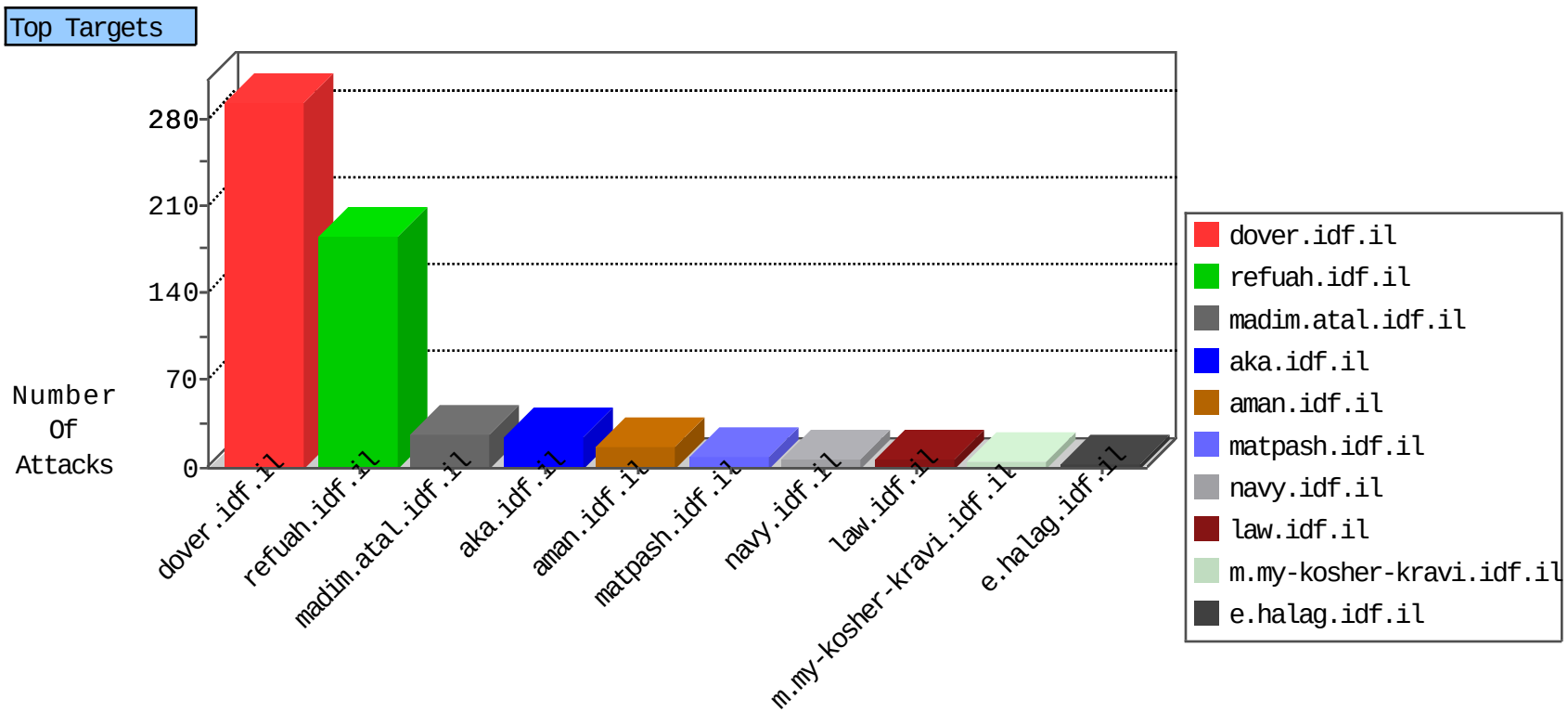
04-24-2015-22:03:06 to 04-24-2015-23:03:06

