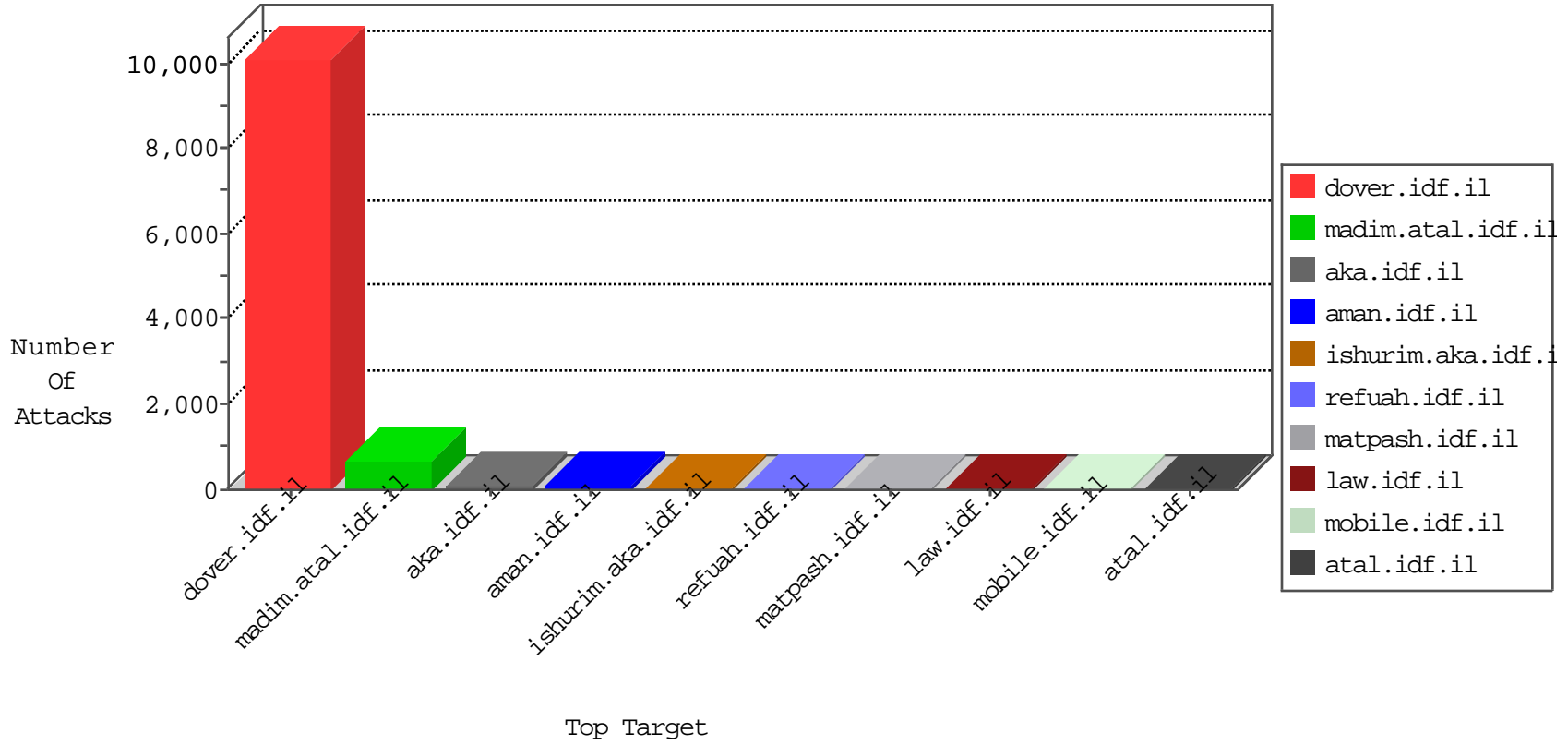
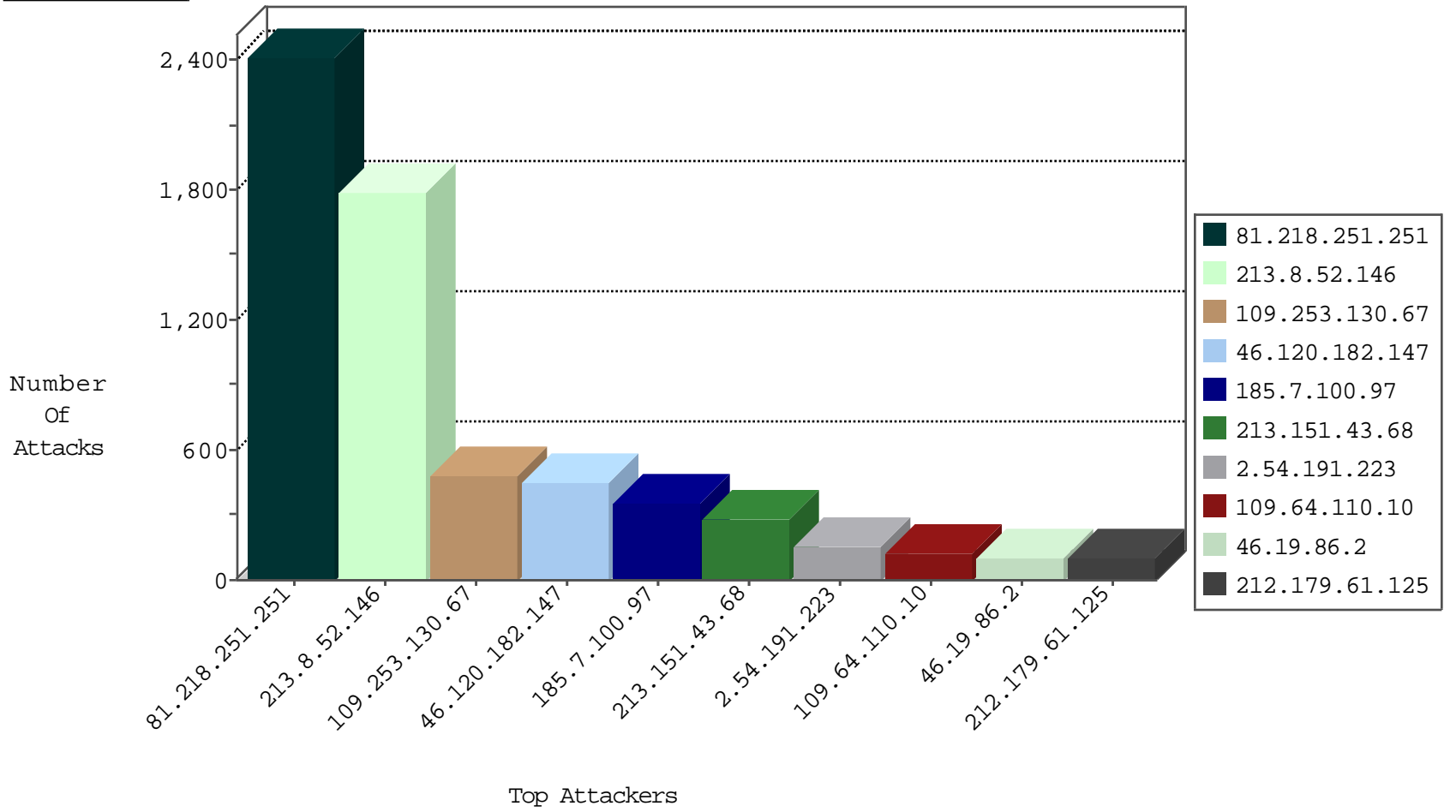




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
192.249.64.249	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5781
212.179.61.125	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2707
79.181.48.85	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	413
84.228.214.236	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	174
79.183.31.165	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	134
194.90.183.90	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
10.0.16.10		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
210.251.217.130	Japan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	4
46.19.85.43	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
194.90.220.241	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.85.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.118.253.114	United Kingdom	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.29.202.206	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
62.0.27.129	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
79.179.24.168	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
212.143.110.33	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
213.57.193.2	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
84.108.164.189	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
188.138.9.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
46.120.37.221	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.27	e.madim.atal.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
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
192.114.23.211	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.151	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.65.30	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
203.223.34.45	Cambodia	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
203.223.34.45	Cambodia	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
203.223.34.45	Cambodia	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
109.253.137.220	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
99.244.135.30	Canada	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
222.69.94.13	China	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
85.65.16.58	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.96.31	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.84.200	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.147.254	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
203.223.34.45	Cambodia	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
203.223.34.45	Cambodia	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
203.223.34.45	Cambodia	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
37.142.116.180	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.101.106	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.174.46	Netherlands	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
213.57.145.172	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.198.181	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.30.250	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.9.7	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
203.223.34.45	Cambodia	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
78.108.161.226	Lebanon	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
81.218.251.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2415
213.8.52.146	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1763
46.120.182.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	444
185.7.100.97	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	359
213.151.43.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	270
2.54.191.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	154
109.64.110.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	122
46.19.86.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	99
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	95
138.134.102.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	80
2.52.32.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
46.19.85.211	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	62
213.8.122.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	61
62.219.183.178	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
62.90.202.222	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	58
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	57
46.19.85.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
174.125.97.213	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
78.108.169.33	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	54
37.26.148.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
80.246.133.24	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
62.0.102.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
77.125.152.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	45
