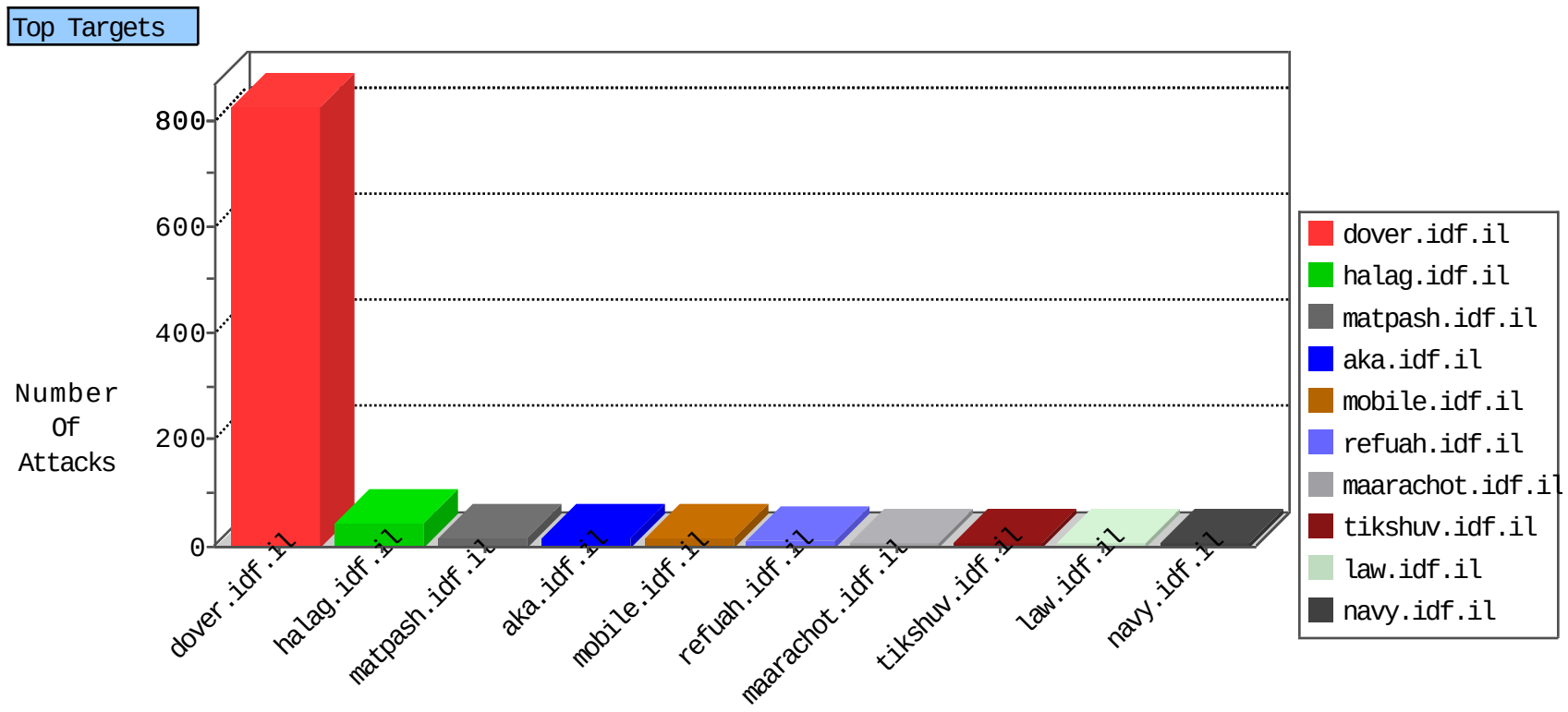
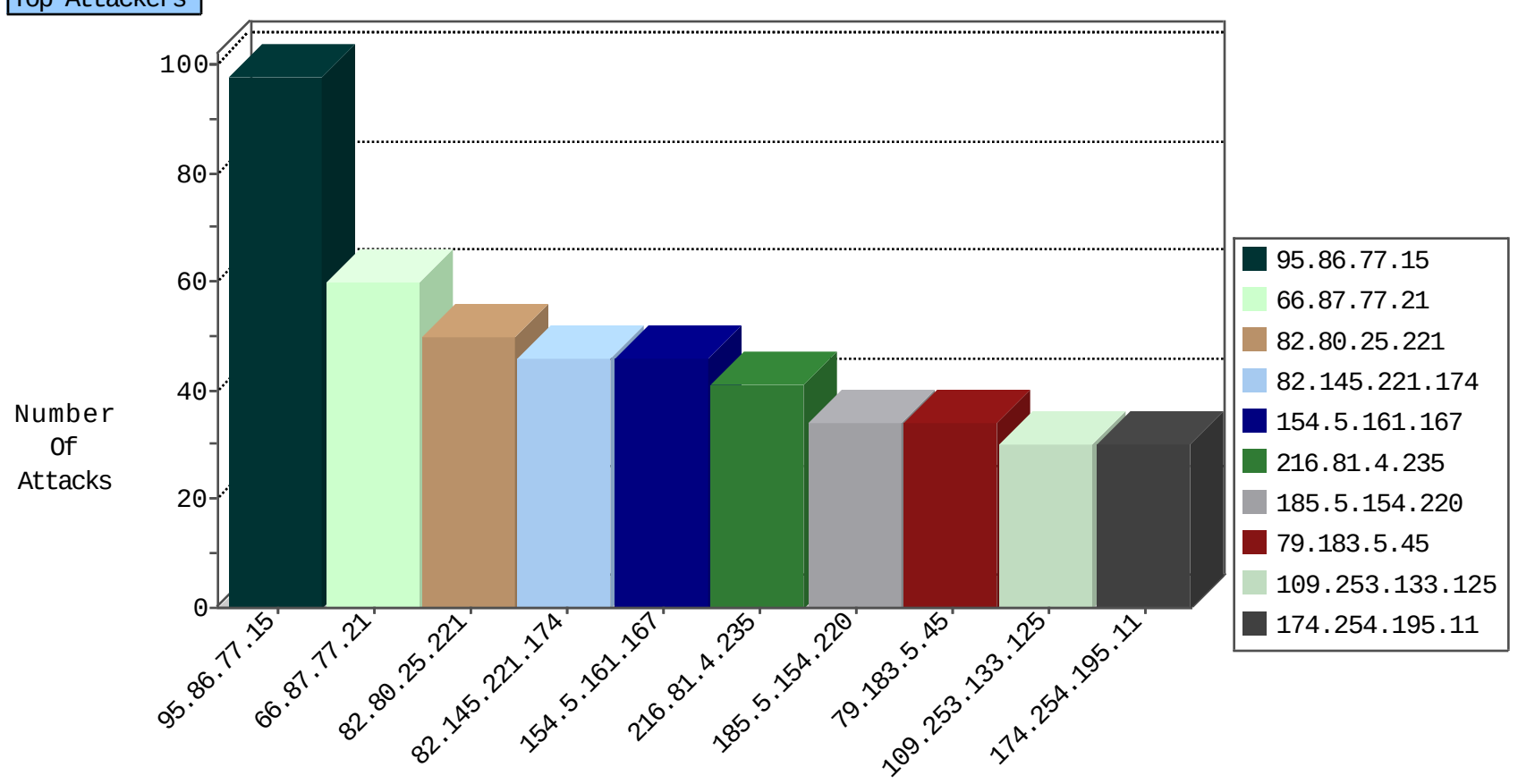
04-19-2015-04:03:08 to 04-19-2015-05:03:08

