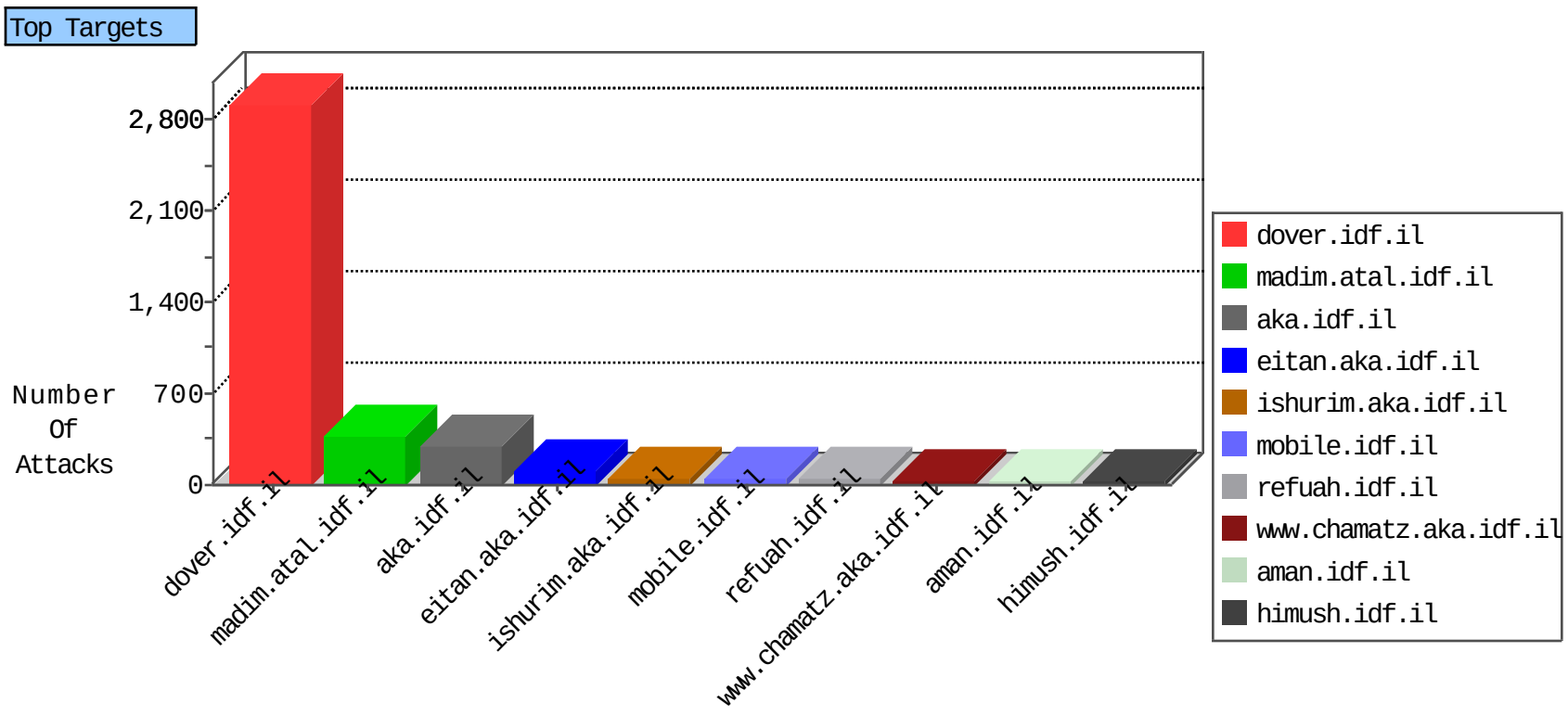
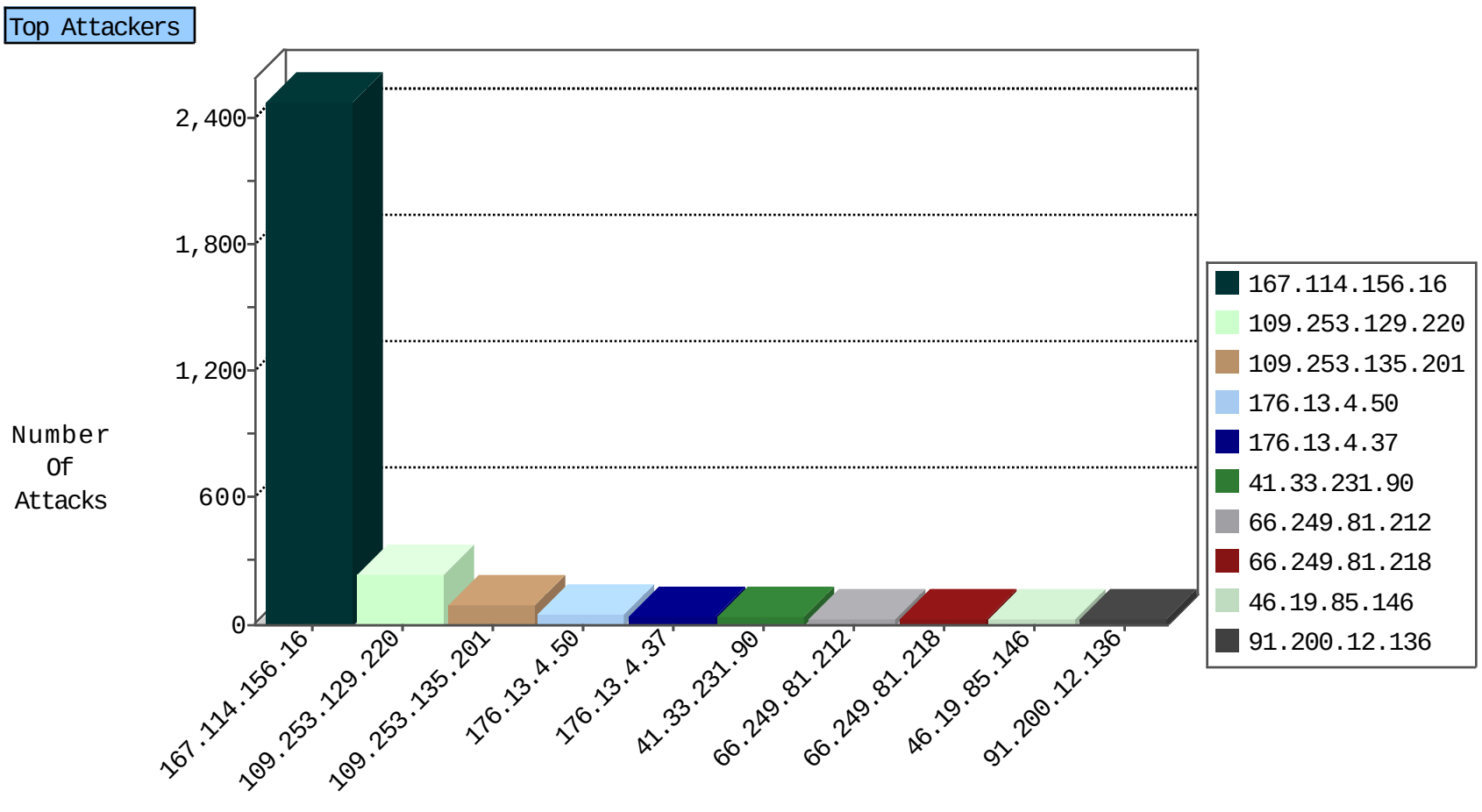
12-22-2015-09:04:09 to 12-22-2015-10:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



