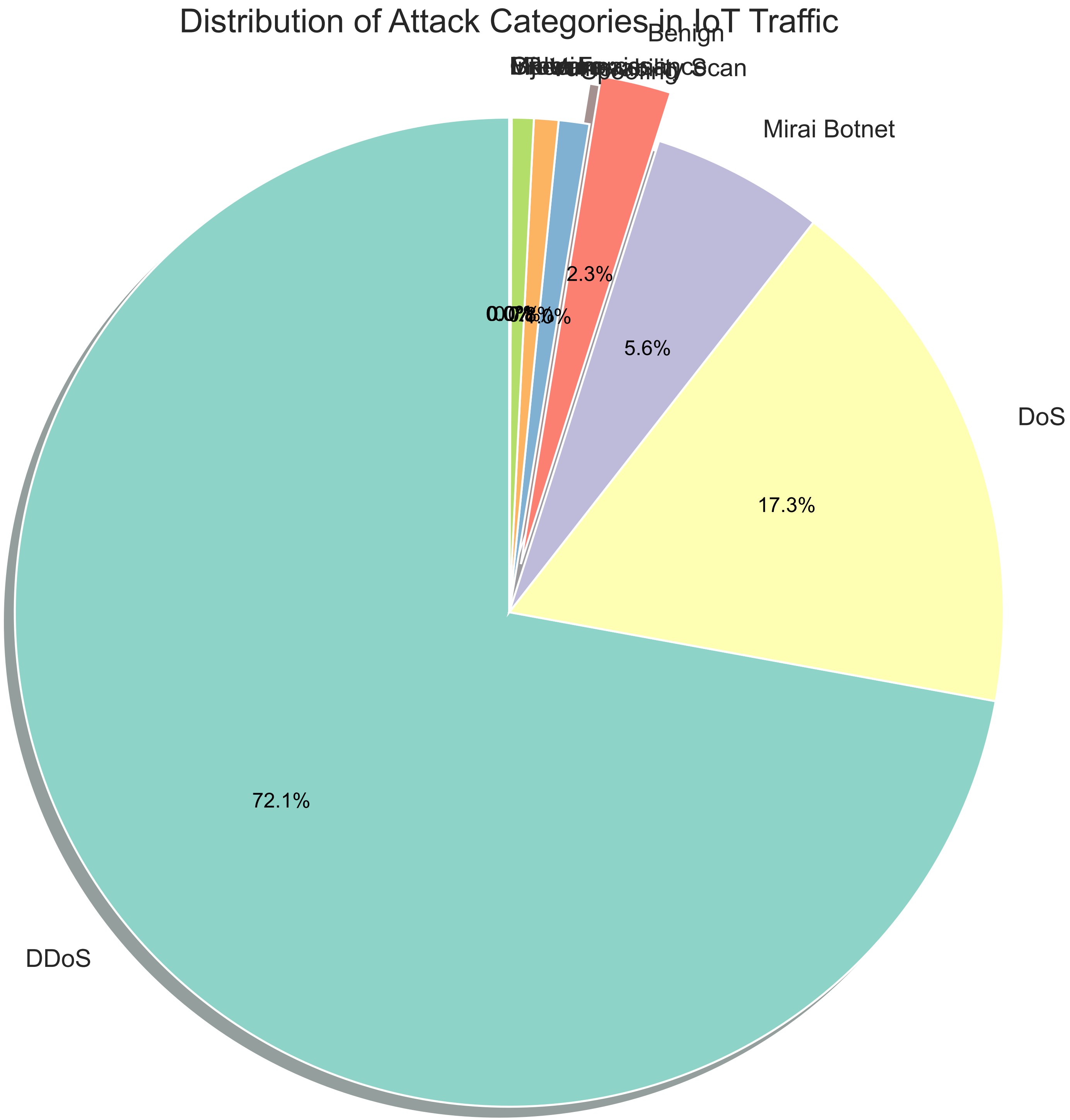
