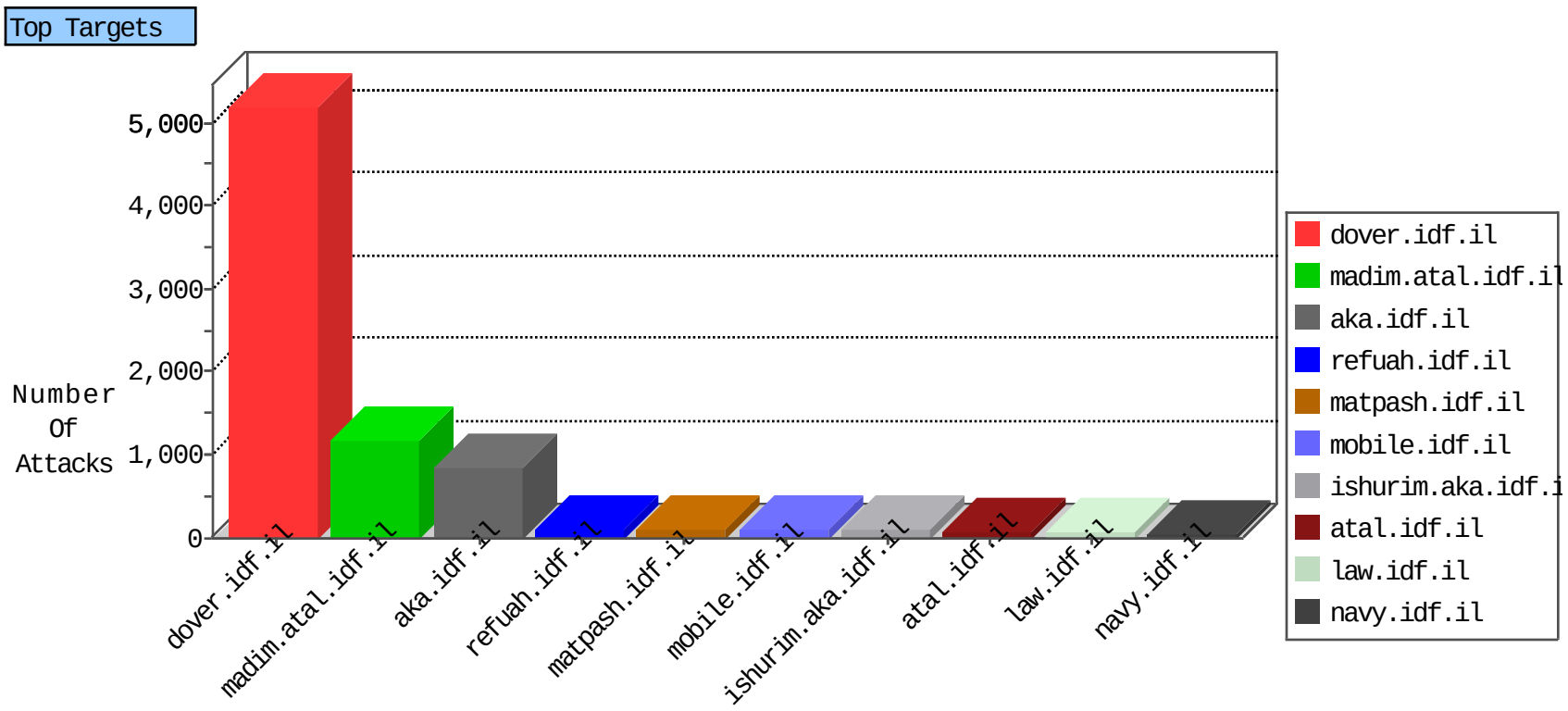
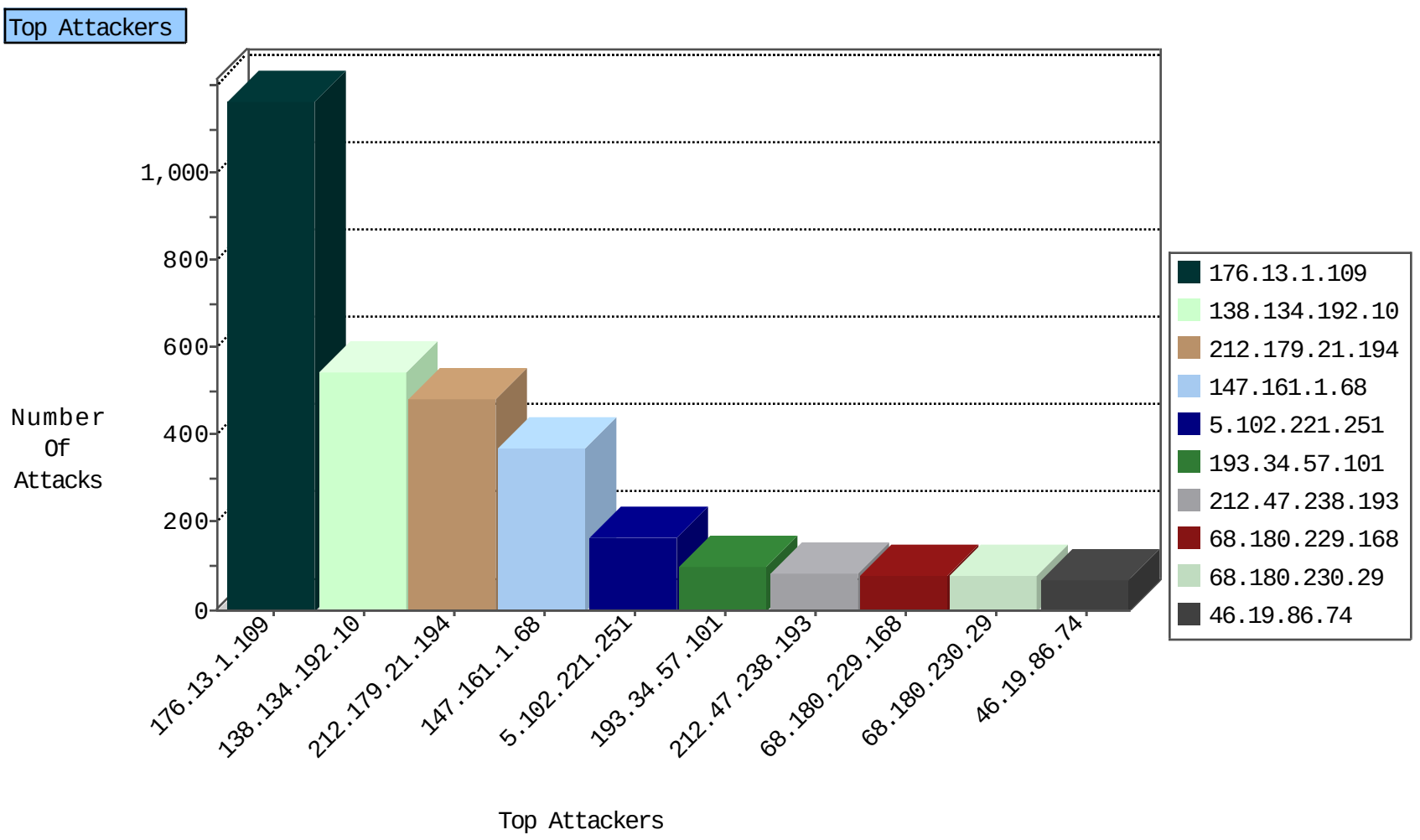
10-19-2015-10:04:09 to 10-19-2015-11:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-19-2015-10:04:09 to 10-19-2015-11:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5790
196.1.240.122	Sudan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	478
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	121
46.19.86.74	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	120
46.19.86.200	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
37.26.148.167	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
91.227.164.5	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	13
109.65.139.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
2.54.5.67	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
82.80.178.132	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.142.222.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.94.130.220	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
37.142.222.152	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
212.150.145.60	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
192.117.150.233	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.33.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.0.40	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
85.112.78.242	Lebanon	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.5.67	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
5.29.57.88	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.179.210.163	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
2.54.156.207	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.85.232	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.19.85.232	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
109.226.21.124	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
94.188.248.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
149.78.232.46	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.232	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
109.226.21.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
5.29.51.180	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.86.221	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.156.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
84.111.81.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.19.86.104	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
31.168.130.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.170.221.60	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

10-19-2015-10:04:09 to 10-19-2015-11:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-19-2015-10:04:09 to 10-19-2015-11:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.64.186.112	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.174.95.81	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
80.246.137.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.57.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.184.195.114	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.107.17.72	147.237.8.27	Seychelles	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.175.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
142.0.41.41	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1
109.73.242.91	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
93.174.95.81	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
93.173.183.88	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.65.151	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.156.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.6.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.227.211.186	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET WEB_SERVER Muieblackcat scanner	1