12-22-2015-09:04:09 to 12-22-2015-10:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3437
66.249.66.75	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3269
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	111
46.39.226.69	Russian Federation	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	3
82.213.16.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
31.223.85.47	Turkey	147.237.76.200	eitan.aka.idf.i	Block_Udp_All_Nets	drop	1
31.223.85.47	Turkey	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
38.229.1.13	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

12-22-2015-09:04:09 to 12-22-2015-10:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-22-2015-09:04:09 to 12-22-2015-10:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
23.96.213.135	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
193.104.41.54	147.237.76.147	Moldova, Republic of	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
172.245.11.57	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
166.63.122.229	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
125.65.165.215	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
95.86.107.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
213.57.241.156	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.130.216.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.104.41.54	147.237.76.202	Moldova, Republic of	e.halag.idf.il	ET SCAN Potential SSH Scan	1
77.126.100.202	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.104.41.54	147.237.76.176	Moldova, Republic of	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.76.42	Moldova, Republic of	refuah.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.87.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.65.165.215	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.141.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
80.246.136.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.104.41.54	147.237.76.177	Moldova, Republic of	ncore.idf.il	ET SCAN Potential SSH Scan	1

12-22-2015-09:04:09 to 12-22-2015-10:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
89.138.176.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
79.179.178.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.246	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
46.19.85.150	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
79.177.30.174	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
66.249.81.218	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
66.249.81.218	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	15
66.249.81.212	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
66.249.81.212	United States	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	14
46.19.86.18	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.176.61.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
199.30.25.197	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
24.237.158.10	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
79.181.70.8	Israel	147.237.76.42	refuah.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	10
212.199.239.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
91.200.12.136	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
91.200.12.136	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	8
91.200.12.136	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	8
46.19.85.103	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.86.199	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.199.10.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.12.87	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.221.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.135.201	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.147	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.82	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.207.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.97	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
147.236.38.168	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
91.200.12.143	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4

12-22-2015-09:04:09 to 12-22-2015-10:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.129.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
109.253.135.201	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.135.201	Block	90
109.253.129.220	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.129.220	Block	79
176.13.4.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
176.13.4.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
176.12.147.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
109.253.129.220	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.253.129.220	Block	22
176.12.149.223	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	9
176.228.8.251	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
79.179.183.139	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.179.183.139	Block	4
176.228.8.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
176.13.4.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.4.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.143.103.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
46.121.229.29	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	3
176.12.140.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.46.75	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
79.183.50.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.179.183.139	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	2
79.180.145.207	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
2.54.186.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.129	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to /x	Block	1
74.208.105.30	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/5/size220x0/17765.jpg	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.166.186.208	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
176.13.10.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
82.102.136.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout2.css	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/e/public/onclick/	Block	1
46.19.85.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
196.22.142.216	South Africa	147.237.77.74	law.idf.il	PHP Attempt	Block	1
91.231.193.150	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
176.13.15.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method pk_id.20.8afc=6dc462e88cbdde35.1447868799.1.1447868800.1447868799. in URL	Block	1
5.29.76.244	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
149.88.113.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
74.208.105.30	United States	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../../images/shared/calendar/prev_but.gif	Block	1
185.32.179.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
82.102.136.67	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
62.0.102.190	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.0.102.190	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1

12-22-2015-09:04:09 to 12-22-2015-10:04:09