UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Corso di “Sicurezza informatica”
Laurea Magistrale in Ingegneria Informatica
A.A. 2023/2024

“Vulnerabilità, Crimini e Criminali”

Prof. Mirco Marchetti

Università di Modena e Reggio Emilia

Crimini ad alta tecnologia in aumento

- High Tech Crime
- Cybercrime
- Computer crime
- Crimine informatico
- Internet crime
- Web crime
- Digital crime
- …

Tutte definizioni che rappresentano i crimini perpetrati mediante l'impiego di di sistemi elettronici, che oggi utilizzano principalmente <u>tecnologie digitali</u>

Altro esempio: *Spamming*

- Perché esiste ancora lo spamming?
- Chi può credere e anticipare soldi per una mail che:
  - ti annuncia di aver vinto 100.000€ ad una lotteria a cui non hai mai partecipato?
  - ti “regala” il 10% di 10M di dollari per far transitare i soldi del solito figlio perseguitato di qualche dittatore africano?
- Eppure “allo spammer basta che lo 0,0001% dei milioni dei destinatari delle loro e-mail risponda positivamente per arrivare a guadagnare dai 7.500 ai 12.500 dollari al giorno!”

Vari crimini penali: pedopornografia, furti di identità, ricatti, spionaggio industriale, …

- "1 out of 5 children received a sexual solicitation or approach over the Internet in a one-year period of time"
- "California warns of **massive ID theft**: Personal data stolen from computers at University of California, Berkeley"
- Possono cercare di rubare i numeri delle carte di credito, del conto Paypal, di eBay, dei dati dell'online banking
- Ma anche i dati di accesso ai giochi online. Esempi (veri):
  - possono rubare le "spade magiche" e poi ricattare per restituirle
  - possono usare un'utenza di poker online per saccheggiare tutti i soldi di quel conto
- Numerosi casi eclatanti di aziende colpite a scopo di:
  - truffe, estorsione
  - furto di brevetti/idee
  - furto di informazioni commerciali rivendute a loro concorrenti

In sintesi

1. Le tecnologie digitali possono essere obiettivo del crimine
2. Le tecnologie digitali possono essere utilizzate come strumento del crimine
3. Le tecnologie digitali possono essere utilizzate come testimoni del crimine

Le 3 possibilità non sono mutuamente esclusive

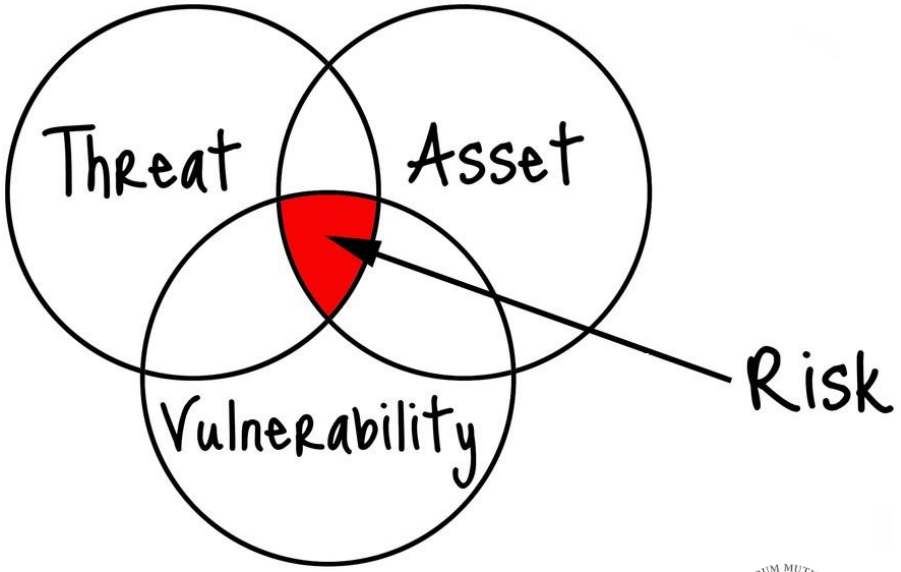
Dove sono le colpe?

