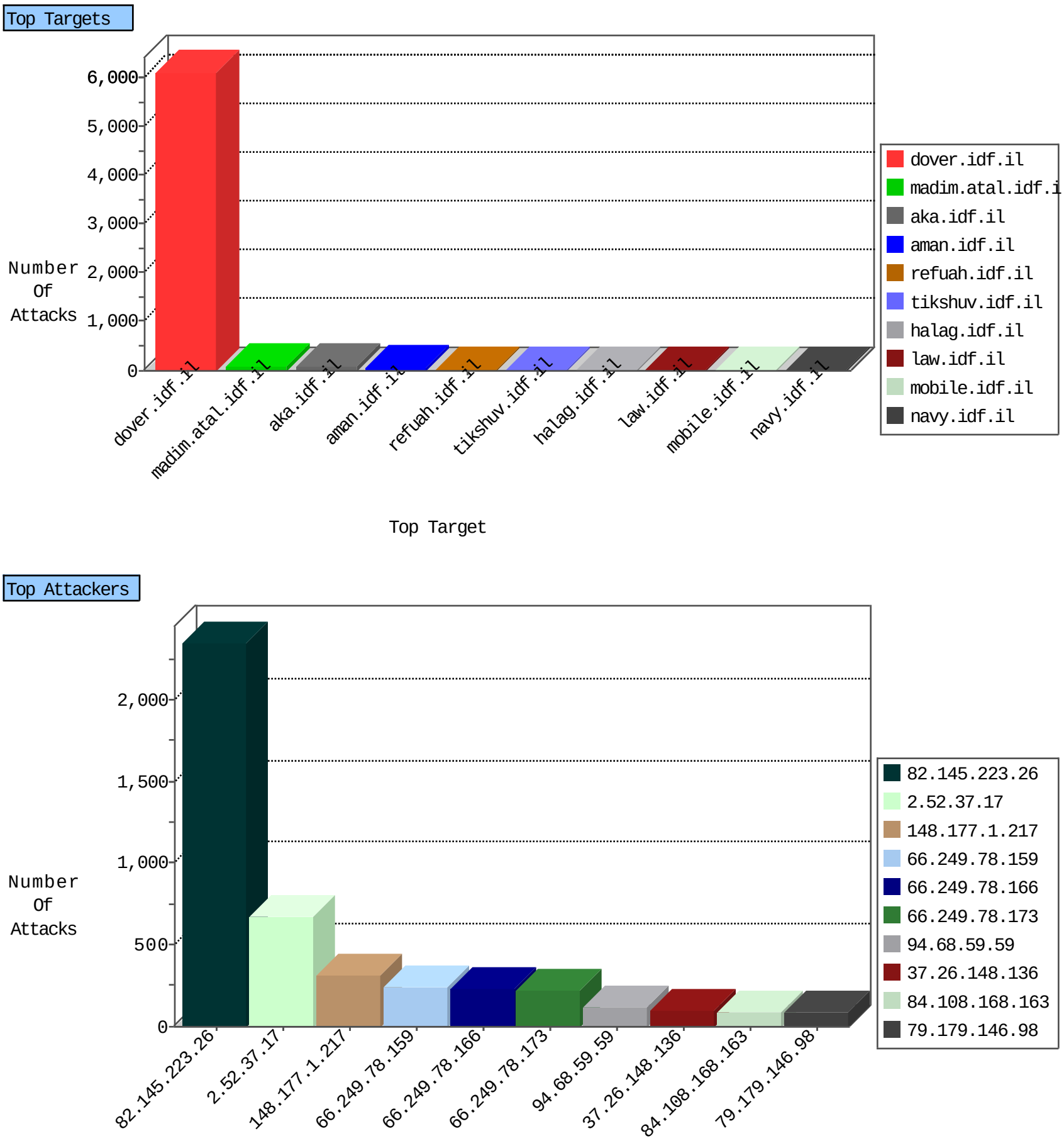
05-01-2015-20:03:01 to 05-01-2015-21:03:01

