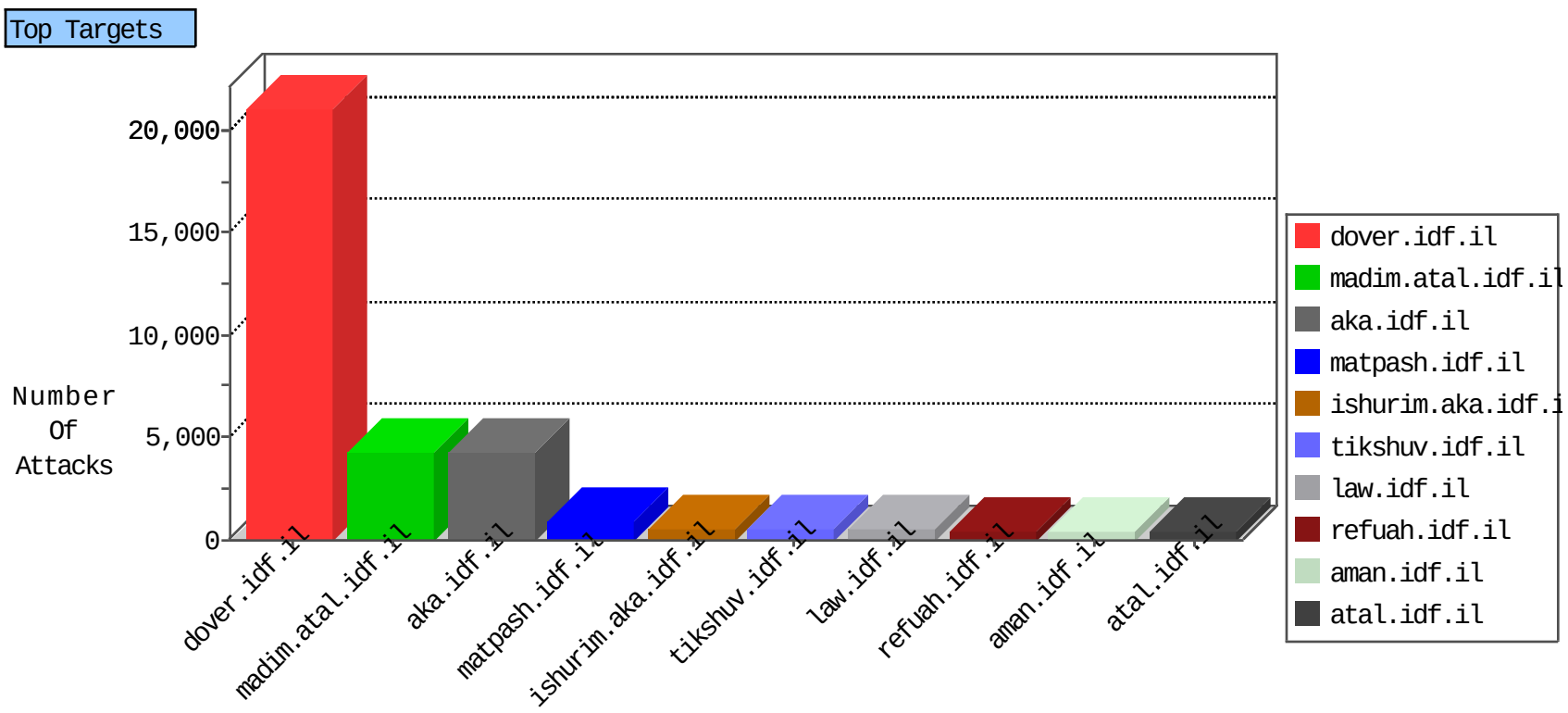
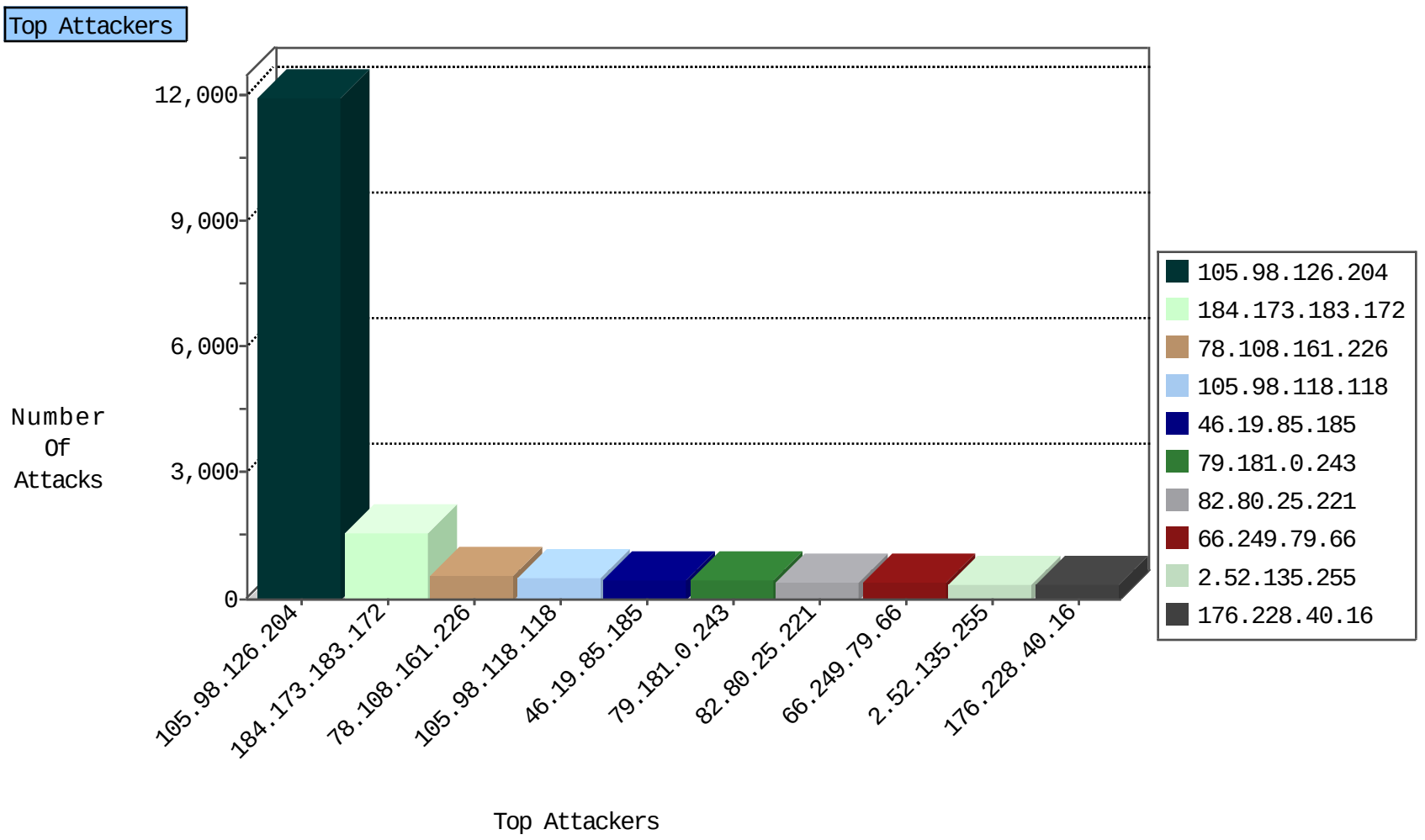
03-26-2015-00:00:06 to 03-27-2015-00:00:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-26-2015-00:00:06 to 03-27-2015-00:00:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
85.64.84.23	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	2107
149.78.50.11	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	630
84.108.66.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	589
84.108.32.168	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	580
5.29.174.188	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	547
109.67.48.16	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	352
85.65.245.148	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	314
197.30.135.18	Tunisia	147.237.0.17	m.my-kosher-kravi.idf.il	TCP Scan (vertical)	drop	279
5.28.180.42	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	269
89.139.21.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	249
79.177.104.93	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	242
46.120.146.147	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	236
192.116.232.69	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	216
46.121.142.226	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	209
84.109.17.214	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
79.181.56.31	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
79.181.196.145	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	147
95.86.123.40	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	146
5.29.38.219	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	140
79.178.52.84	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
79.176.128.23	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
89.139.15.38	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	105
79.183.197.238	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
149.88.99.108	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
212.25.105.125	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
79.177.1.101	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	90
78.24.50.205	Moldova, Republic of	147.237.0.15	kosher-kravi.idf.il	TCP Scan (vertical)	drop	88
77.125.100.220	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
80.246.138.78	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
5.102.224.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
79.182.199.172	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
84.110.208.109	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
192.114.23.211	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
78.24.50.205	Moldova, Republic of	147.237.0.16	my-kosher-kravi.idf.il	TCP Scan (vertical)	drop	71
46.19.86.80	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
80.246.136.195	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	67
157.55.39.67	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	67
54.72.73.168	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	64
2.54.180.55	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
207.46.13.16	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	57
157.55.39.42	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	54
157.55.39.6	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	53
207.46.13.5	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	48
195.34.150.18	Austria	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	46
207.46.13.112	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	45
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	44
52.16.5.197	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	40
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	39
50.87.144.145	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	38
157.55.39.137	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	38

03-26-2015-00:00:06 to 03-27-2015-00:00:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1124
77.125.87.160	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	274
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	187
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	174
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	151
184.173.183.172	United States	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	126
74.208.154.12	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	24
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	23
184.173.233.226	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
184.173.233.226	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
192.115.248.2	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