- Molti (impropriamente) accusano l'infrastruttura e le tecnologie che si utilizzano in Internet
- Ironicamente, **Internet è stata progettata per promuovere il massimo scambio (non ristretto) di informazioni accademiche e scientifiche**

- L'errore non è nel progetto, ma nell'avere cambiato gli obiettivi e l'uso: Internet è diventata un sistema di interconnessione e di comunicazione globale dove vengono trasmessi anche dati sensibili e riservati
- Inoltre, le tecnologie Web hanno reso estremamente facile l'utilizzo dei servizi Internet a una platea (>2 miliardi) di non esperti

Rischio

E’ la probabilità che una determinata **minaccia** ha di sfruttare la **vulnerabilità** di una risorsa (*asset*) e quindi di causare **impatti indesiderati**



Vulnerabilità tecnologiche (1)

Evoluzione dei sistemi informatici

Prima

- Sistemi informatici (CED) non collegati a reti esterne
- Mainframe centrale e terminali “stupidi” (solo video/tastiera)
- Connessioni dedicate, sempre wired e non condivise

Oggi

- Miliardi di sistemi collegati a Internet
- Data center con server distribuiti su reti LAN e WAN
- Terminali intelligenti (PC ma anche smartphone)
- Reti non dedicate
- Trasmissioni digitali di voce e qualunque tipo di dati
- Reti wireless

Vulnerabilità tecnologiche (2)

Evoluzione delle applicazioni e servizi informatici

Prima

- Poche applicazioni informatiche indispensabili per il funzionamento complessivo dell'organizzazione
- Poche informazioni digitalizzate e memorizzate in database
- Pochi dipendenti autorizzati ad accedere alle informazioni digitali
- Poche applicazioni (forse nessuna) con vincoli di interattività e di disponibilità determinanti per il successo dell'organizzazione

Oggi

- Applicazioni informatiche diffuse
- Tutte, ma proprio tutte, le informazioni (anche) in formato digitale
- Molteplici applicazioni devono essere sempre attive, almeno nelle ore di ufficio, e molte operazioni avvengono di notte non presidiate

Vulnerabilità tecnologiche (3)

Sistemi informatici sempre più complessi, eterogenei ed integrati

- Architetture multi-piattaforma
- Necessità di cooperazione: tra livelli e piattaforme, tra servizi e applicazioni: gestionali, servizi di rete, progettazione, produzione, …
- Numero di utenti crescente e non necessariamente con competenze informatiche: dipendenti, clienti, fornitori, personale amministrativo, …
- A causa dell'integrazione dei sistemi informatici, danni provocati da un utente potrebbero ripercuotersi su gran parte dell'organizzazione

Altra vulnerabilità: complessità

Evoluzione dei sistemi informatici sempre più complessi da proteggere in quanto coinvolgono competenze differenziate che non sono facilmente conciliabili

- **Discipline informatiche**:
  - sistemi di autenticazione
  - sistemi di protezione logica
  - reti
  - protocolli di crittografia, …
- **Discipline giuridiche:**
  - normative sulla privacy
  - legislazione vigente in continua evoluzione, …
- **Altre discipline:**
  - psicologia
  - sicurezza fisica degli ambienti, Antincendio, videosorveglianza, …
  - organizzazione aziendale

Ma anche vulnerabilità dovute a …

SVILUPPATORI SOFTWARE

- Il software contiene molti bug
- Non vi è educazione allo sviluppo di software sicuro

SISTEMISTI

- I sistemi operativi ed applicazioni non vengono aggiornati né patchati con regolarità
- L'autenticazione della maggior parte dei servizi è debole

MANAGEMENT

- Mancanza di sensibilità adeguata sui problemi relativi alla sicurezza
- Problemi di budget

