



TINEXTA GROUP

NATIONAL  
SECURITY HUB

# Cybersecurity per National Security Hub

**Marco Ramilli**

---

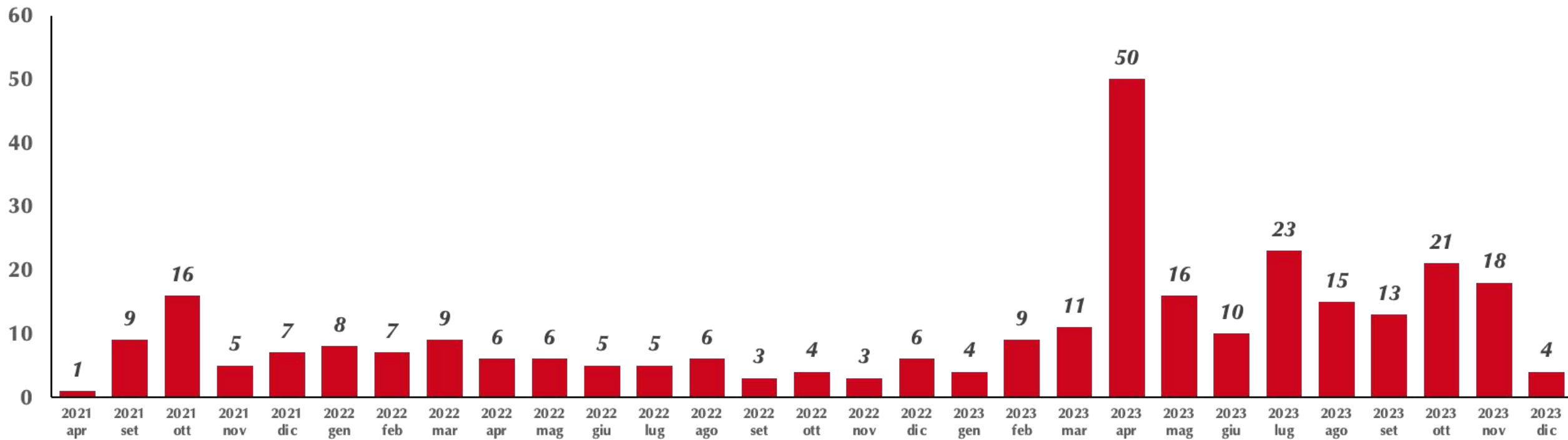
cyber trend  
*-Italia-*

---

