La Storia della Sicurezza delle Informazioni

Anno Accademico 2024/2025
Corso Sicurezza Informatica – Laurea Magistrale
Lezione 1, 2, 3 –Settembre 2024
Docente: Ing. Selene Giupponi

UNIVERSITÀ
DI PARMA

Disclaimer

UNIVERSITÀ DI PARMA

The information contained within this presentation **does not infringe** on any intellectual property nor does it contain tools or recipe that could be in breach with known local National laws.

The information contained in this presentation is for **educational purposes** and **knowledge information** only; the authors **are not responsible** if you will use this material in order to **damage people, assets, things**.

The authors hold the **intellectual property** and **it's not allowed to use this material for different purposes**.

The Hackers Profiling Project is hold by **UNICRI** and **ISECOM** and was **created by Mr. Raoul Chiesa.**

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 **Swascan**, **Security Brokers** and **its own Associated Partners and Companies**.

«Regole» per questo Mini Master

UNIVERSITÀ DI PARMA

Mettete in "mute" i vostri microfoni.

Non attivate il vostro video: appesantisce la connessione ai server del Webinar, e peggiora la qualità dell'audio.

Al termine della lezione ci sarà una **sessione dedicata alle domande e risposte**, di circa **15-20 minuti**: segnatevi quindi le domande che vi verranno in mente man mano, così da discuterle tutti insieme alla fine. Questa sessione di Q&A sarà **moderata** dal back-office di SWASCAN Formazione, per ottimizzarne la gestione.

Durante la lezione **proietteremo alcuni video**, ai quali vi preghiamo di **dedicare speciale attenzione**.

Cosa succederà questa mattina?

UNIVERSITÀ DI PARMA

E' un modulo introduttivo al Mini Master, altamente interattivo e dinamico.

NON E' IL SOLITO MODULO "NOIOSO"!

Abbiamo impostato tutto il materiale che state per visionare con l'obiettivo di farvi capire innanzitutto PERCHé la Cyber Security è importante, e COSA si "cela dietro" gli ecosistemi propri del Cybercrime.

Il mondo sta cambiando: non si tratta solo di "Smart Working" o del vostro lavoro: parliamo anche della vostra privacy e vita di ogni giorno, personale e familiare.

Siamo convinti che al termine di questa lezione avrete appreso dati, informazioni e scenari prima sconosciuti. E che sarete contenti di questa esperienza.

Vogliamo farvi **appassionare a questi temi**.

HACKMAGEDDON

UNIVERSITÀ
DI PARMA

Adesso pensiamo di avere la vostra attenzione ☺

UNIVERSITÀ DI PARMA

Indice – Prima Parte

UNIVERSITÀ DI PARMA

“GLI SCENARI E GLI ATTORI”

- Terminologia
- Statistiche
- Le minacce di oggi
- Un po’ di storia: dall’hacking al Cybercrime…
- …e dal Cyber Espionage all’Information Warfare
- Casi di studio
- Letture consigliate


WiBoy
WiBoy

whois Selene

UNIVERSITÀ DI PARMA

Selene Giupponi:

- **Managing Director Europe, Resecurity Inc.**
- **Computer Engineering Degree** + II Level **Master in Computer Forensics & Digital Investigations**
- General Secretary and Member @ **IISFA** (INFORMATION SYSTEM FORENSICS ASSOCIATION, ITALIAN CHAPTER)
- Active Member of the **IT Engineer Commission**, Engineers Association of the Latina Province
- **Digital Forensics Court Trial Witness** on e-crimes and ICT enhanced crimes
- Consultant for multiple **Law Enforcement agencies** around the world
- Advisor @ **European Courage Focus Group** – Cyber Terrorism & Cybercrime
- **ITU** Roster of Experts Official Member
- **HTCC** HIGH TECH CRIME CONSORTIUM Member
- Co-Founder at **The Security Brokers**
- Trainer at **NATO**, **INTERPOL**
- **CIFI** - Certified Information Forensics Investigator
- Certified Trainer for **SPEKTOR** & **UFED**
- **ECSO** Board of Directors Member

Parole, parole, parole...

UNIVERSITÀ DI PARMA

Terminologia

Nel mondo dell'**InfoSec** abbiamo un *enorme* problema**:**

la terminologia.

- La quale, a sua volta - e già "sporcata"! - ha **interpretazioni** e **logiche** anche molto diverse, in funzione del **settore** in cui la si utilizza ed applica.

...Come se non bastasse, negli **ultimi anni** è scoppiata la **moda** di anteporre il prefisso "cyber" alla maggior parte dei termini!

... dal "Cyber Punk" al "Cyber-Chef" !! ☹

- **Ciò nonostante**, alcuni (grossi) dubbi persistono...persino per i madrelingua!

Ortografia non omogenea...

„Cybersecurity, Cyber-security, Cyber Security ?"

Assenza di definizioni condivise...

Cybercrime é...?

Chi sono gli attori?...

Cyber – Crime/war/terrorism ?

Nei paesi non di lingua inglese, i problemi di comprensione aumentano esponenzialmente

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.

Esempio di digital underground slang (cybercrime)

UNIVERSITÀ DI PARMA

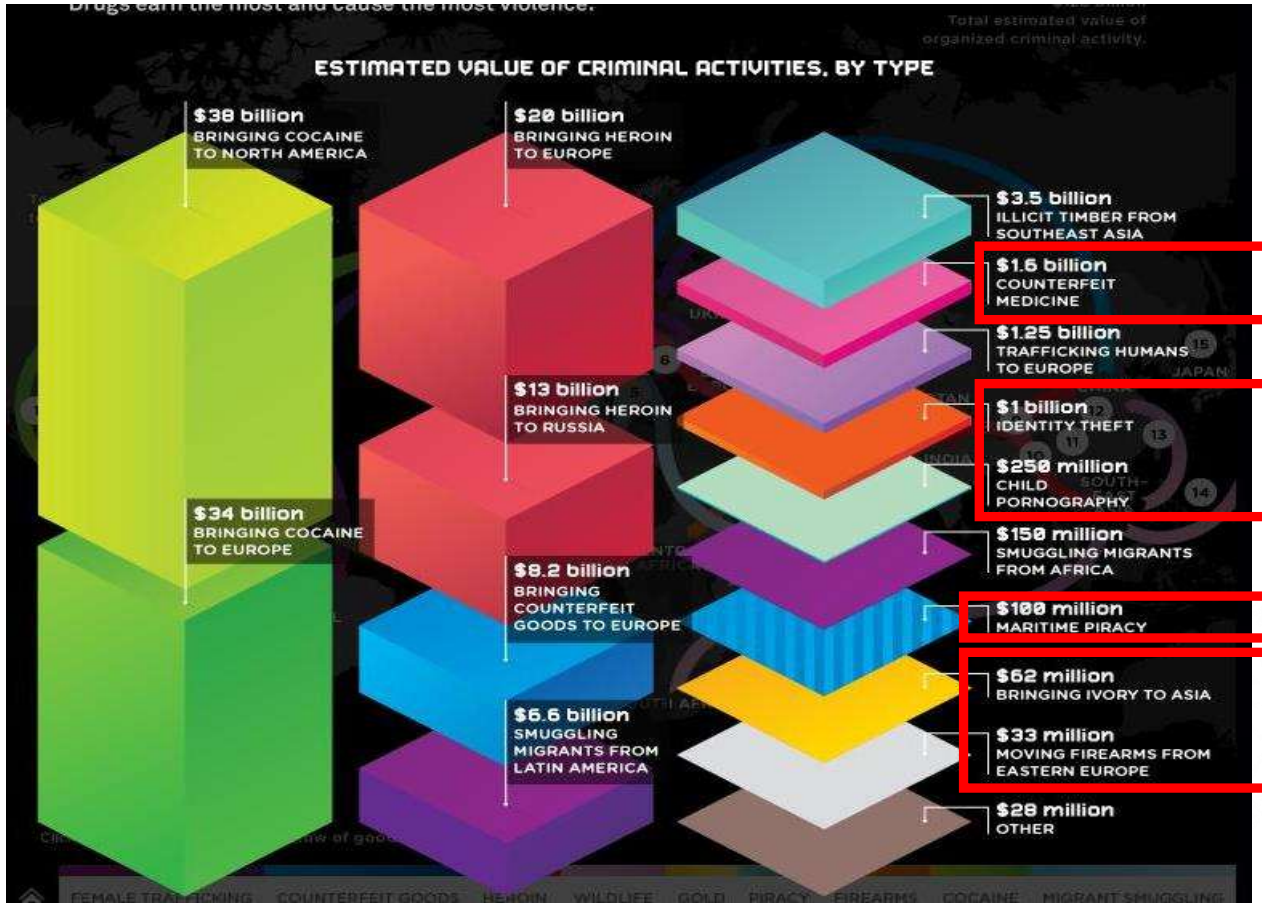
- **Dump checking** – Using specific software or alternatively encoding track data on plastic and using a point of sale terminal to test whether the dump is approved or declined. This provides carders a higher sense of security for obtaining quality dumps fro those who offer them and also a sense of security when doing in store carding.
- **Full info(s)** – Term used to describe obtaining addresses, phone numbers, social security numbers, PIN numbers, credit history reports and so on. Full Info(s) are synonymous with carders who wish to take over the identity of a person or to sell the identity of a person.
- **Holos** – Slang for the word Holograms. Holograms are important for those who make counterfeit plastic credit cards to emulate an existing security feature.
- **ICQ** – An abbreviation for "I Seek You". ICQ is the most widely used instant messaging system for carders. Popular among Eastern Europeans in their Internet culture, it continues to be used for carding activity.
- **IRC** – An abbreviation for "Internet Relay Chat". IRC is a global system of servers through which users can conduct real-time text-based chat, exchange files, and interact in other ways.
- **IDs** – Slang for identification documents. Carders market a variety of IDs, including bills, diplomas, driver's licenses, passports, or anything that can be used as an identity document.
- **MSR (Magnetic Strip Reader)** – Device that can be used for skimming payment card information and/or encoding track information on plastic.
- Phishing – The extraction of information from a target using a hook (usually an e-mail purporting to be from a legitimate company). Phishers spam the Internet with e-mails in hopes of obtaining information that can be used for fraudulent purposes.

Esempio di digital underground slang (cybercrime)

- **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.

Statistiche (Traditional Crime)

Qualcosa è cambiato...



Dark Web

Cyber Crime

Hacking

Dark Web

Le minacce di oggi

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

1. **Negligenza**, **errore umano** e **frodi** realizzati da **Insiders**.

1. **Cybercrime transnazionale organizzato:** incassa circa **60Md $** all'anno (2018) producendo danni diretti ed indiretti per quasi **800Md $** a livello globale.

1. Cyber **Espionage** e Cyber **Warfare**, da parte di soggetti state-sponsored e di mercenari.

CERCHIAMO DI CAPIRE “COSA è SUCCESSO”: UN PO’ DI “STORIA”

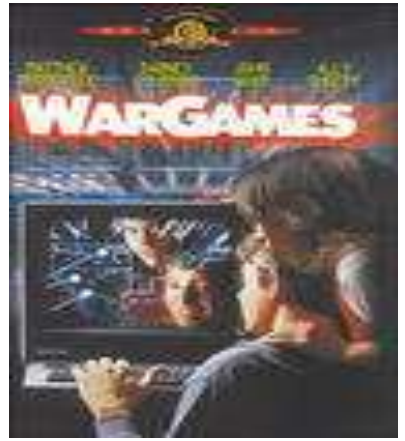
UNIVERSITÀ DI PARMA

Le differenti generazioni dell'hacking

UNIVERSITÀ DI PARMA

- Nascita dell'hacking e dei c.d. "hackers". La **prima generazione** (fine anni '70) era spinta dalla sete di sapere.

- La **seconda generazione** di hackers (anni '80) era spinta dalla **curiosità**, unita alla sete di sapere e al fatto che molti sistemi operativi e reti/sistemi erano apprendibili unicamente "bucandoli". Più tardi, verso la **seconda metà degli anni '80**, il fenomeno unisce fattori di **moda e trend**.



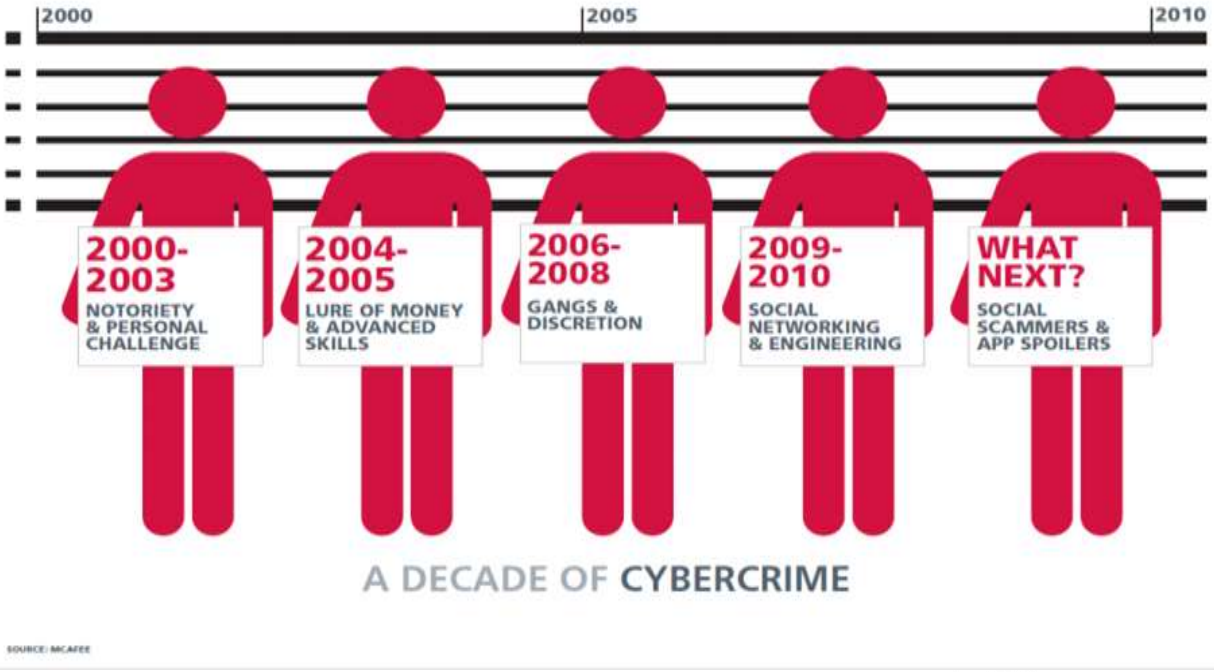
Le differenti generazioni dell'hacking

UNIVERSITÀ DI PARMA

- La **terza generazione** (anni '90) era spinta dalla semplice **voglia di fare hacking**, inteso come un insieme di **curiosità**, voglia di imparare e conoscere **cose nuove**, intenzione di **violare sistemi informatici**, **scambio di informazioni** con la comunità underground. E' in questa fase che si formano i primi gruppi di hackers, che nascono le e-zine hacker e che si propagano le BBS.
- La **quarta generazione** (2000) è mossa dalla **rabbia** e dal **denaro**: si tratta spesso di soggetti con scarse o medie conoscenze tecniche, ma che trovano gagliardo e di moda essere degli hackers, non conoscono o non sono interessati alla storia, alla cultura ed all'etica del phreaking e dell'hacking. Qui l'hacking si mescola alla politica (**Cyber-Hacktivism**) o alla criminalità (**Cybercrime**).

The day money became the focus of malware is the day the Internet changed

Graham Ingram, AusCERT GM



… CON ALCUNI “SIDE EFFECTS”…

UNIVERSITÀ
DI PARMA

"In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, ought with the aid of information soldiers, that is **hackers...**

This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces."

Former Duma speaker Nikolai Kuryanovich, 2007

"I urge you to be more innovative when it comes to emerging threats such as **cybercrime**, environmental crime and counterfeiting, we must stay one step ahead of the criminals. We must also be more effective in stopping the money flows enabled by corruption and money-laundering

Ban Ki-moon, United Nations, 2010


HEY
WE GOT NEW
GAME TO PLAY
yo
CY8ER
WAR
It's Child Play Now

GLI HACKERS, OGGI

UNIVERSITÀ
DI PARMA

Vecchie definizioni / categorie di Hackers

UNIVERSITÀ DI PARMA

- **Black-hat:** those who violate information systems, with or without personal advantage. They are rallied on the "bad" side, crossing over the clear demarcation line between "love for hacking" and the deliberate execution of criminal actions. For these actors, it is normal to violate an information system and to penetrate it its most secret meanders, stealing information and, given their hacker's profile, reselling them to foreign countries.

- **Grey-hat**: those who don't want to be labeled as "black or white" and can consider themselves "ethical hackers." They often could have performed intrusions in information systems, but they have decided not to use this approach.

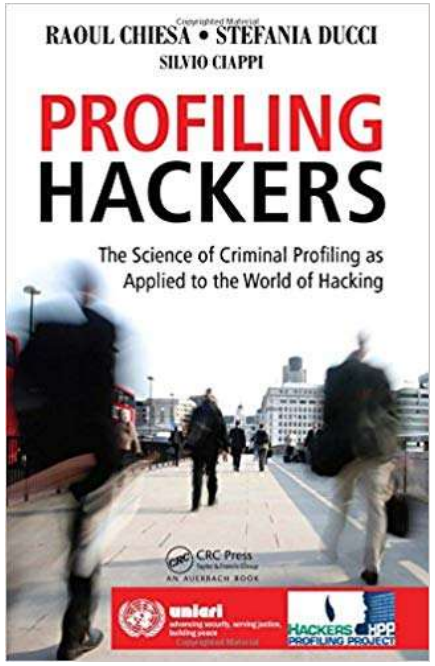
- **White-hat**: also defined "hunters", they have the necessary skill to be a black-hat, but they have decided to side with "the good guys". They collaborate with the Authorities and the Police, they are in the first row in anti computer-crime operations, they are advisors for governments and companies; in their life they don't usually violate computer systems, or if they do, it is never for criminal purposes or for economic gain.

unicri
advancing security, serving justice,
building peace

HACKERS PROFILING PROJECT
HPP

Hackers Profiling

UNIVERSITÀ DI PARMA



- **Applied Research** Project started back in **2004**
- **Field Research** tasks started in **2006** (still on-going)
- Law Enforcement Officers and Government Agencies **loved our profiling approach!**
- **FBI Academy Library** in Quantico, VA (USA)
- FBI cybercrimes **Special Agents must-read** book
- Italian Intelligence Agency (**DIS**) official Hacker's Profiles
- Translated in **different languages** (Italian, Spanish,French, Russian, Chinese, Arabic, etc..)
- **Cutting-edge milestone** from the previous "Black-hat /White-hat" approach

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

unicri
United Nations Interregional Crime and Justice Research Institute

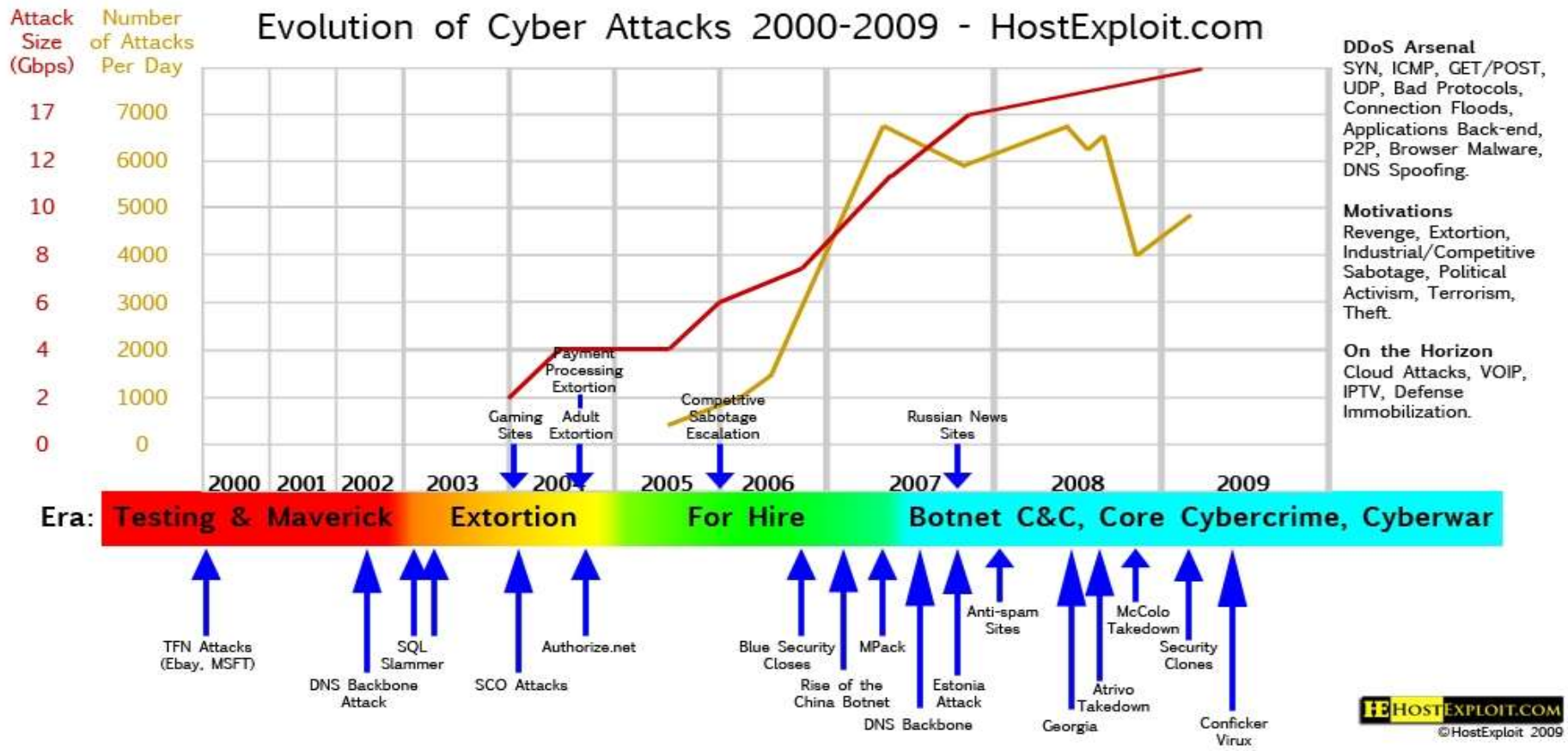
HPP – Hacker's Profiling Project (UNICRI/ISECOM)

UNIVERSITÀ DI PARMA

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

DALL'HACKING AL CYBERCRIME

UNIVERSITÀ
DI PARMA


Evolution of Cyber Attacks 2000-2009 - HostExploit.com
Attack Size (Gbps)
Number of Attacks Per Day
17
12
10
8
6
4
2
0
7000
6000
5000
4000
3000
2000
1000
0
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
Era:
Testing & Maverick
Extortion
For Hire
Botnet C&C, Core Cybercrime, Cyberwar
TFN Attacks (Ebay, MSFT)
DNS Backbone Attack
SQL Slammer
SCO Attacks
Authorize.net
Gaming Sites
Payment Processing Extortion
Adult Extortion
Competitive Sabotage Escalation
Blue Security Closes
Rise of the China Botnet
MPack
DNS Backbone
Estonia Attack
Anti-spam Sites
Russian News Sites
Georgia
Atrivo Takedown
McColo Takedown
Security Clones
Conficker Virux
DDoS Arsenal
SYN, ICMP, GET/POST, UDP, Bad Protocols, Connection Floods, Applications Back-end, P2P, Browser Malware, DNS Spoofing.
Motivations
Revenge, Extortion, Industrial/Competitive Sabotage, Political Activism, Terrorism, Theft.
On the Horizon
Cloud Attacks, VOIP, IPTV, Defense Immobilization.
HostExploit.com
©HostExploit 2009

2011: L'Anno della Svolta

UNIVERSITÀ DI PARMA

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

PriceWaterhouseCoopers LLC
Global Economic Crime Survey 2011

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

Various sources
(UNICRI, UNODC, INTERPOL, EUROPOL, USDOJ)

Anatomia del Cybercrime

UNIVERSITÀ DI PARMA

SCENARIO ALTAMENTE COMPLESSO

- **Attori**
  - Chi sono? Variegati, in costante evoluzione
- **Motivazione**
  - Fama
  - Denaro
  - Ideali
  - Nessuna (?)
- **Prodotti/Servizi**
  - Campagne di affiliation, boosting, advertising, traffic generation, etc…
  - Decine di famiglie di servizi e prodotti «impensabili per l'uomo comune»
  - Li vedremo nelle prossime slide
- **Legislazioni**
  - Non presenti in tutti i Paesi per tutti i reati: carenze nella cooperazione internazionale
  - Cybercrime: profonda presenza in Paesi con problematiche interne (legislazioni, budget, formazione delle Forze dell'Ordine, corruzione)

Definizione e Key Point del Cybercrime

UNIVERSITÀ DI PARMA

- 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 countries:** "paradisi" sia fiscali che legali

Cos'è il Cybercrime?

UNIVERSITÀ DI PARMA

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

Esempi:

- **Furto di Identità**
  - Personal Info
- **Furto di Credit Identity**
  - Financial Info: login bancari, CC/CVV, «fullz», etc
- **Hacking**
  - verso e-commerce, e-banking, Credit Cards 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**
- **Harassment** (Cyberstalking, Cyberbullying, Cybergrooming, ….)

DUE CASI DI STUDIO:

BANKING PHISHING OLANDESE E “MONEY MULES” IN ITALIA

UNIVERSITÀ DI PARMA

Money Rules

(da Striscia la Notizia)

Quanto valgono i tuoi dati?

POLITIE
National Police Agency

Quanto valgono i tuoi dati?