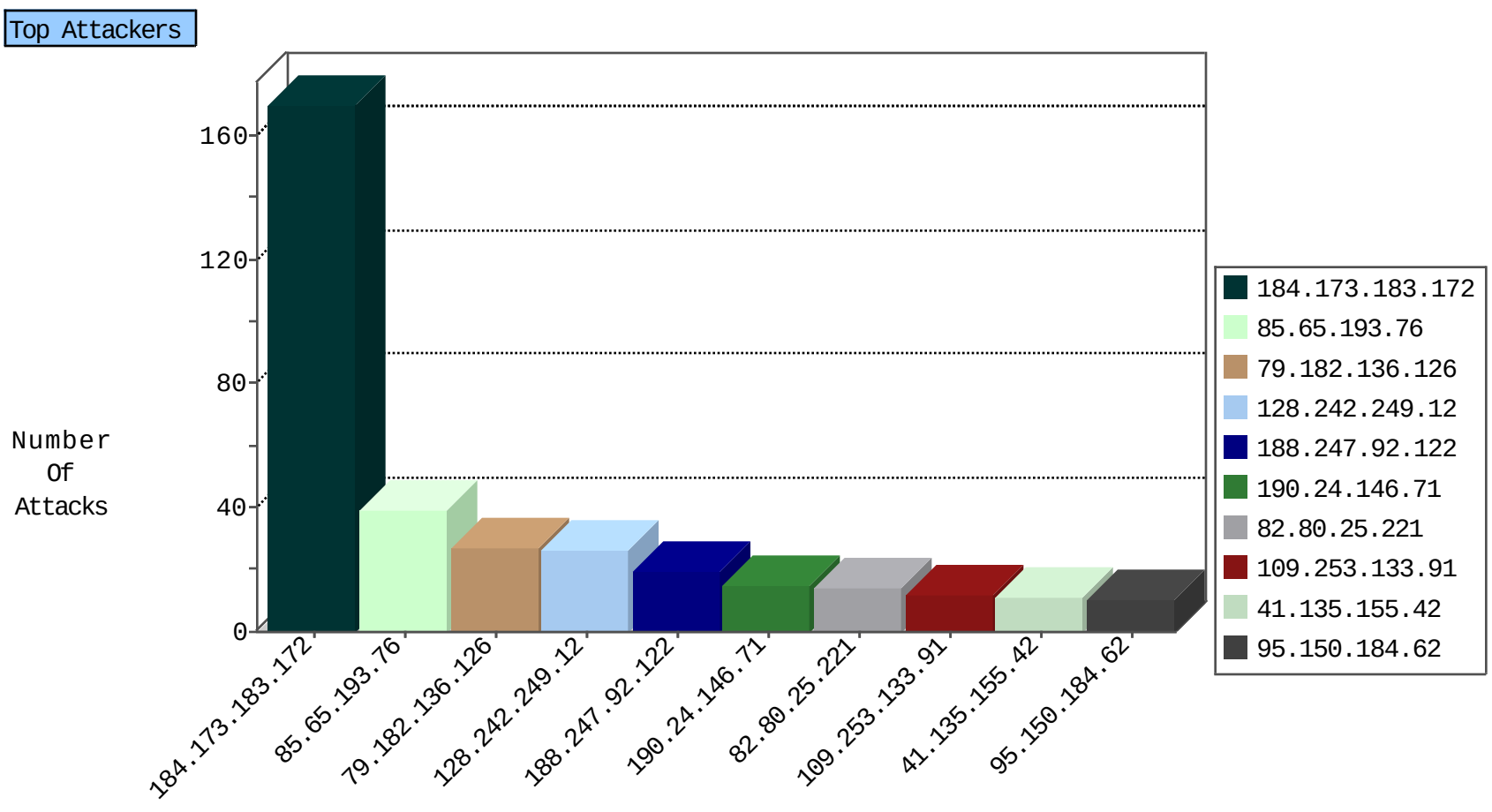
IDF Under Attack
04-24-2015-22:03:06

Top Targets



Top Target

Top Attackers



Top Attackers

04-24-2015-22:03:06 to 04-24-2015-23:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.73.209	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	18088
41.135.155.42	South Africa	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9207
66.249.65.43	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6456
47.19.118.253	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5406
66.249.93.239	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4792
66.249.93.245	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4366
66.249.65.41	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	4038
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3387
220.181.108.177	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	2782
220.181.108.145	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	1199
79.183.37.102	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	425
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	330
108.59.253.71	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	143
46.117.237.78	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	87
46.116.181.62	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
185.32.177.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
172.56.26.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	4
80.246.133.18	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
67.242.47.47	United States	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	3
89.139.161.63	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
188.247.92.122	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
37.26.146.246	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
85.250.116.175	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
85.250.243.121	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
66.249.79.58	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
71.6.165.200	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
66.249.73.217	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
79.178.103.195	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.249.73.201	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
79.183.37.102	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.65.39	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
23.94.190.194	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-24-2015-22:03:06 to 04-24-2015-23:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	170
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	26
89.210.28.128	Greece	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
70.49.44.112	Canada	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.123	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1

04-24-2015-22:03:06 to 04-24-2015-23:03:06

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	14
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.65.26	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
213.57.178.33	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.34	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
119.90.139.72	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
91.224.132.118	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.246	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
31.184.194.115	Russian Federation	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
31.184.194.115	Russian Federation	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
182.23.39.210	Indonesia	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 3072	1
182.23.39.210	Indonesia	147.237.76.86	navy.idf.il	ET SCAN NMAP -f -sS	1
119.90.139.72	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
89.40.71.178	Romania	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.34.246	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
61.183.128.6	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
213.229.75.6	United Kingdom	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
31.184.194.115	Russian Federation	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
182.23.39.210	Indonesia	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 2048	1

04-24-2015-22:03:06 to 04-24-2015-23:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
85.65.193.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
188.247.92.122	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
190.24.146.71	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
109.253.133.91	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
64.202.95.92	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.79.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
151.66.138.242	Italy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
41.135.155.42	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
79.183.37.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
