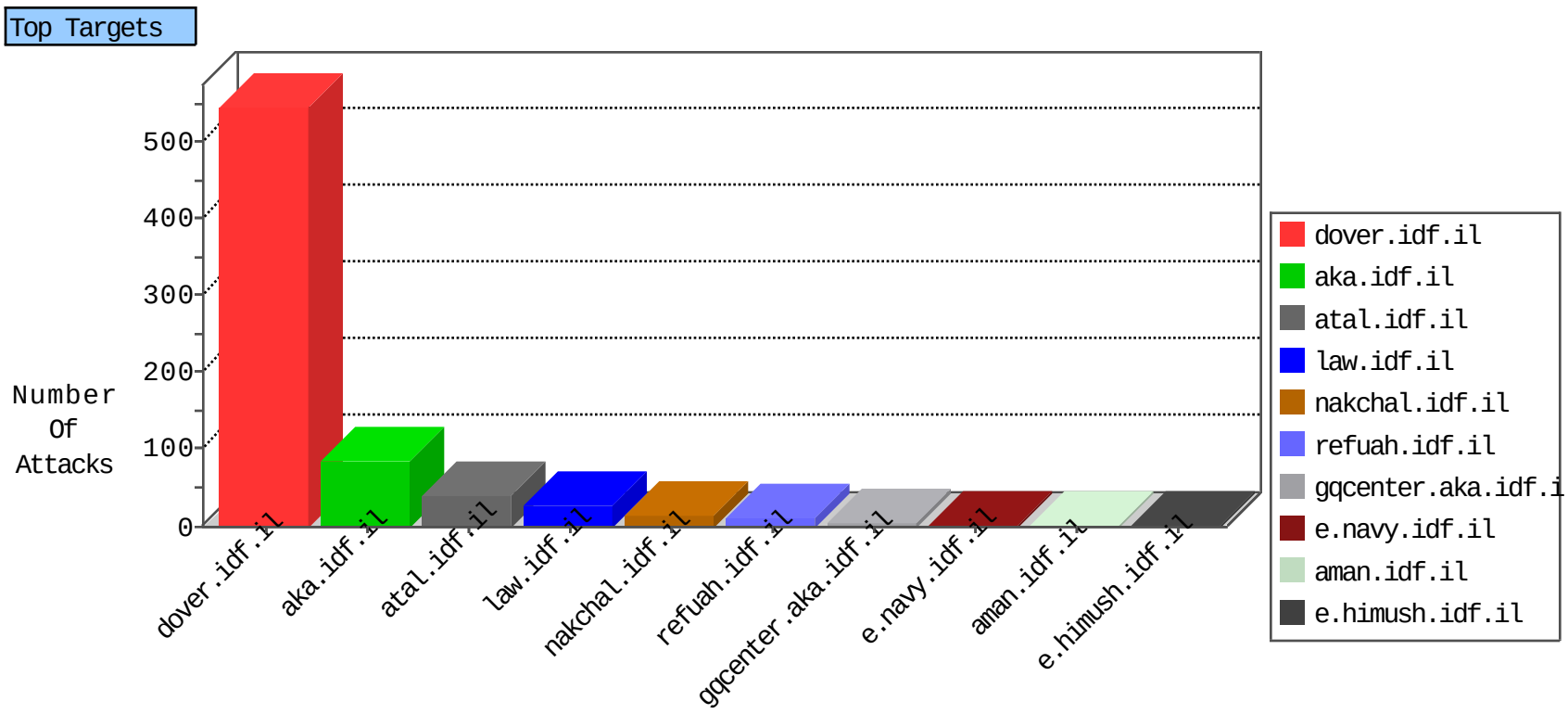
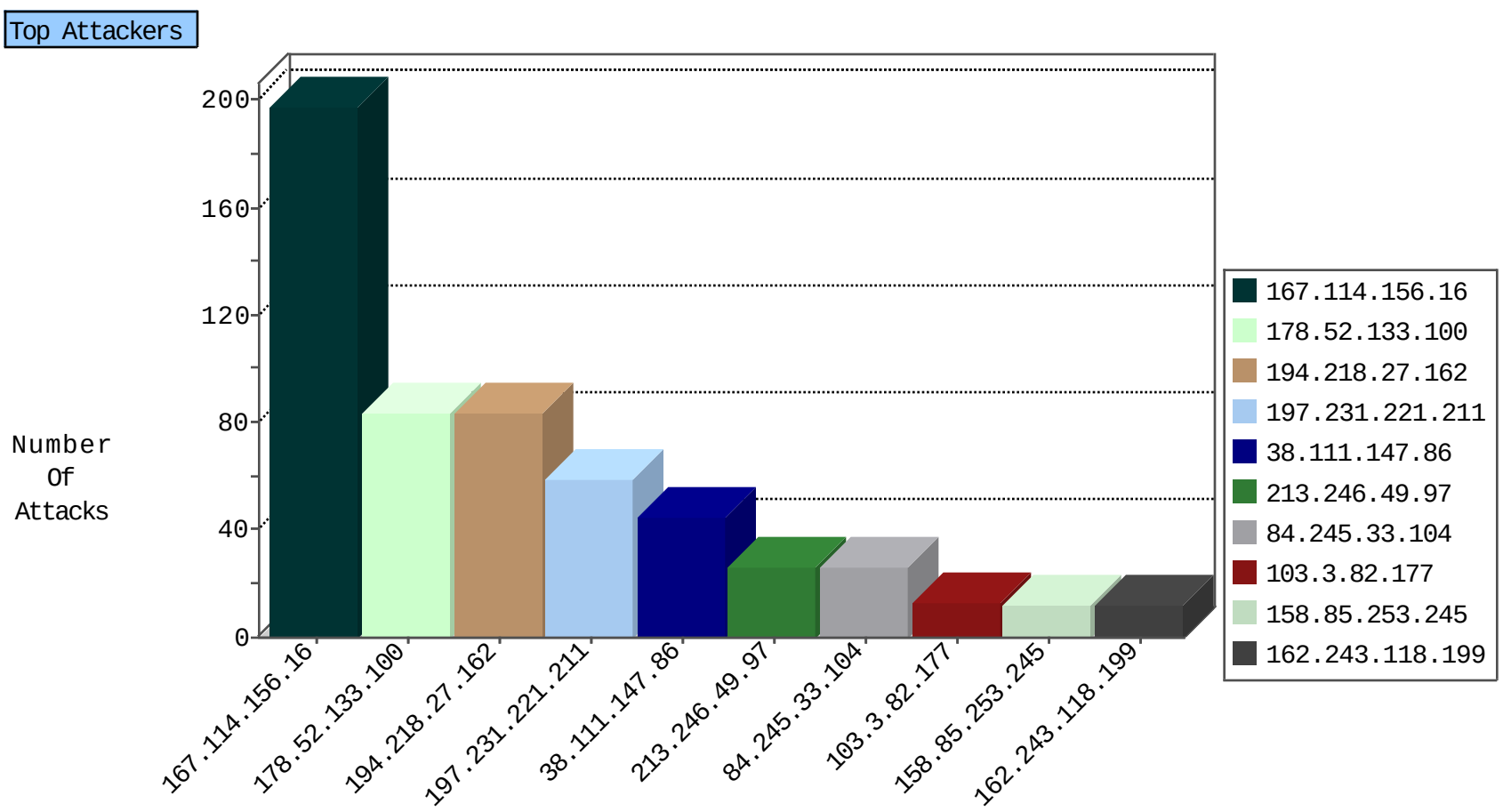
05-02-2016-04:04:08 to 05-02-2016-05:04:08