IDF Under Attack
04-19-2015-04:03:08

Top Targets



Top Attackers



04-19-2015-04:03:08 to 04-19-2015-05:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.87	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	2831
185.26.180.135	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2519
176.12.142.29	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	2
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

04-19-2015-04:03:08 to 04-19-2015-05:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.35	akaws.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
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1

04-19-2015-04:03:08 to 04-19-2015-05:03:08

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	22
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	7
66.249.64.21	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.10	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
217.70.146.17	Italy	147.237.72.166	aka.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
119.147.172.162	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
119.147.172.162	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.228.207.77	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
119.147.172.162	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.228.207.77	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
119.147.172.162	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.228.207.77	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
119.147.172.162	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
122.228.207.77	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
212.47.248.0	France	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
119.147.172.162	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
119.147.172.162	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
119.147.172.162	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
119.147.172.162	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.228.207.77	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
119.147.172.162	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
122.228.207.77	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
119.147.172.162	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
122.228.207.77	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
117.135.163.104	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.66	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

04-19-2015-04:03:08 to 04-19-2015-05:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.86.77.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	98
66.87.77.21	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
82.145.221.174	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
154.5.161.167	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
216.81.4.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
185.5.154.220	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
79.183.5.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
109.253.133.125	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
82.80.25.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
166.182.83.235	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
176.77.105.84	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
66.249.67.96	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
174.254.195.11	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
212.76.127.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
212.76.127.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
207.46.13.1	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.87.96.124	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.67.104	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
157.55.39.173	United States	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
5.29.31.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.67.112	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
76.71.6.69	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
70.192.91.210	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
174.254.195.11	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
37.26.146.200	Israel	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	5
166.216.157.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
174.254.195.11	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
2.52.177.93	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.253.147.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.35	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.76.127.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
77.127.70.65	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	3
216.59.203.172	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.132	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
77.127.70.65	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	3
149.88.100.196	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	6
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	5
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	4
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.147	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
79.176.6.100	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	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	1
198.204.249.34	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
135.23.110.73	Canada	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/	Block	1
69.194.230.99	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp/wp-admin/	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2000/october/15-prop.stm	Block	1
217.70.146.17	Italy	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/images/jdownloads/screenshots/jalang.php.j	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20581-he/dover.aspx	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.28	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
95.173.190.6	Turkey	147.237.76.39	mobile.meitav.idf.il	Illegal HTTP Version	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/french/doctrine/doctrine.stm	Block	1
24.249.104.16	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/old/wp-admin/	Block	1
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/yohalan/forums/asp/showforum.asp	Block	1
207.46.13.10	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
135.23.110.73	Canada	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.73.221	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/statistics/gens.stm	Block	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18775-he/dover.aspx	Block	1
180.76.4.72	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
104.222.192.234		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan	Block	1
66.249.64.16	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8747-he/navy.aspx	Block	1
207.46.13.10	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/klali/default.asp	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.8	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
66.249.78.78	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-9576-he/cogat.aspx	Block	1
66.249.64.84	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
77.127.70.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/xasdfaf.aspx	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/m/	Block	1
188.165.15.27	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/june/mazen.stm	Block	1
109.234.161.36	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/blog/wp-admin/	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Multiple Illegal Parameter Encoding from 66.249.73.211	None	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unknown Parameter siteid in www.aka.idf.il/sites/home/default.asp	None	1
66.249.64.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19484-he/idfgdover.aspx	Block	1
213.251.182.115	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wordpress/wp-admin/	Block	1
157.55.39.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/navmenu/mazi.idf.il	Block	1
66.249.78.87	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.64.94	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on 147.237.77.176//901-9576-he/cogat.aspx	Block	1
79.176.6.100	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 79.176.6.100	Block	1