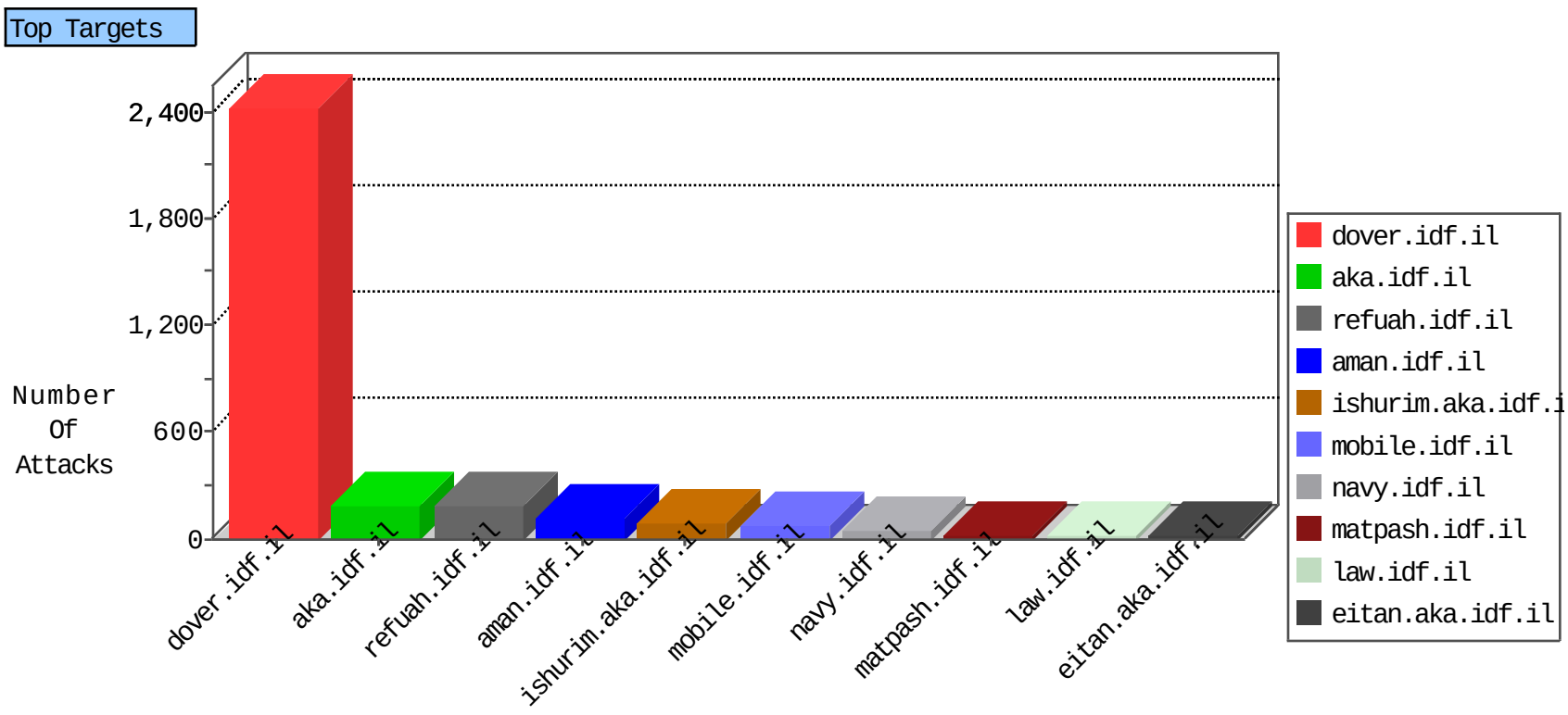
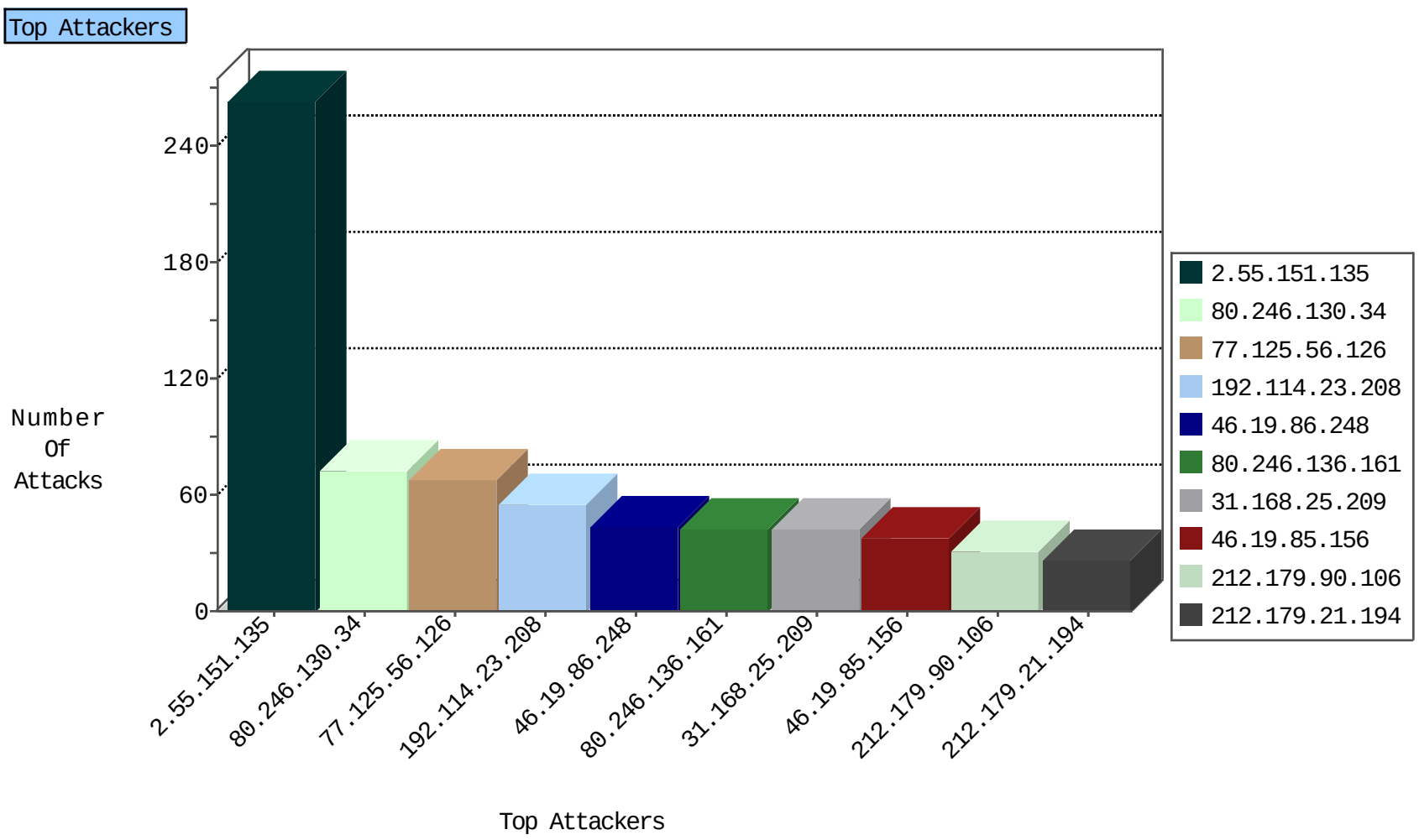
09-18-2016-17:04:01 to 09-18-2016-18:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-18-2016-17:04:01 to 09-18-2016-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.225.154	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
109.66.111.126	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	6
109.66.111.126	Israel	147.237.77.216	dover.idf.il	Black List	drop	6
176.13.232.37	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
129.93.229.138	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Black List	drop	3
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
37.142.10.208	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
194.254.215.12	France	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
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
79.180.138.52	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.208.4.197	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
194.29.178.14	Poland	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
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
46.19.86.110	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-18-2016-17:04:01 to 09-18-2016-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-18-2016-17:04:01 to 09-18-2016-18:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.13.14.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.172.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.193.74.175	147.237.0.17	Gibraltar	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.136.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.138.6.220	147.237.72.156	France	aman.idf.il	portscan: TCP Distributed Portscan	1
62.219.232.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.222.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.22.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.26.213.39	147.237.76.177	China	ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.60.153.178	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.139.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.185.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.69.234	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
62.219.128.187	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
46.19.85.254	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
41.180.9.40	147.237.8.45	South Africa	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1

09-18-2016-17:04:01 to 09-18-2016-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.55.151.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	216
80.246.130.34	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	72
77.125.56.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
31.168.25.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
109.253.221.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
79.177.162.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.248	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
2.55.151.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	23
2.55.151.135	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
46.19.86.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
79.176.133.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.86.248	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
62.219.163.16	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	15
192.114.23.208	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence		monitor	15
109.253.204.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
213.57.73.176	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.176.94.235	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.20.74	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.114.23.208	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.210.168.223	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
109.64.63.84	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.86.19	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.226.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.53.0.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
199.203.92.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.178.178.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.162.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.55.38.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.91	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
199.203.67.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.55.29.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.181.179.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.55.14.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.58.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
80.246.136.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.114.23.208	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
79.178.54.85	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.86.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.55.28.60	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.249	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.55.18.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.85	Europe	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	8
2.53.179.158	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.66.129.157	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.114.23.208	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8

09-18-2016-17:04:01 to 09-18-2016-18:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-18-2016-17:04:01 to 09-18-2016-18:04:01