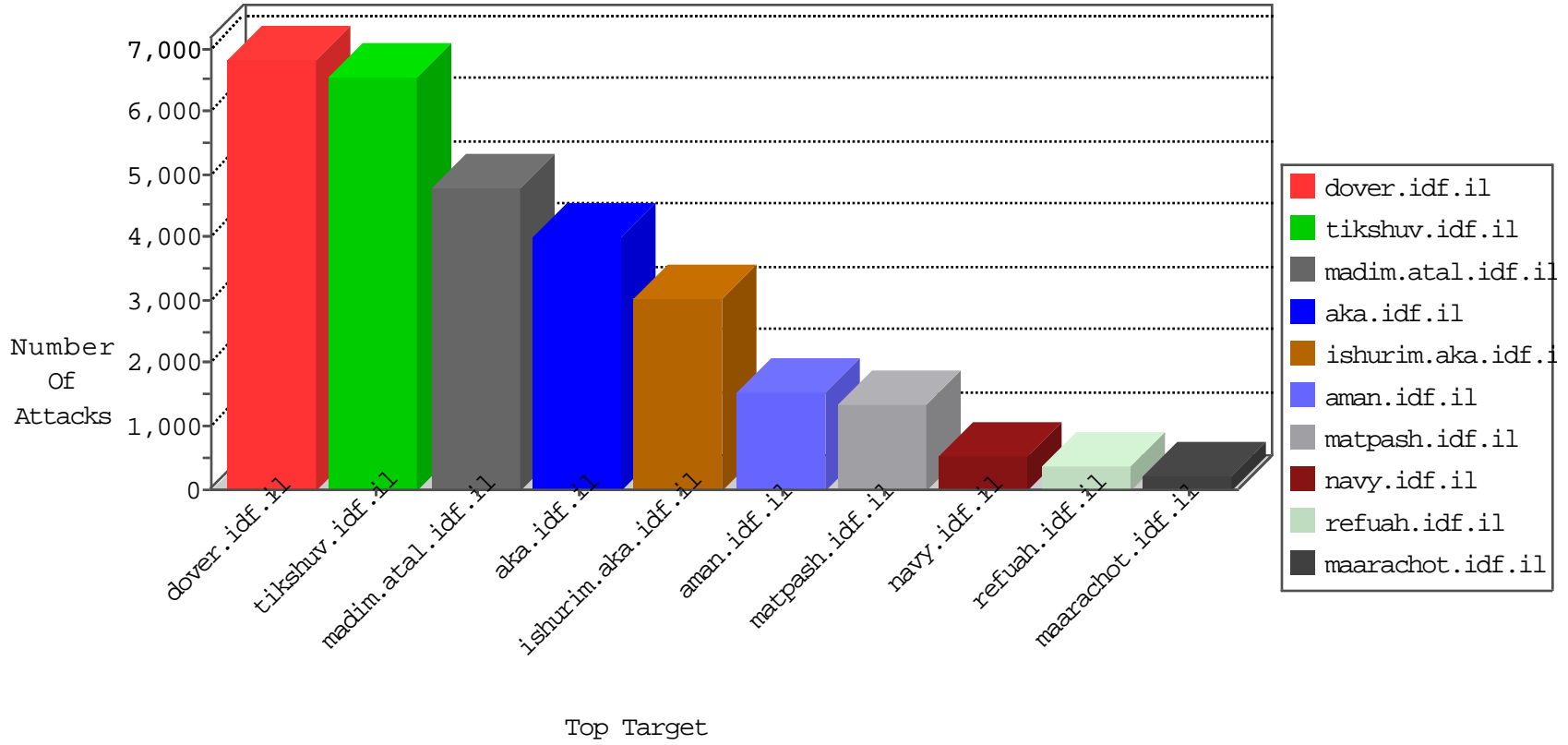


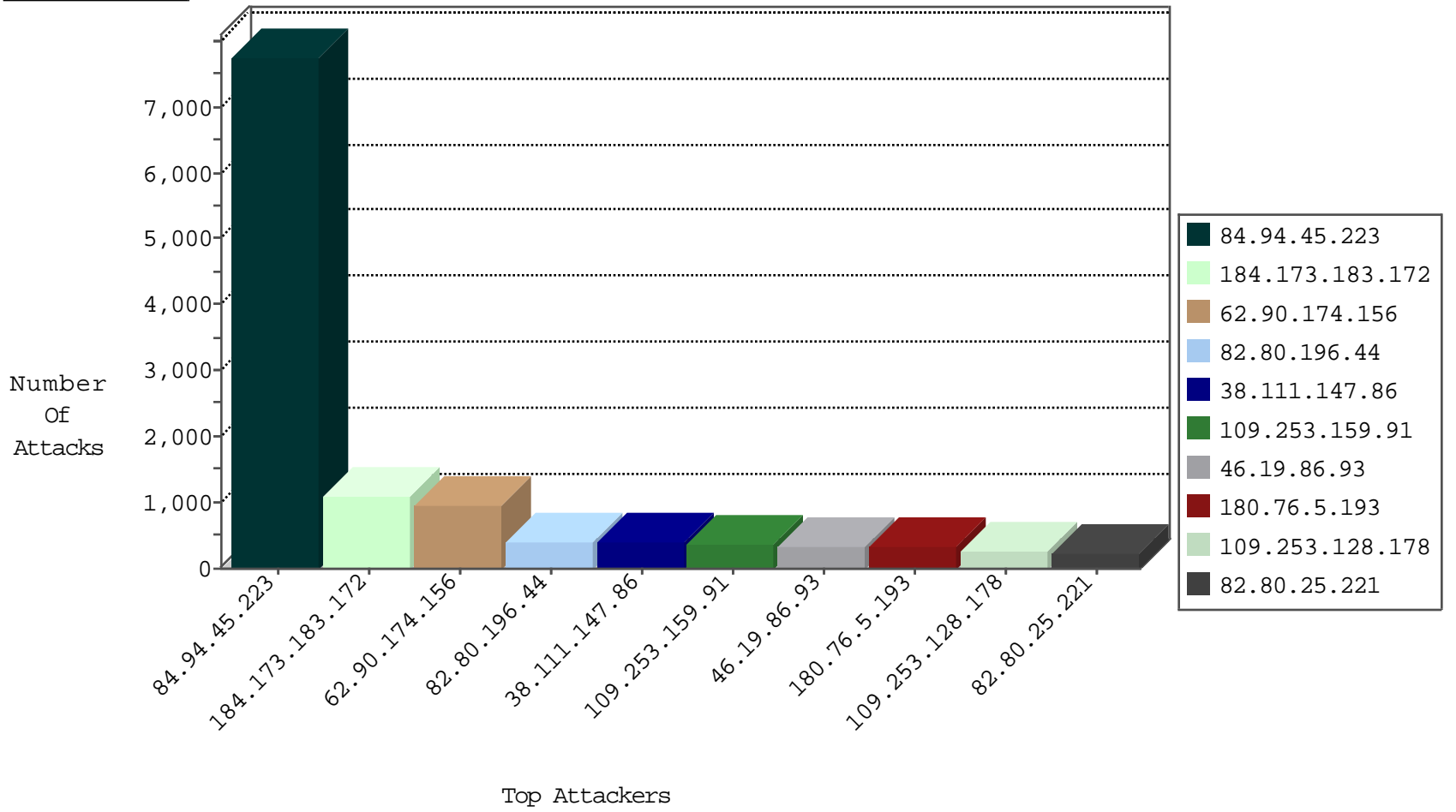
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	IP_Map.site	Name	Device Action	Sum(Packet_Count)
66.249.93.218	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3504
46.121.206.121	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	765
89.139.40.62	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	531
79.182.218.206	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	513
213.57.153.144	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	465
84.109.244.24	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	375
5.29.70.42	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	372
46.19.86.171	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	283
149.78.255.25	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	278
95.86.106.66	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	252
66.249.67.25	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	250
149.78.141.116	United States	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	224
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	221
82.102.141.218	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	212
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	196
87.68.157.109	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	175
109.64.61.157	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
212.199.149.78	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	161
84.94.46.199	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	155
37.46.36.173	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	152
80.246.137.173	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	148
95.86.117.179	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
85.250.229.211	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
79.182.101.239	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
82.102.141.212	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	120
46.19.85.58	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	108
46.120.178.90	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	105
77.125.95.104	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
46.19.86.79	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	93
199.203.172.65	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
46.19.86.53	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
46.19.86.113	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	86
2.54.44.8	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	81
5.102.206.170	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
93.172.132.253	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	76
213.57.239.146	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
109.160.241.207	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	75
109.160.251.43	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	73
77.125.144.206	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-TLS-renegotiation-Cli	dest-reset	71
46.19.85.58	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	66
66.249.67.123	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	66
77.125.101.6	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
37.26.148.226	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
93.172.147.61	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
46.19.85.91	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	61
85.64.76.140	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
82.102.141.199	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	59
46.120.178.90	Israel	147.237.72.167	ishurim.aka.idf.i	Anomaly-SSL-renegotiation-Cli	dest-reset	53
82.102.141.252	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	45

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.94.45.223	Israel	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	6293
84.94.45.223	Israel	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	941
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	644
84.94.45.223	Israel	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	533
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	424
180.76.5.193	China	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	315
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	180
89.139.173.72	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	76
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	39
98.126.107.165	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
123.180.234.186	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
192.115.248.2	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	24
31.154.10.107	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	22
207.232.27.5	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	12
123.180.234.186	China	147.237.77.216	dover.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	10
212.179.162.114	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	8
82.211.223.3	Denmark	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	7
81.218.251.250	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	5
46.120.249.163	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
188.138.9.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	5
176.126.252.12	Romania	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	5
85.25.103.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	4
79.176.185.40	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
116.8.99.232	China	147.237.76.31	nakchal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
5.29.97.163	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
116.8.99.232	China	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
212.227.38.247	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