199.203.226.21	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	12
74.208.154.12	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	12
175.44.25.203	China	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	10
212.150.215.8	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	9
217.194.193.52	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
94.230.86.246	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	8
212.143.41.199	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
46.120.107.249	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	7
79.177.4.76	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
5.28.136.218	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
46.19.85.125	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
109.66.167.94	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
188.102.26.233	Germany	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
31.168.142.17	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
70.49.129.184	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
94.242.228.140	Luxembourg	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
149.88.99.108	United States	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
175.44.25.68	China	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
85.250.189.52	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.76	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
109.65.179.178	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
93.173.23.146	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
87.68.83.223	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
2.54.29.193	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
149.88.103.192	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
213.57.214.141	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.240	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.43.94	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	2
79.176.221.53	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
93.120.27.62	Romania	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	2
85.25.43.94	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	2
203.126.119.66	Singapore	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.43.94	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	2
46.19.85.143	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
192.116.188.9	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.19.85.24	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.43.94	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	2
95.86.124.59	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
2.54.6.98	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2

03-26-2015-00:00:06 to 03-27-2015-00:00:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	393
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	115
85.113.100.132	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	91
74.208.154.12	United States	147.237.72.166	aka.idf.il	SQL Injection - Select From	51
184.173.233.226	United States	147.237.72.166	aka.idf.il	SQL Injection - Select From	15
77.126.137.81	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	14
85.64.84.23	Israel	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	14
80.246.136.16	Israel	147.237.72.167	ishurim.aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	7
88.245.65.42	Turkey	147.237.77.216	dover.idf.il	Tehila defacement attempt (-Hacked By- sent to Web Server)	6
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
197.30.135.18	Tunisia	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
43.255.191.159	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	3
5.22.129.178	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
66.249.67.3	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
141.255.190.190	Sweden	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	2
115.231.218.147	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.162	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	2
176.12.136.12	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
212.179.212.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.248.172.173	Netherlands	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	2
149.78.102.127	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.113.98.10	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
89.248.172.173	Netherlands	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	2
61.240.144.66	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	2
