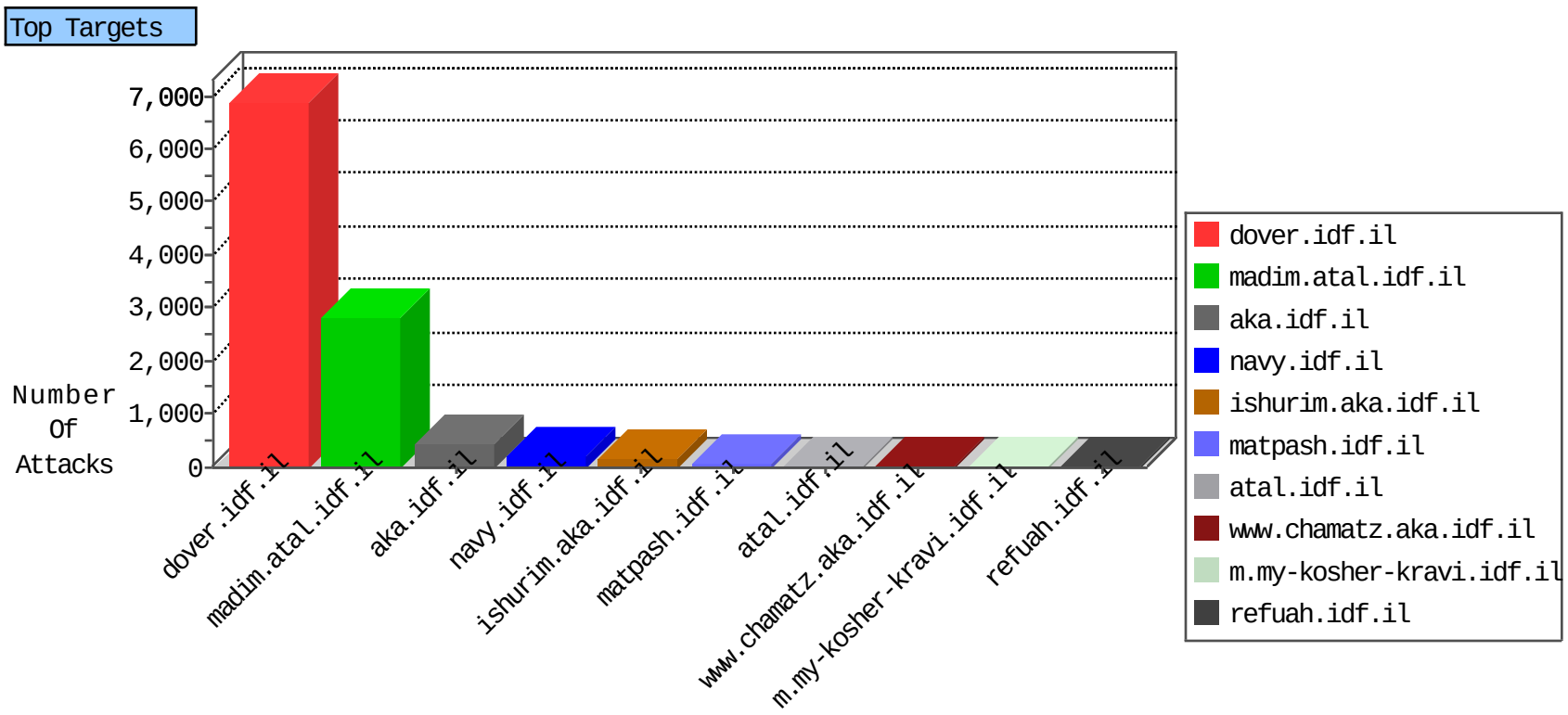
10-25-2015-09:04:05 to 10-25-2015-10:04:05

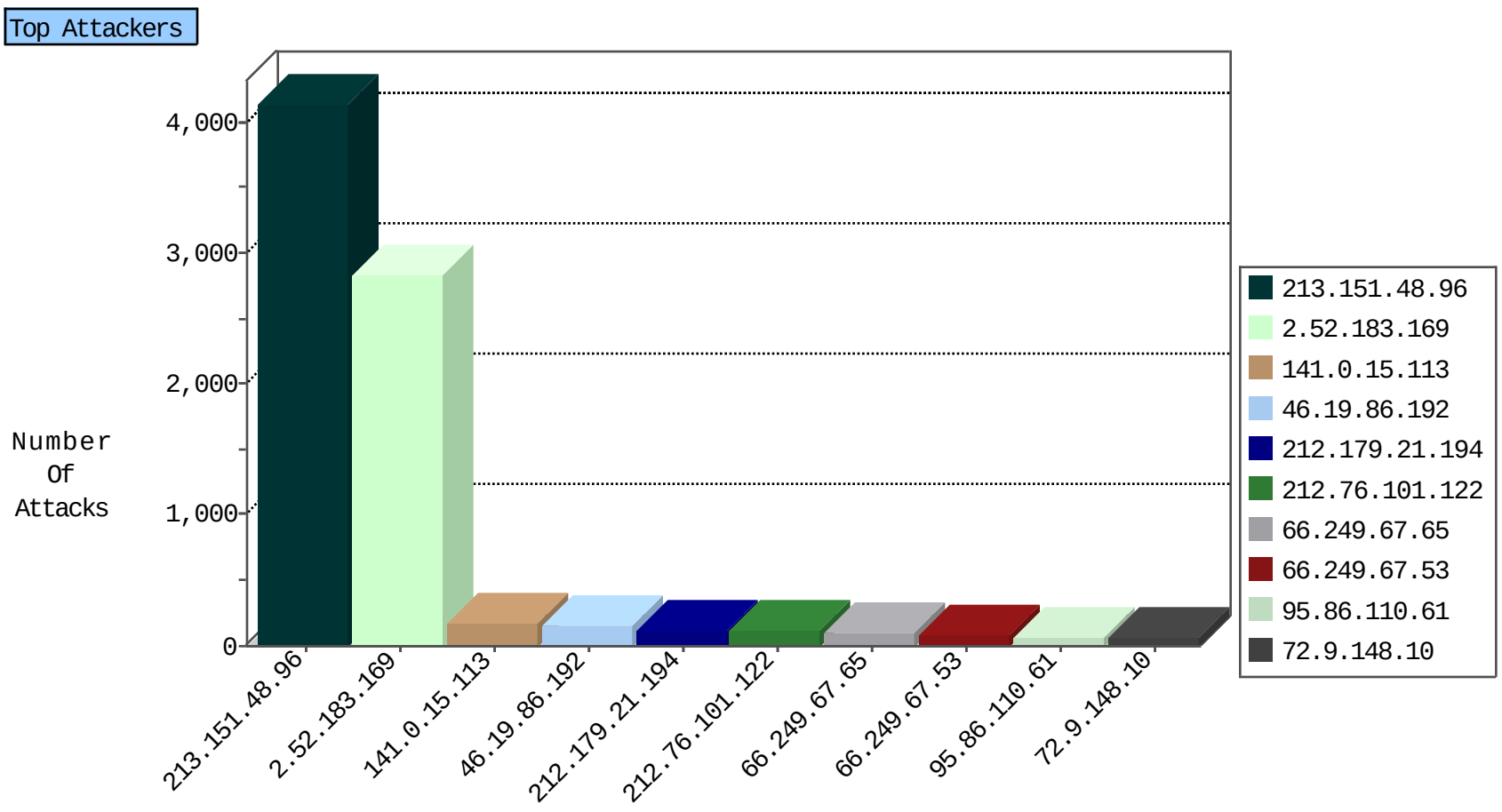
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-25-2015-09:04:05 to 10-25-2015-10:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.2.232	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2652
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	285
84.228.75.222	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	36
81.218.116.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
212.25.106.78	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
2.54.24.206	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	31
185.32.179.99	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
185.32.179.165	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	24
213.57.153.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	22
79.180.5.47	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	21
46.19.86.92	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
176.12.142.176	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	15
212.235.22.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	14
185.32.179.235	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	13
185.32.179.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	11
2.54.153.116	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	9
5.22.131.77	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	8
79.176.64.225	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
46.19.86.132	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
41.230.232.210	Tunisia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
82.166.229.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.32.179.13	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
82.166.229.58	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
93.172.160.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.120.182.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
82.166.22.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.120.182.53	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
82.166.22.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
87.69.213.222	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
81.218.171.104	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.9.123	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.85.195	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
2.52.7.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.69.215.183	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
82.80.144.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
79.177.43.170	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
82.145.217.6	Europe	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
80.246.137.148	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
185.32.179.235	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
176.13.0.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.66.43.44	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
185.32.179.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.137.0	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.226.15.241	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.22.182	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
