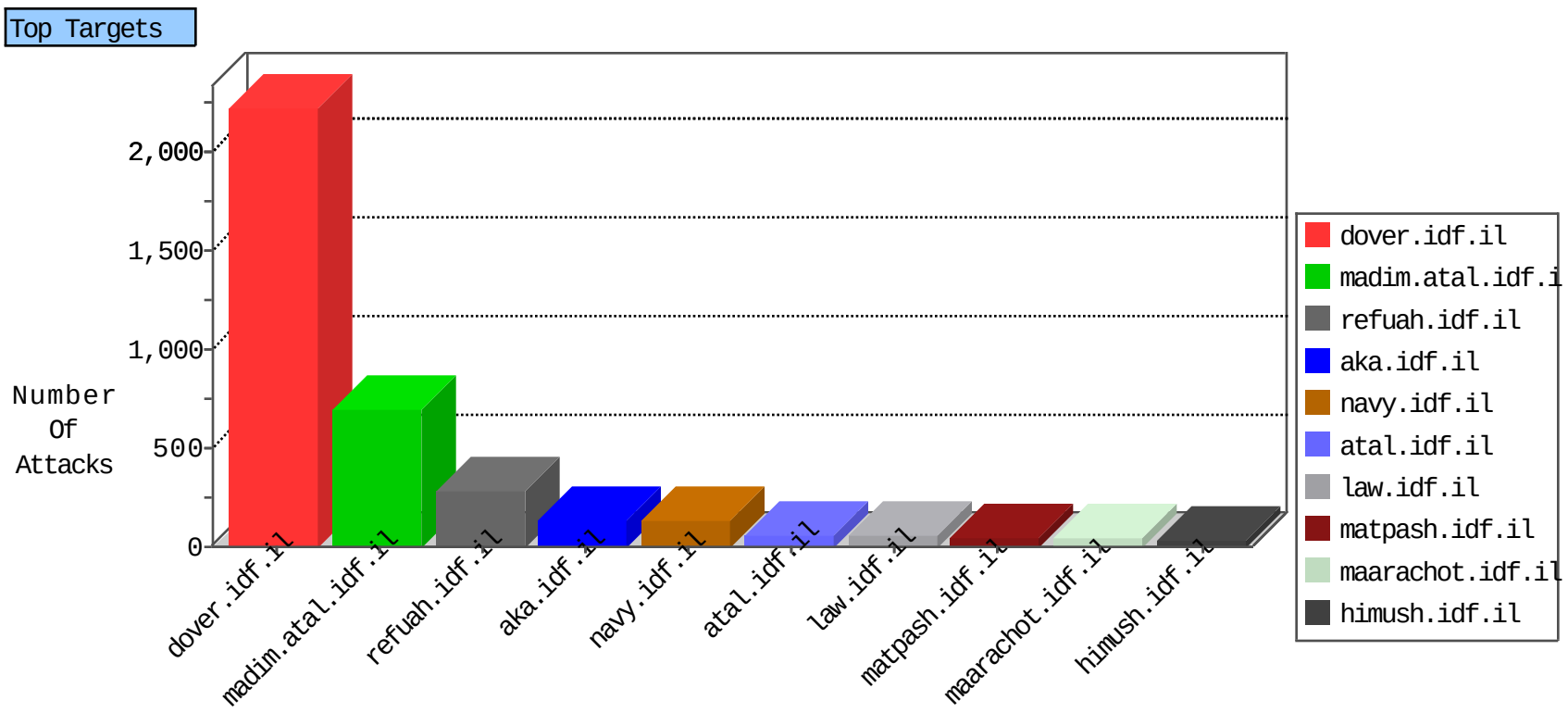
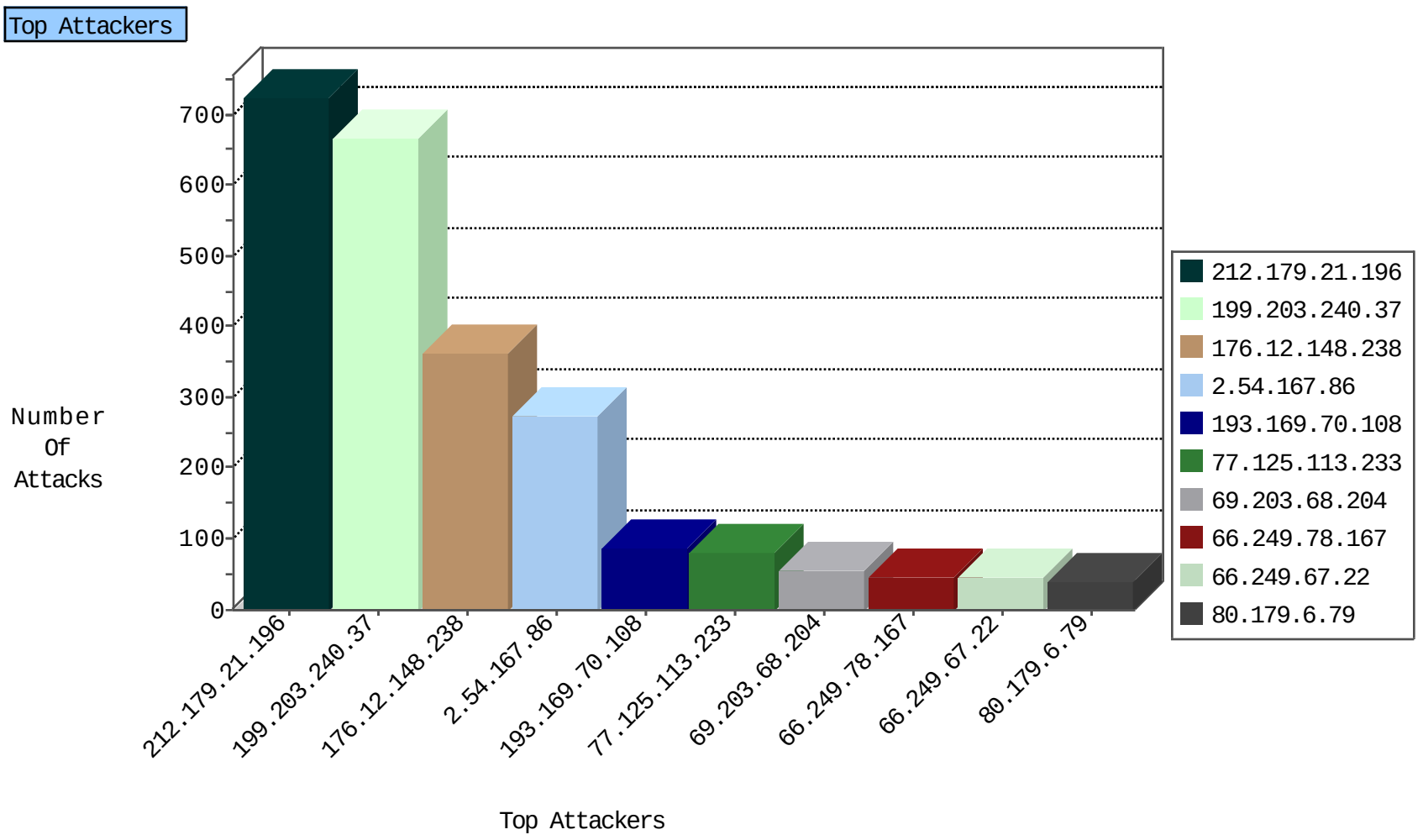
04-12-2015-07:03:05 to 04-12-2015-08:03:05

