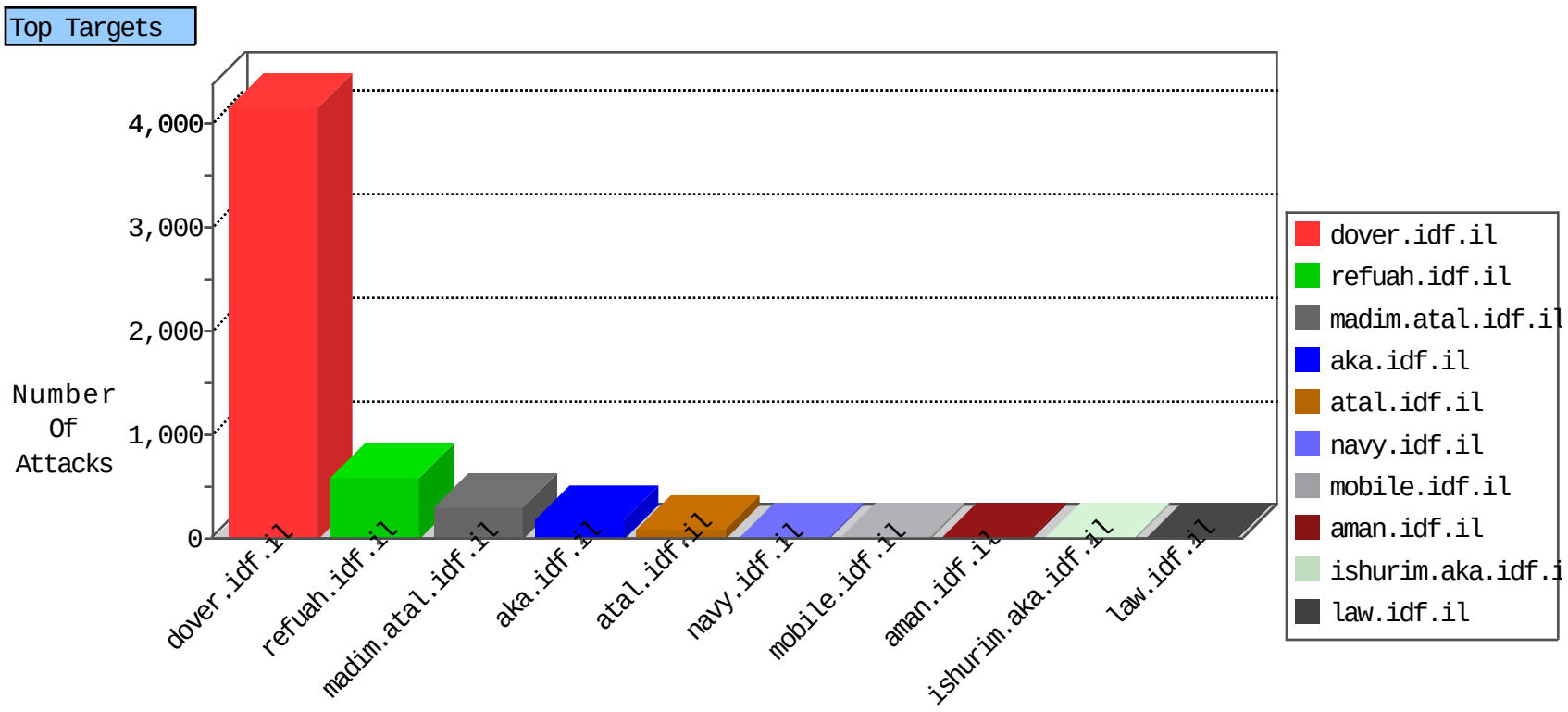
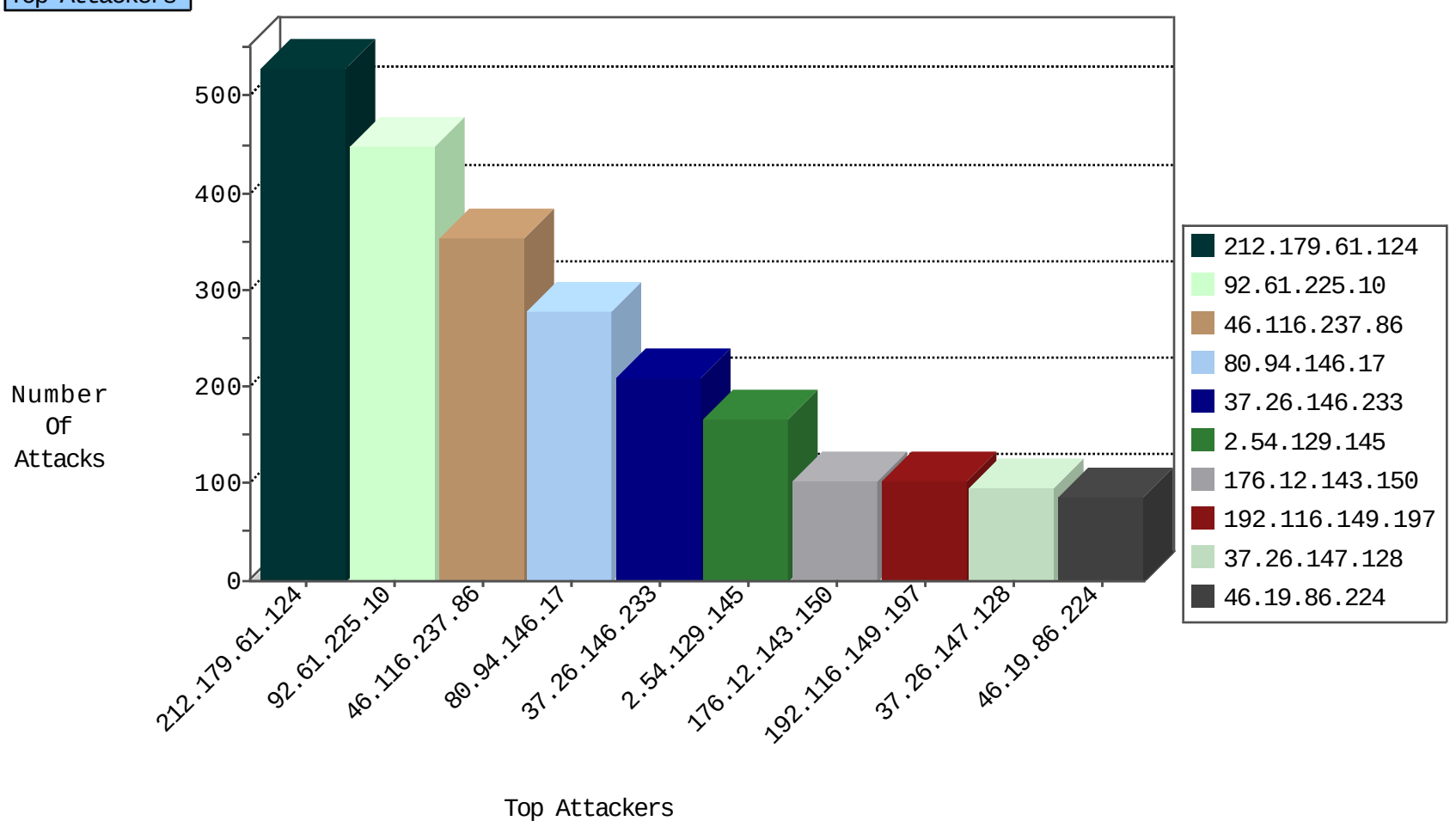
04-16-2015-09:03:07 to 04-16-2015-10:03:07

