

# **Corso di “Sicurezza informatica”**

## **Laurea Magistrale in Ingegneria Informatica**

### **A.A. 2023/2024**

**“Attacchi informatici”**

**Prof. Mirco Marchetti**

**Università di Modena e Reggio Emilia**

# **“Every company is becoming a digital company” (or it has no future)**

**Nel 2024 non esistono linee di business che  
non siano supportate da sistemi e servizi  
informatici e da informazioni in forma digitale.**

**Punto.**

# Alcuni vincitori



WIKIPEDIA  
The Free Encyclopedia



Instagram



BitTorrent™



MEAL SHARING



# Riflessioni

- 1) Perché sono vincenti?**
  
- 2) Quali caratteristiche devono garantire per continuare a essere vincenti?**

# Technologie di interconnessione

## Elementi del cyberspace



**Persone**



**Dati**



ANDROID



Linux

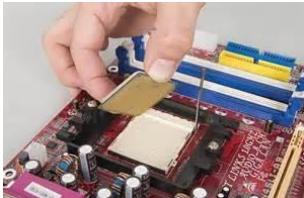


Mac OS X



Microsoft  
Windows

**Software e  
Servizi**



**Hardware**



**UNIMORE**  
UNIVERSITÀ DEGLI STUDI DI  
MODENA E REGGIO EMILIA

# Caratteristica comune

Technologie di interconnessione



Personne

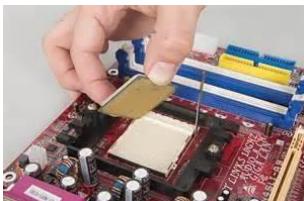


Dati



Software e  
Servizi

ANDROID

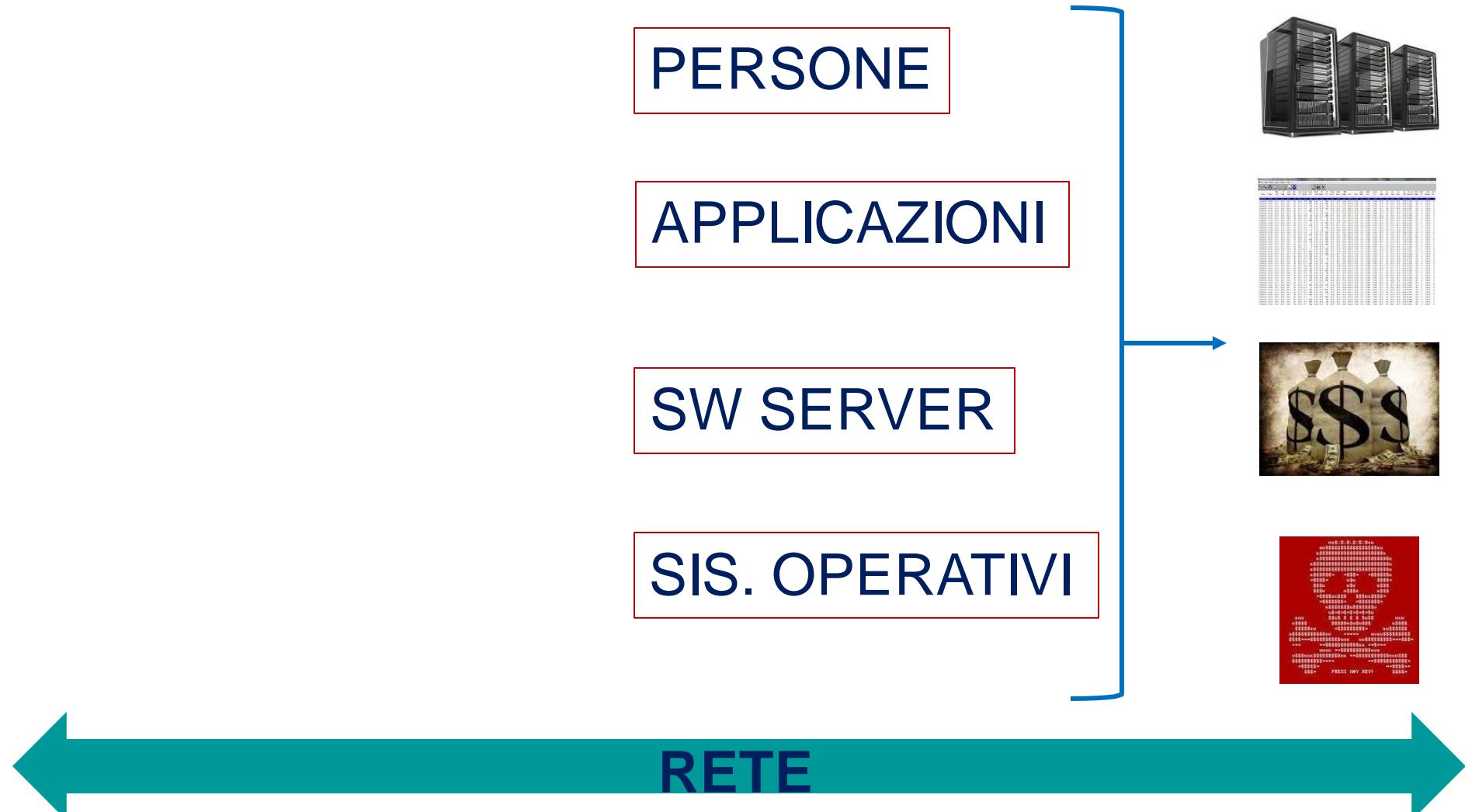


Hardware



UNIMORE  
UNIVERSITÀ DEGLI STUDI DI  
MODENA E REGGIO EMILIA

# Tanti tipi di vulnerabilità



# Tante vulnerabilità: a guardar bene, tutte umane

*Debolezze umane,  
Incompetenza e/o Superficialità*

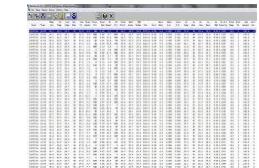
*Software vulnerabile  
Software obsoleto (a volte non aggiornabile)  
Software configurato in modo non corretto  
Default non sicuri  
...*

**PERSONE**

**APPLICAZIONI**

**SW SERVER**

**SIS. OPERATIVI**

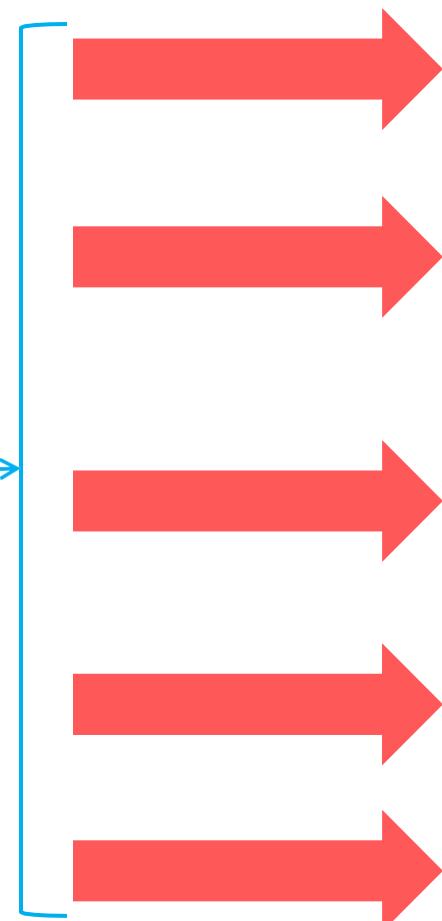


**RETE**

*Software dei protocolli vulnerabile e/o Configurazioni di rete o di apparati errate*

# Vulnerabilità e Attacchi (*tecnologici e psicologici*)

Attacchi



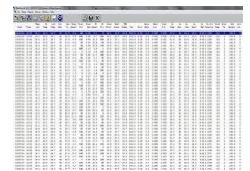
PERSONE

APPLICAZIONI

SERVER

SIS. OPERATIVI

RETE

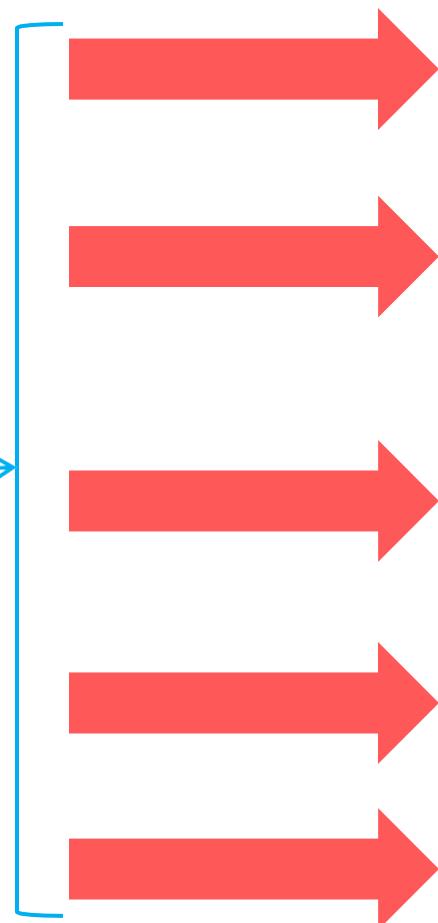


## *Strumenti di attacco*

## *Obiettivi secondari*

## *Obiettivi primari*

Attacchi



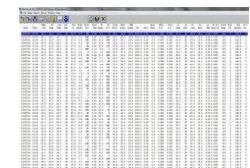
**PERSONE**

**APPLICAZIONI**

**SERVER**

**SIS. OPERATIVI**

**RETE**



# Quali possono essere i danni cyber?

DANNI

- **Furti, truffe, estorsioni**
- **Fermo operatività**
- **Furto informazioni aziendali**
- **Danno reputazionale, Disinformazione**
- **Sanzioni per violazione Legge**
- **Perdita mercato per mancata compliance**



# **Quale danno è più grave?**

**Furti, truffe, estorsioni**

**Fermo operatività**

**Furto informazioni aziendali**

**Danno reputazionale, Disinformazione**

**Sanzioni per violazione Legge**

**Perdita mercato per mancata compliance**

# Verso un mondo “smart” con un nuovo problema



# Health devices

## 1 Consumer products for health monitoring:

These devices -- such as FitBit, Nike FuelBand, or Withings -- generally communicate using BlueTooth to nearby personal mobile devices.



## 2 Wearable, external medical devices:

This category includes portable insulin pumps which often use proprietary wireless protocols to communicate.



## 3 Internally embedded medical devices:

Pacemakers and other medical devices are implanted in the patient but communicate wirelessly, either with proprietary wireless protocols or Bluetooth.



## 4 Stationary medical devices:

These devices, such as hospital-based chemotherapy dispensing stations or homecare cardio-monitoring for bed-ridden patients, often use more traditional wireless networks, such as WiFi networks in hospitals or patients homes.

# Safety



## Germania: donna muore durante attacco ransomware all'ospedale



E' il primo decesso legato a cyberattacco contro una struttura sanitaria. La paziente, destinata all'ospedale di Duesseldorf, è stata trasferita ed è deceduta per il ritardo delle cure. Nel 2017 WannaCry contribuì ad un incremento della mortalità ospedaliera

Bloccati 30 server dell'ospedale universitario di Dusseldorf, sfruttando una vulnerabilità nota da gennaio (CVE-2019-19871) dei gateway Citrix. L'ospedale non era in grado di gestire l'accettazione pazienti e il trasferimento a un altro ospedale è stato fatale

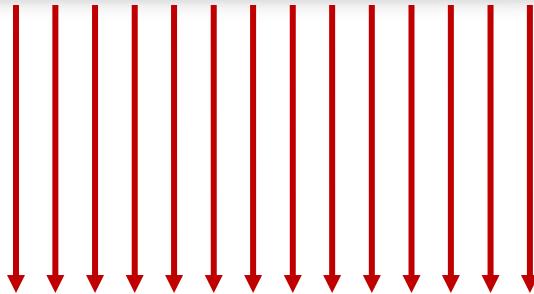
# Nel corso parleremo di “pioggia”, ma soprattutto di come riparare il “tetto”

## MINACCE

Attacchi intenzionali

Guasti, Incidenti

Errori umani



## VULNERABILITÀ AZIENDALI



# Attaccanti vs. Difensori (1)

## Gli attaccanti:

- 1) non hanno limiti spazio-temporali nell'azione e non sono soggetti ai confini legali di un Paese
- 2) hanno molteplici possibilità di creare e acquisire armi da mercati leciti e illeciti
- 3) possono collaborare facilmente perché le informazioni scambiate riguardano altri
- 4) hanno possibilità di mascheramento e falsa attribuzione
- 5) sono favoriti dalla labilità e volatilità delle “prove forensi” (niente DNA, pistole fumanti, guanti di paraffina, stub)
- 6) creano valore (illegale, ma che è sempre valore)
- 7) sono molto favoriti dalla diffusione della cripto-valuta



# Attaccanti vs. Difensori

- I difensori:

- 1) ...
- 2) ...

