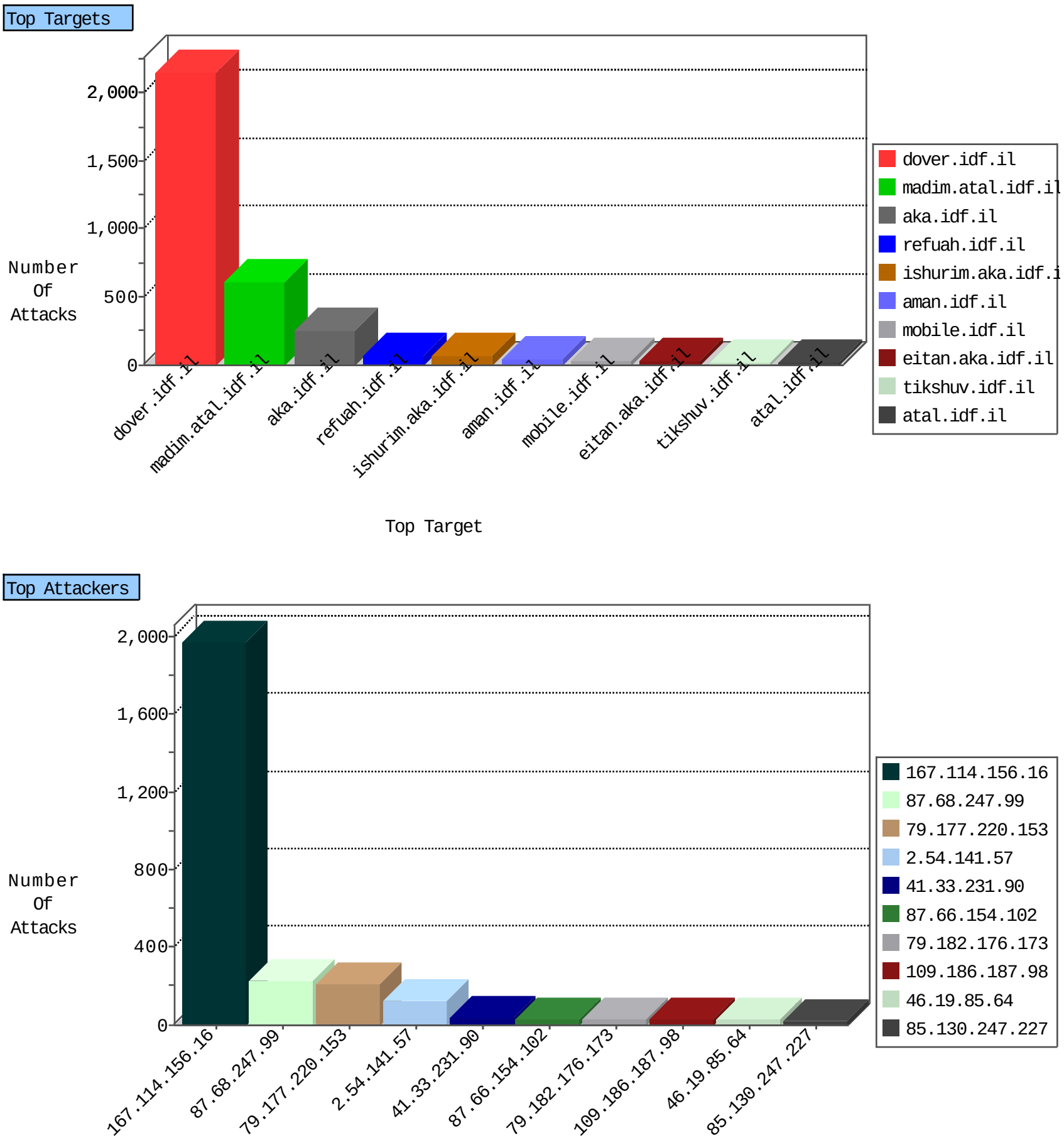
12-24-2015-22:04:02 to 12-24-2015-23:04:02

IDF Under Attack Daily Report



12-24-2015-22:04:02 to 12-24-2015-23:04:02

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	3267
79.177.152.157	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
178.122.141.202	Belarus	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
217.34.35.31	United Kingdom	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
175.139.91.171	Malaysia	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
77.247.178.132	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
173.195.0.21	United States	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
173.195.0.22	United States	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
217.34.35.31	United Kingdom	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.195	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
173.195.0.23	United States	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
77.247.178.132	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

12-24-2015-22:04:02 to 12-24-2015-23:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.215.106	United States	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
149.202.54.6	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

12-24-2015-22:04:02 to 12-24-2015-23:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
132.74.95.21	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
88.249.106.23	147.237.76.42	Turkey	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
78.193.2.8	147.237.76.200	France	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.64.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.104.49.211	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.208	147.237.72.156		aman.idf.il	ET SCAN NMAP -sS window 1024	1
96.57.217.187	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
87.69.59.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
65.61.135.250	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1

12-24-2015-22:04:02 to 12-24-2015-23:04:02

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
46.19.85.64	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	28
46.19.86.186	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.183.191.234	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
2.54.141.57	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
109.67.202.65	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
87.66.154.102	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
87.66.154.102	Belgium	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
109.186.187.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	12
79.183.60.254	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
94.230.86.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
79.182.176.173	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	10
93.173.236.12	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
85.130.247.227	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.64.24.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.141.57	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.54.141.57	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.54.141.57	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.146.246	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
46.163.68.111	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
85.130.247.227	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
109.186.187.98	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.65.100.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.176.173	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence		monitor	6
85.130.247.227	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
89.138.64.19	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.255.3	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.186.187.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.186.187.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.176.173	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
79.182.176.173	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.45	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.141.57	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.45	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.182.176.173	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	5
94.230.86.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.254.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.188	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.102.254.103	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.122	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
94.230.86.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.196	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
199.30.24.40	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.230.86.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.132.212.222	United Kingdom	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

12-24-2015-22:04:02 to 12-24-2015-23:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.220.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	159
87.68.247.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	119
87.68.247.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.54.141.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
79.177.220.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
2.54.13.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
93.173.161.180	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 93.173.161.180	Block	14
87.68.247.99	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 87.68.247.99	Block	8
5.29.199.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.255.3	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
37.26.147.188	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
2.54.10.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.8.204.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.230.86.220	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.121.82.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.243.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
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	1
80.246.136.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
128.127.107.99	Netherlands	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 128.127.107.99 (Unknown SSL Session)	None	1
46.166.170.3	Lithuania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
93.173.161.180	Israel	147.237.72.166	aka.idf.il	Too Many 404: Response Code per Session	Block	1
85.64.88.65	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.45	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
213.57.57.185	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1235-he/atal.aspx	Block	1
79.178.201.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.63.177	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 2.54.63.177	Block	1
176.12.148.174	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19915-he/dover.aspx	Block	1
87.69.51.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.102.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.18	United States	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/general/general.aspx	Block	1
84.108.237.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
128.127.107.99	Netherlands	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
63.143.34.37	United States	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
46.19.86.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.57.244.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.32.179.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.52.51	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
46.121.158.192	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.121.158.192	Block	1
87.69.190.81	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
37.26.147.204	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	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
84.111.127.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.125.10.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.8.142.14	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

12-24-2015-22:04:02 to 12-24-2015-23:04:02