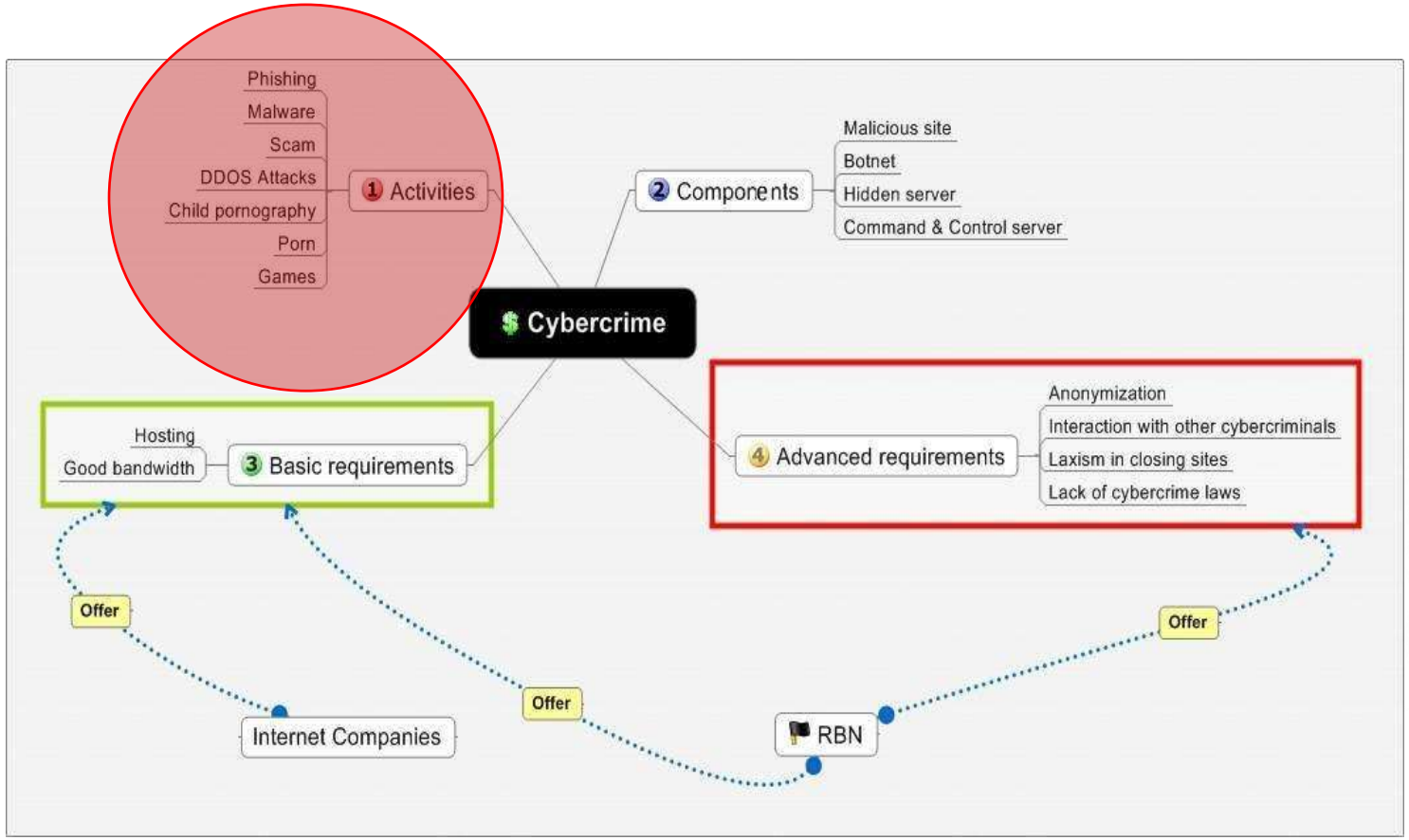
UNIVERSITÀ DI PARMA

>L'Underground Economy

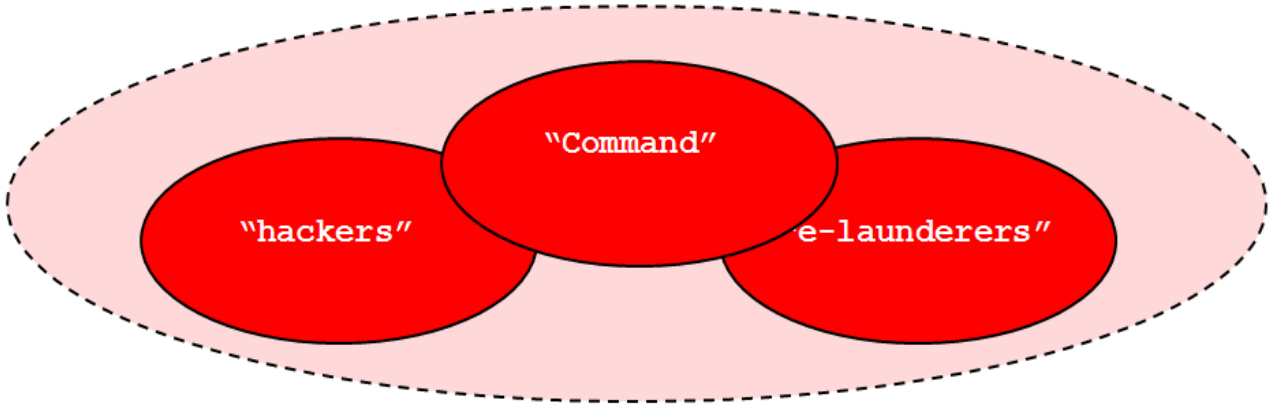
- Quando si parla di Underground Economy la nostra mente va a **piccoli criminali** localizzati in paesi dell'est Europa
- Che utilizzano **modelli «casalinghi»**
- Che **nulla hanno a che fare** con il crimine organizzato ed un'**organizzazione complessa**
- **SBAGLIATO!**
- Vediamo qualche **esempio**...

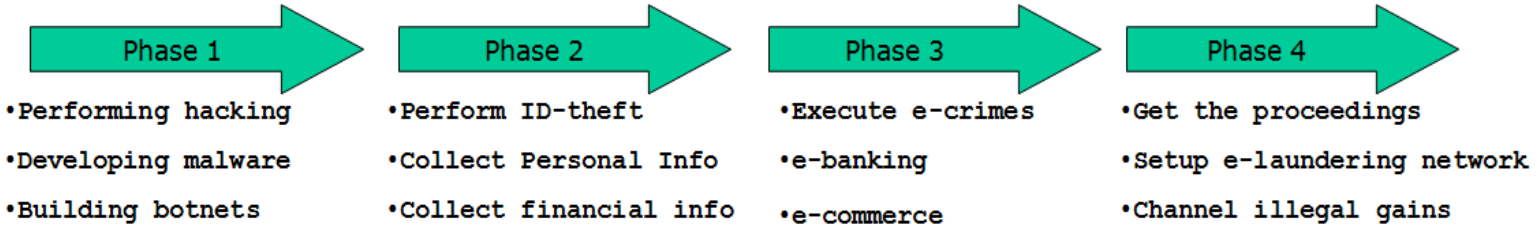
Quando il CO (crimine organizzato) incontra il Cybercrime

>il «Modello RBN» (Russian Business Network)



› Catena del comando (e fasi operative)



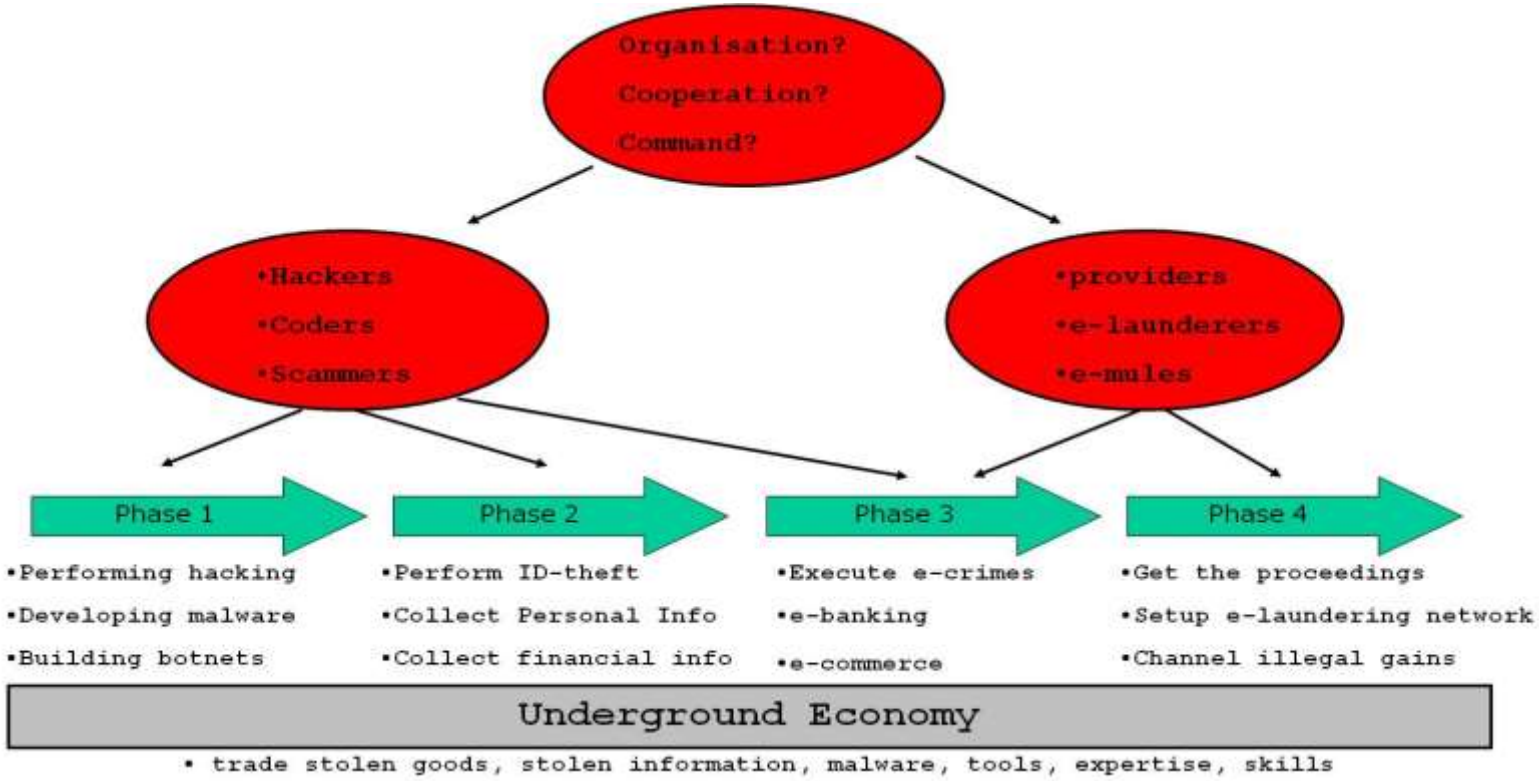


Underground Economy

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

Quando il CO (crimine organizzato) incontra il Cybercrime

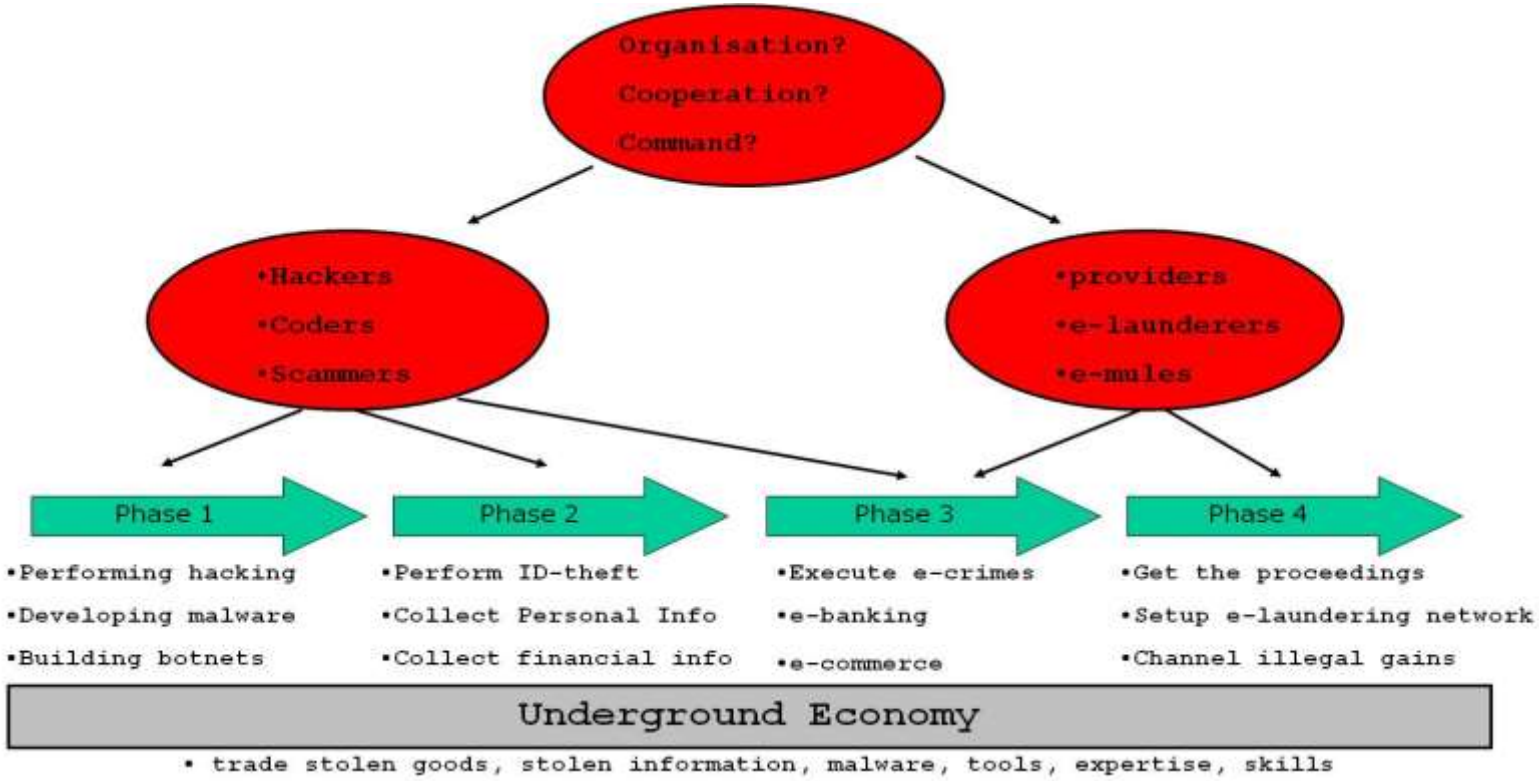
› Approccio basato su «macro unità operative»



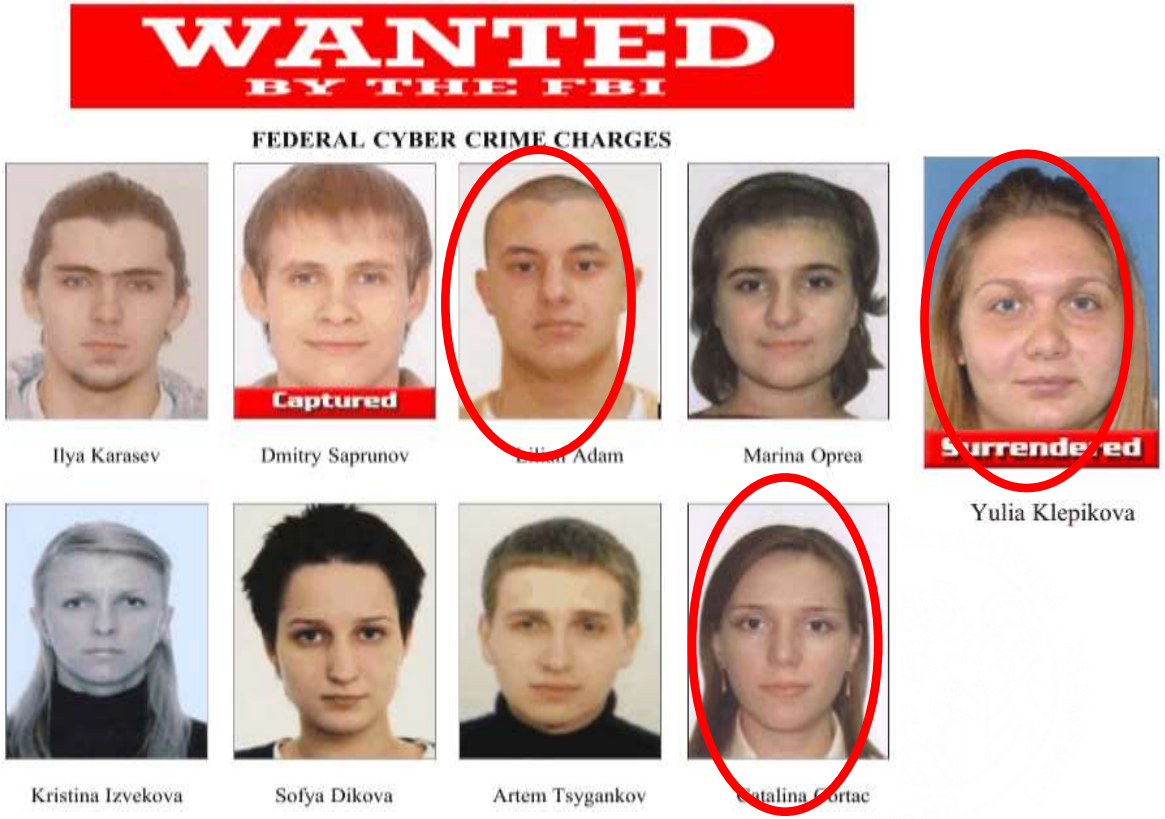
...quello era il modello RBN...ora le cose sono cambiate

UNIVERSITÀ DI PARMA

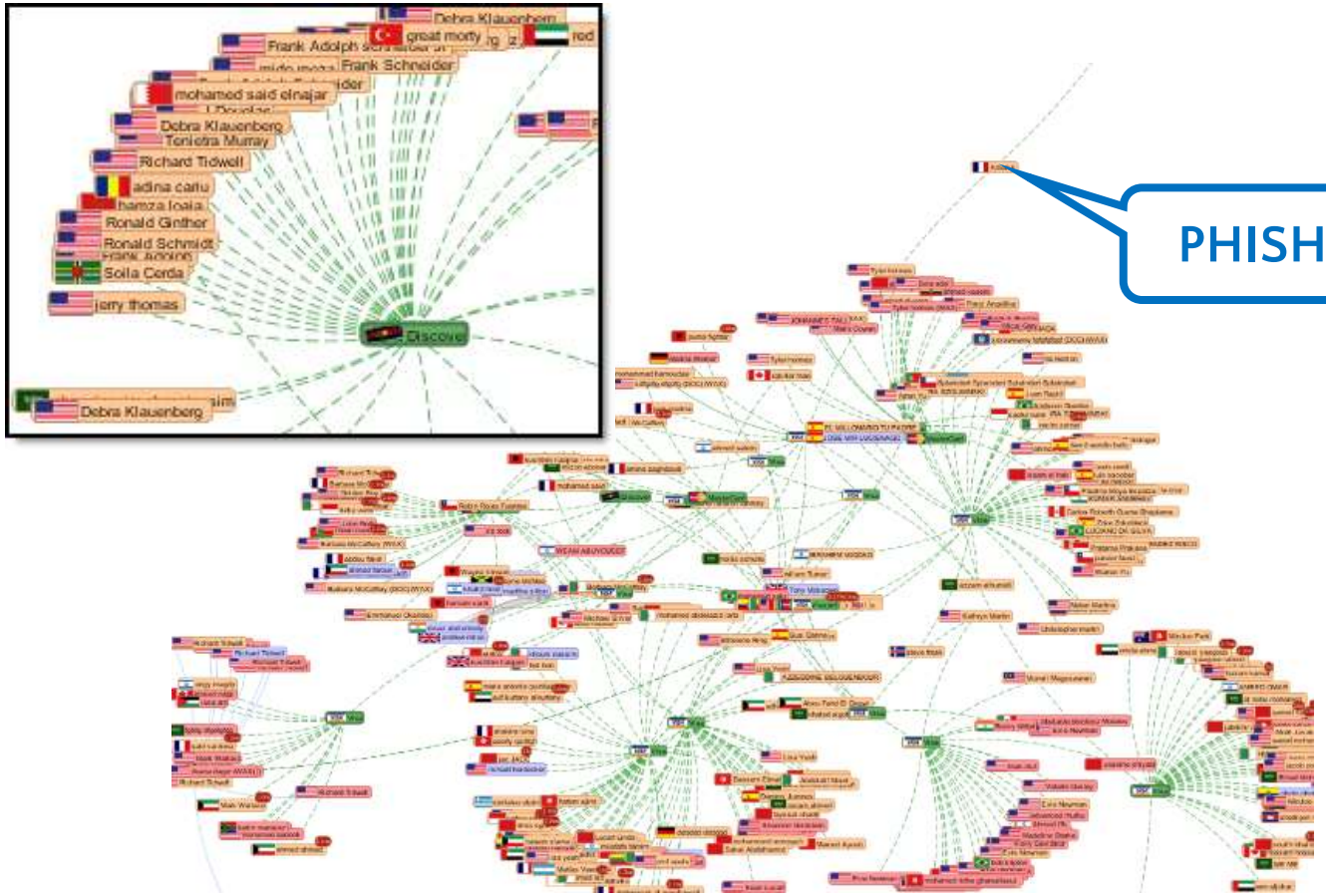
> Approccio basato su «macro unità operative»



Money Mules: «very normal people?»



Livello di «gestione della cyber investigation» molto complesso



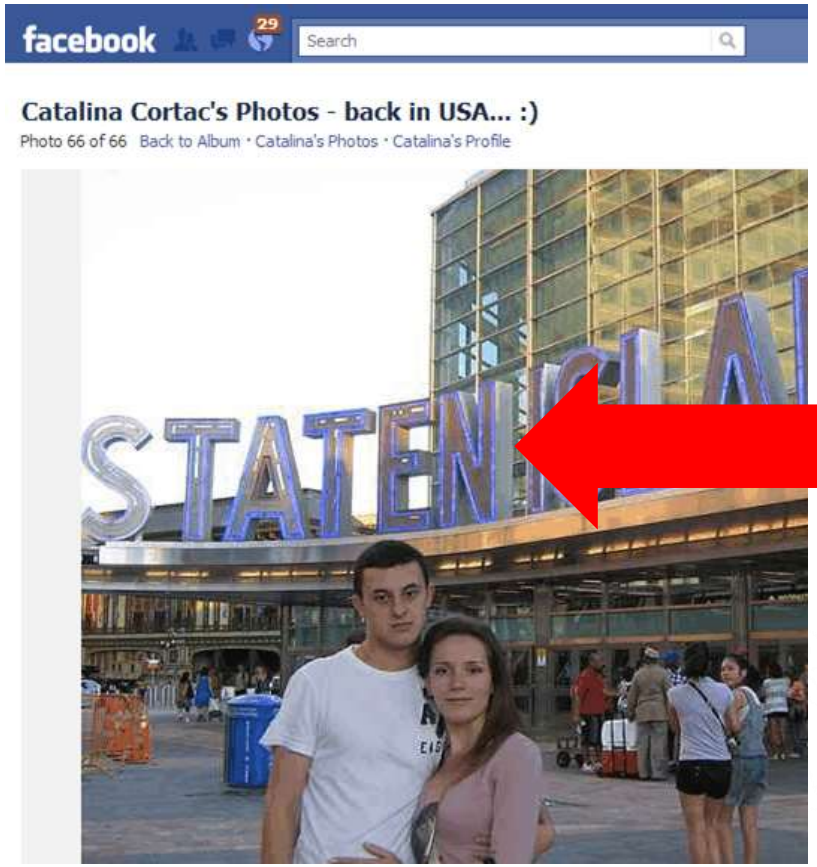
OSINT for Investigations

UNIVERSITÀ DI PARMA

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

-- Deputy Director of National Intelligence, Thomas Fingar

OSINT, social e muli



Catalina Cortac

Lilian Adam

A volte, facili da prendere...

A volte, facili da prendere...

UNIVERSITÀ DI PARMA

Criminal Persona

Money Mule

Real Persona

Yulia Klepikova

Yulia Klepikova

Il crimine, nel passato («crime»)

UNIVERSITÀ DI PARMA

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

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

Per esempio, agli inizi del '900, con l'avvento dell'**automobile**, i "cattivi" iniziarono a **rubarle**.

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

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

Il crimine, nel passato («crime»)

UNIVERSITÀ DI PARMA

Dalle "automobili" alle "informazioni": dal "bene" al "dato"

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

Hai l'informazione,

hai il potere.

