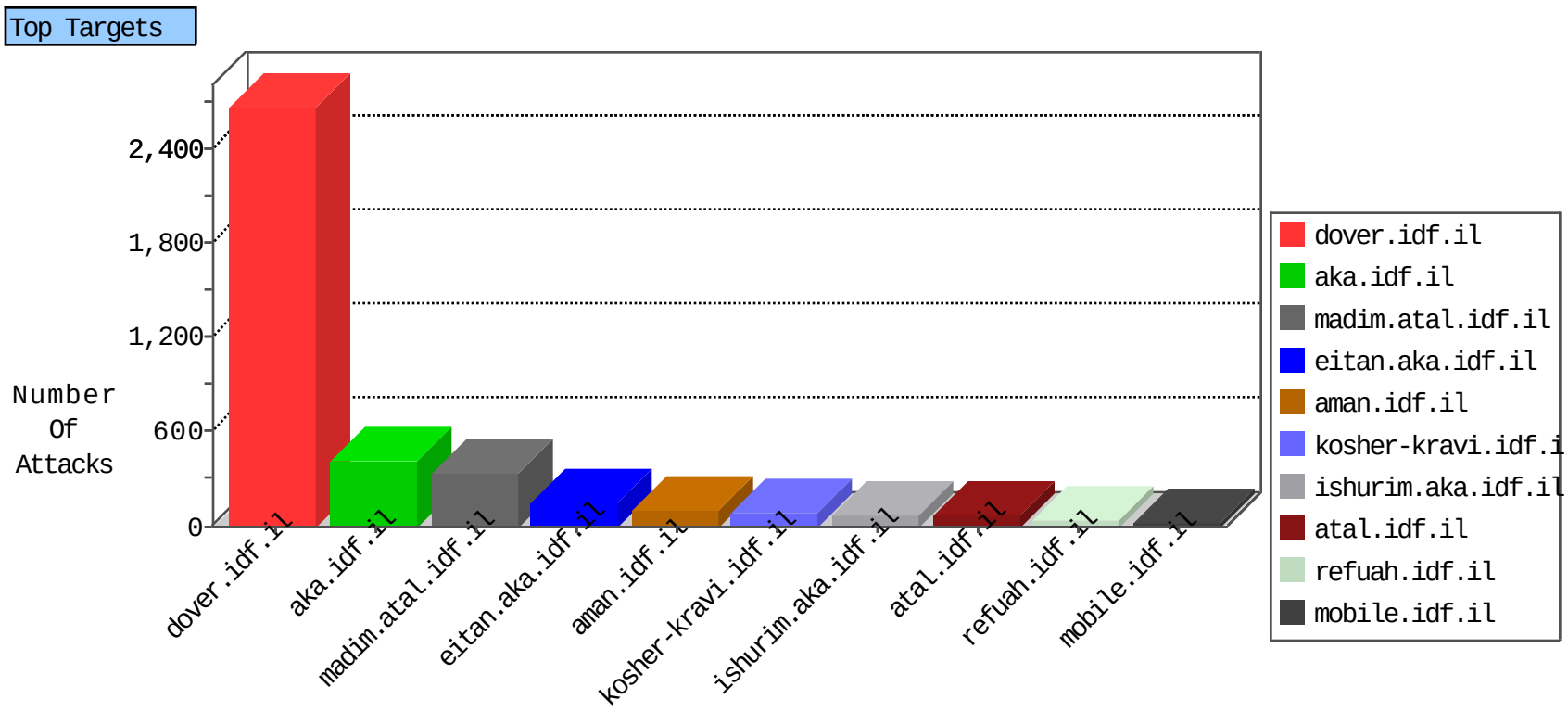
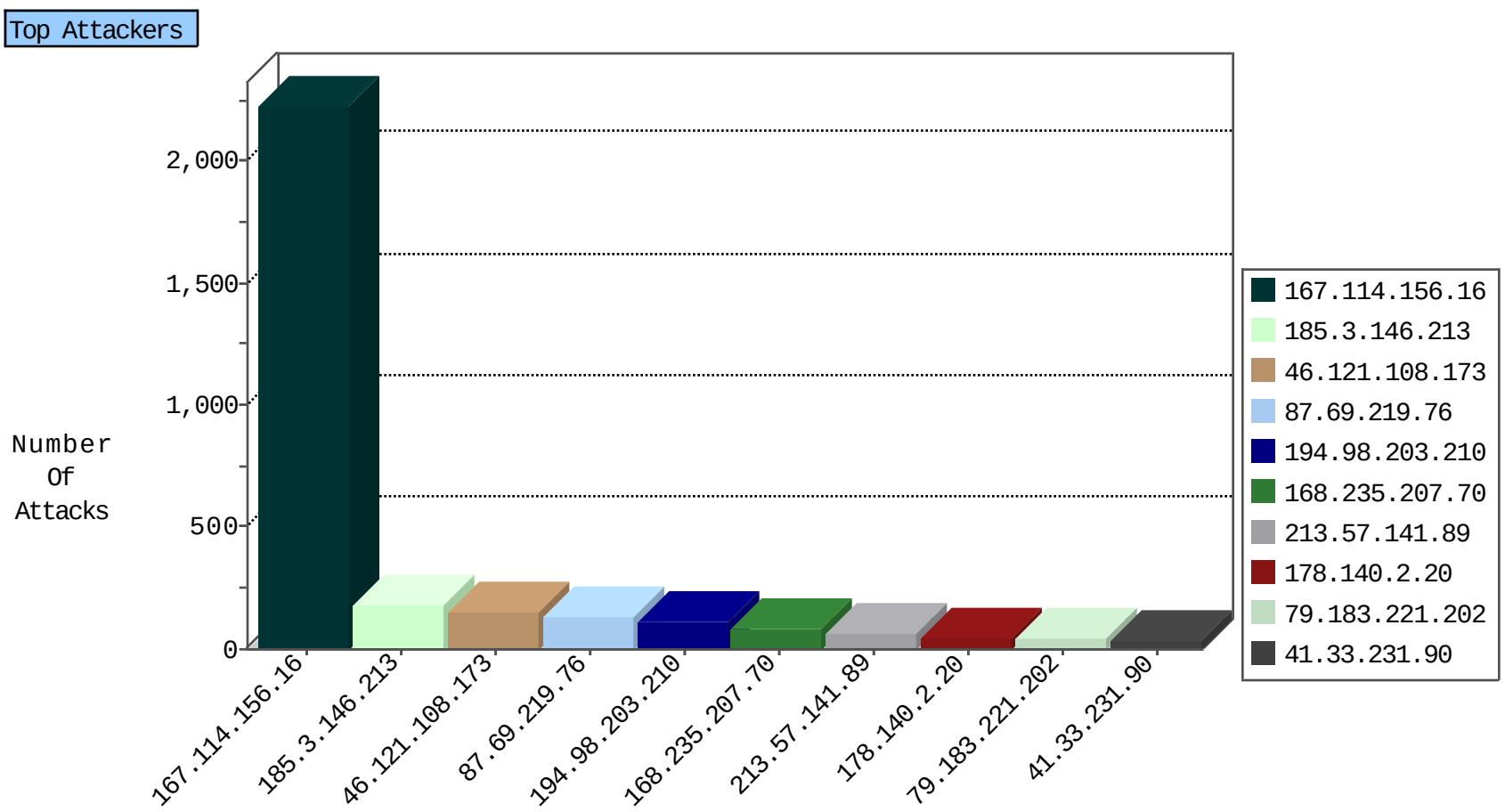
12-12-2015-22:04:05 to 12-12-2015-23:04:05