La cybersecurity non è cavalleresca

La cybersecurity non prevede un  
confronto paritetico tra gli avversari

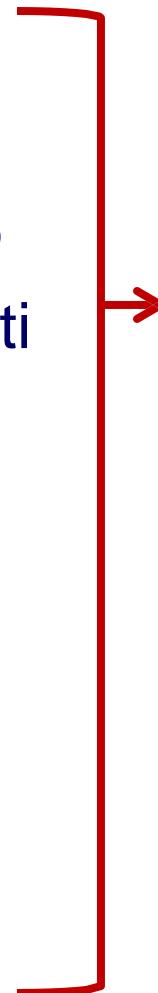
# Cyber criminali (in proprio) – Contractor

- 1. Rubare informazioni (da trasformare in denaro)**
  - a) Identità, indirizzi di posta, credenziali di accesso, carte di credito, profili personali, dati sanitari, ...
  - b) Informazioni aziendali (personale, ruoli, dati commerciali)
  - c) Spionaggio industriale (progetti, investimenti, strategie)
- 2. Rubare denaro ad aziende e persone**
  - a) Furti
  - b) Truffe
  - c) Ricatti
- 3. Lavorare per conto terzi / Offrire servizi**
  - a) Creazione e noleggio di reti di computer infetti (*botnet*)
  - b) SPAM
  - c) Realizzazione, vendita e diffusione di vulnerabilità e *malware*
  - d) Investigazioni illegali
  - e) Riciclaggio di denaro
  - f) Diffamazione e diffusione di informazioni false

# Industria matura: 1) Specializzazione

## Piccoli gruppi che ...

- acquisiscono indirizzi email
- rubano identità digitali
- rubano numeri di carte di credito
- infettano computer per creare reti di computer **zombie (botnet)**
- sanno inventare “storie” per truffe
- effettuano traduzioni
- creano malware
- creano strumenti di attacco
- profilano i comportamenti utente
- ...



## E altri gruppi (non solo privati) che ...

- comprano
- conducono attacchi
- commettono i veri attacchi
- trasformano dati in denaro
- riciclano denaro



## Industria matura: 2) Mercati

### World Wide Web

(risorse indicizzate da Google, Bing, Yahoo)

### DEEP Web

(risorse non indicizzate: include aree locali di aziende e privati, dati a cui si accede mediante autenticazione, contenuti dinamici, cloud, ...)

Cyber FORUM



Circoli chiusi



**UNIMORE**  
UNIVERSITÀ DEGLI STUDI DI  
MODENA E REGGIO EMILIA

## A. Cyber Forum

- Si trovano con Google e si visitano senza software speciali
- Per visione prodotti, ci sono due livelli: con e senza registrazione
- Per l'acquisto, è necessaria la registrazione (tracciano come gli altri siti di e-commerce)
- E' facile entrare per chi è disposto a pagare → Cybercrime as a Service (CaaS)


[Home](#) [Upgrade](#) [Search](#) [Memberlist](#) [Extras](#) [Help](#) [Wiki](#) [Follow](#) [Contact](#)

Hello There, Guest! [Login](#) [Register](#)

Current time: 04-14-2018, 12:07 AM

## Hack Forums


[Common](#) [Hack](#) [Tech](#) [Code](#) [Game](#) [Groups](#) [Web](#) [GFX](#) [Market](#) [Money](#) [World](#)

### Hacks, Exploits, and Various Discussions



Forum		Threads	Posts	Last Post
	<b>Beginner Hacking</b> This is for the entry level hacker wishing to learn more about the art of h4ck5. Moderated By: Mentors E-Wholing Private Investigation Methods and Anonymity	229,645	1,791,495	<b>regarding amazon gift car...</b> 2 minutes ago by white shinobi
	<b>Advanced Hacking</b> If you feel you're past the beginner stages and want to delve deeper into computer security, analysis, and internet exploits you should participate here. Botnets, IRC Bots, and Zombies Pen-testing and Forensics	115,318	942,982	<b>Pink-Panther's AUTOMATED ...</b> 35 minutes ago by superm008


**UNIMORE**

UNIVERSITÀ DEGLI STUDI DI

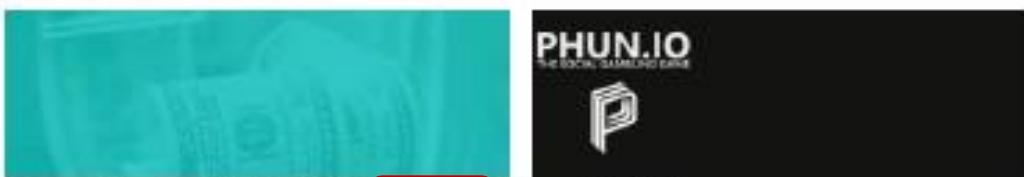
MODENA E REGGIO EMILIA


[Home](#) [Upgrade](#) [Search](#) [Memberlist](#) [Extras](#) [Help](#) [Wiki](#) [Follow](#) [Contact](#)

Hello There, Guest!

[Login](#) [Register](#)

Current time: 04-14-2018, 12:07 AM

**Hack Forums**
[Common](#) [Hack](#) [Tech](#) [Code](#) [Game](#) [Groups](#) [Web](#) [GFX](#) [Market](#) [Money](#) [World](#)
**Marketplace**

Forum	Threads	Posts	Last Post
 <b>Marketplace Discussions</b> This is to be used for rules, policies, feedback, and general discussions about the HF Marketplace. Please read the stickies in this section before conducting business here. Free Services and Giveaways      Appraisals and Pricing Deal Disputes	221,078	2,986,303	<a href="#">Learn How To Start Your O...</a> 25 minutes ago by CYB3RM4N
 <b>Premium Sellers Section</b> This area is only for upgraded member sales threads. Premium Tools and Programs      Cryptography and Encryption Market	86,110	1,599,858	<a href="#">AUTOCASH V2.0 @ AUTOPILOT...</a> 8 minutes ago by Ombra
 <b>Secondary Sellers Market</b> This is a sellers section open to all members. We advise extreme caution in all deals here. Sales threads must follow the policies of HF and we expect you to read them in the help documents. Virtual Game Items      Member Auctions	233,772	1,418,685	<a href="#">[H] 07 Gold 147m+ [W] Cry...</a> 15 minutes ago by Dnine2

**UNIMORE**

UNIVERSITÀ DEGLI STUDI DI

MODENA E REGGIO EMILIA

## B. Dark Web: mezzi prevalenti per i clienti

Non è illegale visitare il Dark Web, ma fornisce accesso a molteplici servizi illegali e vendita illegale di prodotti



### 1. Anonimizzazione della navigazione

- Prevalentemente **TOR** ma non solo

### 2. Criptovaluta

- Prevalentemente  
**MONERO/BITCOIN**, ma non solo

### 3. Identità non certificata (*nickname*)

4. e tanta tanta attenzione perché è anche un regno di truffatori

# Cosa si vende veramente nei Dark Market?

- 1) Carte di credito e di credenziali (login/password)
- 2) Dati (persone, cartelle cliniche, rating finanziari, ecc.)
- 3) Droga
- 4) Farmaci
- 5) Materiale protetto da copyright
- 6) Armi
- 7) Documenti (passaporti, identità, patenti, diplomi, certificati)
- 8) Malware e servizi per attacchi cyber
- 9) Omicidi su commissione
- 10) Persone (per prostituzione e lavoro in semi schiavitù)
- 11) Materiale pedo-pornografico
- 12) Organi per trapianti
- 13) ... *Bufale*



# Quale prodotti costituiscono il maggiore fatturato (stima 80%) dei Dark Market?

- 1) Carte di credito e di credenziali (login/password)
- 2) Dati (persone, cartelle cliniche, rating finanziari, ecc.)
- 3) Droga e farmaci
- 4) Materiale protetto da copyright
- 5) Armi
- 6) Documenti (passaporti, identità, patenti, diplomi, certificati)
- 7) Malware e servizi per attacchi cyber
- 8) Omicidi su commissione
- 9) Persone (per prostituzione e lavoro in semi schiavitù)
- 10) Materiale pedo-pornografico
- 11) Organi per trapianti
- 12) ... *Bufale*



# Droga

## AREA51

[? Get help](#)

1 ₿ = 351.54\$

orders: 0 messages: 0 settings logout

search...



0.000000₿

u again ? really ? gwern

### DRUGS

BENZOS (31)

CANNABIS (82)

DISSOCIATIVES (1)

ECSTASY (26)

OPIOIDS (22)

OTHER (4)

PRECURSORS (0)

PRESCRIPTION (2)

PSYCHEDELICS (11)

STEROIDS/PED (2)

STIMULANTS (89)

### ALCOHOL

ABSINTH (0)

WHISKY/BOURBON (0)

### DIGIT. GOODS

FRAUD (29)

GAMING / CARDS (1)

SOFTWARE (1)

### DOCUMENTS

DRIVER LICENSES (0)

IDS (3)

OTHERS (1)

### OTHERS

DRUG PARAPHERNALIA (2)

ELECTRONICS (2)

OTHERS (5)

### WEAPONS

BLADES/WEAPONS (1)

sort by: Date(Newest) | ship from: Everywhere | ship to: Everywhere | update



Heroin 1.00g (white-rock)

Vendor: AuStore  
Ships from: Australia

1.27722 ₿



Heroin 0.50g (white-rock)

Vendor: AuStore  
Ships from: Australia

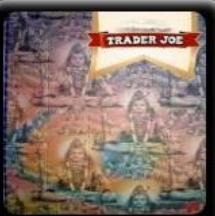
0.65141 ₿



Heroin 0.25g (white-rock)

Vendor: AuStore  
Ships from: Australia

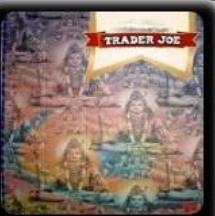
0.39540 ₿



10x Dutch LSD Shiva print 180ug LAB TESTED! - COPY

Vendor: Tr4derJ03  
Ships from: Germany

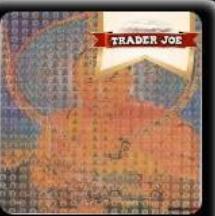
0.28446 ₿



5x Dutch LSD Shiva print 180ug LAB TESTED!

Vendor: Tr4derJ03  
Ships from: Germany

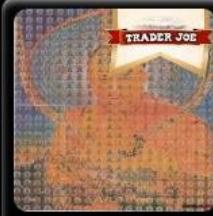
0.15076 ₿



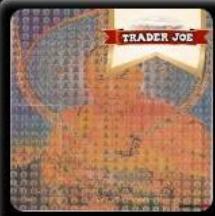
25x Dutch LSD Dalai Lama 225ug LAB TESTED!

Vendor: Tr4derJ03  
Ships from: Germany

0.86760 ₿



10x Dutch LSD Dalai Lama 225ug LAB TESTED!



5x Dutch LSD Dalai Lama 225ug LAB TESTED!



