TLP-GREEN

Agenzia per la Cybersicurezza Nazionale

Luca Montanari
Capo Divisione stato della minaccia, gestione crisi ed esercitazioni

19/3/2025

TLP-GREEN

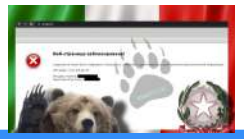
Tendenze della minaccia

TENDENZE DELLA MINACCIA

ATTORI: motivazione vs complessità

TLP-GREEN

Geopolitiche



Hacktivisti

- Attacchi semplici sempre meno potenti (DDoS)
- dotati di limitate capacità ma risorse derivanti da «mercenari»
- campagne di attacco brevi e mirate legate a **geopolitica**
- obiettivo interruzione dei servizi (**D**isponbilità) ai fini di **visibilità mediatica**

Nation State (APT)

- maggiore pericolosità e complessità
- dotati di capacità e risorse
- campagne di attacco su larga scala
- minaccia silente e prolungata
- DWELL time **in decrescita**
- obiettivo è solitamente l'esfiltrazione (**R**iservatezza)

Non Sofisticati

complessità attori

Sofisticati

motivazioni

Cyber Fraud

- motivazioni economiche
- capacità cyber medio/basse, alte in termini di social engineering, **in incremento con AI**
- attacchi basati su opportunità (soggetti vulnerabili tecnicamente o socialmente)
- minaccia talvolta prolungata
- obiettivo esfiltrare (**R**iservatezza) al fine di commettere frodi

Gruppi Ransomware

- motivazioni economiche
- capacità medie e risorse adeguate, in **crescita causa leak di sorgenti di gruppi**
- attacchi basati su opportunità (soggetti vulnerabili o critici)
- minaccia talvolta prolungata
- Obiettivo cifrare ed esfiltrare (**D**isponibilità e **R**iservatezza) al fine di monetizzare tramite **riscatto**