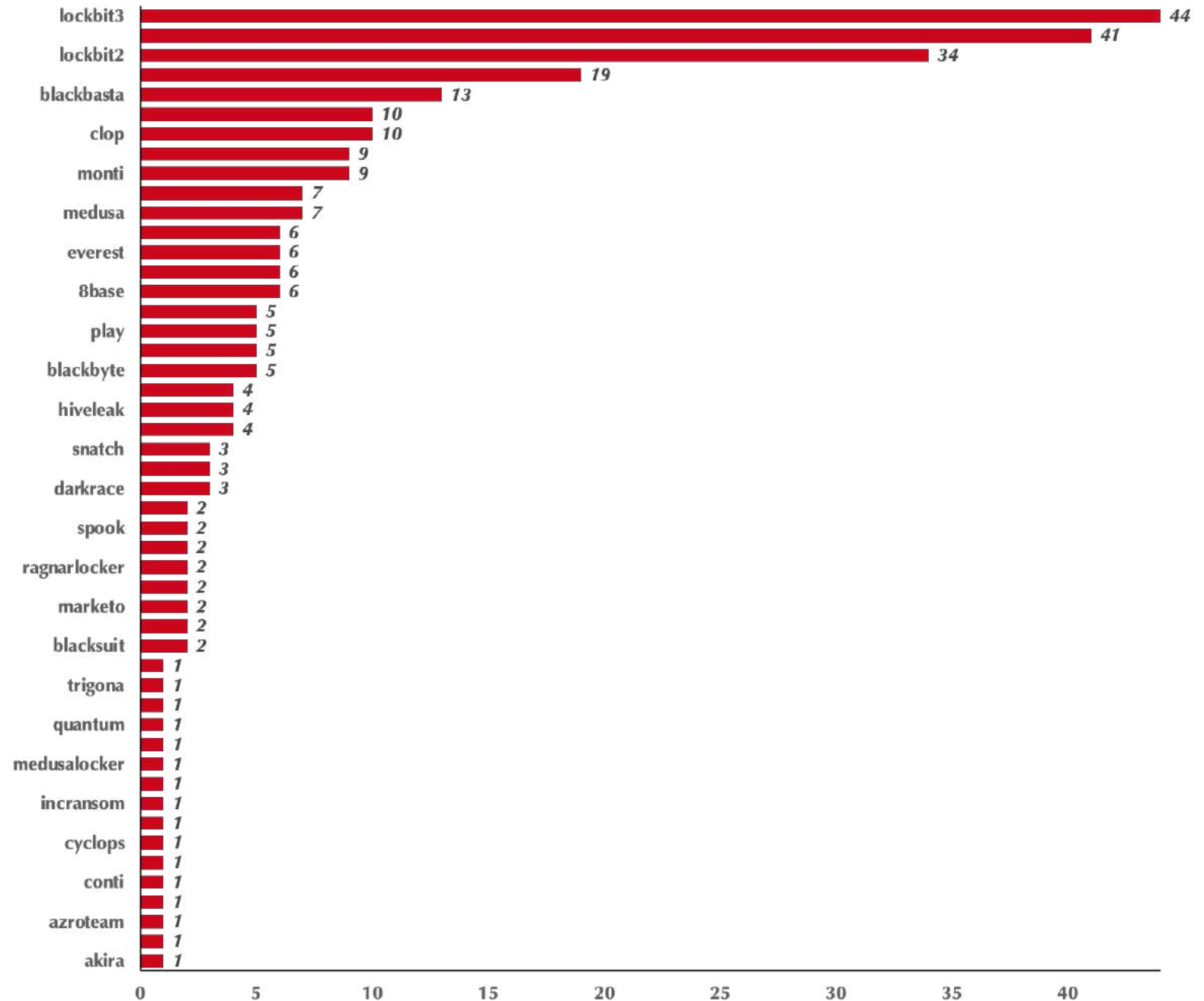


# Il 2023 ha segnato una crescita degli attacchi ransomware in Italia

## Timeline attacchi ransomware da Aprile 2021 ad oggi

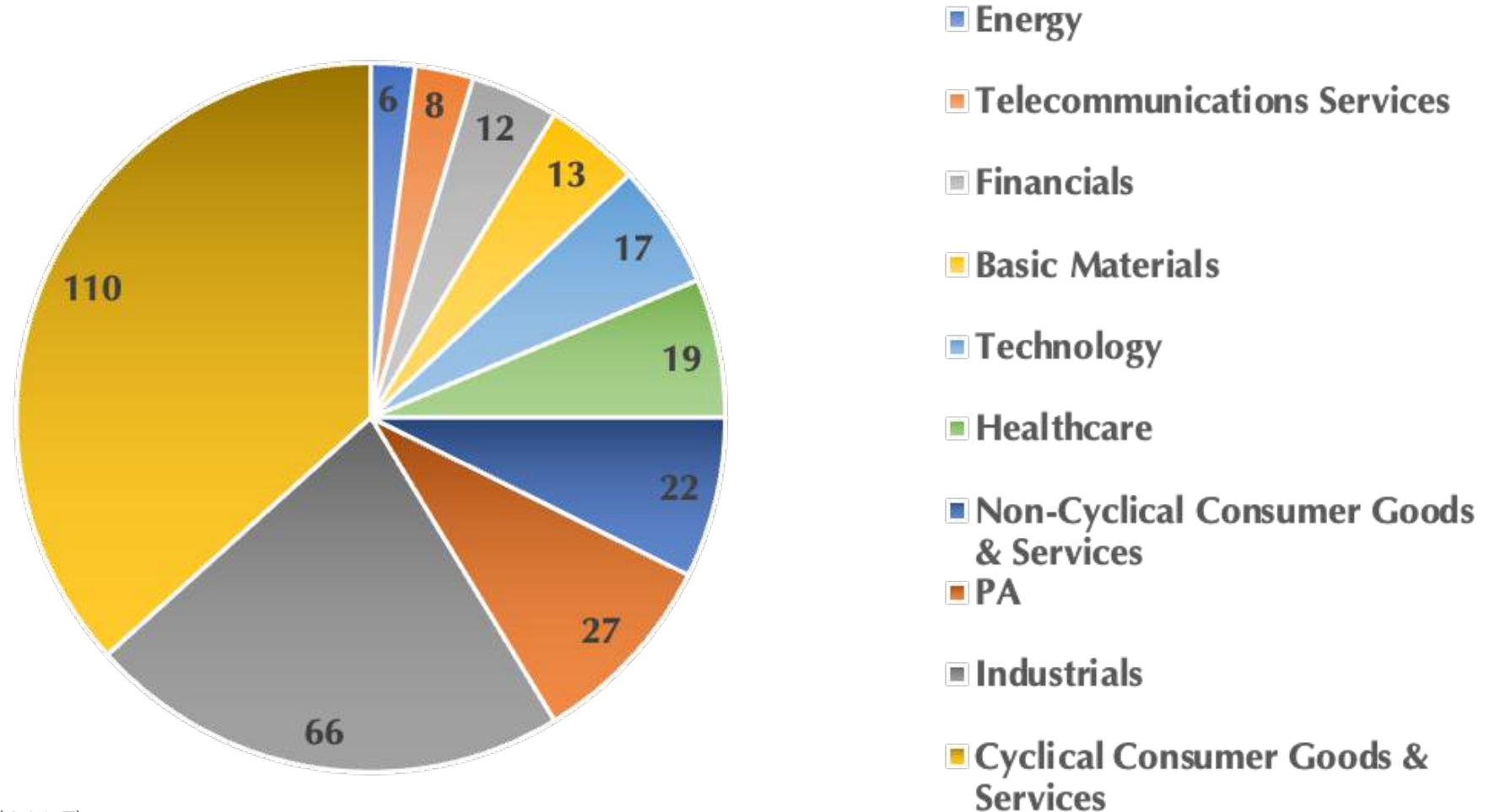


