In UE 4875 incidenti, dal 1° luglio 2024 al 30 giugno 2025

Gli **attacchi DDoS** in UE sono tornati a essere il tipo di incidente dominante e hanno rappresentato il **77% degli incidenti segnalati**, la maggior parte dei quali sono stati implementati da **attivisti**, mentre quelli a opera di criminali informatici rappresentano solo una piccola parte.

Il **ransomware** è identificato come la minaccia più efficace nell'UE.

L'**attivismo** rappresenta quasi l'**80%** del numero totale di incidenti, principalmente attraverso campagne **DDoS** a basso impatto rivolte ai siti web delle organizzazioni degli Stati membri dell'UE. Solo il **2%** degli incidenti di attivismo ha provocato l'**interruzione** del **servizio**.

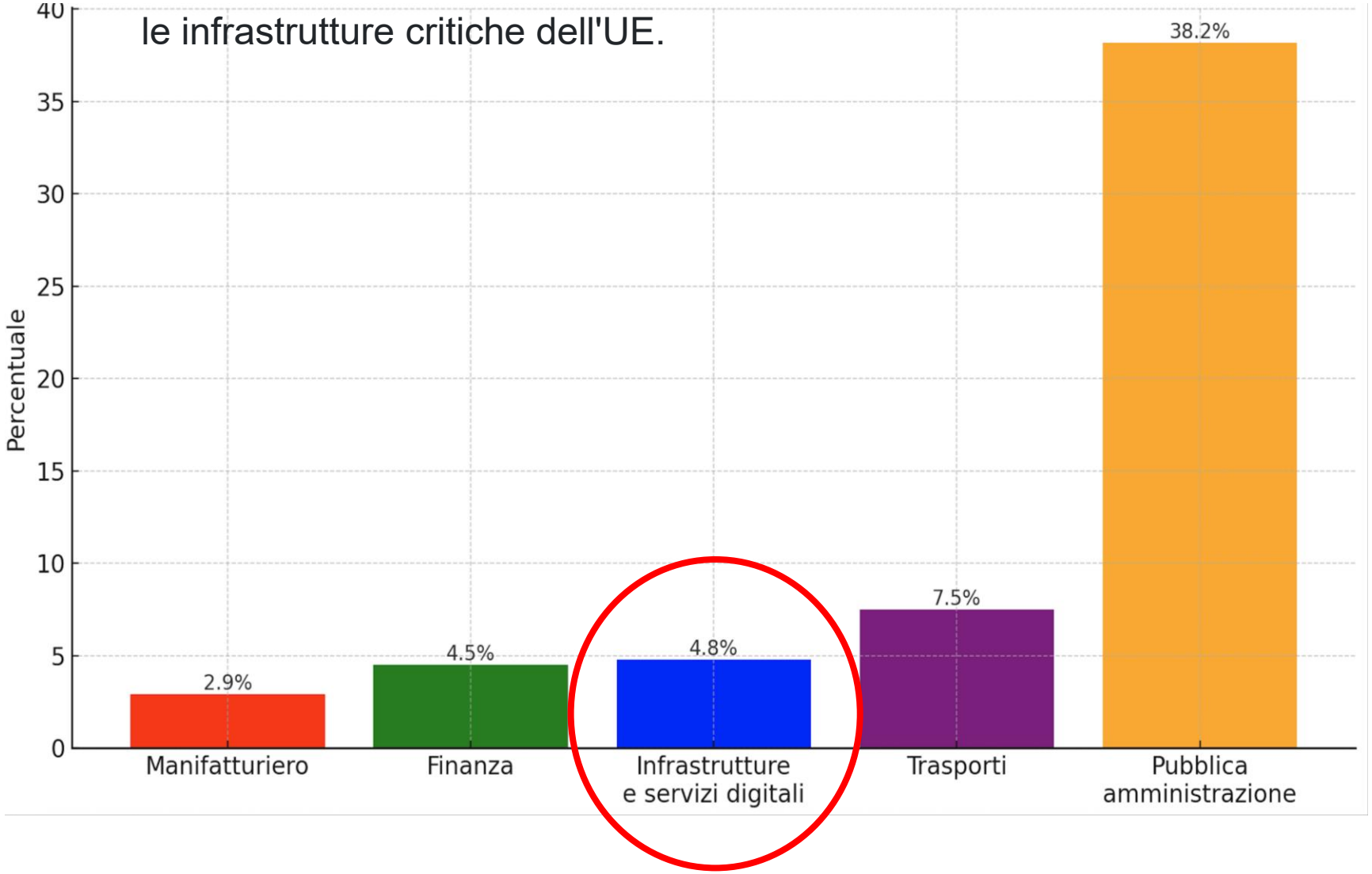
I gruppi **state-sponsored** hanno costantemente intensificato le loro operazioni nei confronti delle organizzazioni dell'UE. Si rilevano attività di **spionaggio** informatico contro il settore della pubblica amministrazione, inoltre l'UE si è trovata di fronte alla **manipolazione** e **disinformazione** di matrice straniera.

