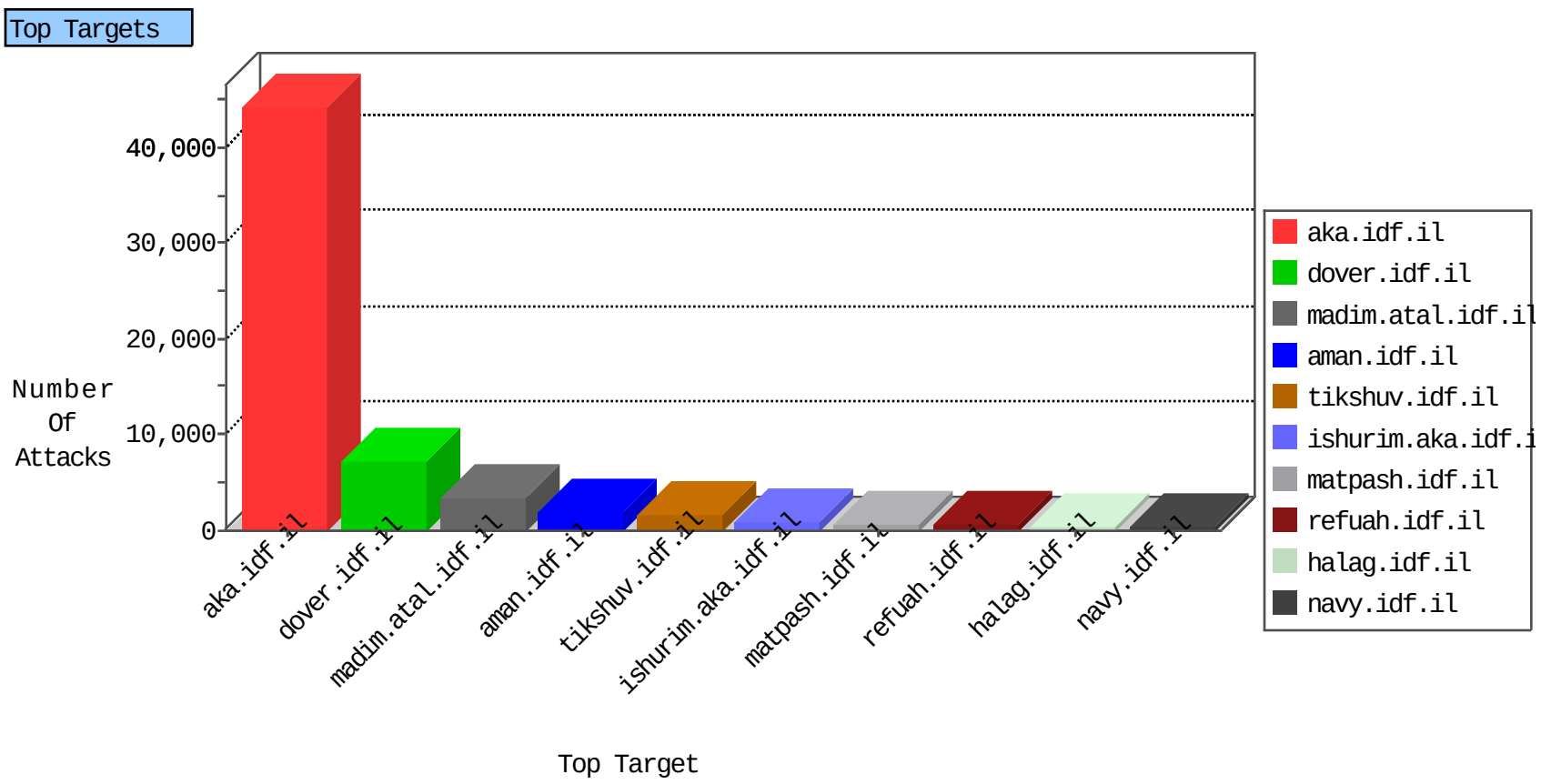
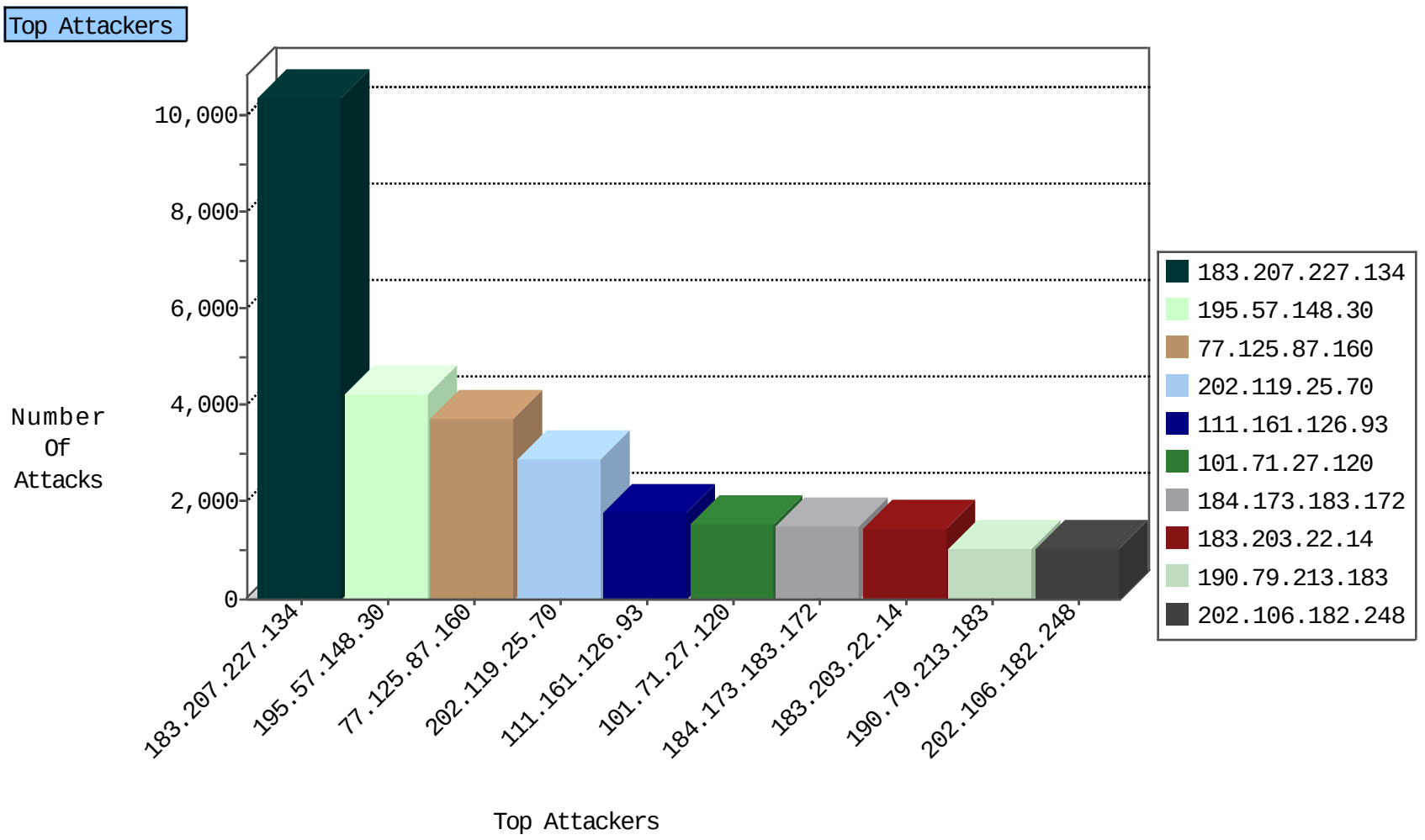
03-18-2015-00:00:00 to 03-19-2015-00:00:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-18-2015-00:00:00 to 03-19-2015-00:00:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
0.0.0.0		147.237.72.166	aka.idf.il	HTTP-POST-Segmented-DoS	dest-reset	13408
220.181.108.173	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	3360
212.143.110.33	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	1104
192.114.182.2	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	798
87.68.36.220	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	775
84.228.175.209	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	646
46.117.62.192	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	491
85.250.61.27	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	466
94.230.86.134	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	459
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	449
147.235.185.74	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	408
79.183.48.146	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	385
109.65.7.215	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	381
79.183.149.163	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	369
46.120.200.212	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	297
109.66.37.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	294
94.159.147.158	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	233
85.64.47.146	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	230
109.66.12.252	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	228
79.181.136.40	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	210
46.120.157.157	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	194
79.176.135.223	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	189
84.94.170.70	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	188
93.172.177.158	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	168
83.130.113.231	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	167
46.19.85.174	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	166
66.249.78.153	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	164
95.86.112.37	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	139
85.250.231.225	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	137
77.125.251.70	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	124
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	124
109.186.145.183	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
109.226.15.5	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
109.160.202.102	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	120
109.64.24.7	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	103
118.26.142.5	China	147.237.72.166	aka.idf.il	HTTP-POST-Segmented-DoS	dest-reset	103
109.67.86.10	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	89
93.173.63.150	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	86
89.138.76.207	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	84
46.19.85.170	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	84
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	82
185.32.179.67	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
213.57.241.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	77
89.138.250.88	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	75
77.127.203.237	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	75
31.168.213.89	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
2.52.0.122	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	74
109.253.139.253	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	74
87.69.96.186	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	72
46.19.85.206	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	72

03-18-2015-00:00:00 to 03-19-2015-00:00:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.87.160	Israel	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	1589
77.125.87.160	Israel	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	1266
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	665
77.125.87.160	Israel	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	623
77.125.87.160	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	263
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	259
184.173.183.172	United States	147.237.77.234	halag.idf.il	DVRep_P-N_40-59	Permit	255
