr(lpMultiByteStr, "KAPTOXA");  
if ( v83 )  
{  
  while ( 1 )  
  {  
    if ( buff_curr_pos >= bufend )  
      break;
```

```
data:00471228 aWvuRee4_7ci_ru db 'www/ree4.7ci.ru/reports/',0 ;  
data:00471243 ; char aDun_exe_2[]  
data:00471243 aDun_exe_2 db 'dun.exe',0 ; DATA XRI  
data:00471248 ; char aOutput_txt_1[]  
data:00471248 aOutput_txt_1 db 'output.txt',0 ; DATA XRI  
data:00471256 aDun_exe_3 db 'dun.exe',0 ; DATA XRI  
data:0047125E ; char aDun_exe_4[]  
data:0047125E aDun_exe_4 db 'dun.exe',0 ; DATA XRI  
data:00471268 aSubst_exe db '\\subst.exe',0 ; DATA XRI  
data:00471271 aDumpGrabberBuR db 'dump grabber bu ree4.',0 ; DATA XRI  
data:00471271 ; DATA XRI  
data:00471287 aUserDirectoryN db 'user directory name:',0 ; DATA XRI  
data:00471287 ; DATA XRI  
data:0047129D aDeleteTheFileA db 'Delete the file after reading
```



POS (in)security

“Kartoxa”/”BlackPOS” Author

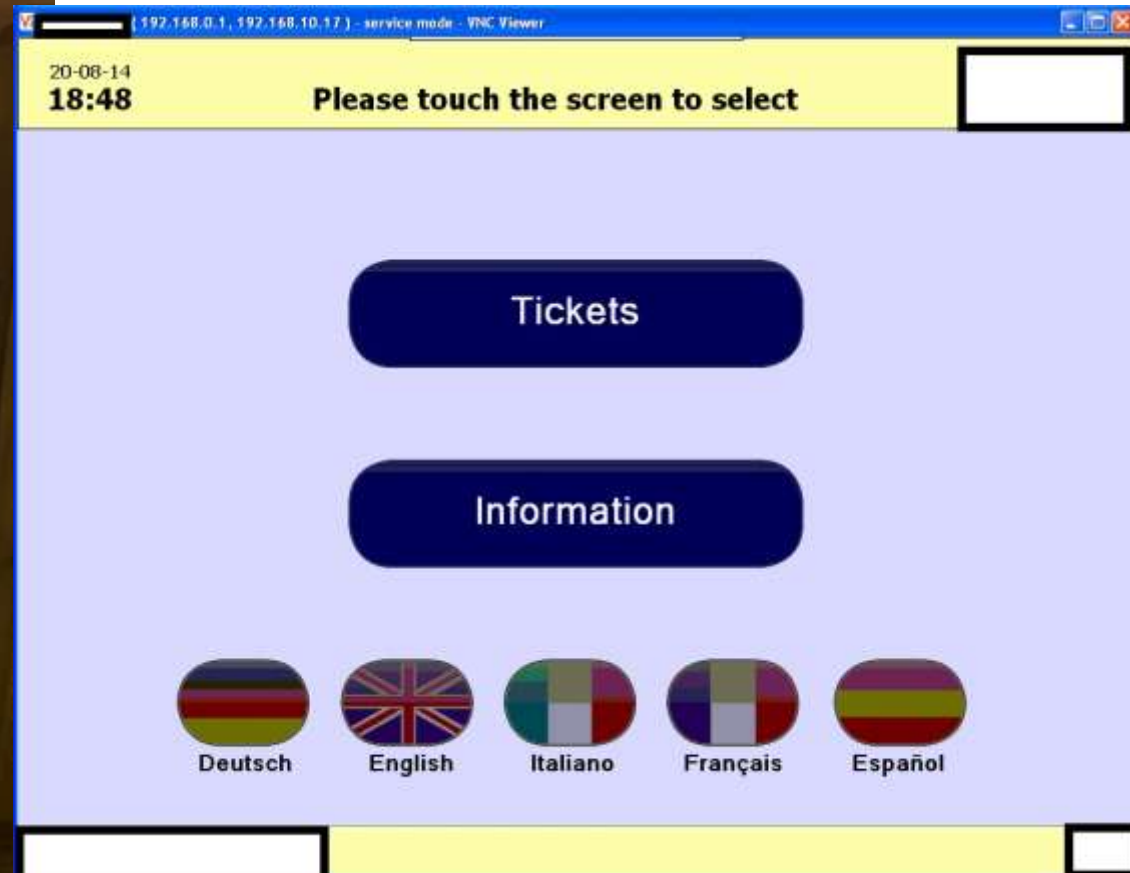
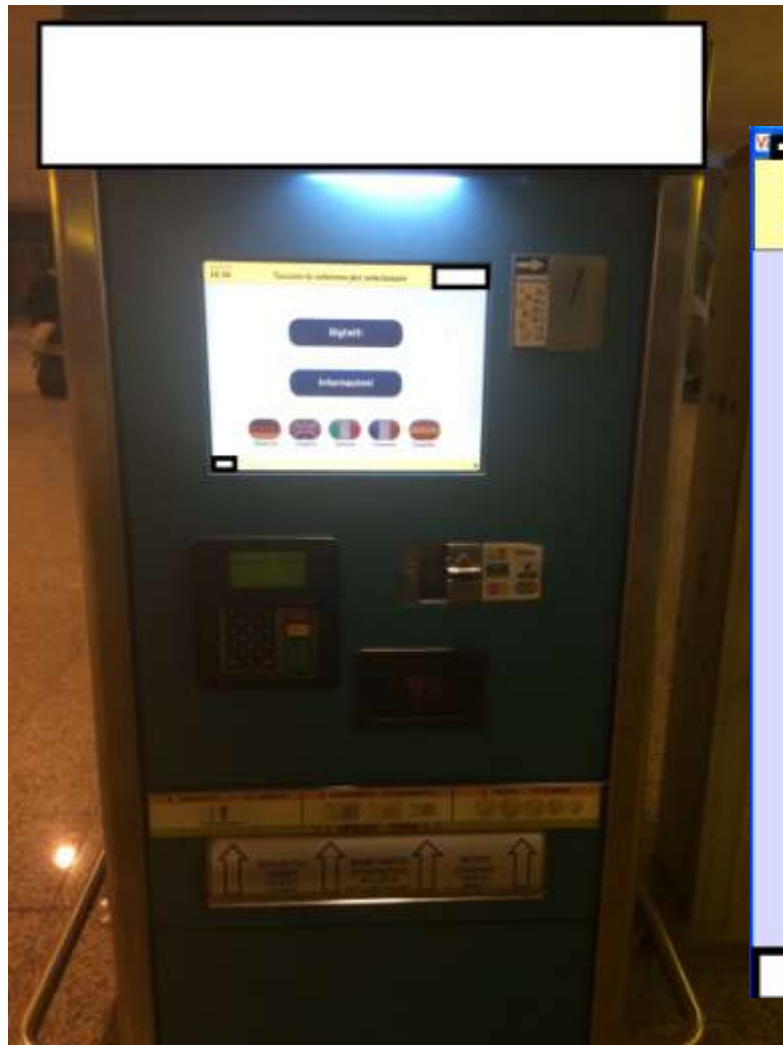


“Yes, I have written it, but for security testing ...”

JackPOS, «primi giorni di vita»



POS (Totem)



POS (Totem)

The image displays two screenshots of a POS (Totem) interface. The first screenshot shows a selection screen with the date 20-08-14 and time 18:49. The text "Please touch the screen to select" is displayed. Three large blue buttons are visible: "Suburban Buses", "Airport Shuttle No Stop Services", and "Tourist Services". A red "Cancel" button is at the bottom left. The second screenshot shows a payment screen with the same date and time, displaying "Please pay" and "18 50". It includes a "You have selected" section with fields for "From", "To", and "Type". A "Payment" section shows "Amount to be paid" as 18.50. A yellow dialog box in the center reads: "Printing...", "Please collect your ticket and your change.", "Thank you...", and "Have a nice trip". Below the dialog, there are icons for various payment methods, including Euro coins and a VISA logo, with some crossed out. A red "Cancel" button is at the bottom right.

