



Università Politecnica delle Marche

Dipartimento di Ingegneria dell'Informazione
Corso di Laurea Magistrale in Ingegneria Informatica e
dell'Automazione

CORSO DI DATA SCIENCE

**Social Network Analysis per l'analisi della topologia
degli attacchi di rete**

Professore

Prof. Domenico Ursino

Studenti

Matteo Risolo

Niccolò De Pascali

ANNO ACCADEMICO 2025/2026

Indice

1	Dataset CIC-IDS-2017	5
1.1	Descrizione del dataset	5
2	Botnet	7
2.1	Analisi descrittiva	7
2.1.1	Parametri del grafo	8
2.1.2	Visualizzazione del grafo	9
2.2	Analisi delle centralità	12
2.2.1	Degree Centrality	13
2.2.2	Closeness Centrality	16
2.2.3	Betweenness Centrality	18
2.2.4	Eigenvector Centrality	22
2.2.5	Riassunto finale	25
2.3	Analisi delle strutture	26
2.3.1	Analisi delle comunità	26
2.3.2	Triadi	28
2.3.3	Clique	31
2.3.4	K-Core	32
2.3.5	Ego Network	34
3	Attacco DOS	36
3.1	Analisi descrittiva	37
3.1.1	Parametri del grafo	37

3.1.2	Visualizzazione del grafo	38
3.2	Analisi delle centralità	41
3.2.1	Degree Centrality	42
3.2.2	Closeness Centrality	42
3.2.3	Betweenness Centrality	44
3.2.4	Eigenvector Centrality	45
3.2.5	Riassunto finale	47
3.3	Analisi delle strutture	47
3.3.1	Analisi delle comunità	48
3.3.2	Triadi	49
3.3.3	Clique	50
3.3.4	K-Core	51
3.3.5	Ego Network	52
4	Benign	54
4.1	Analisi descrittiva	54
4.1.1	Parametri del grafo	55
4.1.2	Visualizzazione del grafo	56
4.2	Analisi delle centralità	57
4.2.1	Degree Centrality	58
4.2.2	Closeness Centrality	59
4.2.3	Betweenness Centrality	61
4.2.4	Eigenvector Centrality	62
4.3	Analisi delle strutture	63
4.3.1	Analisi delle comunità	63
4.3.2	Triadi	64
4.3.3	Clique	65
4.3.4	K-Core	66
4.3.5	Ego Network	67

Capitolo 1

Dataset CIC-IDS-2017

1.1 Descrizione del dataset

Il dataset utilizzato per questo lavoro è il **CIC-IDS-2017**, messo a disposizione dal Canadian Institute for Cybersecurity (CIC). Esso rappresenta uno degli standard più diffusi per la valutazione di sistemi di intrusion detection, in quanto raccoglie traffico di rete reale e realistico, composto sia da attività lecite sia da diversi scenari di attacco. I dati sono forniti sotto forma di flussi di rete e comprendono un ampio insieme di caratteristiche relative alle comunicazioni tra host, come indirizzi IP sorgente e destinazione, porte, protocolli, durata dei flussi e volumi di traffico. Una caratteristica rilevante del CIC-IDS-2017 è la suddivisione temporale del traffico su base giornaliera, dove ciascun giorno è associato a una o più tipologie di attacco specifiche (ad esempio Port Scan, DoS, DDoS, Botnet), oltre a periodi di traffico benigno. Tale organizzazione rende il dataset particolarmente adatto ad analisi temporali e a studi basati su finestre temporali ristrette. Ai fini della Social Network Analysis, i dati di traffico sono stati modellati mediante grafi orientati e pesati, nei quali i nodi rappresentano gli indirizzi IP coinvolti nelle comunicazioni, mentre gli archi direzionati rappresentano i flussi di rete osservati tra una sorgente e una destinazione all'interno della finestra temporale considerata. La direzionalità

degli archi consente di preservare l'informazione sul verso della comunicazione, in quanto questa rappresenta una caratteristica particolarmente rilevante per l'analisi dei pattern di attacco. Infine, il peso associato a ciascun arco corrisponde al numero di flussi osservati tra i due nodi all'interno della finestra temporale considerata.

Capitolo 2

Botnet

Nel contesto della Social Network Analysis, le diverse tipologie di attacco presenti nel dataset CIC-IDS-2017 non generano strutture grafiche con lo stesso livello di complessità informativa. Per questo motivo, il presente lavoro avvia l'analisi a partire dagli scenari di tipo **Botnet**, che rappresentano la classe di attacco più significativa dal punto di vista della Social Network Analysis. Le botnet, infatti, sono caratterizzate da comunicazioni distribuite e cooperative tra più nodi compromessi, dando luogo a strutture di rete più articolate, quali sottografi densi, triadi e pattern di interazione non riconducibili a una singola sorgente dominante. Gli altri scenari di attacco e il traffico benigno verranno affrontati nei capitoli successivi al fine di evidenziare le differenze strutturali rispetto al caso botnet.

2.1 Analisi descrittiva

L'analisi ha avuto inizio con la selezione del file .csv relativo allo scenario di attacco Botnet, corrispondente alla giornata di venerdì all'interno del dataset CIC-IDS-2017, dato che tale giornata è dedicata esclusivamente alla simulazione di attività botnet. Successivamente, al fine di individuare il periodo di maggiore intensità dell'attacco, è stata condotta un'analisi preliminare del traf-

fico con l’obiettivo di identificare il minuto specifico in cui si registra il picco dell’attività malevola, espresso in termini di numero di flussi di rete. Questa fase consente di isolare un intervallo temporale rappresentativo, evitando di includere porzioni di traffico poco significative o diluite nel tempo. Una volta individuato il minuto di massimo impatto dell’attacco, è stata definita una finestra temporale di 11 minuti centrata attorno a tale istante. L’utilizzo di una finestra temporale ristretta permette di catturare le interazioni più rilevanti tra gli host coinvolti, preservando al contempo la leggibilità e la significatività strutturale del grafo costruito. I flussi di rete appartenenti a questa finestra temporale sono stati quindi utilizzati come base per la successiva costruzione del grafo.

2.1.1 Parametri del grafo

Successivamente, dopo aver trasformato gli indirizzi IP in identificativi numerici interi, operazione necessaria per la costruzione del grafo, e dopo aver calcolato i pesi degli archi sulla base del numero di flussi osservati, è stato costruito il grafo relativo alla finestra temporale selezionata, che presenta le seguenti caratteristiche:

- **Dimensioni del grafo:** Il grafo è composto da 446 nodi e 941 archi, indicando una rete di dimensioni considerevoli, nella quale un numero elevato di entità di rete interagisce attraverso un insieme relativamente limitato di relazioni. Ciò suggerisce una struttura complessa ma non densamente interconnessa.
- **Densità:** La densità del grafo diretto è pari a 0,004741, valore molto basso che indica che solo una piccola frazione delle possibili connessioni tra nodi è effettivamente presente. Tale caratteristica evidenzia una rete fortemente sparsa, tipica di scenari di comunicazione botnet, in cui le interazioni non sono distribuite uniformemente.

- **Connettività:** Il grafo non risulta né debolmente né fortemente连通的, indicando la presenza di più componenti separate e l'assenza di un'unica struttura globale completamente raggiungibile. Questo comportamento è coerente con la presenza di sottoreti o gruppi di nodi che comunicano in modo parzialmente indipendente.
- **Clustering:** Il coefficiente di clustering medio, calcolato sulla versione non diretta del grafo, è pari a 0,006730. Tale valore estremamente ridotto indica una scarsa presenza di triangoli locali e, di conseguenza, una bassa tendenza alla formazione di comunità fortemente coese.
- **Raggio, diametro e periferia:** Le metriche di raggio, diametro e periferia sono state calcolate sulla componente connessa più grande del grafo, considerando la versione non diretta e utilizzando come distanza l'inverso del peso degli archi ($\text{cost} = 1/\text{weight}$), in modo da modellare una maggiore intensità di comunicazione come una minore distanza. Il raggio risulta pari a 1,08, mentre il diametro è pari a 2,13, indicando che, all'interno della componente principale, le distanze tra i nodi sono mediamente ridotte. La periferia è costituita da un insieme di nodi con eccentricità massima, rappresentativi delle aree meno centrali della rete.

2.1.2 Visualizzazione del grafo

Per facilitare l'analisi qualitativa della struttura di rete, il grafo è stato visualizzato mediante tre differenti algoritmi di layout, applicati alla componente debolmente connessa più grande. L'utilizzo di più rappresentazioni consente di osservare il grafo da prospettive differenti, mettendo in evidenza caratteristiche strutturali complementari. Per facilitare la visualizzazione i nodi corrispondenti agli indirizzi ip degli attaccanti sono stati colorati di rosso, che in questo caso corrispondono agli ID. 1, 8, 16, 58, 138, 139, dove quest'ultimo rappresenta l'attaccante vero e proprio, mentre gli altri corrispondono alle macchine infetta-

te. Inoltre in tutte le rappresentazioni, la dimensione dei nodi è proporzionale al grado del nodo, ovvero al numero di archi incidenti. I nodi di dimensione maggiore rappresentano quindi host che intrattengono un numero più elevato di comunicazioni all'interno della componente principale, risultando strutturalmente più rilevanti nella rete.

Spring layout: Lo spring layout si basa su un modello *force-directed*, in cui i nodi sono trattati come particelle che si respingono reciprocamente, mentre gli archi agiscono come molle elastiche. Tale rappresentazione tende a collocare al centro i nodi più connessi e a separare quelli periferici, risultando particolarmente utile per individuare nodi centrali, strutture a stella e aree di maggiore concentrazione delle connessioni.

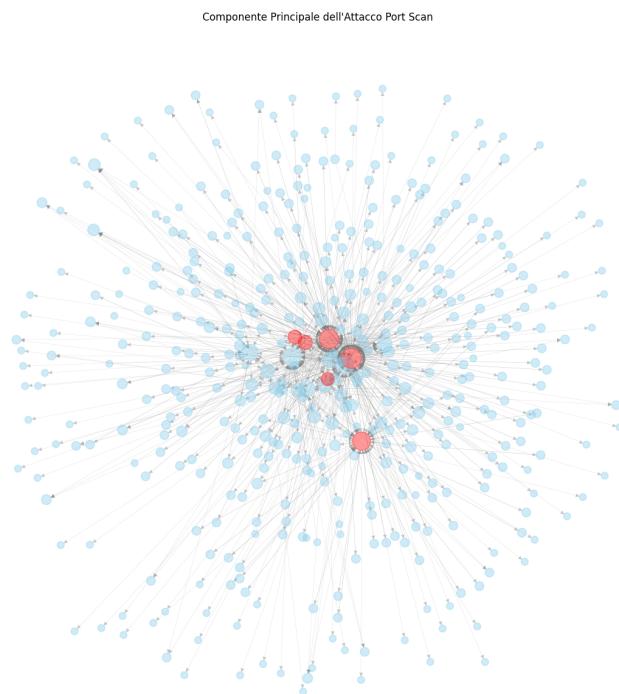


Figura 2.1: Visualizzazione Spring Layout

Circular layout: Nel circular layout i nodi sono disposti uniformemente lungo una circonferenza, indipendentemente dal loro grado di connessione. Questa scelta riduce l'influenza della posizione spaziale sulla percezione delle

relazioni e permette di osservare con maggiore chiarezza la distribuzione degli archi e l'eventuale presenza di nodi che concentrano un numero elevato di connessioni, evidenziando pattern di tipo hub-and-spoke.

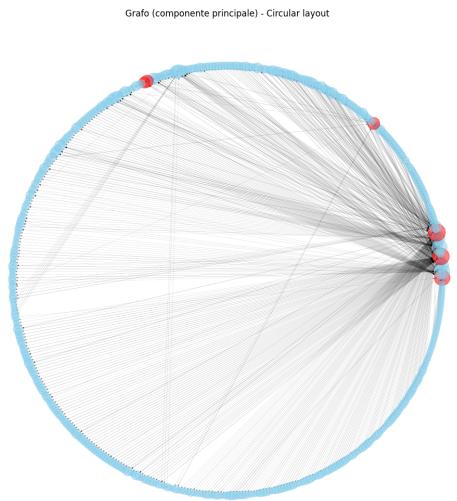


Figura 2.2: Visualizzazione Circular layout

Kamada–Kawai layout: Il Kamada–Kawai layout utilizza un approccio basato sulle distanze topologiche tra i nodi, cercando di posizionare ciascun nodo in modo che le distanze geometriche riflettano il più possibile le distanze di cammino nel grafo. Questa rappresentazione risulta efficace per evidenziare la struttura interna della componente principale, mettendo in risalto sottogruppi di nodi e relazioni più strette tra specifiche porzioni della rete.

Grafo (componente principale) - Kamada-Kawai layout

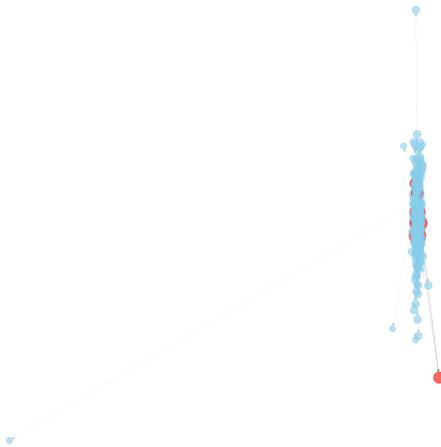


Figura 2.3: Visualizzazione Kamada-Kawai layout

2.2 Analisi delle centralità

Al fine di caratterizzare il ruolo strutturale dei nodi all'interno del grafo, è stata condotta un'analisi delle misure di centralità, strumenti fondamentali della Social Network Analysis per identificare nodi rilevanti, influenti o strategici nelle dinamiche di comunicazione.

La **Degree Centrality** misura il numero di connessioni di un nodo. Nel caso di grafi orientati, essa è stata distinta in in-degree e out-degree, che rappresentano rispettivamente il numero di connessioni entranti e uscenti. Questa misura consente di individuare nodi particolarmente attivi come sorgenti o come destinatari di comunicazioni.

La **Closeness Centrality** valuta quanto un nodo sia vicino, in termini di distanza topologica, a tutti gli altri nodi della rete. Un valore elevato indica nodi che possono raggiungere rapidamente il resto del grafo, risultando potenzialmente efficienti nella propagazione di informazioni o comandi.