85.65.16.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
93.173.248.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
109.253.128.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
77.127.101.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
174.139.217.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
84.109.126.33	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
37.26.146.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
213.151.39.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
176.12.149.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
212.150.255.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
109.253.134.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
109.253.156.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
84.110.82.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
2.54.24.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
212.179.28.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
37.142.118.169	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
176.12.142.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
91.227.71.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
46.19.86.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
195.160.240.11	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
212.199.58.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
109.253.132.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
62.219.239.119	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
80.179.9.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.130.67	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.130.67	Block	484
109.253.157.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
37.26.146.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	57
109.253.138.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	12
46.19.85.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
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	9
217.12.202.39	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	7
178.137.85.64	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	6
109.253.147.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
85.64.150.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	6
77.127.205.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
192.115.116.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	3
77.127.205.242	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.127.205.242	Block	2
37.26.148.246	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.244.124	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/tizmoret/faq/default.asp	None	2
109.253.157.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
66.249.73.219	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchfText in www.law.idf.il/275-he/patzar.aspx	None	1
62.219.228.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
109.253.140.115	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
80.246.138.27	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/foia/foia.stm	Block	1
66.249.81.233	Israel	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/./favicon.ico	Block	1
138.134.102.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
66.249.64.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch/default.asp	Block	1
46.19.86.188	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.himush.atal.idf.il/webresource.axd	Block	1
109.253.130.67	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
2.54.55.249	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
180.76.5.145	China	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
66.249.64.18	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
82.102.141.248	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.147.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
212.179.28.34	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he/patzar.aspx/	Block	1
66.249.93.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
149.88.146.80	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.0.27.129	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1136-he/atal.aspx	Block	1
2.54.148.140	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
217.194.194.48	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	1
66.249.78.94	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
184.105.247.196	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.64.18	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/1144-he/navy.aspx	Block	1
82.145.216.22	Europe	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.57.193.2	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1136-he/atal.aspx	Block	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 70.167.8.42	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.70	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/tmuna/default.asp	Block	1
62.210.114.129	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/8/3198.pdf/trackback/	Block	1