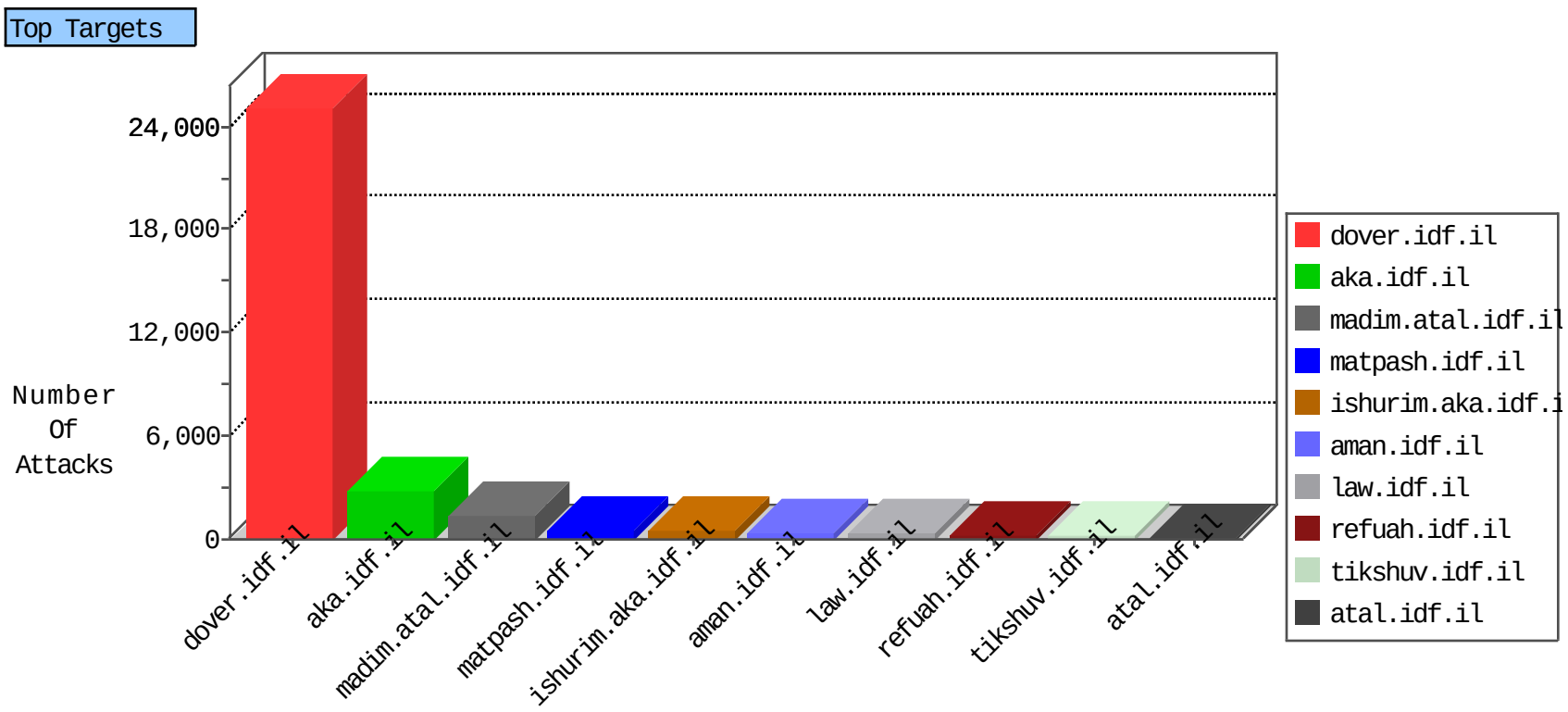
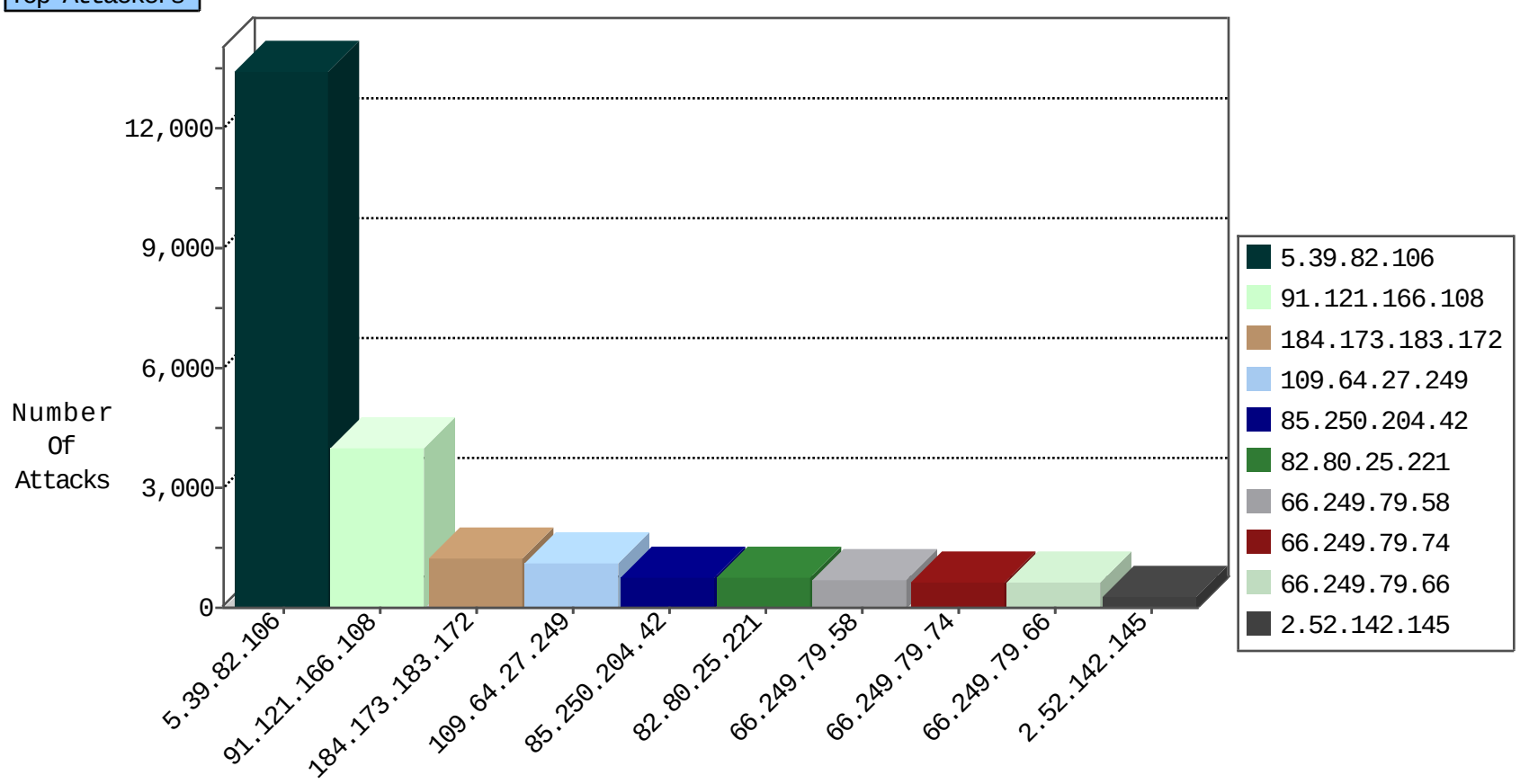
03-21-2015-00:00:10 to 03-22-2015-00:00:10

