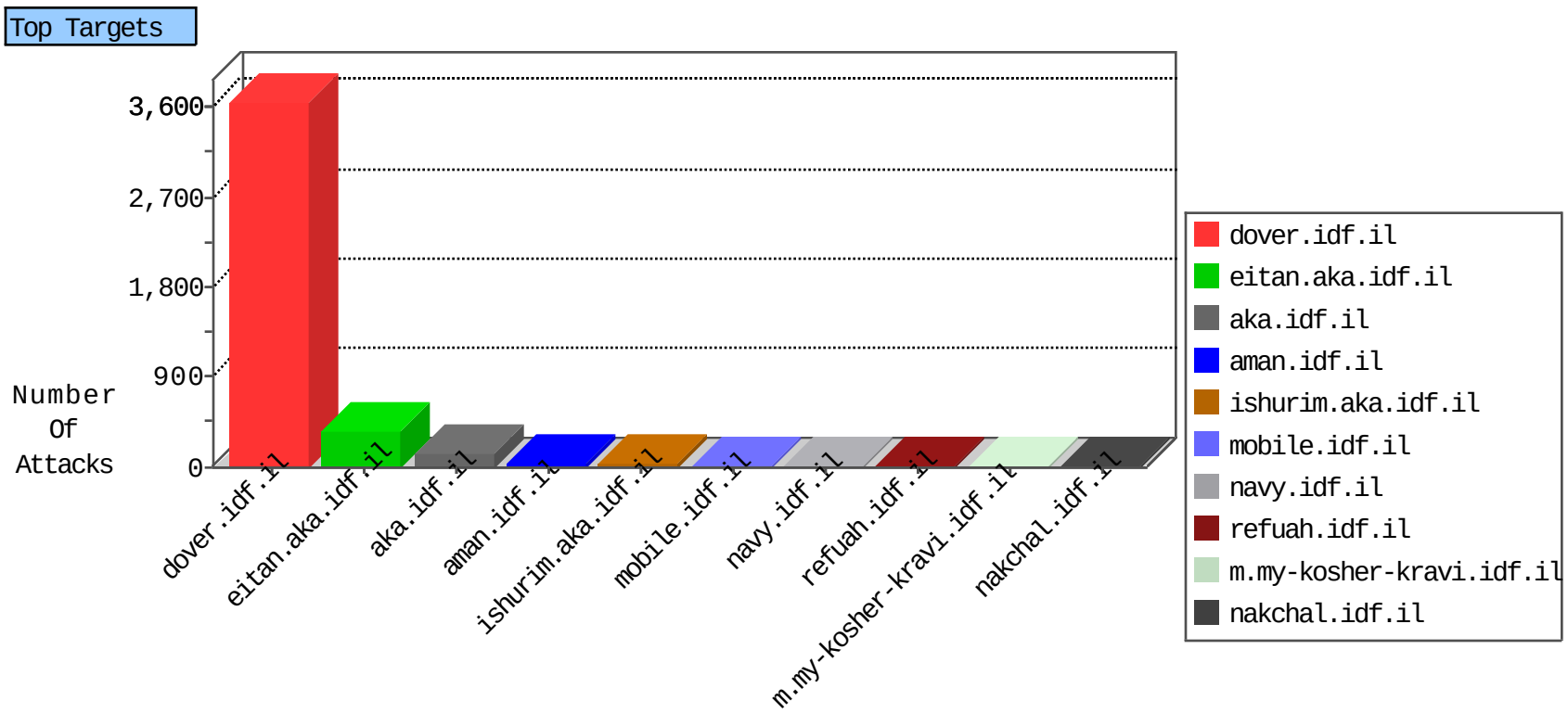
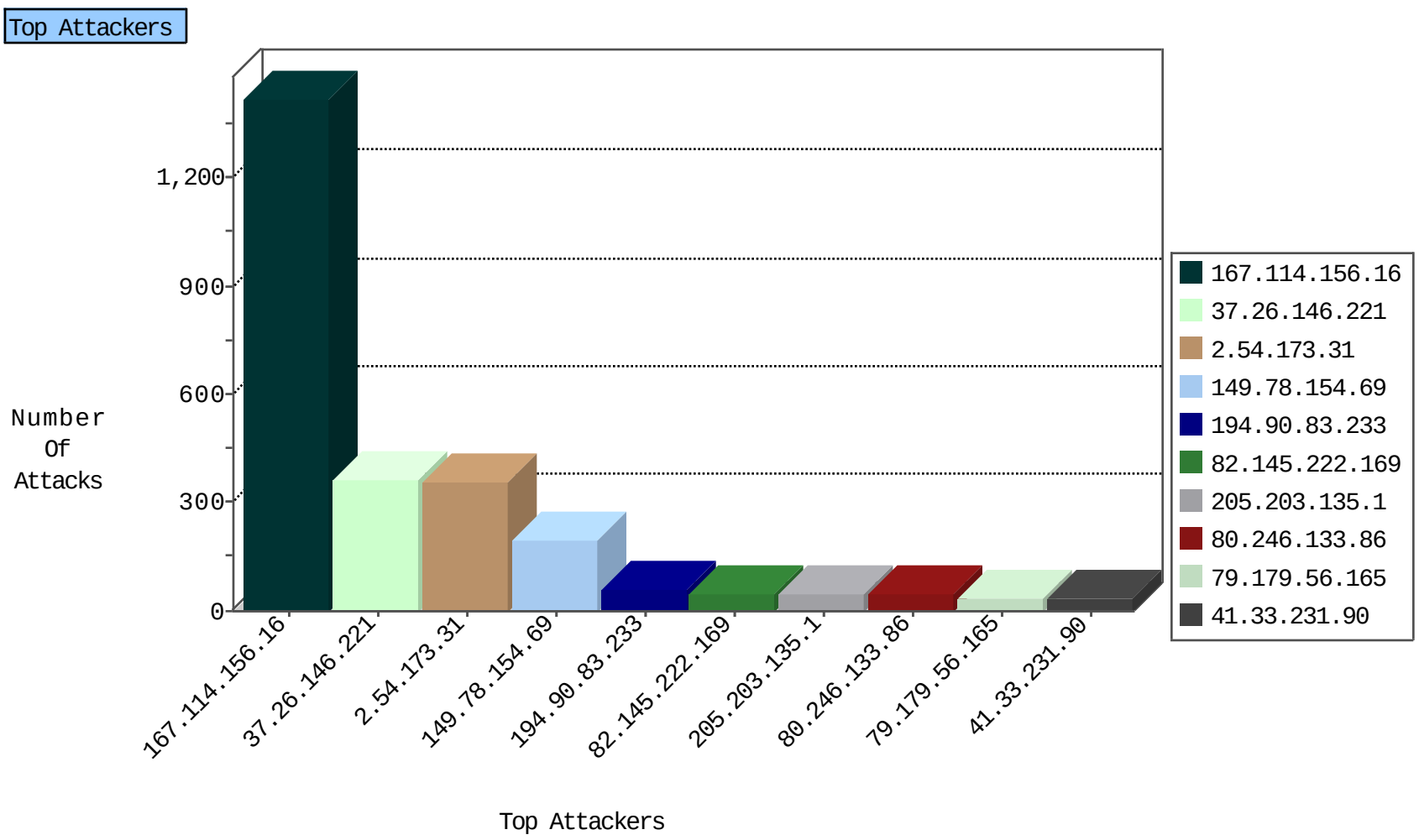
11-03-2015-07:04:09 to 11-03-2015-08:04:09

