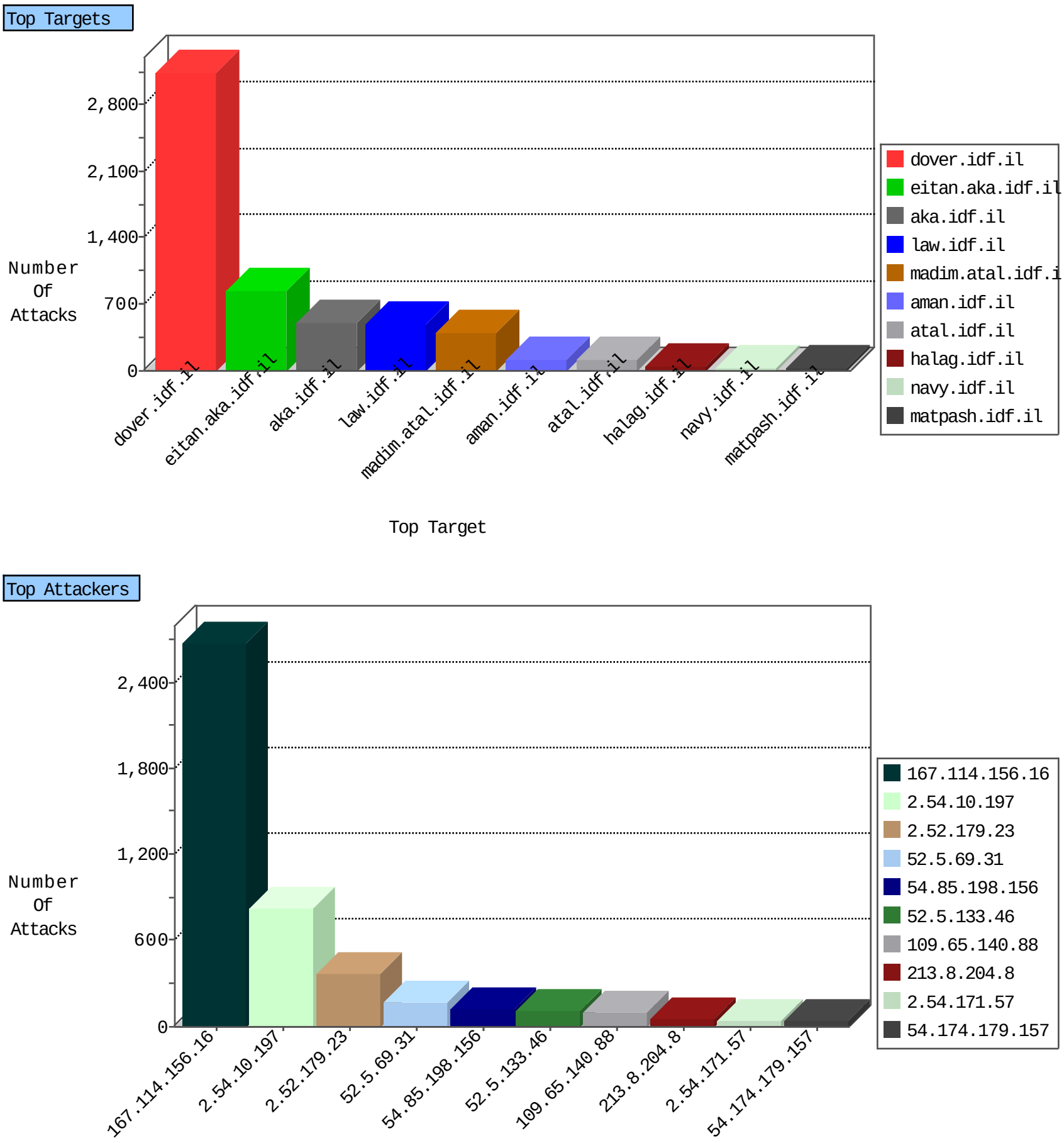
12-01-2015-19:04:09 to 12-01-2015-20:04:09

IDF Under Attack Daily Report



12-01-2015-19:04:09 to 12-01-2015-20:04:09

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	3656
146.185.57.7	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3

12-01-2015-19:04:09 to 12-01-2015-20:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.193	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1
195.154.188.29	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
195.154.188.188	France	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

12-01-2015-19:04:09 to 12-01-2015-20:04:09

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	3
93.173.237.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.172.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.97.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.8.50	Poland	e.tikshuv.idf.i	ET SCAN NMAP -sS window 1024	1
109.67.178.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.61.135	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.8.50	Netherlands	e.tikshuv.idf.i	ET SCAN NMAP -sS window 1024	1
87.68.253.56	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.67.232	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
43.229.53.89	147.237.0.200	Japan	m4u.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.136.11	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.136.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.175.236.44	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1

12-01-2015-19:04:09 to 12-01-2015-20:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.10.197	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	702
52.5.69.31	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	167
54.85.198.156	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	124
52.5.133.46	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	109
109.65.140.88	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	97
213.8.204.8	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	53
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
54.174.179.157	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	36
66.249.69.128	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
100.100.7.61		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.11.59		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	22
213.57.130.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
109.160.237.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
100.100.87.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
91.226.212.49	Ukraine	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	15
100.100.8.243		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.171.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
5.29.132.222	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.176.184.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
100.100.46.239		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
185.27.105.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.146.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.20.103	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
31.154.87.88	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
89.138.76.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.186.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.172.182.162	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.86	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.177.56.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.1	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.190.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.214.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.172.182.162	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.55	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.56.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.94.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.181.190.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.68.152.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

12-01-2015-19:04:09 to 12-01-2015-20:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.179.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	262
2.54.10.197	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.10.197	Block	124
2.52.179.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
2.54.171.57	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 2.54.171.57	Block	18
77.125.75.129	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.125.75.129	Block	9
2.54.151.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.19.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
85.65.63.136	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.210.199.137	Netherlands	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
199.103.62.15	Canada	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	3
185.32.179.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.210.199.137	Netherlands	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 149.210.199.137	Block	3
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.114	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
149.210.199.137	Netherlands	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	2
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.102.254.109	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
199.103.62.15	Canada	147.237.72.166	aka.idf.il	Distributed Admin Blocking	Block	2
2.54.163.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.113	Israel	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	2
95.35.54.128	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
2.54.10.197	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 2.54.10.197	Block	2
176.13.0.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.27.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
199.103.62.15	Canada	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/index.php	Block	2
157.55.39.18	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.183.136.42	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
46.120.169.127	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.169.127	Block	2
78.129.154.135	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
183.171.20.96	Malaysia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.85.113	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.113	Block	1
89.138.76.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.43	Block	1
37.142.68.83	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
83.132.231.68	Portugal	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
213.57.228.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
79.181.190.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
109.66.60.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.56.118	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.120.126.36		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	1
46.19.85.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.175	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/602-2265-he/patzar.aspx - paragraph_12	Block	1
176.67.119.128	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
80.246.136.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1

12-01-2015-19:04:09 to 12-01-2015-20:04:09