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-21-2015-00:00:10 to 03-22-2015-00:00:10

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	7578
91.121.166.108	France	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	1383
109.65.17.181	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	1139
85.250.17.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	832
91.121.166.108	France	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	730
89.139.7.19	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	648
5.39.82.106	France	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	469
46.120.200.212	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	447
87.69.214.26	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	384
66.249.78.153	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	379
77.127.157.176	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	368
109.65.103.145	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	351
105.103.212.214	Algeria	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	340
213.57.144.41	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	335
93.172.8.175	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	320
85.65.167.135	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	261
2.52.143.110	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	245
105.103.212.214	Algeria	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	185
85.65.17.196	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	182
37.142.148.230	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	173
87.68.64.125	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	166
109.66.12.252	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
149.88.45.158	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	144
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	122
213.57.112.237	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
46.121.58.224	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	103
2.52.48.127	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	93
105.103.212.214	Algeria	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	93
149.78.219.199	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
46.19.85.245	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
109.64.112.17	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
109.160.186.110	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
109.66.59.173	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
2.54.2.14	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
79.177.208.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	74
31.168.115.185	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
5.39.82.106	France	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	70
46.116.112.71	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
87.69.149.172	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
109.64.112.17	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	28
2.54.2.14	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	21
5.39.82.106	France	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Tcp	drop	20
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	12
82.145.219.148	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
82.145.219.191	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	5
82.102.141.250	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	5
110.159.179.251	Malaysia	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	5
79.176.114.77	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	4
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	4
134.147.203.115	Germany	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	4

03-21-2015-00:00:10 to 03-22-2015-00:00:10

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	788
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	331
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	202
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	147
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	126
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	111
105.133.10.248	Morocco	147.237.77.216	dover.idf.il	12132: HTTP: BOIC DoS Tool	Block	90
192.187.103.114	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	66
46.19.85.196	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	24
197.15.201.137	Tunisia	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	22
85.159.206.101	Italy	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	22
105.133.232.243	Morocco	147.237.77.216	dover.idf.il	12132: HTTP: BOIC DoS Tool	Block	18
46.19.85.196	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	15
105.103.212.214	Algeria	147.237.77.216	dover.idf.il	12371: TCP: Hulk DDoS Tool	Block	8
89.216.115.6		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	7
212.34.12.155	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
77.125.14.59	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
46.116.237.41	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	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	4
84.108.45.104	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
37.187.129.166	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	4
88.150.187.210	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	4
69.201.190.137	United States	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.65.200.194	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
72.222.134.27	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	3
109.65.61.215	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
37.187.244.40	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	3
77.125.124.1	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
50.66.49.230	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
198.20.70.114	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	3
46.19.85.213	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
85.25.43.94	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	3
46.19.85.23	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.103.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	2
218.6.132.45	China	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	2

03-21-2015-00:00:10 to 03-22-2015-00:00:10

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	605
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	140
216.224.174.86	United States	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	48
37.142.93.49	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
62.90.202.62	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
81.243.149.162	Belgium	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	6
81.243.149.162	Belgium	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
81.243.149.162	Belgium	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
79.179.132.50	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
81.243.149.162	Belgium	147.237.76.44	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
109.253.144.235	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
81.243.149.162	Belgium	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
87.69.222.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
81.243.149.162	Belgium	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
212.154.192.124	Kazakstan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
81.243.149.162	Belgium	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
81.243.149.162	Belgium	147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
24.114.23.39	Canada	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	3
217.160.108.64	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
85.235.130.65	Italy	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
149.78.232.33	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.89	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.179.15.110	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.176.82	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	2
2.54.28.183	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.65.80.247	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.176.8.165	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.208.53	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.183.128.6	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	2
54.247.122.220	Ireland	147.237.72.166	aka.idf.il	ET WEB_SERVER PHP Crawler	2
213.8.129.139	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
77.127.181.233	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.79.5	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
93.173.149.125	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
217.132.209.1	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.130.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	2
66.102.6.202	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
46.116.218.13	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
183.136.216.7	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	2
85.250.40.188	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
195.238.181.159	Ukraine	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	2
149.88.49.36	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.85.182	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.102.254.116	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
122.228.207.77	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	2
79.178.29.188	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.134.60	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2