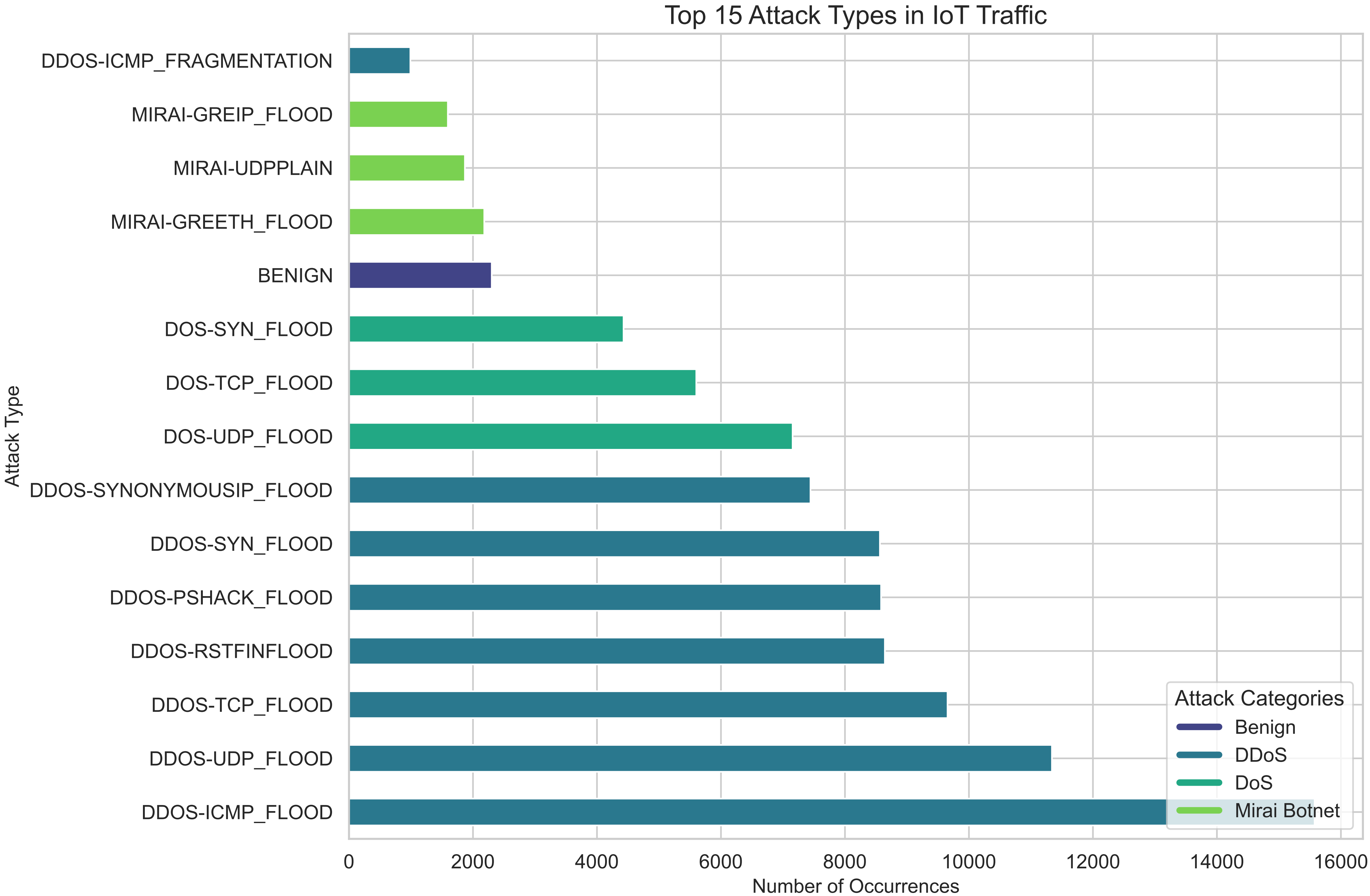