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

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

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

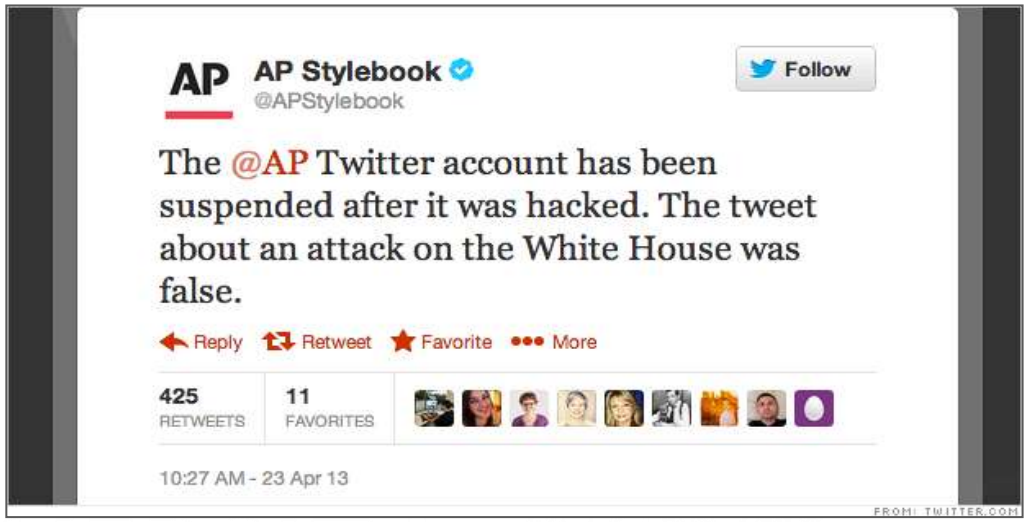
Esempi ? (…imbarazzo della scelta ;-)

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

Un esempio reale: l'attacco ad Associated Press nel 2013

UNIVERSITÀ DI PARMA

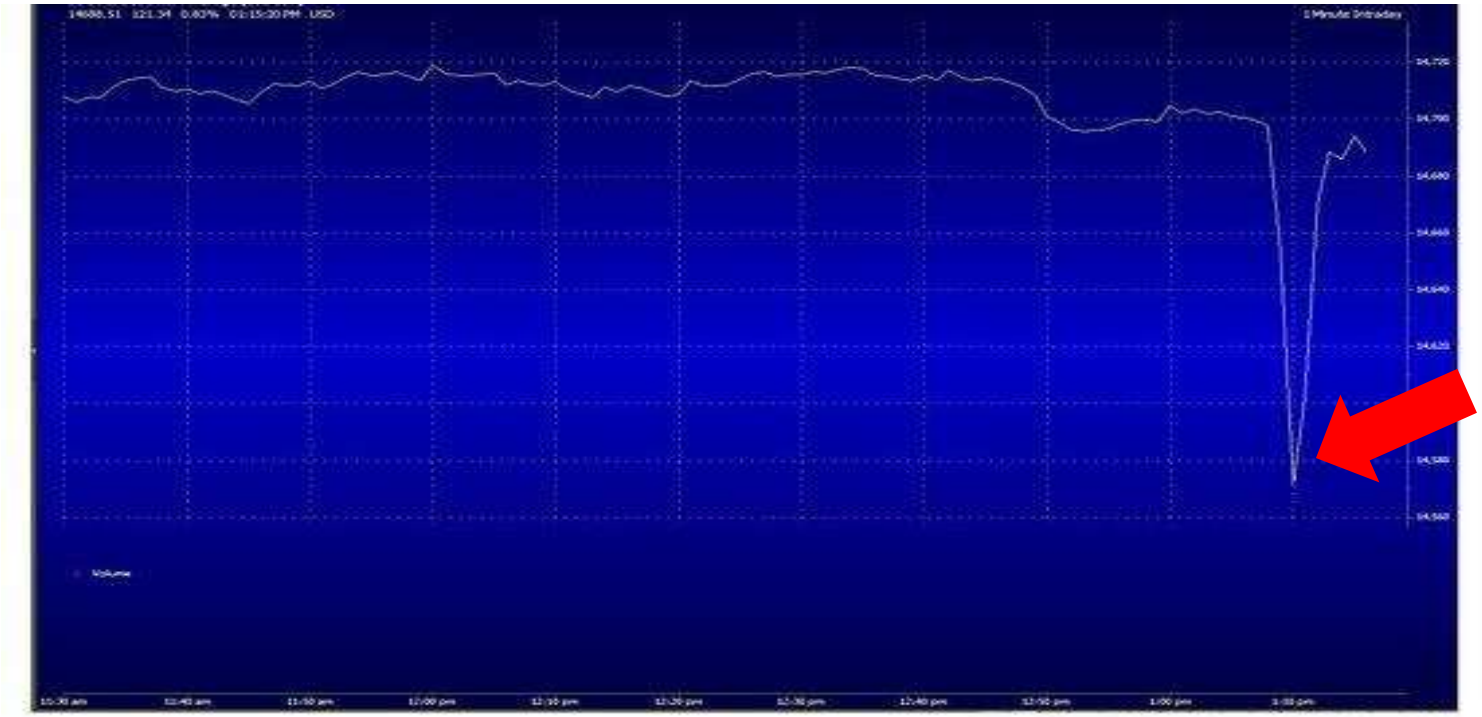
La rapidità delle conseguenze nel cyberspazio è esponenziale



A PsyOps "test" via Twitter (= stavano scherzando)

(by the "Syrian Electronic Army", a pro-Assad mercenary group)

La rapidità delle conseguenze nel cyberspazio è esponenziale



Associated Press Twitter account hijacking caused to NYSE a 53B $ loss in 5 minutes

E senza essere la «Borsa di NYC»...

UNIVERSITÀ DI PARMA

Chi deve aspettarsi gravi danni finanziari dagli #attacchi informatici?
Dipende da quanto sei dipendente dalla #tecnologia o da proprietà #intellettuali
#Tissue regenerix Group è una società medica altamente tecnologia, che si concentra sulla ricerca e sviluppo di prodotti rigenerativi ossei induttivi per il trattamento dei pazienti in tre aree chiave: #Biochirurgia, #Ortopedia e #Odontoiatria

Martedì 27 Gennaio i suoi sistemi informatici sono stati interessati da un attacco informatico con #esfiltrazione di dati gettando il valore del titolo azionario giù fino al 22%.
La società ha dichiarato di aver messo offline i sistemi interessati, nominato specialisti esterni per indagare sull #incidente

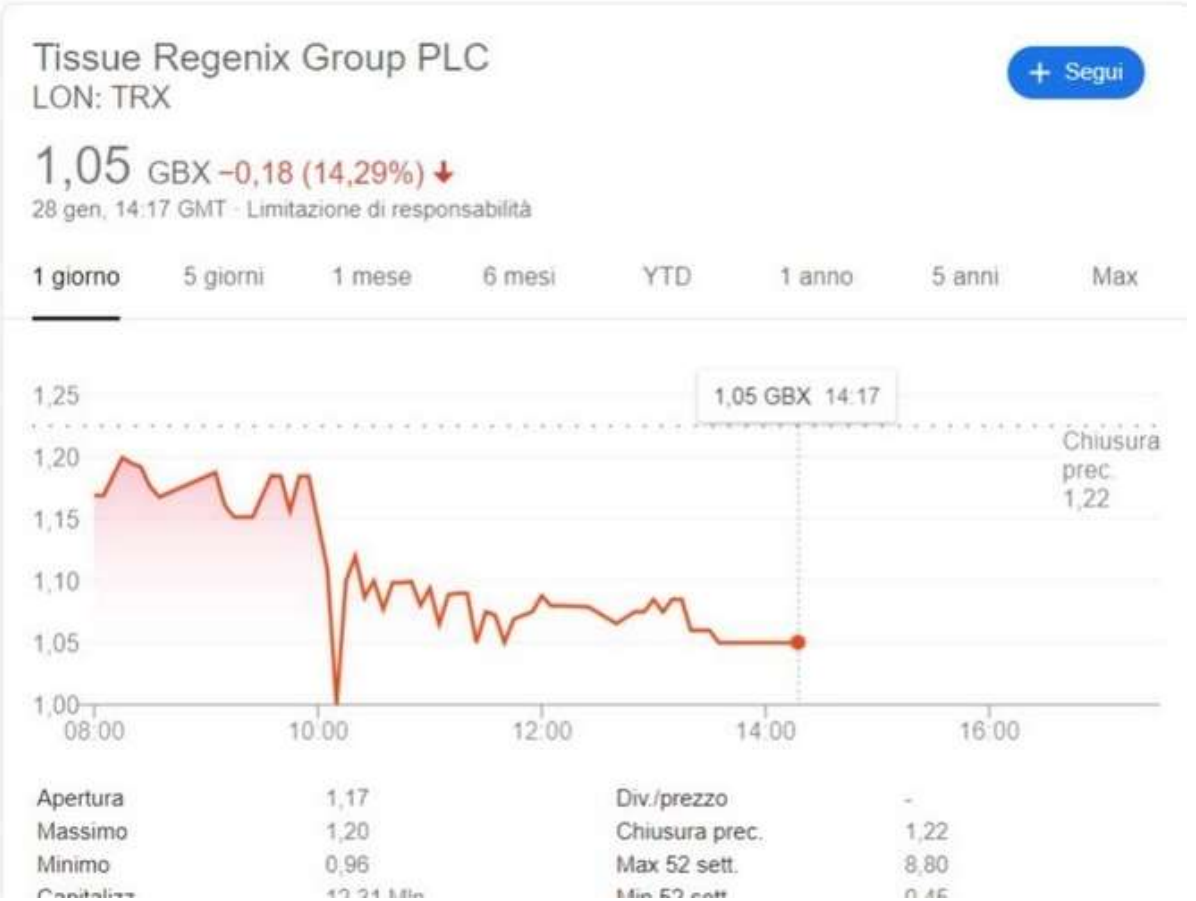
#CyberSecurity #gdpr #malware #hacker #patch #lifefirst KELONY® First Risk-Rating Agency #WPF

See translation

Tissue Regenix Group PLC
LON: TRX
+ Segui

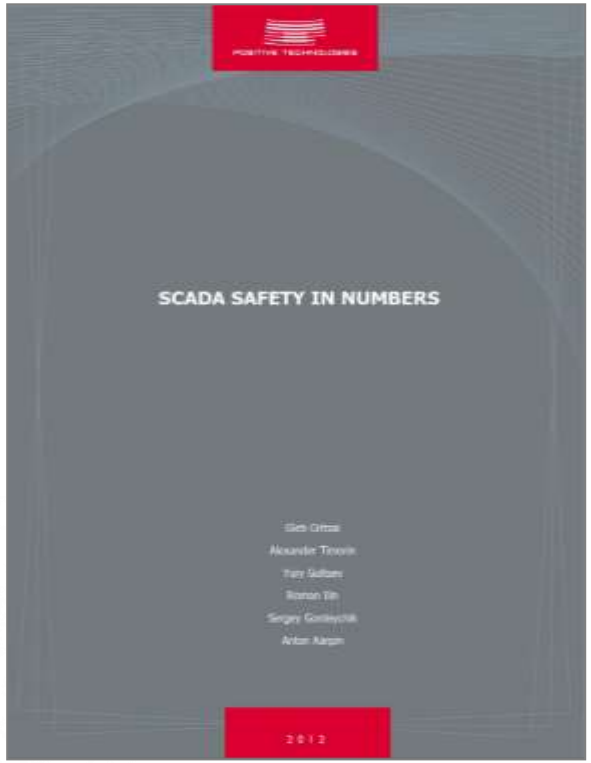
1,05 GBX −0,18 (14,29%)
28 gen, 14:17 GMT · Limitazione di responsabilità

See translation

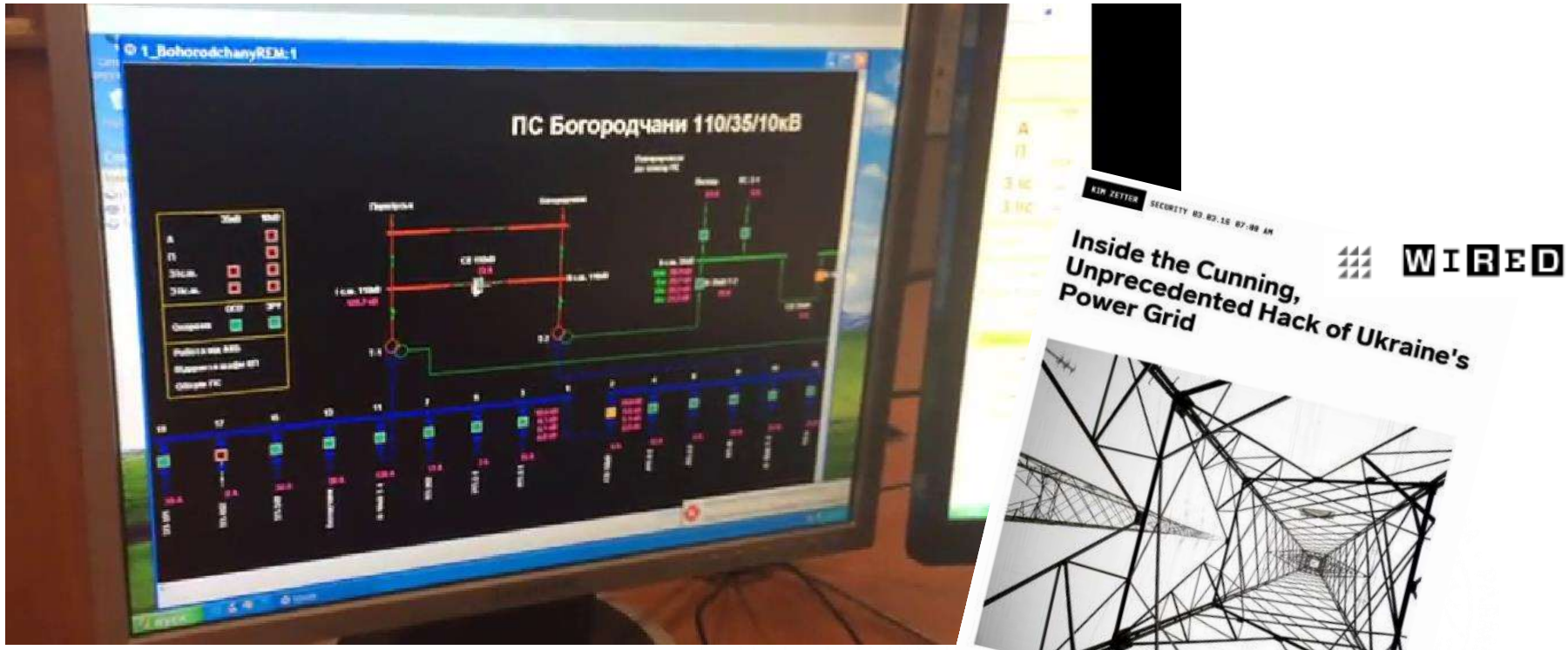


Le infrastrutture critiche oggi sono estremamente a rischio

- The number of detected vulnerabilities has increased by **25 times** (*since 2010*).
- **50%** of vulnerabilities allow to **execute code**.
- There are **exploits for 35% of vulnerabilities**.
- **41%** of vulnerabilities are **critical**. More than **40%** of systems available from the Internet **can be hacked by unprofessional users**. (Metasploit?)
- **54%** and **39%** of systems available from the Internet in Europe and North America respectively are **vulnerable**.
- ...Fate un giro su **Shodan** ☹



CASE STUDIES [Ukraine], VIDEOCLIP TIME!



FLASHBACK:
PERCHE' SUCCEDE TUTTO QUESTO?

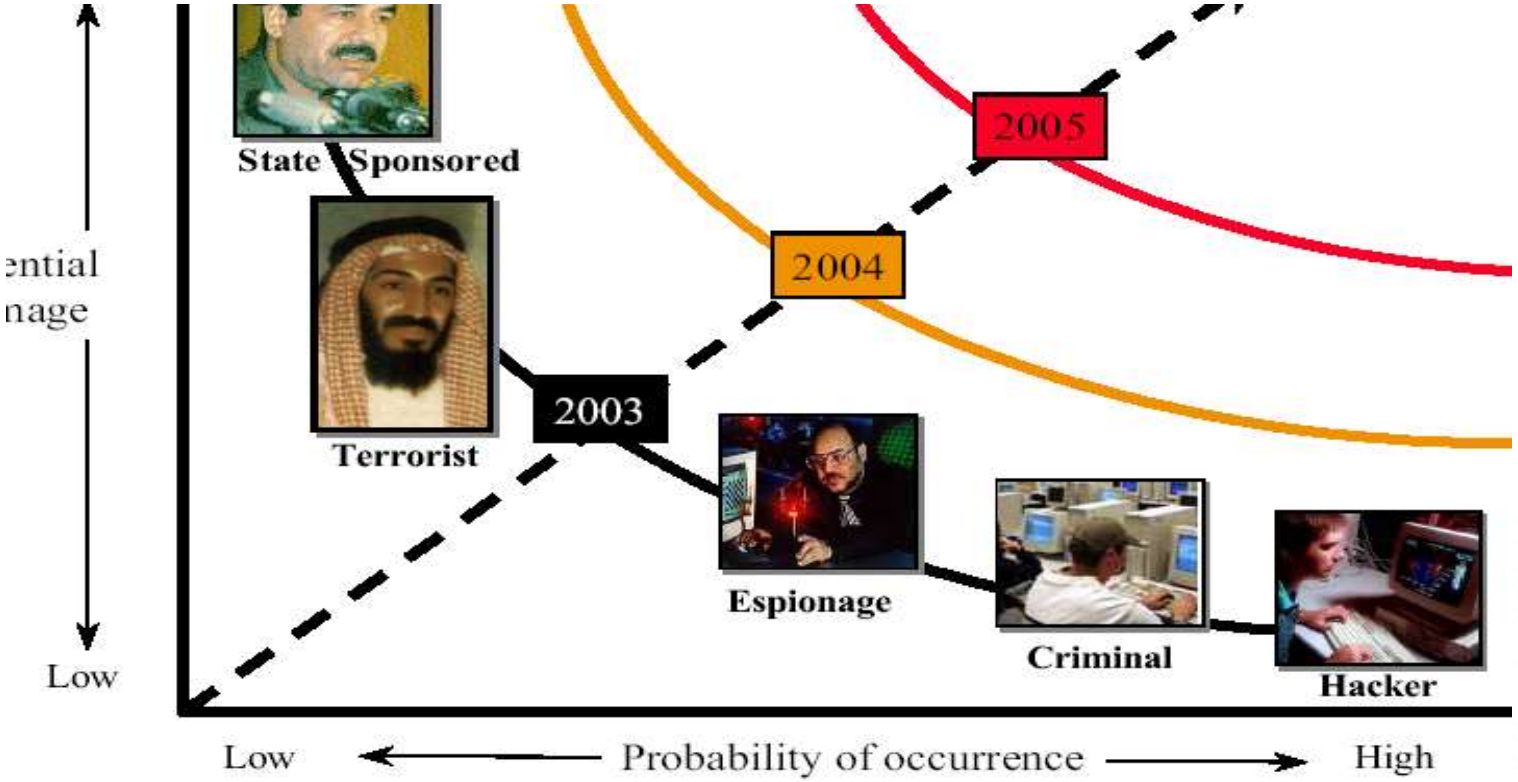
UNIVERSITÀ
DI PARMA

Today's Oil

UNIVERSITÀ DI PARMA

- **L'Informazione e' il petrolio del XXI secolo**
- Information = **Data**
- Information = **Power**
- Data = Bit & Bytes ("**Files**": .ppt, .txt, .doc, .passwd…)
- Data = **Insights**, **Money**, **Reputation**, **Impacts**, **Regulations**, **Fines**

The Threat is Increasing



Source: 1997 DSB Summer Study

From Cybercrime to...

UNIVERSITÀ DI PARMA

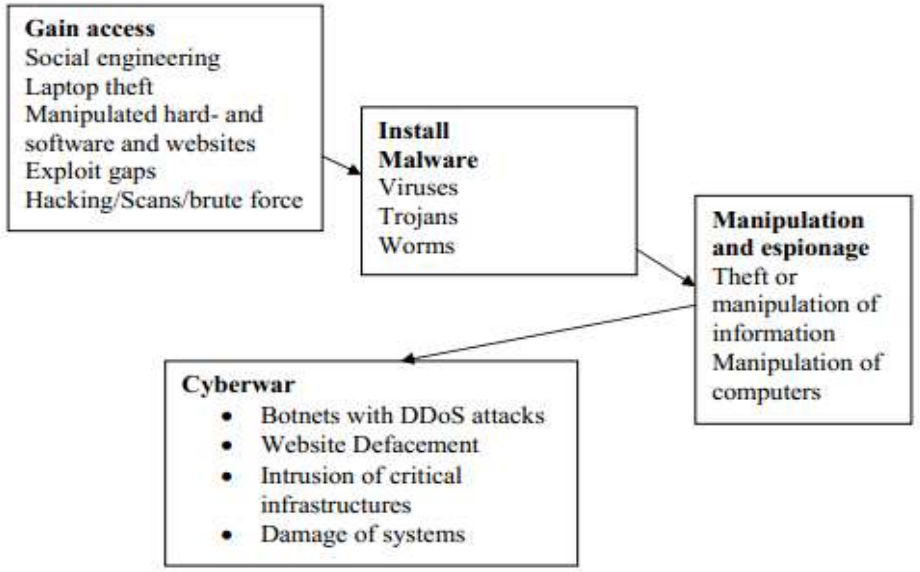
Stiamo parlando di un ecosistema che e' **troppo spesso sottovalutato**: nella maggior parte dei casi, il Cybercrime e' il punto di partenza, o di transito, verso altri ecosistemi:

- **Information Warfare**
- **Black Ops**
- **Cyber Espionage**
- Hacktivism
- (private) **Cyber Armies**
- **Cyber Terrorism**
- **Underground Economy** and **Black Markets**:
  - Organized Crime
  - Carders
  - Botnet owners
  - 0days
  - Malware factories (APTs, code writing outsourcing)
  - Lonely wolves
  - "cyber"-Mercenaries

Cyber * (espionage, crime, war

UNIVERSITÀ DI PARMA

> Come possiamo costatare, non ci sono poi così tante differenze con l'approccio proprio dell'hacking

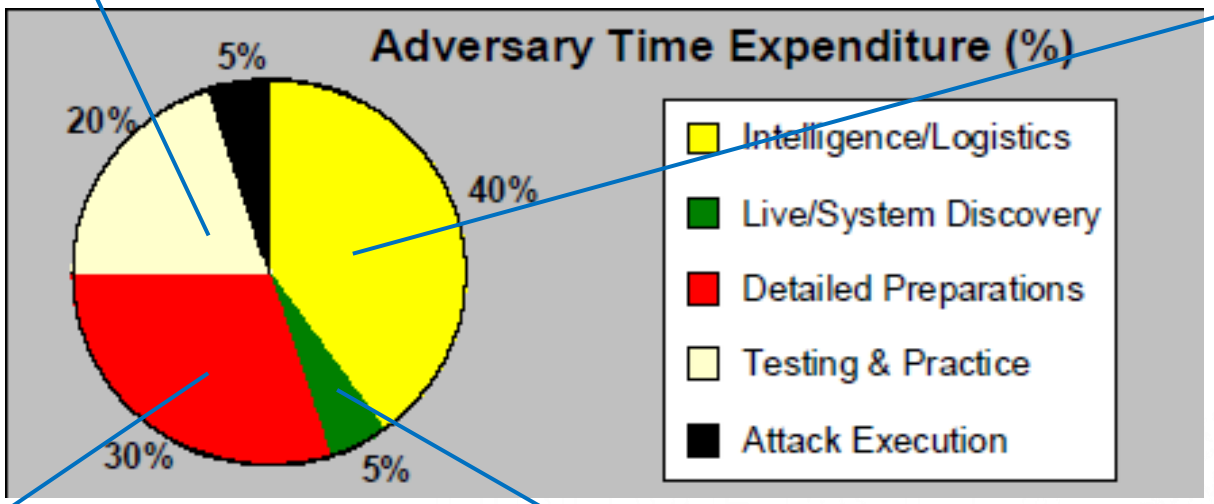


Source: Saalbach: «**Cyberwar** Methods & Practice»

CyberWar VS Cybercrime

UNIVERSITÀ DI PARMA

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



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

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

- Purchase L2/L3 system data

Alexander Klimburg 2012

La discussione sui prezzi

UNIVERSITÀ DI PARMA

Penso che vi ricordiate di questo listino:

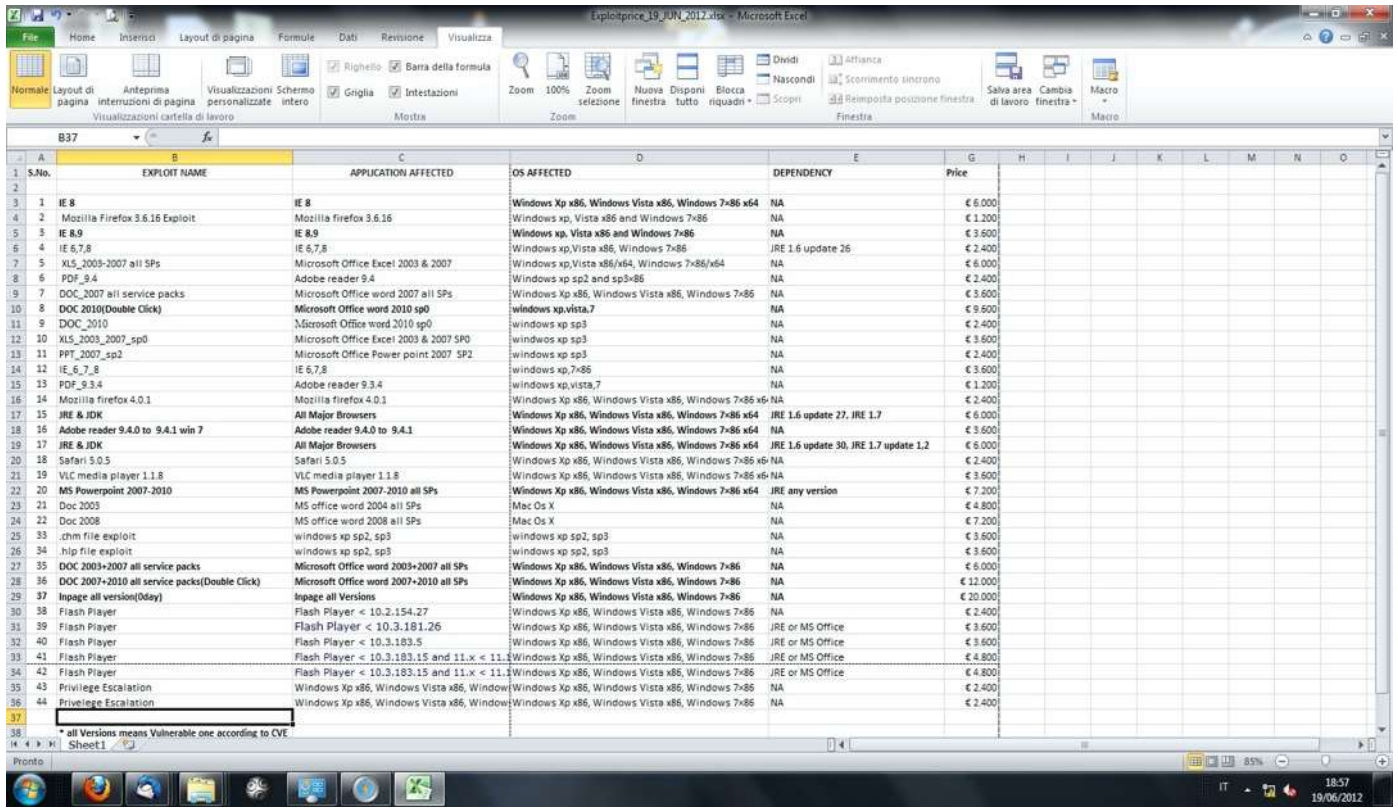
ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

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

La discussione sui prezzi

UNIVERSITÀ DI PARMA

Che ne dite di questo? (roba “cheap”, quella degli indiani) ☺



Exploitprice_19_JUN_2012.xlsx - Microsoft Excel

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

* all Versions means Vulnerable one according to CVE

Dov’è la verità?

