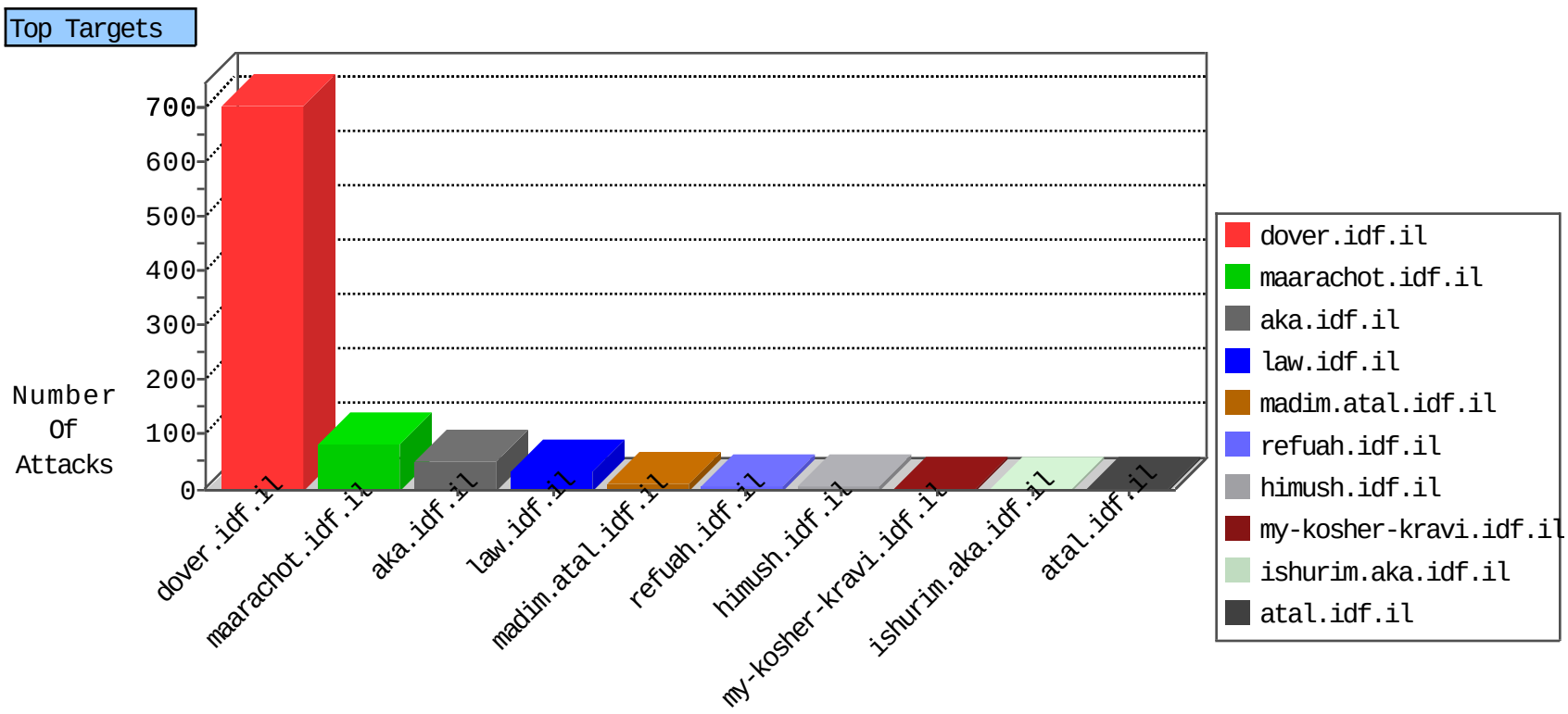
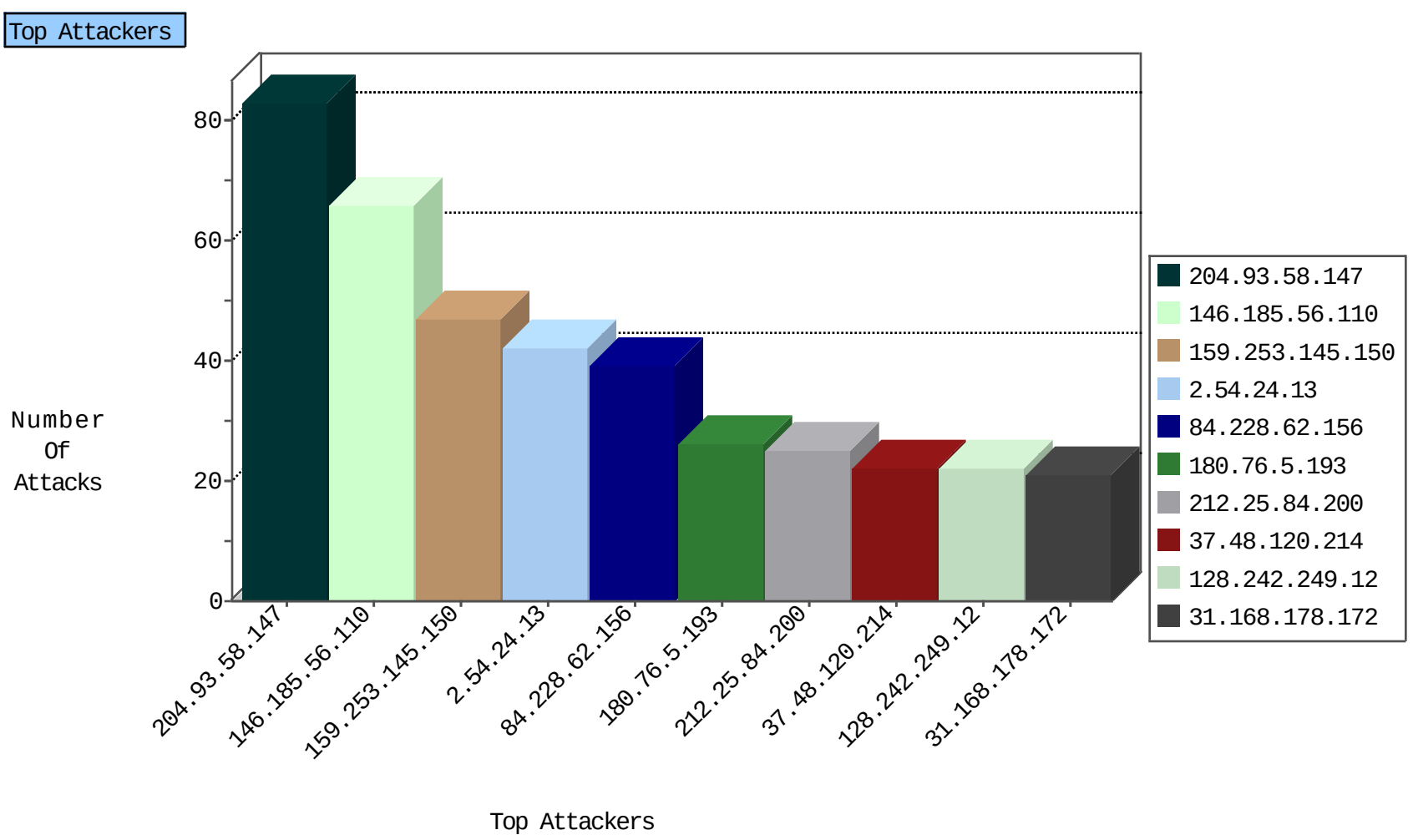
04-27-2015-07:03:06 to 04-27-2015-08:03:06