Economiche

posizione nei quadranti

tendenza

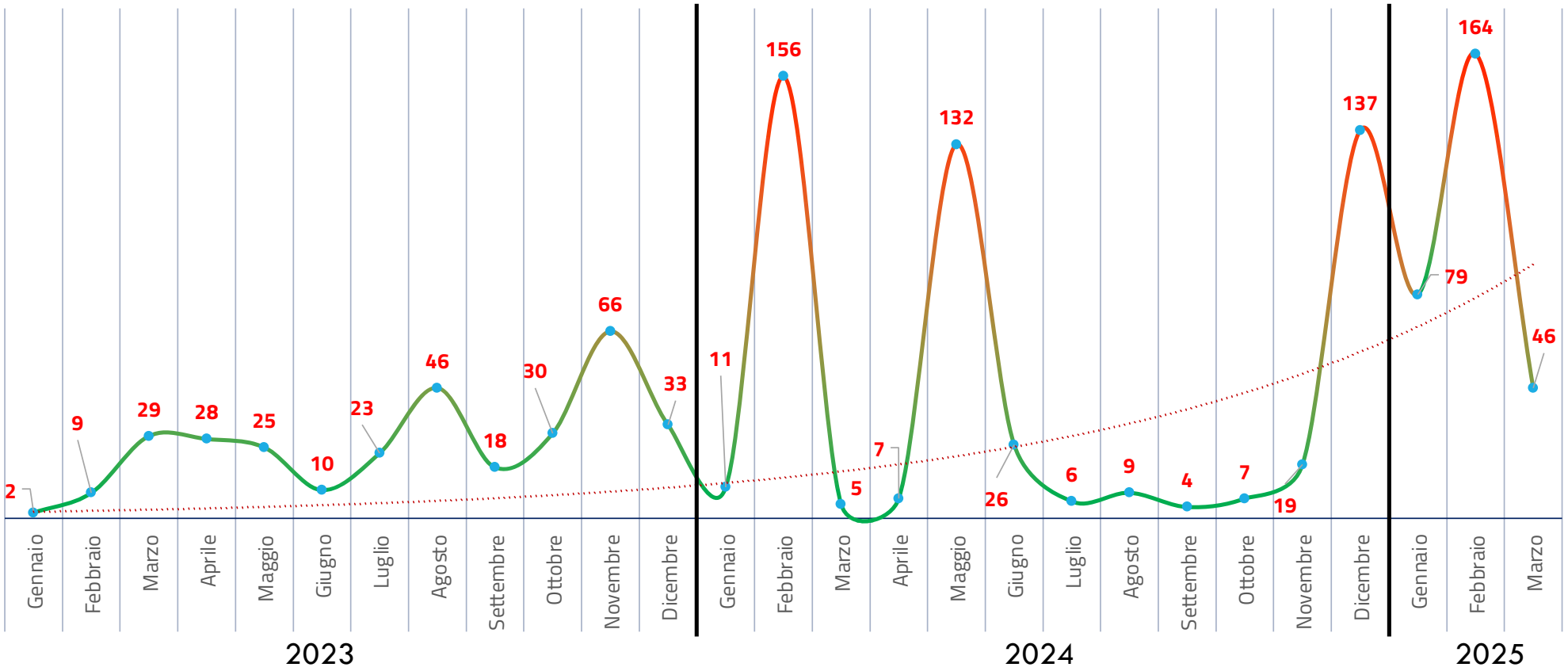
TLP-GREEN

Attacchi DDoS

ATTACCHI DDOS

ANDAMENTO 2023-2025

TLP-GREEN



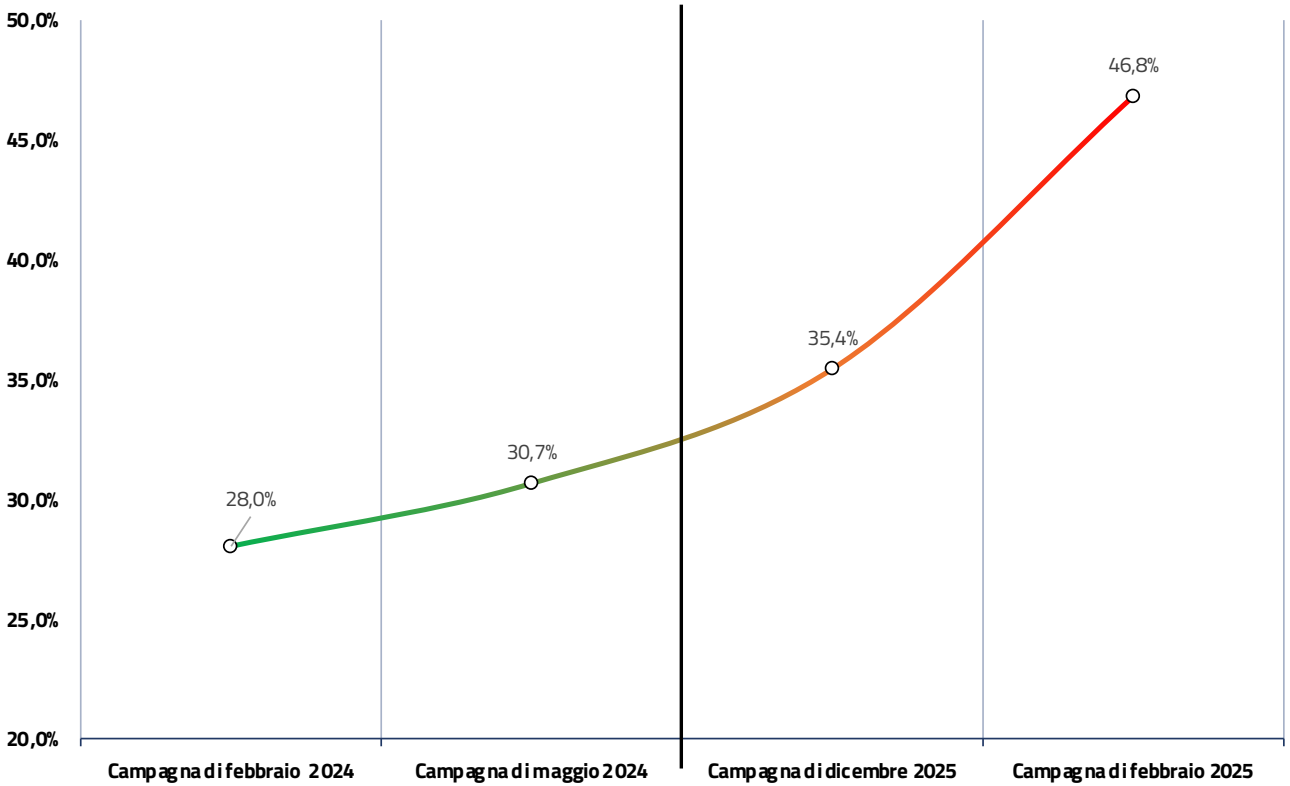
- La crescita del numero di attacchi DDoS dal 2023 è esponenziale.
- Nel 2023 ACN ha censito **319 attacchi**, nel 2024 un totale di **519 attacchi**, nei **primi 2 mesi del 2025 sono 289**

TLP-GREEN

ATTACCHI DDOS

PERCENTUALE DI SOGGETTI NON CRITICI ATTACCATI

Percentuale di soggetti non strutturati rispetto al totale dei soggetti italiani attaccati



Nel corso delle recenti campagne condotte in danno del nostro Paese, si osserva un aumento di attacchi nei confronti di **soggetti non critici**.