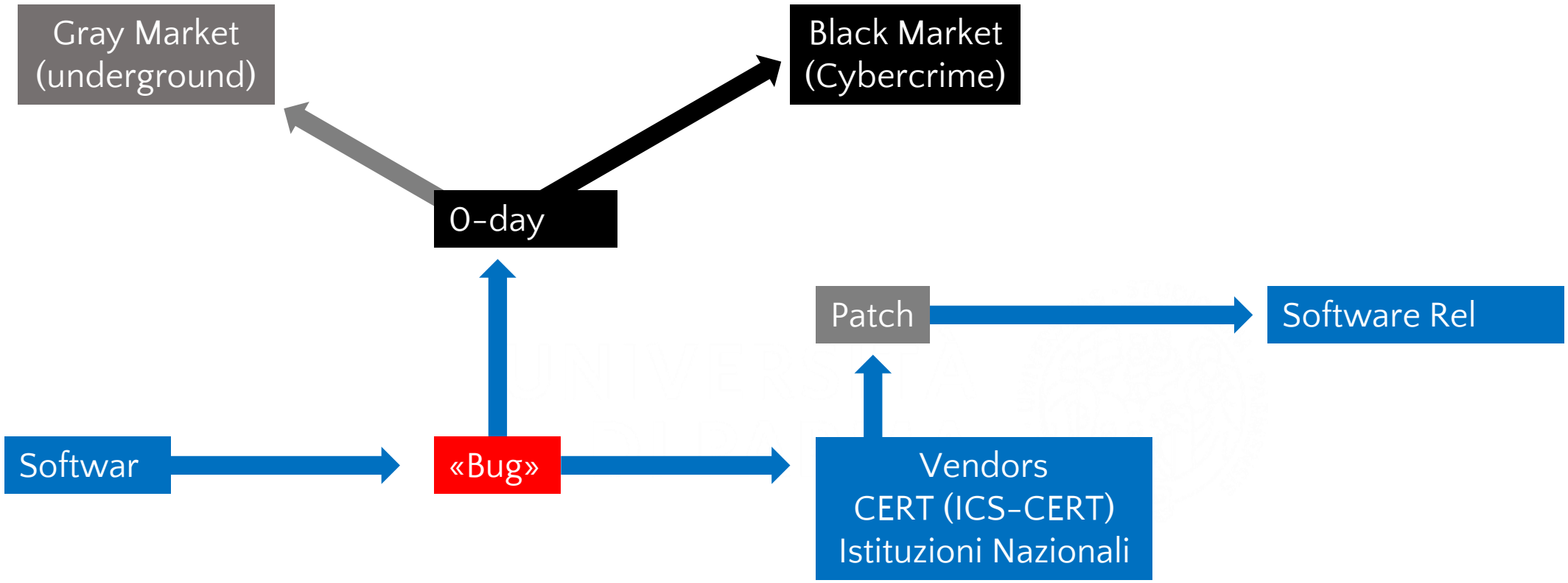
Qual è l’aproccio corretto in tema di «prezzi»?

UNIVERSITÀ
DI PARMA

Realtà oltre il mito

UNIVERSITÀ DI PARMA

> 0-day Market



Un approccio differente (più serio?)

UNIVERSITÀ DI PARMA

Conoscenza Pubblica della vulnerabilità	Tipo di acquirente = SI società di sicurezza IT INT = Agenzie di Intelligence per uso governativo(Protezione sicurezza nazionale) MIL = MoD /attori correlait per uso di guerra CO = Cybercrime	0-day Exploit code + PoC Cost: Min/Max
Y	IS	10K – 50K USD
Y	INT	30K – 150K USD
Y	MIL	50K – 200K USD
Y	CO	5K – 80K USD
N	ALL	X2 – X10

Un approccio differente (più serio?)

UNIVERSITÀ DI PARMA

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

Ma come vengono pagati i prodotti/servizi di Cybercrime?

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

Ma come vengono pagati i prodotti/servizi di Cybercrime?

Probabilmente conoscete **Hawala** o Hewala

….noto anche come **hundi**, è un sistema di trasferimento di valore informale basato sulle prestazioni e l'onore di una vasta rete di mediatori di denaro, che si trova principalmente nel Medio Oriente, Nord Africa, il Corno Africa, e il subcontinente indiano, operano al di fuori di – o in parallelo – rispetto bancario tradizionale, i canali finanziari e sistemi di rimessa.

Imparare l'approccio finanziario dal terrorismo

UNIVERSITÀ DI PARMA

Molti sistemi di pagamento elettronico **seguono il modello HAWALA**

E sono costruiti con infrastrutture **simili**

Ora sono supportati da **un'infrastruttura digitale**

Non vi è traccia nelle reti bancarie

Il denaro **sparisce** in un luogo e **riappare** in un altro

Valute Underground

UNIVERSITÀ DI PARMA

Esaminiamo
alcuni esempi

C’è più di un metodo per trasferire denaro

Valute «Underground»

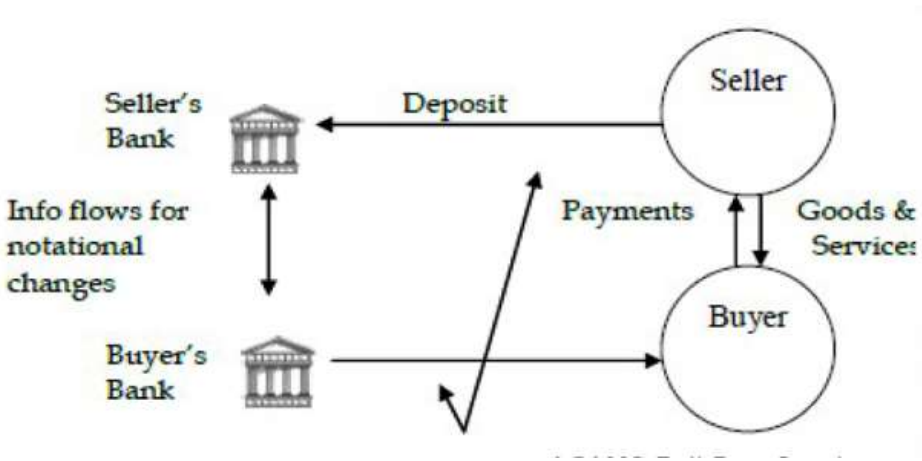
Ovviamente conoscete Paypal e gli altri sistemi di pagamento elettronico “regolari” …sono semplici e poco interessanti

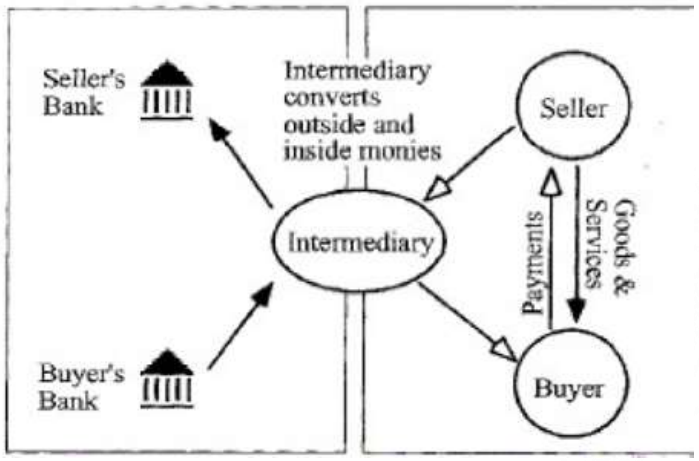
Figure 4: Electronic cash system (Charalampos, 2004)

Valute «Underground»

UNIVERSITÀ DI PARMA

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





Valute «Underground»

UNIVERSITÀ DI PARMA

Getting to know "Underground" money systems

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

Valute «Underground»

UNIVERSITÀ DI PARMA

There are many:

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

Where is webmoney office in Thailand?

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

Pataya!! Where gangsters are ;-)

Valute «Underground»

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

AlertPay, SMS, LiqPay

Valute «Underground»

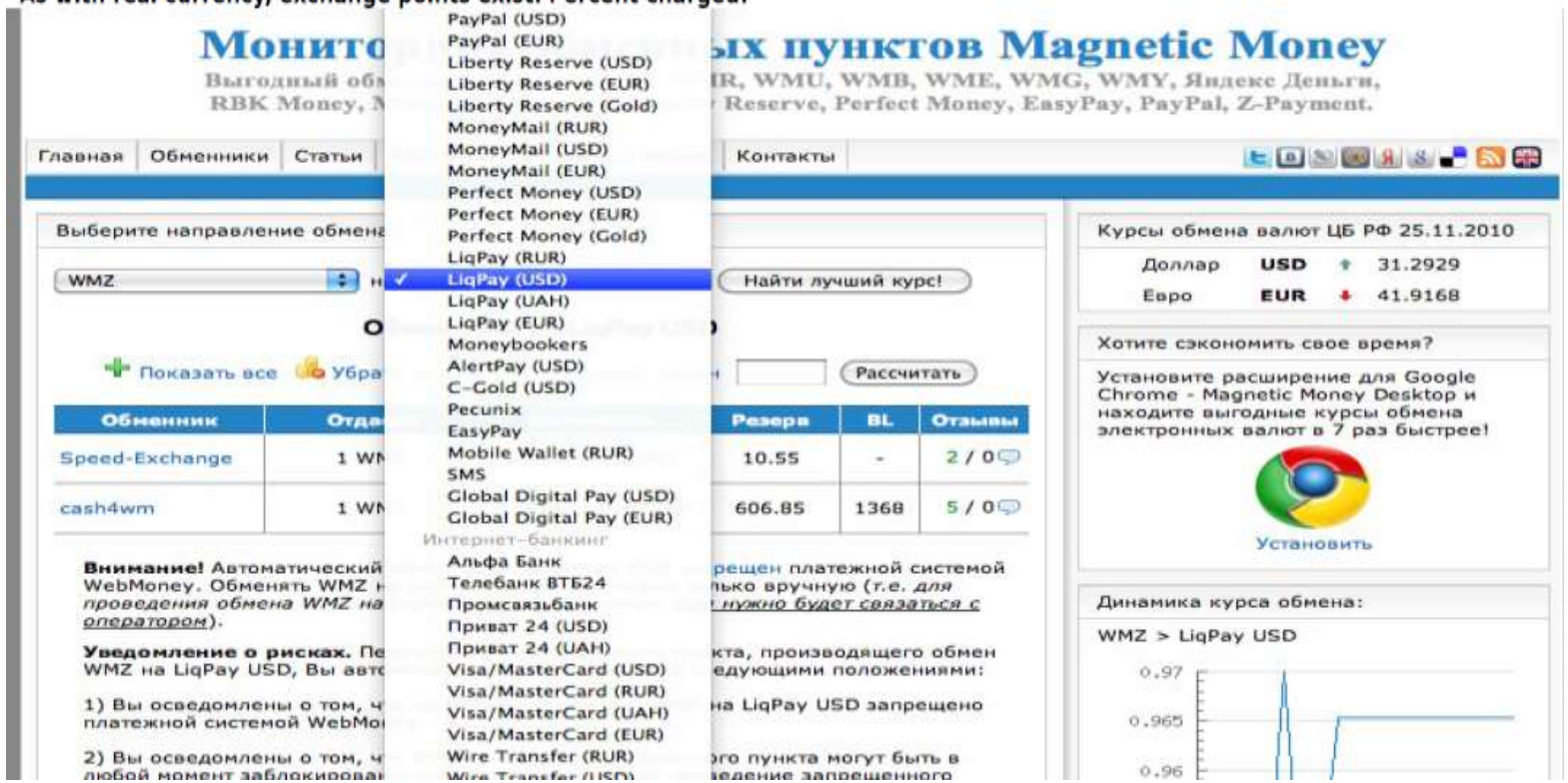
They feature “awesome” geographical locations

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

Valute «Underground»

UNIVERSITÀ DI PARMA

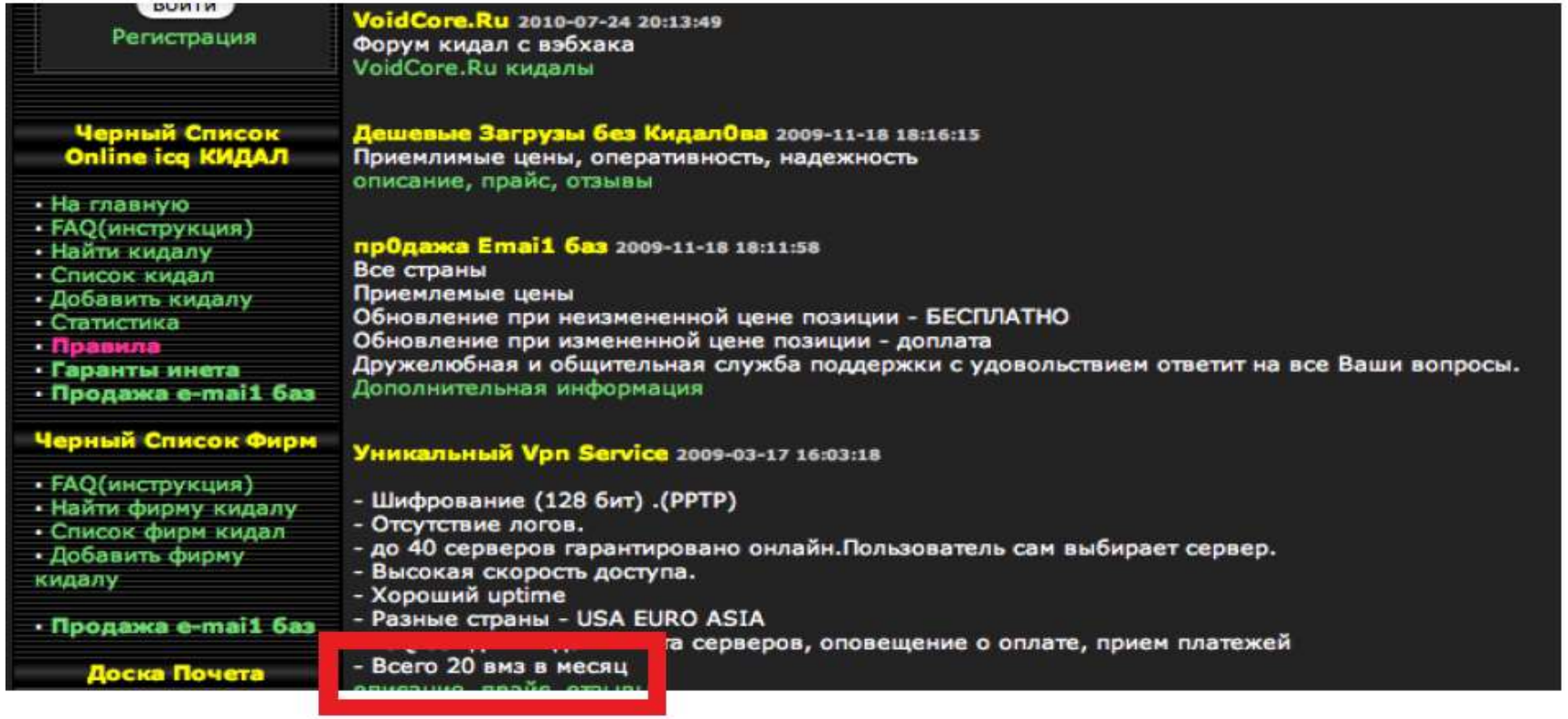
As with real currency, exchange points exist. Percent charged:



Valute «Underground»

UNIVERSITÀ DI PARMA

WMZ - widely used on black markets



Valute «Underground»

UNIVERSITÀ DI PARMA

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

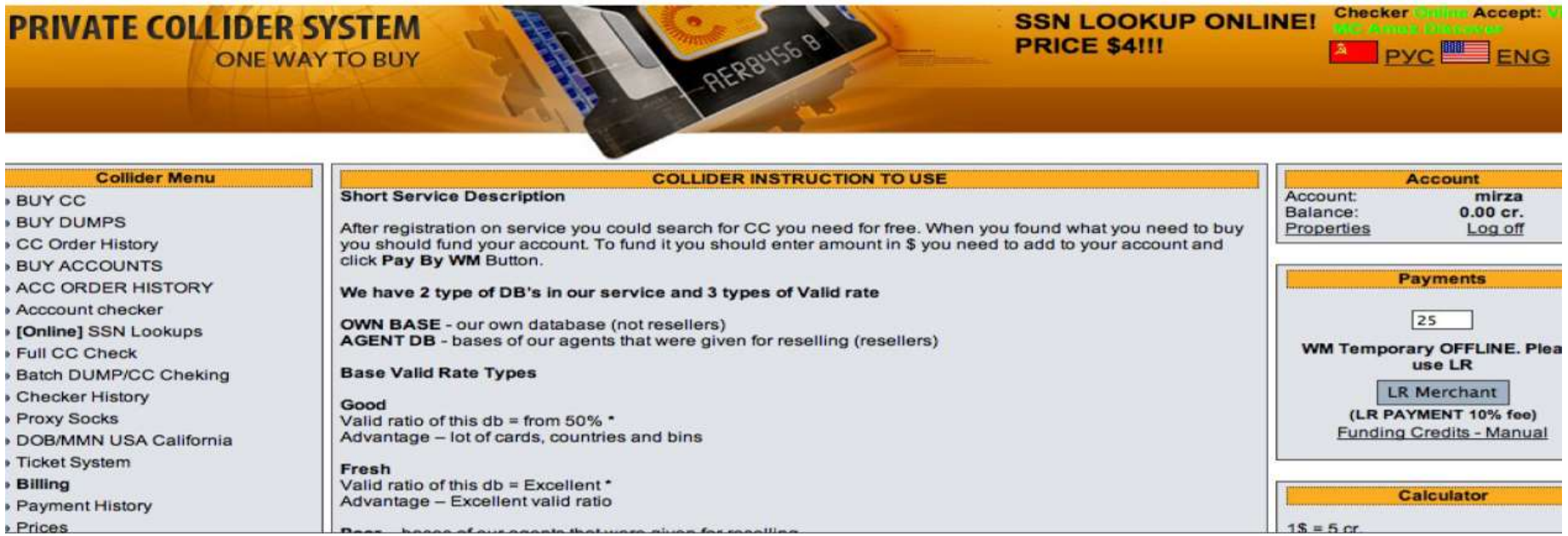
Яндекс халявный картон Найти

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

Valute «Underground»

UNIVERSITÀ DI PARMA

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



Che cosa sta accadendo?

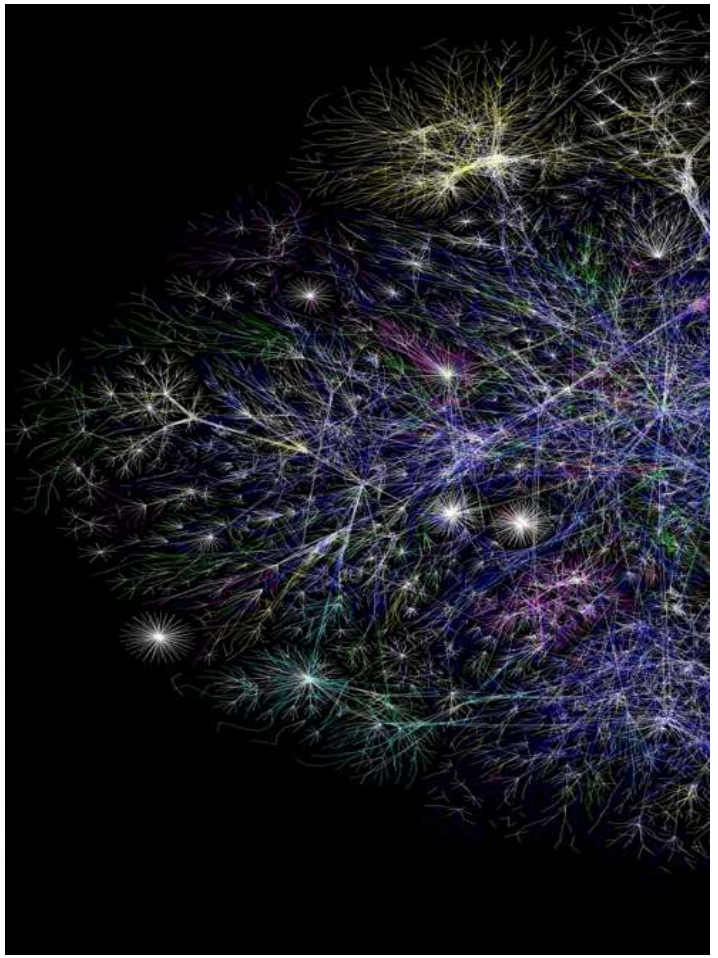
UNIVERSITÀ DI PARMA

- Il **Cybercrime e l'Information Warfare** hanno un **ampio spettro di azione e utilizzano tecniche di intrusione** che sono oggi, in qualche modo, a disposizione di una quantità **crescente di attori,** che li utilizzano per **realizzare obiettivi diversi,** con **approcci e intensità che possono variare profondamente.**

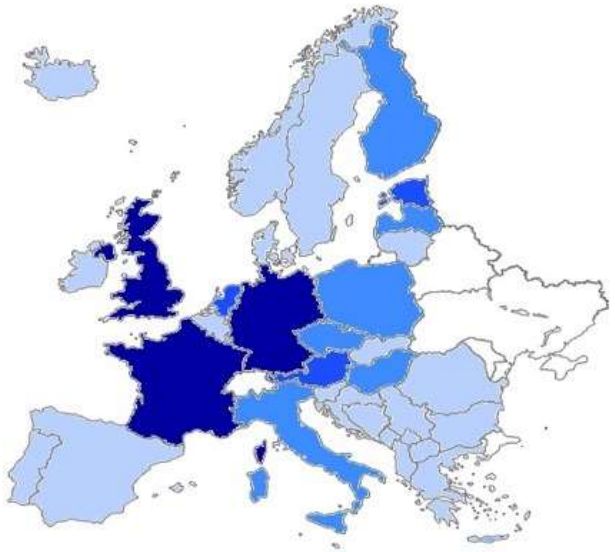
- **Quanto sopra è lanciato contro ogni tipo di target**: Infrastrutture Critiche, sistemi di governo , sistemi militari, aziende private di ogni genere, banche, Media, Gruppi di interesse, privati cittadini ….

  - Stati
  - IC / LEAs
  - Cyber crimine organizzato
  - Hacktivismo
  - Spie industriali
  - Terroristi
  - Corporazioni
  - Cyber Mercenari

Tutti contro tutti



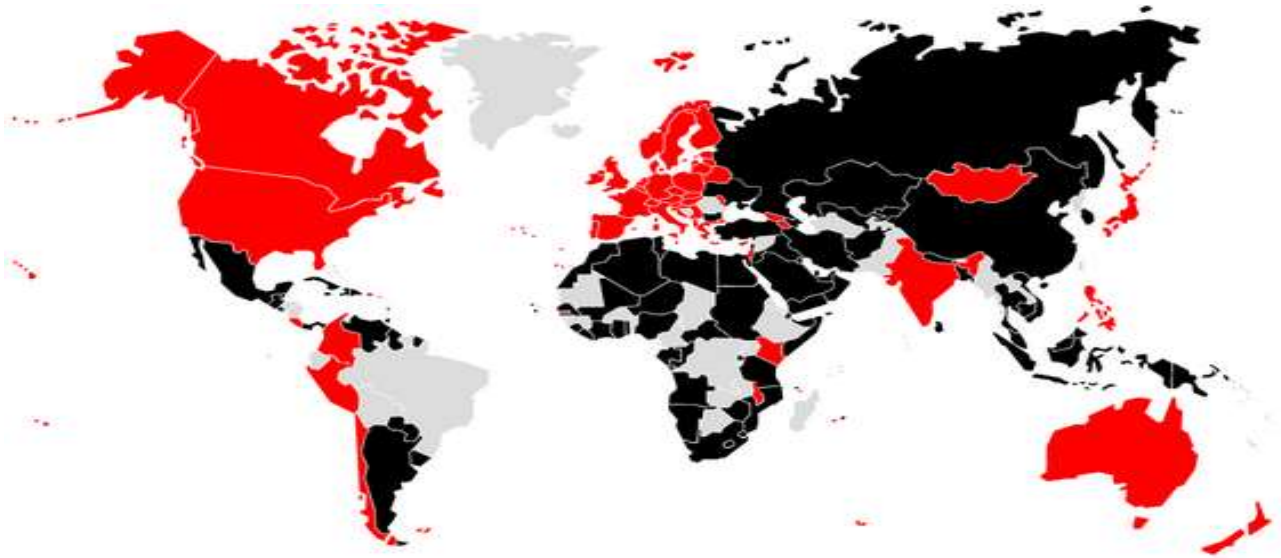
> Cambiamento Geopolitico: 2013 – Mappa della evoluzioni della Cyber difesa negli stati membri (parziale)



Credits: Raoul Chiesa

UNIVERSITÀ DI PARMA

> Cambiamento Geopolitico : 2013 – ITU Dubai Assemblea Generale Dicembre (red=not signed; black=signed)



Credits: Raoul Chiesa

CYBER ESPIONAGE

UNIVERSITÀ
DI PARMA

UNIVERSITÀ DI PARMA

> Il Cybercrime

- Parliamo di un ecosistema che **è spesso sottovalutato:** nella maggioranza dei casi **è il punto di partenza o il transito** verso altri ecosistemi :

1. Guerra dell'Informazione
2. Black Ops
3. **Cyber Espionage (industriale, governativo, militare)**
4. Hacktivismo
5. Cyber Milizie (private)
6. Underground economy e Mercati Neri
   - Crimine organizzato
   - Carders
   - Botnet owners
   - 0days
   - Malware factories (APTs, code-writing outsourcing)
   - Lupi solitari
   - "cyber"-mercenari , Web sommerso, etc

> Operation Nitro, Operation Red Dragon

- Lo spionaggio industriale e commerciale ha raggiunto nell'anno 2011 **livelli senza precedenti**.
  - Sono venute alla luce **attività continuative di intelligence ai danni di importanti industrie**, principalmente occidentali, realizzate tramite **sofisticate intrusioni** da parte di team di **specialisti di altissimo livello**.

- Le così dette "Operation Nitro" ed "Operation Night Dragon" hanno interessato **numerose multinazionali del settore chimico, energetico ed oil & gas**.

- Mediante **attacchi mirati** di tipo *spear phishing* gli aggressori hanno preso il controllo dei pc portatili di alcuni dipendenti, potendo in tal modo utilizzare le **legittime connessioni VPN delle vittime** per connettersi in remoto agli applicativi ed ai server aziendali interni, **assumendone il controllo** tramite malware e/o monitorandone le attività.

- Questo genere di attacchi *stealth*, che si **protraggono per mesi** (in alcuni casi anni) prima di essere scoperti, sono particolarmente insidiosi e difficili da evitare, tanto che nessuna organizzazione oggi può dirsi al riparo da essi.

> Il Cyber Espionage

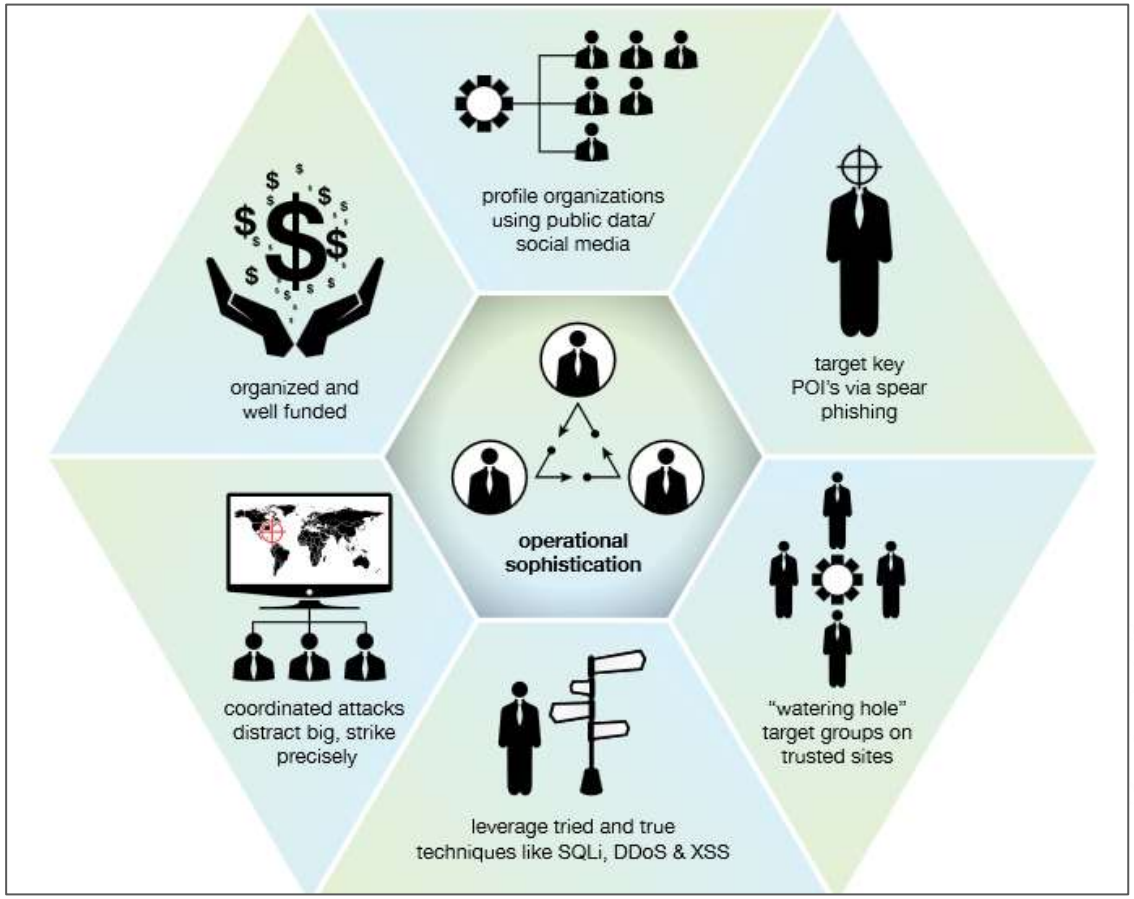
- La **complessità** e i **costi** infrastrutturali ed operativi dello spionaggio (in senso ampio) nel corso degli anni sono **scesi drasticamente**, complice (causa) la rivoluzione informatica e la c.d. "Società Digitale".

- Nella maggior parte dei casi, l'**informazione** risiede (anche, o solo) su **supporti digitali** e **viaggia in rete**.

- Un **primo effetto** è il **totale annullamento** del concetto di "furto" (proprio del crimine) e la **conseguente centralità** del concetto di "copia" (proprio del mondo dello spionaggio):
  - ciò che "è sempre lì", evidentemente "è al sicuro";
  - aumento del tempo necessario alla scoperta;
  - diminuzione del tempo necessario allo smercio e conseguente cash-out.

- Purtroppo gli incidenti (pubblici) toccano **sia il mondo civile che quello militare**:
  - insider (motivazioni politiche, etiche, religiose, fama e mass media, corruzione, ricatto, ignoranza);
  - contractor (fornitori esterni, consulenti, accessi VPN e RAS, etc..);
  - "competitor" (civile e militare) sia *State-Sponsored* che *Independent.*

Un nemico con risorse illimitate



… E PER
“NON FARCI MANCARE NULLA”…

UNIVERSITÀ
DI PARMA

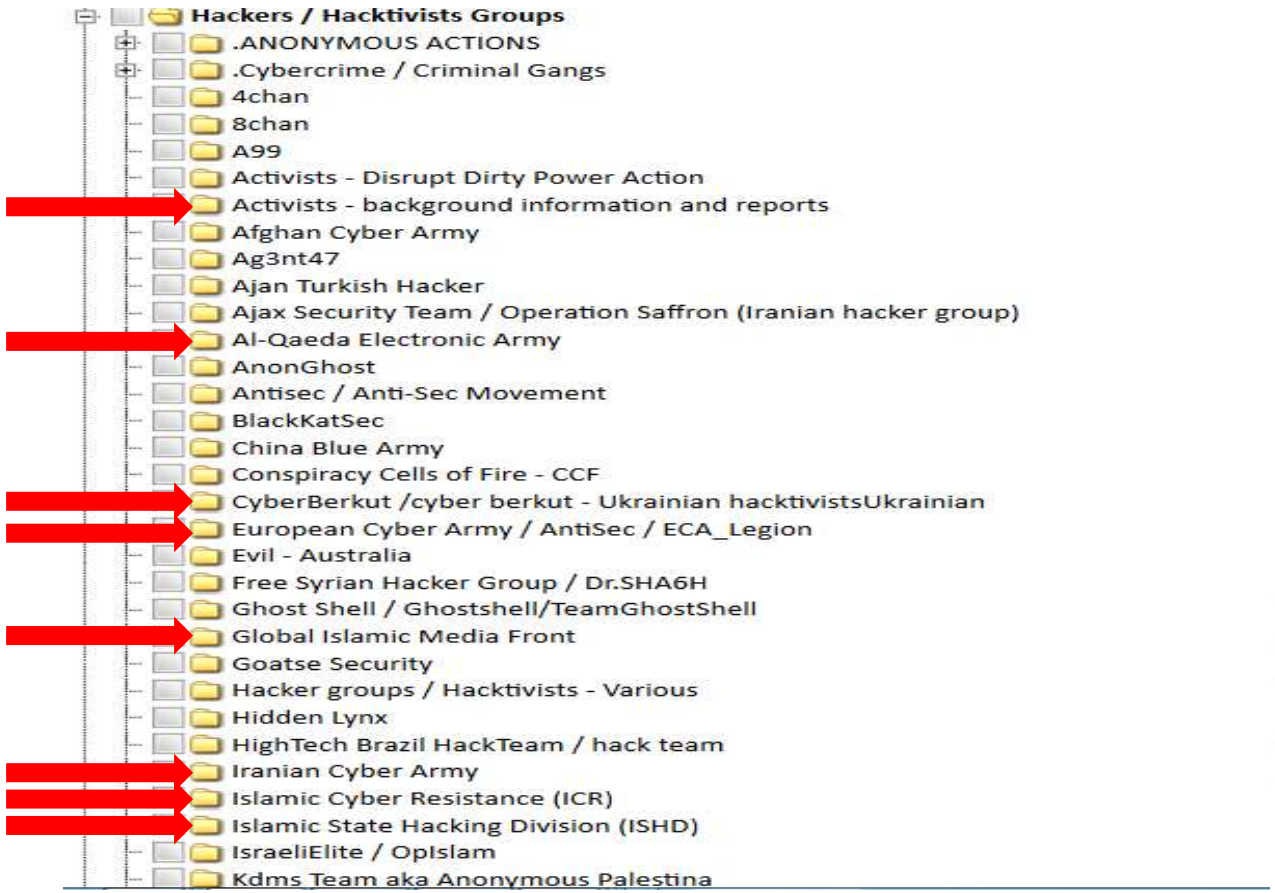
Gruppi noti di “Cyber-Terrorism” (estratto)

UNIVERSITÀ DI PARMA

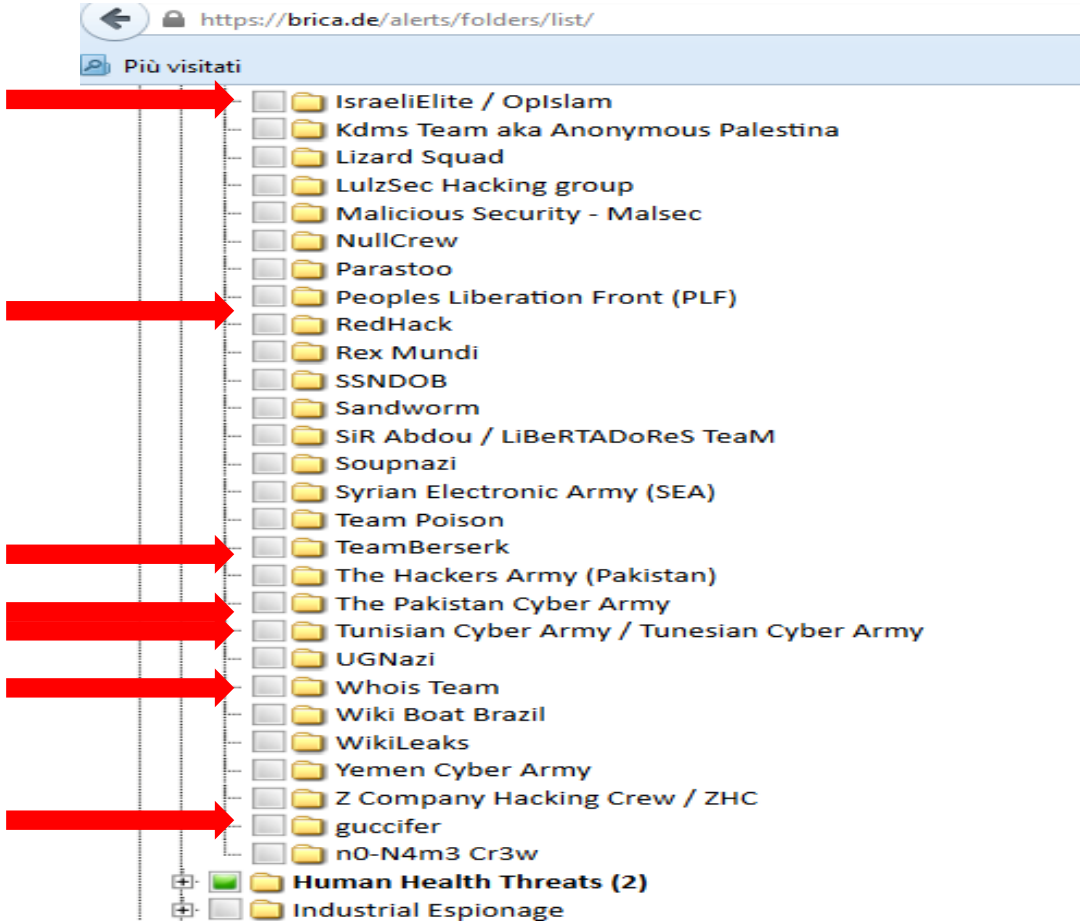
- **Terrorism / Govt Intelligence (8)**
  - **. Specific Terrorist Groups (5)**
    - Abu Sayyaf
    - Ajnad Misr/Soldiers of Egypt
    - Ajnad al-Sham
    - **Al Qaeda/al-Qaida /Al Queda / AQIM/AQAP/AQSL**
    - Al-Murabitoon
    - Al-Qassam / Al-Qassam
    - Al-Shabaab / Al Shabaab / al-Shabab
    - Ansar Bayt al-Maqdis
    - As-Sahab
    - Boko Haram
    - Cyber Caliphate / CyberCaliphate
    - Hezbollah
    - Hizb-ut-Tahrir / HTA (Hizb ut-tahrir America)
    - Houthi militants / Houthi group / Houthi rebel
    - **IS /ISIS/Islamic State/ISIL/Takfiris/AQI/ Daish/ Daesh**
    - Jabhat al-Nusra
    - Jaysh al-Islam
    - Jund al-Khilafa
    - Khorasan
    - Specific Terrorist Groups - Various
    - Tehreek-e-Taliban / Taliban
  - **. Inspire / Azan / Dabiq Terrorist Magazines**
  - **. Terrorist / Govt Intel Alert**
  - .Terrorist / Govt Intel Background reports and Info
  - .Terrorist / Govt Intel News
  - Green Dam
  - Kylin

Remaining subjects for your subscription	99
Global	**100**
Activated subjects	19
Remaining subjects for your subscription	81
Organization	**10**
Activated Search terms	0
Remaining search terms for your subscription	10

Gruppi noti di “Cyber-Terrorism” (estratto)



Gruppi noti di “Cyber-Terrorism” (estratto)

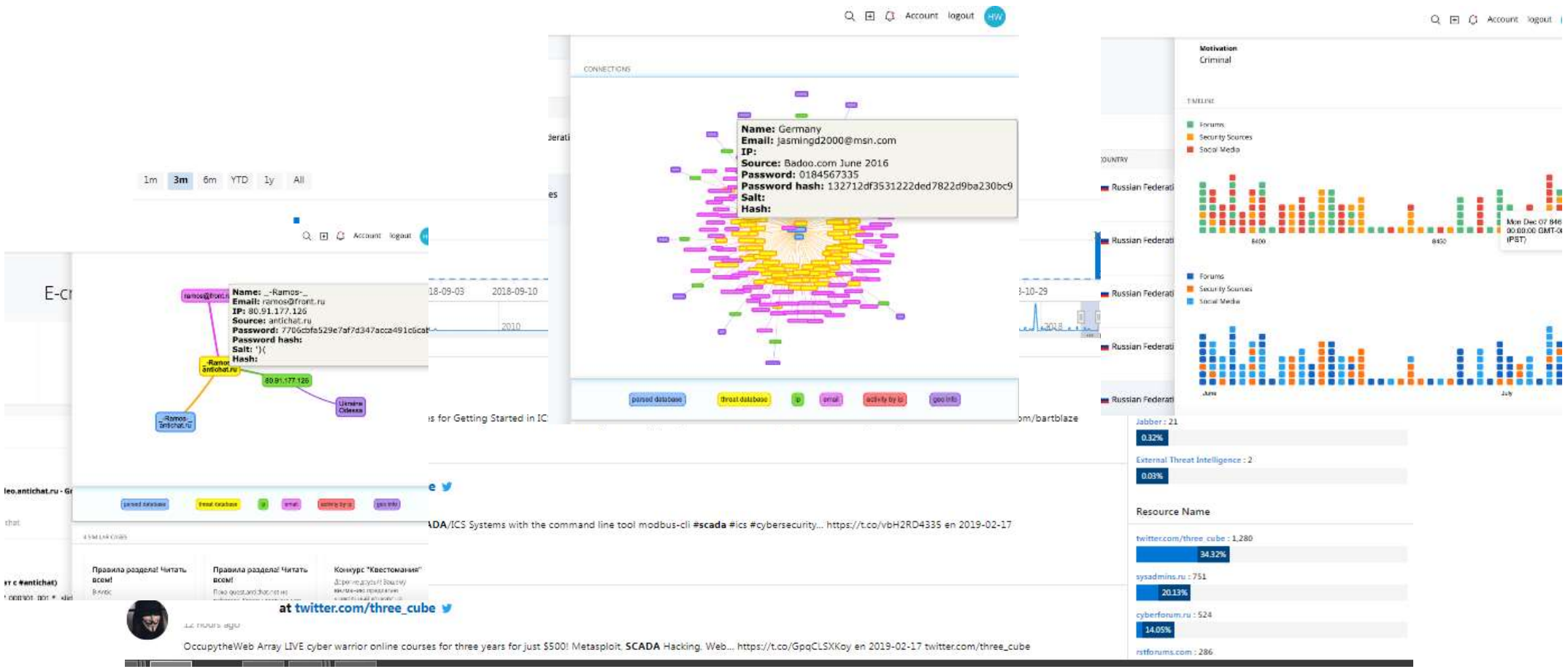


… E CONTESTUALIZZARE”.

UNIVERSITÀ
DI PARMA

APPLIED CYBER INTELLIGENCE (Actors & Correlations)

UNIVERSITÀ DI PARMA



Case Studies [RAT e rischi tecnologici del WEF]

UNIVERSITÀ DI PARMA

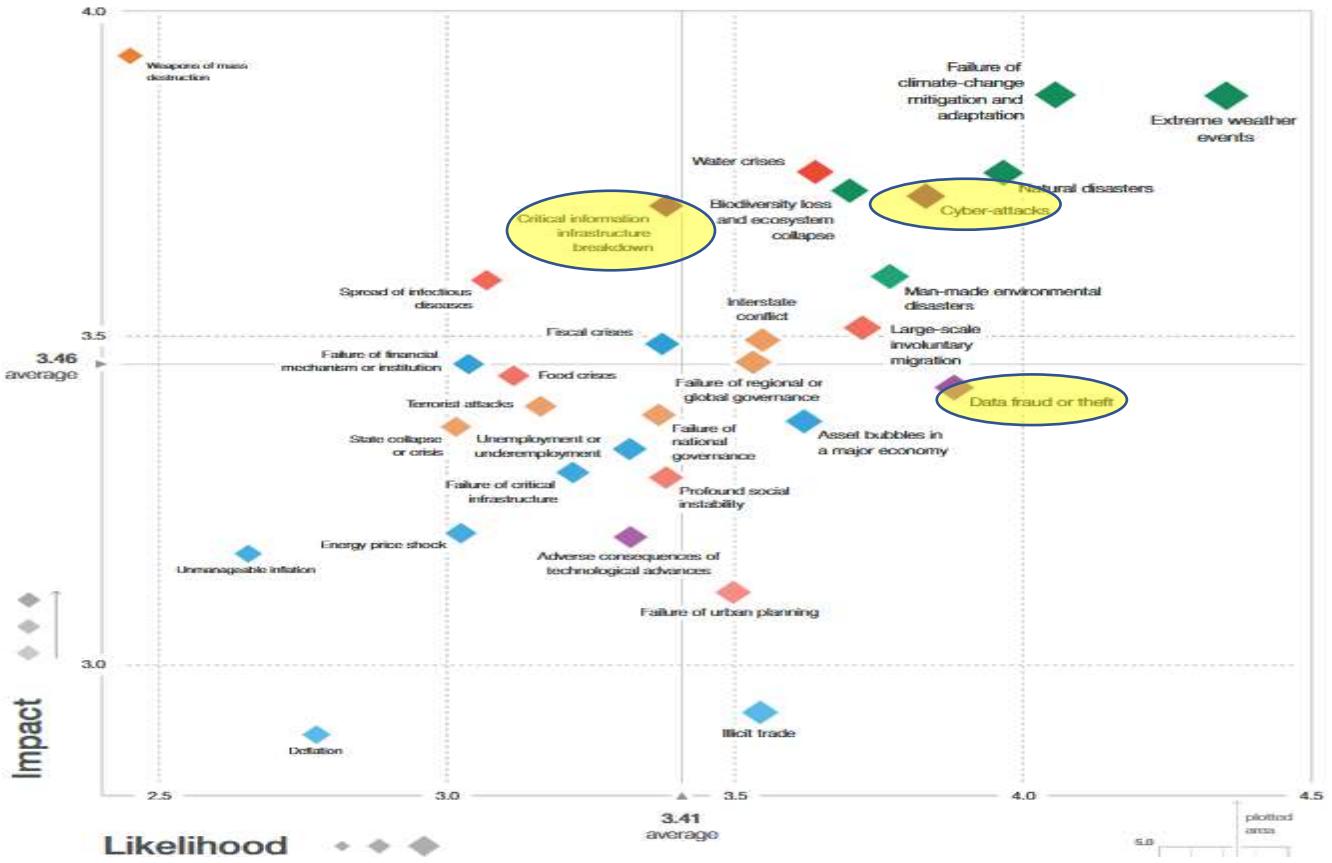
Vittima	Attaccante	Tecniche usate
Multinazionali del settore Chimico ed Oil & Gas	Ignoto (Chinese espionage?)	Spear Phishing, Social Engineering, exploit varie vulnerabilità, Malware (RAT)

- Per primo il World Economic Forum, nei suoi Global Risks Report del **2012 e del 2013**, analizzando le **50 principali minacce globali** e classificandole per **impatto** e **probabilità**, nella sezione "**Rischi tecnologici**" pose al secondo posto, dopo il **cybercrime**, la possibilità di ***critical system failure***, ovvero di **incidenti ad infrastrutture critiche** in grado di scatenare, per **effetto domino**, **impatti negativi a cascata su tutto il sistema socio-economico**.