IDF Under Attack
04-16-2015-09:03:07

Top Targets



Top Attackers



04-16-2015-09:03:07 to 04-16-2015-10:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	115
213.57.46.23	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	88
119.73.253.6	Singapore	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	85
84.228.176.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
109.64.114.118	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
212.117.143.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
80.179.223.31	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.60.43	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
37.142.59.15	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
121.164.88.2	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
31.168.74.43	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
107.154.64.10	United States	147.237.76.39	mobile.meitav.idf.il	L4 Source or Dest Port Zero	drop	1
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-16-2015-09:03:07 to 04-16-2015-10:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.224	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
80.178.2.74	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	5
184.65.73.103	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
71.6.167.142	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
2.54.4.85	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
80.178.2.74	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
122.107.249.146	Australia	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.39	mobile.meitav.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
198.20.69.98	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.92	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	147.237.76.44	e.refuah.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
66.240.236.119	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.44	e.refuah.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
198.20.69.98	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.199	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.200	m4u.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
66.240.236.119	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.24	e.lifestyle.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
66.240.192.138	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1

04-16-2015-09:03:07 to 04-16-2015-10:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.79.132	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	70
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.249.79.5	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.198	United States	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.66	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
58.160.59.37	Australia	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.235.188.210	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
37.8.122.122	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.207	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
111.13.30.109	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
109.66.163.150	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	1
221.235.188.210	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.210	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.43.181	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
128.199.63.237	Singapore	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
111.13.30.109	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -f -sS	1
85.250.109.173	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

04-16-2015-09:03:07 to 04-16-2015-10:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
92.61.225.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	448
212.179.61.124	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	416
46.116.237.86	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	353
80.94.146.17	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	279
37.26.146.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	208
212.179.61.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	113
192.116.149.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	102
37.26.147.128	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	95
46.19.86.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	86
79.179.53.15	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	78
80.178.162.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
176.106.46.74	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	63
178.135.118.117	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	58
24.248.190.4	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
176.12.143.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	48
87.69.217.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	39
213.57.80.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
2.54.4.85	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
176.12.146.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
46.19.86.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
109.253.149.39	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
186.223.172.58	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
207.46.13.77	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
185.5.152.208	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
62.219.65.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
212.179.61.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
80.178.2.74	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	21
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
46.19.86.229	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
178.135.118.114	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
212.143.91.81	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
176.12.140.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
85.64.223.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
176.12.148.204	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
31.168.155.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
71.177.191.245	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
81.218.102.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
84.228.33.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
207.46.13.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
2.54.129.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	167
176.12.143.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	94
31.168.214.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/&	Block	81
176.12.150.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
109.253.143.188	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
37.60.47.203	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	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
149.78.241.72	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
2.54.4.85	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.253.142.137	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$LoginControl$captcha$captchaText in www.aka.idf.il/main/giyus/default.aspx	None	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
80.178.2.74	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
37.26.147.234	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
195.154.183.187	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
66.249.79.128	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8718-he/refuah.aspx	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19666-he/idfgdover.aspx	Block	1
157.55.39.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12535-he/dover.aspx×ž×ª×'×™×™×¡×™×?	Block	1
62.0.60.82	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl22.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
89.139.3.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
216.218.206.67	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.79.58	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8529-he/navy.aspx	Block	1
176.12.150.209	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
80.246.133.168	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
202.228.150.2	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
66.249.79.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9750-he/refuah.aspx	Block	1
66.249.64.14	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
95.173.189.7	Turkey	147.237.77.74	law.idf.il	Illegal HTTP Version	Block	1
5.28.134.234	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https:/www.idf.il/	Block	1
217.69.133.221	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
66.249.79.66	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8226-he/navy.aspx	Block	1
109.253.149.17	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.73.221	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
46.19.85.97	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.118.24.206	Sweden	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
207.46.13.78	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.143	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
66.249.79.5	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.65.14	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	1
95.173.190.6	Turkey	147.237.76.86	navy.idf.il	Illegal HTTP Version	Block	1
79.177.121.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.102.254.61	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
180.76.4.140	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.79.74	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8271-he/navy.aspx	Block	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
66.249.78.27	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
46.19.85.217	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1