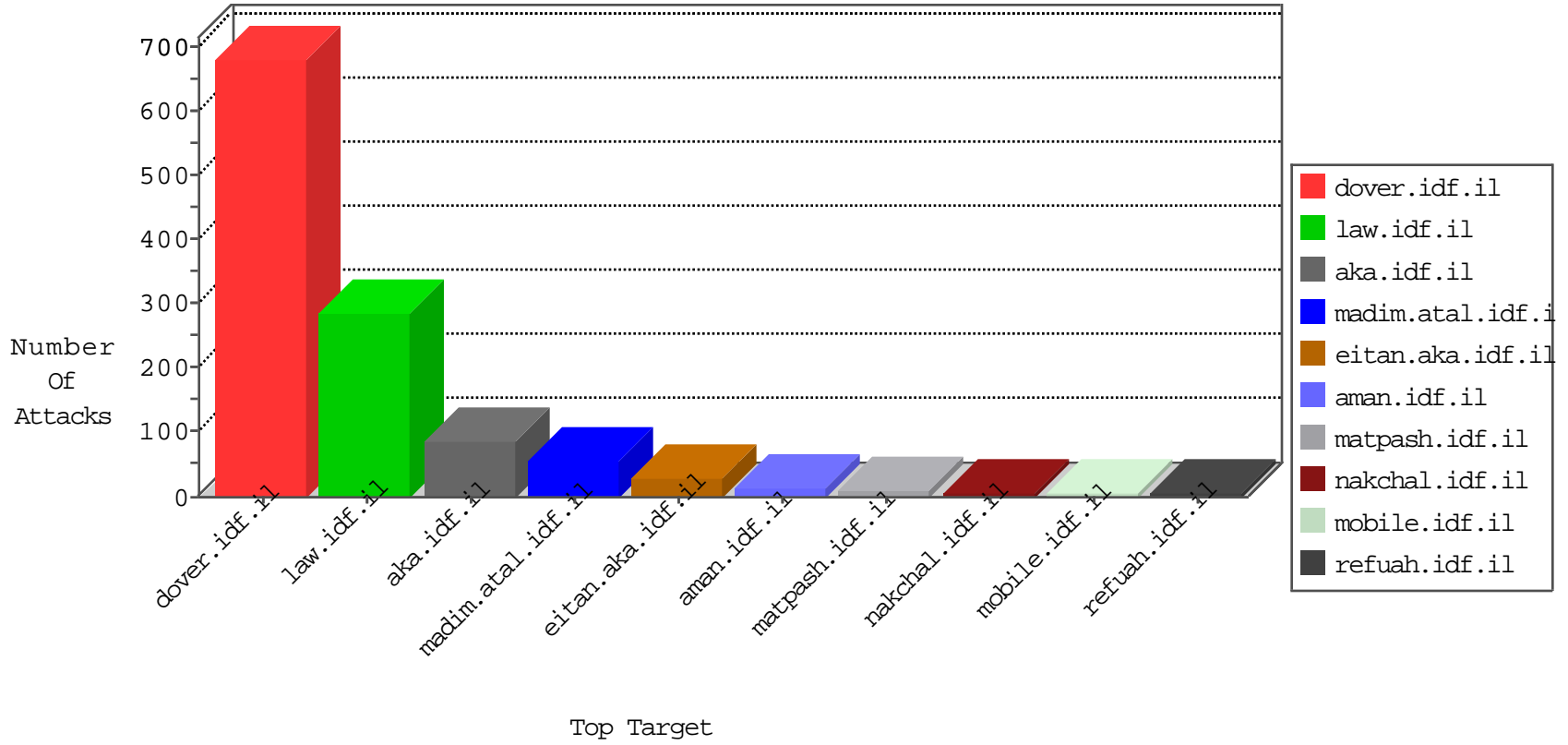


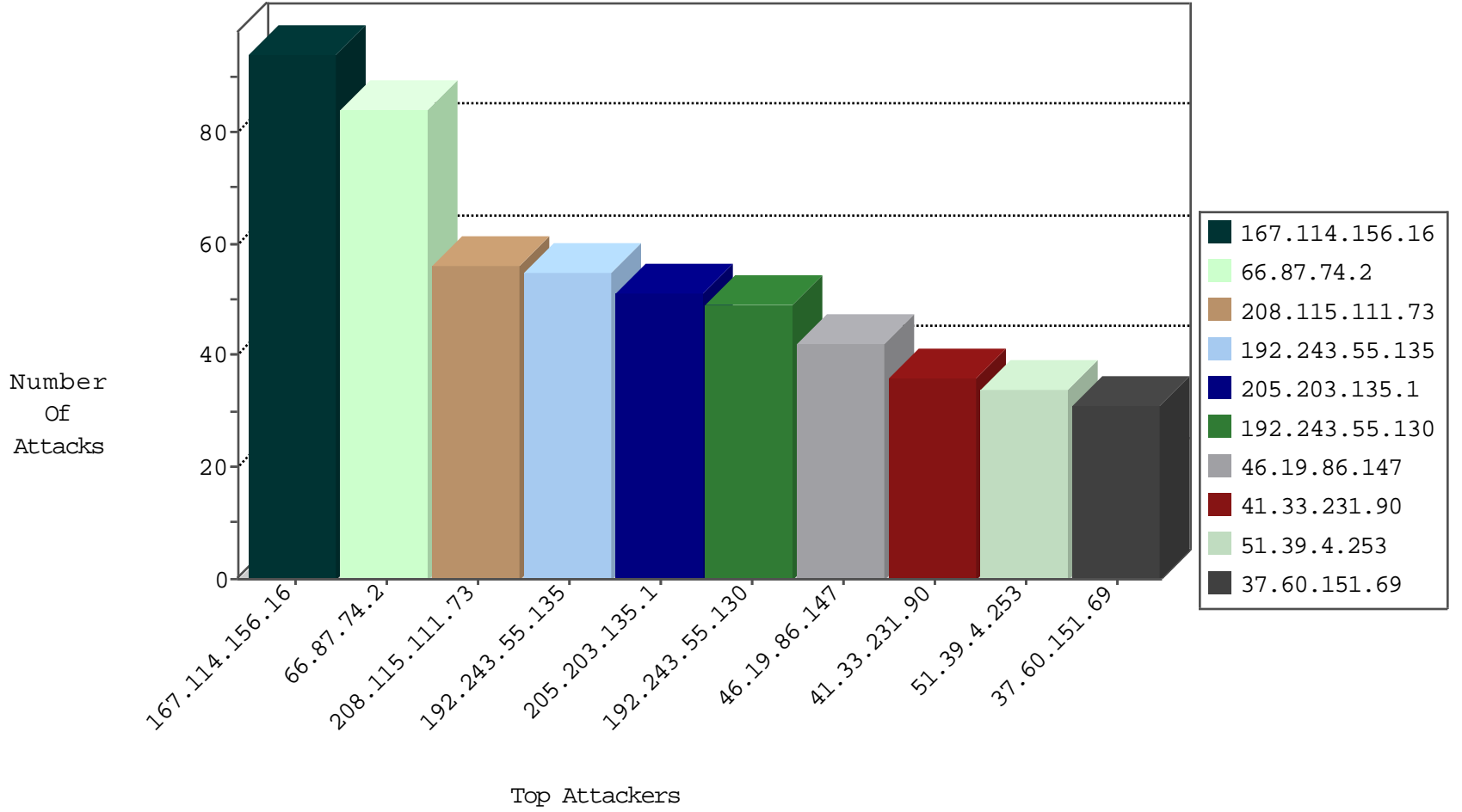
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	5044
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	880
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
79.177.69.254	Israel	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
62.138.2.213	Germany	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
62.138.2.213	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.216.176.244	147.237.0.15	Latvia	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
195.81.248.101	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.120	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
149.78.43.251	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
195.154.54.169	147.237.8.50	France	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.120	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.87.74.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	84
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
51.39.4.253	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
37.60.151.69	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
40.77.167.85	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
82.81.41.217	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
162.243.104.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.71.114.217	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
207.46.13.175	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	10
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
40.77.167.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.135	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.130	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
205.175.118.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
40.77.167.79	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
131.253.25.159	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.132	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	6
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.131	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.129	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.129	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.130	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
109.253.139.160	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.129.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
65.55.210.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
199.30.24.230	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.5	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/apple-app-site-association	Block	1
2.55.15.245	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
157.55.39.246	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in ww.tikshuv.idf.il/site/general.aspx	Block	1
77.75.78.162	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/33/	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.116	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
2.55.15.245	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 2.55.15.245	Block	1
164.132.161.7	Italy	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list6.htm	Block	1
77.237.138.202	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
66.249.64.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/540-he/patzar.aspx	Block	1
207.46.13.175	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
176.13.17.38	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.13.17.38	Block	1
84.111.216.70	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
130.185.155.74	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.93.184	Israel	147.237.72.166	aka.idf.il	URL is Above Root Directory www.aka.idf.il/./images/master/banner.jpg	Block	1
176.13.17.38	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
91.232.100.3	Lebanon	147.237.77.74	law.idf.il	Parameter Type Violation Master\$Header1\$ucHeaderSearch\$txtSearch in www.law.idf.il/205-he/patzar.aspx	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9023-he/refuah.aspx	Block	1
2.53.50.212	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/mobile	Block	1
141.212.122.161	United States	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31/	Block	1
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1