89.31.57.5	Italy	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	4
5.29.185.84	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
116.8.99.232	China	147.237.76.86	navy.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
198.20.70.114	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_P-N_40-59	Permit	4
186.89.249.35	Venezuela	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
108.46.4.227	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	4
198.20.70.114	United States	147.237.8.45	e.eitan.idf.il	DVRep_P-N_40-59	Permit	4
116.8.99.232	China	147.237.76.30	himush.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
188.174.170.36	Germany	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
198.20.70.114	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	3
185.4.227.194	Turkey	147.237.77.235	sviva.idf.il	C1000098: Block - dns poisoning	Block	3
198.20.70.114	United States	147.237.0.200	m4u.idf.il	DVRep_P-N_40-59	Permit	3
85.25.103.50	Germany	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	3
81.7.8.101	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	3
178.32.227.252	France	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	3
37.19.120.95	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
143.199.125.10	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	3
85.25.103.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	3

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	230
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	94
2.54.171.124	Israel	147.237.72.156	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	12
66.249.67.36	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	11
37.142.178.218	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
37.56.125.100	Romania	147.237.77.216	dover.idf.il	ET SCAN Vega Web Application Scan	2
93.172.142.208	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
84.94.182.244	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.131	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
79.183.210.2	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.19.86.27	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
188.138.9.51	Germany	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
109.253.140.43	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.120.249.163	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	2
121.42.54.18	China	147.237.76.198	e.yohanan.idf.il	ET SCAN NMAP -sS window 1024	2
93.173.21.198	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.66	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	2
46.19.86.113	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
5.29.8.230	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
85.250.10.33	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
176.12.140.243	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
121.42.54.18	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	2
79.177.126.240	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
72.143.61.205	Canada	147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
84.109.57.116	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.54.250	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
149.129.31.115	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
115.231.218.23	China	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
89.248.162.228	Netherlands	147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.126.29.129	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
193.169.70.108	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.240.144.64	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
1.93.34.226	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
104.43.193.6		147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.199	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
5.102.253.130	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.169.45.231	United Kingdom	147.237.0.19	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
87.209.151.206	Netherlands	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
222.186.134.6	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
69.29.194.241	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.32.177.231	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.78.192	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
121.42.54.18	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
80.179.223.31	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
207.2.32.65	United States	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.66	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	386
38.111.147.86	United States	147.237.76.86	navy.idf.il		drop	drop	319
208.54.5.204	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	168
199.30.21.202	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	102
46.121.207.194	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	81
185.26.180.24	Europe	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	78
46.19.85.199	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	69
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	66
46.19.86.103	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	66
79.178.131.20	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	64
79.178.168.219	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	59
66.249.81.203	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	56
95.130.88.141	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	54
136.243.36.96	Germany	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	50
79.177.173.227	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	49
109.253.147.149	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
77.64.254.65	Germany	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