IDF Under Attack
05-01-2015-20:03:01

Top Targets



Top Attackers

05-01-2015-20:03:01 to 05-01-2015-21:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
84.108.9.212	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	170
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	108
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	89
5.29.117.52	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
84.110.86.177	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	84
5.28.185.164	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
5.22.129.154	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
10.0.0.8		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.216.62	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
118.237.19.113	Japan	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
62.90.219.214	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
124.232.142.220	China	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

05-01-2015-20:03:01 to 05-01-2015-21:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.186.150.169	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
94.230.86.222	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
149.78.219.106	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1

05-01-2015-20:03:01 to 05-01-2015-21:03:01

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	8
144.99.8.10	United States	147.237.77.216	dover.idf.il	GPL SCAN myscan	2
144.99.8.10	United States	147.237.77.216	dover.idf.il	INDICATOR-SCAN myscan	2
84.108.94.45	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.16.232.231	India	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
220.178.78.138	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
220.178.78.138	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.165	Japan	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
193.107.17.72	Russian Federation	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.165	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
61.183.128.6	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.143.48.200	Korea, Republic of	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 3072	1
61.16.232.231	India	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
221.143.48.200	Korea, Republic of	147.237.72.217	e.idf.il	ET SCAN NMAP -f -sS	1
58.20.54.249	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
220.178.78.138	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.165	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
132.74.95.19	Israel	147.237.77.170	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
43.255.191.165	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.16.232.231	India	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
221.143.48.200	Korea, Republic of	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 2048	1

05-01-2015-20:03:01 to 05-01-2015-21:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.145.223.26	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2350
2.52.37.17	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	625
148.177.1.217	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	318
94.68.59.59	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	121
37.26.148.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	100
84.108.168.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	92
79.179.146.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	89
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	70
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	66
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
46.19.85.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
85.76.179.30	Finland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	52
41.13.246.91	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
188.161.7.30	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
82.145.220.110	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
77.126.240.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
105.225.215.100	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
157.55.81.9	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
23.242.178.102	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
85.65.122.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
93.173.239.235	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
104.172.236.112		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
199.30.25.87	United States	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	19
66.249.64.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
128.226.163.200	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
79.179.21.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.64.76	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
149.78.57.191	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
84.109.56.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
69.175.127.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
207.46.13.8	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
46.121.136.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
82.132.224.222	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
84.108.94.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
64.62.201.13	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.43.85	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.43.85	Block	88
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	30
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	23
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	21
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	18
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	16
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	15
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	14
36.251.25.230	China	147.237.76.42	refuah.idf.il	Multiple Admin Blocking from 36.251.25.230	Block	7
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	6
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	6
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	6
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
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
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	3
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	3
87.69.241.92	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 87.69.241.92	Block	3
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	3
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
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	2
185.53.44.45		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
79.177.168.27	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
207.46.13.114	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/unselecatble.aspx	Block	1
46.229.164.111	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.53	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
185.53.44.98		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//chinuch/printpreview/	Block	1
85.214.247.93	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/search.asp	Block	1
185.53.44.63		147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
176.50.71.107	Russian Federation	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
213.57.182.229	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/650-he/patzar.aspx	Block	1
207.46.13.19	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/yohalan/main/main.asp	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.5	Block	1
185.53.44.92		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/eurl.axd/5df0c720696cf5499921079db353c477/	Block	1
88.208.252.197	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	1
79.183.122.149	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
185.53.44.47		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//kamlar/printpreview/	Block	1
212.179.8.162	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
46.229.164.113	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/110539.pdf,	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/april/08.stm	Block	1
66.249.75.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/templates/general/general.aspx	Block	1
185.53.44.200		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//kamlar/eurl.axd/85cb72ee4185cb41bf92a8916db47e4d/	Block	1
85.250.125.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1