46.121.68.121	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.159	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
79.177.102.67	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.157	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	2
46.116.246.16	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.159	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
89.248.172.173	Netherlands	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	2
43.255.191.157	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	2
89.248.172.173	Netherlands	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	2
89.248.172.173	Netherlands	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
80.246.130.21	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.61.240.66	United States	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
213.204.127.33	Lebanon	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.89	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
89.248.172.173	Netherlands	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	2
105.98.105.229	Algeria	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
89.138.75.23	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.24	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.125.154.180	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.159.5	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.159	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
89.248.172.173	Netherlands	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	2
37.26.147.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
81.218.77.162	Israel	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	2
87.68.47.219	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
89.248.172.173	Netherlands	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	2

03-26-2015-00:00:06 to 03-27-2015-00:00:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
105.98.126.204	Algeria	147.237.77.216	dover.idf.il	SAM rule	drop	drop	7607
105.98.126.204	Algeria	147.237.77.216	dover.idf.il		drop	drop	3601
105.98.126.204	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	599
66.249.79.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	314
66.249.79.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	280
105.98.118.118	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	270
66.249.79.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	240
78.108.161.226	Lebanon	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	115
78.108.161.226	Lebanon	147.237.0.34	tikshuv.idf.il	First packet isn't SYN	drop	drop	106
105.98.118.118	Algeria	147.237.77.216	dover.idf.il		drop	drop	96
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	91
78.108.161.226	Lebanon	147.237.76.86	navy.idf.il	First packet isn't SYN	drop	drop	86
66.87.116.113	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	85
213.244.82.139	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	64
78.108.161.226	Lebanon	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	61
192.118.118.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
66.249.73.244	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
158.169.150.9	Belgium	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	56
5.35.111.143	Russian Federation	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	43
78.108.161.226	Lebanon	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	43
5.22.129.178	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	37
109.253.142.26	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
176.12.149.80	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
46.116.94.160	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	34
105.98.118.118	Algeria	147.237.77.216	dover.idf.il	SAM rule	drop	drop	33
213.8.96.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
223.73.36.240	China	147.237.72.166	aka.idf.il	SAM rule	drop	drop	30
109.253.144.82	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.145.119	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.131.231	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
212.29.214.138	Israel	147.237.72.166	aka.idf.il	SAM rule	drop	drop	29
64.41.200.102	United States	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	28
2.54.156.106	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
109.253.158.203	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
176.12.146.136	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.142.45	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
193.43.246.250	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