# Le principali gang responsabili degli attacchi degli ultimi 2 anni in Italia



# I principali business colpiti negli ultimi 2 anni in Italia (secondo la classificazione Thomson Reuters)

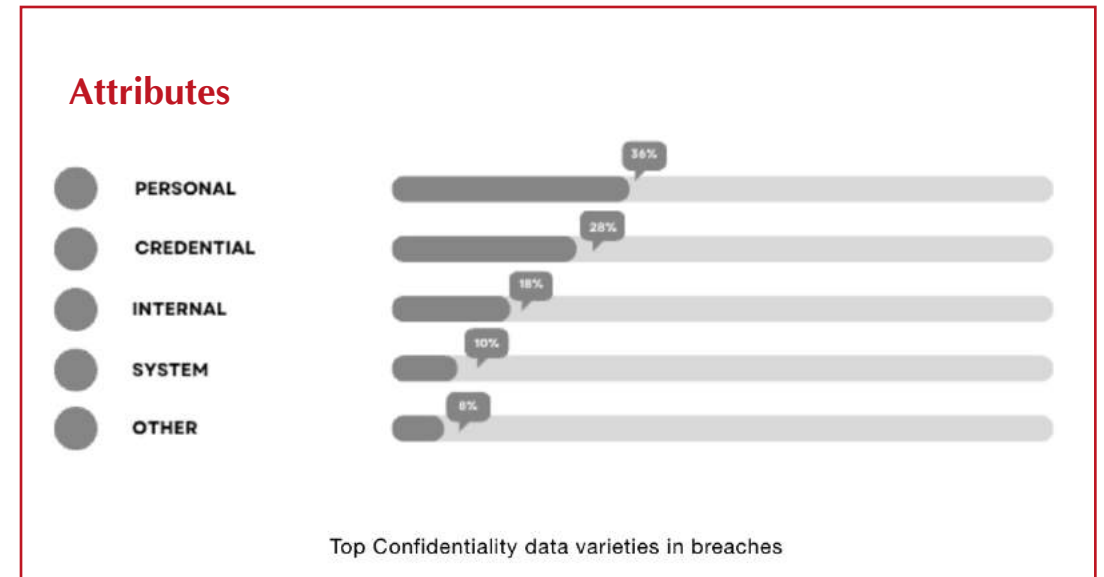