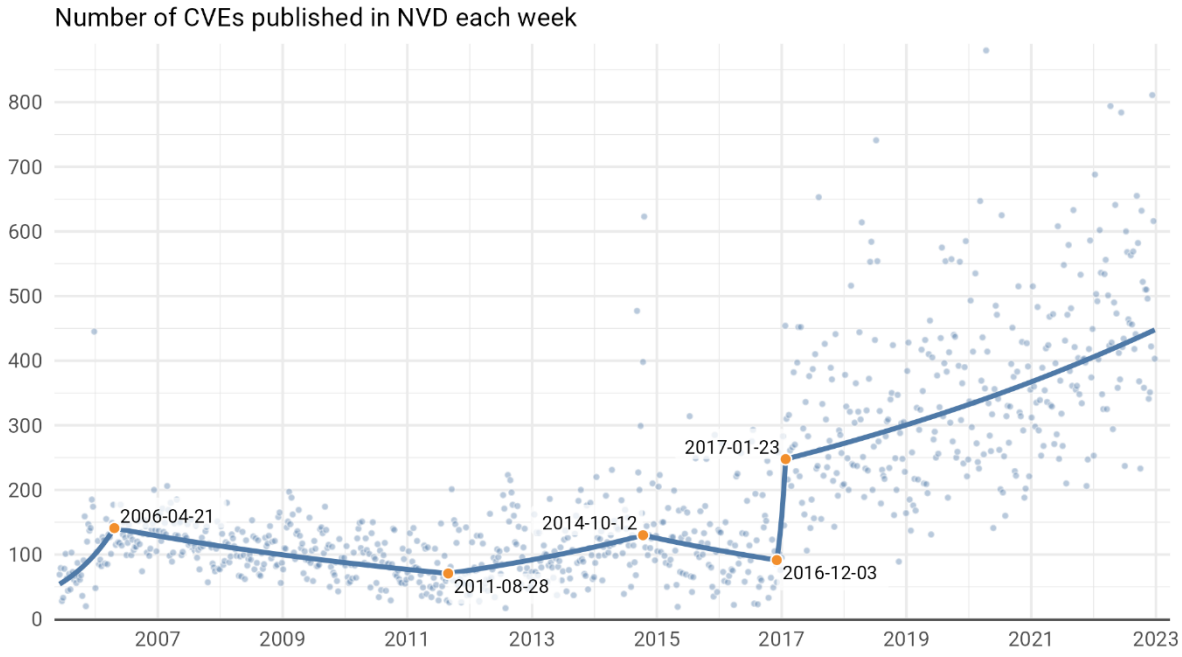
PERSONALE

- Mancanza di cultura e sensibilità adeguata (post-it, scelta password, gestione attachment di email, …) – rischi di *social engineering*