12x Iced Grapefruit F2 Female Seeds \*special strain\*



50g Jack Herer A+++ Coffeshop Quality Weed



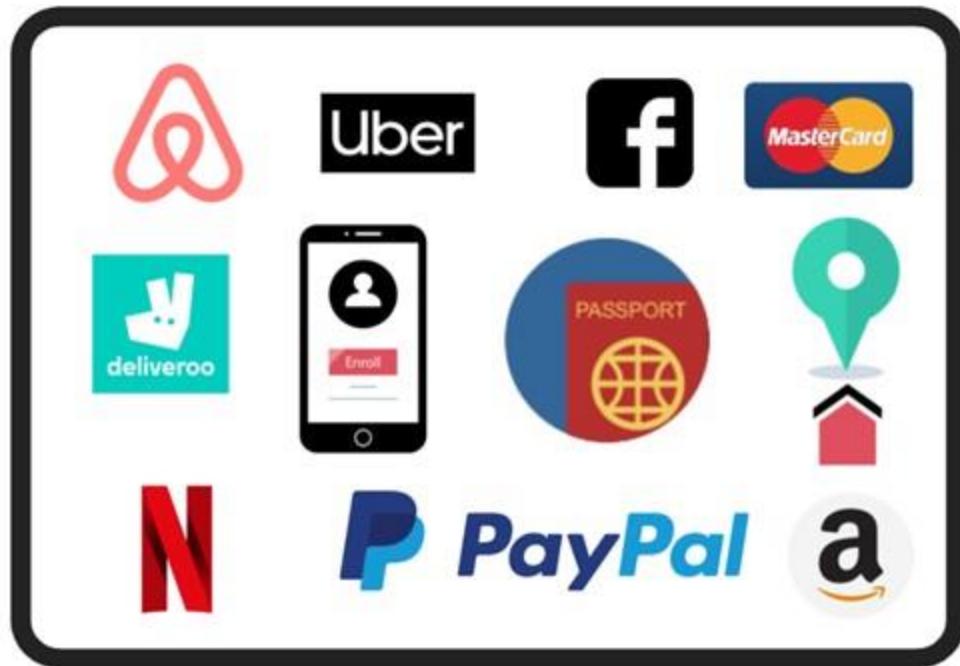
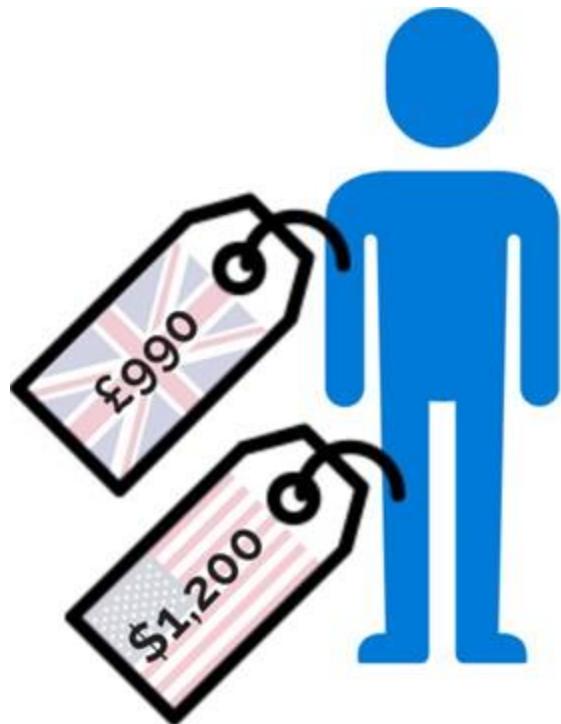
20g Jack Herer A+++ Coffeshop Quality Weed



10g Jack Herer A+++ Coffeshop Quality Weed

# Tanta droga

# Credenziali



# Armi e Passaporti

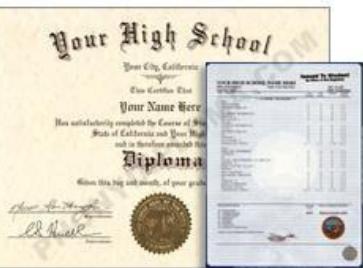
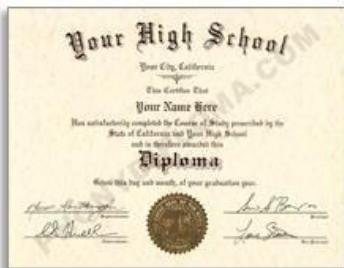
The screenshot shows a website interface for a gun store or similar service. At the top, there's a navigation bar with categories like "Handgun", "Rifle", "Shotgun", "Glock", "Revolver", "Pistol", "Semi-Auto", and "Shotgun". Below the navigation, there's a search bar and a "Sort by" dropdown menu. The main content area is titled "Armi" and displays a grid of firearms. Each item has a small image, a name, and a price. For example, a Glock 17 is listed at \$499.99. To the right of the grid, there's a sidebar with sections for "Categories", "Handguns", "Rifles", "Shotguns", "Glock", "Revolver", "Pistol", "Semi-Auto", and "Shotgun". At the bottom, there's a section titled "Materiale" with a list of items.



# High School

## Diploma

From \$75, they look and feel just like those from a real school! Choose a state seal in raised "puffy" gold ink or fully embossed gold foil stickers. Different paper colors and sizes too.



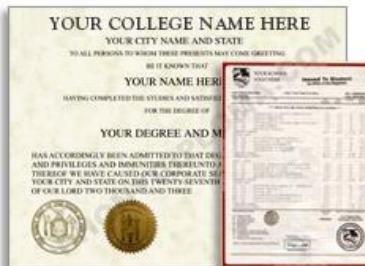
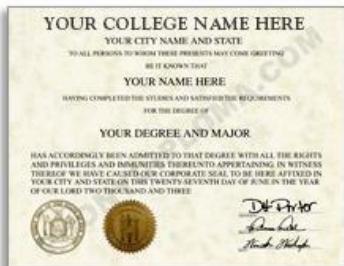
## Transcript



# College & University

## Diploma

From \$125, Fake Diplomas for College, Fake Transcript for College, Fake Diploma and Transcript Package for College, "Actual Match" designs based on original layouts, wording, emblems or budget-friendly "Regional Designs". Top quality diploma parchment paper, fully customized for most degrees and majors.

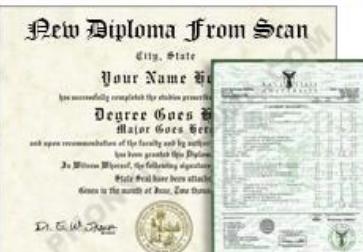


## Transcript



# From Your Scan

From \$250, email us a scan of an original. We'll recreate the graphics with your text changes. NOT cheap "cut and paste" - fully recreated. Prompt price quotes for all levels of complexity.



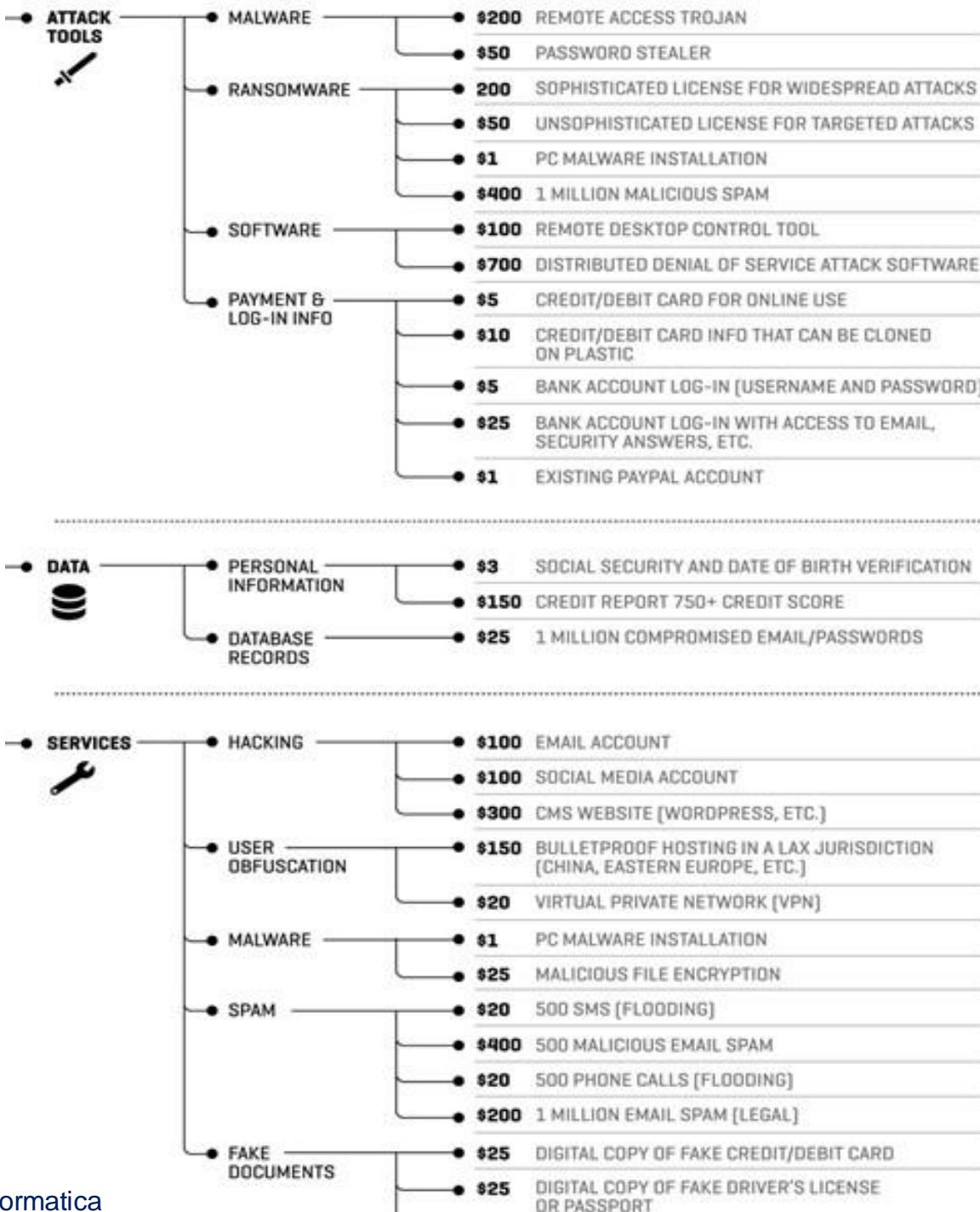
**Send Us Your Scan  
CLICK HERE**

# Certificates

From \$250, they look and feel just like those from a real school! Different paper colors and sizes too.