La **Betweenness Centrality** quantifica la frequenza con cui un nodo si colloca sui cammini minimi tra altre coppie di nodi. Essa permette di indivi-

duare nodi che svolgono un ruolo di intermediazione o di controllo del traffico, potenzialmente critici per la connettività della rete.

Infine, la **Eigenvector Centrality** misura l'importanza di un nodo tenendo conto non solo del numero delle sue connessioni, ma anche dell'importanza dei nodi a cui è connesso. Questa misura consente di identificare nodi inseriti in regioni della rete strutturalmente rilevanti e densamente interconnesse.

2.2.1 Degree Centrality

La Degree Centrality è stata utilizzata come prima misura per individuare i nodi con il maggior numero di interazioni all'interno della rete botnet. Di seguito i risultati delle analisi.

Tabella 2.1: Top 5 Nodi per Degree Centrality

Nodo	In-Degree Centrality	Out-Degree Centrality	Degree Centrality
16	0.3002	0.3792	0.4041
8	0.2167	0.2641	0.2641
3	0.1151	0.1129	0.1716
1	0.1151	0.1242	0.1287
11	0.0745	0.0993	0.0993

Tabella 2.2: Bottom 5 Nodi per Degree Centrality

Nodo	In-Degree Centrality	Out-Degree Centrality	Degree Centrality
178	0.0023	0.0000	0.0023
175	0.0023	0.0023	0.0023
173	0.0023	0.0023	0.0023
172	0.0023	0.0023	0.0023
445	0.0000	0.0023	0.0023

L'analisi dei nodi con i valori più elevati di degree centrality evidenzia una forte eterogeneità nella distribuzione delle connessioni. In particolare, i nodi

1, 8 e 16, che corrispondono alle macchine infettate, presentano valori significativamente superiori rispetto alla media della rete. Tali nodi mostrano sia un elevato out-degree, indicativo di un'intensa attività di comunicazione verso altri host, sia un in-degree non trascurabile, suggerendo un ruolo attivo nelle dinamiche di scambio all'interno della botnet. Questo comportamento è coerente con la presenza di host compromessi che partecipano attivamente alla propagazione o al coordinamento delle attività malevole. Accanto a questi nodi, altri vertici con elevata degree centrality presentano valori più contenuti ma comunque rilevanti, indicando una partecipazione secondaria alla comunicazione, potenzialmente riconducibile a nodi di supporto o a entità coinvolte in un numero limitato di interazioni. Al contrario, i nodi con i valori più bassi di degree centrality risultano caratterizzati da un numero estremamente ridotto di connessioni, spesso limitato a una sola comunicazione entrante o uscente.

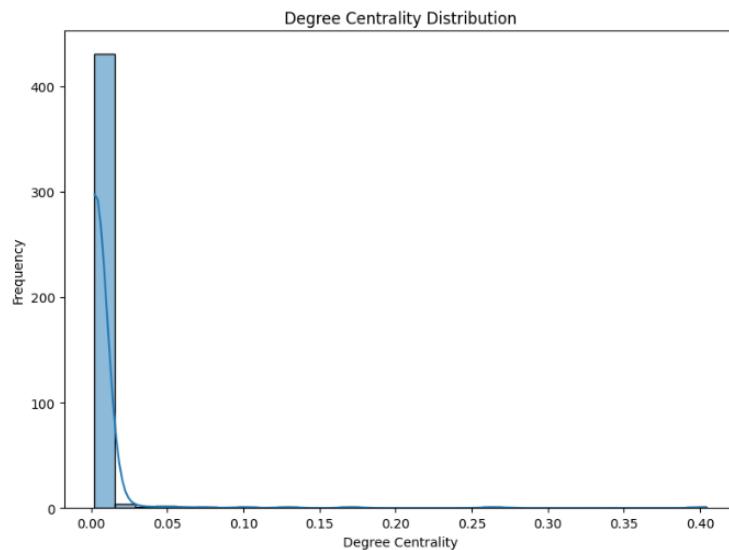


Figura 2.4: Distribuzione della degree centrality

La distribuzione della Degree Centrality mostra un andamento fortemente asimmetrico, con la grande maggioranza dei nodi concentrata su valori molto bassi e una coda lunga verso destra. Ciò indica che la maggior parte degli host partecipa a un numero limitato di comunicazioni, mentre pochi nodi presentano valori di degree centrality significativamente elevati, concentrando una quota

rilevante delle interazioni complessive. Questo comportamento è coerente con una struttura tipica degli scenari botnet, in cui un numero ristretto di macchine infettate svolge un ruolo centrale nella comunicazione, mentre la restante parte dei nodi rimane periferica e scarsamente connessa.

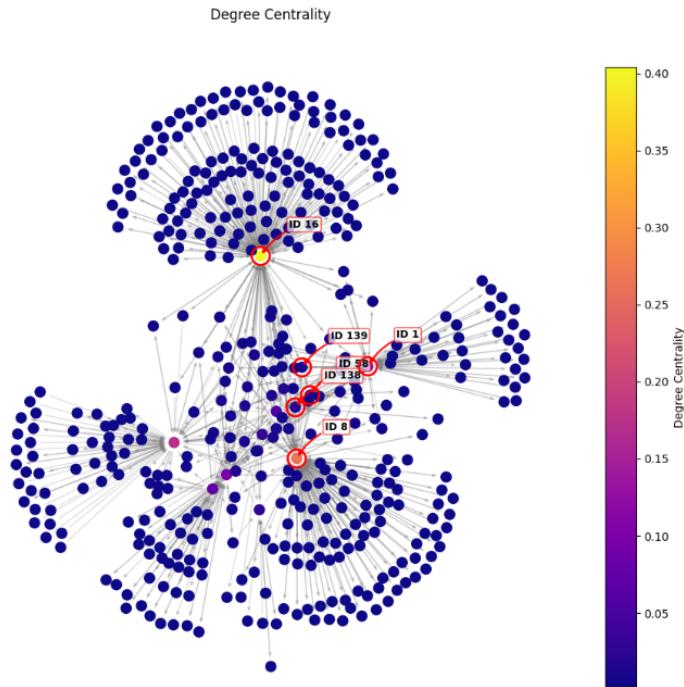


Figura 2.5: Heatmap Degree centrality

Dall’analisi dell’Heatmap si osserva chiaramente la presenza di pochi nodi con degree centrality elevata, evidenziati da colori più chiari e marcatori distintivi, che occupano posizioni centrali nella rete. In particolare, i nodi identificati come ID 1, ID 8 e ID 16, corrispondenti a macchine infettate, risultano tra i più connessi, confermando il loro ruolo centrale nelle comunicazioni della botnet. Attorno a tali nodi si dispongono numerosi nodi periferici con valori di centralità molto ridotti, collegati principalmente a un singolo hub, confermando quindi una configurazione fortemente sbilanciata e gerarchica, tipica di scenari botnet, in cui un numero ristretto di nodi compromessi funge da punto di aggregazione del traffico, mentre la maggior parte degli host mantiene un ruolo marginale e scarsamente interconnesso.

2.2.2 Closeness Centrality

La Closeness Centrality è stata analizzata per valutare la posizione dei nodi all'interno della rete in termini di vicinanza topologica agli altri nodi. Di seguito i risultati delle analisi.

Tabella 2.3: Top 5 Nodi per Closeness Centrality

Nodo	Closeness Centrality
8	1.6157
127	1.6137
230	1.6105
139	1.6092
128	1.5958

Tabella 2.4: Bottom 5 Nodi per Closeness Centrality

Nodo	Closeness Centrality
87	0.6123
66	0.6123
154	0.6123
93	0.6024
228	0.5890

L'analisi dei nodi con i valori più elevati di closeness centrality evidenzia la presenza di nodi collocati in posizioni strutturalmente centrali all'interno della componente principale. Tra questi, il nodo 8, già identificato come macchina infetta, presenta il valore più elevato, confermando il suo ruolo di nodo fortemente integrato nella rete botnet. Accanto ad esso emergono altri nodi con valori di degree relativamente contenuti ma con elevata closeness, indicando che la centralità di tali nodi non dipende necessariamente dal numero di connessioni, bensì dalla loro posizione strategica nella struttura del grafo.

In particolare, la presenza del nodo 139, identificato come attaccante principale, tra i nodi con maggiore closeness centrality suggerisce che esso occupi una posizione favorevole per raggiungere rapidamente un'ampia porzione della rete. Questo comportamento è coerente con un ruolo di coordinamento o di controllo, in cui la capacità di interagire efficientemente con altri nodi risulta più rilevante del semplice numero di connessioni dirette. Al contrario, i nodi con i valori più bassi di closeness centrality risultano fortemente periferici, con distanze elevate rispetto al resto della rete, indicando un coinvolgimento minimo nelle dinamiche di comunicazione.

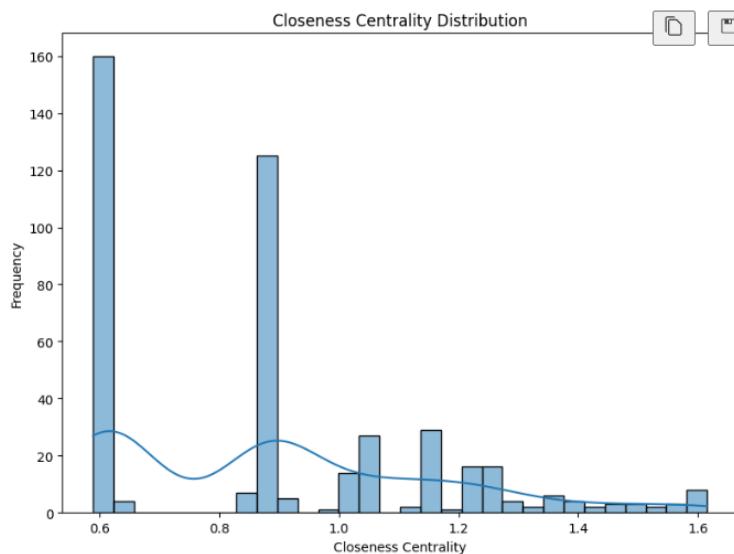


Figura 2.6: Distribuzione della Closeness centrality

La distribuzione della Closeness Centrality evidenzia una marcata eterogeneità nella posizione dei nodi all'interno della rete. Una parte consistente dei nodi presenta valori bassi di closeness, indicando una collocazione periferica e una distanza elevata rispetto al resto della componente principale. Tali nodi risultano difficilmente raggiungibili e poco efficienti nel diffondere o ricevere informazioni. Al contrario, un numero limitato di nodi mostra valori di closeness centrality elevati, collocandosi in posizioni topologicamente privilegiate. Questi nodi sono in grado di raggiungere rapidamente gran parte della rete

attraverso cammini brevi, suggerendo un ruolo strategico nelle dinamiche di comunicazione della botnet.

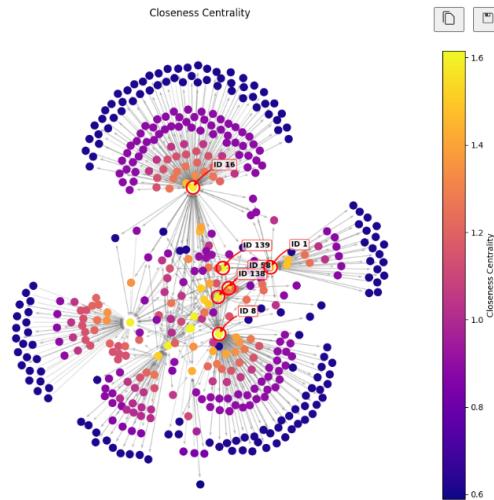


Tabella 2.5: Top 5 Nodi per Betweenness Centrality

Nodo	Betweenness Centrality
8	0.6661
16	0.5590
139	0.5299
127	0.4977
3	0.2485

Tabella 2.6: Bottom 5 Nodi per Betweenness Centrality

Nodo	Betweenness Centrality
152	0.0000
151	0.0000
150	0.0000
149	0.0000
445	0.0000

8 e 16, ovvero le macchine infette, presentano i valori più elevati, confermando il loro ruolo non solo come nodi altamente connessi, ma anche come punti di passaggio privilegiati nelle comunicazioni della botnet. Tali nodi risultano quindi fondamentali per la propagazione del traffico all'interno della rete. Un risultato particolarmente significativo è la presenza del nodo 139, identificato come attaccante principale, tra i nodi con betweenness centrality più elevata. Questo dato suggerisce che il nodo 139 svolga un ruolo di snodo strutturale, fungendo da collegamento tra diverse porzioni della rete e contribuendo in modo rilevante alla connettività complessiva. Al contrario, i nodi con betweenness centrality nulla risultano esclusi dai cammini minimi che collegano altre coppie di nodi. Tali nodi presentano un ruolo puramente periferico e non contribuiscono in modo significativo alla mediazione del traffico, risultando strutturalmente irrilevanti dal punto di vista dell'interconnessione della rete.

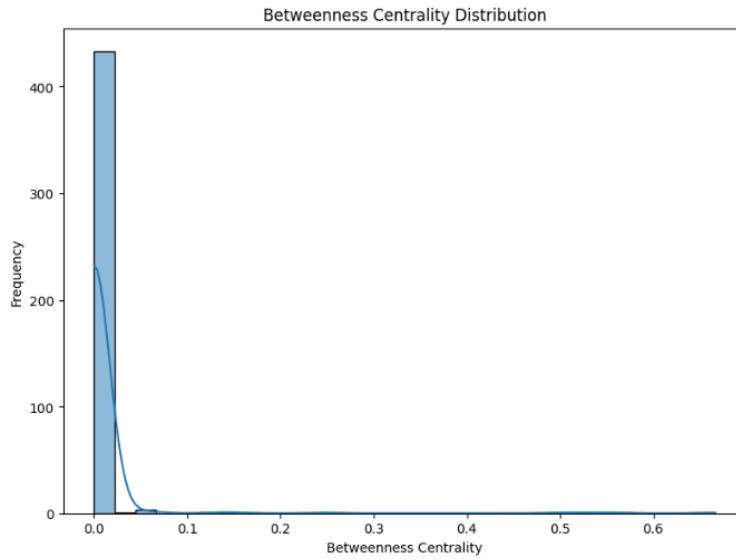


Figura 2.8: Distribuzione della Betweenness Centrality

La distribuzione della Betweenness Centrality mostra una forte concentrazione dei nodi su valori prossimi allo zero, indicando che la maggior parte degli host non partecipa ai cammini minimi che collegano altre coppie di nodi. Questo comportamento evidenzia una rete in cui l’intermediazione del traffico è affidata a un numero estremamente ridotto di nodi. La presenza di una coda lunga verso valori elevati di betweenness centrality indica invece l’esistenza di pochi nodi strutturalmente critici, che fungono da punti di passaggio privilegiati tra diverse porzioni della rete. Tali nodi rivestono un ruolo chiave nel mantenimento della connettività e nella propagazione delle comunicazioni all’interno della botnet.