Gli hacktivisti selezionano sempre più le vittime in modo da avere **maggior possibilità di rivendicare l'attacco**.

I soggetti più strutturati riescono a mitigare sempre più facilmente questi attacchi.

ATTACCHI DDOS

CONTROMISURE

TLP-GREEN

Pubblicazioni sul sito web CSIRT Italia

- **A partire da maggio 2022 sul sito del CSIRT Italia è stata pubblicata una lista di contromisure specifiche ed avviata la pubblicazione periodica di alert specifici sulle vulnerabilità sfruttate dai DDoS;**

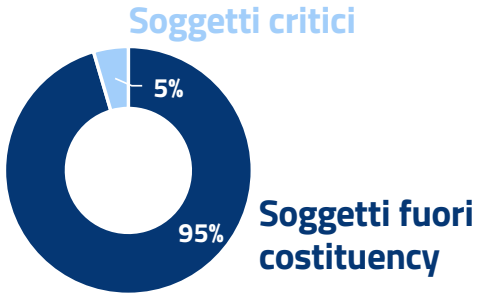
- Il 22 febbraio 2025, ACN ha pubblicato un documento specifico sulla minaccia DDoS, che descrive le **diverse tipologie di attacchi**, **le tecniche e le tattiche adottate** dai cybercriminali, nonché fornisce **raccomandazioni e contromisure**. Inoltre, presenta un modello semplificato di riferimento, utile per identificare gli asset più esposti e orientare con maggiore precisione le **strategie di mitigazione**.