109.65.75.246	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	45
184.32.7.70	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
82.80.34.112	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
176.12.149.205	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
132.68.245.47	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
90.212.66.202	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	40
84.95.123.108	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	39
31.210.178.241	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
132.3.65.82	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.93.155	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
79.183.155.51	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
82.145.221.116	Europe	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	32
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
62.0.58.186	Israel	147.237.72.167	ishurim.aka.idf.i	First packet isn't SYN	drop	drop	32
31.168.132.131	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
109.253.133.215	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
79.183.224.136	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
84.228.153.173	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
62.0.58.186	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	31
176.12.142.95	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.159.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
82.80.142.80	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
41.131.117.128	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
109.253.134.90	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
157.55.39.191	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.150.67	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.139.52	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.138.159	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.148.25	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.139.99	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
176.12.150.40	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
62.90.174.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	937
109.253.159.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	355
46.19.86.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	325
109.253.128.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	253
46.19.86.195	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.195	Block	221
109.253.137.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	198
46.19.85.144	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.144	Block	195
82.102.141.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
82.102.141.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	175
109.253.129.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	161
109.253.129.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	138
50.75.153.195	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 50.75.153.195	Block	116
109.253.140.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	108
109.253.157.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	104
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	103
109.253.136.156	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.136.156	Block	98
176.12.139.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	92
176.12.150.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
176.12.140.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	86
46.19.85.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	84
109.253.143.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	78
109.253.146.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	59
109.253.156.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
176.12.144.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	52
109.253.138.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
176.12.151.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	49
46.19.86.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	47
176.12.141.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
213.8.16.83	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 213.8.16.83	Block	40
176.224.50.32	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 176.224.50.32	Block	38
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	37
109.253.141.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	36
176.12.142.183	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.142.183	Block	33
176.12.136.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
176.12.136.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
109.253.143.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	31
132.72.172.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
37.26.147.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
77.125.161.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.125.161.159	Block	23
176.224.50.32	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 176.224.50.32	Block	22
2.54.38.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	21
176.12.142.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	19
109.67.68.176	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	None	19
17.228.4.81	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.tehila.gov.il/errorpage/templates/errorpage.aspx	Block	18
176.224.50.32	Saudi Arabia	147.237.77.216	dover.idf.il	PHP Attempt	Block	17
93.172.168.95	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 93.172.168.95	Block	16
213.8.98.2	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	14
176.12.138.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	13
109.253.129.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	13