03-21-2015-00:00:10 to 03-22-2015-00:00:10

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
5.39.82.106	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5603
91.121.166.108	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3615
5.39.82.106	France	147.237.77.216	dover.idf.il		drop	drop	2390
5.39.82.106	France	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	2125
5.39.82.106	France	147.237.77.216	dover.idf.il	SAM rule	drop	drop	778
66.249.79.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	556
66.249.79.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	530
66.249.79.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	504
5.39.82.106	France	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	118
144.76.90.230	Germany	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	106
76.109.47.51	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	104
5.39.82.106	France	147.237.77.216	dover.idf.il	SYN retransmit with different sequence	Bad TCP sequence	monitor	92
82.169.240.25	Netherlands	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	88
101.171.255.247	Australia	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	87
187.39.3.206	Brazil	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	76
109.160.187.255	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	66
91.121.166.108	France	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	64
91.121.166.108	France	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	61
176.12.149.200	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
5.39.82.106	France	147.237.77.216	dover.idf.il		Bad TCP sequence	monitor	49
79.182.8.71	Israel	147.237.76.42	refuah.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
91.121.166.108	France	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	43
74.6.254.122	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	40
5.39.82.106	France	147.237.77.216	dover.idf.il	SYN retransmit with different sequence	Bad TCP sequence	alert	38
176.12.143.210	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
5.102.254.116	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	32
188.216.243.147	Italy	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.140.186	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.146.31	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.144.38	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.157.143	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.135.90	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
157.55.39.187	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
192.187.126.162	United States	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	28
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.147.130	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.150.161	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.149.217	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
109.253.144.32	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
186.4.31.150	Costa Rica	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	24
176.12.139.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
2.52.48.127	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	23
2.52.48.127	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	23
2.52.48.127	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	23
94.252.145.237	Syrian Arab Republic	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	21
77.127.203.21	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	21
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
188.139.227.98	Syrian Arab Republic	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	19
176.12.148.1	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.39.82.106	France	147.237.77.216	dover.idf.il	Too Many of the Same Response Code (400) in IP from 5.39.82.106	Block	1706
109.64.27.249	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/priv.dog.settings/getstatistics	Block	1121
85.250.204.42	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 85.250.204.42	Block	748
5.39.82.106	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	407
2.52.142.145	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.52.142.145	Block	284
46.240.43.83	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	240
66.249.79.58	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	103
176.12.137.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	101
176.12.140.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	96
66.249.79.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	95
66.249.79.74	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	81
144.76.90.230	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 144.76.90.230	Block	78
79.176.28.183	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 79.176.28.183	Block	49
216.224.174.86	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	48
77.126.39.243	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/tizmoret/faq/default.asp parameter	None	41
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	36
176.12.151.44	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.12.151.44	Block	29
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	29
176.12.136.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	27
216.224.174.86	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 216.224.174.86	Block	23
176.12.137.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	22
192.187.126.162	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.187.126.162	Block	22
176.12.147.11	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	18
5.39.82.106	France	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 5.39.82.106	Block	17
5.39.82.106	France	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 5.39.82.106	Block	17
5.39.82.106	France	147.237.77.216	dover.idf.il	Multiple Malformed URL from 5.39.82.106	Block	17
77.125.15.85	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	17
79.179.166.196	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.179.166.196	Block	16
17.142.151.181	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.181	Block	14
17.142.149.149	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.149.149	Block	14
192.99.39.235	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
41.137.70.162	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	11
144.76.195.119	Germany	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 144.76.195.119	Block	11
213.251.182.10	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	10
5.29.217.87	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	10
213.57.174.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	9
17.142.152.37	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.37	Block	9
176.12.151.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	9
17.142.151.79	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.79	Block	8
149.88.139.205	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	8
167.114.64.100	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	8
207.46.13.43	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.43	Block	8
17.142.144.105	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.144.105	Block	7
157.55.39.131	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.131	Block	7
176.12.149.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	7
192.116.126.125	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
84.94.170.156	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 84.94.170.156	Block	7
17.142.151.188	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.151.188	Block	6
17.142.152.47	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.47	Block	6
17.142.152.153	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.152.153	Block	6