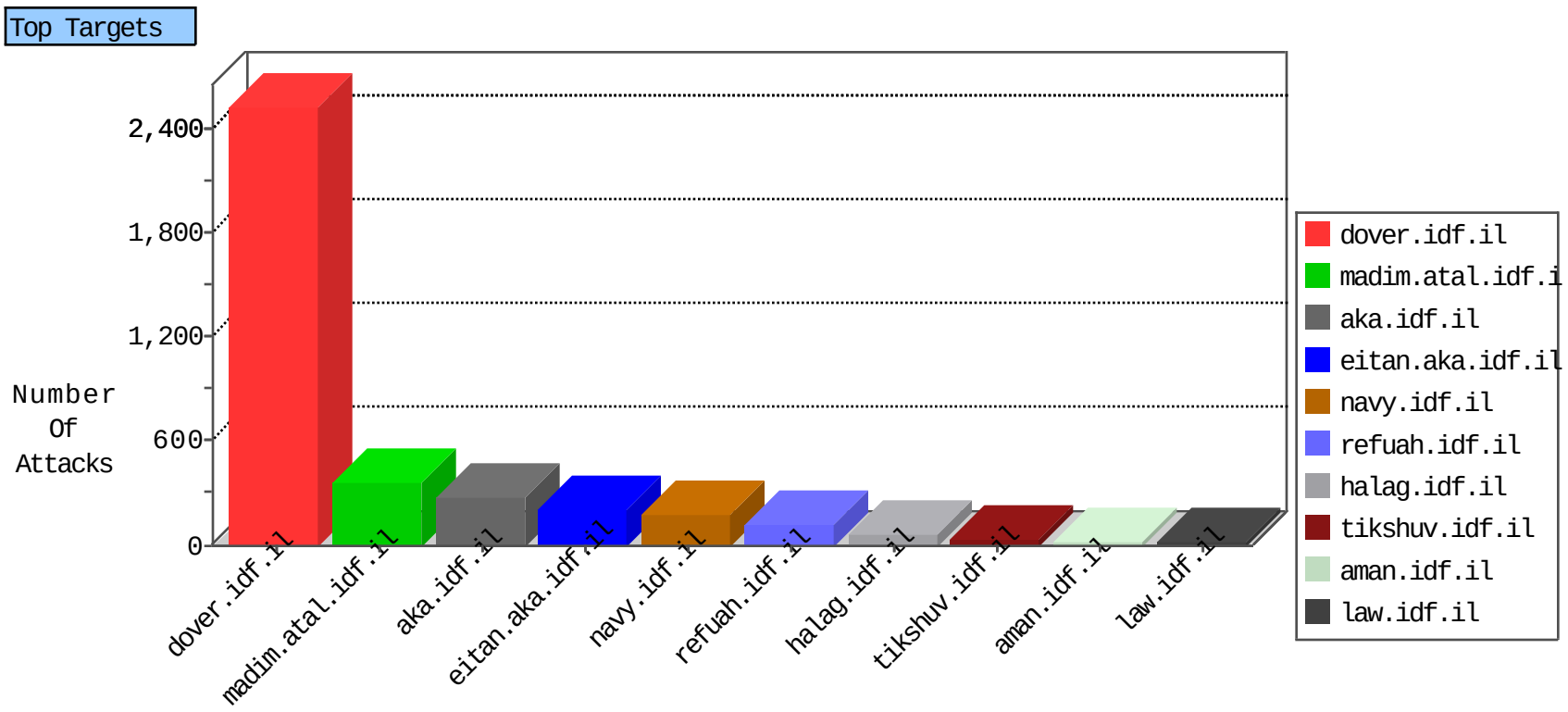
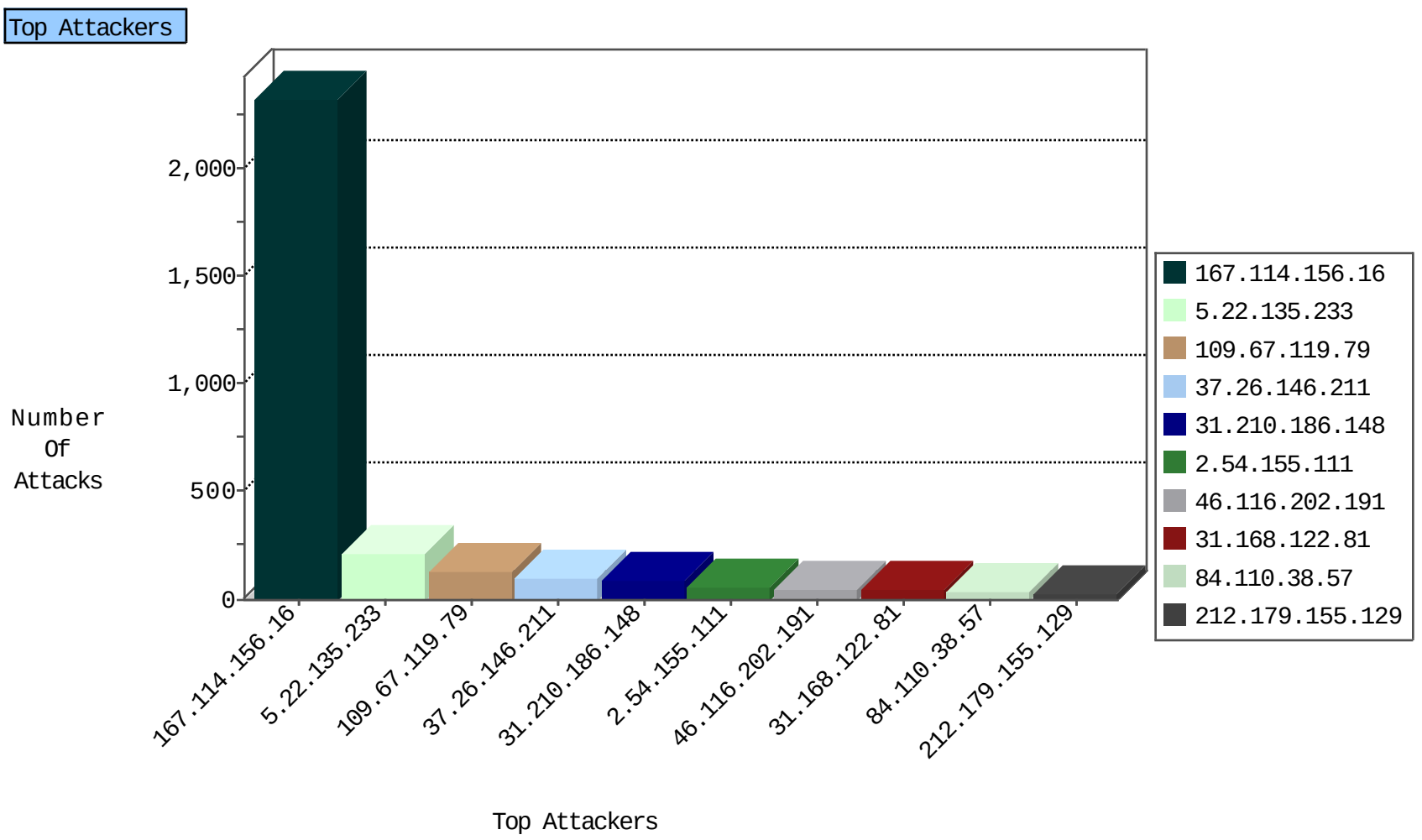
03-14-2016-22:04:08 to 03-14-2016-23:04:08

