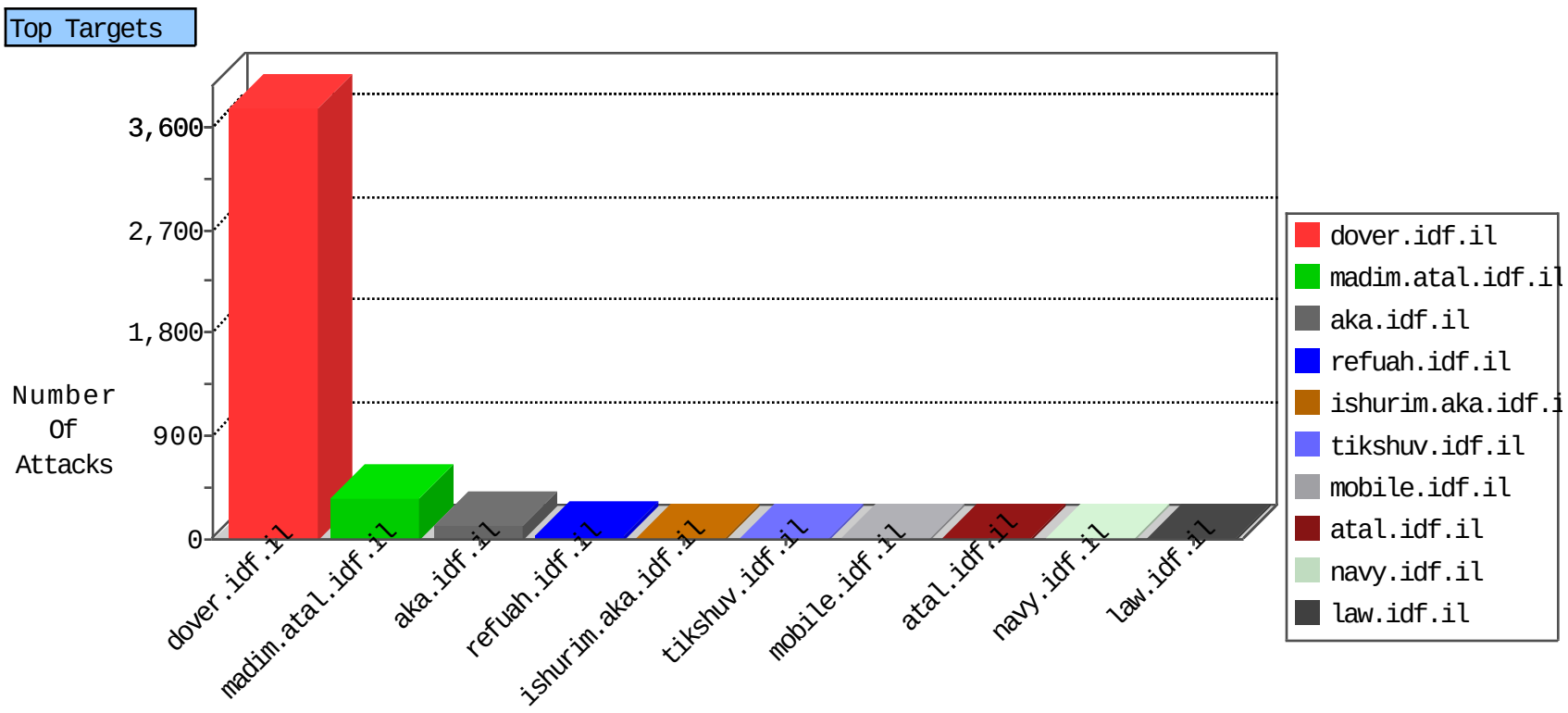
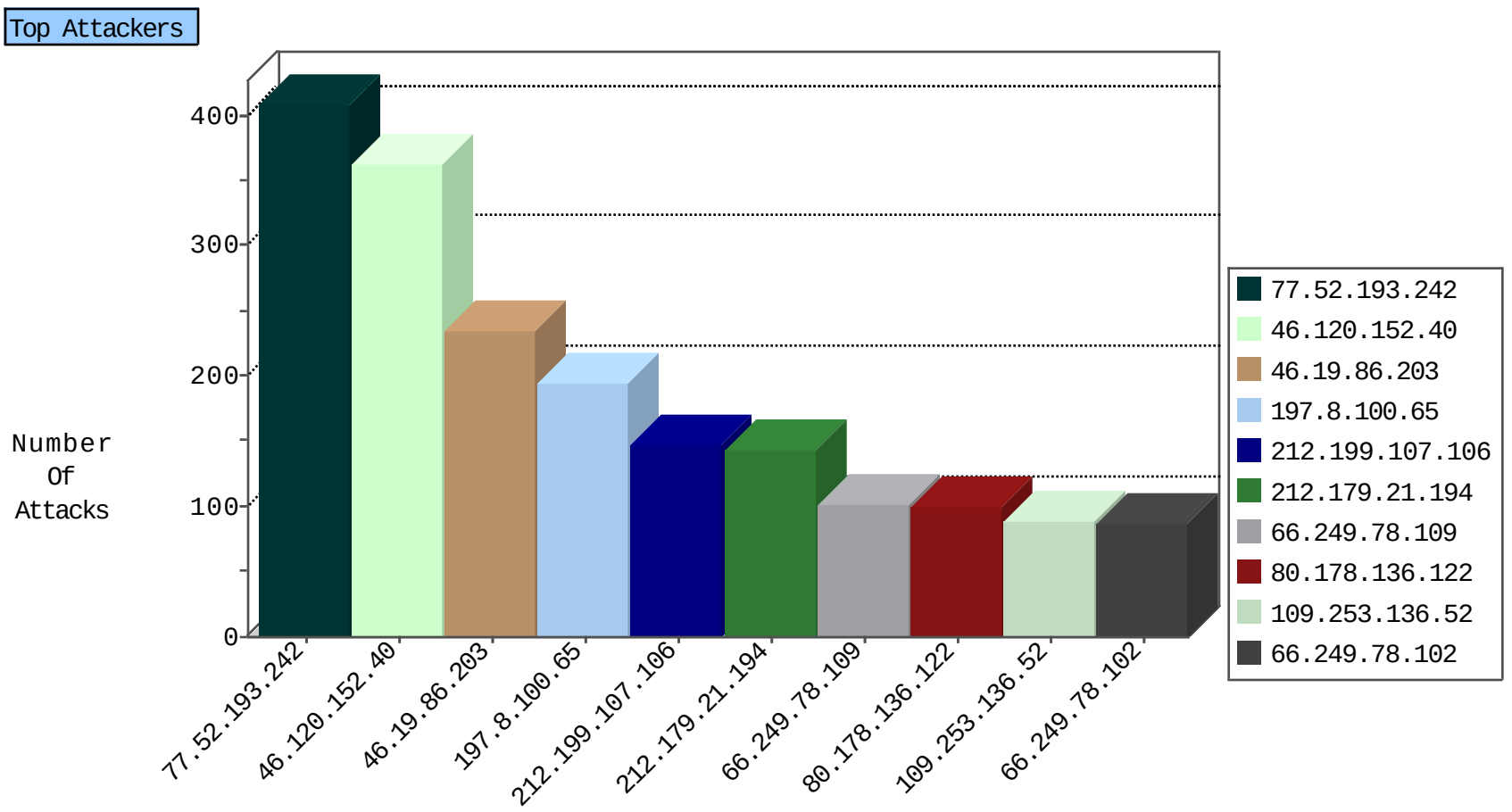
04-27-2015-20:03:07 to 04-27-2015-21:03:07

