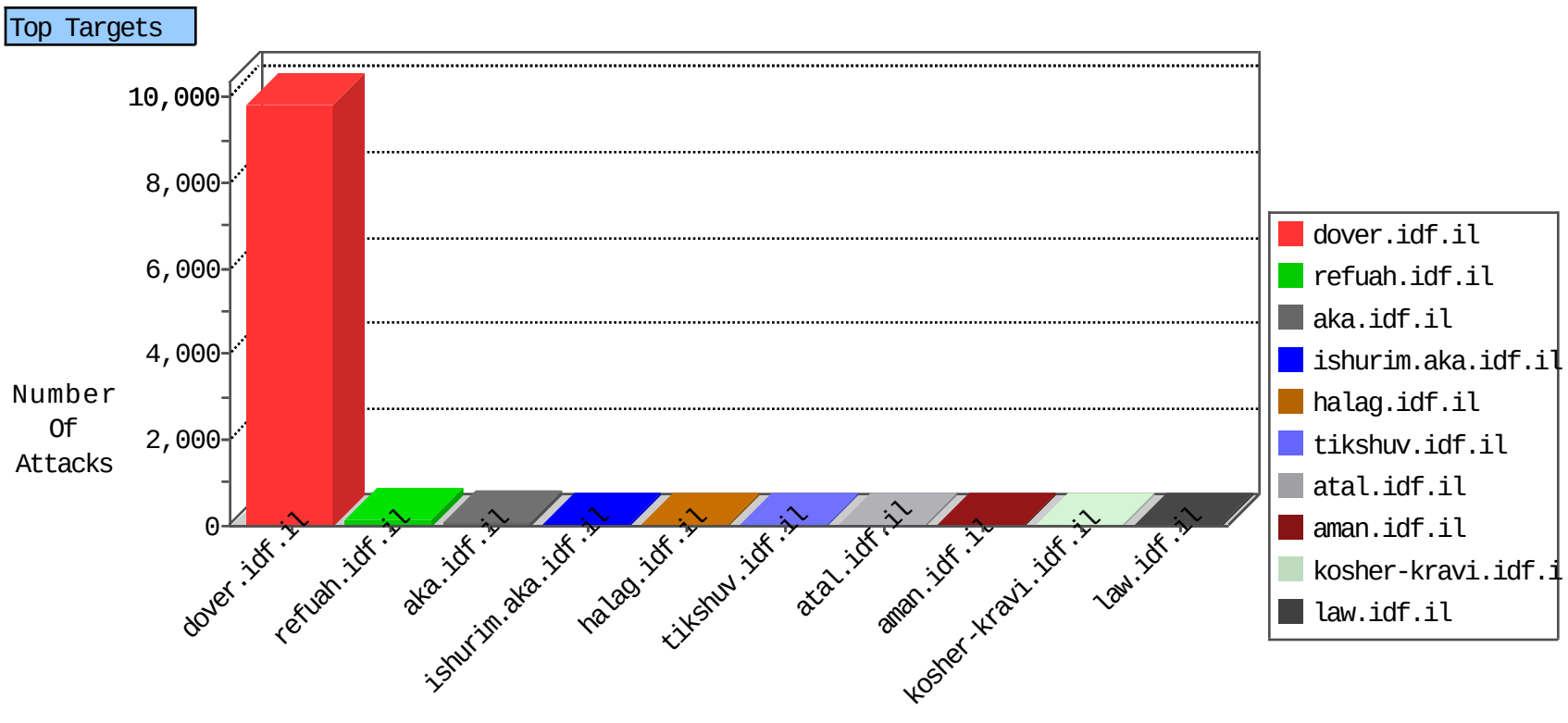
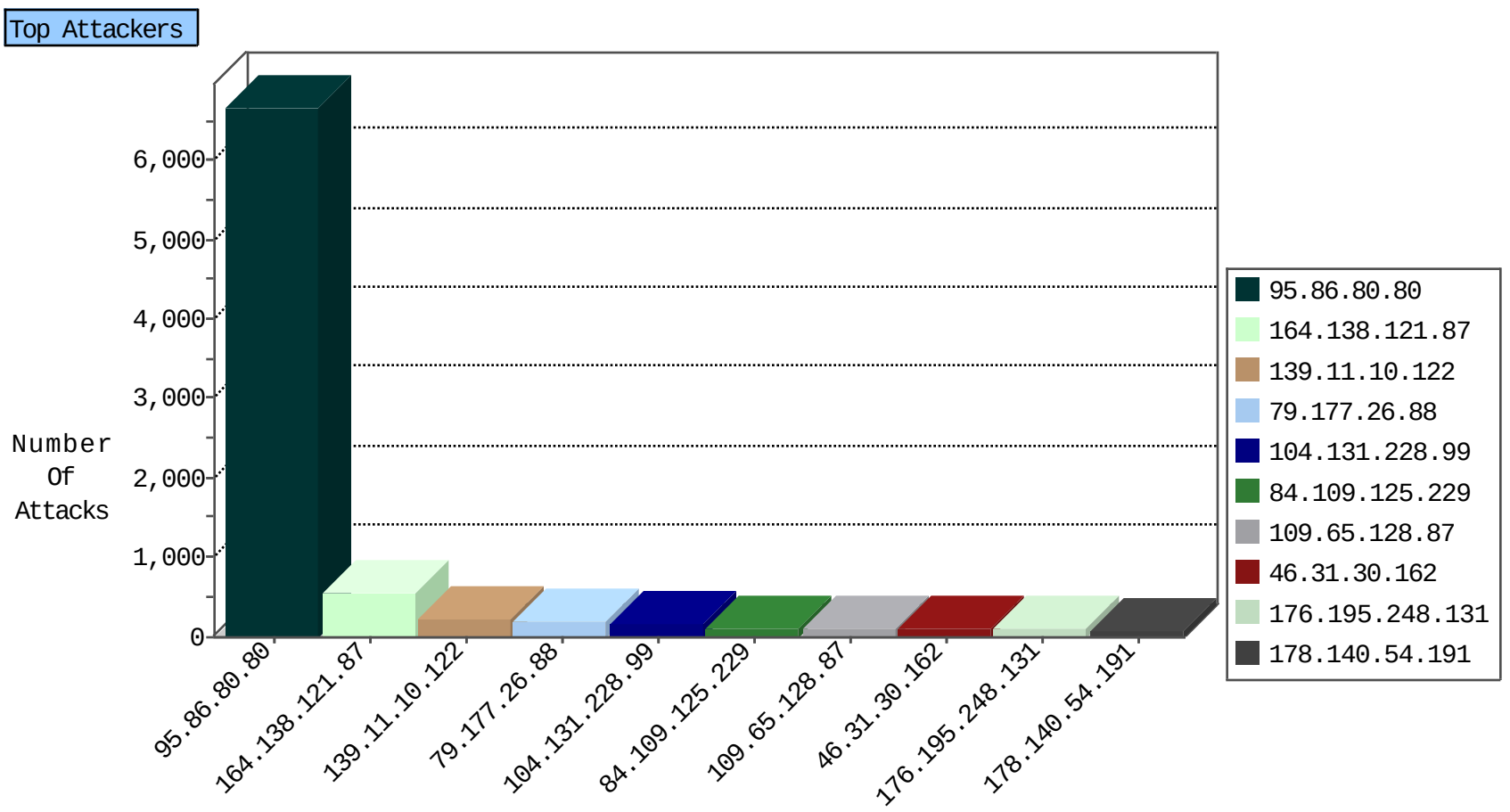
05-08-2015-15:03:01 to 05-08-2015-16:03:01