# Cyber tools



## C. Gruppi underground

- Molti di questi forum non sono pubblicamente noti
- Scopi illegali: criminali, antagonisti, terroristici
- E' estremamente difficile accedere
- Bisogna avere un nome e un passato
- Accesso:
  - In alcuni si accede per presentazione (di uno o più "soci") grazie a competenze o a informazioni possedute
  - In altri, non si accede se non si fa parte di etnie, gruppi religiosi, gruppi pregressi, conoscenze personali

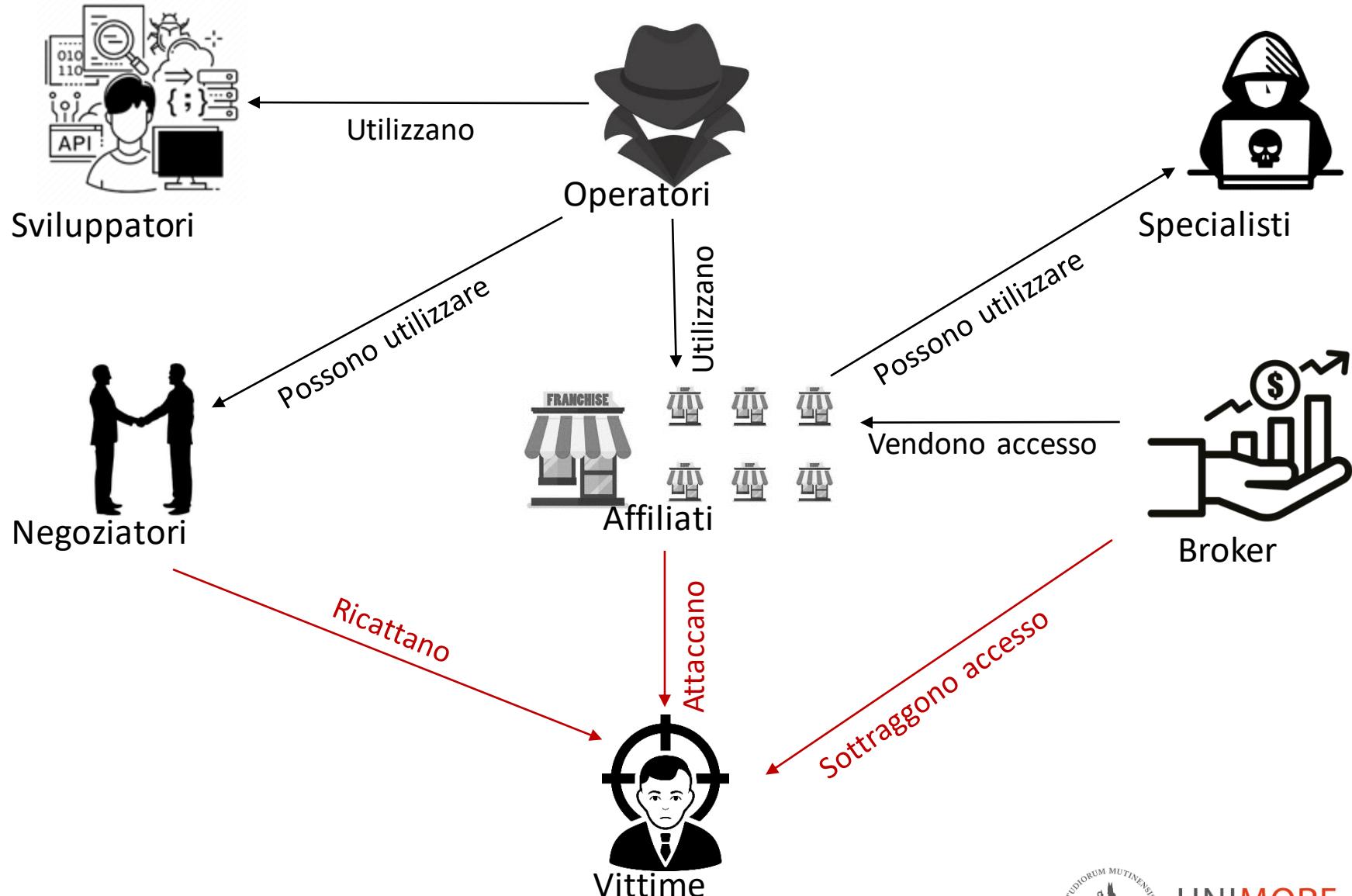
HIDDEN/DARK  
FORUM



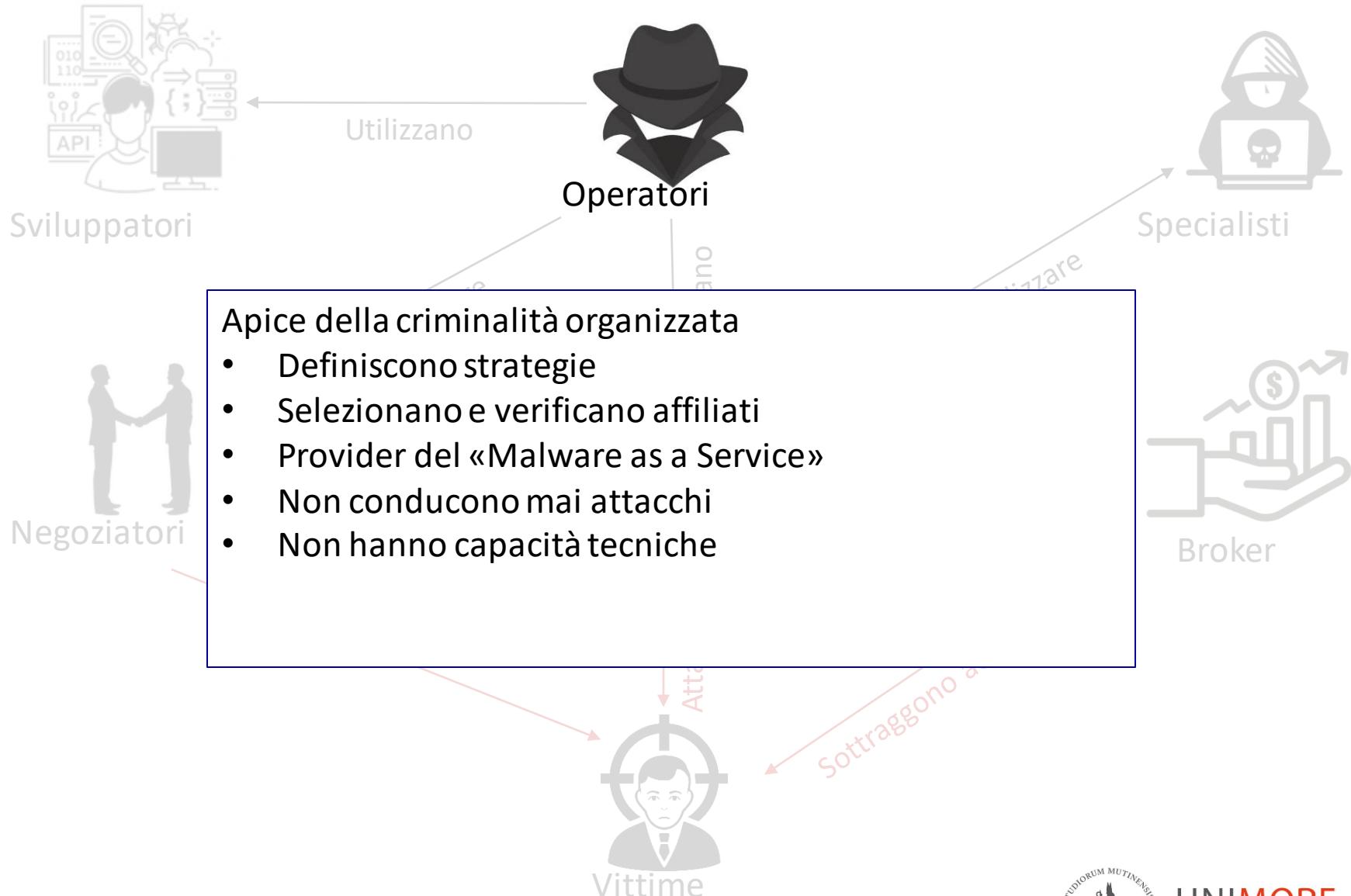
**UNIMORE**  
UNIVERSITÀ DEGLI STUDI DI  
MODENA E REGGIO EMILIA

# Caso di studio: ransomware

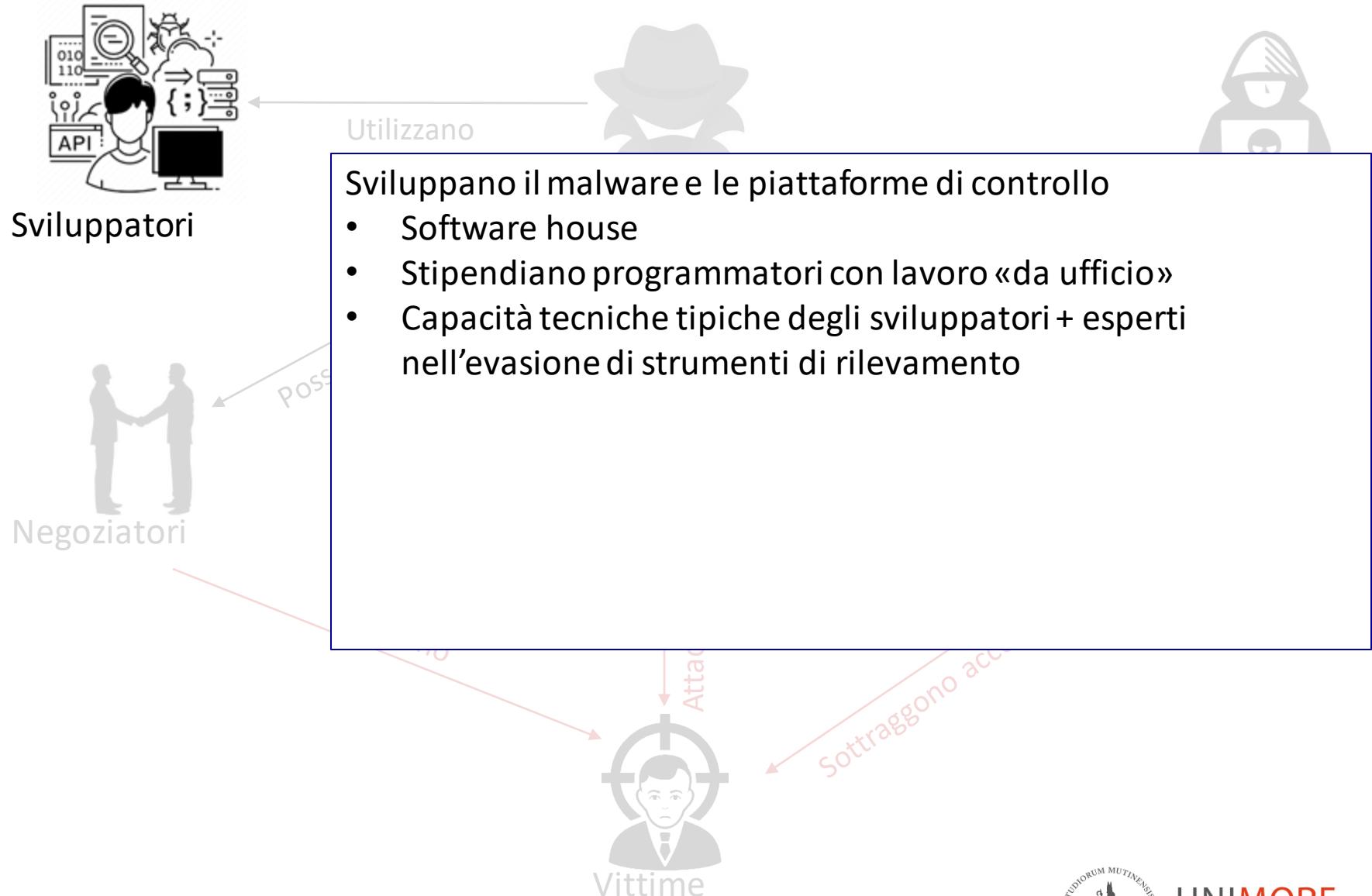
# Ransomware – criminalità organizzata



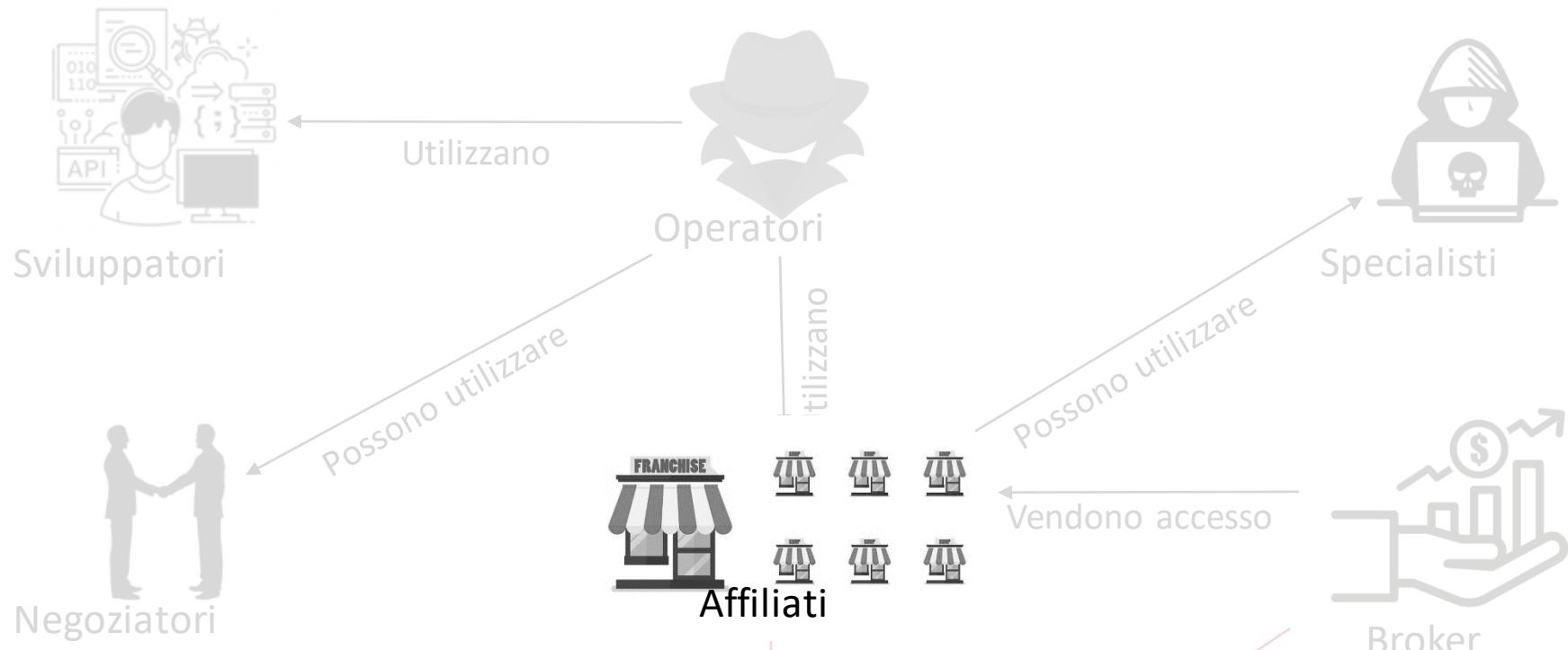
# Ransomware – criminalità organizzata



# Ransomware – criminalità organizzata



# Ransomware – criminalità organizzata



Affiliati a un programma «Malware as a service»

- Scarse capacità tecniche, buona conoscenza di un settore
- Noleggiano un ransomware con identificatore specifico
- Comprano accessi dai Broker
- Percepiscono una percentuale su eventuali riscatti (tipicamente tra il 60% e il 90%)

# Ransomware – criminalità organizzata

Ottengono accessi illeciti a sistemi delle vittime

- Tecniche opportunistiche (phishing, SMSishing, password deboli, vulnerabilità note)
- Tecniche mirate (phishing targeted, social engineering, corruzione dipendenti infedeli)
- Valutano gli accessi che sono riusciti ad ottenere e li vendono a un affiliato



Utilizzano



Specialisti



Broker



**UNIMORE**

UNIVERSITÀ DEGLI STUDI DI  
MODENA E REGGIO EMILIA



Vittime

Sottraggio

# Ransomware – criminalità organizzata

Attaccanti informatici con elevate competenze tecniche

- Conducono attività «tailor-made»
- Assoldati dagli affiliati per target da cui si prevede un ROI elevato
- Movimento laterale, persistenza, esfiltrazione di grandi volumi di dati



Specialisti



Broker

Negoziatori

Affiliati



Vittime

Ricattano

Attaccano

Sottraggono accesso

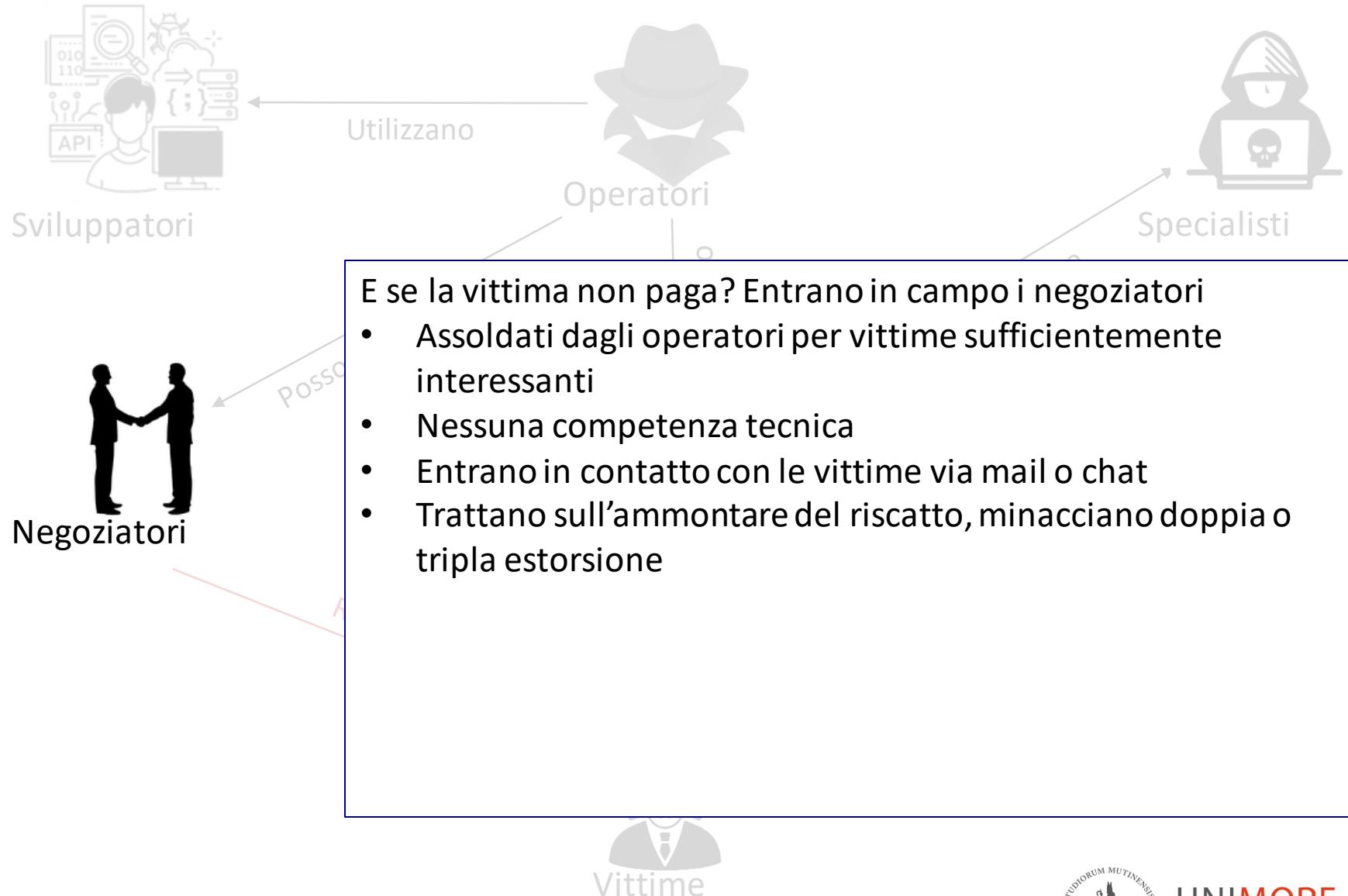


**UNIMORE**

UNIVERSITÀ DEGLI STUDI DI

MODENA E REGGIO EMILIA