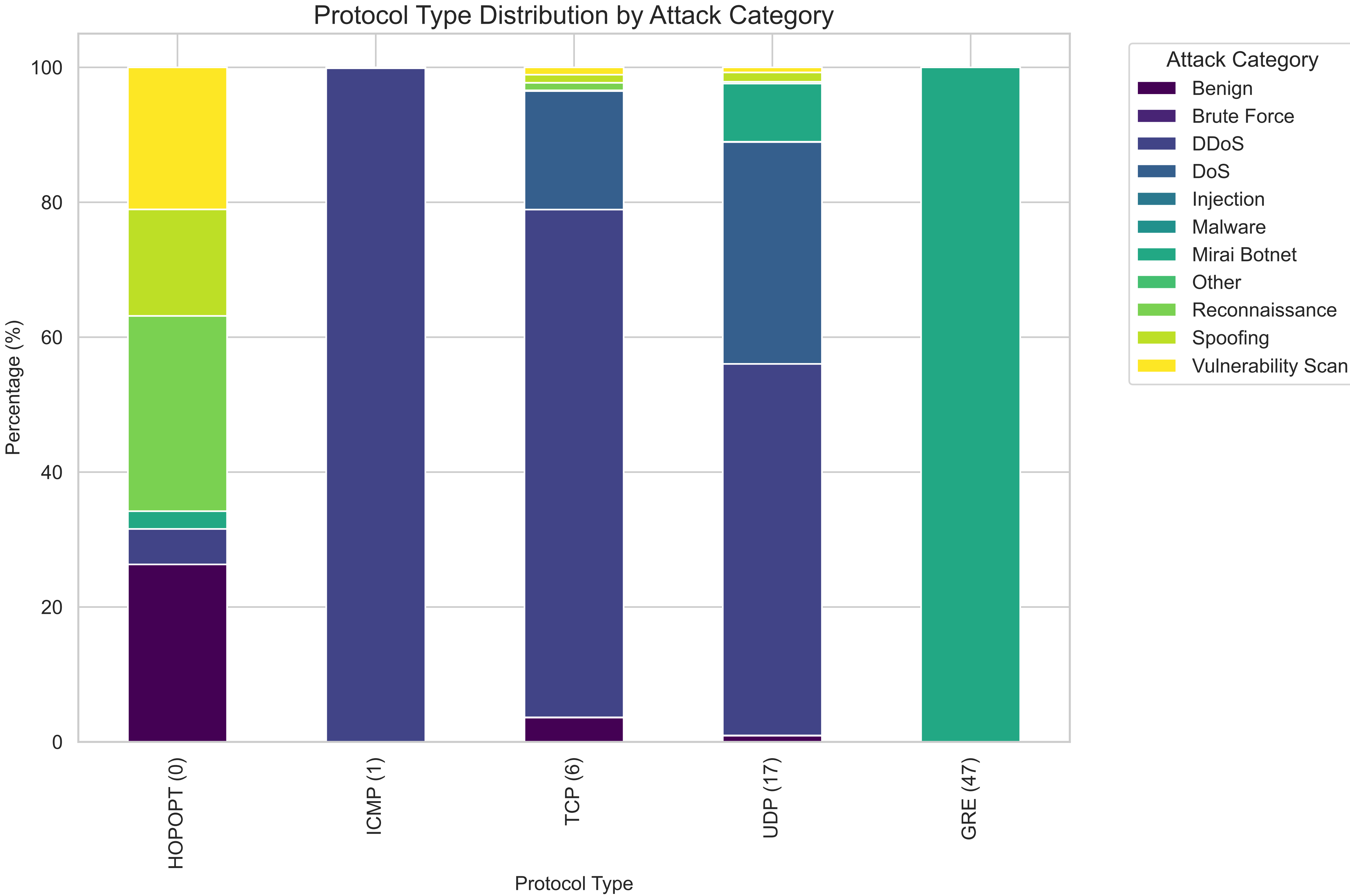