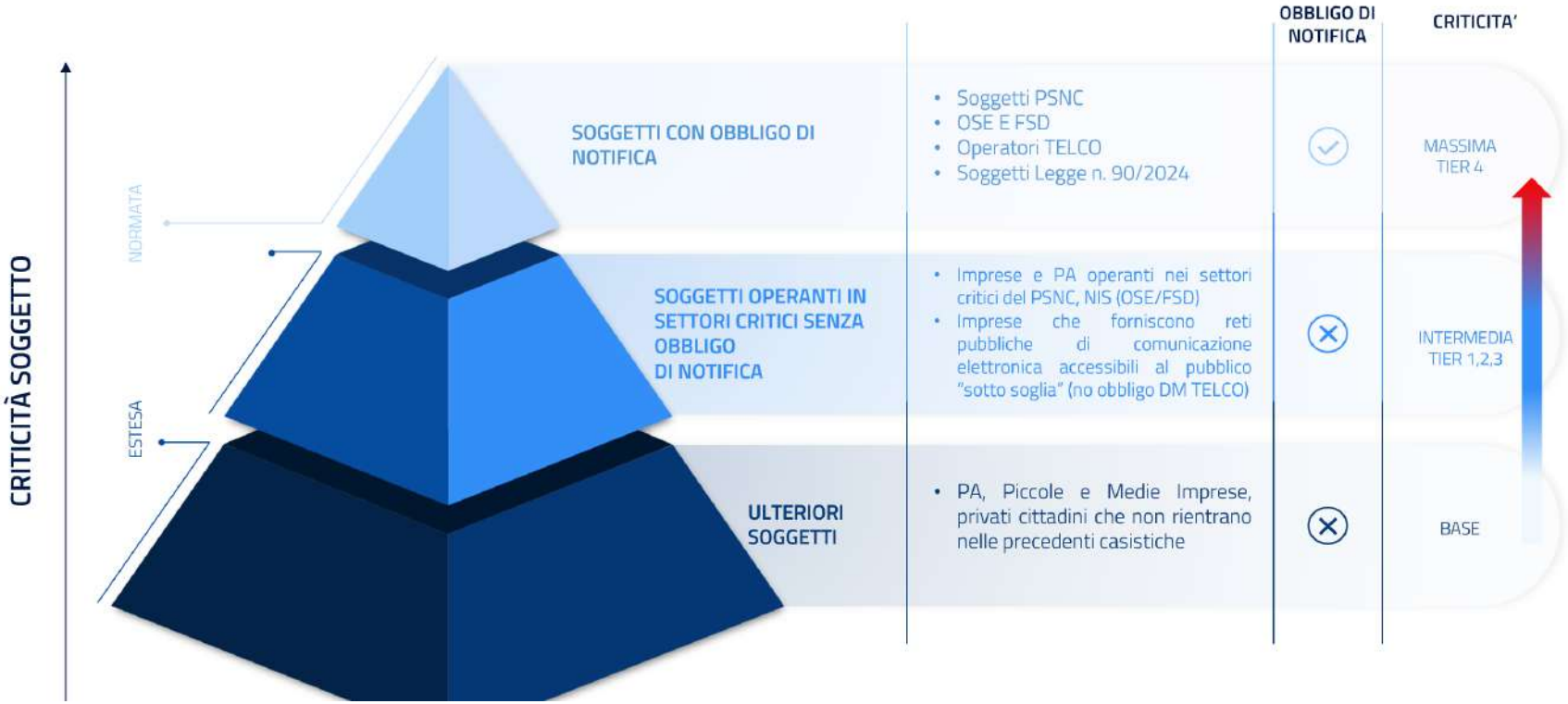
TLP-GREEN

RANSOMWARE

NUMERI E CRITICITÀ DELLE VITTIME

- Nel 2024 ACN ha censito un numero di vittime superiore al 2023 (+20%), tuttavia gli attacchi risultano sempre più opportunistici e meno nei confronti dei soggetti più critici





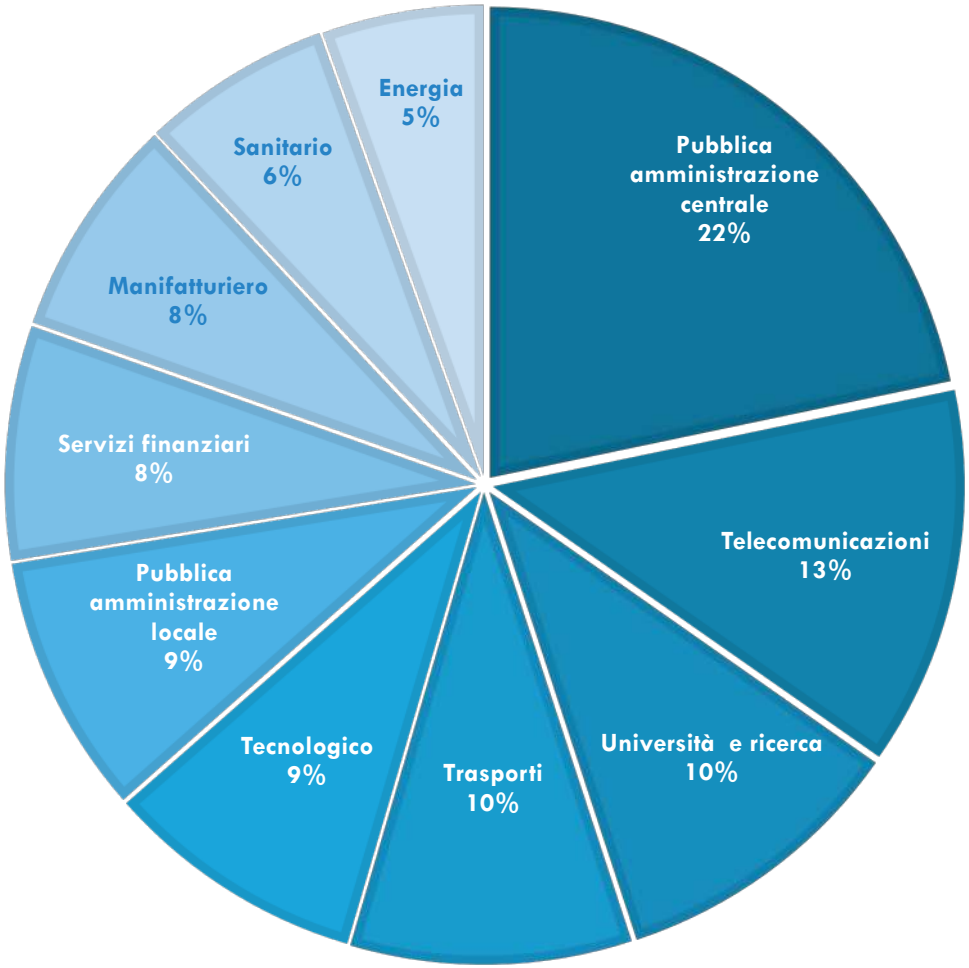
NUMERO DI VITTIME ACCERTATE PER CRITICITÀ

	4.55%
	18,69%
	76,77%

TLP-GREEN

Settori più impattati

SETTORI DELLE VITTIME 2024 (TOP10)