109.64.20.79	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.26.147.208	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
80.246.137.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
80.246.139.152	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
176.12.138.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
123.73.9.253	China	147.237.77.235	sviva.idf.il	Frk_Under_Attack_Con_Tcp	drop	2

10-25-2015-09:04:05 to 10-25-2015-10:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.74.114.77	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

10-25-2015-09:04:05 to 10-25-2015-10:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.162.116.221	147.237.0.34	Sweden	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
31.13.97.105	147.237.72.166	Ireland	aka.idf.il	portscan: TCP Distributed Portscan	1
185.100.85.71	147.237.76.30		himush.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.110.240	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.175.225.230	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential SSH Scan	1
89.175.225.230	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
82.81.31.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
54.72.73.168	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.3.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.52.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.21.73	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
89.175.225.230	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential SSH Scan	1
89.175.225.230	147.237.72.166	Russian Federation	aka.idf.il	ET SCAN Potential SSH Scan	1
62.90.215.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

10-25-2015-09:04:05 to 10-25-2015-10:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.151.48.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4144
141.0.15.113	Europe	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	171
46.19.86.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
212.76.101.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	119
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	88
95.86.110.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
46.19.85.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
85.64.35.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
80.74.100.98	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
77.3.7.212	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
46.19.86.192	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
46.19.86.171	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
80.246.133.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
86.247.0.19	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
85.250.77.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.18.206.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
68.180.230.29	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	17
37.26.147.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
46.116.242.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.19.86.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.65.168.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
2.54.189.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
80.178.147.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
149.78.226.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