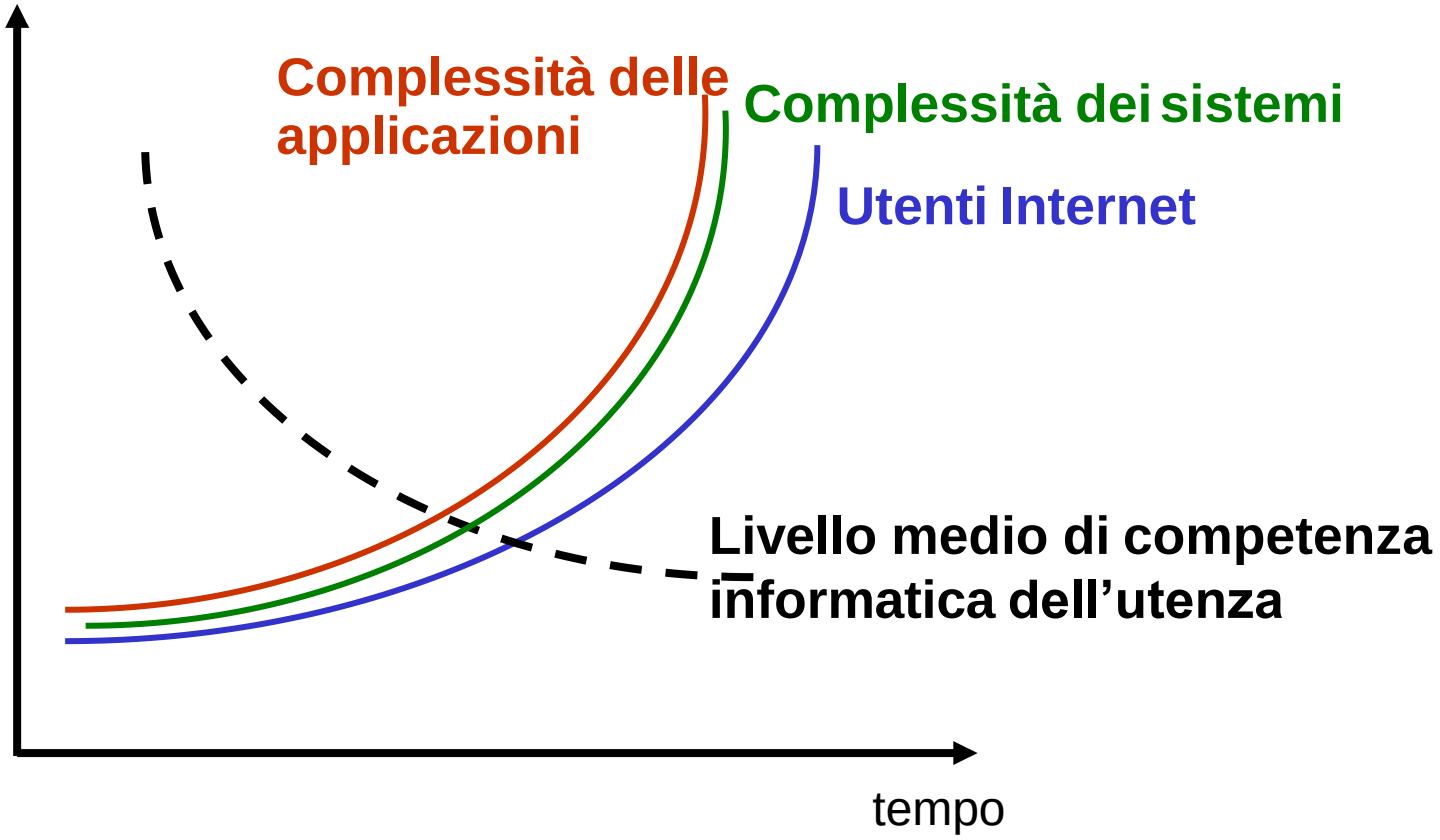
La vulnerabilità indotta dal time-to-market

Bug del software

I software presenti sul mercato, a causa di necessità di marketing, sono sempre poco testati. Questo fa in modo che i sistemi operativi e le applicazioni siano vulnerabili a particolari tipi di attacchi.