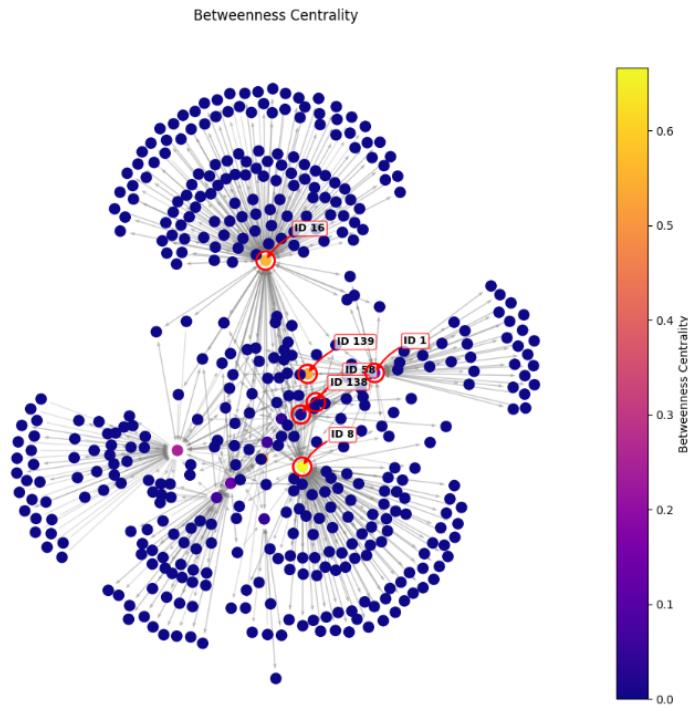


Figura 2.9: Heatmap della Betweenness centrality

Si osserva come le macchine infette (in particolare i nodi ID 8 e ID 16) presentino valori elevati di betweenness centrality, confermando il loro ruolo di snodi di intermediazione nelle comunicazioni della botnet. Inoltre, come è già stato evidenziato precedentemente, il nodo ID 139 emerge chiaramente come uno dei nodi più rilevanti in termini di intermediazione, suggerendo una funzione di collegamento tra sottostrutture distinte del grafo. La maggior parte dei nodi, rappresentata da colori più scuri, mostra valori prossimi allo zero, indicando un ruolo marginale nei processi di intermediazione. Questa rappresentazione visiva rafforza l'interpretazione di una rete fortemente gerarchica, in cui la capacità di instradare il traffico è concentrata in un numero limitato di nodi chiave.

2.2.4 Eigenvector Centrality

La Eigenvector Centrality è stata analizzata per valutare l'importanza dei nodi tenendo conto non solo del numero delle connessioni, ma anche della rilevanza strutturale dei nodi adiacenti.

Tabella 2.7: Top 5 Nodi per Eigenvector Centrality

Nodo	Eigenvector Centrality
127	0.7064
230	0.6021
8	0.3376
128	0.1064
11	0.0786

Tabella 2.8: Bottom 5 Nodi per Eigenvector Centrality

Nodo	Eigenvector Centrality
32	0.000005
66	0.000005
115	0.000005
106	0.000005
72	0.000005

L'analisi dei nodi con i valori più elevati di eigenvector centrality mette in evidenza un insieme di nodi che, pur non presentando necessariamente i valori più alti di degree, risultano inseriti in regioni della rete altamente interconnesse. In particolare, i nodi 127 e 230 mostrano i valori più elevati di eigenvector centrality, indicando una collocazione in prossimità di nodi strutturalmente rilevanti. Il nodo 8, quindi una delle macchine infette, presenta anch'esso un valore elevato di eigenvector centrality, confermando la sua connessione con nodi centrali e il suo inserimento nel cuore della struttura della rete. I nodi

con i valori più bassi di eigenvector centrality risultano invece collocati ai margini della rete, con connessioni limitate a nodi scarsamente rilevanti. Tali nodi presentano un ruolo puramente periferico e non contribuiscono in modo significativo alla struttura centrale della botnet.

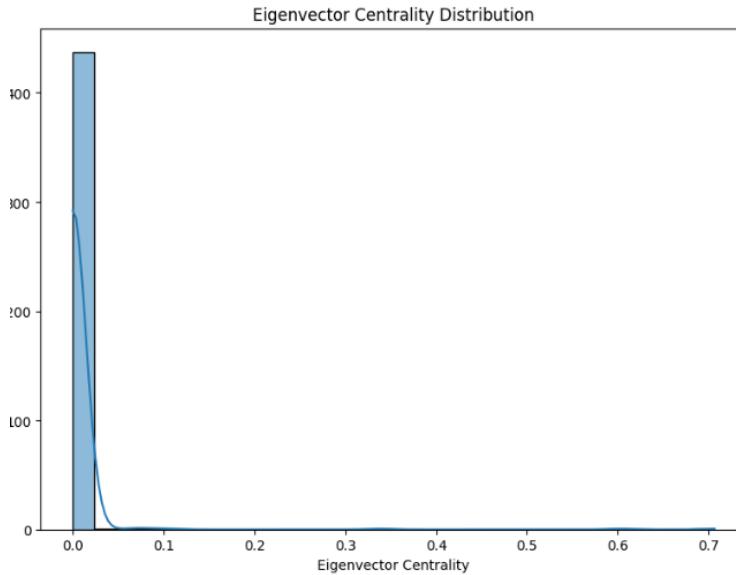


Figura 2.10: Distribuzione della Eigenvector Centrality

La distribuzione della Eigenvector Centrality evidenzia una forte concentrazione dei nodi su valori prossimi allo zero, indicando che la maggior parte degli host è connessa a nodi strutturalmente poco rilevanti. Solo un numero molto limitato di nodi presenta valori significativamente più elevati, formando una coda pronunciata nella parte destra della distribuzione. Questo andamento conferma la presenza di un nucleo ristretto di nodi altamente influenti, inseriti in regioni della rete densamente interconnesse, mentre la grande maggioranza dei nodi rimane relegata in una periferia strutturale.

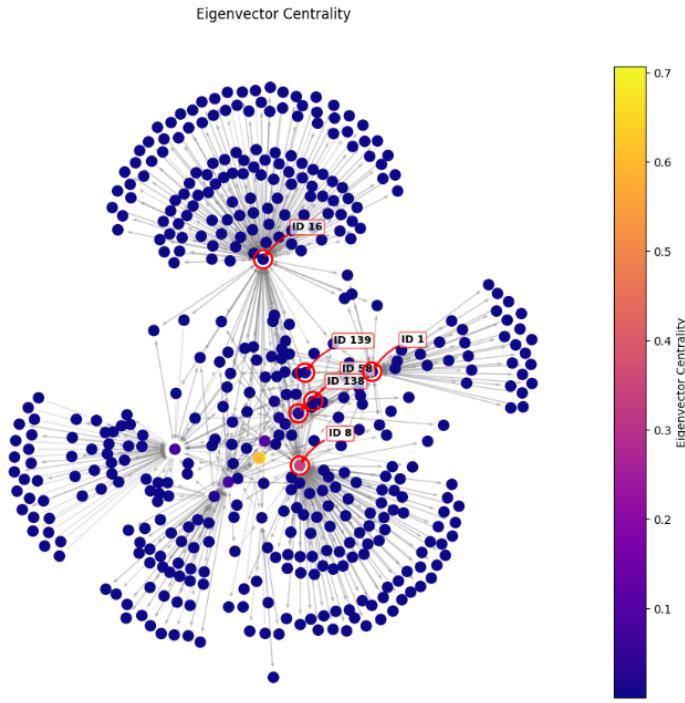


Figura 2.11: Heatmap della Eigenvector Centrality

Dalla figura precedente si osserva come solo un numero molto limitato di nodi presenti valori elevati di eigenvector centrality, mentre la grande maggioranza degli host rimane caratterizzata da valori prossimi allo zero. In particolare, alcuni nodi già emersi nelle analisi precedenti tra cui ID 8 e ID 16 risultano collocati nel nucleo centrale della rete, confermando il loro inserimento in una struttura di comunicazione fortemente interconnessa. Al contrario, il nodo ID 139, pur svolgendo un ruolo rilevante in termini di intermediazione, mostra un'influenza più contenuta secondo questa misura. I nodi periferici, rappresentati da colori più scuri, risultano connessi prevalentemente a nodi poco rilevanti e non contribuiscono in modo significativo alla struttura centrale della botnet.

2.2.5 Riassunto finale

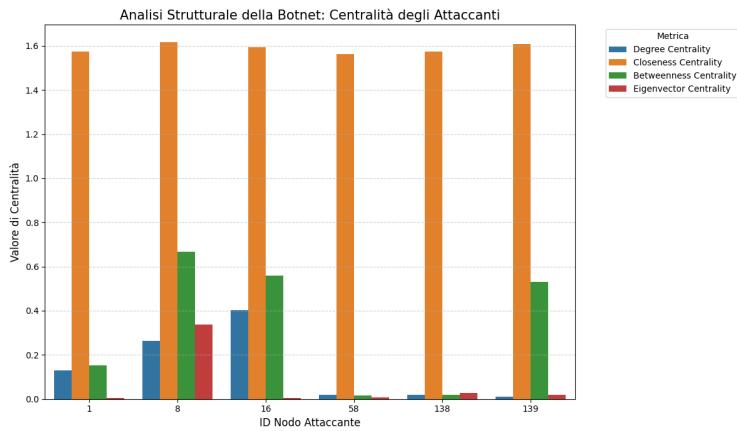


Figura 2.12: Grafico riassuntivo degli attaccanti

Il grafico precedente riassume i valori delle principali misure di centralità calcolate per i nodi identificati come attaccanti o macchine infette, consentendo un confronto diretto tra i diversi ruoli strutturali all'interno della botnet. Si osserva come le macchine infette, in particolare i nodi 8 e 16, presentino valori elevati di degree e closeness centrality, indicando un'elevata attività di comunicazione e una posizione topologicamente centrale nella rete. Tali nodi risultano quindi fortemente integrati nella struttura della botnet e coinvolti direttamente nello scambio di traffico. Il nodo ID 139, identificato come attaccante principale, mostra invece un profilo differente: pur presentando valori contenuti di degree ed eigenvector centrality, esso evidenzia valori elevati di betweenness e closeness centrality, suggerendo un ruolo di intermediazione strategica tra diverse porzioni della rete. Questo comportamento è coerente con una funzione di coordinamento o controllo piuttosto che di partecipazione massiva alle comunicazioni. Nel complesso, il confronto tra le centralità evidenzia una chiara differenziazione dei ruoli all'interno della botnet, distinguendo nodi altamente attivi, nodi strutturalmente influenti e nodi che svolgono una funzione di snodo, confermando la natura gerarchica e organizzata della rete analizzata.

2.3 Analisi delle strutture

Oltre alle misure di centralità, l'analisi della rete è stata estesa allo studio delle strutture del grafo, con l'obiettivo di individuare pattern di interazione ricorrenti e sottostrutture significative che descrivono il livello di cooperazione e organizzazione tra i nodi.

Le **triadi** rappresentano configurazioni elementari composte da tre nodi e permettono di analizzare la presenza di relazioni locali e di schemi di interazione ricorrenti. Lo studio delle triadi consente di valutare il grado di chiusura e la tendenza dei nodi a formare relazioni indirette, fornendo indicazioni sulla cooperazione locale all'interno della rete.

Le **clique** sono sottografi completi in cui ciascun nodo è connesso a tutti gli altri. L'individuazione delle clique permette di identificare gruppi di nodi fortemente interconnessi, potenzialmente riconducibili a insiemi di host che collaborano in modo coordinato nelle attività della botnet.

Il **k-core** identifica sottografi in cui ogni nodo è connesso ad almeno k altri nodi dello stesso sottografo. Questa struttura consente di isolare il nucleo della rete, evidenziando le porzioni più dense e resistenti, che tendono a persistere anche in presenza della rimozione di nodi periferici.

Infine, le **ego-network** descrivono il sottografo costituito da un nodo di interesse (ego) e dai suoi vicini diretti, insieme alle relazioni tra essi. L'analisi delle ego-network permette di studiare in dettaglio il contesto locale di nodi specifici, in particolare quelli strutturalmente rilevanti, chiarendo il loro ruolo operativo all'interno della botnet.