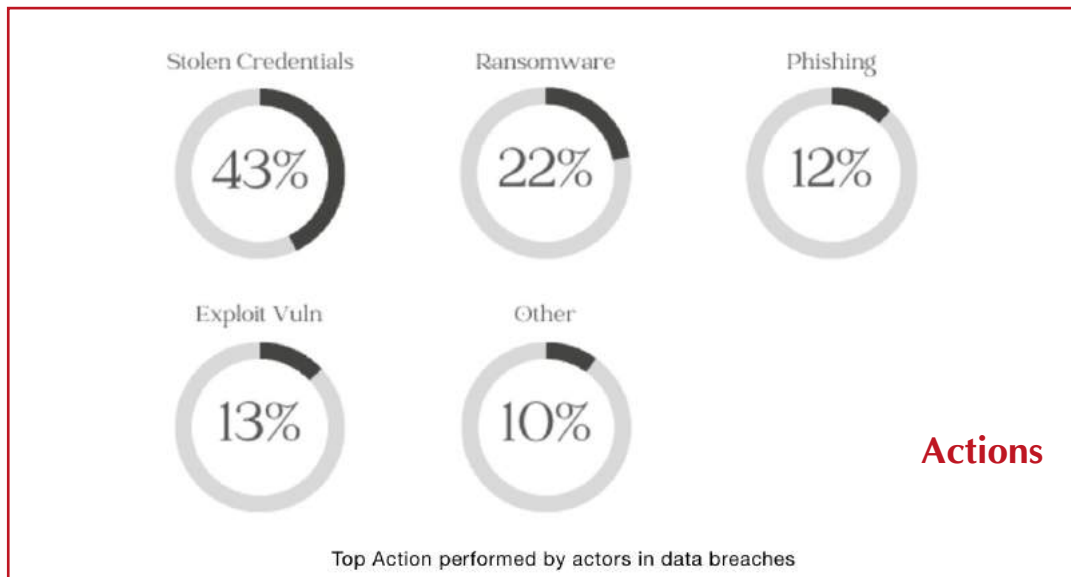
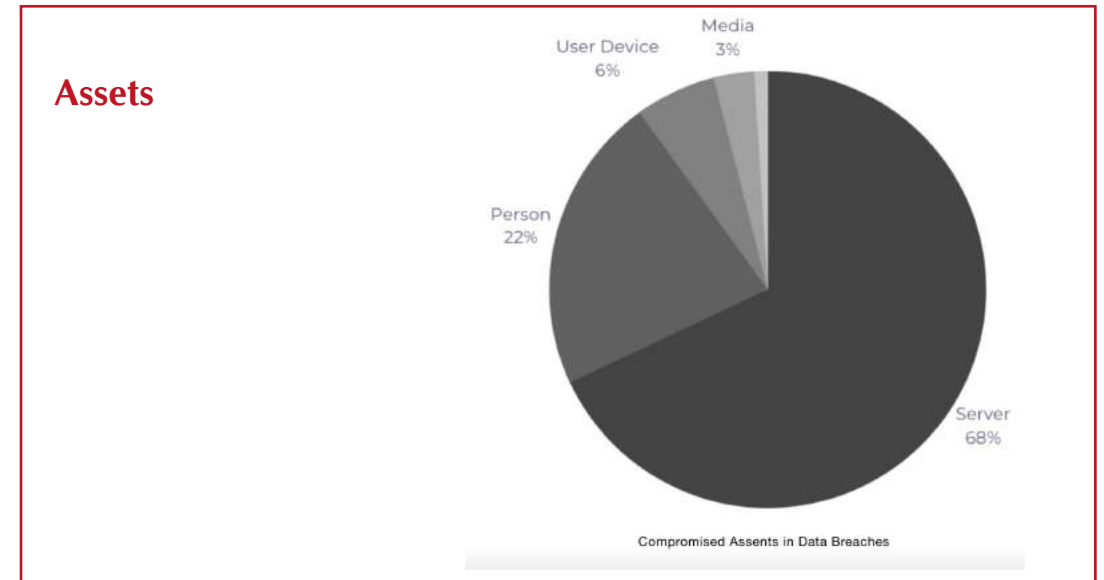
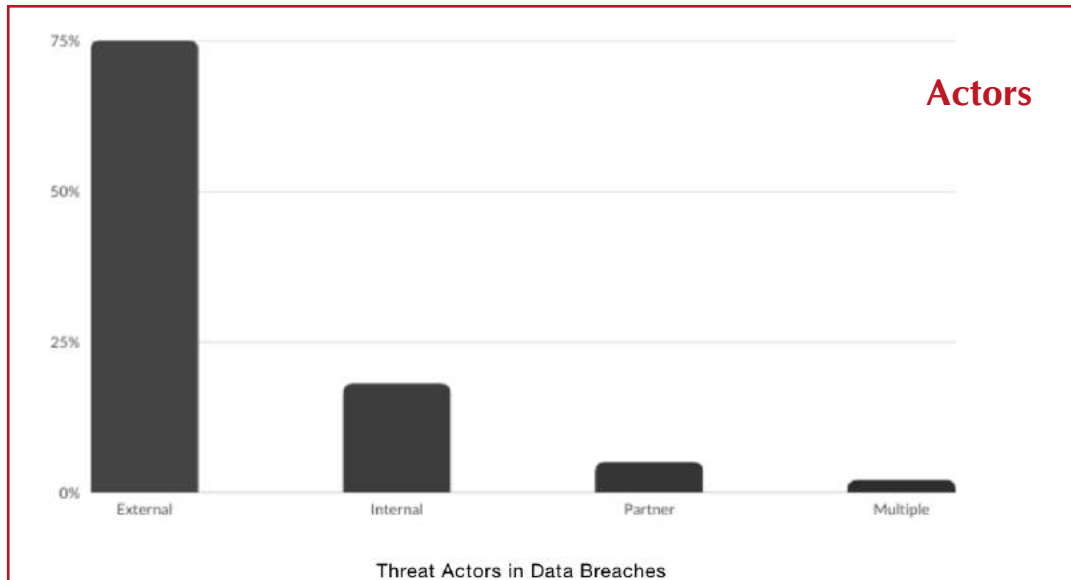
## Attacchi ransomware per business da Aprile 2021 ad oggi