Distribution of Attack Categories in IoT Traffic
Benign
Mirai Botnet
DoS
DDoS
2.3%
5.6%
17.3%
72.1%

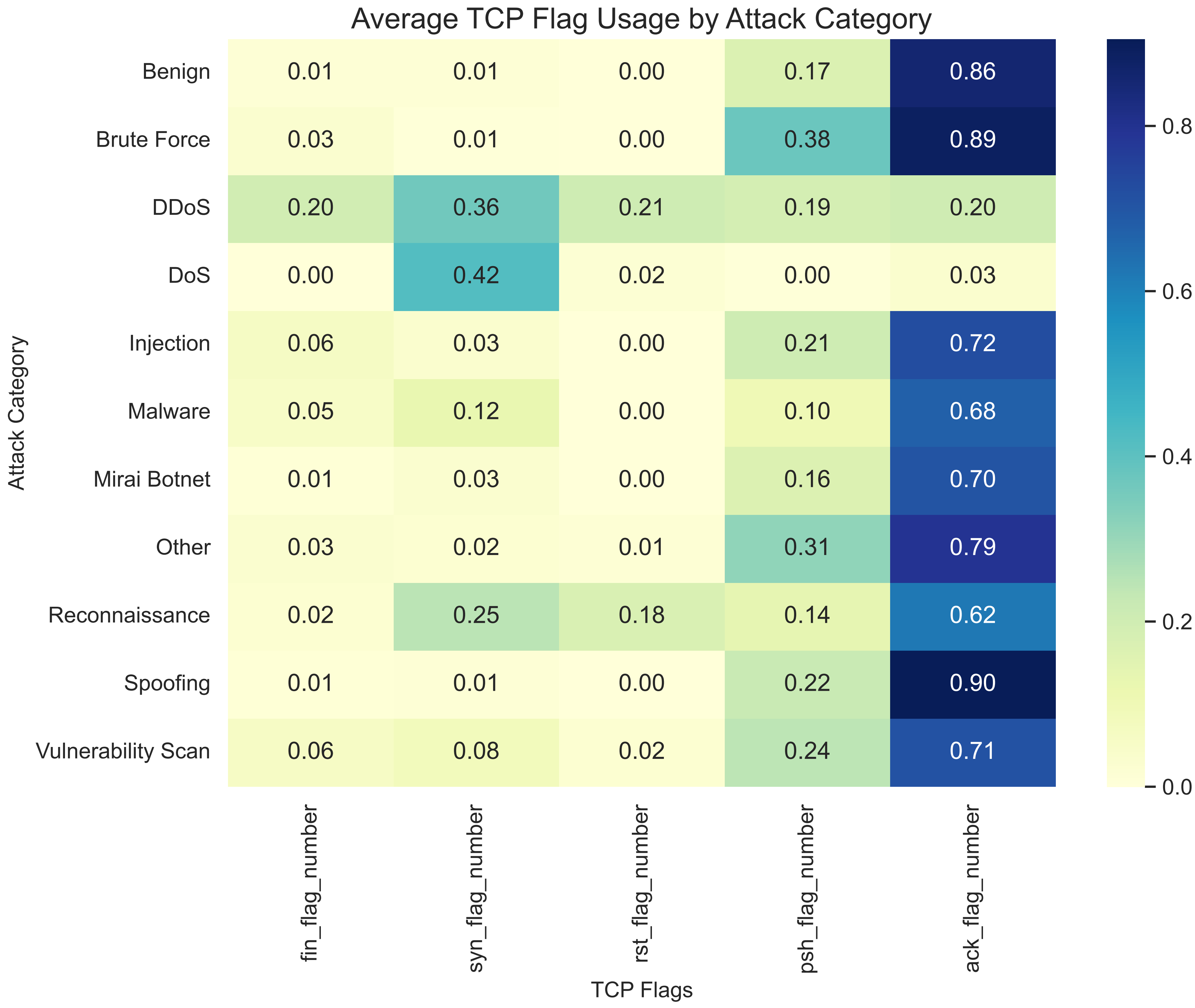
This pie chart illustrates the distribution of different attack categories in our IoT traffic sample. The predominance of DDoS attacks (shown in large segments) indicates their prevalence in IoT environments,
likely due to the ease of compromising numerous IoT devices to form botnets. The relatively small proportion of benign traffic (highlighted by the slight separation from the pie) demonstrates the imbalanced nature of our dataset, which is common in security datasets where attack traffic is deliberately collected. For SMEs, this visualization emphasizes the importance of implementing DDoS protection mechanisms as a primary security control for their IoT deployments.