2.3.1 Analisi delle comunità

Come prima analisi viene effettuata l'analisi delle comunità:

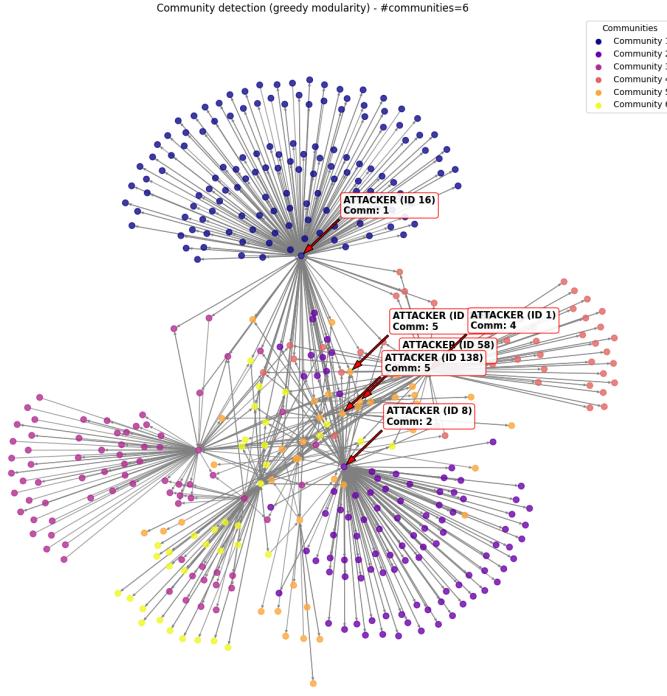


Figura 2.13: Analisi delle comunità

La figura mostra il risultato dell’analisi di community detection applicata alla componente debolmente connessa più grande del grafo botnet. Tale analisi suddivide la rete in comunità massimizzando la modularità, ovvero la densità delle connessioni interne ai gruppi rispetto a quelle tra gruppi differenti. In questo caso l’algoritmo individua sei comunità distinte. La visualizzazione evidenzia una chiara struttura modulare della rete, in cui i nodi tendono ad aggregarsi in sottogruppi relativamente ben separati, collegati tra loro da un numero limitato di archi. È particolarmente rilevante notare come i nodi identificati come attaccanti o macchine infette risultino distribuiti in comunità differenti. In particolare, nodi quali ID 16, ID 8, ID 1, ID 58, ID 138 e ID 139 emergono come elementi centrali all’interno delle rispettive comunità, suggerendo che ciascun gruppo possa essere associato a una porzione specifica dell’attività botnet o a un sottoinsieme di host coordinati. La presenza di più comunità, ciascuna con un proprio nodo dominante, indica che l’attacco non è

organizzato come un'unica struttura monolitica, ma piuttosto come un insieme di sottostrutture parzialmente indipendenti, coordinate attraverso nodi di collegamento. Questo risultato è coerente con un'architettura botnet distribuita, progettata per aumentare la resilienza e ridurre l'impatto dell'isolamento di singoli nodi.

2.3.2 Triadi

L'analisi delle triadi è stata condotta per studiare le strutture locali della rete e valutare il grado di chiusura delle relazioni tra piccoli gruppi di nodi

Tabella 2.9: Analisi delle Triadi: Statistiche della Rete Generale

Descrizione	Conteggio Totale
Triadi Chiuse	19
Triadi Aperte	29.444

Tabella 2.10: Analisi Dettagliata delle Triadi per ID Attaccante (Botnet)

ID Nodo	Triadi Totali	Chiuse	Aperte	Chiusura (%)
16	15.931	1	15.930	0.01%
8	6.786	1	6.785	0.01%
1	1.596	3	1.593	0.19%
138	36	2	34	5.56%
58	36	0	36	0.00%
139	10	0	10	0.00%

A livello globale, la rete botnet presenta un numero estremamente ridotto di triadi chiuse, pari a 19, a fronte di un numero molto elevato di triadi aperte, pari a 29 444. Questo squilibrio indica una struttura fortemente poco chiusa, in cui le interazioni tra i nodi raramente danno luogo a relazioni triangolari. Tale comportamento suggerisce l'assenza di una cooperazione locale diffusa

e una prevalenza di comunicazioni dirette. L'analisi dettagliata delle triadi che coinvolgono i nodi attaccanti conferma ulteriormente questa caratteristica strutturale. La maggior parte degli attaccanti presenta esclusivamente triadi aperte, con un coefficiente di chiusura nullo o prossimo allo zero. In particolare, i nodi ID 58 e ID 139 mostrano un numero limitato di triadi totali, tutte di tipo aperto, indicando interazioni puntuale e non cooperative. I nodi ID 16 e ID 8, pur partecipando a un numero molto elevato di triadi, presentano una sola triade chiusa ciascuno, con un tasso di chiusura pari a circa 0,01%. Questo risultato evidenzia che, anche nei nodi più centrali e attivi, le relazioni tendono a rimanere non transitive. Un'eccezione parziale è rappresentata dal nodo ID 138, che mostra un tasso di chiusura più elevato (5,56%), pur su un numero complessivo di triadi molto ridotto. Nel complesso, questi risultati indicano che la botnet analizzata è caratterizzata da interazioni prevalentemente aperte, con una cooperazione locale minima anche tra nodi strutturalmente rilevanti.

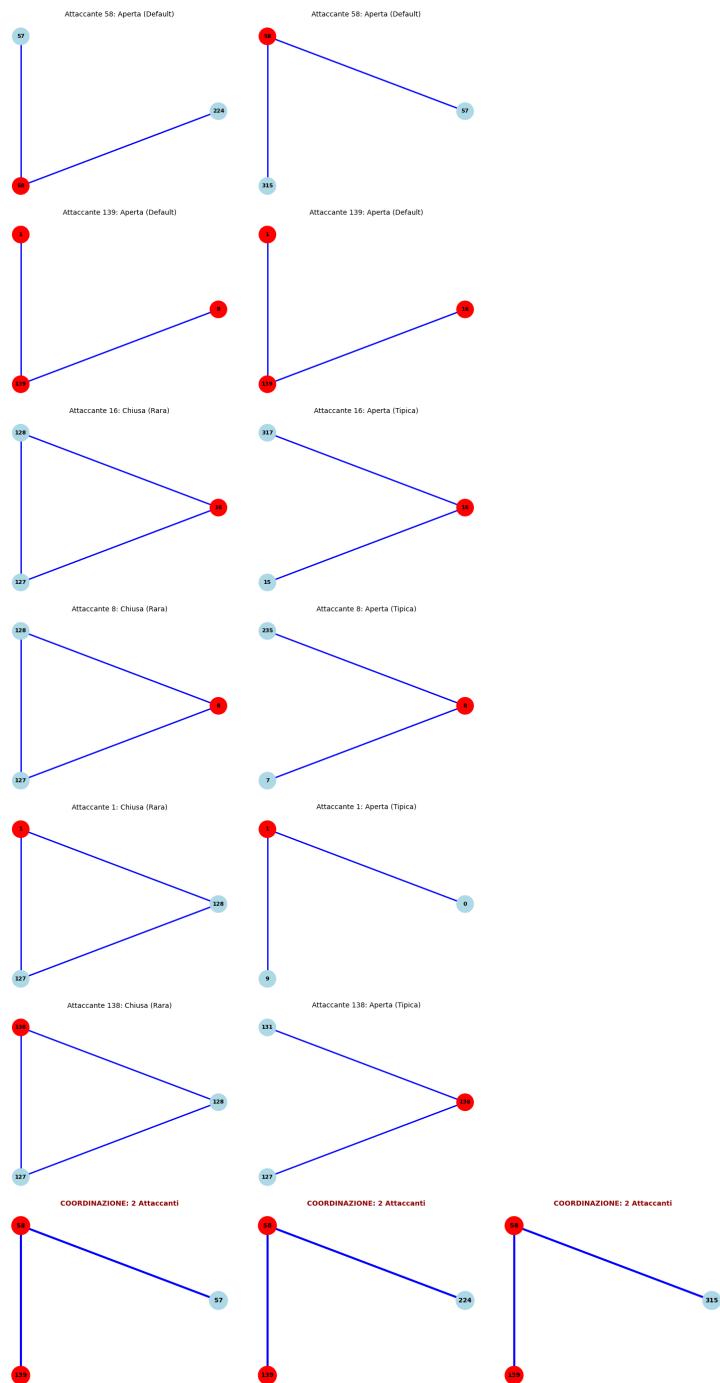


Figura 2.14: Visualizzazione delle triadi (2 per ogni attaccante) e alla fine tre triadi che hanno almeno 2 attaccanti

2.3.3 Clique

L'analisi delle clique è stata condotta per individuare sottostrutture completamente connesse, ovvero gruppi di nodi in cui ogni elemento è direttamente collegato a tutti gli altri.

Tabella 2.11: Analisi Generale delle Clique

Parametro	Valore
Numero Totale di Clique	559
Dimensione Massima Clique	3
Esempio Clique Principale	[1, 127, 128]

Tabella 2.12: Analisi Mirata delle Clique per i Nodi Botnet

ID Nodo	Numero Clique	Dimensione Massima Clique
16	178	3
8	116	3
1	56	3
58	9	2
138	8	3
139	5	2

A livello globale, la rete presenta un numero complessivo di 559 clique, con una dimensione massima pari a 3. Questo risultato indica che le strutture completamente connesse sono limitate a triangoli, mentre non emergono sottografi più densi. Un esempio di clique di dimensione massima è costituito dai nodi [1, 127, 128]. La limitata dimensione massima delle clique suggerisce una rete priva di gruppi altamente coesi e caratterizzata da interazioni prevalentemente non reciproche, coerentemente con quanto emerso dall'analisi delle triadi. L'analisi focalizzata sui nodi attaccanti evidenzia comportamenti differenziati. I nodi 58 e 139 partecipano a un numero ridotto di clique, tutte di dimensione 2,

indicando l'assenza di cooperazione locale strutturata. Al contrario, i nodi 16, 8, 1 e 138 risultano coinvolti in clique di dimensione 3. In particolare, i nodi 16 e 8, già emersi come centrali nelle analisi precedenti, partecipano a un numero elevato di clique, suggerendo un ruolo di aggregazione di più connessioni locali, pur in assenza di una forte densità relazionale.

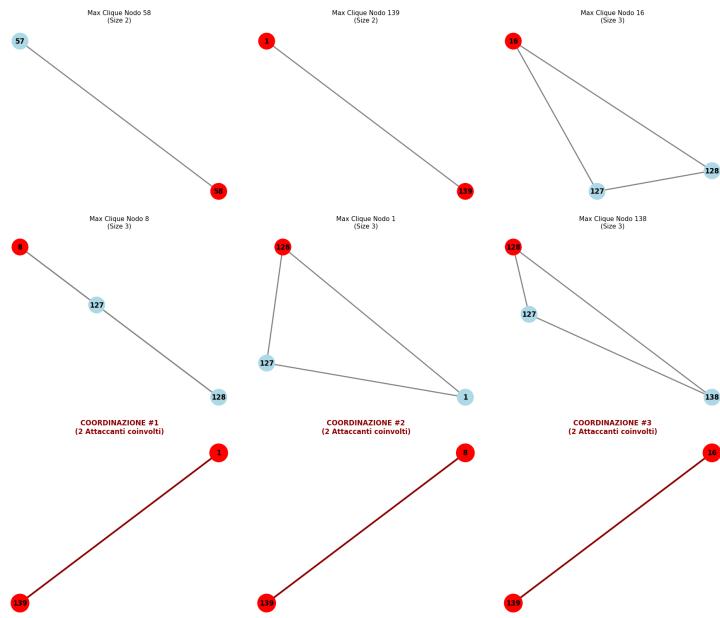


Figura 2.15: Visualizzazione delle clique (1 per ogni attaccante) e alla fine 3 che coinvolgano almeno 2 attaccanti

2.3.4 K-Core

L'analisi del k-core è stata condotta per individuare le porzioni più dense e strutturalmente resilienti della rete.

Tabella 2.13: Analisi Generale della Distribuzione K-Core

Livello del Core (k)	Numero di Nodi
$k = 1$	363
$k = 2$	40
$k = 3$	18
$k = 4$	23

Tabella 2.14: Posizionamento dei Nodi Botnet nei K-Core

ID Nodo	Livello K-Core
16	4
8	4
1	4
58	4
139	4
138	3

La distribuzione dei k-core mostra una forte prevalenza di nodi a bassa integrazione strutturale. In particolare, 363 nodi appartengono al 1-core, mentre il numero di nodi diminuisce progressivamente all'aumentare di k . Il k massimo della rete è pari a 4, con 23 nodi appartenenti al core massimo.

Questa distribuzione evidenzia una rete composta prevalentemente da nodi periferici, affiancata da un nucleo ristretto e altamente interconnesso, che rappresenta la parte più compatta e resistente della struttura. L'analisi del posizionamento dei nodi attaccanti all'interno dei k-core rivela un risultato particolarmente significativo. I nodi 1, 8, 16, 58 e 139 risultano tutti appartenere al k-core massimo ($k = 4$), indicando una massima integrazione strutturale all'interno della rete. Questi nodi non solo sono centrali secondo le misure di centralità analizzate in precedenza, ma fanno anche parte del nucleo più denso e resiliente del grafo. Al contrario, il nodo 138 appartiene al k-core intermedio ($k = 3$), suggerendo una posizione meno integrata rispetto agli altri attaccanti. Pur risultando coinvolto nelle attività della botnet, tale nodo appare collocato in una regione più periferica del nucleo centrale, con un livello di connessione inferiore.

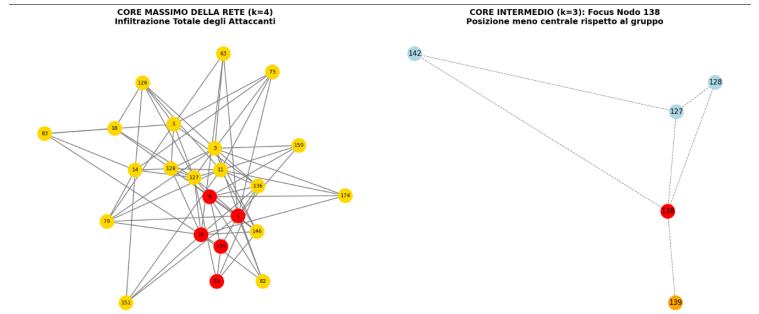


Figura 2.16: Visualizzazione del K-Core

2.3.5 Ego Network

L’analisi delle ego-network è stata condotta per esaminare in dettaglio il contesto locale dei nodi attaccanti, considerando ciascun nodo come ego e analizzando il sottografo formato dai suoi vicini diretti (alter) e dalle connessioni tra essi.

Tabella 2.15: Analisi delle Ego-Networks dei Nodi Botnet

ID Nodo (Ego)	Vicini Diretti (Size)	Connessioni nell’Intorno
16	179	180
8	117	118
1	57	60
138	9	11
58	9	9
139	5	5

I nodi 58, 139 e 138 presentano ego-network di dimensioni ridotte, con un numero limitato di vicini diretti e una densità locale relativamente elevata. In particolare, i nodi 58 e 139 mostrano una struttura poco estesa e priva di una chiara configurazione gerarchica, mentre il nodo 138, pur presentando un numero di connessioni leggermente superiore, rimane inserito in una rete locale compatta.

