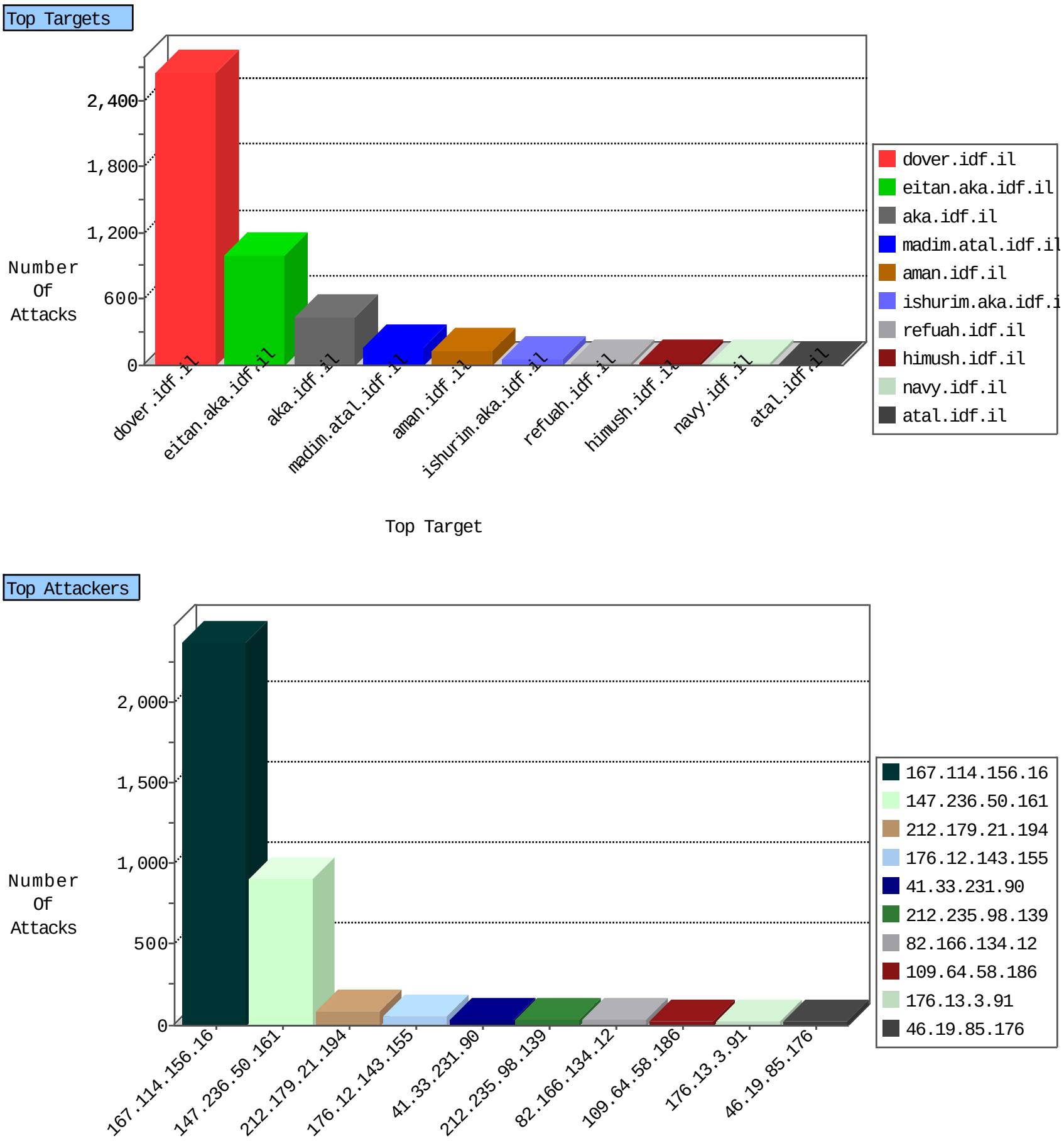
12-06-2015-14:04:03 to 12-06-2015-15:04:03

IDF Under Attack Daily Report



12-06-2015-14:04:03 to 12-06-2015-15:04:03

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	3570
66.249.64.186	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	52
134.147.203.115	Germany	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
167.88.7.246	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
167.88.7.229	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
167.88.7.249	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
167.88.7.230	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	drop	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
167.88.7.244	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1

12-06-2015-14:04:03 to 12-06-2015-15:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-06-2015-14:04:03 to 12-06-2015-15:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
104.128.144.131	147.237.72.166	Canada	aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.40.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.63.17	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.113.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.204.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.92.242	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
46.19.85.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.143.64	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	1
40.115.58.160	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.160.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.51.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.16.240	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.89.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.169.251.74	147.237.76.177	Germany	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.206	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.117.141.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.189.206.16	147.237.76.44	New Zealand	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.174	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.143.64	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	1
37.142.101.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.65.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-06-2015-14:04:03 to 12-06-2015-15:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
147.236.50.161	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	828
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	38
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	34
82.166.134.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
80.246.137.148	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
46.19.85.243	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.85.8	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
62.0.200.164	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
213.57.128.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
185.120.125.31		147.237.72.166	aka.idf.il	drop	SAM rule	drop	14
109.66.41.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.12.141.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.64.58.186	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	12
212.143.49.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.64.58.186	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
77.125.154.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.64.195.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.39.56	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.85.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.181.127.42	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.64.151.178	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.8	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
121.54.38.114	Philippines	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	7
108.171.128.166	United Kingdom	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
84.94.41.65	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
157.55.39.112	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.145.217.246	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
157.55.39.112	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.74.6	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.15	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.130.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.181	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.133.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
132.64.201.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
121.54.38.114	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.57.158.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.175	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.120.125.4		147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
84.94.152.45	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.175	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.130.89	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

12-06-2015-14:04:03 to 12-06-2015-15:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
147.236.50.161	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 147.236.50.161	Block	81
176.12.143.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
176.13.3.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.12.145.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
46.19.85.190	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.19.85.190	Block	22
176.12.143.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
46.19.86.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
109.67.134.140	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 109.67.134.140	None	5
46.19.85.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
176.13.12.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.67.134.140	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	2
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.85	Block	2
5.29.167.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.85	Block	2
89.138.241.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.241.226.42	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
2.52.191.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.98	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
78.30.195.34	Russian Federation	147.237.77.74	law.idf.il	Parameter Type Violation FileName in www.mag.idf.il/templates/getfile/getfile.aspx	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
46.19.85.85	Israel	147.237.77.216	dover.idf.il	Malformed URL	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
37.19.116.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.35.118	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/valtam	Block	1
2.54.38.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.74.112.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.143.49.22	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
46.116.202.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
148.177.129.213	Europe	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
46.19.85.132	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
78.30.195.34	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
199.203.172.65	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd	None	1
176.13.16.20	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.104	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/eng	Block	1
95.86.69.159	Israel	147.237.72.166	aka.idf.il	Unknown Parameter usg in www.aka.idf.il/main/rabanut/general.aspx	None	1
66.249.93.206	Israel	147.237.72.166	aka.idf.il	URL is Above Root Directory www.aka.idf.il/../images/bg.gif	Block	1
46.166.188.247	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
176.12.140.210	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
2.71.44.151	Sweden	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.94.120.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
213.151.62.179	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
2.50.132.110	United Arab Emirates	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
79.179.60.128	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
46.19.86.0	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
140.242.217.2	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/8/size338x0/1808.jpg	Block	1

12-06-2015-14:04:03 to 12-06-2015-15:04:03