176.12.139.22	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
213.8.96.180	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	25
78.108.161.226	Lebanon	147.237.77.234	halag.idf.il	First packet isn't SYN	drop	drop	25
109.253.146.132	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.151.157	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.143.227	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
46.19.85.185	Israel	147.237.0.19	madim.atal.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.140.97	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.144.79	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
62.0.215.129	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	23
176.195.251.102	Russian Federation	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	23

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.181.0.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	453
46.19.85.185	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.185	Block	436
2.52.135.255	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.52.135.255	Block	372
109.66.168.23	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/priv.dog.settings/getstatistics	Block	337
37.26.147.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	324
176.228.40.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	317
85.250.122.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	265
5.29.209.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	242
2.54.7.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	196
132.70.66.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	176
2.54.15.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	154
105.98.105.229	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.98.105.229	Block	153
105.98.105.229	Algeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	152
2.54.170.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	132
109.253.156.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	117
109.253.131.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	102
109.253.132.62	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.132.62	Block	102
80.246.136.88	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	96
46.19.86.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	90
109.253.149.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	90
82.102.141.253	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	88
105.98.126.204	Algeria	147.237.77.216	dover.idf.il	Multiple Post Request - Missing Content Type: 'none'	Block	78
109.253.146.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	77
149.78.155.71	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	77
105.98.126.204	Algeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	76
109.253.158.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	74
109.253.131.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	60
66.249.79.58	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	54
105.98.118.118	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 105.98.118.118	Block	47
185.32.176.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	46
105.98.118.118	Algeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	46
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	35
66.249.79.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	35
109.253.129.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	33
79.177.1.101	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.177.1.101	Block	27
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	26
109.253.147.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	24
176.228.40.16	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.228.40.16	Block	23
77.125.103.186	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	21
2.54.26.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	21
66.249.79.74	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	19
79.182.138.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	19
109.253.158.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	18
31.210.186.142	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	16
99.120.102.206	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 99.120.102.206	Block	16
84.94.107.94	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.94.107.94	Block	14
81.218.251.250	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 81.218.251.250	Block	13
109.65.190.7	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.65.190.7	Block	13
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	12
80.246.140.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	11