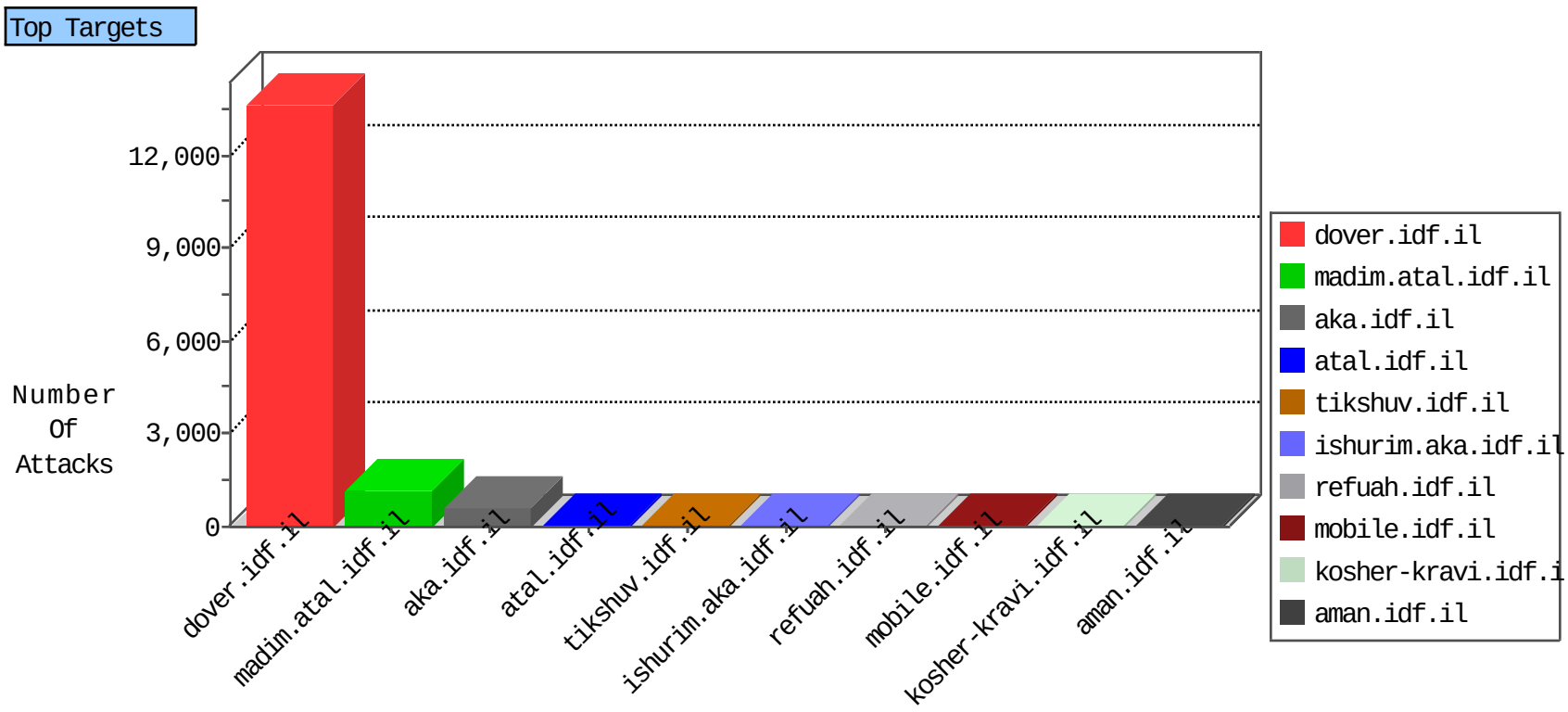
11-08-2015-14:04:03 to 11-08-2015-15:04:03