IDF Under Attack
04-27-2015-07:03:06

Top Targets



Top Attackers



04-27-2015-07:03:06 to 04-27-2015-08:03:06

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	5106
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3537
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	47
84.228.116.252	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
46.116.134.59	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
192.3.190.242	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
46.210.161.189	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
49.241.246.147	Japan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

04-27-2015-07:03:06 to 04-27-2015-08:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
159.253.145.150	United States	147.237.77.216	dover.idf.il	C095: Suspicious Addresses MFA	Permit	41
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	26
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	22
91.135.111.75	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	2
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.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
93.120.27.62	Romania	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.35	akaws.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
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
2.54.1.59	Israel	147.237.76.39	mobile.meitav.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.38	e.e.meitav.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
71.6.135.131	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1

04-27-2015-07:03:06 to 04-27-2015-08:03:06

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	5
61.160.224.128	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
119.226.235.211	India	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
61.160.224.128	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
37.26.147.217	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
70.114.200.189	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.110.196	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.77.79.43	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
134.191.232.70	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.160.224.128	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
59.106.108.116	Japan	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
91.224.132.118	Russian Federation	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.255	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.126.163	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	1
218.77.79.43	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
204.93.58.147	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.160.224.128	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
184.154.52.26	United States	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1

04-27-2015-07:03:06 to 04-27-2015-08:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
204.93.58.147	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	82
146.185.56.110	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	65
2.54.24.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
84.228.62.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
212.25.84.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
31.168.178.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
2.54.180.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
2.52.174.143	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
95.35.27.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.75.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
134.191.232.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
2.54.145.114	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
157.55.39.59	United States	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
159.253.145.150	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
74.4.177.98	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
85.64.170.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.220.146.24	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.120.169.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
176.12.148.118	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
85.17.242.234	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
31.44.133.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
2.54.51.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
2.52.56.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.220.146.20	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.220.146.21	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
134.191.232.71	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
69.171.235.116	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.220.146.22	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
77.126.233.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.1	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
66.249.75.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.149.61.224	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
69.171.228.122	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
84.228.183.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.199.57.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.231	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
84.108.65.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.69.40	Israel	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
176.12.148.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	7
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.228.203.254	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
212.117.136.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/scriptresource.axd	None	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
176.12.148.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.69	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
109.64.171.236	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.himush.atal.idf.il/	Block	1
66.249.79.159	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/m/	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
188.138.17.205	France	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
80.246.136.151	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.117.136.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/kapatz/webresource.axd	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
66.249.64.73	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
109.65.42.2	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 109.65.42.2	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
66.249.75.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-14464-en/dover.aspx,	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.1	Block	1
175.139.181.106	Malaysia	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx	Block	1
81.218.48.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
213.151.57.72	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan	Block	1
178.137.85.64	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.32	Block	1
109.65.42.2	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unknown Parameter c... in www.aka.idf.il/miluim/templates/inner.asp	None	1
66.249.75.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0729-2.stm	Block	1
176.12.137.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
61.135.190.69	China	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19//	Block	1
89.234.68.104	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
180.76.4.59	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.69.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1588-he/refuah.aspx	Block	1
146.185.56.110	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
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	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/sachar/faq/outerfaq.asp	None	1
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34//	Block	1
89.234.68.105	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/smalim.aspx	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1129-he/dover.aspx	Block	1
184.105.247.196	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/displayonesoldier.asp-docid=28709	Block	1
80.246.133.55	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1