- Pubblica amministrazione centrale
- Telecomunicazioni
- Università e ricerca
- Trasporti
- Tecnologico
- Pubblica amministrazione locale
- Servizi Finanziari
- Manufatturiero
- Sanitario
- Energetico

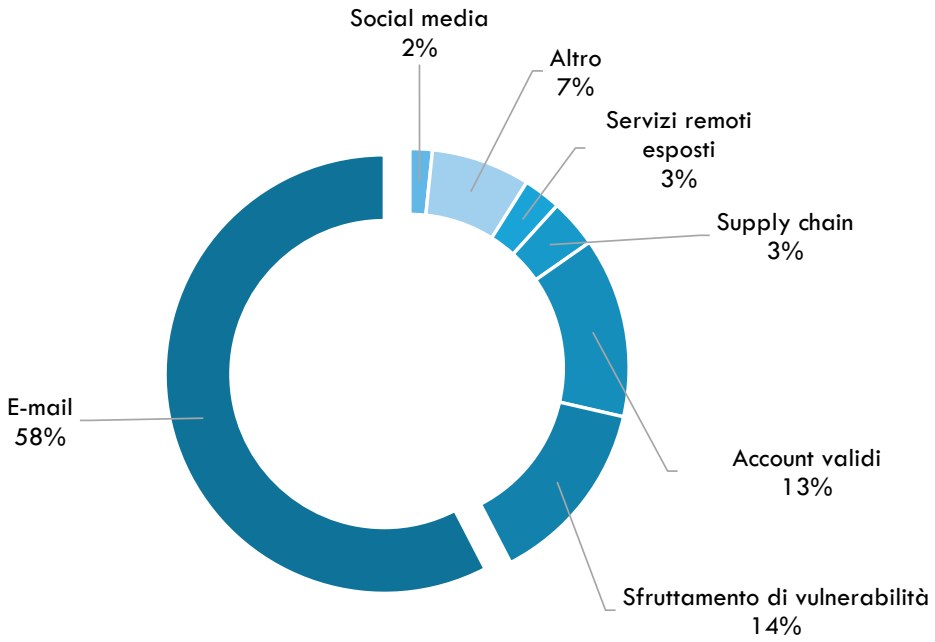
TLP-GREEN

Vettori d’attacco e impatti

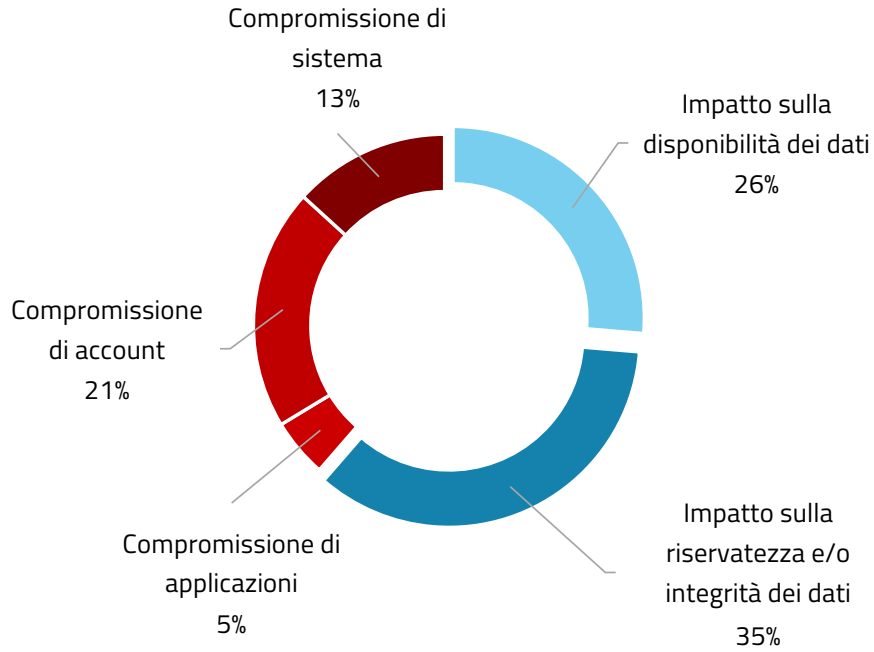
INCIDENTI CYBER

TLP-GREEN

VETTORI D'ATTACCO E IMPATTI



Vettori d'attacco



Impatti degli incidenti

- L'e-mail – e quindi il fattore umano – è il vettore d'attacco di più della metà degli incidenti
- Gli impatti sono in maggioranza sui dati (esfiltrazioni, cifrature, ecc…). Per circa il 40% sui sistemi, account e applicazioni.

Grazie


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT