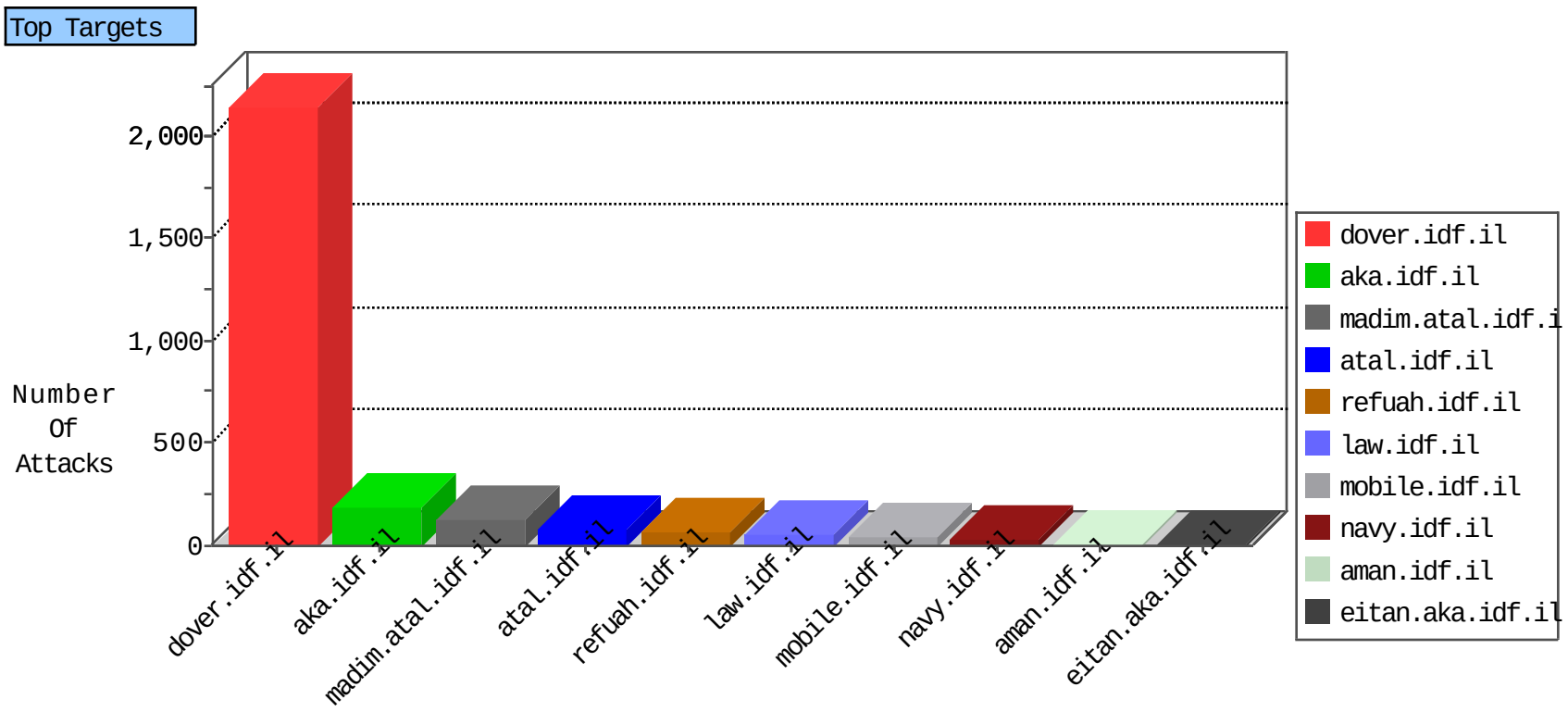
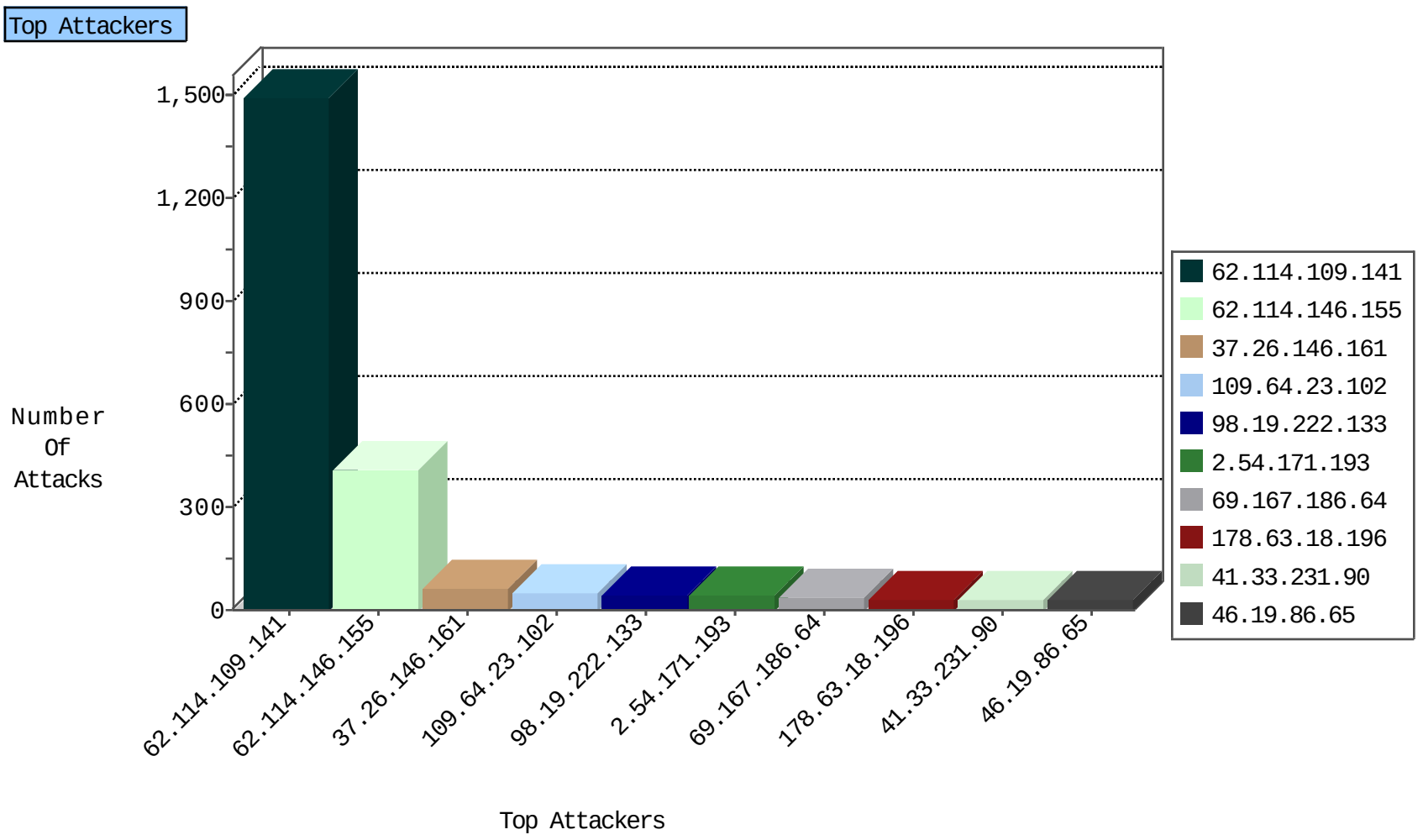
02-16-2016-00:04:05 to 02-16-2016-01:04:05

IDF Under Attack
Daily Report





02-16-2016-00:04:05 to 02-16-2016-01:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.114.109.141	Egypt	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	9354
62.114.109.141	Egypt	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1828
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	466
177.179.65.20	Brazil	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	22
128.0.73.15	Denmark	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
89.248.160.138	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
173.208.206.204	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
107.150.60.78	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	drop	1
27.156.2.122	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
70.199.194.231	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
191.17.194.221	Brazil	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.138	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
128.0.73.15	Denmark	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

02-16-2016-00:04:05 to 02-16-2016-01:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.19.222.133	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
69.167.186.64	United States	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
46.137.81.122	Ireland	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
87.242.112.35	Russian Federation	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	8
46.137.81.122	Ireland	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
178.63.18.196	Germany	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
87.106.179.116	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
178.63.18.196	Germany	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.96.128.60	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
178.63.18.196	Germany	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
87.242.112.35	Russian Federation	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
69.167.186.64	United States	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
66.135.63.82	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	3

02-16-2016-00:04:05 to 02-16-2016-01:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.19.222.133	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	33
69.167.186.64	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	21
178.63.18.196	147.237.76.86	Germany	navy.idf.il	SQL Injection - Select From	20
46.137.81.122	147.237.77.233	Ireland	atal.idf.il	SQL Injection - Select From	14
87.242.112.35	147.237.77.216	Russian Federation	dover.idf.il	SQL Injection - Select From	14
66.96.128.60	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	10
87.106.179.116	147.237.77.74	Germany	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	3
77.126.148.17	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN NMAP -sA (2)	2
79.180.161.184	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN NMAP -sA (2)	2
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
146.148.116.152	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
130.211.100.171	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
118.140.105.132	147.237.0.200	Hong Kong	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
118.140.105.132	147.237.0.16	Hong Kong	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.219.238.10	147.237.76.196		e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.21	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.104.41.141	147.237.77.243	Moldova, Republic of	mobile.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
146.148.116.152	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
50.204.188.142	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
121.201.27.61	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
118.140.105.132	147.237.0.17	Hong Kong	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
104.219.238.10	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.21	147.237.0.33	Netherlands	idf.il	ET SCAN Potential VNC Scan 5900-5920	1

02-16-2016-00:04:05 to 02-16-2016-01:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.114.109.141	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	352
62.114.146.155	Egypt	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	91
62.114.146.155	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	91
62.114.146.155	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	91
62.114.146.155	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	77
62.114.109.141	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	63
62.114.146.155	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	56
62.114.109.141	Egypt	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	50
109.64.23.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
62.114.109.141	Egypt	147.237.77.216	dover.idf.il	drop		drop	31
62.114.109.141	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
79.182.152.201	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
46.19.86.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
1.39.50.135	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
149.78.193.136	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.8.204.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
213.57.178.72	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
80.178.157.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
66.96.128.60	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
109.253.202.59	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
95.35.60.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.165.98	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.26.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.231	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
24.114.69.66	Canada	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.117	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.147.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.177.1.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
177.185.192.50	Brazil	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
46.19.86.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
62.219.137.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
93.172.225.210	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
188.120.148.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.165.98	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.183.201.190	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.117	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.128.27	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.180.203.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.64.33.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
69.58.178.57	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.156.179	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.146.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
2.54.171.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
5.29.163.189	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 5.29.163.189	Block	12
149.78.193.136	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
5.29.163.189	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	6
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	4
213.57.178.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.1.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
213.57.178.72	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.29.237.139	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
46.19.86.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
58.64.181.66	Hong Kong	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
31.146.48.32	Georgia	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
213.8.204.75	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.73	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.29.55.3	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$60 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
149.88.192.103	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.183.128.217	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
62.114.109.141	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
31.146.48.32	Georgia	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
213.8.204.75	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
69.58.178.57	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
46.117.179.108	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
157.55.39.151	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/index-files/list1.xls	Block	1
79.183.128.217	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
62.114.146.155	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
31.168.149.54	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
109.65.58.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
46.118.114.111	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	1
199.30.24.69	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.183.128.217	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php	Block	1
65.55.210.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.202.59	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
79.182.152.201	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
80.178.157.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20978-he/dover.aspx&sa=u&ved=0ahukewivtqfs6_rkahwdliwkhffyb7gqfggmmae&usg=afqjcnfpecc5tshxnzefnkaohgjycbchiq	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.183.128.217	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1

02-16-2016-00:04:05 to 02-16-2016-01:04:05