IDF Under Attack Daily Report





05-02-2016-04:04:08 to 05-02-2016-05:04:08

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	8996
94.230.86.172	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	203
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	103
94.102.52.10	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

05-02-2016-04:04:08 to 05-02-2016-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.245.33.104	Netherlands	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
213.246.49.97	France	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	7
23.91.70.119	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.246.49.97	France	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
84.245.33.104	Netherlands	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
108.67.169.124	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.246.49.97	France	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
185.81.157.33	France	147.237.77.170	maarachot.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

05-02-2016-04:04:08 to 05-02-2016-05:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
84.245.33.104	147.237.77.74	Netherlands	law.idf.il	SQL Injection - Select From	14
213.246.49.97	147.237.77.233	France	atal.idf.il	SQL Injection - Select From	14
108.67.169.124	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	6
23.91.70.119	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.197	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
58.187.229.210	147.237.77.121	Vietnam	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
58.187.229.210	147.237.77.121	Vietnam	e.navy.idf.il	ET SCAN NMAP -f -sS	1
13.94.46.116	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
13.82.55.149	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
210.212.93.46	147.237.76.197	India	e.himush.idf.il	ET SCAN Potential SSH Scan	1
125.22.40.140	147.237.77.170	India	maarachot.idf.il	ET SCAN Potential SSH Scan	1
58.187.229.210	147.237.77.121	Vietnam	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
13.82.55.149	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 2048	1
13.82.55.149	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN NMAP -f -sS	1
122.54.115.7	147.237.76.31	Philippines	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

05-02-2016-04:04:08 to 05-02-2016-05:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
178.52.133.100	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	42
178.52.133.100	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	42
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	32
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
103.3.82.177	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
158.85.253.245	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	12
162.243.118.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
191.190.6.228	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.188.160.223	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
104.140.83.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
106.38.241.149	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.146.158	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
172.56.27.104	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
31.193.51.17	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.9.127.69	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
164.132.161.48	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.30.25.44	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.160.245.147	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
90.211.92.65	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
173.252.112.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
65.55.210.105	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
72.32.42.129	United States	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
164.132.161.3	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.126	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.184.3.122	Japan	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.211	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
87.69.16.146	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
66.249.88.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.116	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.204	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

05-02-2016-04:04:08 to 05-02-2016-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-02-2016-04:04:08 to 05-02-2016-05:04:08