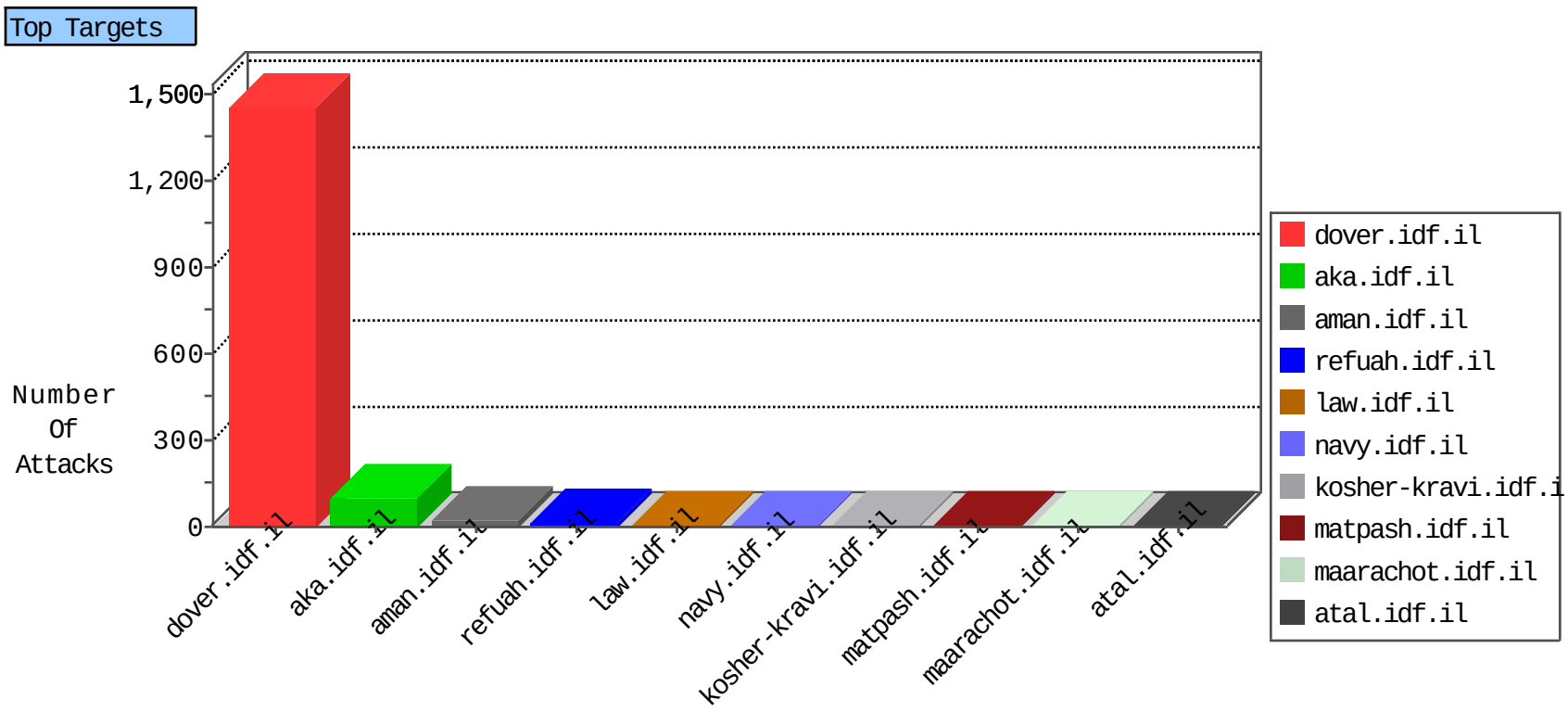
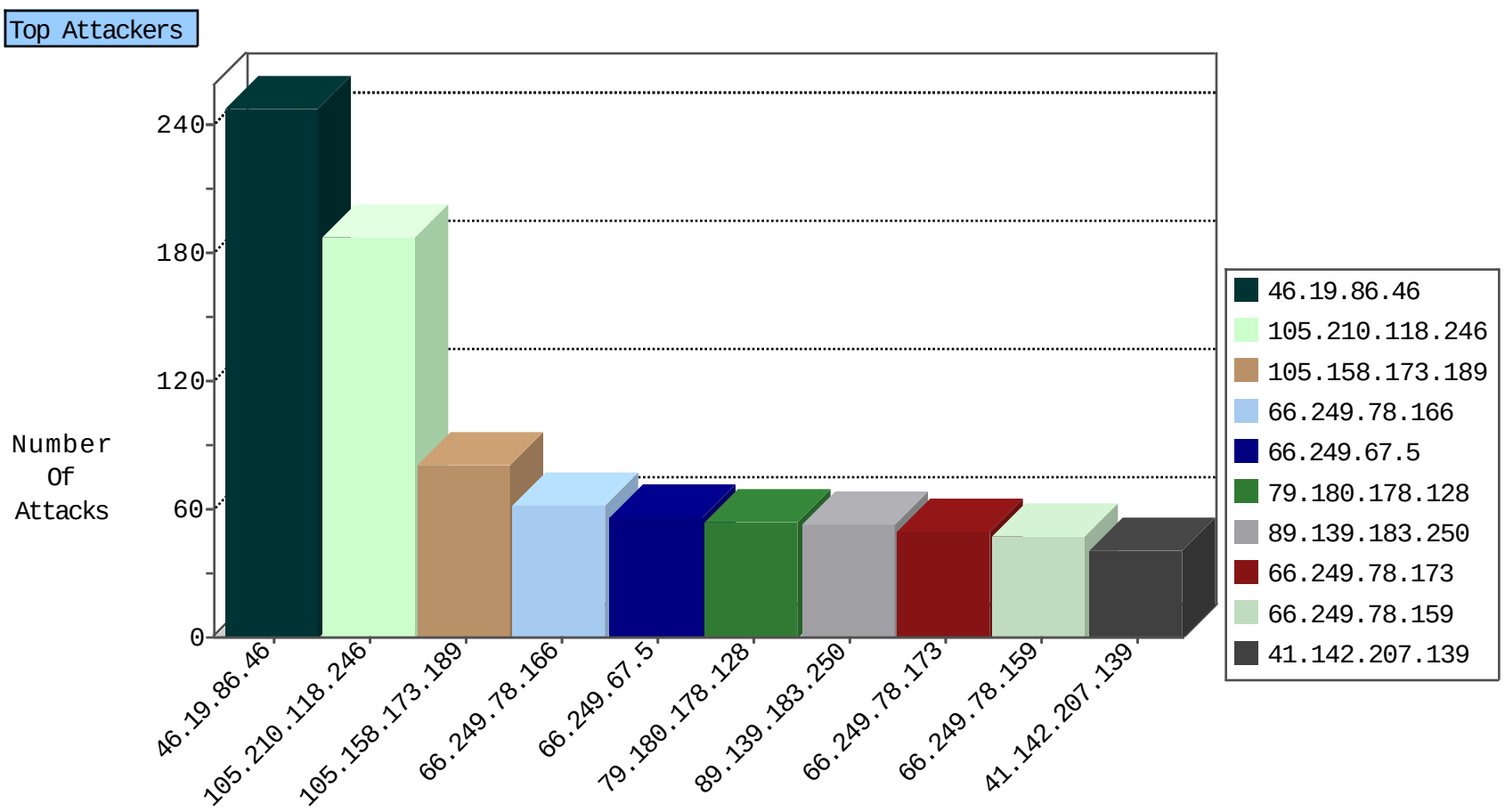
04-17-2015-01:03:02 to 04-17-2015-02:03:02