Fonte: dati YOROI (OSINT)

# 2023 Breaches and Incidents

Fonte: <https://marcoramilli.com/2023/06/22/2023-breaches-and-incidents-personal-notes/>



---

la guerra e i threat actors

---



# I raggruppamenti dei threat actors nelle guerre di oggi

- La guerra tra Israele e Hamas è una guerra contemporanea, una **guerra ibrida**, in cui si mescolano diverse strategie e tattiche su piani diversi, seguendo la dinamica del conflitto russo-ucraino.
- Da una parte, Israele, noto come la “Start-up Nation,” un Paese che ha fatto della tecnologia il suo punto di forza; dall’altra, Hamas, un attore non statale ma soprattutto analogico.
- La **dimensione cyber** solleva la guerra dai limiti dello spazio dando la possibilità a chiunque disponga di un computer di prendervi parte.
- Ad oggi, si contano circa **120 gruppi hacker** che forniscono supporto a una delle parti coinvolte, con un numero nettamente più elevato a favore di Hamas (100 circa contro 20); e 4 gruppi neutrali, alcuni dei quali con collegamenti al collettivo “Anonymous”, partecipano al conflitto senza prendere parte a uno o l’altro fronte



*Circa 100 threat actors, molti filorussi (Anonymous Sudan, AnonGhost, killnet, Storm-1133, etc.)*



*Circa 20 threat actors, (Indian Cyber Force, SilenOne, Garuna Ops, Team UCC Ops, etc.)*



---

# il ruolo duale dell'IA nel mondo cyber

---



# L'IA viene utilizzata dai criminali informatici per realizzare attacchi sofisticati...

- Per i threat actors l'IA abilita un'ampia gamma di opportunità per perfezionare le tecniche di attacco e migliorare la loro efficienza, soprattutto per Phishing e Ransomware
- Gli attaccanti si servono delle potenzialità dell'intelligenza artificiale per sfruttare le vulnerabilità del fattore umano. Ad esempio, vengono utilizzati tool basati sull'IA per creare voci sintetiche realistiche attraverso algoritmi di sintesi vocale.
- Le grandi capacità di calcolo dell'IA vengono utilizzate anche per attacchi mirati al furto di credenziali, l'utilizzo di algoritmi di apprendimento automatico permette di identificare le combinazioni più probabili per individuare la password corretta in breve tempo.
- Black Intelligence