2.52.5.225	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.79.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
95.150.184.62	United Kingdom	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
95.150.184.62	United Kingdom	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
84.94.103.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.176.155.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
162.243.222.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.67.195.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
24.248.57.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.64.9.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.133.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.65.124.247	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.173.181.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.181.179.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
82.232.62.250	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
173.252.74.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
85.234.133.149	United Kingdom	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
198.48.92.104	United States	147.237.76.34	yohalan.idf.il		drop	drop	1
149.88.9.39	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
173.252.74.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
85.234.133.149	United Kingdom	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
80.12.59.131	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
201.57.249.2	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
79.178.203.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
128.232.110.28	United Kingdom	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
85.250.116.175	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
96.246.228.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
79.180.96.117	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
139.228.163.26	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
82.80.179.222	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
5.108.119.160	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.66.177.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
198.48.92.104	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.120.161.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
141.212.122.148	United States	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

04-24-2015-22:03:06 to 04-24-2015-23:03:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.182.136.126	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.182.136.126	Block	26
66.249.73.238	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//mobile/	Block	3
213.57.47.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	3
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	2
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	2
176.12.147.156	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
79.177.27.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
176.12.149.197	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
84.110.215.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
38.99.97.97	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/â€Ž	Block	1
116.39.92.155	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1038-en/dover.aspx/rk=0/rs=yifi30zu7ewhem9kdcyykmwjve0-	Block	1
79.182.136.126	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.73.222	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//mobile/	Block	1
188.138.17.205	France	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
84.228.140.5	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.81.222	Israel	147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../favicon.ico	Block	1
46.19.86.171	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.86.171	Block	1
149.88.24.118	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.230	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mobile/	Block	1
192.111.149.138	United States	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1
2.54.10.109	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/aaron.stm	Block	1
46.19.86.171	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	1
157.55.39.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/brothers/skira/default.asp-catid=57479&docid=	Block	1
79.182.178.80	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
192.111.149.138	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
2.54.61.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
94.23.30.222	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
62.210.114.129	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/8/3198.pdf/trackback/	Block	1
83.149.35.59	Russian Federation	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	1
37.142.191.56	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.144.11	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1

04-24-2015-22:03:06 to 04-24-2015-23:03:06