POS (Totem)

V [] (192.168.29.4, [] 0) - service mode - VNC Viewer

MODULO - FATTURE - Versione []

Utilità

Modulo FATTURAZIONE

€ + - [] NIX ESC

Archivi
Fatturazione
Utilità

SELEZIONE SCONTRINI

Cassa	Scontrino	Data	Ora	V
		--		
		--		
		--		

Ins Nuovo F3 Cancella (F6) Lettura Casse

Messaggi riportati per ogni tentativo fallito

IntNix11 - Scontrino 14-08-140050 02 già elaborato in precedenza
MOVECR - VUOTO

Crono
Processo <control> in corso

NUM CAPS 6:54:37 pm

Record: 1/3 Record Unlocked

18:54
20/08/2014

POS (Totem)

* ANSA, 29 settembre 2014

http://www.ansa.it/sito/notizie/tecnologia/software_a_pp/2014/09/29/parcheggi-e-biglietterie-nuovo-obiettivo-hacker_8c6b810d-c10e-45b7-9fd0-839bff92b5b0.html

EDIZIONI ANSA > Mediterraneo | Europa | NuovaEuropa | Latina | Brasil | English | Realestate |

ANSA.it Software&App Fai la ricerca

[Cronaca](#) [Politica](#) [Economia](#) [Regioni +](#) [Mondo](#) [Cultura](#) [Tecnologia](#)

PRIMOPIANO • HI-TECH • INTERNET & SOCIAL • TELECOMUNICAZIONI • SOFTWARE & APP

ANSA.it > Tecnologia > Software & App > **Parcheggi e biglietterie, nuovo obiettivo hacker**

Parcheggi e biglietterie, nuovo obiettivo hacker

Esperto, carte credito ora clonate da 'totem' casse automatiche

Titti Santamato
29 settembre 2014
20:27
ANALISI

[Suggerisci](#)
[Facebook](#)
[Twitter](#)
[Google+](#)
[Altri](#)

[A+](#) [A](#) [A-](#)

[Stampa](#)
[Scrivi alla redazione](#)



Parcheggi e biglietterie, nuovo obiettivo hacker [CLICCA PER INGRANDIRE](#)

Non solo bancomat, acquisti via Internet e transazioni di e-banking, nel mirino degli hacker ci sono ora le casse automatiche, quelle che comunemente usiamo per fare un biglietto del treno in stazione o per pagare il parcheggio in città. A lanciare l'allarme un team Usa-italiano di esperti nel settore sicurezza.

"Stiamo seguendo da diversi mesi le tracce di svariati gruppi di cybercriminali che si sono specializzati nelle frodi via Pos. Esistono da anni ma quello che è cambiato è il modus operandi di questi gruppi

Fresh stuff (FEB 18 2015, h. 16.15)

BRI Subject ▾ Alert Risk Dashboard ▾ Archive ▾ News Library Ask us CVSS Account ▾

Quick

Latest Generic Subjects And Updates

824,386 alerts available

Technology


BigFish Games Breached, Payment Info Exposed

 0 minutes ago


Malicious Emails Can Cause Gmail App to Crash: Researcher

 1 hour, 17 minutes ago 


New Web flaw enables powerful social engineering attacks

 2 hours, 55 minutes ago

BadUSB Vulnerabilities Live in ICS Gear Too


 3 hours, 52 minutes ago

Celebrity chef Jamie Oliver's website hacked, redirects to exploit kit


 5 hours, 26 minutes ago

Industry


BigFish Games Breached, Payment Info Exposed

 0 minutes ago


BadUSB Vulnerabilities Live in ICS Gear Too

 3 hours, 52 minutes ago

OpChapelHill: Hackers Deface Military Boarding School Website

 4 hours, 41 minutes ago


No, Bank of Ireland isn't running a routine security check on your account

 5 hours, 54 minutes ago

Siemens OpenSSL Vulnerabilities (Update 6) (ICSA-14-108-036)

Global


BigFish Games Breached, Payment Info Exposed

 0 minutes ago


Malicious Emails Can Cause Gmail App to Crash: Researcher

 1 hour, 17 minutes ago 


BadUSB Vulnerabilities Live in ICS Gear Too

 3 hours, 52 minutes ago

OpChapelHill: Hackers Deface Military Boarding School Website

 4 hours, 41 minutes ago

Celebrity chef Jamie Oliver's website hacked, redirects to exploit kit

 5 hours, 26 minutes ago

Universal SSH Key Manager (UKM)



Discover

- * Si collega all'ambiente
- * Raccoglie informazioni su host, user e sulle chiavi
- * Scopre e mostra le relazioni di trust

Remediate

- * Lock down dell'environment
- * Identifica le key operations non autorizzate
- * Abilita le notifiche automatiche

Manage

- * Gestisce ed automatizza i setup delle keys e la loro rimozione
- * Si integra ai processi e strumenti esistenti attraverso le API

UKM: overview

Discover

- **Effettua l'inventario** delle chiavi SSH
- Mappa le **Relazioni di Trust**
- **Traccia le attività** delle chiavi
- Identifica le **chiavi non utilizzate** o **non necessarie**
- Identifica le **autorizzazioni non necessarie**

Remediate

- **Rimuove** le chiavi non utilizzate
- **Riposiziona** le chiavi alle directory "root owned"
- **Aggiorna** le autorizzazioni
- **Rinnova** le chiavi vecchie e non-compliant
- **Centralizza** il controllo

Manage

- **Collega** il processo di autorizzazione ai **sistemi di ticketing** esistenti
- Gestisce e si occupa dell'**enforcement delle configurazioni SSH**, a livello **centralizzato**
- **Automatizza** la rimozione delle chiavi, collegandosi a **AD** o **LDAP**
- **Monitora** in maniera continuativa, per **rilevare e correggere le violazioni**

Exfiltration

- * Use the encrypted tunnel **to steal data and exfiltrate it back** to the hackers server
- * **Blind security ops** as to what has been taken and by whom
- * Make it **difficult for forensics teams** to do an investigation
- * **Slow down** remediation/response activities

* “exfiltrate”=a word used in place of 'data theft', to mean an unauthorized release of data from within a computer system or network.