IDF Under Attack Daily Report





12-12-2015-22:04:05 to 12-12-2015-23:04:05

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	3395
168.235.207.70	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
168.235.207.70	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
94.102.51.38	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
172.98.67.15		147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
168.235.207.70	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	1
52.53.222.9	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

12-12-2015-22:04:05 to 12-12-2015-23:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.142	Italy	147.237.72.166	aka.idf.il	C228: HTTP: AhrefBot crawler	Block	1

12-12-2015-22:04:05 to 12-12-2015-23:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
193.105.134.220	147.237.76.198	Sweden	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
166.63.125.149	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
74.203.240.228	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 2048	1
54.183.201.4	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
166.63.125.149	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
166.63.125.149	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.195	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
74.203.240.228	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 4096	1
74.203.240.228	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -f -sS	1
54.183.201.4	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
54.183.201.4	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -f -sS	1

12-12-2015-22:04:05 to 12-12-2015-23:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.207.70	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	70
194.98.203.210	France	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	66
213.57.141.89	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	48
178.140.2.20	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	35
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
79.183.221.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
194.98.203.210	France	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	alert	23
46.19.85.144	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
79.183.221.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
76.126.183.46	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
79.176.161.18	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
178.140.235.131	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	17
213.57.141.89	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
5.22.131.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
109.66.113.232	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.116.235.181	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.116.235.181	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.54.130.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
109.67.33.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
109.67.33.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
87.69.219.76	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	11
80.246.133.170	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.121.108.173	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
77.127.170.3	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.255	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
194.98.203.210	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
213.8.204.61	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
217.132.29.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
217.132.29.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.142.221.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
89.138.80.148	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
95.86.105.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
213.8.204.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
95.86.105.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.0.101.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.93.15	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
62.0.101.97	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.120.101.210	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.198.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.136.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.8.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.222.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.79.193	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

12-12-2015-22:04:05 to 12-12-2015-23:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.3.146.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	144
46.121.108.173	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.121.108.173	Block	137
87.69.219.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
87.69.219.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	57
185.3.146.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	38
5.22.131.105	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	5
46.19.85.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
2.54.44.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.3.146.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	3
109.67.132.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.69.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
109.65.160.235	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	3
85.64.101.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
176.63.8.127	Hungary	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	2
109.67.33.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.148.228	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
185.120.126.201		147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/booklets.aspx	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
79.179.184.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.125.50		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.217.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.145.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.210.163	Israel	147.237.72.156	aman.idf.il	Abnormally Long Request method	Block	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/report1010to1610.aspx	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.86.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.34	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/faq/faq.aspx	Block	1
79.179.210.163	Israel	147.237.72.156	aman.idf.il	Malformed URL	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.57.54.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
80.246.136.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.210.163	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name (Ã•Ã´R[[#16]]ÃƒDJÃ“Ã¶Ã•/5x[[#30]]ÂžÂ¤Â¶[[#22]]Â—Â›Â-[[#2]]yÃŒÂŸKÂ™Ã…HÃ†Ã¿Ã‹Â'?Ã™uÂ‡[[#21]]	Block	1
157.55.39.173	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/giyus/qanda/default.asp	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.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
85.64.150.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.43.68.70	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	1
207.46.13.67	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
79.179.210.163	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 79.179.210.163 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
109.67.115.55	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
77.126.2.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
213.57.228.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
91.127.65.165	Slovakia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
194.98.203.210	France	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
80.246.136.79	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.210.163	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Value	Block	1
176.12.138.189	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1

12-12-2015-22:04:05 to 12-12-2015-23:04:05