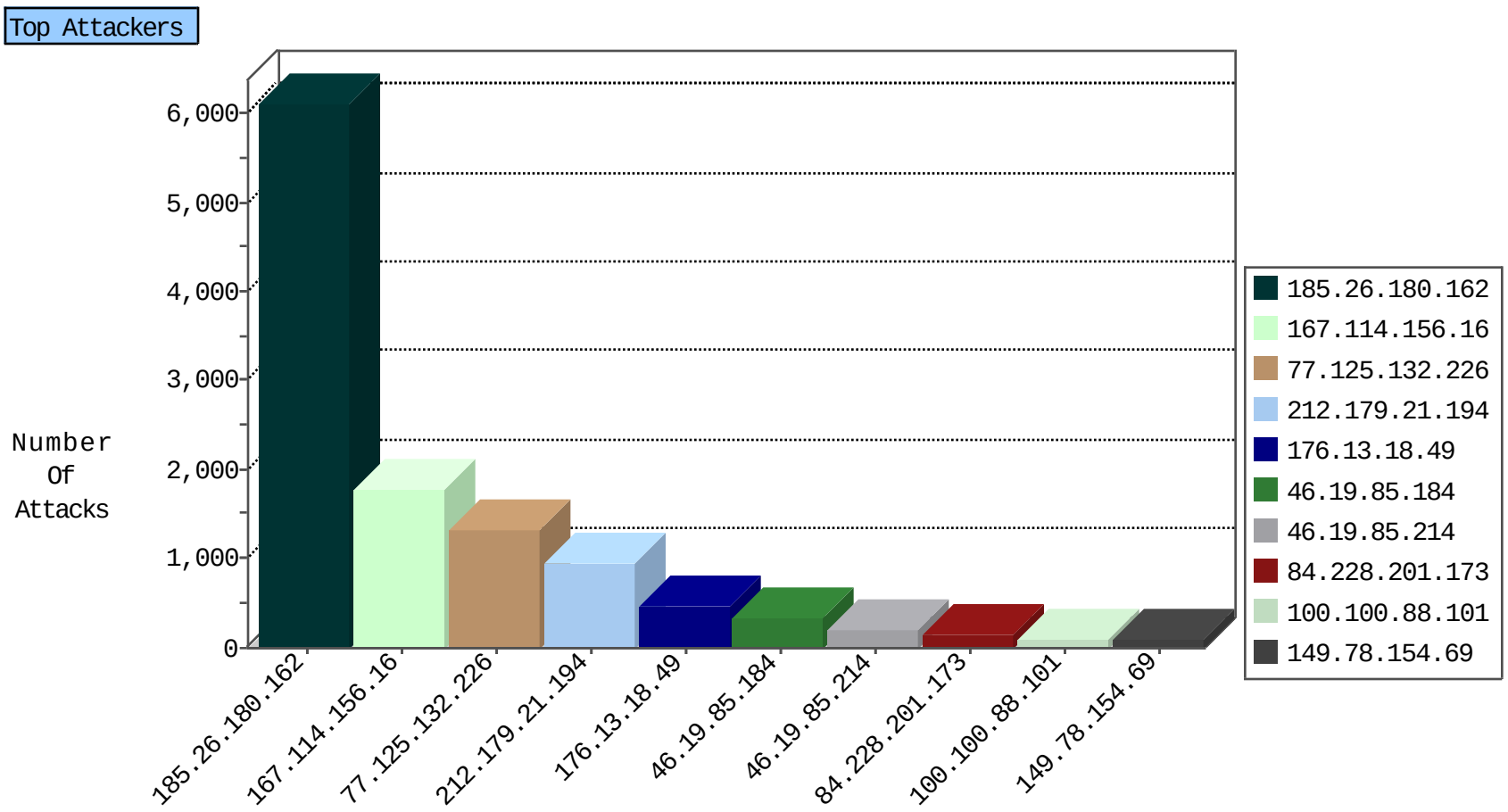
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-08-2015-14:04:03 to 11-08-2015-15:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.26.180.162	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6217
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2954
212.179.21.194	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2525
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	112
95.35.189.70	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
109.66.3.29	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.117.98.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
109.67.100.198	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.143.96.222	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
82.80.154.137	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
77.127.216.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
95.35.189.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
212.179.210.163	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
176.13.0.213	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
222.186.34.48	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
134.147.203.115	Germany	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
10.0.0.1		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
85.250.195.165	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
61.197.125.142	Japan	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

11-08-2015-14:04:03 to 11-08-2015-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.76.69	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
109.186.146.36	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
93.173.166.152	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
52.1.90.117	United States	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
223.73.45.53	China	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
109.64.116.214	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-08-2015-14:04:03 to 11-08-2015-15:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.26.149.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.139.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
121.41.116.64	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
121.41.116.64	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.67.155.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.38.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.179.161.7	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.194.147	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.158.12	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.238.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.185.20	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
121.41.116.64	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
121.41.116.64	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
121.41.116.64	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
84.111.140.235	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.6.4	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.212.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.151.54.209	147.237.76.30	Ukraine	himush.idf.il	ET SCAN NMAP -sS window 1024	1

11-08-2015-14:04:03 to 11-08-2015-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.26.180.162	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6041
77.125.132.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1334
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	947
46.19.85.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	209
100.100.88.101		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	88
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
46.19.86.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	73
79.181.138.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
176.67.109.239	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
176.13.23.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
87.69.38.135	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
46.210.134.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
213.151.32.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
84.109.33.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
198.251.52.101	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
146.122.203.34	United States	147.237.0.34	tikshuv.idf.i	drop	First packet isn't SYN	drop	42
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
5.29.198.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
213.8.99.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
81.218.133.196	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
93.173.61.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
95.35.189.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
109.67.2.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
84.247.161.206	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
212.143.3.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
46.19.85.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
66.102.8.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
66.102.8.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
188.161.184.76	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
100.100.80.161		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
2.54.41.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
176.12.144.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
79.181.2.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
2.54.155.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
192.114.91.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
212.25.123.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
212.143.96.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
84.108.237.149	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
82.80.36.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
95.186.152.253	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
79.179.121.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
89.139.190.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19

11-08-2015-14:04:03 to 11-08-2015-15:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.18.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	217
176.13.18.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	195
46.19.85.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	149
46.19.85.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
84.228.201.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.85.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	70
84.228.201.173	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 84.228.201.173	Block	61
46.19.85.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
46.19.86.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
176.13.18.49	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.18.49	Block	47
46.19.85.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
46.19.85.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
176.12.139.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
209.88.198.1	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 209.88.198.1	Block	6
176.12.138.142	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
109.186.164.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	5
84.94.176.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
157.55.2.168	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
209.88.198.1	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on www.logistics.atal.idf.il/sip_storage/files/1/size338x0/1531.jpg	Block	3
176.12.150.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.22.103	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
209.88.198.1	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/7/size338x0/1877.jpg	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
2.52.137.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
212.179.132.202	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
31.168.11.194	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachr	Block	1
104.236.110.194		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspxshared/usercontrols/headerupper/	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
89.139.190.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
159.203.135.194	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
79.179.174.62	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
45.55.192.83		147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
2.54.12.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
104.131.86.101	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
176.13.5.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
62.210.88.201	France	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.google.pl/search	Block	1
159.203.73.14	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
80.246.136.99	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.125.161.23	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
212.179.132.204	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.26.147.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.236.204.80		147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1

11-08-2015-14:04:03 to 11-08-2015-15:04:03