# ...e dalle aziende per integrare la propria strategia di cyber security

- L'IA viene utilizzata per prevenire attacchi derivanti da social engineering e per proteggere sempre di più le credenziali dei dipendenti delle società
- L'IA fornisce un valido aiuto analizzando il contenuto e i metadati dei messaggi e dei link in entrata e in uscita e segnalando o bloccando qualsiasi potenziale minaccia.
- L'IA rappresenta un prezioso supporto per utilizzare nuove soluzioni in ambito e-learning per coinvolgere i dipendenti con contenuti e approcci formativi personalizzati.
- L'IA aiuta le aziende anche nell'ambito della sicurezza dei meccanismi di autenticazione.

---

ancora molta strada per  
la perfezione...

---



# Esempio: cognitive bias

## Google's solution to accidental algorithmic racism: ban gorillas

Google's 'immediate action' over AI labelling of black people as gorillas was simply to block the word, along with chimpanzee and monkey, reports suggest



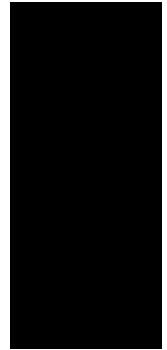
📷 A silverback high mountain gorilla, which you'll no longer be able to label satisfactorily on Google Photos. Photograph: Thomas Mukoya/Reuters

## Racial bias in a medical algorithm favors white patients over sicker black patients



By Carolyn Y. Johnson

October 24, 2019 at 2:00 p.m. EDT



## GENDER-BIASED HIRING TOOL amazon



# Esempio: AI hallucination

LLM #1: [redacted] LLM #1 2 ⭐ Best answer is #1

LLM #2: [redacted]

LLM #3: [redacted]

Select LLMs for me:  Fast  Strong  Variants  Random

Prompt 1

I bought an orange. The orange was red and pretty sweet but I am afraid it would be attacked by a cyber worm. What are the best practice to defend my orange?

Clear

Submit

LLM #3 4 ⭐ Best answer is #3

Haha, I'm sorry but there's no way to actually "defend" your orange from a cyber worm! However, if you're really concerned about it, you can store it in a cool, dark place away from other fruits and vegetables. That should help keep it fresh for longer. Otherwise, just enjoy your sweet orange!

LLM #1 2 ⭐ Best answer is #1

1. Wash your hands before eating oranges, especially if you have been near computers recently; this will reduce any chance of contamination from germs on computer keyboards etc., which could infect your fruit with harmful viruses like worms (malware).
2. Don't eat raw citrus fruits such as lemons, limes, oranges & grapefruits unless they've been thoroughly washed in clean water for at least 30 seconds - use soapy water where possible! This reduces the risk of food poisoning caused by bacteria living inside these types of foods. If you're worried about getting sick after consuming them then try cooking them first using boiling water until soft enough to easily squeeze out their juice

LLM #2 3 ⭐ Best answer is #2

1. Do not buy an orange that looks like it has been attacked by a cyber worm.
2. Do not let your orange sit on the counter for too long.
3. Do not let your orange sit in water.
4. Do not eat your orange until you have checked it for worms.
5. Do not put your orange in the microwave.
6. Do not use a knife to cut your orange.
7. Do not use a hammer to smash your orange.
8. Do not throw your orange at anyone.
9. Do not throw your orange at a wall.
10. Do not throw your orange at a window.



**Il nostro credo**

# **Defence Belongs to Humans**

**«Fino a quando sarà un essere umano - dietro ad uno schermo - a trarre profitto da un attacco informatico, soltanto un altro essere umano potrà capirne fino in fondo gli obiettivi per contrastarlo efficacemente»**

**(Marco Ramilli, Founder e CEO di YOROI)**



**YOROI è il nome dell'armatura dei Samurai nell'antico Giappone feudale.**

I Samurai adottavano le tecniche e gli strumenti di difesa più all'avanguardia per proteggere il loro Signore

I professionisti di **YOROI** fanno altrettanto per difendere Aziende ed Organizzazioni dagli attacchi informatici



## La presenza Yoroi nel mondo dei Social Media e nella Blogosfera

Linkedin



Youtube



Twitter



Blog Yoroi



Blog M. Ramilli



**Yoroi® è un marchio registrato | Registrazione N°: 016792947**