Evoluzione delle vulnerabilità



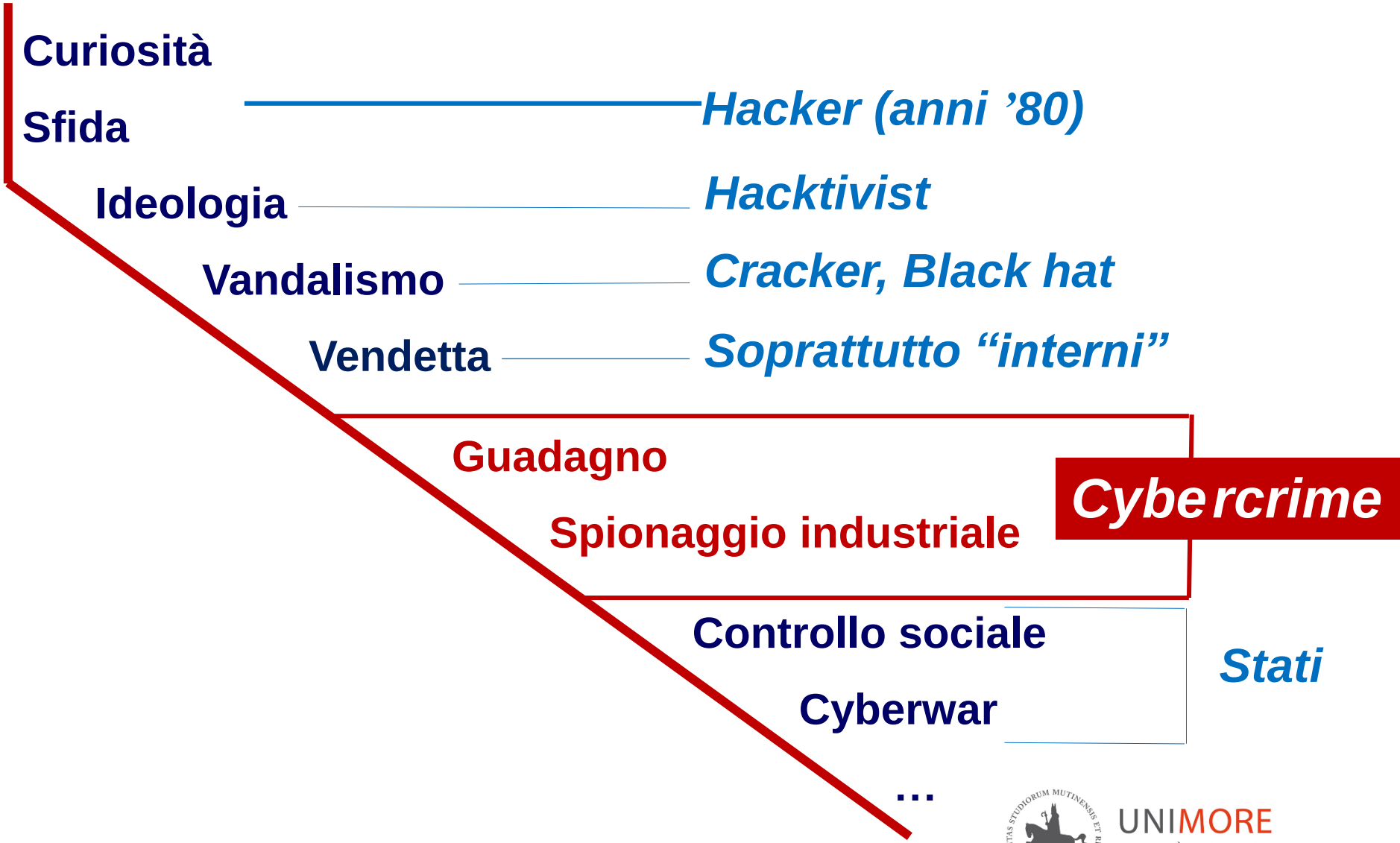
Attaccanti

Condividere il significato dei termini

- **HACKER (?)**
- **CRACKER**
- **LAMER**
- **BLACK HAT**
- **WHITE HAT**

Nell'ambito del corso si userà il termine ATTACKER o AVVERSARI. HACKER è un complimento da meritare

Il mondo degli attacchi è molto esteso e in continua evoluzione



Evoluzione degli “attacker”

- **Anni 70’: *nasce la cultura hacker***
  - Inoffensiva nella maggior parte dei casi
  - Raramente malintenzionata
- **Anni ’80: *si diffonde la cultura hacker***
- **Anni ’90: *Internet vandals***
  - Prevalentemente giovanile
  - Spesso malintenzionata, ma non per denaro
    - Intrusioni nei sistemi, Diffusione virus, Denial-of-Service
- **Anni 2000: *nascono i professionisti del cybercrime***
  - “I giovani sono cresciuti: questo è il loro lavoro”
  - La motivazione è essenzialmente economica
    - **SPAM**, nato come strategia di Web marketing, oggi nasconde: frodi (es., 419 advance fee fraud), phishing, diffusione di malware, ecc.
    - **Brand impersonification**: la tattica più comune per acquisire informazioni personali (credenziali di accesso, identità, altri dati)
- **Presente/futuro: cybercrime, *cyberwar*, *cyberterrorism***

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Motivazioni degli attacker “old style”

- Principî hacker
- Sfida, anche se …
  - Pochi attacker individuano e sfruttano vulnerabilità precedentemente sconosciute
  - La stragrande maggioranza degli attacker ripete attacchi noti e documentati
- Fama all’interno di “circoli”
- Soggetti dediti ad ideare codici in grado di infettare le risorse presenti nella Rete

Motivazioni degli attacker “moderni”

- Guadagno personale
- Assunti dalla criminalità organizzata (*Mafia boys*)
- Spionaggio industriale e statale
- Ideologia
  - Hactivism (Hacking+Activism)
  - Cyberterrorismo
- Squilibrio mentale / Stupidità

E non dimenticare: l'attacker interno

- Il pericolosissimo **attacker interno**, con varie possibili motivazioni:
  - frustrazioni lavorative
  - licenziamenti ritenuti ingiusti
  - ambizioni di carriera frustrate
  - corruzione
  - ricatto
  - difficoltà finanziarie (strozzini collegati alla cybermafia)
  - …
- I dipendenti hanno molte informazioni che un esterno non conosce e spesso trovano le porte (quelle fisiche) aperte!