# Ransomware – criminalità organizzata



# Cosa cambia per le vittime

Siamo uno tra i tanti, non motiviamo un attacco targeted

Un broker che riesce a sottrarre un accesso mediante tecniche opportunistiche

Il broker ci reputa sufficientemente interessanti e ci vende a un affiliato

L'affiliato si avvale di specialisti per condurre attacchi con complessità simile a un attacco targeted



# Come si attacca un'organizzazione

# Metodologie di attacco

Gli attaccanti ragionano sul *Return of Investment*

## APPROCCIO 1:

*Lancio tante esche, qualcuno abboccherà e lo attacco*



## APPROCCIO 2:

*Provo a verificare (automaticamente) quale azienda è vulnerabile e la attacco*



## APPROCCIO 3:

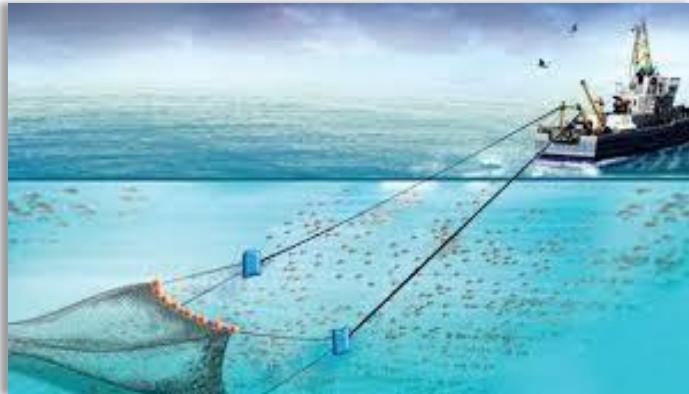
*Punto e attacco una specifica azienda*



**Due categorie di attacchi, soliti tre obiettivi:**

**1) *risposta*, 2) *click su un link*, 3) *apertura di un allegato***

## ATTACCHI GENERALIZZATI



## ATTACCHI MIRATI



# Gli attacchi di phishing nascono con il Web

- La prima campagna di phishing risale al **1996** contro i clienti di *America On Line*, il più grande ISP del tempo
- → Obiettivo: acquisire login e password per collegarsi a Internet senza pagare
- Nel 2020, più del 50% degli attacchi informatici di successo a un'azienda inizia con una mail di phishing. C'è chi arriva a stimare l'80-90%
- **Sono passati 25 anni e la situazione non è migliorata.**  
Anzi ...

# Attacco psicologico *generalizzato*

- **Sfruttare *vulnerabilità* umane**
  - Eccesso di fiducia
  - Curiosità
  - Bramosia di guadagni
  - Bramosia di regali, vincite, ecc.
  - Ideologia
  - Timori e paure (personal)li
  - Pseudo-conoscenza
  - Pseudo-innamoramento
  - Narcisismo
  - ...

**METODO:** Lanciare  
tante esche,  
qualcuno abboccherà



# Attacchi generalizzati

- **Soliti agganci (evergreen):**
  - Opportunità economiche e finanziarie
  - Opportunità relazionali e sessuali
  - Opportunità lavorative
  - Opportunità caritatevoli e sociali
  - Vincite
- **Agganci adattativi:**
  - Legati alle notizie del momento  
(oggi, Covid)

**Finte provenienze:**

Google (13%)
Amazon (13%)
WhatsApp (9%)
Facebook (9%)
Microsoft (7%)
Outlook (3%)
Apple (2%)
Netflix (2%)
PayPal (2%)



