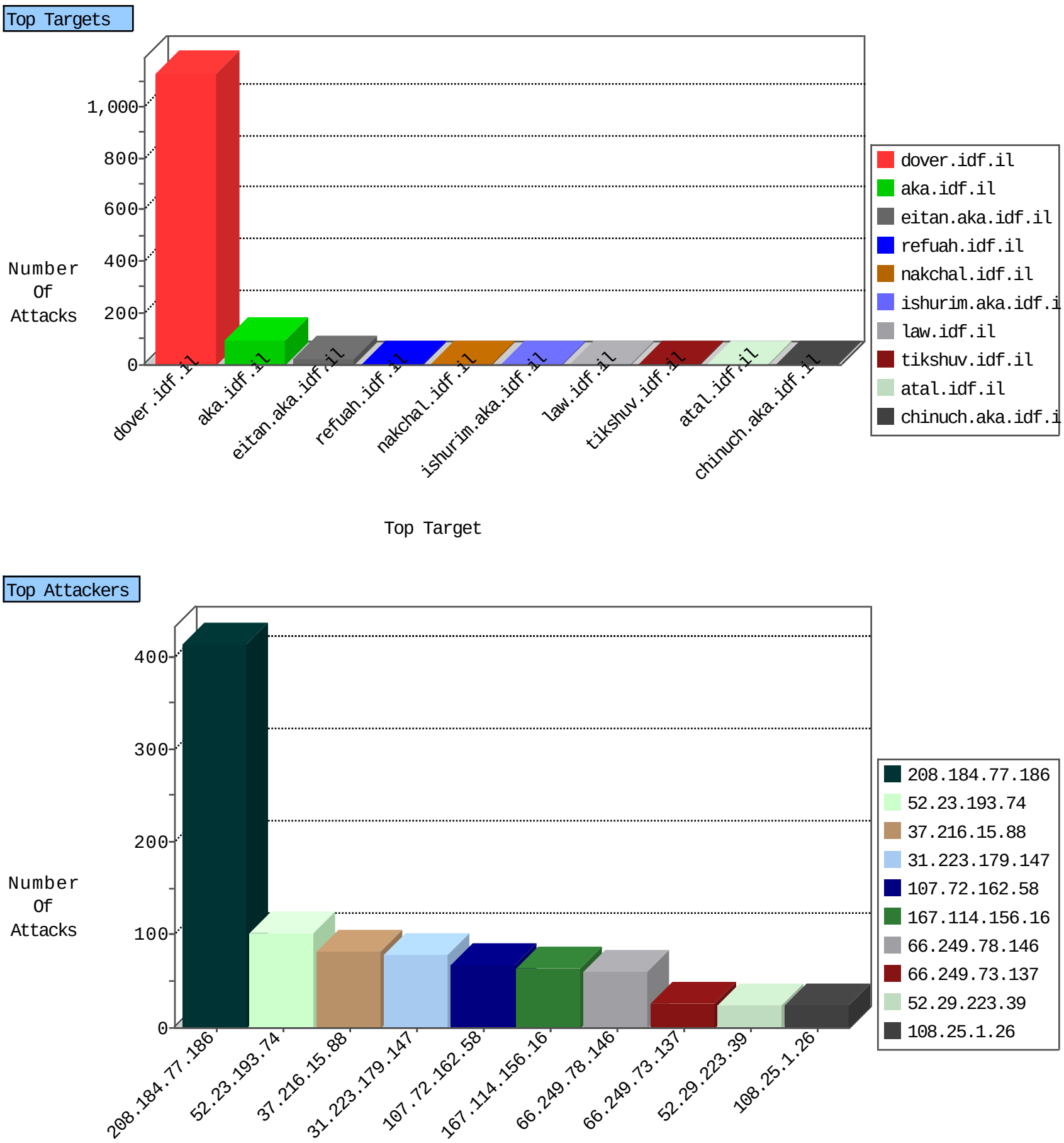
05-05-2016-02:04:06 to 05-05-2016-03:04:06

IDF Under Attack Daily Report



05-05-2016-02:04:06 to 05-05-2016-03:04:06

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	2354
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	289
185.80.130.186	Lithuania	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

05-05-2016-02:04:06 to 05-05-2016-03:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-05-2016-02:04:06 to 05-05-2016-03:04:06

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
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
82.102.241.65	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
5.39.222.253	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.88	147.237.76.31	Lithuania	nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.88	147.237.0.16	Lithuania	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.160.38	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
208.100.26.228	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.88	147.237.77.19	Lithuania	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.88	147.237.0.33	Lithuania	idf.il	ET SCAN Potential SSH Scan	1
163.172.140.23	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
120.26.115.52	147.237.0.200	China	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1

05-05-2016-02:04:06 to 05-05-2016-03:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
208.184.77.186	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	414
52.23.193.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
37.216.15.88	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
31.223.179.147	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
107.72.162.58	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
108.25.1.26	United States	147.237.77.216	dover.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	24
54.72.73.168	Ireland	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	18
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
203.145.94.84	Hong Kong	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
157.55.39.134	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
8.37.227.68	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
70.95.80.199	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.73.137	United States	147.237.77.216	dover.idf.il	drop		drop	6
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.165.230.5	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
166.182.3.248	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.73.137	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
8.37.227.69	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	5
66.249.73.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
66.249.73.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.65.165.25	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
188.141.51.67	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.88.92.12	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
67.82.29.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
73.171.202.86	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.202	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.65.2	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.125.4.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.1.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
8.37.227.81	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
141.8.142.1	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.73.137	Israel	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	2
149.202.239.135	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.87.136.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.117.123.94	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
88.251.92.204	Turkey	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2

05-05-2016-02:04:06 to 05-05-2016-03:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.239.135	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	5
66.249.73.192	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
23.106.244.56	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
207.46.13.178	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
88.251.92.204	Turkey	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/wp-login.php	Block	1
2.53.50.132	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
164.132.161.76	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
67.247.0.250	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
37.47.66.193	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	1
88.251.92.204	Turkey	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9709-he/refuah.aspx	Block	1
5.255.253.75	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.200.45.31	Germany	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/shared/usercontrols/headerupper/	Block	1
54.210.18.124	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
88.251.92.204	Turkey	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/	Block	1
17.142.156.103	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
87.69.135.66	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
54.210.18.124	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
66.249.93.98	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
23.81.69.249	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
188.143.232.34	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.34	Block	1
88.251.92.204	Turkey	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
66.249.73.137	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-he/dover.aspx	Block	1
149.202.239.135	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.93.110	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1

05-05-2016-02:04:06 to 05-05-2016-03:04:06