Tali caratteristiche sono coerenti con una struttura mista, compatibile con traffico di servizio o con nodi che non svolgono un ruolo primario nel coordinamento dell'attacco. Al contrario, i nodi 16, 8 e 1 mostrano ego-network di dimensioni significativamente maggiori, caratterizzate da un numero elevato di vicini diretti e da una densità locale molto bassa. In questi casi, il nodo attaccante risulta connesso a numerosi host che, tuttavia, non comunicano tra loro. Questa configurazione è riconducibile a un modello comunicativo fortemente accentrato, in cui il nodo centrale funge da punto di coordinamento e instradamento del traffico verso un ampio insieme di nodi subordinati. Le visualizzazioni associate mostrano chiaramente questa struttura, con il nodo ego al centro e una vasta periferia di nodi foglia.

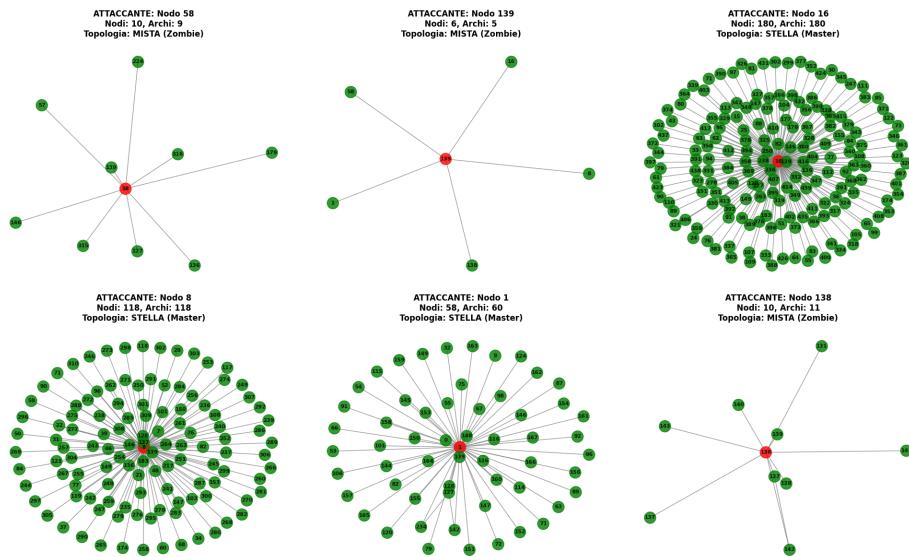


Figura 2.17: Visualizzazione dell'Ego Network per ogni attaccante

Capitolo 3

Attacco DOS

Dopo l’analisi approfondita dello scenario botnet, l’attenzione viene ora rivolta all’attacco di tipo **Denial of Service (DoS)**, con l’obiettivo di fornire un termine di confronto rispetto a una tipologia di attacco caratterizzata da una struttura fortemente centralizzata e non cooperativa. Nel dataset CIC-IDS-2017, l’attacco DoS è riconducibile a un singolo nodo attaccante che genera un elevato volume di traffico verso un insieme di vittime, dando luogo a una topologia di rete semplice e altamente sbilanciata.

Le tipologie di attacco **Port Scan** e **DDoS**, pur essendo state analizzate e sviluppate durante il lavoro, non vengono descritte in dettaglio nella presente relazione in quanto producono strutture di rete sostanzialmente analoghe a quelle osservate per il DoS, sia dal punto di vista grafico sia dal punto di vista delle metriche di Social Network Analysis. Per tale motivo, l’analisi DoS viene utilizzata come caso rappresentativo degli attacchi centralizzati, evitando ripetizioni ridondanti e mantenendo la trattazione focalizzata sugli aspetti strutturalmente più significativi.

3.1 Analisi descrittiva

L’analisi descrittiva dell’attacco DoS è stata condotta seguendo la stessa procedura adottata per lo scenario botnet. In particolare, è stato selezionato il file del dataset relativo al giorno in cui si manifesta l’attacco, individuato il periodo di massima intensità del traffico e definita una finestra temporale ristretta per la costruzione del grafo. La metodologia di costruzione del grafo, così come la definizione di nodi, archi e pesi, rimane invariata rispetto a quanto già descritto nella sezione precedente.

3.1.1 Parametri del grafo

Il grafo costruito per l’attacco DoS è composto da 400 nodi e 807 archi, dimensioni che riflettono la presenza di un numero consistente di host coinvolti, ma con una struttura complessivamente semplice. La densità del grafo diretto, pari a 0,005056, indica una rete fortemente sparsa, in cui solo una frazione minima delle possibili connessioni è effettivamente presente.

Il grafo non risulta connesso, né in senso debole né in senso forte, evidenziando la presenza di più componenti separate. Tale caratteristica è coerente con la natura dell’attacco DoS, in cui le comunicazioni sono concentrate su specifiche relazioni dirette tra l’attaccante e le vittime, senza generare una rete diffusamente interconnessa.

Il coefficiente di clustering medio, calcolato sulla versione non diretta del grafo, assume un valore molto basso (0,004103), confermando l’assenza di strutture locali chiuse e di cooperazione tra nodi, in linea con una topologia di tipo fortemente centralizzato.

Le misure di raggio e diametro, calcolate sulla componente connessa più grande e utilizzando una distanza inversamente proporzionale al peso degli archi, risultano rispettivamente pari a 1,27 e 2,52. Tali valori indicano che la maggior parte dei nodi è raggiungibile in un numero molto ridotto di passi,

a conferma di una struttura compatta e poco profonda. I nodi appartenenti alla periferia rappresentano host marginali, collocati ai limiti della componente principale e caratterizzati da un ruolo secondario nella dinamica dell'attacco.

Nel complesso, i parametri strutturali descrivono una rete semplice, sparsa e fortemente sbilanciata, coerente con un attacco DoS condotto da un singolo nodo centrale verso un insieme di vittime indipendenti.

3.1.2 Visualizzazione del grafo

Successivamente sono state effettuate le visualizzazioni del grafo relative all'attacco DoS, ed anche in questo caso sono state realizzate sulla componente debolmente connessa più grande, utilizzando tre differenti layout al fine di evidenziare in modo complementare la struttura della rete. In questo è presente un solo attaccante il cui indirizzo ip corrisponde al nodo con ID 52.

Spring layout mette chiaramente in evidenza una struttura fortemente sbilanciata, caratterizzata dalla presenza di un singolo nodo centrale attorno al quale si dispongono numerosi nodi periferici. Le forze di attrazione e repulsione del layout producono una configurazione compatta in prossimità dell'attaccante, mentre le vittime risultano distribuite radialmente, senza connessioni significative tra loro. Questa rappresentazione evidenzia in modo immediato la natura centralizzata dell'attacco.

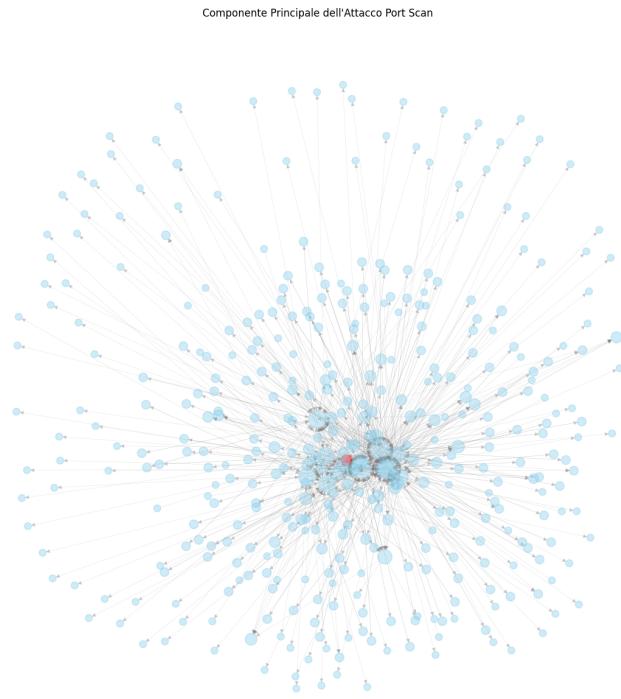


Figura 3.1: Visualizzazione Spring Layout

Circular layout consente di osservare la distribuzione dei nodi lungo una circonferenza, rendendo evidente la presenza di un insieme ristretto di nodi maggiormente connessi, verso i quali convergono numerosi archi. In questa visualizzazione le connessioni non risultano concentrate esclusivamente sull'attaccante, ma mostrano una parziale dispersione verso altri nodi intermedi, indicando una struttura comunque sbilanciata ma non riconducibile a una stella pura. Il grafo evidenzia quindi una topologia fortemente centralizzata, con alcuni nodi che svolgono un ruolo dominante rispetto a una vasta periferia di host meno connessi.

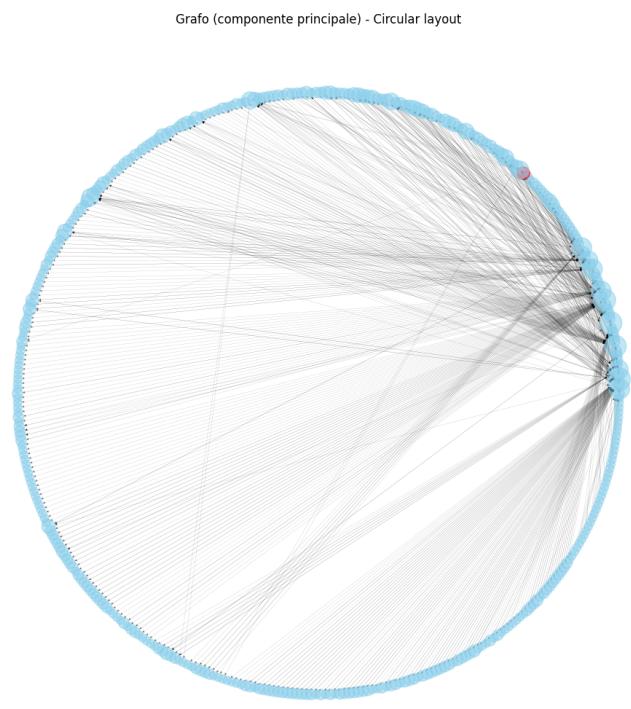


Figura 3.2: Visualizzazione Circular Layout

Kamada-Kawai layout enfatizza le distanze topologiche tra i nodi, collocando l'attaccante in una posizione ben separata rispetto al resto della rete. In questa rappresentazione, il nodo centrale risulta chiaramente distinguibile, mentre il gruppo delle vittime appare concentrato in una regione compatta ma subordinata, collegata quasi esclusivamente al nodo attaccante. Tale layout rafforza l'interpretazione di una rete poco profonda e priva di articolazioni strutturali complesse.

Grafo (componente principale) - Kamada-Kawai layout



Figura 3.3: Visualizzazione Kamada-Kawai Layout

3.2 Analisi delle centralità

L’analisi delle misure di centralità è stata condotta in forma mirata, con l’obiettivo di caratterizzare il ruolo strutturale del nodo attaccante (ID 52) e sulla principale vittima (ID 53), identificata come web server Ubuntu, in quanto unici nodi funzionalmente rilevanti all’interno di una struttura fortemente centralizzata. Considerata la natura dell’attacco DoS, l’attenzione è rivolta esclusivamente ai nodi funzionalmente rilevanti, evitando analisi di ranking estese e concentrandosi sulle misure più significative per l’interpretazione del comportamento dell’attacco. Per le stesse ragioni, le rappresentazioni grafiche delle centralità sono volutamente limitate rispetto a quanto fatto nello scenario botnet, in quanto le distribuzioni globali risultano poco informative. Vengono pertanto riportate solo le visualizzazioni ritenute utili a supportare l’interpretazione dei ruoli principali all’interno della rete.

3.2.1 Degree Centrality

Tabella 3.1: Analisi di Centralità per i Nodi 52 e 53

Nodo	In-Degree	Out-Degree	Degree
52	0.0050	0.0050	0.0050
53	0.0227	0.0302	0.0302

Il nodo attaccante (ID 52) presenta valori molto contenuti sia di in-degree che di out-degree centrality, con un degree centrality complessivo pari a 0,0050. Questo risultato indica che l'attaccante stabilisce un numero limitato di relazioni distinte nella rete. Tale comportamento è coerente con la natura dell'attacco DoS, in cui l'efficacia dell'azione malevola non dipende dalla molteplicità delle connessioni, ma dall'invio reiterato e intensivo di traffico verso uno specifico bersaglio.

La vittima (ID 53), corrispondente a un web server Ubuntu, mostra un valore di degree centrality superiore (0,0302) rispetto all'attaccante. Questo incremento è dovuto alla presenza sia di connessioni malevole provenienti dall'attaccante sia di comunicazioni legittime generate da altri host della rete. Di conseguenza, il nodo 53 risulta strutturalmente più connesso, pur non svolgendo alcun ruolo attivo nell'attacco.

3.2.2 Closeness Centrality

Tabella 3.2: Closeness Centrality per i Nodi 52 e 53

Nodo	Closeness Centrality
52	1.2671
53	1.2682

Il nodo attaccante presenta un valore elevato di closeness centrality pari a 1,267, indicando che esso si colloca in una posizione topologicamente vicina

alla maggior parte dei nodi della componente principale. Questo risultato è coerente con la natura dell'attacco DoS: l'attaccante non necessita di un elevato numero di connessioni, ma risulta strutturalmente vicino al resto della rete grazie alla scarsa profondità del grafo. La vittima mostra un valore di closeness centrality sostanzialmente analogo e leggermente superiore (1,268). Tale comportamento è giustificabile dal ruolo del nodo come servizio centrale della rete, che intrattiene comunicazioni sia legittime sia malevole, risultando quindi facilmente raggiungibile da un'ampia porzione dei nodi. Altri nodi invece, presentano valori di closeness ancora più elevati, ma tali risultati sono da interpretare alla luce della struttura complessiva del grafo e non indicano necessariamente un ruolo attivo nell'attacco.

