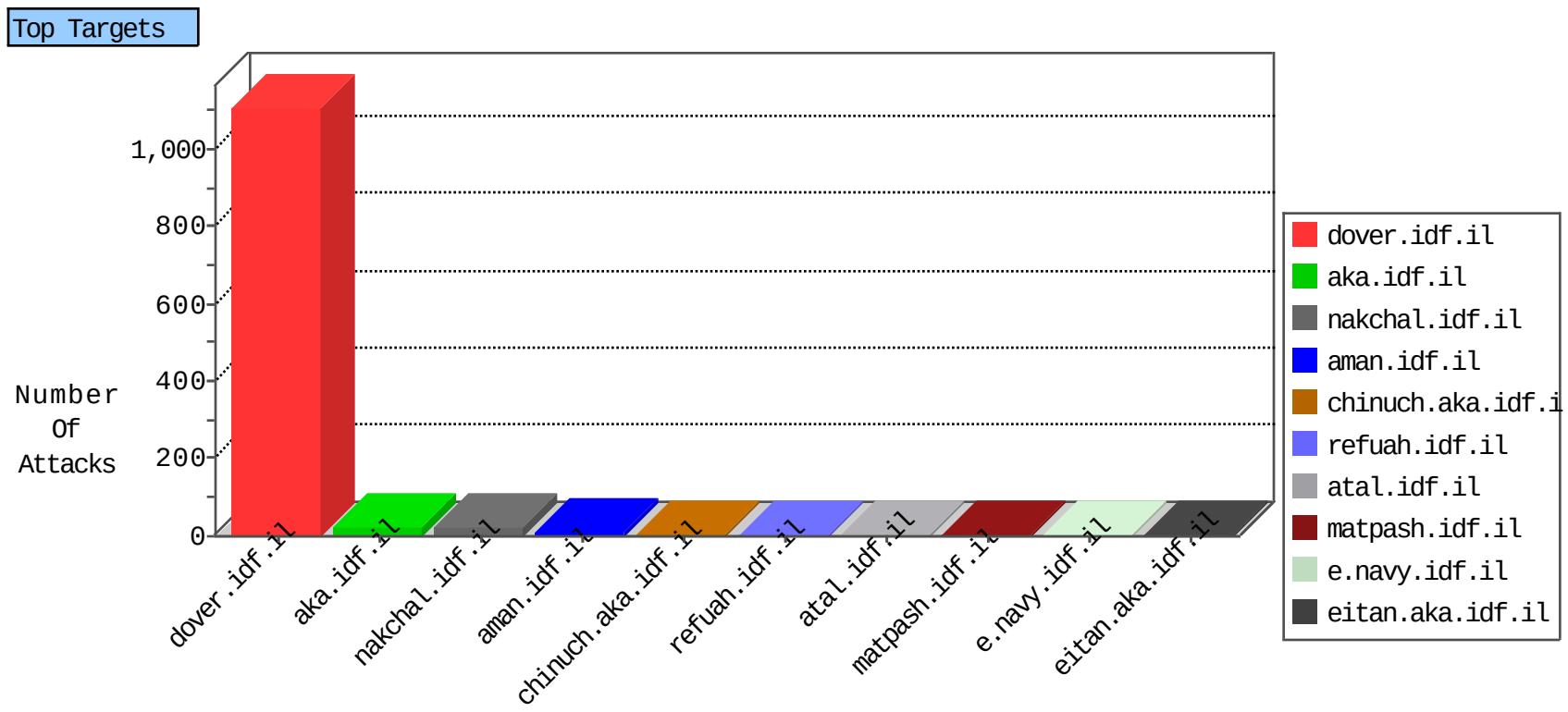
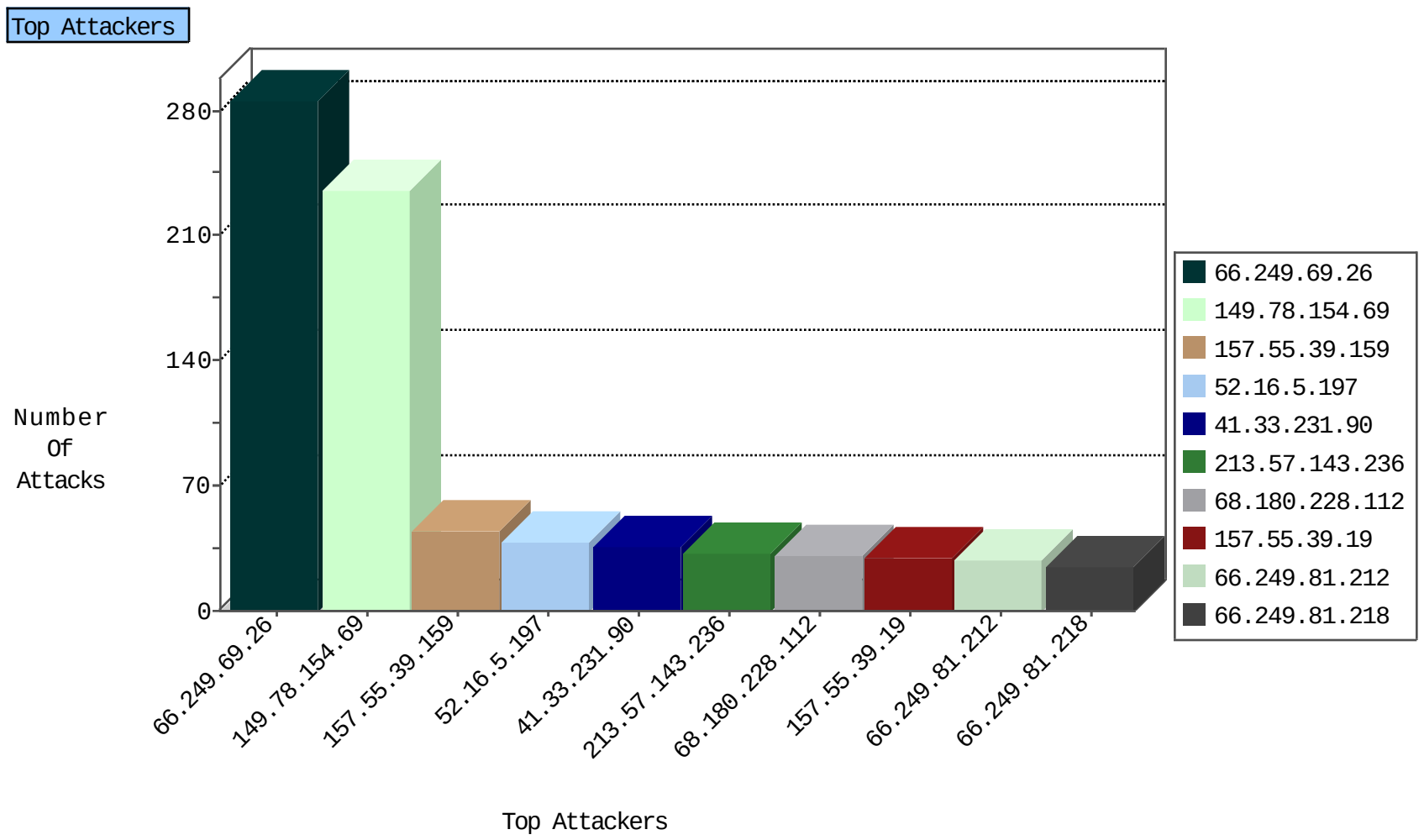
02-14-2016-03:04:05 to 02-14-2016-04:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-14-2016-03:04:05 to 02-14-2016-04:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
100.12.193.114	United States	147.237.77.121	e.navy.idf.il	Frk_Under_Attack_Con_Tcp	drop	1