Top 15 Attack Types in IoT Traffic
Attack Type
DDOS-ICMP_FRAGMENTATION
MIRAI-GREIP_FLOOD
MIRAI-UDPPLAIN
MIRAI-GREETH_FLOOD
BENIGN
DOS-SYN_FLOOD
DOS-TCP_FLOOD
DOS-UDP_FLOOD
DDOS-SYNONYMOUSIP_FLOOD
DDOS-SYN_FLOOD
DDOS-PSHACK_FLOOD
DDOS-RSTFINFLOOD
DDOS-TCP_FLOOD
DDOS-UDP_FLOOD
DDOS-ICMP_FLOOD
0
2000
4000
6000
8000
10000
12000
14000
16000
Number of Occurrences
Attack Categories
Benign
DDoS
DoS
Mirai Botnet

This horizontal bar chart presents the top 15 most frequent attack types in our IoT traffic sample, color-coded by their broader attack categories. The predominance of different DDOS attack variants (particularly ICMP_FLOOD, UDP_FLOOD, and TCP_FLOOD) illustrates the diverse tactics attackers employ to overwhelm IoT networks. The color coding helps visualize the relative frequency of different attack categories, with DDoS attacks (in darker shades) clearly dominating the threat landscape. For SMEs, this visualization emphasizes that they need layered defense mechanisms capable of detecting various flooding techniques, not just protection against a single attack vector.

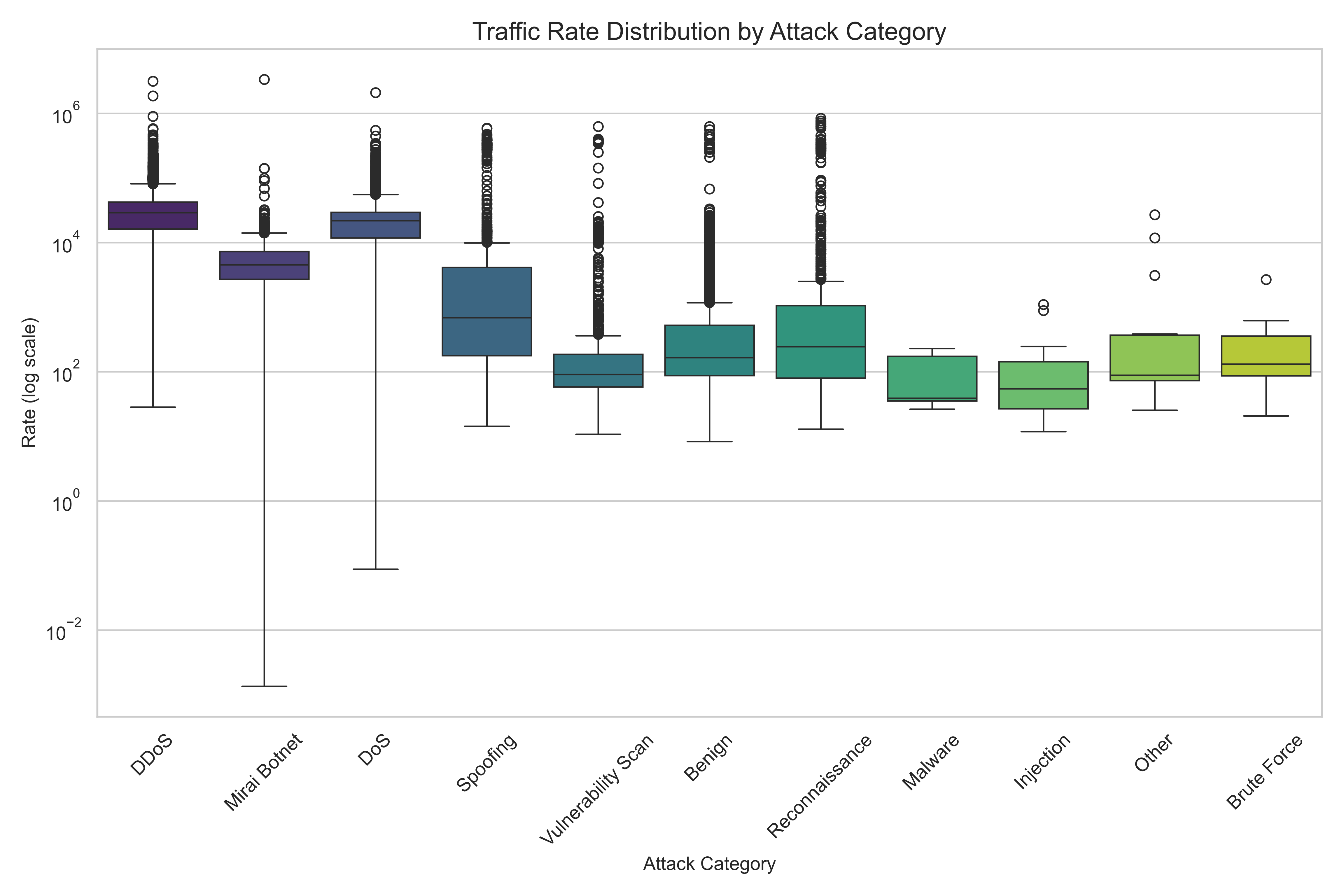

Protocol Type Distribution by Attack Category
Percentage (%)
0
20
40
60
80
100
HOPOPT (0)
ICMP (1)
TCP (6)
UDP (17)
GRE (47)
Protocol Type
Attack Category
Benign
Brute Force
DDoS
DoS
Injection
Malware
Mirai Botnet
Other
Reconnaissance
Spoofing
Vulnerability Scan