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	193
184.173.183.172	United States	147.237.76.30	himush.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	108
119.6.144.74	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	97
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	96
119.6.144.74	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	56
46.116.237.41	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	35
23.91.127.146	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	32
37.130.227.133	United Kingdom	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	28
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	27
64.150.190.73	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
96.31.33.34	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	16
64.150.190.73	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
96.31.33.34	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	16
23.91.127.146	United States	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	15
37.187.129.166	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	12
77.127.246.134	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	10
2.52.34.12	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	9
46.116.208.185	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
176.58.67.237	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	7
91.207.4.22	Ukraine	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	6
212.34.12.133	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
46.19.85.106	Israel	147.237.77.226	www.chamatz.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
194.114.146.227	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
192.116.232.69	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
96.44.189.101	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
94.230.86.230	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
93.173.231.246	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	5
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	5
2.52.129.32	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
198.20.70.114	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	5
213.57.30.187	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
93.172.12.77	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
109.226.14.43	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
85.25.103.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	4
85.64.229.239	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
31.168.241.35	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
199.67.203.140	Europe	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	4
176.126.252.12	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
85.250.190.253	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4

03-18-2015-00:00:00 to 03-19-2015-00:00:00

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	355
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	108
64.150.190.73	United States	147.237.72.166	aka.idf.il	SQL Injection - Select From	32
109.253.133.55	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
173.0.225.60	United States	147.237.77.216	dover.idf.il	SERVER-WEBAPP Setup.php access	5
79.177.135.207	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.67.14	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	4
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	3
46.19.85.189	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
81.218.251.250	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.1.243	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	2
5.22.130.224	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
157.55.39.132	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.64.216.38	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	2
79.181.214.17	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.80.196.44	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
61.240.144.66	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
84.111.65.42	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
128.61.240.66	United States	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
84.95.207.155	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.178.28.42	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.140.79	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.253.141.138	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
91.135.111.75	Israel	147.237.72.167	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
