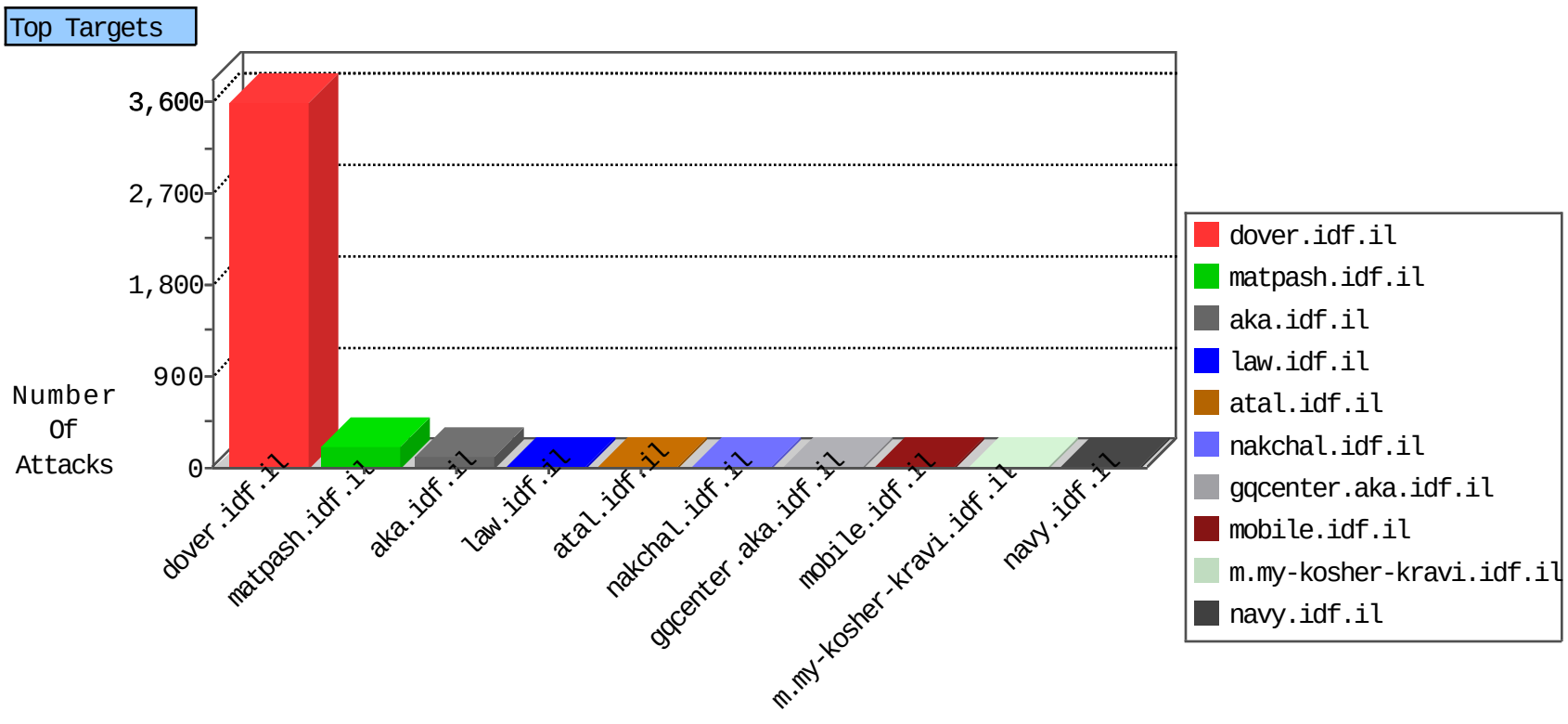
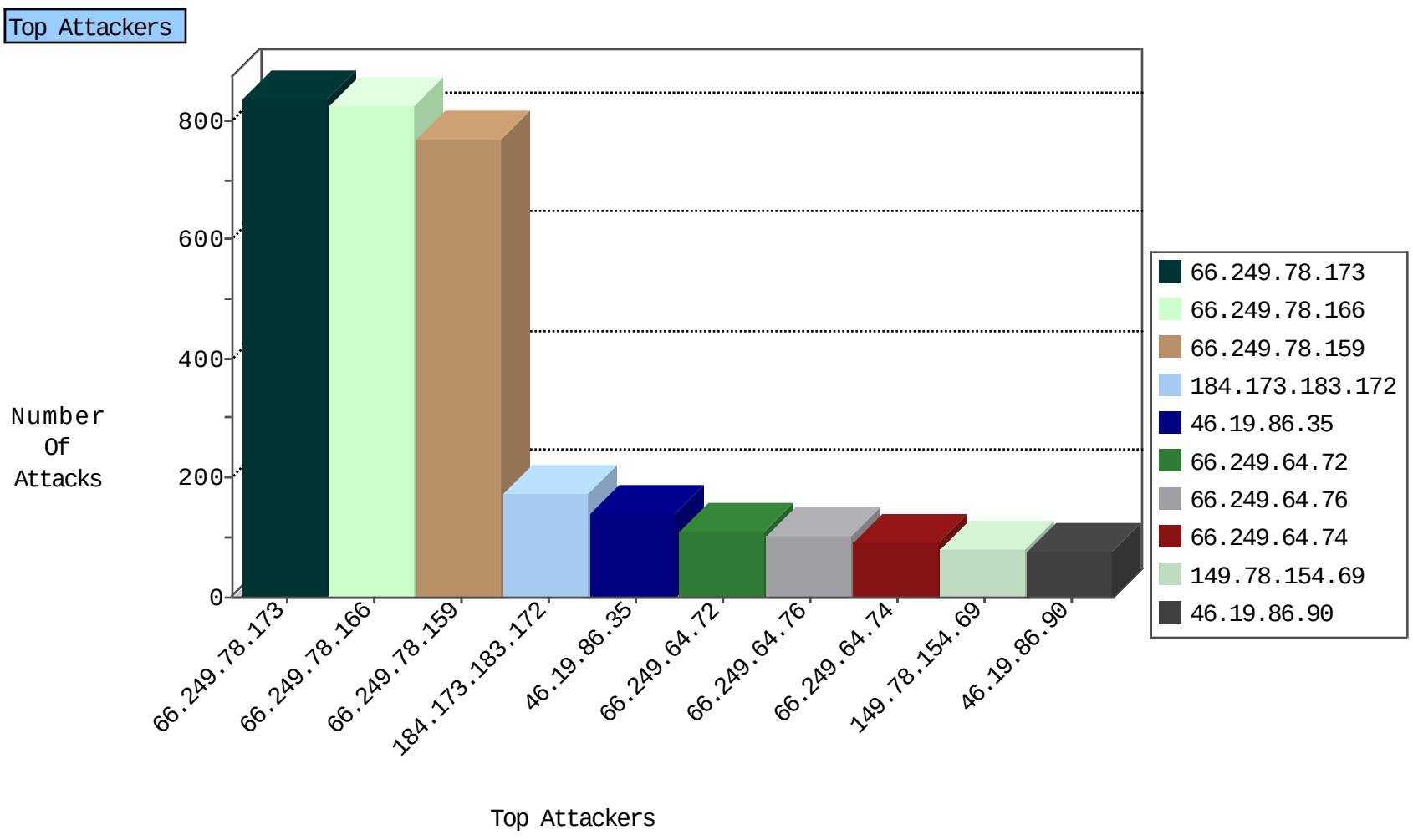
05-02-2015-02:03:03 to 05-02-2015-03:03:03