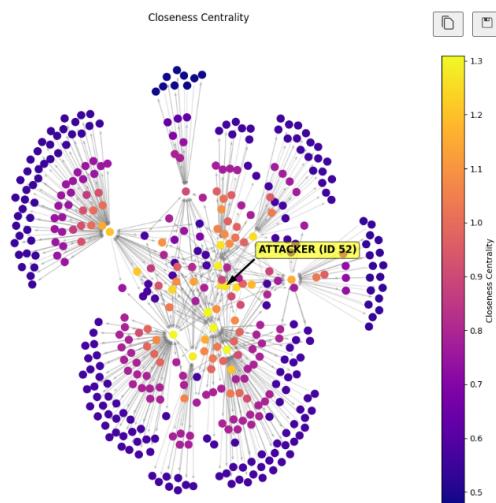


Figura 3.4: Heatmap Closeness Centrality

Dall'analisi dell'heatmap risulta che il nodo attaccante emerge con un valore di closeness relativamente elevato, rappresentato da un colore molto chiaro, ciò dimostra che l'attaccante si colloca in una posizione topologicamente favorevole all'interno della rete. Tale risultato è coerente con quanto scoperto precedentemente, in cui la presenza di cammini brevi consente all'attaccante di raggiungere rapidamente gran parte dei nodi, pur in assenza di un elevato numero di connessioni dirette. Si osserva inoltre che valori di closeness com-

parabili sono assunti anche da altri nodi centrali, tra cui la vittima principale e alcuni nodi intermedi. I nodi periferici, rappresentati da colori più scuri e disposti ai margini della visualizzazione, risultano invece caratterizzati da distanze maggiori dal resto della rete, coerentemente con il loro ruolo marginale nella dinamica dell'attacco.

3.2.3 Betweenness Centrality

Tabella 3.3: Betweenness Centrality per i Nodi 52 e 53

Nodo	Betweenness Centrality
52	0.0150
53	0.0246

Il nodo attaccante presenta un valore di betweenness centrality molto basso (0,0150), indicando che esso non svolge un ruolo di instradamento o di collegamento tra sottoreti differenti. Questo risultato è coerente con la dinamica dell'attacco DoS: l'attaccante genera traffico diretto verso il bersaglio senza mediare comunicazioni tra nodi terzi.

La vittima principale mostra anch'essa un valore di betweenness centrality contenuto (0,0246). Sebbene il nodo riceva traffico da più sorgenti, esso non risulta coinvolto in modo significativo nei percorsi che collegano altri nodi della rete, confermando il suo ruolo passivo di bersaglio dell'attacco. Un comportamento differente è osservabile per il nodo 114, che presenta un valore di betweenness centrality sensibilmente più elevato (0,7169). Tale risultato suggerisce che questo nodo si colloca su numerosi cammini minimi della rete, assumendo un ruolo di intermediazione strutturale.

3.2.4 Eigenvector Centrality

Tabella 3.4: Eigenvector Centrality per i Nodi 52 e 53

Nodo	Eigenvector Centrality
52	0.7066
53	0.7046

Nel contesto dell’attacco DoS, il nodo attaccante presenta un valore di eigenvector centrality molto elevato (0,7066). Questo risultato indica che l’attaccante è direttamente connesso a nodi che rivestono un ruolo centrale nella rete, riuscendo così a collocarsi in una posizione di elevata influenza strutturale senza la necessità di numerose connessioni.

Un comportamento analogo si osserva per il nodo 53, vittima dell’attacco, che mostra un valore di eigenvector centrality altrettanto elevato (0,7046). Anche in questo caso, a fronte di un degree moderato, la vittima risulta connessa a nodi altamente centrali, riflettendo il suo ruolo di punto focale del traffico generato durante l’attacco DoS.

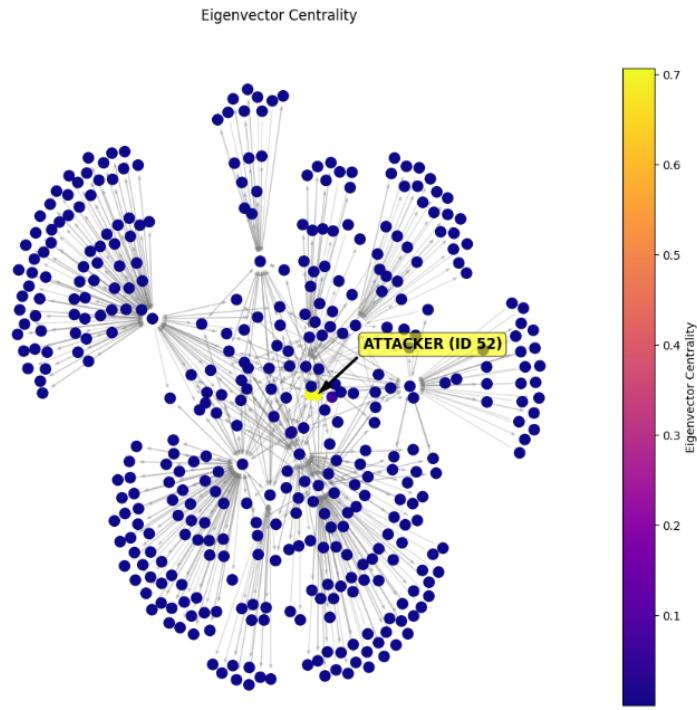


Figura 3.5: Heatmap Eigenvector Centrality

La rappresentazione della heatmap evidenzia una forte concentrazione dei valori di eigenvector centrality su un numero estremamente limitato di nodi. In particolare, il nodo attaccante ID 52 emerge chiaramente per colore e intensità, confermando il valore numerico elevato della metrica e il suo inserimento in una porzione strutturalmente rilevante della rete. La maggior parte dei nodi presenta valori prossimi allo zero, segnalando un ruolo marginale dal punto di vista dell'influenza strutturale. Questo comportamento è coerente con la dinamica tipica di un attacco DoS: pochi nodi centrali (attaccante e vittima) risultano connessi a nodi che, a loro volta, non contribuiscono alla diffusione strutturale del traffico.

3.2.5 Riassunto finale

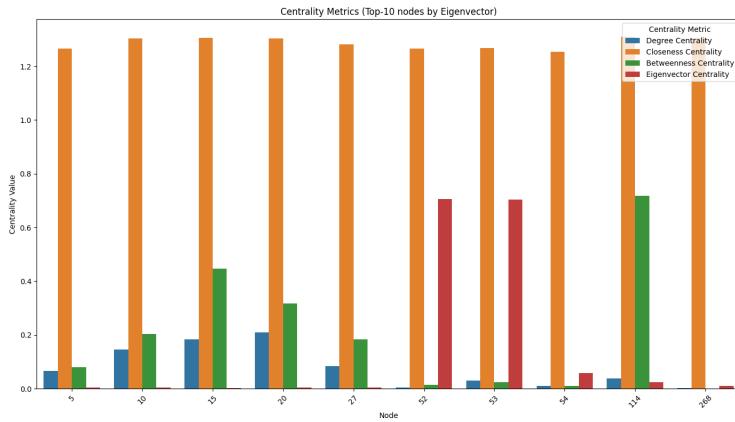


Figura 3.6: Grafico riassuntivo

Il grafico riassuntivo mostra le principali metriche di centralità limitatamente ai nodi con i valori più elevati di eigenvector centrality, scelta motivata dalla necessità di includere esplicitamente il nodo attaccante (ID 52) e la vittima principale (ID 53), che risultano strutturalmente rilevanti secondo questa metrica. Dal confronto emerge che l'attaccante e la vittima presentano valori elevati di closeness ed eigenvector centrality, indicando una posizione centrale rispetto ai cammini minimi e una connessione con nodi a loro volta rilevanti. Al contrario, degree e betweenness centrality rimangono contenute, coerentemente con una dinamica DoS in cui non vi è funzione di intermediazione né coordinazione tra più sorgenti; Inoltre la vittima mostra un degree leggermente superiore rispetto all'attaccante, riflettendo il ruolo di endpoint che riceve un numero maggiore di connessioni.

3.3 Analisi delle strutture

Dopo lo studio delle centralità, l'analisi strutturale consente di approfondire la forma e l'organizzazione locale e globale della rete, mettendo in evidenza

schemi ricorrenti di connessione, livelli di coesione e ruoli operativi dei nodi coinvolti nell'attacco DoS.

3.3.1 Analisi delle comunità

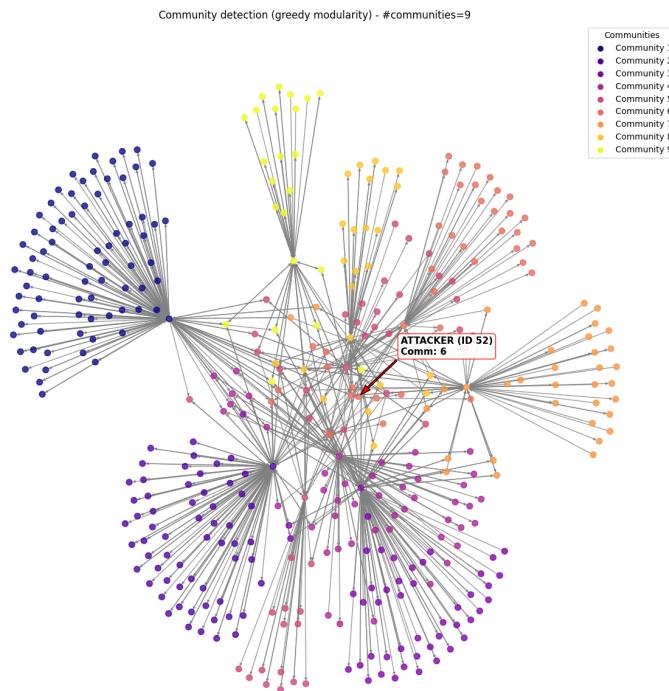


Figura 3.7: Analisi delle comunità

L'algoritmo di community detection individua 9 comunità all'interno della componente principale del grafo. Le comunità risultano prevalentemente organizzate attorno a nodi centrali che fungono da hub locali, con numerosi nodi periferici scarsamente interconnessi tra loro.

Il nodo attaccante (ID 52) appartiene a una specifica comunità (Comm. 6) e si colloca in una posizione strutturalmente rilevante all'interno di essa. Tuttavia, non emerge una vera separazione funzionale tra comunità “attaccanti” e “vittime” : le comunità riflettono principalmente raggruppamenti topologici indotti dal traffico piuttosto che forme di coordinazione malevola.

3.3.2 Triadi

Tabella 3.5: Analisi delle Triadi: Statistiche della Rete Generale

Descrizione	Conteggio Totale
Triadi Chiuse	15
Triadi Aperte	16.263

Tabella 3.6: Focus Analitico sulle Triadi: Nodo 52

Parametro	Valore
Triadi Totali	1
Triadi Chiuse	0
Triadi Aperte	1
Percentuale di Chiusura	0.00%

L'analisi triadica della rete evidenzia una struttura estremamente povera di chiusura. A livello globale, il numero di triadi aperte è nettamente predominante rispetto alle triadi chiuse, confermando una rete scarsamente coesa e priva di relazioni reciproche tra i nodi periferici.

Focalizzando l'attenzione sull'attaccante (ID 52), si osserva la presenza di una sola triade, esclusivamente aperta, che coinvolge la vittima e un ulteriore nodo.



Figura 3.8: Visualizzazione delle triadi dell’attaccante

3.3.3 Clique

Tabella 3.7: Analisi Generale delle Clique nella Rete

Parametro	Valore
Numero Totale di Clique	509
Dimensione Massima Clique (Benign)	3
Esempio Clique Principale	[1, 114, 113]

Tabella 3.8: Analisi delle Clique: Focus Nodo 52

Parametro	Valore
Partecipazione in Clique (n.)	2
Dimensione Massima Clique	2
Parte della Clique Principale	NO

L’analisi delle clique mostra che la rete presenta un numero complessivo elevato di clique, ma tutte di dimensione molto ridotta. La clique massima, di dimensione 3, è osservata esclusivamente in porzioni di traffico benigno e rappresenta interazioni locali tra nodi non coinvolti nell’attacco. Focalizzandosi

sull'attaccante (ID 52), si osserva che il nodo partecipa a sole 2 clique, entrambe di dimensione 2, riconducibili a semplici coppie di nodi. Questi risultati confermano che, nel contesto dell'attacco DoS, non emergono strutture di cooperazione o coordinazione tra più nodi. Le clique individuate che coinvolgono l'attaccante sono limitate a relazioni dirette attaccante–vittima,

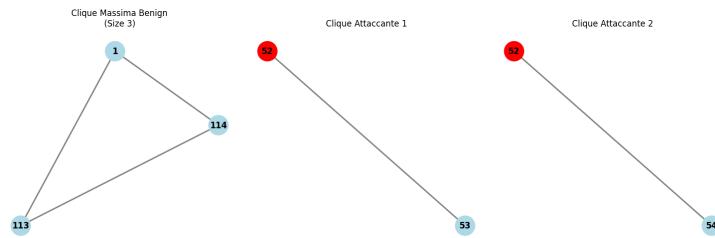


Figura 3.9: Visualizzazione delle Clique dell'attaccante

3.3.4 K-Core

Tabella 3.9: Analisi Generale della Distribuzione K-Core

Livello del Core (k)	Numero di Nodi
$k = 1$	398
$k = 2$	70
$k = 3$	38
$k = 4$	24
$k = 5$	20

Tabella 3.10: Posizionamento e Gerarchia del Nodo 52

Parametro	Valore
K-core massimo della rete	5
K-core di appartenenza (Nodo 52)	2
Appartenenza al Largest K-Core	NO

L'analisi del k-core consente di valutare il livello di integrazione strutturale dei nodi, identificando il nucleo più denso e coeso della rete. Nel caso in esame,

la distribuzione dei k-core mostra una progressiva riduzione del numero di nodi all'aumentare di k , fino a un core massimo pari a $k = 5$, composto da un insieme ristretto di nodi fortemente interconnessi, riconducibili a traffico prevalentemente benigno.

L'attaccante risulta collocato in un guscio $k = 2$, insieme a pochi altri nodi, tra cui la vittima. Questo posizionamento indica che, pur generando un numero significativo di connessioni, l'attaccante non partecipa alla struttura più coesa della rete e rimane separato dal core principale.