This stacked bar chart shows how different attack categories utilize various network protocols. Each bar represents a protocol type, with colored segments showing the proportion of each attack category observed using that protocol. For example, TCP (protocol 6) shows a mix of attack types, while ICMP (protocol 1) is dominated by DDoS attacks. This visualization helps SMEs understand which protocols are most commonly exploited in IoT environments. The chart reveals that some attack types have strong protocol preferences - DDoS attacks frequently leverage ICMP, while reconnaissance activities predominantly use TCP. This information is crucial for configuring network monitoring tools to focus on the most vulnerable protocols for specific threats.



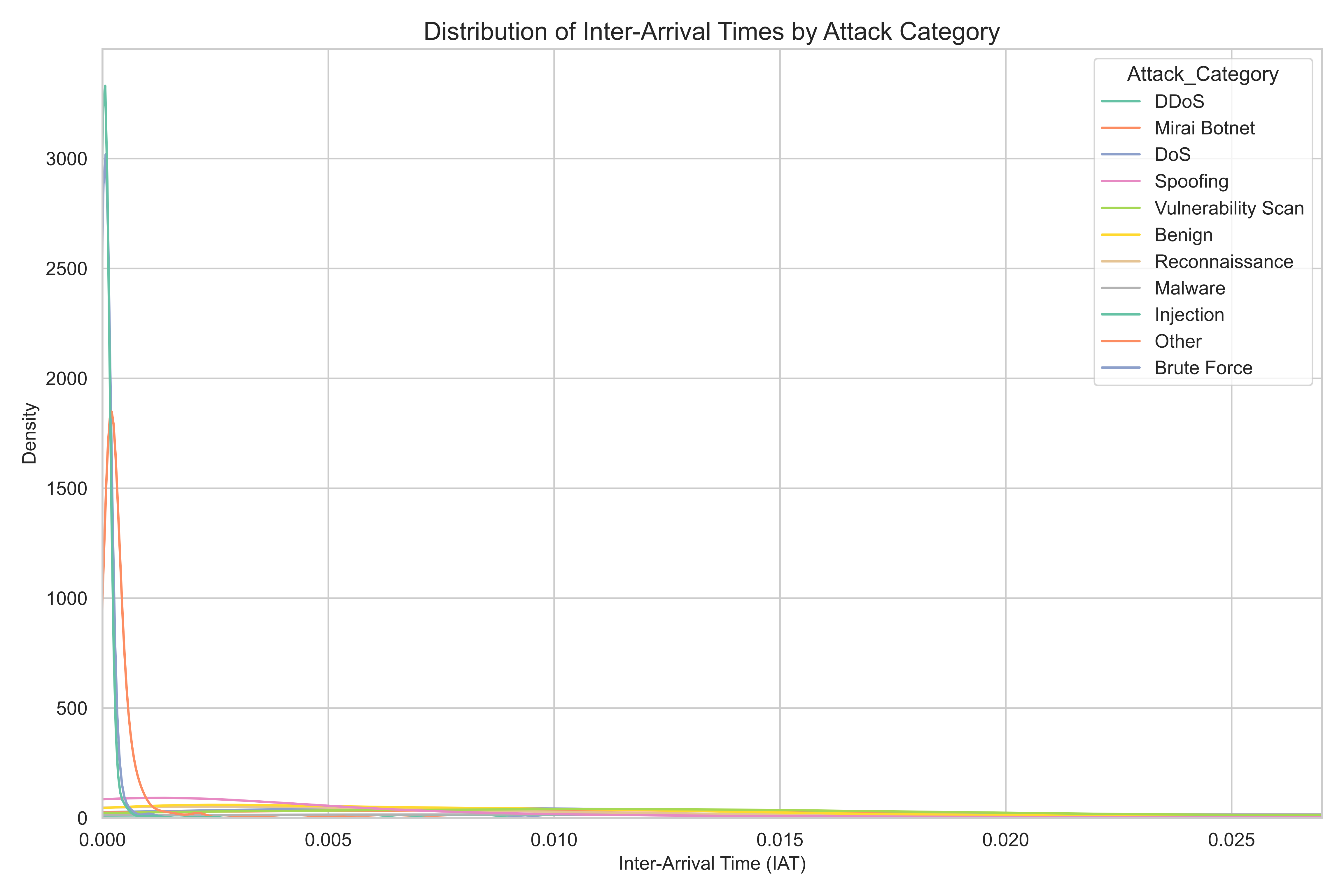
Average TCP Flag Usage by Attack Category
Attack Category
TCP Flags
Benign
Brute Force
DDoS
DoS
Injection
Malware
Mirai Botnet
Other
Reconnaissance
Spoofing
Vulnerability Scan
fin_flag_number
syn_flag_number
rst_flag_number
psh_flag_number
ack_flag_number
0.01 0.01 0.00 0.17 0.86
0.03 0.01 0.00 0.38 0.89
0.20 0.36 0.21 0.19 0.20
0.00 0.42 0.02 0.00 0.03
0.06 0.03 0.00 0.21 0.72
0.05 0.12 0.00 0.10 0.68
0.01 0.03 0.00 0.16 0.70
0.03 0.02 0.01 0.31 0.79
0.02 0.25 0.18 0.14 0.62
0.01 0.01 0.00 0.22 0.90
0.06 0.08 0.02 0.24 0.71
0.0
0.2
0.4
0.6
0.8