197.205.174.163	Algeria	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	2
109.253.138.21	Israel	147.237.76.30	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
94.159.235.123	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.67	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
84.228.22.82	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
179.157.35.224	Brazil	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.165	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
122.228.207.199	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
54.173.80.78	United States	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
112.133.130.208	Korea, Republic of	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.77.79.43	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
2.52.58.168	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.171.162	Netherlands	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.133.192	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
128.61.240.66	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
122.228.207.77	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
31.168.172.145	Israel	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
104.245.99.48		147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
207.46.13.133	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
109.226.14.43	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

03-18-2015-00:00:00 to 03-19-2015-00:00:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
183.207.227.134	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	10366
195.57.148.30	Spain	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4223
202.119.25.70	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2924
111.161.126.93	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1791
101.71.27.120	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1574
183.203.22.14	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1422
190.79.213.183	Venezuela	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1029
202.106.182.248	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1022
111.1.3.36	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	961
190.207.160.54	Venezuela	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	836
190.205.104.161	Venezuela	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	823
186.95.25.149	Venezuela	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	811
202.108.50.75	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	720
182.118.23.7	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	712
61.152.102.40	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	663
114.80.182.132	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	661
163.177.79.4	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	653
113.105.224.95	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	562
190.36.144.26	Venezuela	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	533
36.34.90.248	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	502
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	498
190.79.240.215	Venezuela	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	485
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	476
103.27.24.114	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	474
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	468
117.177.243.79	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	456
120.192.249.74	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	441
190.79.57.104	Venezuela	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	429
103.27.24.113	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	425
101.251.211.234	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	416
190.198.163.75	Venezuela	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	357
101.251.211.237	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	313
106.37.177.251	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	303
123.138.185.50	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	300
124.161.94.8	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	300
218.27.136.164	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	265
118.26.142.5	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	248
60.26.90.15	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	247
58.61.29.233	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	243