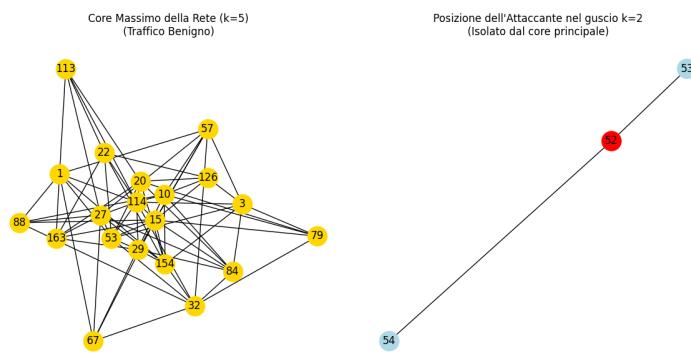


Figura 3.10: Visualizzazione del K-Core dell'attaccante e quello massimo

3.3.5 Ego Network

Tabella 3.11: Analisi della Ego-Network: Nodo 52

Parametro	Valore
Vicini Diretti (Nodi raggiunti)	3
Archi Totali nella Ego-net	2
Densità Locale	Bassa

L'ego-network dell'attaccante (Nodo 52) evidenzia una struttura estremamente semplice e poco articolata, composta da 3 nodi complessivi e 2 archi. Il nodo 52 risulta connesso unicamente alle due controparti principali (i nodi 53 e 54), senza relazioni secondarie tra i vicini né ulteriori ramificazioni.

Dal punto di vista strutturale, ciò indica che l'attaccante non è inserito in un contesto locale denso, ma opera attraverso connessioni dirette e mirate verso le vittime, coerentemente con un attacco DoS di tipo diretto. L'assenza di legami tra i nodi dell'intorno conferma inoltre una bassa densità locale, escludendo dinamiche di coordinamento complesso o cooperazione tra più nodi attaccanti. L'ego-network del Nodo 53 mostra invece una struttura più estesa e articolata, con 13 nodi e 22 archi, caratterizzata da numerose connessioni tra i vicini. Questa configurazione è tipica di un nodo di servizio legittimo, inserito nel core del traffico benigno, che interagisce regolarmente con più host della rete. L'ego-network del Nodo 54, invece, risulta limitato ma non isolato, con 5 nodi e 4 archi. La struttura è semplice e lineare, indicativa di un host legittimo con basso carico di comunicazioni, coinvolto nell'attacco DoS come vittima secondaria ma non centrale nella topologia della rete.

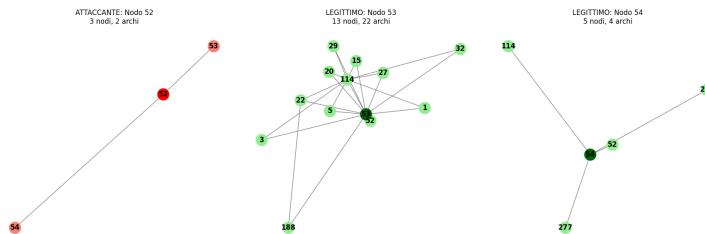


Figura 3.11: Visualizzazione dell'Ego Network dell'attaccante e dei suoi 2 vicini

Capitolo 4

Benign

L’analisi del traffico BENIGN viene introdotta con l’obiettivo di fornire una baseline strutturale di riferimento per la rete, utile al confronto con i comportamenti osservati negli scenari di attacco precedentemente analizzati. Il traffico benigno rappresenta il funzionamento ordinario della rete, in assenza di attività malevole, e consente di evidenziare come le metriche di centralità e le strutture topologiche si distribuiscano in condizioni operative normali.

Anche in questo caso, il grafo è stato costruito applicando le stesse metodologie adottate per gli attacchi, al fine di garantire la piena confrontabilità dei risultati. Tuttavia, l’analisi viene mantenuta volutamente più sintetica, concentrando sugli aspetti strutturali più significativi e sulle differenze rispetto ai pattern tipici degli attacchi DoS e Botnet.

4.1 Analisi descrittiva

Per il traffico BENIGN è stata condotta un’analisi descrittiva applicando le stesse procedure di preprocessing e costruzione del grafo utilizzate per gli scenari di attacco. In particolare, dopo l’individuazione della finestra temporale di interesse, i flussi di rete sono stati aggregati per costruire un grafo orientato e pesato, al fine di analizzare la struttura della rete in condizioni operative

normali.

4.1.1 Parametri del grafo

Il grafo relativo al traffico BENIGN è composto da 736 nodi e 1 528 archi, dimensioni superiori rispetto agli scenari di attacco analizzati in precedenza, a testimonianza di una maggiore varietà di host coinvolti e di interazioni distribuite nel tempo. La densità del grafo diretto, pari a 0,002825, indica una rete complessivamente sparsa, coerente con un traffico legittimo in cui le comunicazioni sono distribuite su più coppie di nodi senza una concentrazione eccessiva.

Il grafo non risulta connesso, né in senso debole né in senso forte, evidenziando la presenza di più componenti separate, tipiche di una rete reale in cui non tutti gli host comunicano tra loro all'interno della finestra temporale considerata.

Il coefficiente di clustering medio, calcolato sulla versione non diretta del grafo, assume un valore pari a 0,0114, superiore a quello osservato nello scenario DoS e comparabile, seppur inferiore, a quello riscontrato nella botnet. Questo valore suggerisce una maggiore presenza di interazioni locali rispetto agli attacchi centralizzati, pur senza indicare una struttura fortemente coesa o caratterizzata da sottostrutture densamente interconnesse.

Le misure di raggio e diametro, calcolate sulla componente connessa più grande utilizzando una distanza inversamente proporzionale al peso degli archi, risultano rispettivamente pari a 1,2 e 2,34. Tali valori indicano una rete poco profonda, in cui la maggior parte dei nodi è raggiungibile in pochi passi, coerentemente con un traffico ordinario privo di colli di bottiglia strutturali. I nodi appartenenti alla periferia rappresentano host marginali, coinvolti in comunicazioni sporadiche e non centrali nella dinamica complessiva della rete.

4.1.2 Visualizzazione del grafo

Per il traffico benigno vengono riportate solo 2 visualizzazioni del grafo, in quanto le differenti modalità di layout non introducono variazioni interpretative significative rispetto a quanto già osservato negli scenari di attacco. La rappresentazione scelta è sufficiente a evidenziare la struttura distribuita e l'assenza di nodi dominanti. La visualizzazione del grafo relativo al traffico benigno tramite **spring layout** evidenzia una struttura complessivamente distribuita, priva di nodi dominanti chiaramente identificabili. Le connessioni risultano diffuse su un numero elevato di nodi, con una concentrazione centrale dovuta alla componente connessa principale, ma senza la marcata centralizzazione osservata negli scenari di attacco. Tale configurazione è coerente con un traffico legittimo, caratterizzato da interazioni eterogenee e non orchestrate.

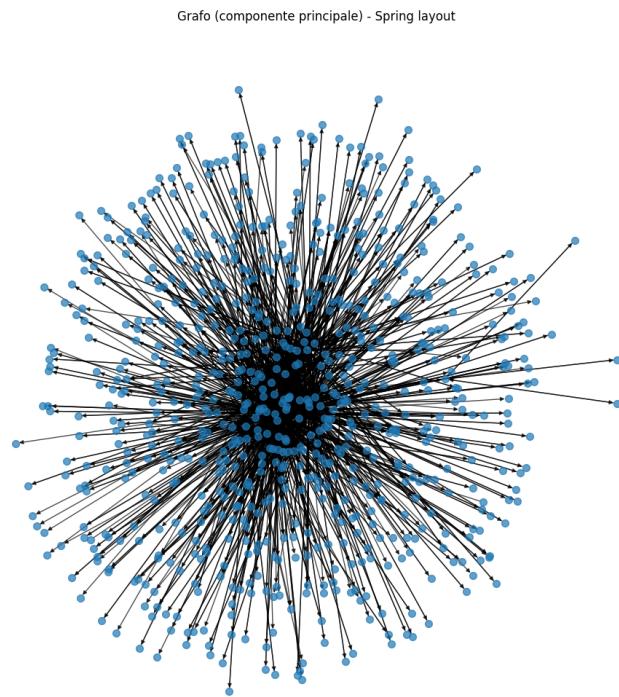


Figura 4.1: Visualizzazione Spring Layout

Il **Kamada–Kawai layout**, pur restituendo una rappresentazione più compatta della componente principale, conferma le stesse evidenze strutturali.

rali: l'assenza di hub isolati o di pattern a stella suggerisce una rete in cui i flussi sono distribuiti tra più host senza un punto di controllo o di pressione univoco. I pochi nodi periferici risultano distanti dal nucleo centrale, indicando comunicazioni sporadiche o marginali, tipiche di un contesto operativo ordinario.

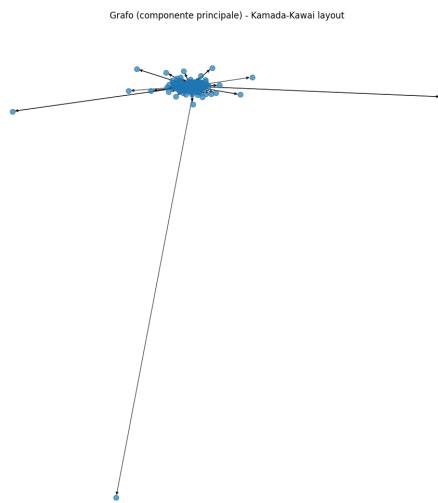


Figura 4.2: Visualizzazione Kamada-Kawai layout

4.2 Analisi delle centralità

Per il traffico benigno, l'analisi delle centralità è stata condotta in forma volutamente sintetica. In assenza di comportamenti anomali o nodi malevoli, l'obiettivo non è l'individuazione di outlier critici, bensì la caratterizzazione statistica globale della rete. Di conseguenza, l'attenzione è posta principalmente sulle distribuzioni dei valori e su pochi nodi rappresentativi, evitando analisi di dettaglio non informative ai fini del confronto con gli scenari di attacco.

Tabella 4.1: Top 5 Nodi per Degree Centrality

Nodo	In-Degree Centrality	Out-Degree Centrality	Degree Centrality
1	0.3697	0.4638	0.4652
3	0.1896	0.2756	0.2756
12	0.0859	0.1091	0.1091
7	0.0587	0.0668	0.0668
36	0.0314	0.0587	0.0655

Tabella 4.2: Bottom 5 Nodi per Degree Centrality

Nodo	In-Degree Centrality	Out-Degree Centrality	Degree Centrality
292	0.0014	0.0014	0.0014
293	0.0014	0.0014	0.0014
294	0.0014	0.0000	0.0014
295	0.0014	0.0000	0.0014
733	0.0000	0.0014	0.0014

4.2.1 Degree Centrality

L'analisi dei Top-5 nodi per degree centrality mostra nodi (ad es. 1, 3 e 12) con valori significativamente più alti rispetto alla media. Ciò indica nodi centrali dal punto di vista operativo, ma non necessariamente anomali, tipici di infrastrutture o servizi condivisi. Al contrario, i Bottom-5 nodi presentano valori di degree estremamente ridotti, prossimi allo zero. Questi nodi risultano periferici, scarsamente coinvolti nelle comunicazioni e pienamente compatibili con normali comportamenti di host poco attivi.

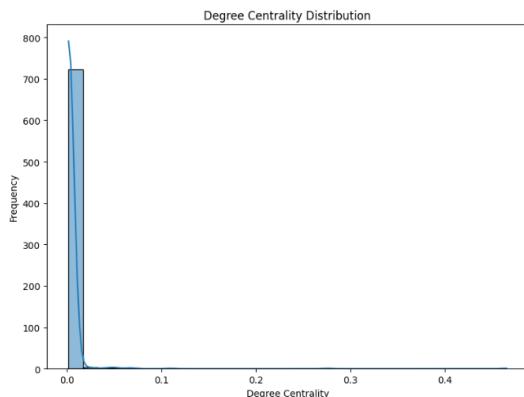


Figura 4.3: Distribuzione della Degree Centrality

Dalla distribuzione della degree centrality emerge una forte asimmetria: la grande maggioranza dei nodi presenta valori molto bassi, mentre solo pochi nodi concentrano un numero elevato di connessioni. Questa struttura è coerente con un traffico benigno, in cui pochi nodi svolgono il ruolo di punti di servizio o aggregazione, mentre la maggior parte degli host mantiene comunicazioni limitate.

4.2.2 Closeness Centrality

Tabella 4.3: Top 5 Nodi per Closeness Centrality

Nodo	Closeness Centrality
183	1.7537
1	1.7534
557	1.7508
12	1.7493
4	1.7401

Tabella 4.4: Bottom 5 Nodi per Closeness Centrality

Nodo	Closeness Centrality
702	0.5721
700	0.5721
698	0.5721
694	0.5721
699	0.5721

I nodi con valori di closeness più elevati, come i nodi 183, 1, 557 e 12, risultano strutturalmente ben posizionati all'interno della componente principale. In particolare, il nodo 1 combina un'elevata closeness con un'elevata degree, confermandosi come nodo centrale naturale del traffico benigno. Al contrario, il nodo 557 presenta una closeness molto alta pur avendo un grado minimo, evidenziando come la closeness catturi una proprietà globale della rete indipendente dalla semplice numerosità delle connessioni dirette.

I nodi con i valori di closeness più bassi, tra cui 694, 698, 699, 700 e 702, mostrano valori identici e prossimi al minimo, associati a degree estremamente ridotto e betweenness nulla. Questi nodi risultano chiaramente collocati in posizioni periferiche della rete, in linea con quanto già emerso dall'analisi della periferia e del diametro della componente connessa principale.

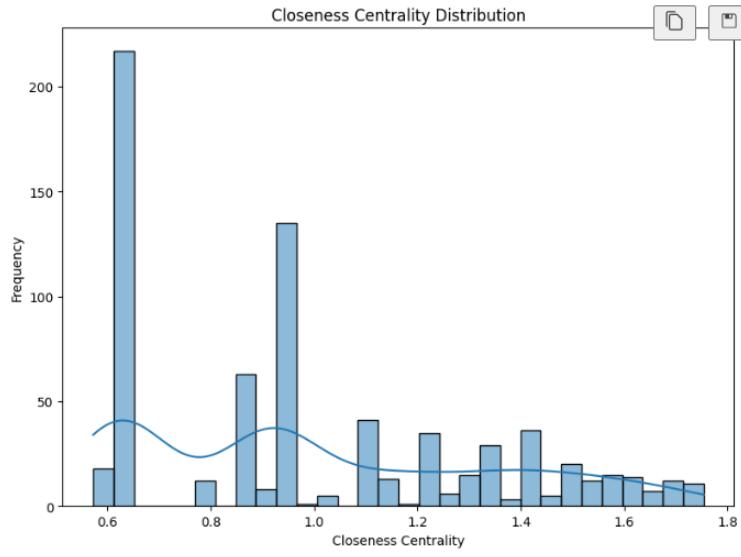


Figura 4.4: Closeness Centrality

La distribuzione della closeness centrality mostra una marcata eterogeneità dei valori, con una maggiore dispersione rispetto a quanto osservato per la degree centrality. Questa caratteristica è coerente con una rete reale e non artificiale, in cui l'accessibilità globale non è concentrata su un singolo nodo ma distribuita tra più elementi con ruoli differenti.