176.13.2.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
192.117.235.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
132.185.161.132	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.27	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
84.228.15.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
37.26.147.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.26.149.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.0.9	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.2.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.149.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.7.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.7.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
213.57.153.162	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.178.213.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.183.169	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2832
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	56
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	52
147.236.238.180	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4466.jpg	Block	42
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	28
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	28
84.94.161.118	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	28
80.74.114.77	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 80.74.114.77	Block	14
176.12.147.204	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
85.130.240.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
207.46.13.48	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/tizmoret/home/default.asp	None	14
46.19.85.174	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14
80.74.114.77	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	14
176.13.20.243	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	14
87.69.172.233	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	14
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/undefined	Block	14
46.19.86.136	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	14
171.96.182.141	Thailand	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	14
80.246.139.21	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	14
176.106.227.53	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	14
109.64.187.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
79.177.20.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/resources/controls/captcha.ashx	Block	14
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/894-en/eitan.aspx	Block	14
46.19.86.181	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	14
171.96.182.141	Thailand	147.237.77.216	dover.idf.il	eMail Hoarding	Block	14
185.32.179.140	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/tfasim.aspx	None	14
137.116.71.170	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/robots.txt	Block	14
79.181.35.151	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	14
66.249.65.54	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/sachar/klali.aspx	Block	14
176.12.146.70	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/profs.asp	Block	14
188.165.15.121	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20041220a.htm	Block	14
37.142.68.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	14