Data Leak e Data Breach: punti chiave e sfide del mercato

- Come **abilitare gli accessi esterni** agli utenti (fornitore, IT in outsourcing, maintenance providers) con un **auditing appropriato ed efficiente** dell'access control?
- Come **garantire** la compliance con le normative e gli standard di sicurezza, come il **PCI-DSS**?
- Come fare audit e controllare le attività interne ed esterne degli **utenti privilegiati**?
- Come ottenere visibilità, auditing, allarmi, intrusion e data loss prevention **anche per le connessioni cifrate**?

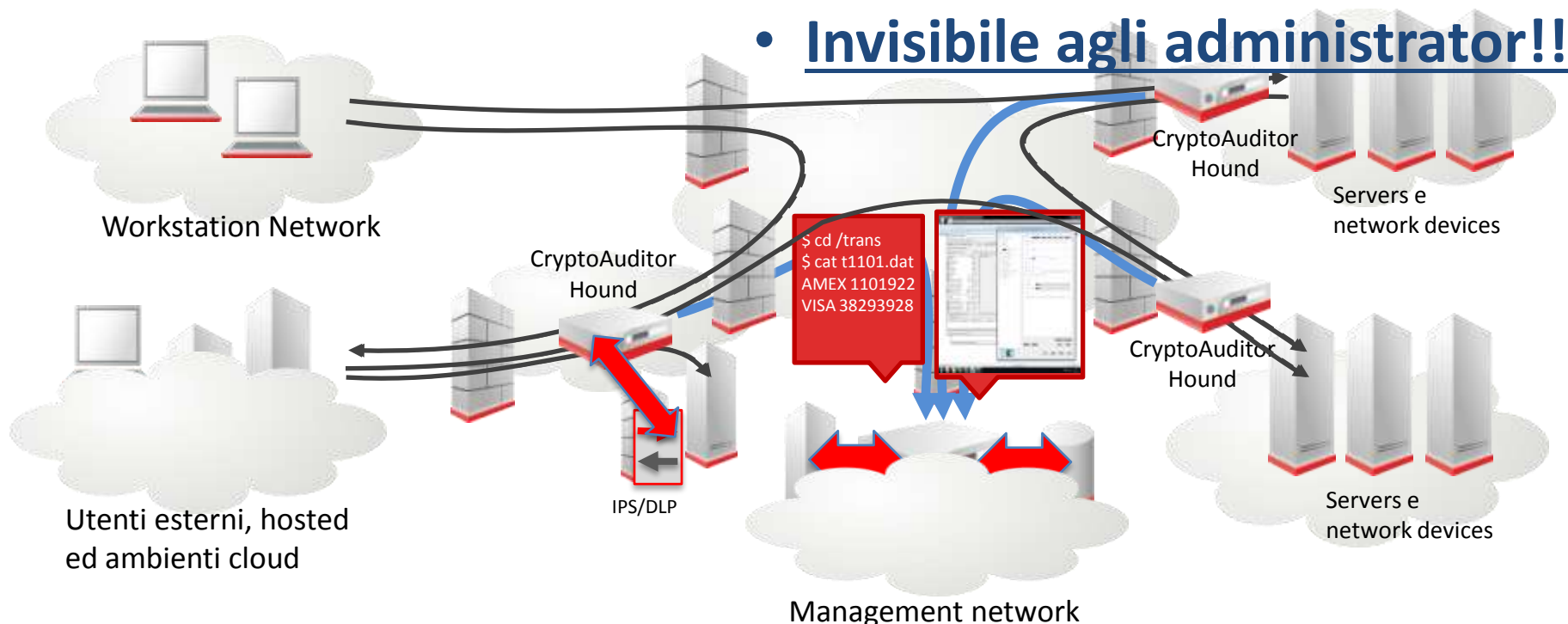


CryptoAuditor

- **In-line** audit
- **Agent-less** su tipologia bridge, router o bastion-host
- **Management centralizzato**, audit trail storage e reporting.