4.2.3 Betweenness Centrality

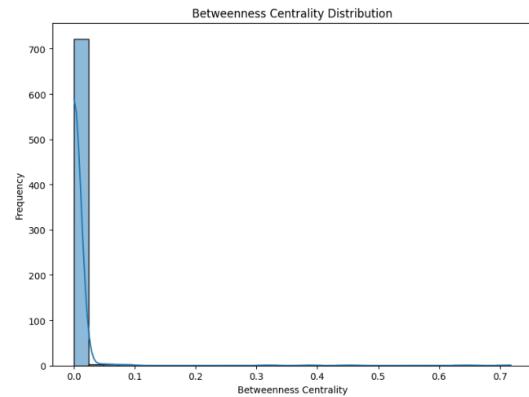


Figura 4.5: Distribuzione della Betweenness Centrality

La distribuzione della betweenness centrality mostra una marcata concentrazione dei valori prossimi allo zero, indicando che la quasi totalità dei nodi non svolge alcun ruolo di intermediazione nei cammini minimi della rete. Solo un numero estremamente ridotto di nodi presenta valori significativamente più elevati, fungendo da punti di passaggio privilegiati tra porzioni diverse del grafo. Questo comportamento è tipico di una rete benigna, in cui l'instradamento del traffico è affidato a pochi nodi centrali e non emergono schemi di instradamento forzato o anomalo.

4.2.4 Eigenvector Centrality

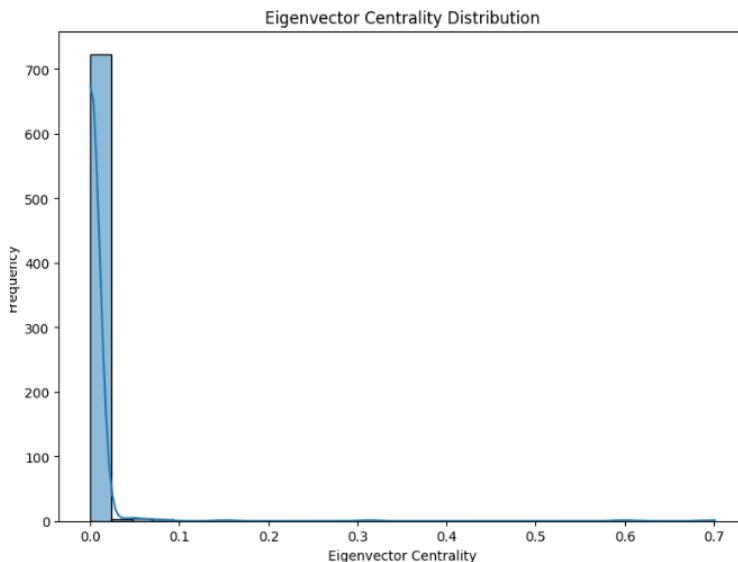


Figura 4.6: Distribuzione della Eigenvector Centrality

La distribuzione della eigenvector centrality evidenzia una struttura fortemente sbilanciata, con la maggior parte dei nodi caratterizzata da valori molto bassi. Ciò indica che la rete è composta prevalentemente da nodi collegati a elementi strutturalmente poco rilevanti, mentre solo pochi nodi risultano connessi ad altri nodi centrali. Questo pattern è coerente con una topologia legittima, in cui l'importanza strutturale è concentrata su un insieme ristretto

di nodi di servizio, senza la presenza di concentrazioni anomale riconducibili a comportamenti malevoli.

4.3 Analisi delle strutture

L'analisi delle strutture di rete è finalizzata a caratterizzare l'organizzazione interna del traffico benigno, verificando l'assenza di pattern riconducibili a comportamenti coordinati o malevoli. A differenza dei casi di attacco, l'obiettivo non è individuare nodi anomali, ma descrivere una struttura coerente, distribuita e funzionalmente stabile, tipica di comunicazioni legittime.

4.3.1 Analisi delle comunità

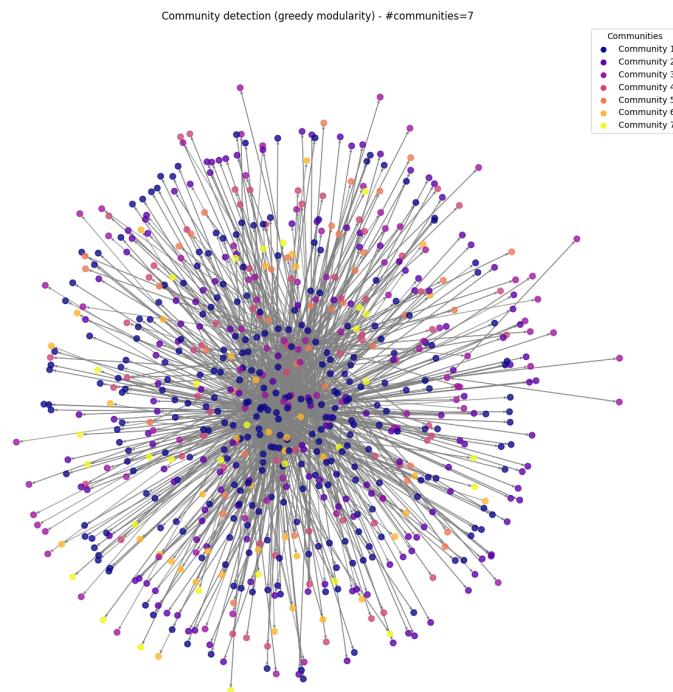


Figura 4.7: Analisi delle comunità

L'analisi delle comunità evidenzia la presenza di 7 comunità all'interno della componente principale della rete. La suddivisione non mostra comunità netta-

mente separate o isolate, ma gruppi parzialmente sovrapposti che convergono verso un nucleo centrale ad alta densità di connessioni. Dal punto di vista strutturale, questa configurazione è coerente con un traffico benigno: le comunità riflettono insiemi di nodi che comunicano più frequentemente tra loro (ad esempio servizi, client o sottoreti funzionali), senza però presentare una frammentazione rigida o una separazione marcata.

4.3.2 Triadi

Tabella 4.5: Analisi Globale delle Triadi nella Rete

Tipologia di Triade	Conteggio Totale
Triadi Chiuse	59
Triadi Aperte	86.548
Totale Triadi	86.607

L'analisi delle triadi mostra una netta prevalenza di triadi aperte (86 548) rispetto alle triadi chiuse (59), a fronte di un numero molto elevato di triple connesse (86 607).

Questa distribuzione indica una rete poco transitiva, in cui i nodi tendono a collegarsi tramite catene lineari piuttosto che formare piccoli gruppi fortemente interconnessi. Dal punto di vista strutturale, il risultato è coerente con un traffico benigno, caratterizzato da comunicazioni funzionali punto-punto e da un'assenza di micro-strutture collaborative o coordinamenti chiusi tipici di comportamenti anomali o malevoli.

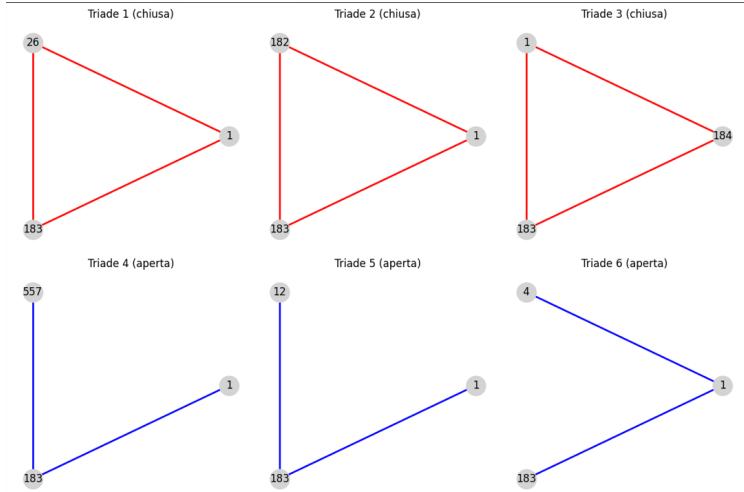


Figura 4.8: Visualizzazione di alcune triadi

4.3.3 Clique

Tabella 4.6: Analisi Generale delle Clique nella Rete

Parametro Strutturale	Valore
Numero Totale di Clique	843
Dimensione Massima Clique	5

L'analisi delle clique evidenzia la presenza di 843 clique complessive, con una dimensione massima pari a 5 nodi. Le clique di dimensione maggiore condividono in gran parte gli stessi elementi centrali (in particolare i nodi 26, 182, 183 e 184), a indicare gruppi ristretti di host fortemente interconnessi.

Dal punto di vista strutturale, la presenza di clique di piccola dimensione e limitate numericamente è coerente con scenari di traffico benigno, in cui pochi nodi (ad esempio server o servizi condivisi) concentrano comunicazioni reciproche, senza però formare strutture estese o pattern di coordinazione anomala tipici di attività malevole organizzate.

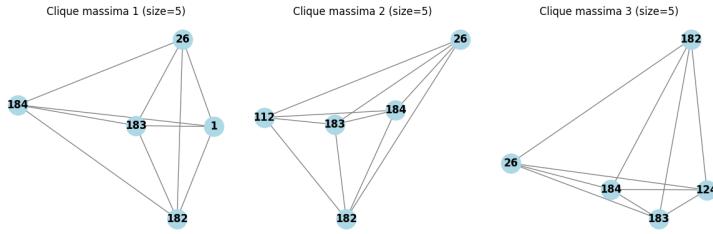


Figura 4.9: Visualizzazione delle Cliques

4.3.4 K-Core

Tabella 4.7: Analisi Generale della Distribuzione K-Core

Livello del Core (k)	Numero di Nodi
$k = 1$	734
$k = 2$	96
$k = 3$	41
$k = 4$	23
$k = 5$	18

Tabella 4.8: Statistiche di Coreness Massima

Parametro	Valore
K-core massimo della rete	5
Nodi nel Core principale ($k = 5$)	18

L’analisi k-core mostra una rete fortemente sbilanciata verso i core periferici: la quasi totalità dei nodi appartiene ai k-core bassi ($k = 1$ e $k = 2$), mentre solo 18 nodi risultano nel core massimo ($k = 5$). Questo indica che la maggior parte degli host ha poche connessioni reciproche stabili, tipico di traffico benigno non coordinato.

Il largest k-core ($k = 5$) è composto da un insieme ristretto di nodi (tra cui 1, 26, 182, 183, 184, 112), che coincidono con quelli emersi anche nell’analisi delle clique. Tali nodi rappresentano il nucleo strutturale della rete, caratterizzato

da interazioni più dense e reciproche, verosimilmente riconducibili a servizi centrali o infrastrutture condivise, senza evidenze di isolamento o penetrazione anomala da parte di nodi sospetti.

Sottografo 5-core (componente principale, non diretto)

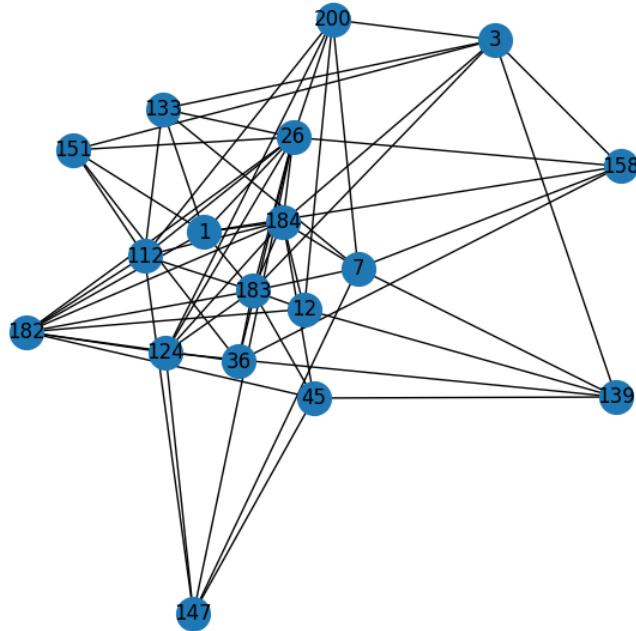


Figura 4.10: Visualizzazione del K-Core

4.3.5 Ego Network

Tabella 4.9: Analisi delle Ego-Networks per i Nodi Principali

ID Nodo (Ego)	Nodi (Size)	Archi (Edges)	Densità Locale
1	342	354	Media-Bassa
3	203	203	Nulla
12	81	83	Bassa

L'ego-network del nodo 1 è estremamente ampio (342 nodi, 354 archi) e presenta una struttura molto estesa, indice di un nodo altamente integrato e connesso a una porzione significativa della rete. Questo comportamento è

coerente con un nodo infrastrutturale o di servizio, che funge da punto di aggregazione per numerose comunicazioni lecite.

L'ego-network del nodo 3 (203 nodi, 203 archi) mostra una dimensione rilevante ma più contenuta rispetto al nodo 1. La struttura risulta meno densa, suggerendo un ruolo centrale ma secondario, compatibile con un nodo di supporto o instradamento all'interno del traffico benigno.

Infine, l'ego-network del nodo 12 (81 nodi, 83 archi) evidenzia un intorno locale significativamente più ridotto, pur mantenendo una connettività coerente. Questo profilo indica un nodo ben connesso ma non dominante, inserito nel core della rete senza assumere un ruolo di hub principale.

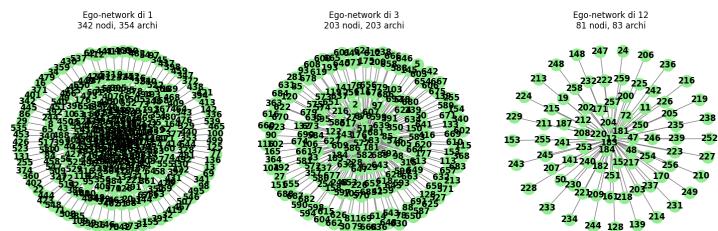


Figura 4.11: Visualizzazione dell'Ego Network