IDF Under Attack
05-08-2015-15:03:01

Top Targets



Top Attackers



05-08-2015-15:03:01 to 05-08-2015-16:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
85.65.122.165	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	78
46.19.86.238	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
146.185.239.100	Russian Federation	147.237.77.74	law.idf.il	block-sp-traf1	drop	1

05-08-2015-15:03:01 to 05-08-2015-16:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
197.162.14.7	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
79.182.152.14	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
84.228.130.106	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
149.88.6.113	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.178	e.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
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.19	madim.atal.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
66.240.192.138	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
106.38.241.102	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.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
188.138.9.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.216	dover.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
66.240.192.138	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
2.54.159.198	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.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
198.20.70.114	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
82.102.169.113	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

05-08-2015-15:03:01 to 05-08-2015-16:03:01

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	6
80.246.133.241	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.31	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sA (2)	2
144.0.0.60	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
36.248.9.135	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
144.0.0.60	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
109.67.116.42	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
195.178.167.163	Sweden	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
80.82.78.27	Netherlands	147.237.76.86	navy.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
188.138.9.51	Germany	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
157.7.237.231	Japan	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
60.18.162.244	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
157.7.237.231	Japan	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -f -sS	1
52.64.100.124	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 2048	1
144.0.0.60	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
36.248.9.135	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
144.0.0.60	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
36.248.9.135	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
144.0.0.60	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
93.158.215.110	Netherlands	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.27	Netherlands	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
67.159.16.2	United States	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
157.7.237.231	Japan	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
52.64.100.124	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 3072	1
144.0.0.60	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
52.64.100.124	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -f -sS	1

05-08-2015-15:03:01 to 05-08-2015-16:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
95.86.80.80	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6675
164.138.121.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	540
139.11.10.122	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	224
79.177.26.88	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	199
104.131.228.99		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	156
84.109.125.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	104
46.31.30.162	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	92
176.195.248.131	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	91
178.140.54.191	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	87
77.127.247.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
176.77.66.238	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	56
164.138.116.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
79.181.150.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
77.125.214.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
109.65.128.87	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	48
109.65.128.87	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	48
89.139.171.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
79.176.155.253	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
89.178.16.76	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
79.183.25.248	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	33
79.179.166.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
85.65.221.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
144.160.226.91	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	24
31.223.179.78	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
24.77.223.33	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
149.101.1.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
94.159.162.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
2.52.48.39	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
172.11.11.182	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
93.173.176.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
87.68.26.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
85.65.225.187	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
2.52.164.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
79.181.1.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
94.230.86.128	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
109.67.194.153	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	14
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
195.34.150.18	Austria	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	12
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
197.162.14.7	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12

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	5
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
157.55.39.255	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 157.55.39.255	Block	4
2.52.20.38	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	4
176.228.136.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
95.86.86.254	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
85.64.144.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.116.189.232	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
66.249.64.251	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.64.251	Block	2
79.182.152.14	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.117.25.95	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding www.aka.idf.il/main/giyus/userdetails/function () { var c = math.round(this[2] / 100 * 255); if (this[1] == 0) { return [c, c, c]; } else { var a = this[0] r 360; var e = a e g = math.round((this[2] * (100 - this[1])) / 10000 * 255); var d = math.round((this[2] * (6000 - this[1] * e)) / 600000 * 255); var b = math.round((this[2] * (6000 - this[1] * (60 - e))) / 600000 * 255); switch (math.floor(a / 60)) { case 0: return	Block	1
188.138.17.205	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//	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
66.249.69.55	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il//eitan/listpage/	Block	1
46.242.3.101	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/b+2xprpblphdlz/adfdoelu1iylpt8a9aoc7+wg1or8qckdnejg6lgqd+llmoylxge64nohy5xloirbcyqtwmp8isoctu/z0xpizzeimgkfxjljtni4/qd1mv/sk5h9tjp46ncg5o4ajpxyybinzfbcgi697x1dyef3xhnte73tffrwk	Block	1
46.19.85.42	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
216.70.113.32	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
109.65.171.52	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.67.23	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
46.121.108.84	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
197.162.14.7	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/869-2339-he/patzar.aspx	Block	1
66.249.69.63	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il//eitan/listpage/	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2001/august/14.stm	Block	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/june/tarek.stm	Block	1
95.86.111.128	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.163.200.109	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
178.137.19.143	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
142.54.185.250	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.67.36	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
46.121.108.237	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
85.250.8.21	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
207.46.13.44	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 207.46.13.44	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-6468-he/patzar.aspx	Block	1
66.249.69.82	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.173.184.200	Turkey	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/schem/english/main	Block	1
79.176.17.151	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/bamahane	Block	1
46.116.212.35	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
188.138.1.218	Germany	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid\u003d59336 in www.aka.idf.il/main/giyus/general.aspx	None	1
150.70.97.99	Japan	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
46.121.247.55	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
85.250.200.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.44	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/sitemap/sitemap.aspx	Block	1