176.13.17.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
117.135.163.104	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1

10-19-2015-10:04:09 to 10-19-2015-11:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
138.134.192.10	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	544
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	451
147.161.1.68	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	374
5.102.221.251	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	168
193.34.57.101	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
212.47.238.193	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	82
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	69
196.1.240.122	Sudan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	59
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	59
188.49.169.153	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	57
217.6.229.230	Germany	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	54
80.230.21.137	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
213.55.104.254	Ethiopia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	50
84.94.130.220	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
46.19.85.136	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
79.179.51.207	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	48
5.29.119.252	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	46
192.117.176.130	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	45
176.58.71.32	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
37.60.46.177	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
2.54.1.78	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	43
62.90.16.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
54.244.22.103	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
70.199.65.152	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	42
66.249.78.173	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
176.13.5.127	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
46.19.85.115	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
212.235.98.139	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	34
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
203.217.18.248	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	33
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
176.12.144.130	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
46.19.86.200	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
46.19.86.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
176.13.10.26	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
213.204.127.27	Lebanon	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
5.108.140.103	Saudi Arabia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
212.143.120.151	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
62.90.5.212	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
46.19.85.50	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
194.90.66.15	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
46.120.106.141	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
2.52.179.0	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
93.172.184.58	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
2.54.131.4	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
5.29.69.119	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.1.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1166