Tipiche azioni riscontrate in università

- Usare l'identità elettronica di altri
- Non rispettare le regole di sicurezza di accesso
- Scaricare e installare software proprietario senza licenza
- Scaricare file (musica, video, libri) protetti da diritto di autore

- Più rare, ma ci sono state anche azioni del seguente tipo:
  - Installazione di spyware, rootkit nei computer delle biblioteche
  - Archivi di materiale pornografico

Tipiche scuse

- “Non sapevo cosa stavo facendo”
- “Non sapevo che fosse sbagliato/proibito”
- “Non stavo pensando”
- “Avendo potuto farlo, pensavo che fosse lecito”
- “Avendo potuto accedere, l’ho usato”
- “Non ho fatto niente di grave. Perché siete così arrabbiati per questo fatto?”

➔ **“Ignorantia legis…”: non conoscere le regole interne e la legge non può essere accettata come difesa**

Chi sono gli *avversari*?

Professionisti

- Criminali

- Gruppi specializzati statali e para-statali
- Contractor
- Aziende “Big brother”

Patologici

- Predatori
- Conoscenti
- Ex

Ideologizzati

- Hacktivist
- Terroristi
- Antagonisti

Persone normali

- Talvolta, noi stessi …
- Dipendenti interni

Motivazione dei professionisti
→ soldi

Negli anni ’50 al rapinatore di banche Willie Sutton fu chiesto perché rapinava banche.

Risposta: **“That’s where the most money is.”**

Oggi, molti soldi si trovano in Internet e Web
Così come quasi tutte le informazioni che possono essere trasformate in soldi

→**ATTACCHI:** truffe, ricatti, riciclaggio di denaro, furti di denaro e informazioni, …

Notizie

- La **buona notizia**: c'è una piccola minoranza di criminali tra i miliardi di utenti Internet

- La **cattiva notizia**:
  - un ladro di automobili può rubare solo un'auto alla volta
  - un singolo criminale da un solo computer può causare danni a un numero elevatissimo di reti e di computer sfruttando "aiutanti software"

Opportunità per gli attacker

- Per violare una cassaforte, un ladro deve superare molte barriere fisiche, allarmi e deve sapere come violare una cassaforte

- Per violare un computer, nella maggior parte dei casi, non ci sono barriere fisiche (i computer sono già connessi), e ci sono poche barriere logiche
- Molti attacker non devono essere “maghi” del computer, ma devono sapere dove scaricare qualche programma scritto da altri che conoscono bene i computer
  - ogni mese vengono “pubblicati” oltre 50 strumenti di attacco (nuovi o perfezionamenti delle versioni precedenti)
  - Ogni giorno vengono prodotti circa 300.000 malware nuovi