02-14-2016-03:04:05 to 02-14-2016-04:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-14-2016-03:04:05 to 02-14-2016-04:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
175.6.228.149	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
94.102.48.193	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
69.197.145.242	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
60.1.251.86	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.193	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
69.197.145.242	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential SSH Scan	1
69.197.145.242	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1

02-14-2016-03:04:05 to 02-14-2016-04:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
213.57.143.236	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	31
46.19.85.147	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
107.167.104.83	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
46.19.86.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.130	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
208.109.97.62	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.64.26.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.69.82	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
106.39.253.104	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
54.162.16.100	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
1.82.229.215	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
42.81.69.136	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
130.193.51.80	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.86.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
40.115.22.29	United States	147.237.0.35	akaws.idf.il	drop		drop	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
40.115.22.29	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
40.115.22.29	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
146.185.239.102	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.27	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
40.115.22.29	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
146.185.239.102	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
130.193.51.80	Russian Federation	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
40.115.22.29	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
193.96.188.175	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
93.174.93.218	Netherlands	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.26	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	284
149.78.154.69	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	235
157.55.39.159	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	45
52.16.5.197	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	38
68.180.228.112	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	31
157.55.39.19	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	30
66.249.81.212	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	28
66.249.81.218	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	24
192.249.66.247	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	23
50.87.144.145	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	22
40.77.167.100	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	19
208.109.97.62	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	18
84.250.71.21	Finland	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	18
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	15
82.80.25.221	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	10
45.35.64.142		147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	9
37.26.148.143	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	6
46.19.85.112	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	6
80.246.133.233	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	6
2.54.165.173	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
46.244.69.39	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
98.218.82.62	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
205.203.135.1	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
37.46.39.228	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
54.144.83.141	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
81.218.135.184	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	3
68.187.173.78	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	3
107.170.119.178	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	3
73.155.73.247	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	3
83.105.46.220	United Kingdom	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	3
2.52.42.154	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	3
199.30.24.237	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	3
65.55.210.156	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	3
95.35.132.62	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
54.162.16.100	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
213.57.57.239	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
193.96.188.175	Germany	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
172.56.7.233	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
69.9.56.82	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.i	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
89.139.150.64	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
2.54.132.32	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
212.179.42.227	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
162.243.57.54	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
204.13.201.138	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	1
180.76.15.149	China	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	1
87.69.100.14	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	1
36.229.217.44	Taiwan	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	1
124.170.43.191	Australia	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	1
62.210.77.51	France	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	1

02-14-2016-03:04:05 to 02-14-2016-04:04:05