Il **phishing** (60%), seguito dallo sfruttamento delle vulnerabilità (21,3%), sono i due principali punti di accesso alle intrusioni.

Per quanto riguarda gli obiettivi valutati di questi incidenti, quasi l'**80%** erano incidenti guidati dall'**ideologia**, eseguiti esclusivamente da attivisti attraverso DDoS.

Contenuto da fonti pubbliche, elaborato con IA, non si riferisce ad alcuna organizzazione specifica

L'analisi settoriale delle minacce evidenzia come obiettivi le infrastrutture critiche dell'UE.



- La stretta corrispondenza tra i settori con il punteggio più elevato e i **settori che rientrano nell'ambito di applicazione della direttiva NIS2** sottolinea l'importanza della direttiva stessa.
- Il **53,7%** del numero totale di incidenti riguarda **soggetti essenziali**, quali definiti dalla **direttiva NIS2**.
- **3** dei primi **5** settori presi di mira sono rimasti **costantemente ai primi posti** per due **anni consecutivi**, mentre la pubblica amministrazione ha visto un notevole aumento degli incidenti quest'anno, guidato dall'aumento degli attacchi DDoS di matrice attivista.

Contenuto da fonti pubbliche, elaborato con IA, non si riferisce ad alcuna organizzazione specifica

Cronologia stato di Azure | Microsoft Azure

Data evento	Durata	Causa principale	Servizi cloud impattati	Portata
9 ottobre 2025	~4 ore (07:50-11:59 UTC)	Bug in Azure Kubernetes Service (AKS) e metadata errato propagato in Azure Front Door dopo bypass del sistema di protezione	Azure Portal, AKS, servizi dipendenti da AFD	Europa e Africa (~26% infrastruttura AFD)
9 ottobre 2025 (sera)	~4 ore (19:43-23:59 UTC)	Problemi di disponibilità Azure Portal dopo migrazione del traffico di nuovo attraverso AFD	Azure Portal, gestione amministrativa	 Globale
29 ottobre 2025	~8 ore (15:41 UTC-00:05 UTC del 30/10)	Errore di configurazione in Azure Front Door (AFD) con metadata corrotto; bug software nel sistema di protezione	Microsoft 365, Teams, Outlook, Xbox Live, Minecraft, Power Apps, Intune, Entra, Purview, Defender, siti terze parti (Costco, Starbucks, Alaska Airlines)	 Globale
5-6 novembre 2025	~9 ore (17:00 UTC del 5/11 - 02:25 UTC del 6/11)	Evento termico nel datacenter: calo di tensione che ha causato spegnimento unità di raffreddamento, con conseguente surriscaldamento e attivazione meccanismi di sicurezza	Virtual Machines, Azure Database PostgreSQL/MySQL Flexible Server, Azure Kubernetes Service, Storage, Service Bus, Virtual Machine Scale Sets, Databricks	West Europe

Gli incidenti di ottobre-novembre 2025 hanno evidenziato vulnerabilità ricorrenti nell'infrastruttura Azure, con **tre eventi critici** in **meno di un mese**. Il disservizio del 29 ottobre è stato il più grave, con perdite economiche stimate fino a 16 miliardi di dollari.

Contenuto da fonti pubbliche, elaborato con IA, non si riferisce ad alcuna organizzazione specifica