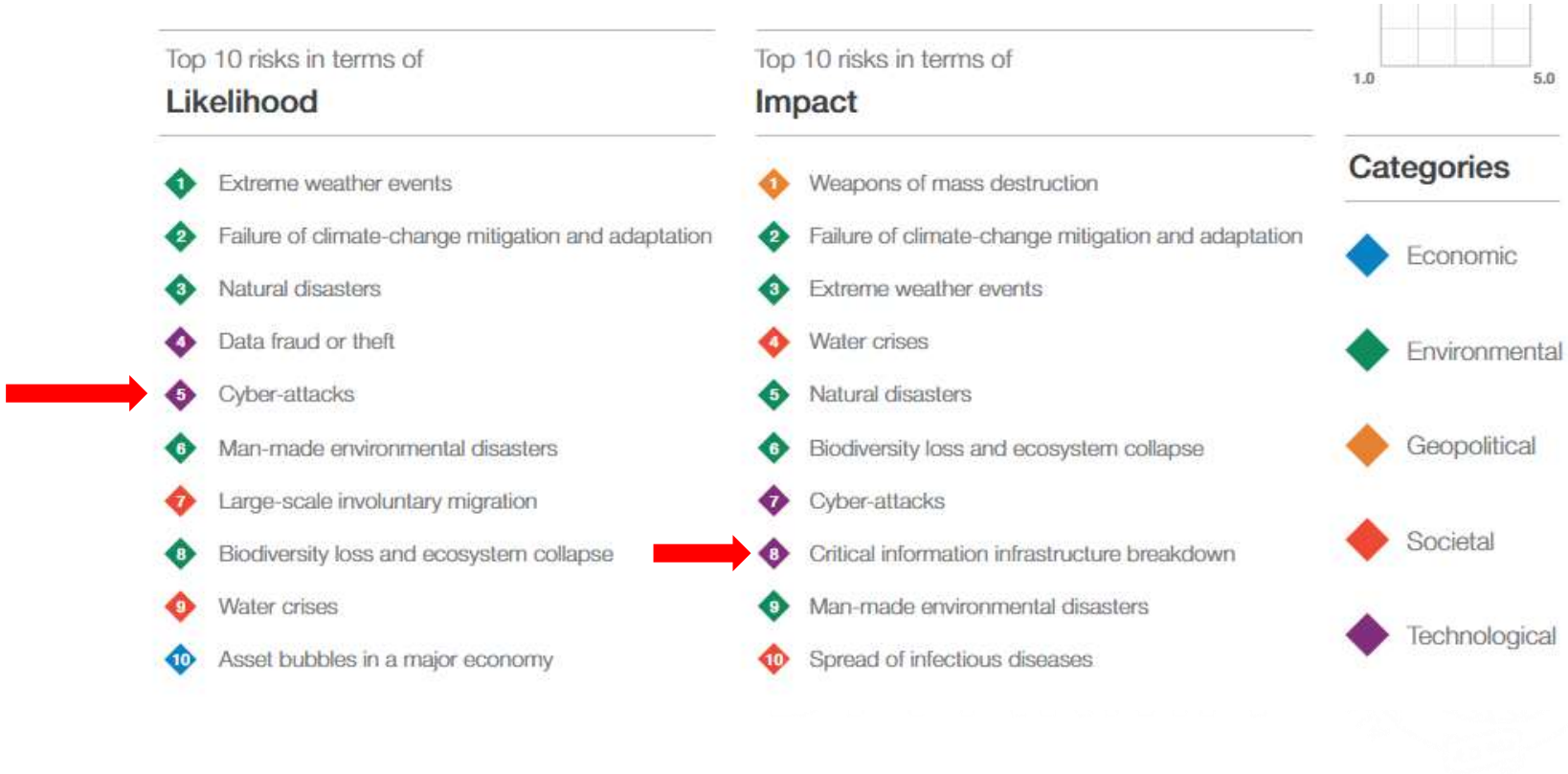
- I **sistemi informatici deputati al controllo dell'automazione in ambito industriale** sono una delle principali fonti di rischio in un'ottica di *critical system failure*: pur essendo pensati per **offrire le massime garanzie** in termini di continuità e di sicurezza operativa, **storicamente non sono stati progettati tenendo in considerazione la possibilità di attacchi informatici**.

https://www.weforum.org/reports/the-global-risks-report-2020

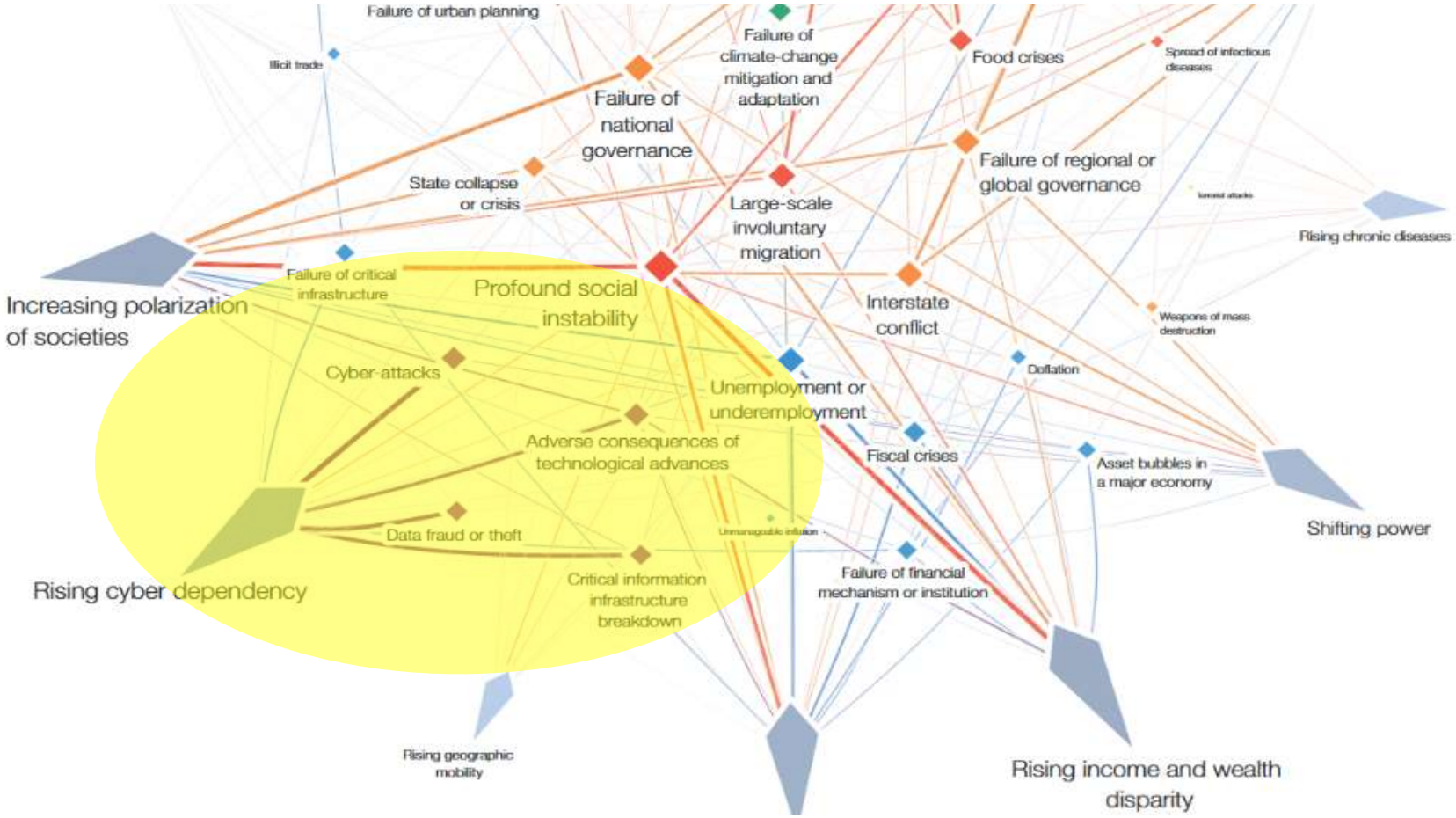
Case Studies [WEF Report 2019]



Case Studies [WEF Report 2019]



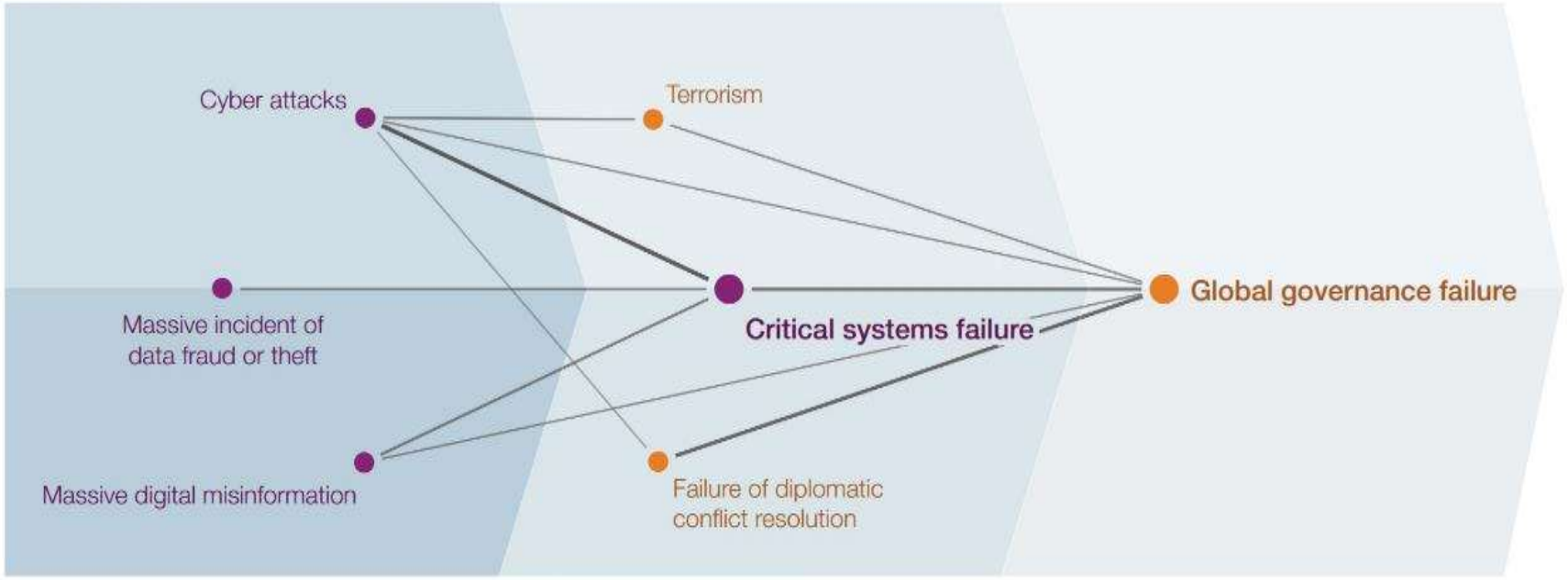
Case Studies [WEF Report 2019]



Case Studies [WEF Report 2019]

UNIVERSITÀ DI PARMA

Figure 17: The Dark Side of Connectivity Constellation



Origin Risk
Increasing capabilities for cyber crime and attacks.

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

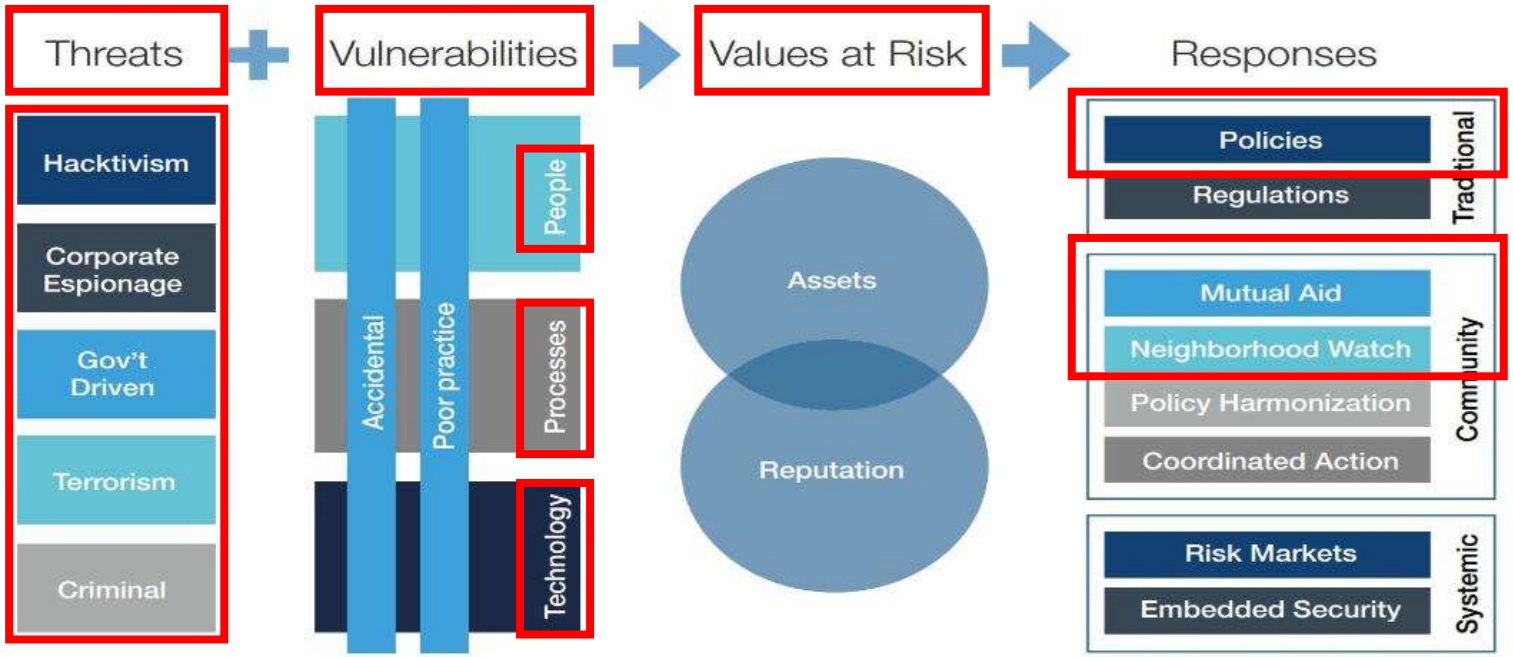
Manifestation
The traditional system of global governance is undermined.

Source: World Economic Forum

Case Studies [WEF Report 2019]

UNIVERSITÀ DI PARMA

Figure 41: Framework for Cyber Threats and Responses



Source: World Economic Forum

Indice – Seconda Parte

UNIVERSITÀ DI PARMA

“AUTODIFESA DIGITALE, BUONE REGOLE E CONSIGLI”

- Security Awareness
- Statistiche
- Esercitiamoci insieme
- Security policies e cyber security awareness
- COVID-19 e Smart Work
- Reading Rooms
- Q&As

CYBER SECURITY AWARENESS

UNIVERSITÀ
DI PARMA

Videoclip time!

UNIVERSITÀ DI PARMA

Perché la Security Awareness è importante

- Perché troppo spesso **gli utenti sottovalutano l'importanza delle informazioni presenti on-line.**
- Anche a **livello personale** e **fuori dal contesto lavorativo**)
    - Videoclip: il «Mago» belga

Il veicolo di contagio più frequente...

UNIVERSITÀ DI PARMA

Il veicolo di contagio più frequente...

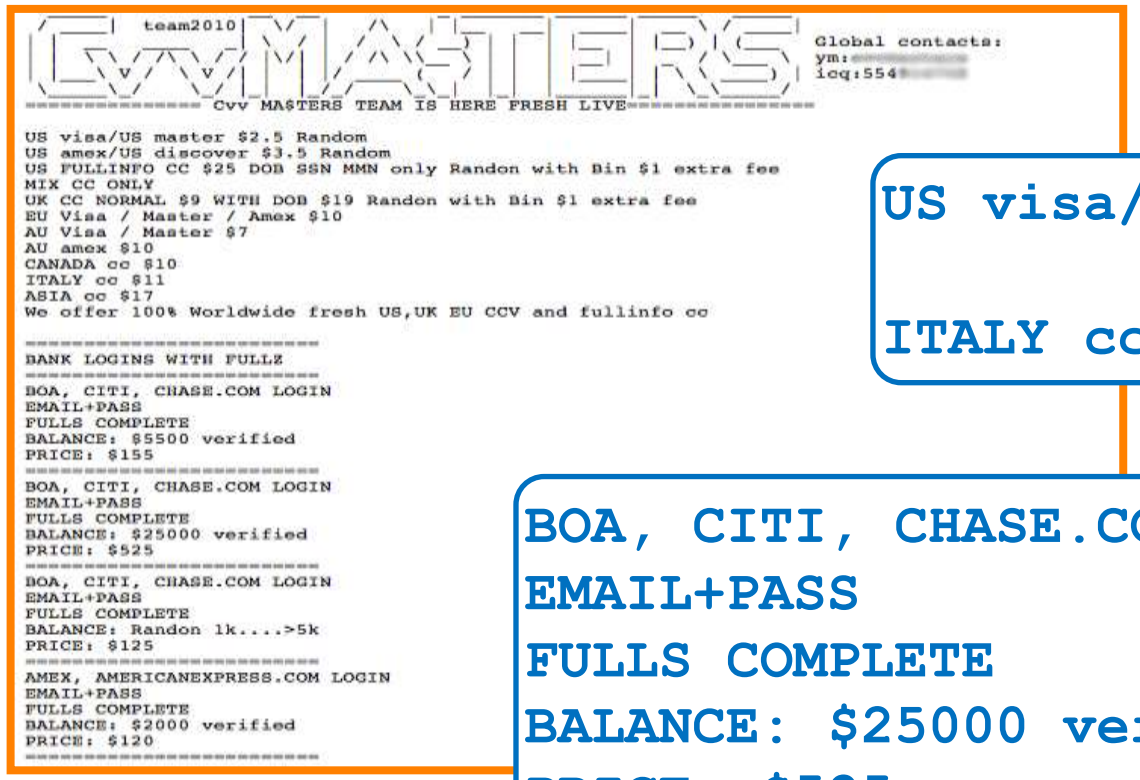
Il veicolo di contagio più frequente...

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

$146.000
USD/settimana

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

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

=========================================
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: [redacted]
or [redacted]

ICQ: [redacted]

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”).

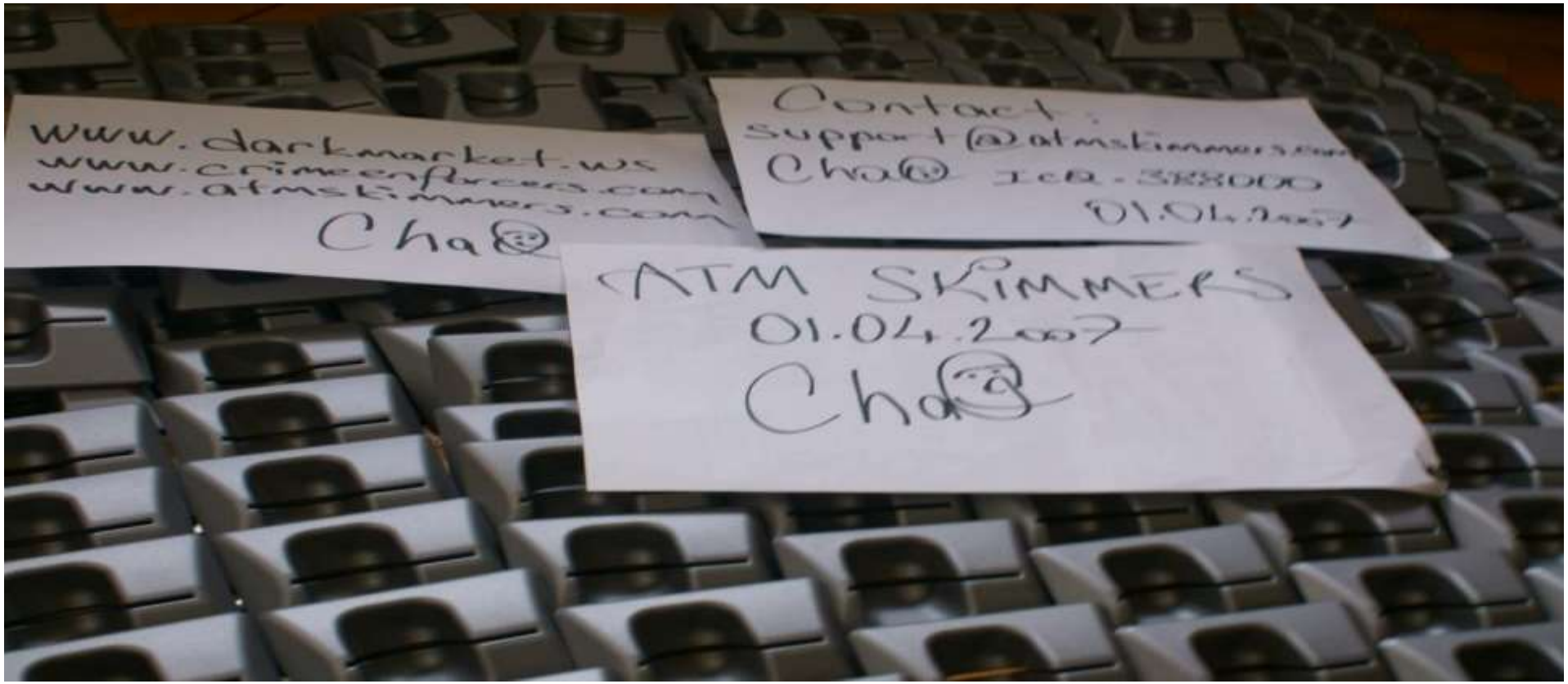


```
 team2010
 MASTERS
Global contacts:
ym:
icq:554
========== Cvv MA$TERS TEAM IS HERE FRESH LIVE==========

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

==========
BANK LOGINS WITH FULLZ
==========
BOA, CITI, CHASE.COM LOGIN
EMAIL+PASS
FULLS COMPLETE
BALANCE: $5500 verified
PRICE: $155
==========
BOA, CITI, CHASE.COM LOGIN
EMAIL+PASS
FULLS COMPLETE
BALANCE: $25000 verified
PRICE: $525
==========
BOA, CITI, CHASE.COM LOGIN
EMAIL+PASS
FULLS COMPLETE
BALANCE: Randon 1k....>5k
PRICE: $125
==========
AMEX, AMERICANEXPRESS.COM LOGIN
EMAIL+PASS
FULLS COMPLETE
BALANCE: $2000 verified
PRICE: $120
==========
```

US visa/US master $2.5 Random

ITALY cc $17

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


www.darkmarket.ws
Ciao
Contact:
ATM SKIMMERS
01.04.2007
Ciao

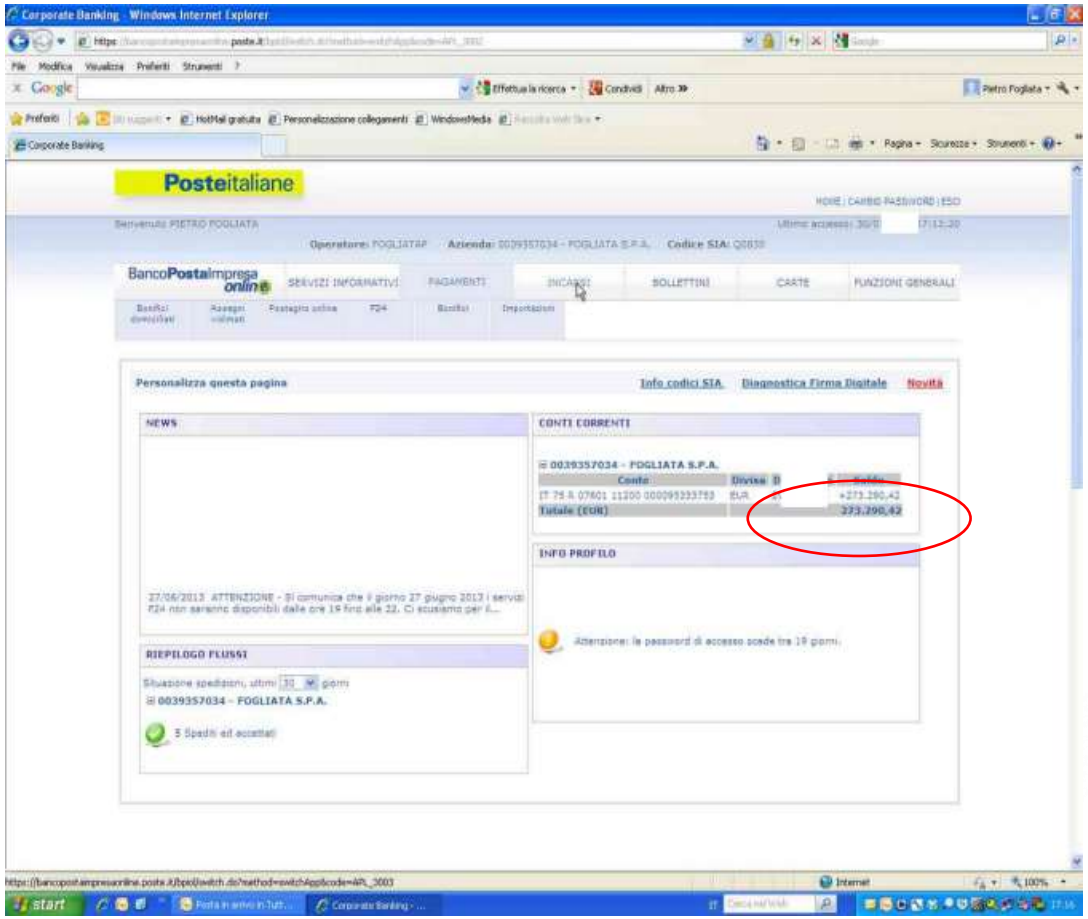
#	Card number	Expire	Country	Site	Card	Type	Status	Bank	IP	Date
☐	487038000	11/16	US	Amazon	VISA	DEBIT	CLASSIC	FIRSTBANK PUERTO RICO	72.50.84.69	02.04.2014 17:18:03
☐	411111111	06/17	OT	Facebook	VISA	none	none	JPMORGAN CHASE BANK, N.A.	117.208.175.43	02.04.2014 18:32:37
☐	521324376	11/15	OT	Paypal	MASTERCARD	DEBIT	PLATINUM	TINKOFF CREDIT SYSTEMS	46.42.18.71	02.04.2014 18:56:56
☐	558828001	08/15	US	Paypal	MASTERCARD	none	STANDARD	CITIBANK SOUTH DAKOTA, N.A.	24.39.157.218	02.04.2014 19:07:52
☐	522078041	01/17	OT	Facebook	MASTERCARD	none	none	none	92.108.76.166	02.04.2014 20:12:20
☐	401288888	12/14	GB	Ebay	VISA	none	none	none	81.109.88.31	02.04.2014 21:54:12
☐	513648200	05/15	FR	Ebay	MASTERCARD	CREDIT	STANDARD	MASTERCARD FRANCE S.A.S.	89.90.10.156	02.04.2014 22:16:42
☐	411770403	06/16	US	Amazon	VISA	DEBIT	PLATINUM	BANK OF AMERICA, N.A.	216.15.123.114	02.04.2014 22:17:07
☐	406001201	01/15	OT	Paypal	VISA	DEBIT	CLASSIC	ALPHA BANK	79.167.211.68	03.04.2014 00:13:38
☐	525678114	11/17	ES	Facebook	MASTERCARD	DEBIT	STANDARD	BANCO NACIONAL DE MEXICO, S.A.	201.141.176.172	03.04.2014 00:45:23
☐	411773394	12/16	US	Amazon	VISA	DEBIT	PLATINUM	BANK OF AMERICA, N.A.	64.206.92.97	03.04.2014 00:59:09
☐	404936000	03/17	OT	Paypal	VISA	none	none	none	80.244.19.22	03.04.2014 01:16:02
☐	434256206	02/17	US	Ebay	VISA	DEBIT	none	WELLS FARGO BANK, N.A.	201.170.244.126	03.04.2014 01:45:08
☐	406774000	01/15	OT	Ebay	VISA	CREDIT	PLATINUM	BANCO INTERAMERICANO DE FINANZAS, S.A.E.M.A.	200.62.153.210	03.04.2014 01:49:31
☐	434256206	02/17	US	Ebay	VISA	DEBIT	none	WELLS FARGO BANK, N.A.	201.170.244.126	03.04.2014 01:56:36
☐	487038000	11/16	US	Amazon	VISA	DEBIT	CLASSIC	FIRSTBANK PUERTO RICO	72.50.87.5	03.04.2014 02:02:29
☐	455255023	10/13	OT	Facebook	VISA	CREDIT	GOLD PREMIUM	TARJETAS BANAMEX S.A. DE C.V. SOFOM ENTIDAD REGULADA	187.244.40.195	03.04.2014 02:03:47
☐	518954072	06/15	OT	Facebook	MASTERCARD	none	STANDARD	BANK LEUMI LE-ISRAEL BM	93.173.160.236	03.04.2014 02:13:35
☐	453744500	09/16	CA	Amazon	VISA	none	none	THE BANK OF NOVA SCOTIA	69.71.69.28	03.04.2014 04:33:31
☐	601100099	12/19	OT	Facebook	DISCOVERY	CREDIT	PLATINUM	none	186.45.182.9	03.04.2014 05:01:08
☐	455632113	10/14	OT	Paypal	VISA	CREDIT	CLASSIC	BANK CENTRAL ASIA	125.166.228.196	03.04.2014 05:11:29
☐	409851300	02/19	OT	Paypal	VISA	DEBIT	ELECTRON	BBVA BANCOMER S.A.	187.205.244.159	03.04.2014 05:25:08
☐	374970256	06/17	FR	Amazon	AMEX	CHARGE CARD	GOLD	BNP PARIBAS - AIR FRANCE	80.14.51.204	03.04.2014 05:36:44
☐	422109200	07/20	OT	Paypal	VISA	DEBIT	CLASSIC	ASIA COMMERCIAL BANK	123.18.115.188	03.04.2014 06:27:38
☐	487038000	11/16	US	Amazon	VISA	DEBIT	CLASSIC	FIRSTBANK PUERTO RICO	72.50.85.69	03.04.2014 07:27:44
☐	558158802	05/14	US	Paypal	MASTERCARD	none	BUSINESS	JPMORGAN CHASE BANK, N.A.	99.114.149.202	03.04.2014 08:07:51
☐	468817040	09/21	OT	Paypal	VISA	DEBIT	ELECTRON	ANDHRA BANK	117.207.251.7	03.04.2014 08:32:03
☐	421627629	10/17	OT	Paypal	VISA	DEBIT	CLASSIC	ICICI BANK LTD	182.64.134.172	03.04.2014 09:27:22
☐	438628001	08/15	OT	Facebook	VISA	CREDIT	PLATINUM	CITIBANK, N.A.	115.118.167.111	03.04.2014 10:15:05
☐	540058077	03/18	IT	Facebook	MASTERCARD	none	none	none	151.49.158.230	03.04.2014 14:13:31
☐	540205204	02/18	ES	Ebay	MASTERCARD	none	STANDARD	BANCO SABADELL S.A.	80.31.18.111	03.04.2014 14:31:52
☐	461726700	12/17	OT	Facebook	VISA	CREDIT	PLATINUM	CITIBANK (HONG KONG) LIMITED	119.237.130.150	03.04.2014 16:44:04