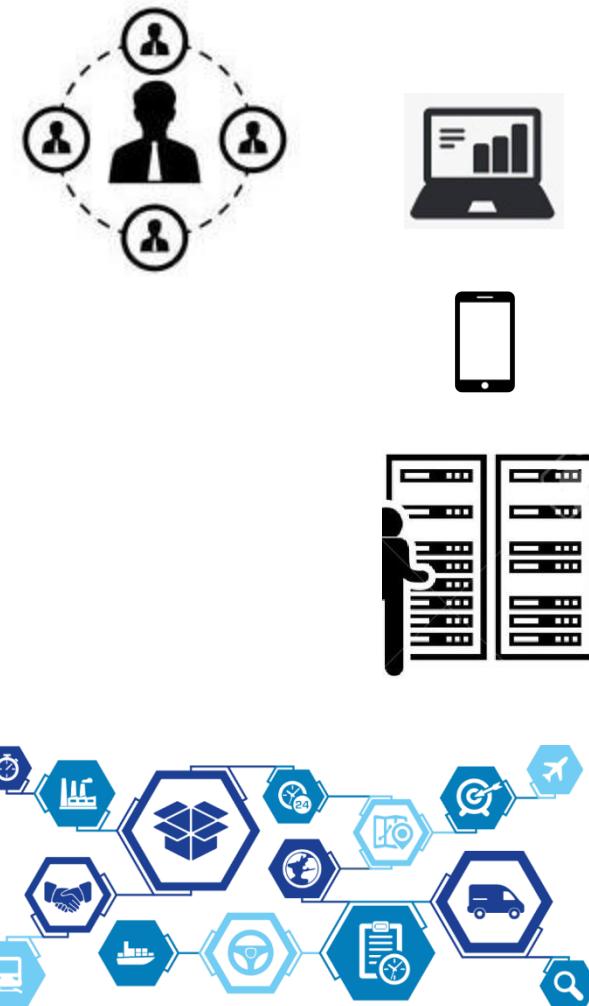
# Tipologie di messaggi

- **Origine (apparente) dei messaggi:**
  - Servizi che hanno accesso a una carta di credito: banche, Amazon, e-Bay, PayPal
  - Servizi che hanno accesso a informazioni personali: Facebook, Instagram, LinkedIn
  - Servizi di storage cloud: iCloud, Drive, Dropbox;
  - Autorità: uffici legali, polizia postale, direttore o reparto IT dell'azienda della vittima
  - Colleghi di lavoro o persone che la vittima conosce
- Nel messaggio il criminale cerca di far leva su curiosità o sulle emozioni del destinatario oppure di approfittare di un momento di disattenzione. Spesso queste e-mail hanno carattere di urgenza e richiedono un'azione immediata: un click a un link o il download di un allegato



# “Attacchiamo una specifica azienda”

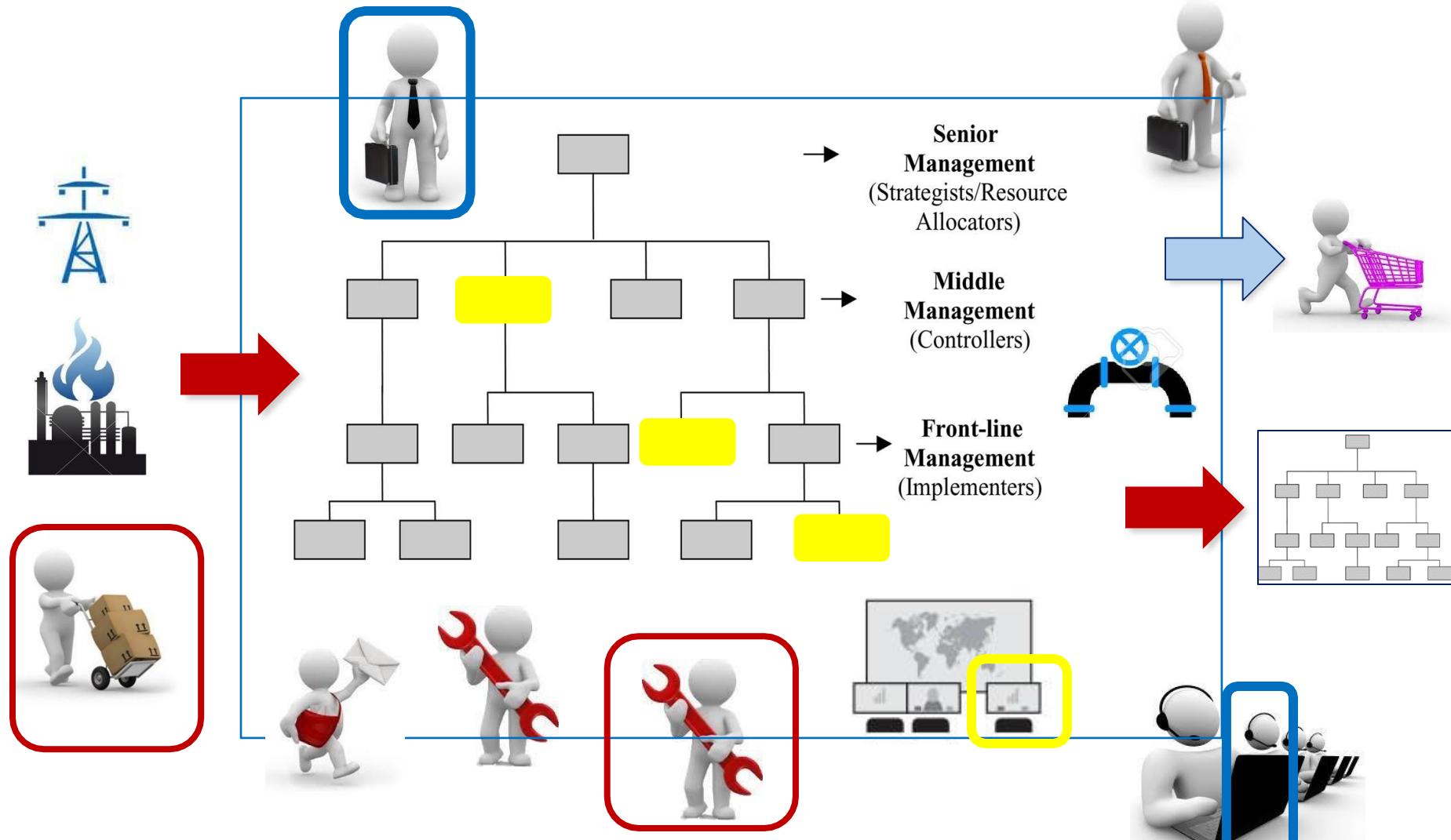
1. Intelligence
2. Individuazione degli obiettivi  
(dipendenti, tecnologie, fornitori)
3. Contatto (persone, dispositivi  
informatici personali e aziendali)
4. Individuazione delle vulnerabilità  
(personal, tecnologiche)
5. Sfruttamento delle vulnerabilità  
(personal, tecnologiche)
6. Attacco e raccolta benefici



# Tecniche – *prima fase*

- L'attacker ha bisogno di molte informazioni che gli serviranno per essere credibile e convincente con l'interlocutore vittima
- Questa ricerca è mirata alla conoscenza di vari particolari:
  - organigramma dell'organizzazione
  - lista di eventuali partner commerciali
  - alcuni indirizzi di e-mail o numeri di telefono degli utenti all'interno dell'organizzazione
  - come è strutturata la rete
  - quali sono le persone chiave
  - quali sono le relazioni tra i vari comandi/enti/reparti
  - ogni altra notizia che potrebbe essere utile alla conoscenza dell'ambiente da "colpire"

# Target umani in azienda



INTERNI

SEMI-INTERNI

ESTERNI

# Social engineering

- Molti attacker hanno dichiarato di reperire la maggior parte delle informazioni necessarie a sferrare un attacco non attraverso tecniche informatiche, ma più semplicemente chiedendole alle potenziali vittime: utilizzando tecniche cosiddette di **Social Engineering**
- Uno dei più famosi *social engineer* → *Kevin Mitnick*
- (5 anni in prigione, oggi consulente di cyber security)

# *E' un libro del 2002 ... Purtroppo ancora moderno*



## Il fattore umano è l'anello più debole della sicurezza

Il libro descrive le strategie di *social engineering* per penetrare nelle reti. Si tratta di espedienti per sfruttare la buona fede, l'ingenuità o l'inesperienza delle persone che hanno accesso ai sistemi informatici aziendali e alle info.

La manipolazione del fattore umano, la capacità di ricostruire le intenzioni, la mentalità e il modo di pensare del nemico, diventa lo strumento più micidiale ed efficace.



# Social engineering

## →Carpire informazioni con la psicologia

- Il Social Engineering prevede un insieme di tecniche psicologiche e non informatiche usate per indurre la vittima a:
  - rivelare i dati personali o sensibili riguardante lei o la propria organizzazione
  - oppure ad aprire degli attachment infetti
  - visitare un sito che magari contenga un dialer o qualche altro materiale pericoloso
- Essendo un insieme di tecniche psicologiche, il social engineering non prevede una preparazione informatica ma una conoscenza della potenziale vittima e del suo contesto



## Tecniche – seconda fase

- Esaurita la raccolta della documentazione, l'attacker deciderà il modo in cui dovrà avvenire l'attacco, che potrebbe essere:
  - per telefono
  - oppure via e-mail
  - oppure Social network
  - più raramente di persona



- Il bravo *social engineer* è “fantinoso”

# Attacchi psicologici mirati

- 1) **Intelligence:** il Web e i social (soprattutto, Linkedin) facilitano le azioni di intelligence dell'attaccante
- 2) **Aggancio credibile (perché mirato\*)**
- 3) **[Comunicazioni innocue]**
- 4) **Messaggio “fatale”**

**METODO:** Colpisco la persona giusta dopo averla studiata



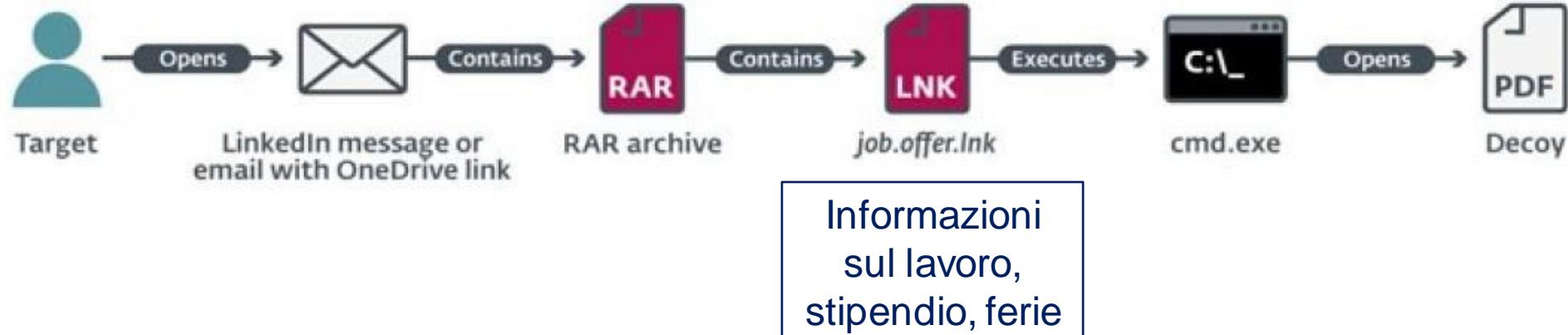
---

\* Una mail che arriva da una banca qualsiasi è facilmente identificabile. Una mail che arriva dalla tua banca richiede molta più attenzione

# Attacco psicologico mirato

- **Sfruttare vulnerabilità umane (HUMINT)**
  - Eccesso di fiducia
  - Scarsa osservanza delle regole
  - Abitudini e resistenza al cambiamento
  - Ignoranza e incompetenza
  - Ideologia e fanatismo (religiosa, politica, sportiva, sanitaria, ...)
  - Timori e paure (personalì e sui famigliari)
  - Insoddisfazione e desiderio di vendetta
  - Perversioni, immoralità e ricattabilità
  - Sesso e innamoramento
  - Bramosia di guadagni
  - Narcisismo
  - Debiti
  - ...

