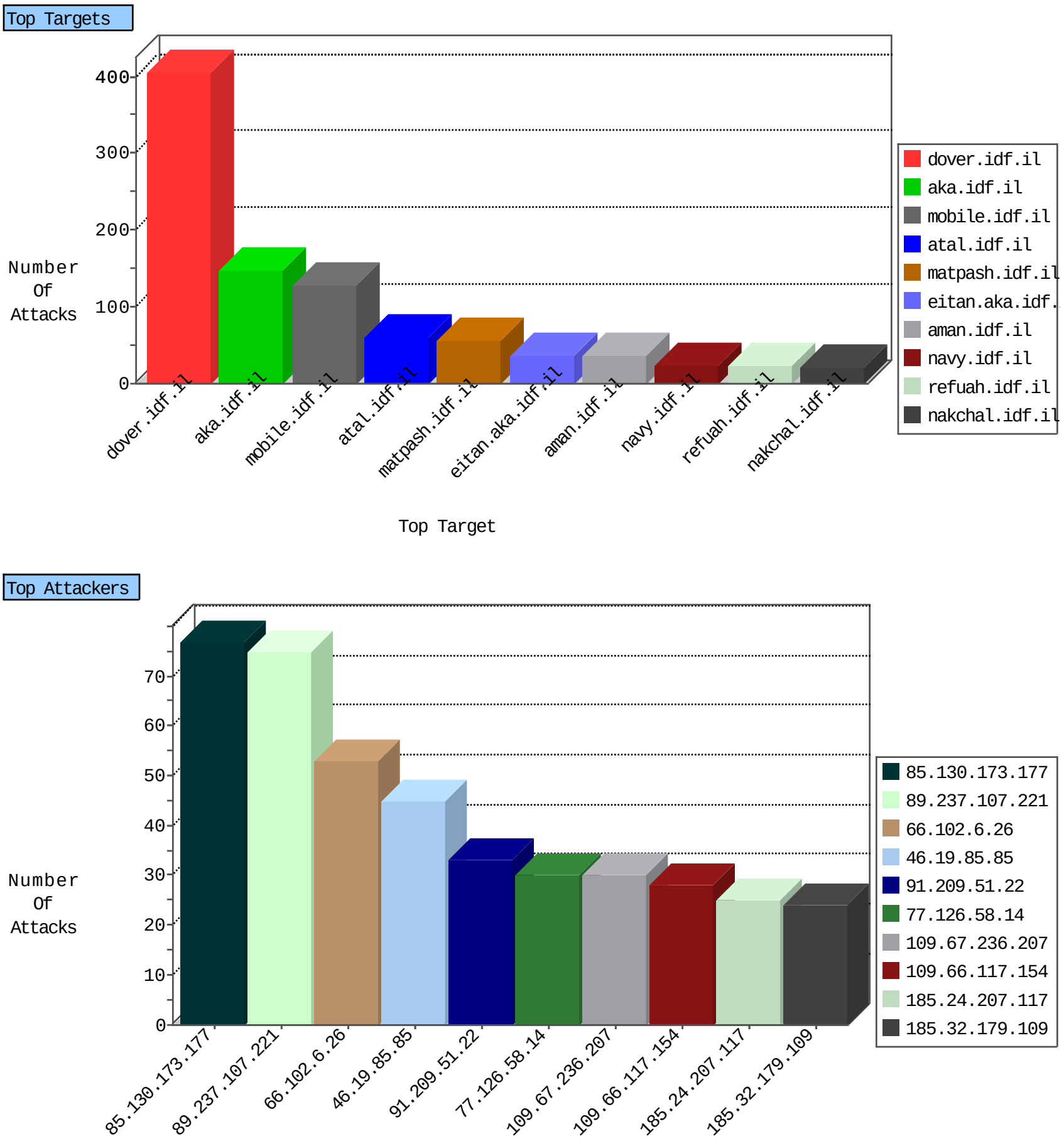
09-18-2016-18:04:06 to 09-18-2016-19:04:06

IDF Under Attack Daily Report



09-18-2016-18:04:06 to 09-18-2016-19:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
222.186.56.24	China	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
142.54.174.85	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
69.30.193.252	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
204.12.220.82	United States	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-18-2016-18:04:06 to 09-18-2016-19:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.209.51.22	Ukraine	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	20
91.209.51.22	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	13

09-18-2016-18:04:06 to 09-18-2016-19:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.102.6.26	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	53
66.249.64.163	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
79.180.193.182	147.237.0.34	Israel	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
46.116.100.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.163.183	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.225.124	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
24.105.159.242	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.131.60	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.29.194.36	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.231.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.193.74.175	147.237.76.147	Gibraltar	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.21.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.243.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.3.147.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.106.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
117.135.131.60	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
24.105.159.242	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.131.60	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.65.41.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.84.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.116.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-18-2016-18:04:06 to 09-18-2016-19:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.237.107.221	France	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
77.126.58.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.67.236.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
109.66.117.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
85.130.173.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
85.130.173.177	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	26
85.130.173.177	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
89.237.107.221	France	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
185.32.179.109	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
160.158.186.119	Tunisia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	22
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
51.235.107.7	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
185.24.207.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
2.55.134.22	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
185.24.207.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
100.92.214.126		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
109.67.198.40	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.19.86.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.253.231.156	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
176.13.231.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.230	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
37.26.148.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	8
212.199.239.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.214	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.32.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
109.253.208.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.85	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.231.152	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.32.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
93.172.103.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.85	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.108.10.175	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
31.154.81.73	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.203.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.139.32.232	France	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.232.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.120.164.181	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.230	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
77.139.32.232	France	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
169.255.184.215	Tanzania, United Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4

09-18-2016-18:04:06 to 09-18-2016-19:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-18-2016-18:04:06 to 09-18-2016-19:04:06