IDF Under Attack
04-27-2015-20:03:07

Top Targets



Top Attackers



04-27-2015-20:03:07 to 04-27-2015-21:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
109.186.168.137	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	69
37.26.147.151	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	60
212.76.121.52	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
101.8.152.240	Taiwan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	4
46.116.247.71	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
37.26.146.232	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
222.186.50.213	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
80.246.139.124	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
31.210.186.152	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.116.118.148	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
198.12.64.170	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
66.249.64.66	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
109.66.110.124	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
37.26.148.244	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-27-2015-20:03:07 to 04-27-2015-21:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	25
85.25.43.94	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	2
77.125.151.119	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
77.127.137.243	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
2.54.149.56	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	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	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
84.108.238.90	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.86	navy.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
37.142.127.27	Israel	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.72.167	ishurim.aka.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
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
218.30.103.52	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
54.191.131.53	United States	147.237.77.205	prisha.idf.il	19690: HTTP: Microsoft IIS Integer Overflow Vulnerability	Block	1
85.250.197.80	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
94.159.186.3	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	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
198.20.69.98	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1

04-27-2015-20:03:07 to 04-27-2015-21:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
178.216.51.2	Sweden	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
213.165.69.91	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
94.73.165.106	Turkey	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
205.234.138.122	United States	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
79.177.188.123	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.64.64	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
195.211.167.193	United Kingdom	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
46.120.200.30	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.183.59.203	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
84.228.196.163	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
62.210.7.167	France	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
178.62.90.133	Netherlands	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
178.62.55.97	Netherlands	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
109.253.141.167	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
79.27.233.145	Italy	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
65.98.59.26	United States	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
178.62.106.22	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
178.62.90.133	Netherlands	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
1.93.23.196	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
178.62.55.97	Netherlands	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
95.86.102.188	Israel	147.237.77.233	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1

04-27-2015-20:03:07 to 04-27-2015-21:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
77.52.193.242	Ukraine	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	409
46.19.86.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	234
197.8.100.65	Tunisia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	195
212.199.107.106	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	147
212.179.21.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	131
80.178.136.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	100
109.253.136.52	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	88
79.183.59.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	72
5.29.227.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
176.12.141.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	60
80.179.13.138	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
66.249.78.109	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	46
46.19.86.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
66.249.78.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
66.249.78.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
204.115.190.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
66.249.78.95	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	35
94.159.156.79	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
2.54.173.220	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
66.249.78.102	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
66.249.81.212	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
79.177.159.156	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
66.87.152.97	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
66.249.78.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
89.139.44.51	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
98.14.138.114	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
77.126.8.63	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
212.143.254.66	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
84.229.160.36	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
69.193.141.150	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
80.246.133.214	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
204.13.204.162	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
176.12.137.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
207.46.13.95	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
66.249.81.218	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
37.26.147.151	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
176.12.151.211	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
109.64.19.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
46.121.118.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
37.26.148.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
109.253.141.167	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
93.173.174.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.120.152.40	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.120.152.40	Block	362
2.54.10.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
98.14.138.114	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
89.139.44.51	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
212.150.174.130	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
213.165.69.91	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.165.69.91	Block	3
81.218.199.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	3
79.180.162.248	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
87.69.241.92	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/master/	Block	2
178.216.51.2	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//&amp	Block	2
205.234.138.122	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//&amp	Block	2
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
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-17057-en/dover.aspx	Block	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/home.asp/info.asp	Block	1
80.246.133.109	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
24.15.69.250	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.216.51.2	Sweden	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.177.27.31	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
69.171.228.120	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage	Block	1
66.249.64.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	1
213.165.69.91	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&amp	Block	1
84.111.211.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
79.181.39.191	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
202.46.49.195	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1224-2.stm	Block	1
76.10.176.221	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
149.88.13.234	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
46.116.192.69	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
81.52.142.148	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/main.stm	Block	1
79.177.206.247	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/null	Block	1
69.171.228.123	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files	Block	1
98.14.138.114	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
66.249.64.78	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
85.64.62.3	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.161.174	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.28.184.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.73	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
77.237.138.202	Czech Republic	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	Block	1
89.145.95.2	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.120.142.253	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
81.218.101.3	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
178.216.51.2	Sweden	147.237.77.216	dover.idf.il	Multiple signatures from 178.216.51.2	Block	1
79.178.170.110	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.170.110	Block	1
69.171.235.117	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/894-he	Block	1
109.66.115.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
85.65.111.199	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.42	Block	1
80.178.212.24	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1