# Recente esempio di phishing mirato a dipendenti di aziende dell'aeronautica, spazio e difesa



# **CEO fraud: l'Amministrazione come target**

1. Gli attaccanti acquisiscono le credenziali di caselle di posta del personale amministrativo che esegue i bonifici o che ha relazioni con clienti e fornitori. L'azione viene condotta mediante *phishing* o riutilizzo di credenziali disponibili in rete, monitoraggio della mailbox e utilizzo della stessa per l'invio di false fatture o vere fatture con IBAN modificato
2. Gli attaccanti compromettono il mail server dell'impresa, in modo da riuscire a leggere e sostituire le mail in tempo reale. Evitano l'uso di canali di comunicazione fraudolenti e sono meno rilevabili
3. I criminali riescono a installare software malevolo sui PC o gli smartphone del personale amministrativo mediante azioni di *social engineering* condotte su sorgenti aperte e social network e che sono finalizzate a identificare le relazioni tra i dipendenti della società. In tal modo, sono in grado di inviare false mail con richieste di bonifici fraudolenti verso IBAN creati ad hoc

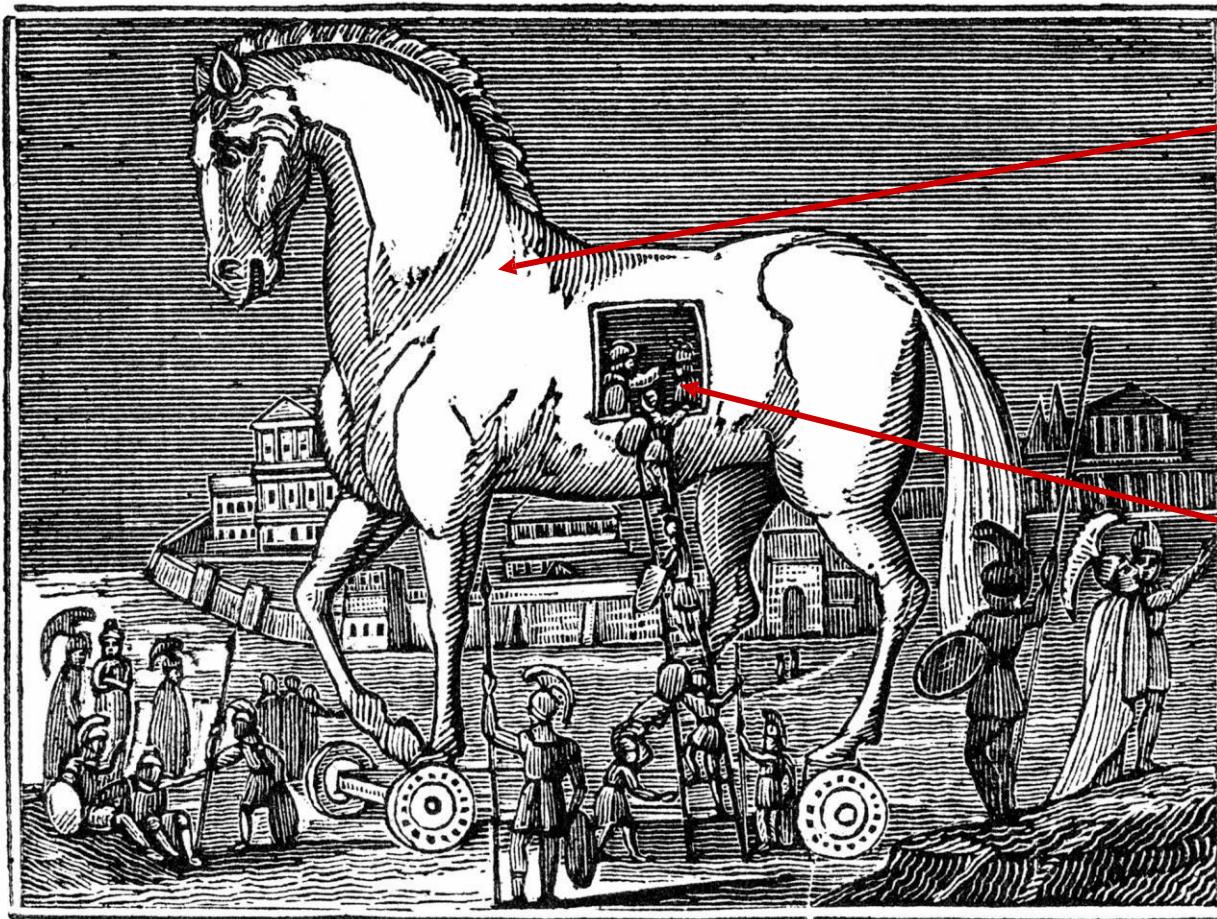


# La verità sulla possibilità dei cyber attacchi

**“La grande maggioranza degli attacchi cyber è causato da vulnerabilità software spesso note, combinate con ingegneria sociale”**

[Report Verizon, 2015]

# *Trojan: il mezzo tecnico più utilizzato per la “conquista” di un computer aziendale*



qualsiasi file

Malware

Spyware

Remote Code  
Execution (RCE)

Remote Access  
Trojan (RAT)

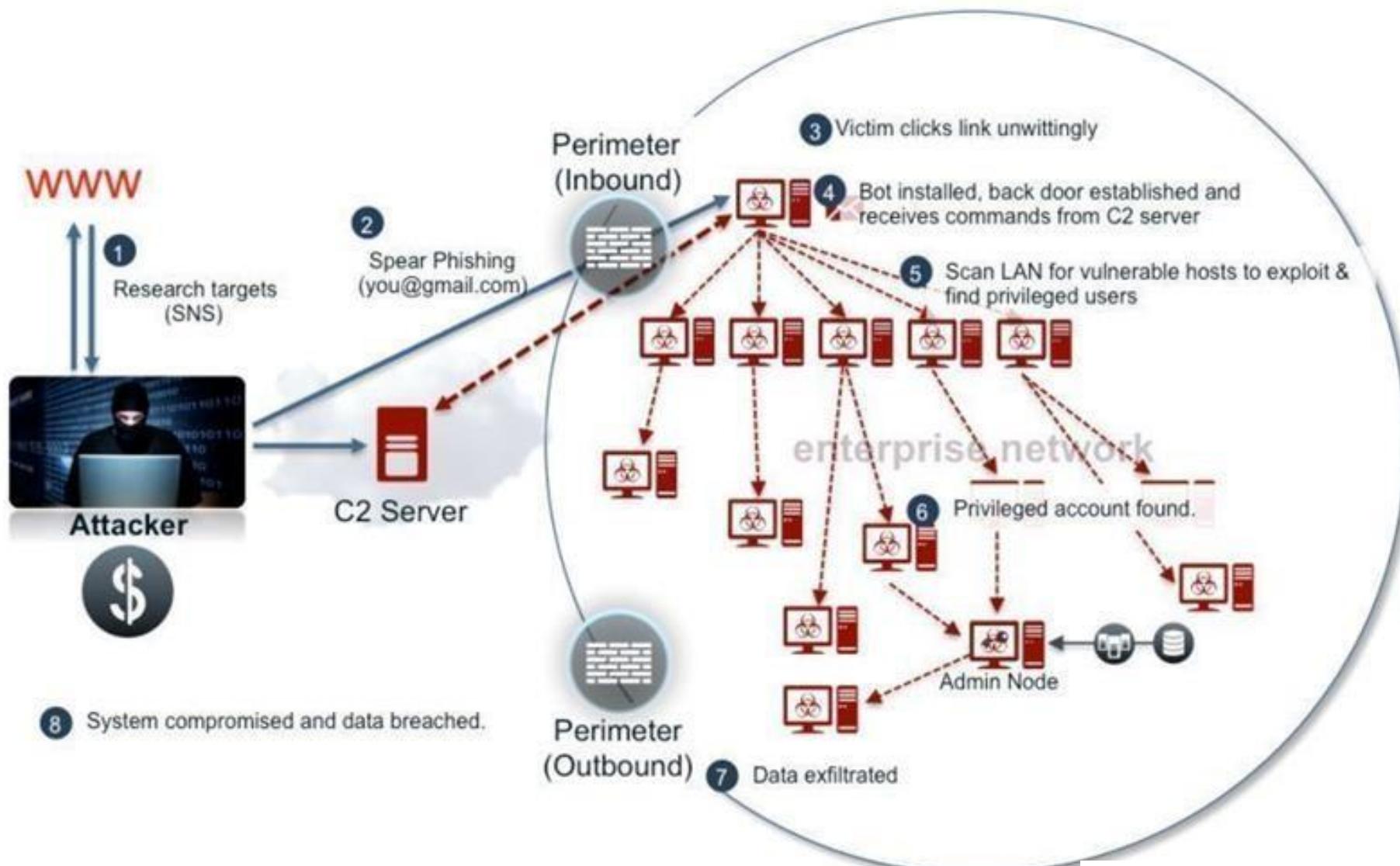


**UNIMORE**

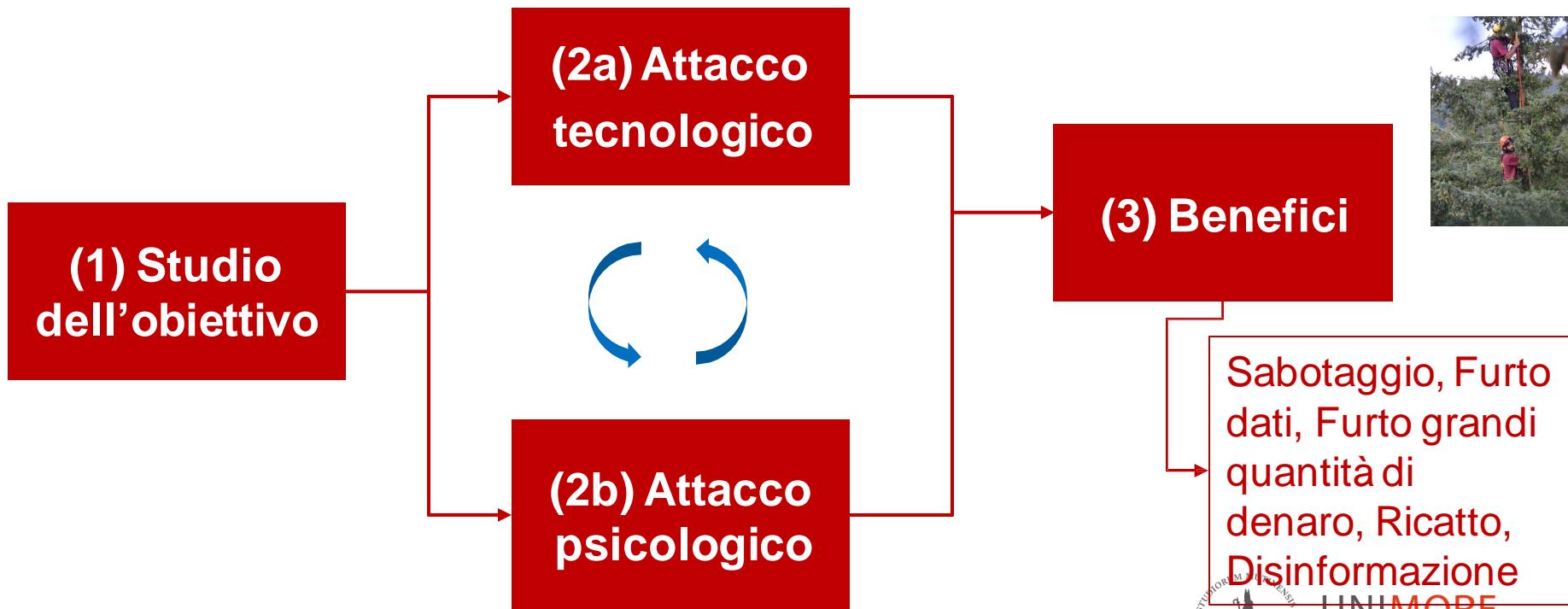
UNIVERSITÀ DEGLI STUDI DI

MODENA E REGGIO EMILIA

# Movimenti laterali all'interno della rete aziendale per arrivare a uno o più target



# Sintesi parte 1: Attacco generalizzato e mirato



# **La peggiore vulnerabilità: Quando gli avversari sono interni**

# I 10 tipi di avversari interni

1. Spie industriali che si introducono in azienda o prendono contatti con persone che sono in azienda
2. Dipendenti di aziende partner
3. Consulenti
4. Dipendenti licenziati, contrattisti non confermati
5. Stagisti temporanei
6. Dipendenti distratti
7. Amministratori di sistema incompetenti
8. Dipendenti insoddisfatti
9. Dipendenti ideologizzati
10. Dipendenti bramosi di guadagno o in difficoltà economica

# Motivazioni

- **Azioni deliberate** per motivi di:
  - delusione e vendetta (non apprezzamenti, mancate promozioni, ...)
  - ricatto
  - bramosia di guadagno
  - danneggiamento (azienda, superiore, pari grado)
  - corruzione
- **Azioni non deliberate:**
  - inesperienza
  - mancata conoscenza delle norme
- **Azioni sottostimate:**
  - scarsa condivisione delle norme aziendali e delle norme in genere (es., privacy)
  - ipotesi di bassa probabilità di essere scoperto
  - scarsa percezione del crimine
  - sfida (tendenze antisociali) e curiosità