ESTONIA
LATVIA
BELARUS
UKRAINE
UNITED STATES
Miami
Sold stolen identity data to conspirators in Eastern Europe.
Sold materials to make fake cards.
CHINA


citi
Bank of America
AIG
DBS
HSBC
citibank
BANK OF CHINA
VISA
OMC CARD
BANKTONE
Standard Chartered
PLATINUM
GOLD
usbank
HANG SENG BANK
CHASE


krab


СВИДЕТЕЛЬСТВО О РОЖДЕНИИ
РОДИТЕЛИ:
РСФСР


Corporate Banking - Windows Internet Explorer
Posteitaliane
BancoPostaimpresa online
SERVIZI INFORMATIVI
PAGAMENTI
INCASSI
BOLLETTINI
CARTE
FUNZIONI GENERALI
Personalizza questa pagina
Info codici SIA
Diagnostica Firma Digitale
Novità
NEWS
CONTI CORRENTI
0039357034 - FOGLIATA S.P.A.
INFO PROFILO
RIEPILOGO FLUSSI
0039357034 - FOGLIATA S.P.A.
start


Internet Banking - Windows Internet Explorer
https://corporate.bpergroup.net/eb/bcam-corporate/index
Preferiti
Internet Banking
Pagina
Sicurezza
Strumenti
Venerdì
Banca della Campania
Informazioni
Disposizioni
Servizi
Rubriche
Gestione
Preferiti
ESCI
CONTI PORTAFOGLIO
Conti Anticipi
Dossier Titoli
Lavori con: 51185399/ Amm./ Tutti i Codici SIA
Voglio lavorare con:
Tutti i Codici SIA
EUR 3.911.771,90
HELP CENTER
TUTORIAL
FAQ
Causale
Causale CBI
Divisa
Dare
Avere
7168878256 POSTE ITALIANE SPA NEG.
13 MOTIVO DIFETTO DI PROVVISTA-ART.2.
00066 SPESE
EUR
18,90
UCE S.R.L. ABI/CAB 01030-33911-FAVORE
T S.P.A.-CRO 20711134903-NC N.. 1975-
.. 1975-2313
00048 BONIFICO
EUR
1.797,98
INO MARIA CIRA ABI/CAB 02008-03449-
EGAWATT S.P.A.-CRO 47204641509-BEN
210 ORD SNNMCR64M68F839H LAVORI
ZONE STRAORDINARIA APP.TO C.SO
EMENUELE N. 715 NAPOLI-ACCONTO ORDINE
.2 013
00370 BONIFICOPER RISTRUTTURAZIONE
EUR
200,00
00367 RIT.
Fine
Siti attendibili
100%
start
Sessione A - DS...
Il Mattino - Hom...
Internet Bankin...
17.33

Viceoclip time!

UNIVERSITÀ DI PARMA

Guardate questo video e cercate di "capire" **quali tecniche utilizza** il cybercriminale e **quali errori fanno** le sue varie vittime.

ESERCITIAMOCI TUTTI INSIEME

UNIVERSITÀ
DI PARMA

Covid-19 & Smart Work

UNIVERSITÀ
DI PARMA

Tutte le relazioni di business si spostano nelle più diverse modalità remote

UNIVERSITÀ DI PARMA

Sì, io ti sento...
Parla, parla, parla!

Mi senti?
Riesci a sentirmi?

Mi vedi?

Ma che c...!
Io sento benissimo!!

Mi senti?

Attiva il microfono
che io non ti sento

Prima di iniziare: il «caso Zoom»...

SECURITY

Internal Senate memo warns Zoom poses 'high risk' to privacy, security

Two federal overseers have also advised agencies not to use Zoom's free or commercial service.

Brennan/AP Photo

la Repubblica

Attacco porno a scuola, Singapore vieta Zoom

divieto dopo un'incursione con contenuti pornografici. L'app di videoconferenze ancora alle prese con bombing e altri guai legati alla sicurezza

Gli "Zoombombing" stanno diventando un problema

Sono le azioni di disturbo organizzate introducendosi nelle ormai quotidiane videochiamate e riunioni a distanza, che spesso diventano vere aggressioni verbali

torino

HOME | CRONACA | SPORT | FOTO | RISTORANTI | ANNUNCI LOCALI | CAMBIA EDIZIONE | VIDEO | METEO

Videolezioni su Zoom, l'ombra degli hacker sui licei torinesi: "Rubate le nostre password"

…e l'underground digitale

UNIVERSITÀ DI PARMA

Caso Teams

UNIVERSITÀ DI PARMA

www.cyberark.com › threat-research-blog › be... ▾ Traduci questa pagina

Beware of the GIF: Account Takeover Vulnerability in Microsoft ...

3 giorni fa - This **vulnerability** would have affected every user who uses the **Teams** desktop or web browser version. CyberArk worked with **Microsoft** Security ...

www.welivesecurity.com › 2020/04/27 › micros... ▾ Traduci questa pagina

Microsoft Teams flaw could let attackers hijack accounts ...

3 giorni fa - CyberArk has now described a possible attack scenario: "We found that by leveraging a sub-domain takeover **vulnerability** in **Microsoft Teams**, ...

www.scmagazine.com › ... › Vulnerabilities ▾ Traduci questa pagina

Microsoft Teams vulnerability patched, could lead to account ...

2 giorni fa - **Microsoft's Teams** collaboration platform contains a **vulnerability** that can be exploited with a malicious GIF enabling an attacker to take over a ...

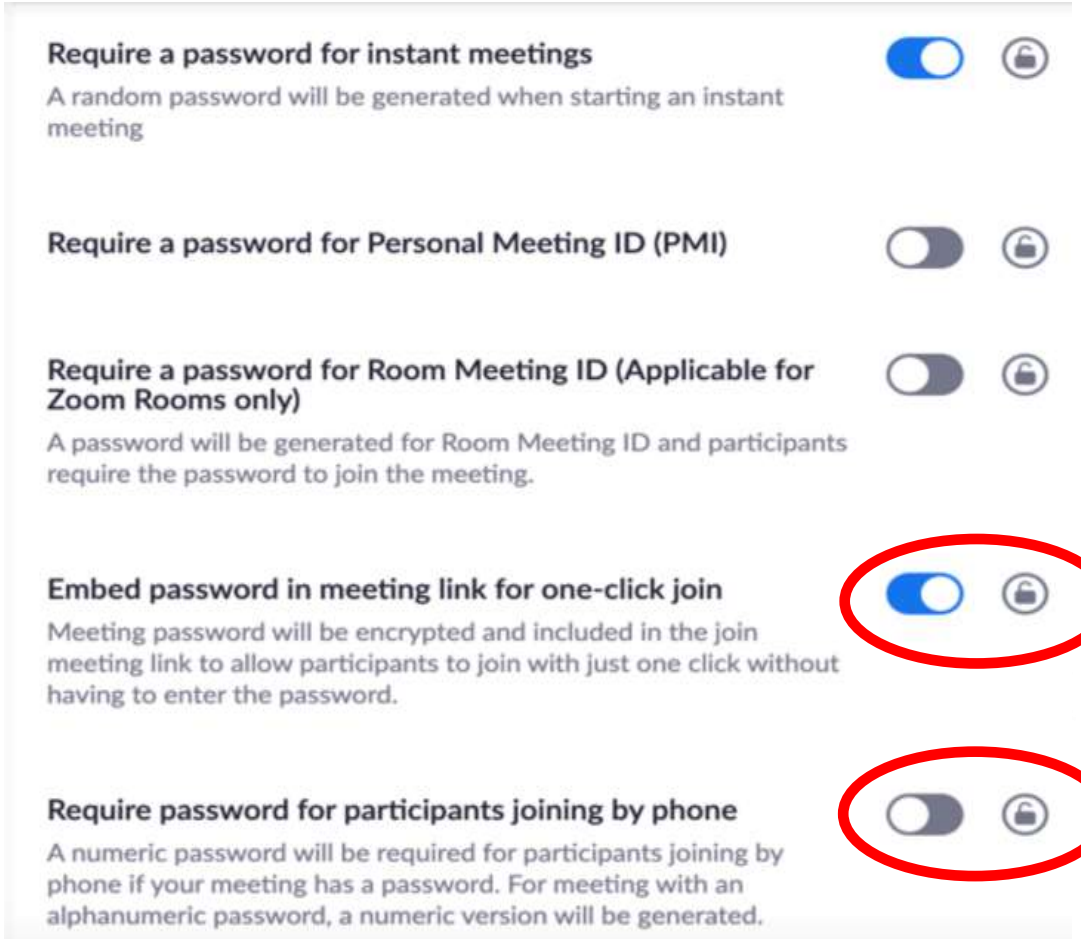
www.cbronline.com › news › teams-vulnerabilit... ▾ Traduci questa pagina

Microsoft Teams Vulnerability Let Hackers "Take Over Entire ...

3 giorni fa - **Microsoft's** collaboration platform **Teams** contained a **vulnerability** that allowed hackers to send out a GIF that only had to been seen, in order ...

Perché siamo qui?

UNIVERSITÀ DI PARMA



Un cambio di mindset

UNIVERSITÀ DI PARMA

- La slide precedente è un esempio emblematico di ciò che vogliamo insegnarvi.

- Le opzioni di sicurezza **ci sono ma non sono impostate di default**: dobbiamo abilitarle noi ☺

Remote Work VS Smart Work

UNIVERSITÀ DI PARMA

Differenze dal punto di vista tecnico

- **Remote work**: lavoro che si svolge a distanza rispetto alla sede centrale, da casa o da un luogo decentrato specifico

- **Smart work**: non è obbligatorio legarsi a un luogo fisico fisso in cui lavorare (casa, sede distaccata, ma anche un ristorante, un pub o un parco se presente una connessione Wi-Fi).
  - **BYOD**

Remote Work VS Smart Work

UNIVERSITÀ DI PARMA

Altre differenze

- **Remote work:** Contratto di telelavoro, accesso al luogo di svolgimento per ragioni di sicurezza sul lavoro, richiesta di impianti a norma, comunicazioni all'INAIL con indicazione dell'indirizzo, parità di trattamento retributivo, diritto alla disconnessione
- **Smart work:** Accordo fra le parti (sospeso in questo momento d'emergenza), parità di trattamento retributivo, diritto alla disconnessione, sicurezza del lavoratore, comunicazioni obbligatorie semplificate

Scenario e Problematiche

UNIVERSITÀ DI PARMA

Utilizzo dei PC “di casa” e non di quelli aziendali

↓

Assenza o drastica diminuzione degli strumenti di difesa in essere

↓

Aumento del rischio di contagi informatici e dell’esposizione degli utenti e degli asset digitali utilizzati

↓

Innalzamento dell’interesse del cybercrime….
…. e **lancio massivo di campagne di phishing** e **schemi di frode coordinati**

«Cyber Hygiene» & Common Sense

UNIVERSITÀ DI PARMA

- Backup
- OS Patching
- AV
- Phishing
- Buon senso e consigli

Backup

UNIVERSITÀ
DI PARMA

Avere un backup aggiornato è la condizione ideale per mitigare possibili danni conseguenti a:

- Rottura dell'hardware
- Sovrascritture incidentali di files
- Contagio da ransomware e malware

Backup – Domande

UNIVERSITÀ DI PARMA

- Da quanto tempo non avete fatto un backup?
- Backup disponibile solo sui server aziendali?
- Concetto di backup incrementale
- Organizzazione dei propri dati (di lavoro) sui PC di casa
- Strumenti HW e SW per backup
- Cloud e backup: cifratura dei dati

OS Patching

UNIVERSITÀ DI PARMA

Aggiornare sempre il proprio OS (Sistema Operativo) ed il software / le applicazioni installate.

NOTA: Questo vale **anche ed in particolar modo** per i vostri smartphone e tablet, e per i **dispositivi personali**.

Phishing & Ingegneria Sociale

UNIVERSITÀ DI PARMA

Com'era prevedibile, stiamo assistendo ad un aumento esponenziale degli attacchi di phishing (email "esca") e di molteplici malware (software malevoli).

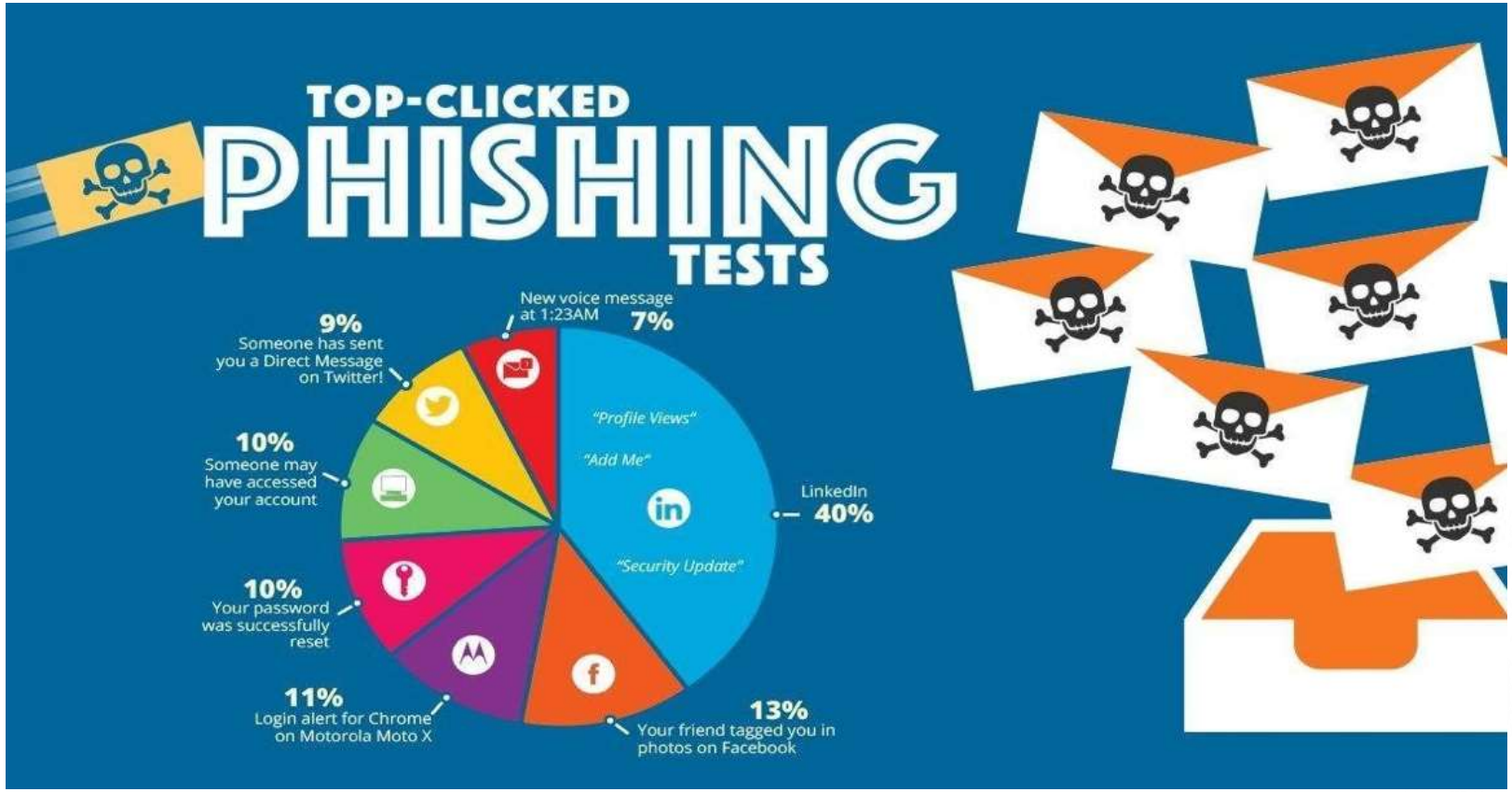
Queste truffe usano la scusa del COVID-19, e di varie parole chiave ad esso correlate, per invogliare l'utente ad aprire allegati infetti, o a cliccare su URL che a loro volta portano a siti fake, o violati e contagiati.

Phishing & Ingegneria Sociale

UNIVERSITÀ DI PARMA

- **Phishing di account personali VS sicurezza aziendale**
  - Spesso stessa password, o variante della stessa
  - Facilitano attacchi phishing mirati ed usano “leva psicologica”
- **Credenziali compromesse di terze parti**
  - Ad esempio della nostra utenza PEC, il vostro account Netflix, etc…
- **Credenziali aziendali compromesse presenti su Dark Web**
  - Poche aziende hanno ad oggi gli strumenti per informarsi in tempo reale
  - Impatti lato GDPR e sanzioni economiche

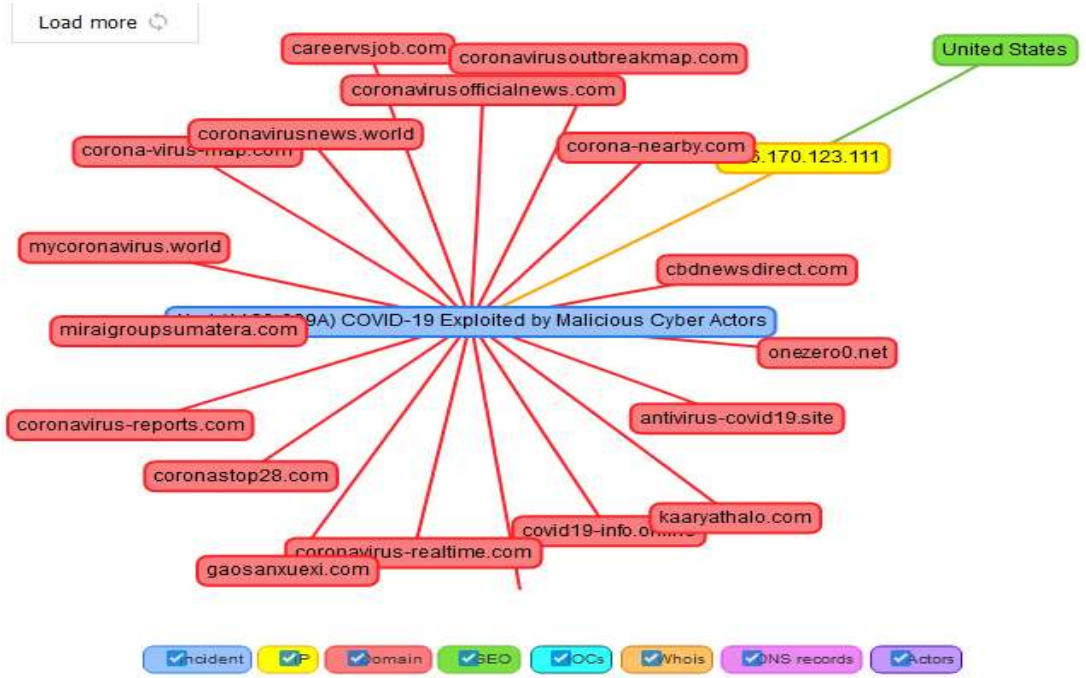
Phishing & Ingegneria Sociale



Phishing & Ingegneria Sociale

UNIVERSITÀ DI PARMA

Esempio: propagazione del malware del WHO



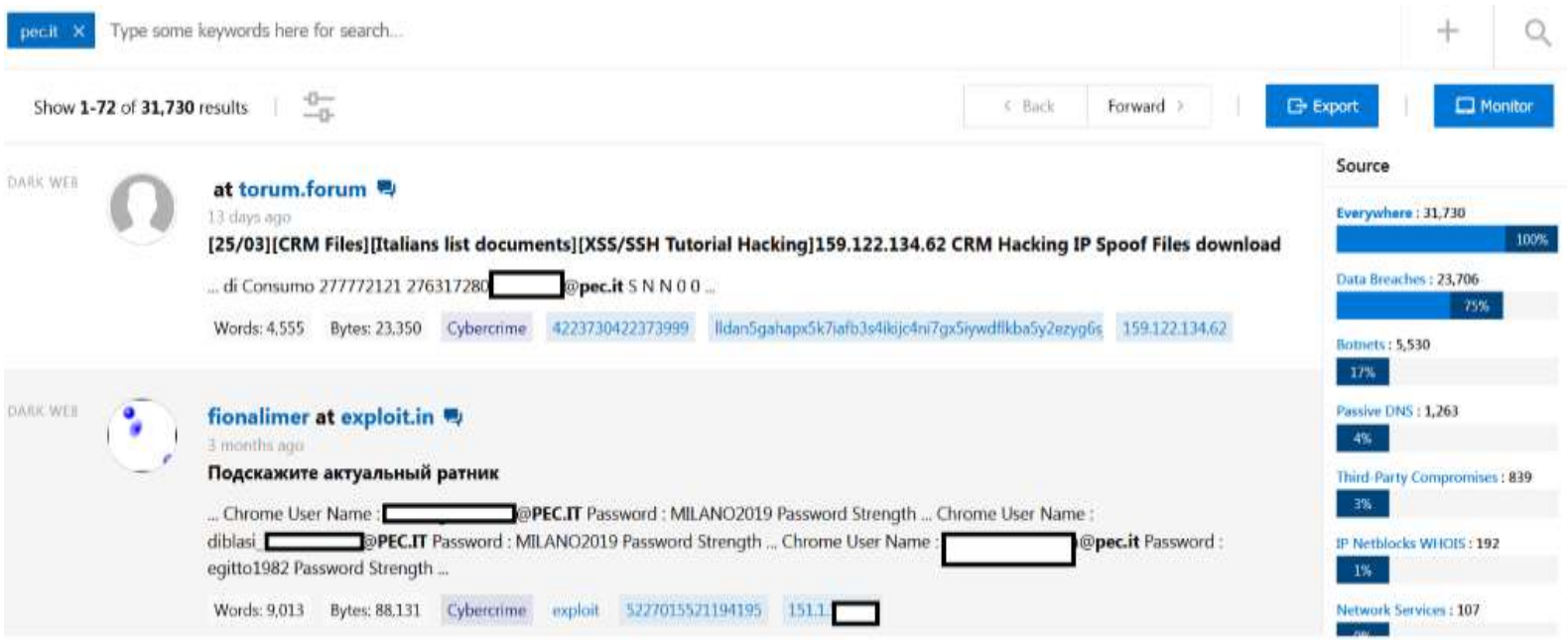
NOTA: non andate sui siti riportati in questo screenshot!

Phishing & Ingegneria Sociale

UNIVERSITÀ DI PARMA

Phishing & Ingegneria Sociale

UNIVERSITÀ DI PARMA



AV (Anti-Virus)

UNIVERSITÀ DI PARMA

Oggigiorno gli AV “standard”, purtroppo, non sono più uno strumento efficace al 100% contro le infezioni.

Ad esempio bloccano solo i malware già noti e conosciuti (dei quali esiste un “signature”), ma nulla possono contro vulnerabilità “zero-day’ e, soprattutto, contro quei malware non ancora identificati dal produttore o i file-less attack – ne parleremo tra poco.

AV (Anti-Virus)

UNIVERSITÀ DI PARMA

Ciò nonostante, avere un antivirus “a bordo” è misura quanto meno obbligatoria (chiamiamola best practice o “buon senso del padre di famiglia”).

- Aggiornare sempre l’antivirus: “signatures” ed “engine”
- Provare ad utilizzare una VM (Virtual Machine) con Windows

Live examples: IOC e AV detection rate

UNIVERSITÀ DI PARMA

Type some keywords here for search...