IDF Under Attack
04-17-2015-01:03:02





04-17-2015-01:03:02 to 04-17-2015-02:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2720
220.181.108.87	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	413
84.110.60.31	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	156
202.83.110.123	Singapore	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
118.244.154.47	China	147.237.77.233	atal.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
2.54.49.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
124.232.142.220	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

04-17-2015-01:03:02 to 04-17-2015-02:03:02

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	4
89.139.183.250	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.216.115.6		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	2
64.235.53.43	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	2
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.15	kosher-kravi.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
71.6.167.142	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.156	aman.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
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
167.57.11.130		147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
85.25.43.94	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.166	aka.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
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.28	e.mobile-ks.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
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
197.200.13.59	Algeria	147.237.0.15	kosher-kravi.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.170	maarachot.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	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
105.158.173.189	Morocco	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	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	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1

04-17-2015-01:03:02 to 04-17-2015-02:03:02

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	8
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.161	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.137	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.159	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
78.129.180.9	United Kingdom	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.168	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	Cote D'Ivoire	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.16.206	Russian Federation	147.237.76.38	e.e.meitav.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
58.20.54.249	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
168.235.154.235		147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
105.158.173.189	Morocco	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
43.255.191.168	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
78.129.180.9	United Kingdom	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.168	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
168.235.154.235		147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
58.20.54.249	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
105.158.173.189	Morocco	147.237.77.216	dover.idf.il	SQL Injection - Select From	1
43.255.191.168	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
94.31.43.151	United Kingdom	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1

04-17-2015-01:03:02 to 04-17-2015-02:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.86.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	248
105.210.118.246	South Africa	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	188
105.158.173.189	Morocco	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
66.249.67.5	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
79.180.178.128	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	54
89.139.183.250	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	50
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
41.142.207.139	Morocco	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
37.142.48.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
71.106.162.189	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
24.252.217.27	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
72.69.250.183	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
46.121.239.192	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
71.194.246.30	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
176.12.143.239	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
105.42.133.105		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
68.180.228.117	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
46.116.42.144	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
207.46.13.77	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
93.218.97.45	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
128.252.16.235	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
96.35.142.5	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
212.76.105.157	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
66.249.64.76	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
109.65.152.194	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	7
85.65.74.210	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
79.178.22.127	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
197.135.127.251	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
50.158.251.99	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
192.115.103.88	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
46.19.86.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
212.76.127.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
64.22.71.223	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
94.228.34.250	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
108.6.126.97	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
46.19.85.134	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
85.65.172.246	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
79.178.176.19	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
105.158.173.189	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 105.158.173.189	Block	12
5.102.199.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
105.158.173.189	Morocco	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
91.214.98.33	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
176.12.140.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
66.249.67.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
104.61.228.201		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
109.67.50.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
207.46.13.31	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sviva	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jenin.stm" target="_blank	Block	1
66.249.67.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/main/stm	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mpm/neot_yuvalim.asp	Block	1
197.200.13.59	Algeria	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/80	Block	1
66.249.78.134	Israel	147.237.76.30	himush.idf.il	Unknown Parameter SortDir in www.chimush.atal.idf.il/1324-he/himush.aspx	None	1
157.55.39.4	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/dov.stm	Block	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2001/october/20.stm	Block	1
66.249.67.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
181.88.177.153	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/grapheat.stm	Block	1
105.158.173.189	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-ar	Block	1
61.135.190.72	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
77.105.55.121		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
198.20.69.74	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
207.46.13.104	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
188.165.15.78	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/320/patzar.aspx	Block	1
109.65.155.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
61.135.190.201	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
77.237.138.51	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0429-2.stm	Block	1
66.249.67.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	1
157.55.39.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
104.128.144.130		147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.50	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
207.46.13.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.133	Block	1
188.165.15.78	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.78	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
64.22.71.223	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper	Block	1
79.180.21.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/120403-2.stm	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1399-he/atal.aspx	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/common/includes/bignewswnd.asp	Block	1
37.16.72.139	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1

04-17-2015-01:03:02 to 04-17-2015-02:03:02