# Azioni deliberate: principale motivo?

- Nel 90% degli incidenti investigati, la motivazione principale è stata la **vendetta**
- Nel 62% dei casi, gli attacchi sono stati predeterminati e preparati in anticipo
- Il 57% degli attaccanti si è auto-definito “arrabbiato”
- Nell’80% dei casi, i colpevoli avevano evidenziato comportamento sospetto o negativo ai propri colleghi prima dell’attacco
- Solo il 43% aveva effettivo accesso a livello di super-utente
- Il 64% degli attaccanti ha utilizzato sistemi remoti per portare a termine l’attacco
- La maggior parte degli “incidenti” non ha richiesto un livello di competenza tecnica molto elevato

# *Perché degli elevati rischi interni*

- Ci sono norme per la difesa della privacy del dipendente
- Ci sono “barriere psicologiche” a considerare pericoloso il tuo collega o il tuo dipendente
- “I datori di lavoro ritengono di avere una relazione con i dipendenti basata sulla fiducia e li considerano come il bene aziendale più prezioso. Ma la natura estesa dell’infrastruttura aziendale, unitamente a una base impiegatizia allargata, spesso globale e complessa nella struttura – impiegati, consulenti, partner e collaboratori – rende il rischio interno una delle principali sfide che i manager si trovano a dover affrontare: indipendentemente dal fatto che tale rischio sia intenzionale o meno, c’è. Ed è reale”



# I casi dolosi più famosi



**Interno  
non tecnico**



**Dipendente  
azienda**



**Contractor  
esperto**  
*(addirittura con diritti di  
amministratore di sistema)*



**UNIMORE**  
UNIVERSITÀ DEGLI STUDI DI  
MODENA E REGGIO EMILIA

# Gli Stati entrano nel cyberspace

# Cyber and Information Warfare

- 1) Progettare, costruire, configurare, rendere sicure e operative i sistemi e le reti di comunicazioni in modo da garantire la disponibilità, integrità e confidenzialità dei dati e l'autenticazione degli utenti e delle risorse
- 2) Sviluppare capacità attiva e passiva cyber per proteggere i dati, le reti, le operazioni e ogni altro sistema e servizio informatico
- 3) Stabilire il controllo sulle risorse informatiche e informative, e sulle reti e sistemi di comunicazione degli stati avversari
- 4) Sviluppare *cyber and information weapon* per il sabotaggio di reti di computer, applicazioni software e servizi degli avversari
- 5) Utilizzare Cyber+Electronic Warfare per acquisire informazioni ed eventualmente modificare i dati trasmessi
- 6) PSYOP - Sviluppare sistemi di pressione psicologica sull'avversario (inclusa disinformazione, negazione e inganno utilizzando tutti i media inclusi i social network)



# Due dichiarazioni a confronto

“State and non-state actors use digital technologies to achieve economic, industrial and military advantage, foment social instability, increase control over content in cyberspace, and achieve other strategic goals - ***often faster than our ability to understand the security implications and mitigate potential risks.***



Their cyber activities present both counterintelligence and security threats”

«A prova dell'elevato rischio che sta correndo il Paese sulle ricerche per il vaccino anti-Covid, a luglio 2020 il leader repubblicano alla Camera, **Kevin McCarthy**, ha presentato un disegno di legge per  fermare e sanzionare i cyber criminali stranieri che tentano di sottrarre informazioni riservate in questo settore»



# Gli attori del gioco cyber duro

Cyber criminali “seri”

Stati



Aziende specializzate

State-related actor



**UNIMORE**  
UNIVERSITÀ DEGLI STUDI DI  
MODENA E REGGIO EMILIA

# ***State-related actors***

***Contractor, Apparati della difesa, Apparati Intelligence, Gruppi para-statali, APT, Aziende specializzate:***

- Sono molto competenti: leggono, studiano e si aggiornano sui nuovi metodi di attacco e di difesa
- Dispongono di budget elevati e di strumenti sofisticati
- Sono pagati per raggiungere un obiettivo: non si fermano davanti a ostacoli tecnologici e umani ⑦ E' questione di tempo
- Sono persone sospettose: cambiano luoghi e strumenti, sanno che ci sono “cyber defenser” e tentativi di infiltrazioni
- Sfruttano tutti i vantaggi possibili: anonimato, distanza, server intermedi, mobilità, scambi informativi, cooperazione
- Sono persone fantasiose in grado di adattare continuamente gli attacchi e i sistemi di anonimizzazione alle nuove difese

# APT: definizione NIST SP 800-39

*“APT is an adversary that possesses sophisticated levels of expertise ...*

*Their objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of*

- *exfiltrating information,*
- *undermining or **impeding critical aspects of a mission, program, or organization,***
- *or positioning itself to carry out these objectives in the future.”*

[https://docs.google.com/spreadsheets/d/1H9\\_xaxQHpWaa4O\\_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=1864660085](https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=1864660085)

# Il “mercato” dei dati

# Il modello di business del Web

- L'utente paga l'oggetto (PC, tablet, smartphone) per usufruire del servizio
- L'utente non paga per il servizio →
  - In realtà, paga mediante una (consapevole o inconsapevole) cessione dei propri dati che vengono utilizzati direttamente e/o rivenduti a pro della pubblicità personalizzata



Nonostante l'attenzione mediatica degli ultimi anni, pochi sono informati (e ancor meno preoccupati) sulle tecniche utilizzate per influenzare le opinioni commerciali e politiche sfruttando i dati che i cittadini stessi seminano e che sono facilmente recuperabili da tanti



Genere, Cittadinanza, Etnia, Lingua, Emigrazione

Livello di studio, Posizioni di lavoro, Tipologia di azienda

Proprietà di auto, moto, biciclette, Intenzioni di acquisto

Residenza, Casa di proprietà, Altre case

Genitori, Madri e tipologie

Relazioni e tipi di relazioni

Posizioni, Viaggi di lavoro, Vacanze

Reddito, Ricchezza, Propensione alla spesa e al debito

Orientamenti religiosi, politici, sessuali

Dati sanitari

Dati genetici

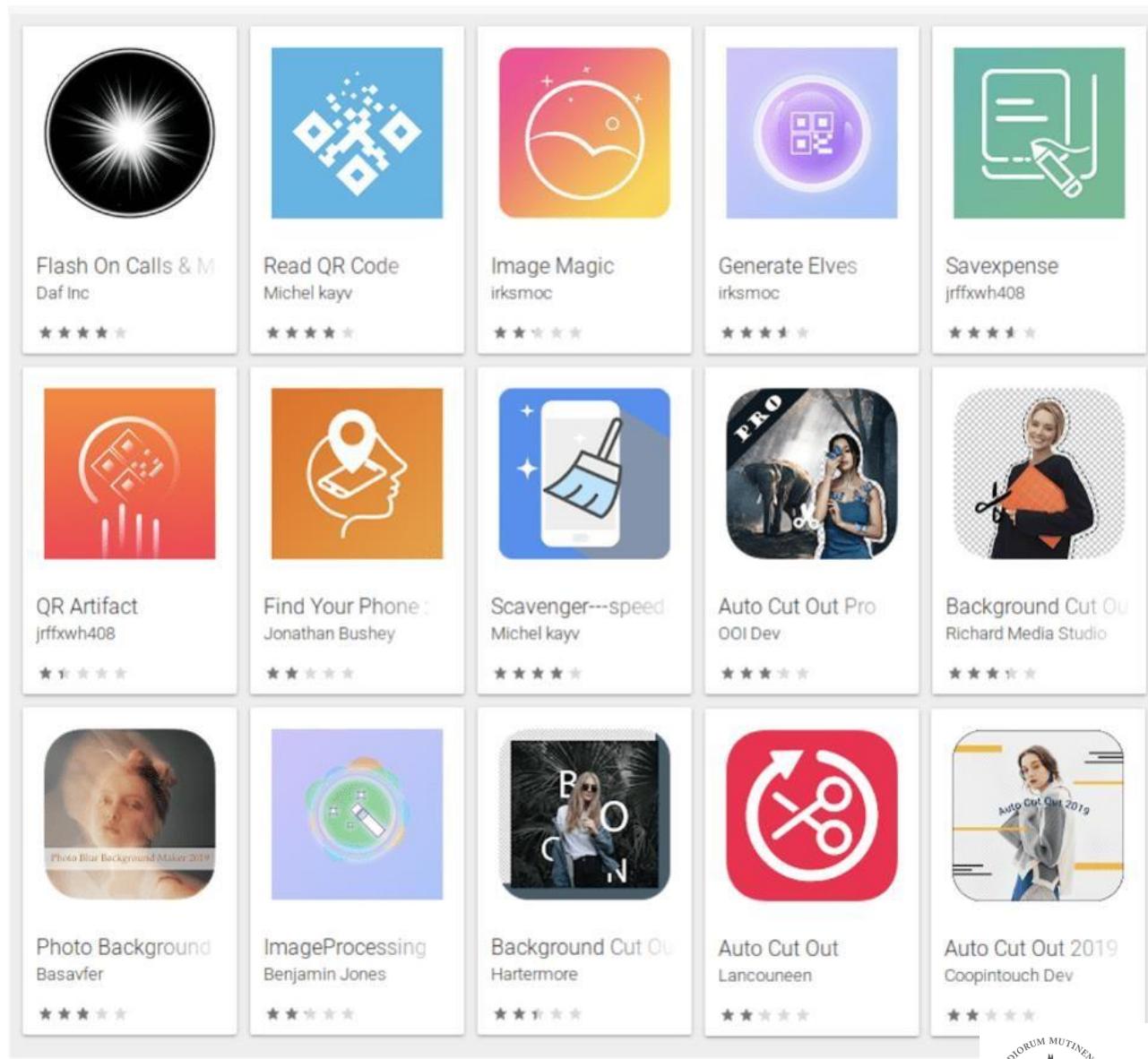
Mente

98 personal data points



Micro-targeting  
UNIMORE  
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

# App progettate per “acquisire dati”



# App mediche che “profilano”



# Elaborazione dati – Vendita e Utilizzo (profitto)



# **Domanda 1: *Stimare mercato***

# **Data broker:** Acxiom, Epsilon, Experian e altri 5000

## Esempio: **Experian**

- “Our US database has access to the freshest data from more than 300 million individuals and 126 million households, more than 50 years of historical information, thousands of attributes to reveal demographics, purchasing habits, lifestyles, interests and attitudes”
- “Using that data, we can address 85% of the US, link to 500 million email addresses and segment individuals into 71 unique types according to categories like financial personality and ethnic insight”
- “We can help companies reach the right audiences with the best messages”



# Clienti *insospettabili*(?)

- Dipartimento di Stato americano
- Governi
- Eventi sportivi
- Pepsi
- Mercedes-Benz
- Tanti musicisti (es., Puff Daddy, 50 Cents)
- ...

# La “disinformazione” non è mai fine a se stessa



**Promuovere idee sociali,  
commerciali, politiche**



**Danneggiare idee,  
reputazione, brand**

# Da “fake news” a “alternative facts”



# **Informatica e Web, nate con obiettivi pro libertà, sono in realtà *dual use***

- 1) Tecnologie per la libertà di informazione** ← Non potendo la censura, il Web viene inondato da tante *distrazioni* e da *fake news* (tenendo conto che l'attenzione e il tempo degli utenti sono limitati, il meccanismo sta funzionando)
- 2) Tecnologie per il controllo sociale**



## Singapore: un modello di vita basato sulla tecno-etica

*Attenzione: ai cittadini piace!*

«Le persone sono soddisfatte della situazione, che assicura sicurezza, ordine, pulizia, e attrae investitori e benessere»

«A Singapore si respira un senso di armonia sociale di cui i cittadini sembrano essere orgogliosi»



# Sistema di credito sociale

<https://logicmag.io/china/the-messy-truth-about-social-credit/>