Trojan.Downloader.LnK.Gen Additional_CSD_Rebate.pdf.lnk	**Analysis date:** 8 Apr, 2020 **File type:** Windows shortcut **Detection ratio:** 21 / 60 **MD5:** 120e3733e167fcabdfd8194b3c49560b **SHA256:** f8b053e32eed9a5e814c89eec50e743a906f1aadc7a6f58e25f0410863c5ec4a
HEUR:Exploit.MSOffice.Generic	**Analysis date:** 8 Apr, 2020 **File type:** Rich Text Format **Detection ratio:** 35 / 60 **MD5:** fef12d62a3b2fbf1d3be1f0c71ae393e **SHA256:** 0dd9d9638a59b6fbab792b7781962571b653c44ebae3d9b8351937ec71f0af8b
Trojan-Downloader.BAT.wGet.ah 58954102	**Analysis date:** 8 Apr, 2020 **File type:** Text **Detection ratio:** 17 / 60 **MD5:** adebf3b5cb93645489b332033bc764ad **SHA256:** 19270639537a2241861eae2bbf4b4095fc6e1915e4dee476d2e4f277992733fd
ca73cb1feccd34d651eb2ae5094d8311bfb2bdc29455005d450ac9c8ee6bbdef.exe	**Analysis date:** 8 Apr, 2020 **File type:** Win32 EXE **Detection ratio:** 0 / 73 **MD5:** 60b7c0fead45f2066e5b805a91f4f0fc **SHA256:** 80c10ee5f21f92f89cbc293a59d2fd4c01c7958aacad15642558db700943fa22

AV detection rate (esempio: 1/5)

UNIVERSITÀ DI PARMA

ANTIVIRUS	RESULT	UPDATE
ALYac	(not set)	8 Apr, 2020
APEX	(not set)	7 Apr, 2020
AVG	(not set)	7 Apr, 2020
Acronis	(not set)	15 Mar, 2020
Ad-Aware	(not set)	7 Apr, 2020
AegisLab	(not set)	7 Apr, 2020
AhnLab-V3	(not set)	7 Apr, 2020
Alibaba	(not set)	27 May, 2019
Antiy-AVL	(not set)	8 Apr, 2020
Arcabit	(not set)	7 Apr, 2020
Avast	(not set)	7 Apr, 2020
Avast-Mobile	(not set)	7 Apr, 2020
Avira	(not set)	8 Apr, 2020
Baidu	(not set)	18 Mar, 2019

AV detection rate (esempio: 2/5)

UNIVERSITÀ DI PARMA

Baidu	(not set)	18 Mar, 2019
BitDefender	(not set)	8 Apr, 2020
BitDefenderTheta	(not set)	7 Apr, 2020
Bkav	(not set)	7 Apr, 2020
CAT-QuickHeal	(not set)	8 Apr, 2020
CMC	(not set)	21 Mar, 2019
ClamAV	(not set)	7 Apr, 2020
Comodo	(not set)	7 Apr, 2020
CrowdStrike	(not set)	2 Jul, 2019
Cybereason	(not set)	16 Jun, 2019
Cylance	(not set)	8 Apr, 2020
Cyren	(not set)	8 Apr, 2020
DrWeb	(not set)	8 Apr, 2020
ESET-NOD32	(not set)	7 Apr, 2020
Emsisoft	(not set)	8 Apr, 2020

AV detection rate (esempio: 3/5)

UNIVERSITÀ DI PARMA

Endgame	(not set)	26 Feb, 2020
F-Prot	(not set)	7 Apr, 2020
F-Secure	(not set)	7 Apr, 2020
FireEye	(not set)	16 Mar, 2020
Fortinet	(not set)	7 Apr, 2020
GData	(not set)	7 Apr, 2020
Ikarus	(not set)	7 Apr, 2020
Invincea	(not set)	7 Apr, 2020
Jiangmin	(not set)	8 Apr, 2020
K7AntiVirus	(not set)	7 Apr, 2020
K7GW	(not set)	7 Apr, 2020
Kaspersky	(not set)	7 Apr, 2020
Kingsoft	(not set)	8 Apr, 2020
MAX	(not set)	8 Apr, 2020
Malwarebytes	(not set)	7 Apr, 2020

AV detection rate (esempio: 4/5)

UNIVERSITÀ DI PARMA

ANTIVIRUS	RESULT	UPDATE
ALYac	(not set)	8 Apr, 2020
APEX	(not set)	7 Apr, 2020
AVG	(not set)	7 Apr, 2020
Acronis	(not set)	15 Mar, 2020
Ad-Aware	(not set)	7 Apr, 2020
AegisLab	(not set)	7 Apr, 2020
AhnLab-V3	(not set)	7 Apr, 2020
Alibaba	(not set)	27 May, 2019
Antiy-AVL	(not set)	8 Apr, 2020
Arcabit	(not set)	7 Apr, 2020
Avast	(not set)	7 Apr, 2020
Avast-Mobile	(not set)	7 Apr, 2020
Avira	(not set)	8 Apr, 2020
Baidu	(not set)	18 Mar, 2019

AV detection rate (esempio: 5/5)

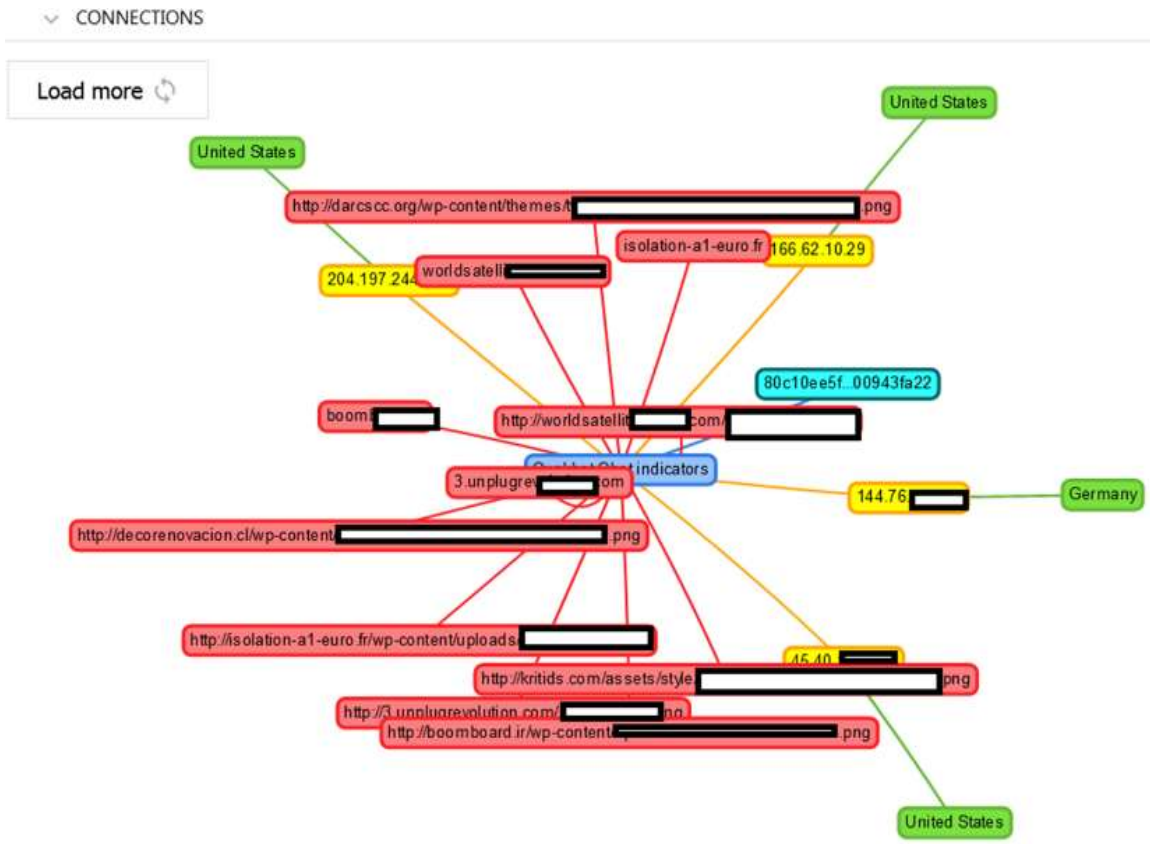
UNIVERSITÀ DI PARMA

SymantecMobileInsight	(not set)	10 Feb, 2020
TACHYON	(not set)	8 Apr, 2020
Tencent	(not set)	8 Apr, 2020
TotalDefense	(not set)	7 Apr, 2020
Trapmine	(not set)	23 Jan, 2020
TrendMicro	(not set)	7 Apr, 2020
TrendMicro-HouseCall	(not set)	8 Apr, 2020
Trustlook	(not set)	8 Apr, 2020
VBA32	(not set)	7 Apr, 2020
VIPRE	(not set)	8 Apr, 2020
ViRobot	(not set)	7 Apr, 2020
Webroot	(not set)	8 Apr, 2020
Yandex	(not set)	7 Apr, 2020
Zillya	(not set)	7 Apr, 2020
ZoneAlarm	(not set)	8 Apr, 2020

Propagazione del malware

UNIVERSITÀ DI PARMA

Siti infettati
per contagiare



I servizi ai quali siamo esposti

UNIVERSITÀ DI PARMA

Privo di adeguati strumenti di difesa ed a causa degli utilizzi ludici mischiati a quelli professionali, il PC si espone principalmente a:

- Contagio attraverso il browser a causa di siti e pagine infette
- Diventare vittime di phishing e campagne mirate
- Furto credenziali e-banking
- Furto login e password intranet e/o accesso VPN aziendale
- Installazione non autorizzata di keylogger
- Botnet con esfiltrazione dei dati
- Botnet per azioni criminose (ad esempio, attacchi DDoS) e conseguenti responsabilità legali

Esempi di utenti già colpiti…/1

UNIVERSITÀ DI PARMA

Date
13 Mar 2020, 17:40pm
IP 151.53.xxx.xx Bot
Country **Italy**
Machine ID 6ade8f7c-f0cf-41c3-ab7e-4aexxxxxxxxx
Hostname **DESKTOP-MNXXYY (aless)**
Botnet **plist_202003_arkei**
Address **Italy,Naples,IT**
Request Type **Browser history**
Software **GoogleChrome**

Telegram/D877F783D5D3EF8C013 Mar 2020, 17:40pm

Files/desctop.zip13
Mar 2020, 17:40pm Telegram/map113 Mar 2020, 17:40pm

Cookies/Google Chrome_Default.txt
13 Mar 2020, 17:40pm

*Files **gia' esfiltrati** dalla botnet*

Esempi di utenti già colpiti…/2

UNIVERSITÀ DI PARMA

History/Google Chrome_Default.txt

- https://**postepay.poste.it/gamma/carte-postepay.html Carte** Postepay
- https://www.skidrowcodex.net/ SKiDROW CODEX GAMES - DOWNLOAD AND PLAY PC GAMES
- https://www.skidrowcodex.net/page/2/ SKiDROW CODEX GAMES - DOWNLOAD AND PLAY PC GAMES
- https://www.skidrowcodex.net/page/3/ SKiDROW CODEX GAMES - DOWNLOAD AND PLAY PC GAMES
- https://www.filecrypt.cc/pax/iox.html Redirect
- https://**it.usenet.nl/registrazione**/?utm_source=AF%5FTA%5F103197&utm_medium=AFNE&utm_campaign=438993&utm_content=0%5F1
- https://sofifa.com/ Giocatori FIFA 20 3 mar 2020 SoFIFA
- https://www.hidemyass.com/it-it/proxy Proxy Web gratuito | Navigazione online anonima | Hide My Ass!
- https://www.hidemyass-freeproxy.com/process/it-it GamesTorrents | Descargar Juegos Torrent Gratis
- https://www.likevisibility.com/ **Comprare Follower Instagram, Fan Facebook LikeVisibility**
- https://postepay.poste.it/ppay/private/pages/index.html Accedi o Registrati
- http://**gmail.com/ Posta in arrivo (4.186)** - xxxxxxxxxxxxxxxxx@gmail.com - Gmail

Esempi di utenti già colpiti.../3

UNIVERSITÀ DI PARMA

Informazioni esfiltrate dalla botnet

Date: Fri Mar 13 17:40:12 2020
MachineID: 6ade8f7c-f0cf-41c3-ab7e-4ae80923ad90
GUID: {705680a4-aa51-11e9-9ffc-806e6f6e6963}
Path: C:\Users\aless\AppData\Local\Temp\xhE6axAk.exe
Work Dir: C:\ProgramData\I7M1LBMXQ1AH5JN18WWL5LPBV
Windows: Windows 10 Home [x64]
Computer Name: DESKTOP-MNXXXXX
User Name: aless
Display Resolution: 1920x1080
Display Language: it-IT
Keyboard Languages: Italiano (**Italia**) / Inglese (Stati Uniti d'America)
Local Time: 13/3/2020 17:40:12
TimeZone: UTC1
[Hardware]
Processor: AMD Ryzen 5 2400G with Radeon Vega Graphics
CPU Count: 8
RAM: 7092 MB
VideoCard: AMD Radeon(TM) RX Vega 11 Graphics
[Network]
IP: 151.53.xxx.xx
Country: Italy (IT)
City: Ercolano (Campania)
ZIP: 80056
Coordinates: 40.8112,14.3528
ISP: INFOSTRADA (WIND Telecomunicazioni S.p.A)

Esempi di utenti già colpiti…/4

UNIVERSITÀ DI PARMA

“Lo studente”

- https://web.**whatsapp.com**/ https://web.whatsapp.com/
- https://www.**subito.it**/ Subito: compra e vendi vicino a te - Annunci gratuiti
- https://www.**zooplus.it/checkout**/overview Alimenti e accessori per cani, gatti e animali domestici | zooplus
- https://www.**iliad.it**/account/ iliad - Benvenuto in iliad
- https://www.samsung.com/it/ Samsung **Italia** | Smartphone | Elettrodomestici | TV
- https://**iostudio.pubblica.istruzione.it/voucher MIUR** - Ministero dell'Istruzione, dell'Università e della Ricerca
- https://iam.pubblica.istruzione.it/iam-ssum/sso/l**ogin?goto=**https%3A%2F%2Fiostudio.pubblica.istruzione.it%3A443%2Fvoucher MIUR –Ministero dell'Istruzione, dell'Università e della Ricerca
- https://www.google.com/search?q=**minecraft**+server&oq=minecraft+server&aqs=chrome..69i57j0l5.22155j0j7&sourceid=chrome&ie=UTF-8 minecraft server - Cerca con Google
- https://www.minecraft.net/it-it/download/server/ Download server for Minecraft | Minecraft

Esempi di utenti già colpiti…/5

UNIVERSITÀ DI PARMA

Browsers/AutoComplete/MozillaFireFox_pip323o3.default-1485616945327-1556918316871.txt

email_address hxxxxxx@googlemail.com
username MxxxxiMxxxx
vb_login_username isac
if false
emailconfirm hxxxxx@googlemail.com
ev Microdata
log x1337
id 673040592830731
LOGIN_USER admin
cd[Schema.org] []
phone 011711212786
ips_username x1234x
email antXXXXX-m-XX@web.de

(funzionalità “autocomplete”)

Date	18 May 2019, 9:54am
IP	91.192.xxx.xx
Bot Country	Switzerland
Machine ID	a21b684-ef82f2e6-65ae38f1
Hostname	M44xx(matzereh)
Botnet	**logs08092019/LogsOtrabotka**
Address	Switzerland,CH
Request Type	**Browser autocomplete**
Software	MozillaFirefox

email Jennifer XXXXXXX
btcinput 0.00271428
email jenniferXXXXXXX
subject password is
btcinput 0.00267608
website @x1337xx
btcinput 0.00338736

Finta Email da Apple

UNIVERSITÀ DI PARMA

II tuo lD AppIe e stato utilizzato per accedere a i..

Mittente Apple Data 2020-01-26 17:48

Per proteggere la tua privacy, le immagini remote di questo messaggio sono state bloccate.
Visualizza immagini

Gentile Cliente,

il tuo ID Apple è stato utilizzato per accedere a iCloud da un browser web.

Data e ora: **26 gennaio 2020, 17:36 PDT**

Indirizio IP , Luogo: **178.213.13.136, Russia - Moscow**

Se recententemente hai eseguito l'accesso a iCloud, puoi ignorare questa email.

Se recententemente non hai eseguito l'accesso a iCloud e ritieni che qualcun altro

Finta Email da Apple

UNIVERSITÀ DI PARMA

Corpo del Messaggio

Gentile Cliente,

il tuo ID Apple è stato utilizzato per accedere a iCloud da un browser web.

Data e ora: **26 gennaio 2020, 17:36 PDT**

Indirizio IP , Luogo: **178.213.13.136, Russia - Moscow**

Se recententemente hai eseguito l'accesso a iCloud, puoi ignorare questa email.

Se recententemente non hai eseguito l'accesso a iCloud e ritieni che qualcun altro possa aver eseguito l'accesso al tuo account, clicca sul link seguente per riavviare il informazioni Il mio ID Apple.

Cordiali saluti,

Supporto Apple

Finta Email da Apple

UNIVERSITÀ DI PARMA

Ma
in realtà...

Return-Path: <app@rep.com>
X-Original-To: selene@giupponis.it
Delivered-To: selene@giupponis.it
X-No-Auth: unauthenticated sender
Received: from lipik (localhost.localdomain [127.0.0.1])
by lipik.liponet.sk (Postfix) with SMTP id A91D829BBA
for <selene@giupponis.it>; Sun, 26 Jan 2020 17:48:03 +0100 (CET)
X-No-Auth: unauthenticated sender
Received: from lipik.liponet.sk (www.liponet.sk [195.168.209.56])
by in-6.smtp.seeweb.it (Postfix) with ESMTP id 73B49140114C
for <selene@giupponis.it>; Sun, 26 Jan 2020 17:48:04 +0100 (CET)
Received: from lipik (localhost.localdomain [127.0.0.1])
by lipik.liponet.sk (Postfix) with SMTP id A91D829BBA
for <selene@giupponis.it>; Sun, 26 Jan 2020 17:48:03 +0100 (CET)
Subject: Il tuo ID Apple e stato utilizzato per accedere a iCloud da un browser web
Date: Sun, 26 Jan 2020 17:48:03 +0100
Mime-Version: 1.0
Content-Type: text/html; charset="iso-8859-1"
To: selene@giupponis.it
Content-Transfer-Encoding: quoted-printable
From: Apple<app@rep.com>
Message-Id: <20200126164803.A91D829BBA@lipik.liponet.sk>
X-Virus-Scanned: clamav-milter 0.99.2 at in-6.smtp.seeweb.it
X-Virus-Status: Clean
X-Spam-Status: No, score=2.5 required=7.0 tests=GB_GOOGLE_OBFUR,
GOOG_REDIR_HTML_ONLY,HTML_MESSAGE,HTML_MIME_NO_HTML_TAG,
HTML_TEXT_INVISIBLE_FONT,MIME_HTML_ONLY,PDS_DBL_URL_TNB_RUNON,SPF_HELO_NONE,
SPF_NONE autolearn=disabled version=3.4.0
X-Spam-Level: **
X-Spam-Checker-Version: SpamAssassin 3.4.0 (2014-02-07) on in-6.smtp.seeweb.it

Fatevi delle domande, dateci delle risposte 1/2

UNIVERSITÀ DI PARMA

Quanto ritiene probabile il rischio di poter essere vittima di una frode o un raggiro tramite Internet (cyber attack)?

- Molto probabile
- Abbastanza probabile
- Non molto probabile
- Molto improbabile
- Non lo so / nessuna risposta

Per quale ragione?

- Ritengo di avere attuato le opportune precauzioni
- Ritengo che i servizi a cui accedo siano ragionevolmente protetti
- Non ritengo di essere un possibile obiettivo di un cyber attack
- Non ritengo che il cyber attack sia una minaccia concreta
- Non lo so / nessuna risposta

Sui suoi dispositivi informatici (PC, smartphone, tablet…) utilizza sistemi di protezione contro virus o attacchi hacker?

- Si, su tutti i miei dispositivi e ne verifico il costante aggiornamento
- Si, su tutti i miei dispositivi ma non ne verifico il costante aggiornamento
- Si, ma non su tutti i miei dispositivi
- No, non li utilizzo
- Non so / nessuna risposta

Quando riceve un allegato non atteso tramite e-mail da un familiare, conoscente o amico, come si comporta?

- Non apro mai allegati inattesi e verifico con il mittente
- Verifico che l'allegato non contenga virus, quindi lo apro
- Apro l'allegato solo se non mi sembra sospetto
- Apro sempre gli allegati se ne conosco il mittente
- Non so / nessuna risposta

Fatevi delle domande, dateci delle risposte 2/2

UNIVERSITÀ DI PARMA

Le è capitato di subire un tentativo di frode tramite telefono o messaggio negli ultimi 12 mesi?

- Si
- No

Pensi all'ultima volta in cui ha ricevuto un'email di phishing, come si è comportato?

- L'ho immediatamente riconosciuta e cancellata
- Ho cliccato sul link dell'email
- Ho cliccato sul link e dopo ho inserito I dati richiesti
- Niente, non ho fatto nulla
- Non so / non ricordo

Quando accede a reti Wi-Fi pubbliche (es. ufficio, comune, bar, sala d'attesa...) come si comporta?

- Non accedo mai a reti Wi-Fi pubbliche per evitare rischi
- Accedo solo a reti Wi-Fi protette da password
- Accedo a reti Wi-Fi solo se conosciute
- Accedo a reti Wi-Fi e non mi assicuro mai dell'affidabilità
- Non so / nessuna risposta

Recap del «buon senso»

UNIVERSITÀ DI PARMA

- **Non esistono** “fortune immediate”: eredita’ di parenti lontani e deceduti, lotterie, etc.
- **Esaminate con cura** il MITTENTE delle email sospette (ed anche di quelle “strane” come richieste, sebbene non “sospette a prima vista”)
- **Leggete** sempre **con attenzione** il TESTO delle email che vi arrivano: lingua, forma, contenuto e richieste
- **Non fornite mai** Utenza e Password **in risposta ad una email**
- Nel **dubbio**, **alzate il telefono** e **richiamate** il “mittente” **a voce**
- **Non fornite password, PIN o altre informazioni al telefono** se vi chiamano per chiedervele (appendete e **richiamate voi al numero che gia’ conoscete ed usate abitualmente**)
- **Non aprite allegati email** se siete dubbiosi: **contattate l’IT e/o inoltrate loro l’email sospetta**
- Per i CFO: **verificate sempre che la parte iniziale** (Country) **dell’IBAN** sia “IT”, o comunque **che corrisponda all’IBAN al quale effettuate bonifici abitualmente** (frode “BEC” o “Man in the Mail”)

Recap del «buon senso»

UNIVERSITÀ DI PARMA

Alcuni consigli anti-phishing e "anti-scam" di Kevin Mitnick, **l'hacker più famoso del mondo** nonché **amico storico di Raoul**, ed **altre risorse gratuite** per...

#staysafeonline&offline!

https://www.digitree.it/covid-19-awareness-resource-kit/

Letture /1

UNIVERSITÀ DI PARMA

- **The Kingpin: la storia della più grande rapina digitale del secolo**, Kevin Poulsen, 2013, Hoepli
- **Fatal System Error: the Hunt for the new Crime Lords who are bringing down the Internet**, Joseph Menn, Public Affairs, 2010
- **Profiling Hackers: the Science of Criminal Profiling as applied to the world of hacking,** Raoul Chiesa, Stefania Ducci, Silvio Ciappi, CRC Press/Taylor & Francis Group, 2009
- **H.P.P. Questionnaires 2005-2010**
- **Stealing the Network: How to Own a Continent, (an Identity), (a Shadow)** (V.A.), Syngress Publishing, 2004, 2006, 2007
- **Stealing the Network: How to Own the Box**, (V.A.), Syngress Publishing, 2003
- **Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier**, Suelette Dreyfus, Random House Australia, 1997
- **The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage**, Clifford Stoll, DoubleDay (1989), Pocket (2000)
- **Masters of Deception: the Gang that Ruled Cyberspace**, Michelle Stalalla & Joshua Quinttner, Harpercollins, 1995
- **Kevin Poulsen, Serial Hacker**, Jonathan Littman, Little & Brown, 1997
- **Takedown**, John Markoff and Tsutomu Shimomura, Sperling & Kupfler, (Hyperion Books), 1996
- **The Fugitive Game: online with Kevin Mitnick**, Jonathan Littman, Little & Brown, 1997
- **The Art of Deception**, Kevin D. Mitnick & William L. Simon, Wiley, 2002
- **The Art of Intrusion**, Kevin D. Mitnick & William L. Simon, Wiley, 2004
- **@ Large: the Strange Case of the World's Biggest Internet Invasion**, Charles Mann & David Freedman, Touchstone, 1998

Letture /2

UNIVERSITÀ DI PARMA

- **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

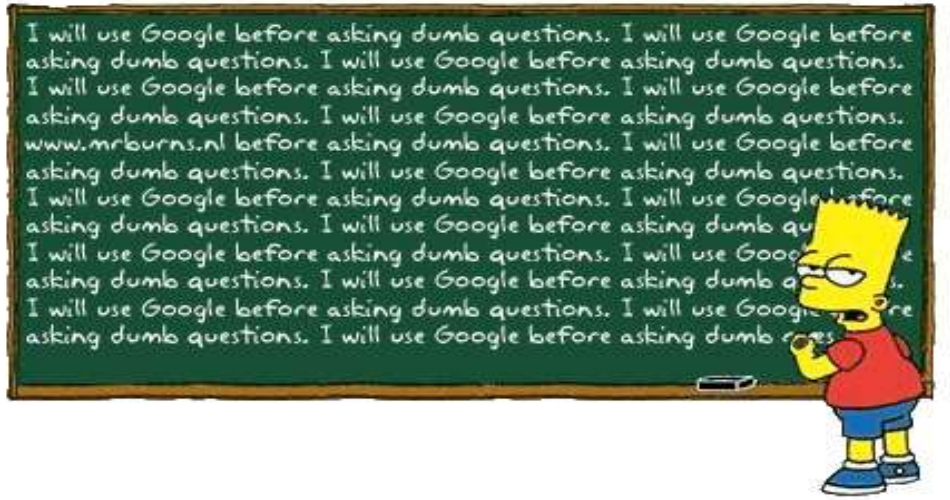
Domande e Risposte

UNIVERSITÀ DI PARMA

Thanks for your attention!

Ing. Selene Giupponi

Selene.Giupponi@unipr.it



Dall'Hacking al CyberCrime, passando per il Cyber Espionage e l'Information Warfare

Selene.Giupponi@unipr.it

UNIVERSITÀ
DI PARMA