- Virtual / Hardware **appliance**

- **Replay** delle sessioni SSH e RDP
- Optical Character Recognition (**OCR**)
- **Integrazione** con DLP, IPS, SIEM, Anti-Virus tramite **protocollo ICAP**
- End-user **policy control**

- **Invisibile agli administrator!!**



Esempi di utilizzo del Crypto Auditor

- **Controllo degli accessi utente** (di terza parte, parte, esterni o interni) tramite lo **UserID Mapping: non hanno bisogno della password di root** sui server critici!
- **Monitoring delle sessioni SSH** per **prevenire data leakage**: tramite lo **stesso CryptoAuditor** oppure integrandosi con un **DLP esistente**.
- **Utilizzo degli Audit trails** (video o trascrizioni di sessione) come **prova forense**.
- **Presentazione di report** agli auditor IT.
- **Utilizzo di topologie** bridge, router o jumpserver in **funzione delle necessità**.



CryptoAuditor

ssh CryptoAuditor™

Home Trails and Logs Reports Policy Settings

42: SSH to 10.12.0.130 by administrator 1 day, 23 hours ago

Channels 1

Session replay

```
Directory of C:\Documents and Settings\Administrator
10/12/2012 01:38 PM <DIR> .
10/12/2012 01:38 PM <DIR> ..
11/30/2012 12:15 PM <DIR> Desktop
10/12/2012 01:37 PM <DIR> Favorites
11/24/2012 10:24 AM <DIR> My Documents
10/12/2012 04:38 PM <DIR> Start Menu
10/11/2012 04:38 PM 0 Start_Trace.log
1 File(s) 0 bytes
6 Dir(s) 24,901,398,528 bytes free

C:\Documents and Settings\Administrator\Desktop
C:\Documents and Settings\Administrator\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is B07E-A834

Directory of C:\Documents and Settings\Administrator\Desktop
11/30/2012 12:15 PM <DIR> .
11/30/2012 12:15 PM <DIR> ..
11/30/2012 11:32 AM 681,927 Kalendar.txt
1 File(s) 681,927 bytes
2 Dir(s) 24,901,398,528 bytes free

C:\Documents and Settings\Administrator\Desktop>
```

Search results

- 2012-12-15 13:25:53 [00:00:13] Administrator@dr Volume in drive C: has no label. Volume Serial Number is B07E-A834 in has no...
- 2012-12-15 13:26:06 [00:00:26] Administrator@dr Volume in drive C: has no label. Volume Serial Number is B07E-A834 in has no...
- 2012-12-15 13:26:25 [00:00:45] Administrator@dr Volume in drive C: has no label. Volume Serial Number is B07E-A834 in has no...
- 2012-12-15 13:26:41 [00:01:01] Administrator@dr Volume in drive C: has no label. Volume Serial Number is B07E-A834 in has no...

Type session

Auditing policy output only

Session type shell

Start time 2012-12-15 13:25:40

End time 2012-12-15 13:27:12

Last update 2012-12-15 13:27:12

More details

- Disabilita i c.d. “protocol subchannels”: copy & paste, **tunneling**, printing...
- “Restrict by content”: carte di credito, numeri di conti, informazioni personali o dei dipendenti, etc...
- Le sessioni possono essere **terminate in tempo reale**
- Database con “search by keyword”

ssh CryptoAuditor™

Home Trails and Logs Reports Policy Admin Settings Policy

99: RDP to 100.168.149.146 by testuser 18 hours ago

Channels 1

Session replay

Start testuser

Type rdp

Auditing policy output only

Start time 2012-12-18 18:50:22

End time 2012-02-28 08:08:07

Last update 2012-02-18 08:57:52