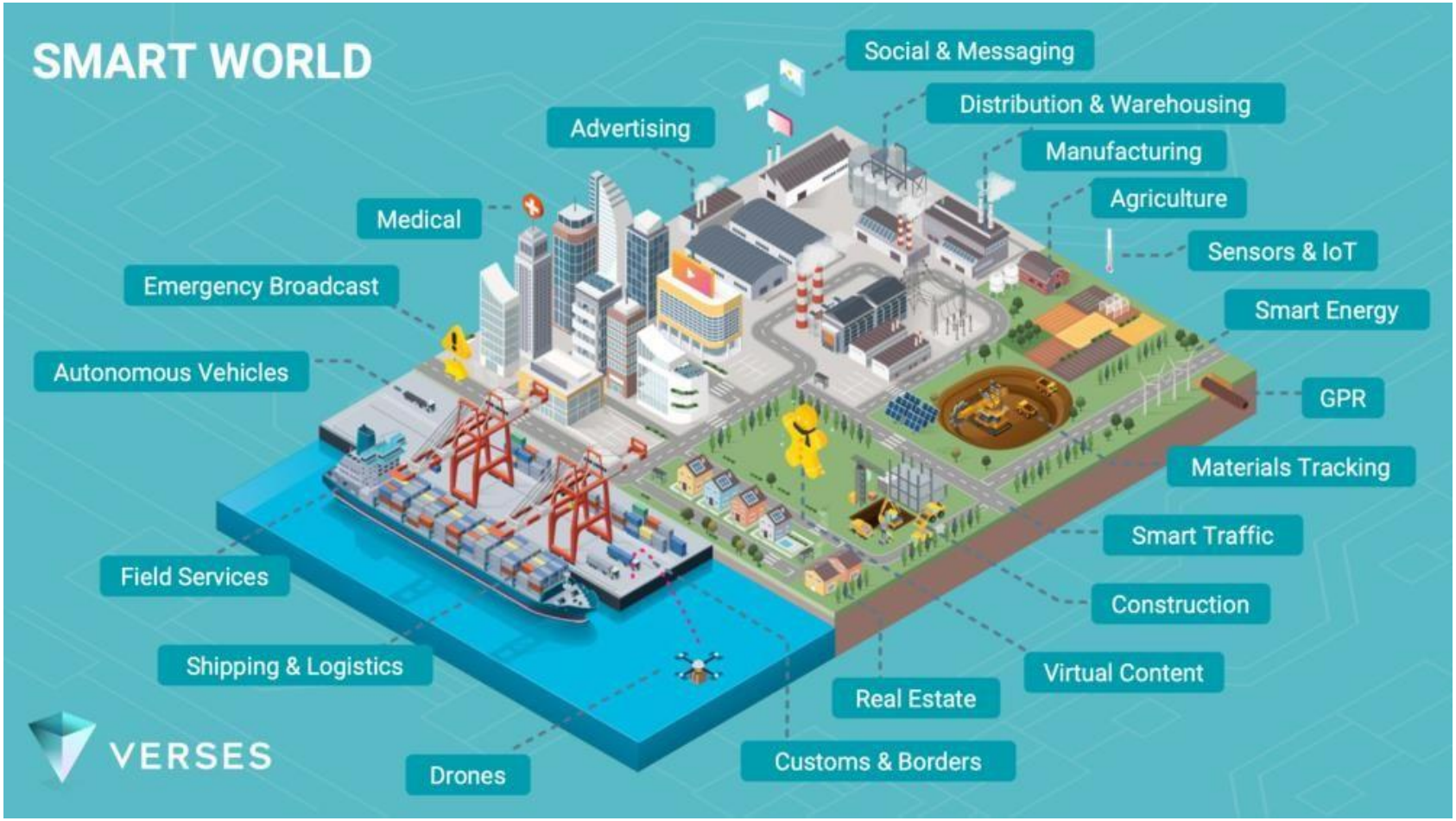
Tempi di “sopravvivenza”

- Un computer non protetto collegato ad Internet subisce tentativi di attacco mediamente:
  - entro 55 minuti nel 2003
  - entro 16 minuti nel 2004
  - entro 4 minuti nel 2007
  - … poi hanno smesso di fare simili studi …
- Nostri studi (datati) hanno rilevato:
  - una media di un attacco al minuto su un PC domestico con sistema operativo Windows collegato a una delle più diffuse linee ADSL
  - in una settimana, sono state raccolte circa 379 tipologie di attacchi diversi (non 379 attacchi, ma 379 tipi di attacchi!)

Gli 8 modi prevalenti per attaccarvi

1. **Applicativi non aggiornati**
2. **Sistemi operativi obsoleti**
3. **Malware** preso tramite allegati di posta e siti Web infetti
4. **Password banali**, di default, non aggiornate, usate per servizi diversi e di diversa importanza
5. **Phishing** (con agganci tramite email e social network)
6. **Uso di computer condivisi** in hotel, aeroporti, …
7. **Uso di Wi-Fi aperte**

Ma la situazione peggiorerà …



… quindi ben vengano i “difensori”