IDF Under Attack
04-12-2015-07:03:05

Top Targets



Top Attackers



04-12-2015-07:03:05 to 04-12-2015-08:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	193
220.181.108.149	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	69
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	47
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	47
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	37
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	33
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	30
66.249.93.168	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	29
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	28
66.249.78.86	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	26
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	23
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	21
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	16
66.249.64.136	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	15
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	15
66.249.93.176	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	14
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	13
66.249.64.128	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	13
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	13
66.249.78.242	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	12
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	11
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	10
66.249.93.242	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.64.63	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	10
66.249.93.245	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	9
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.64.147	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	9
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	8
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	8
66.249.78.248	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.64.55	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	7
66.249.64.59	United States	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	7
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.93.172	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.89.103	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.78.60	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	5
66.249.65.200	United States	147.237.0.19	madim.atal.idf.il	Block_Ip_Web_In	drop	5

04-12-2015-07:03:05 to 04-12-2015-08:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
2.54.130.39	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
212.143.156.51	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

04-12-2015-07:03:05 to 04-12-2015-08:03:05

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
43.255.191.165	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
27.50.132.61	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
104.171.114.254		147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
104.171.114.254		147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
58.20.54.249	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
46.162.115.130	Sweden	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
203.150.228.208	Thailand	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
27.50.132.61	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
27.50.132.61	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
104.171.114.254		147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1

04-12-2015-07:03:05 to 04-12-2015-08:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	725
199.203.240.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	666
193.169.70.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	88
77.125.113.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	81
69.203.68.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
80.179.6.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
2.54.167.86	Israel	147.237.0.19	madim.atal.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
109.65.3.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
109.253.139.138	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
46.19.85.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
109.160.219.205	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
109.253.147.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
39.36.69.204	Pakistan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
109.253.135.37	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
79.182.172.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
176.193.217.81	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
46.19.86.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
128.242.249.13	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	7
46.19.85.21	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	7
176.67.58.69	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.118	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.85.134	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
27.32.157.149	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.85.118	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.121.242.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
62.128.48.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.21	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	4
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
84.228.144.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.82	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
93.172.20.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
84.228.49.188	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
89.138.25.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3

04-12-2015-07:03:05 to 04-12-2015-08:03:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.148.238	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.12.148.238	Block	362
2.54.167.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	240
176.12.146.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
176.12.140.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
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
52.1.33.44	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/shared/usercontrols/headerupper/	Block	2
2.52.43.100	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
52.4.217.78	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
91.200.12.54	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
2.52.42.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
149.78.253.190	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.172.68.148	Europe	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
54.207.82.68	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
217.195.176.194	Denmark	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
37.26.146.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.170.44.157	United Kingdom	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.0.126	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
110.22.129.147	Australia	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0113-3.stm	Block	1
217.195.176.194	Denmark	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
41.190.226.80	Cameroon	147.237.77.74	law.idf.il	Distributed Admin Blocking	Block	1
79.170.44.157	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
52.4.217.78	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/klali/null	Block	1
212.179.197.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
115.25.81.71	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
41.190.226.80	Cameroon	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
52.4.217.78	United States	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/rights/asp/info.asp	None	1
212.179.197.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0217-2.stm	Block	1
125.209.235.178	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
46.19.85.21	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
176.12.148.238	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
93.172.20.88	Israel	147.237.76.30	himush.idf.il	Unauthorized Method POST for www.chimush.atal.idf.il/1340-he/himush.aspx	None	1
54.207.82.68	United States	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
217.69.133.72	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
37.16.72.139	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1

04-12-2015-07:03:05 to 04-12-2015-08:03:05