IDF Under Attack
05-02-2015-02:03:03





05-02-2015-02:03:03 to 05-02-2015-03:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3728
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2859
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	210
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
210.195.124.143	Malaysia	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
66.240.192.138	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

05-02-2015-02:03:03 to 05-02-2015-03:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	173
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	38
98.31.12.102	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	3
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.65.4.158	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1

05-02-2015-02:03:03 to 05-02-2015-03:03:03

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	7
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.75.44	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
61.175.255.61	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
218.77.79.43	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
208.88.126.181	United States	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
178.32.251.100	France	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
104.167.117.197		147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.161	Japan	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
221.229.166.28	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
61.175.255.61	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
221.143.48.200	Korea, Republic of	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.161	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
61.175.255.61	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
218.77.79.43	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
104.167.117.197		147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.161	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
104.167.117.197		147.237.77.121	e.navy.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.161	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
221.143.48.200	Korea, Republic of	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1

05-02-2015-02:03:03 to 05-02-2015-03:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.86.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	140
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	129
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	122
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	121
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	88
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	81
46.19.86.90	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	78
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	72
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
46.117.9.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	45
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
66.249.64.72	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
189.217.177.162	Mexico	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
66.249.64.76	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
192.114.23.18	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
64.79.133.117	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	17
179.159.214.157	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
66.249.64.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
68.186.169.231	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
157.55.39.47	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.249.75.13	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
66.249.64.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
87.126.139.233	Bulgaria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
66.249.64.74	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
69.145.43.79	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
79.176.29.118	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
195.154.235.127	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
209.133.111.215	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
66.249.64.76	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
157.55.39.46	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
184.173.183.174	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
98.31.12.102	United States	147.237.77.216	dover.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	225
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	206
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	192
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	182
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	180
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	178
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	174
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	173
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	171
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	49
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	25
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	25
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	23
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	21
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	21
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	21
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	20
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.197	Block	13
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	10
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	10
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.190	Block	5
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	3
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	3
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	3
157.55.39.46	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.46	Block	2
212.224.119.139	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
178.137.166.68	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	2
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
176.12.139.202	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.101	Block	2
185.53.44.90		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.69.34	Block	1
185.53.44.71		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0108-3.stm	Block	1
84.94.77.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.30.25.124	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.53.44.123		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.53.44.123	Block	1
66.249.64.130	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.130	Block	1
185.53.44.53		147.237.72.166	aka.idf.il	Unknown Parameter catId in aka.idf.il/patzar/home/	None	1
178.137.19.143	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
185.53.44.95		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.53.44.95	Block	1
66.249.75.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	1
185.53.44.90		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1125-2.stm	Block	1
66.249.64.144	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/31082010shvuee.aspx	Block	1
185.53.44.63		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info12.stm	Block	1
185.53.44.202		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.53.44.202	Block	1