This heatmap reveals the average TCP flag usage patterns across different attack categories, providing insight into the network behavior signatures of various attacks. Darker colors indicate higher average flag values. For example, the elevated SYN flag values in DDoS attacks likely indicate SYN flood attacks, while reconnaissance activities show distinctive patterns in RST and ACK flags as they probe for open ports and services. Understanding these flag patterns is vital for SMEs implementing network security monitoring, as they can be used to create effective detection rules for identifying suspicious traffic. The visualization also demonstrates how different attack categories manipulate TCP connections in distinctive ways that diverge from normal benign traffic patterns.



Traffic Rate Distribution by Attack Category
Rate (log scale)
10^6
10^4
10^2
10^0
10^{-2}
DDoS
Mirai Botnet
DoS
Spoofing
Vulnerability Scan
Benign
Reconnaissance
Malware
Injection
Other
Brute Force
Attack Category

This box plot shows the distribution of traffic rates across different attack categories, using a logarithmic scale to accommodate the wide range of values. The boxes represent the interquartile range (IQR) of rates for each category, with the horizontal line showing the median value. Outliers are shown as individual points. DDoS and DoS attacks typically exhibit much higher traffic rates than other categories, as expected from their flooding nature. In contrast, reconnaissance and injection attacks operate at lower rates, making them potentially harder to detect through simple rate-based thresholds. This visualization helps SMEs understand appropriate rate-based thresholds for different types of attacks, informing the configuration of intrusion detection systems and traffic anomaly detection tools.



Distribution of Inter-Arrival Times by Attack Category
Density
Inter-Arrival Time (IAT)
0
500
1000
1500
2000
2500
3000
0.000
0.005
0.010
0.015
0.020
0.025
Attack_Category
DDoS
Mirai Botnet
DoS
Spoofing
Vulnerability Scan
Benign
Reconnaissance
Malware
Injection
Other
Brute Force

This density plot illustrates the distribution of Inter-Arrival Times (IAT) across different attack categories. IAT measures the time between consecutive packets, providing insight into the temporal patterns of different attacks. DDoS and DoS attacks typically show concentrated distributions with very short IATs, reflecting their high-volume, high-frequency nature. In contrast, reconnaissance activities often exhibit more dispersed IAT patterns as they methodically probe the network. Benign traffic generally shows a wider, more natural distribution of inter-arrival times. For SMEs, these distinct temporal signatures can be leveraged in security monitoring systems to identify anomalous traffic patterns that deviate from normal behavior, even when traditional indicators like packet content or header information appear legitimate.