111.7.128.171	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	229
207.241.226.144	United States	147.237.77.216	dover.idf.i	SAM rule	drop	drop	207
36.250.74.87	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	205
221.10.102.203	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	202
196.217.44.232	Morocco	147.237.77.216	dover.idf.i		drop	drop	191
38.111.147.86	United States	147.237.76.86	navy.idf.il		drop	drop	148
115.28.238.147	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	130
200.113.169.210	Chile	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	128
212.72.7.91	Oman	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	124
124.88.67.13	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	123
125.39.66.68	China	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	116

03-18-2015-00:00:00 to 03-19-2015-00:00:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.147.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	321
109.253.139.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	270
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	267
176.12.143.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	240
2.54.142.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	182
2.54.134.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	145
5.29.199.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	133
109.253.159.96	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.159.96	Block	128
79.183.1.221	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.183.1.221	Block	109
176.12.137.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	98
109.253.134.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	77
93.173.191.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	75
176.12.138.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	70
176.12.138.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	70
109.253.149.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	69
37.140.188.30	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.140.188.30	Block	66
176.12.139.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	65
176.12.143.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	64
109.253.129.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	61
46.19.85.47	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	61
176.12.139.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	59
176.12.136.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	59
176.12.139.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	55
176.12.140.0	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	55
176.12.145.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	54
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	53
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	50
109.253.128.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	48
79.177.167.31	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.177.167.31	Block	45
109.253.145.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	44
176.12.139.45	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.139.45	Block	42
176.12.142.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	40
176.12.145.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	38
176.12.145.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	37
176.12.151.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	35
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	35
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	35
176.12.140.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	27
176.12.144.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	26
176.12.141.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	25
176.12.140.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	23
176.12.150.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	21
188.165.15.200	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.200	Block	21
176.12.143.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	20
85.64.175.240	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 85.64.175.240	Block	17
37.77.122.96	Italy	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.77.122.96	Block	16
109.253.147.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	16
79.177.207.134	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	15
176.12.149.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	14
212.29.198.17	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	14

03-18-2015-00:00:00 to 03-19-2015-00:00:00