IDF Under Attack Daily Report





11-03-2015-07:04:09 to 11-03-2015-08:04:09

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	2533
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	463
2.54.175.22	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	55
37.142.68.27	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
46.19.85.66	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	24
84.228.165.6	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
79.179.18.143	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
2.54.58.26	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
84.189.220.17	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.178.226.225	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.25.102.63	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
79.182.184.4	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
199.203.215.1	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.154.94.24	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.237	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
87.69.86.172	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.24.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
66.249.78.224	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.7.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
2.54.181.153	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
71.6.216.39	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
50.97.195.27	United States	147.237.77.61	e.cogat.idf.il	Invalid TCP Flags	drop	1
212.25.102.63	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
149.78.215.93	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
71.6.216.61	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
192.0.86.187	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
213.57.234.91	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
46.19.86.144	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.30.185	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

11-03-2015-07:04:09 to 11-03-2015-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-03-2015-07:04:09 to 11-03-2015-08:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	4
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
185.58.201.28	147.237.76.86	Lebanon	navy.idf.il	ET SCAN NMAP -sA (2)	2
162.248.10.134	147.237.0.16	Canada	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
149.78.133.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.129.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.90.155.46	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
162.248.10.134	147.237.0.16	Canada	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
162.248.10.134	147.237.0.16	Canada	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
85.250.145.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
36.84.67.23	147.237.77.216	Indonesia	dover.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1

11-03-2015-07:04:09 to 11-03-2015-08:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.26.146.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	366
2.54.173.31	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	348
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	197
194.90.83.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
82.145.222.169	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
80.246.133.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
79.179.56.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
213.57.234.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
100.100.23.206		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	28
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
192.117.12.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
146.115.89.236	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.83.158	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
52.2.57.144	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
50.18.94.121	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
100.100.39.102		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
85.64.102.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
176.12.136.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.128	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
207.46.13.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.26.148.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
199.203.215.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
2.54.175.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
37.127.112.217	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.183.221.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.147.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.228.165.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.39.102		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
149.78.133.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.154.94.23	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
176.13.7.207	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.103	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	12
5.108.140.190	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
84.189.220.17	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.13.2.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

11-03-2015-07:04:09 to 11-03-2015-08:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.173.31	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.173.31	Block	10
84.109.1.56	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.109.1.56	Block	5
46.19.85.231	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	3
23.253.237.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-22902-he/	Block	3
84.109.1.56	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
2.54.173.75	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	3
66.249.78.66	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
2.54.21.200	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	2
176.12.138.178	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.13.3.154	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/7/size220x0/17467.jpg	Block	1
104.131.147.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
208.115.111.73	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
5.9.41.74	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.9.41.74	Block	1
174.129.237.157	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
199.16.156.126	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/7/size220x0/17467.jpg	Block	1
46.117.40.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.41.149	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
76.100.161.163	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized Method GET for www.aka.idf.il/iturim/asp/searchresults.asp	Block	1
5.9.41.74	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
208.90.155.46	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 208.90.155.46 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
46.121.141.140	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
2.54.173.31	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	1
139.193.9.80	Indonesia	147.237.77.74	law.idf.il	Illegal Byte Code Character in Header Value	Block	1
77.125.86.24	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71507-he/maarachot.aspx	Block	1
66.249.78.234	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
208.90.155.46	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/iturim/asp/searchresults.asp	Block	1
139.193.9.80	Indonesia	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Header Value from 139.193.9.80	Block	1
79.177.29.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.67.247	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71854-he/maarachot.aspx	Block	1
178.137.81.238	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
46.19.85.55	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.109.1.56	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
66.249.78.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16789-he/dover.aspx	Block	1
208.115.111.73	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/giyus/forum/asp/showforum.asp	None	1
157.55.39.164	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/home/default.aspx	Block	1
81.218.157.23	Israel	147.237.77.216	dover.idf.il	Distributed NULL Character in Method	Block	1
66.249.67.251	Israel	147.237.72.166	aka.idf.il	Unauthorized Method GET for aka.idf.il/iturim/asp/searchresults.asp	Block	1

11-03-2015-07:04:09 to 11-03-2015-08:04:09