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	78
68.180.229.168	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/headerupper/	Block	78
78.154.170.6	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	65
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	52
109.226.21.124	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	39
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/67906.pdf	Block	39
192.118.78.57	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	39
2.54.0.73	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	26
192.118.78.201	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
176.13.8.18	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
46.19.86.104	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/jquery.jcarousel.css	Block	13
85.250.147.57	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	13
213.151.35.218	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$chkBitulTlushim in aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	13
80.246.136.78	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
66.249.93.132	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	13
185.32.179.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
46.19.85.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
157.55.39.212	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
82.166.199.237	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	13
31.28.229.39	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.law.idf.il/templates/getfile/getfile.aspx	Block	13
217.194.203.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
212.179.21.194	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	13
176.13.10.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
66.249.64.168	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	13
46.19.85.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layoutdev.css	Block	13
2.52.62.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
213.151.35.218	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrwo/	Block	13
80.246.139.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
66.249.93.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/datepicker.css	Block	13
185.32.179.149	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	13
46.19.85.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
176.12.147.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
84.110.110.196	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyu	Block	13
31.28.229.39	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation InfoCenterItem in www.law.idf.il/templates/getfile/getfile.aspx	Block	13
213.8.41.250	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	13
77.127.206.235	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
176.13.10.87	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	13
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	13
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	13
216.218.206.68	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	13
66.249.93.140	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	13
188.225.185.210	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	13
176.12.149.124	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	13
46.19.86.46	Israel	147.237.77.243	mobile.idf.il	Multiple Untraceable SSL Sessions from 46.19.86.46 (Open Mode)	None	13
84.111.81.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13
31.28.229.39	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1399-en/dover.aspx	Block	13
213.57.168.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	13