IDF Under Attack Daily Report





03-14-2016-22:04:08 to 03-14-2016-23:04:08

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	HTTP Page Flood Attack	forward	4805
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4031
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	40
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
213.159.209.5	Russian Federation	147.237.8.46	e.chinuch.idf.il	Invalid TCP Flags	drop	1
103.23.21.217	Indonesia	147.237.76.39	mobile.meitav.idf.il	Invalid L4 Header Length	drop	1

03-14-2016-22:04:08 to 03-14-2016-23:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.224.80	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	14
5.29.38.113	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
37.205.0.49	Turkey	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
61.135.189.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
64.31.44.6	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
69.204.195.101	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
85.64.49.108	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.204.195.101	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
93.180.64.135	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.204.195.101	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
217.132.56.209	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.204.195.101	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.204.195.101	United States	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Block	2

03-14-2016-22:04:08 to 03-14-2016-23:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
64.31.44.6	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
37.205.0.49	147.237.77.74	Turkey	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
37.26.146.211	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
40.121.62.231	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
5.160.14.250	147.237.76.39	Iran, Islamic Republic of	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
199.255.137.114	147.237.0.34	Belgium	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
199.255.137.114	147.237.0.34	Belgium	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
5.160.14.250	147.237.76.42	Iran, Islamic Republic of	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
5.160.14.250	147.237.76.30	Iran, Islamic Republic of	himush.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.195	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
199.255.137.114	147.237.0.34	Belgium	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
198.20.69.74	147.237.77.205	United States	prisha.idf.il	ET DROP Dshield Block Listed Source	1
149.78.154.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-14-2016-22:04:08 to 03-14-2016-23:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.119.79	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	132
31.210.186.148	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	63
46.116.202.191	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	52
31.168.122.81	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	51
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
212.179.155.129	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
197.116.222.58	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
217.128.3.15	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
31.210.186.148	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
2.54.155.111	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
46.19.86.31	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.155.111	Israel	147.237.76.86	navy.idf.il	SYN Attack		reject	13
84.110.38.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
37.26.149.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.3.144.29	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.246.136.201	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
197.96.66.125	South Africa	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
37.26.149.160	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	8
37.26.149.160	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
2.54.155.111	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
79.177.56.156	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.155.111	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.155.111	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.186	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.110.38.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.52	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.1.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.70	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.27	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.110.38.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.210.168.41	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.52	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.130.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.110.38.57	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.70	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.249	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.65.139	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.238.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.185.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.110.38.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.120.131.194	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	6
46.19.85.249	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.68.245.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.51	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.83.69	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.27	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.22.135.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	214
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	75
212.76.101.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.23.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
37.26.149.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
213.151.62.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.222.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.204.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.150.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.166.240.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.58.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.77.235.216	Romania	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
79.177.96.67	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
37.26.146.211	Israel	147.237.0.19	madim.atal.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.147.142	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
95.77.235.216	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
37.26.148.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.104.144	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
79.181.125.167	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
5.102.224.80	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/forums	Block	1
188.33.95.232	Poland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.65.188	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
46.19.85.66	Israel	147.237.76.86	navy.idf.il	Illegal HTTP Version __atuvs=56e71ee061222853000; __atssc=facebook%3B6	Block	1
84.108.237.80	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
207.241.229.32	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/general/general.aspx	Block	1
178.216.200.48	Poland	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
66.249.64.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
109.186.156.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
217.128.3.15	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.93.237.70	Norway	147.237.77.74	law.idf.il	PHP Attempt	Block	1
79.181.125.167	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
31.168.14.74	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
197.96.66.125	South Africa	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20638-he/idfgdover.aspx	Block	1
157.55.39.139	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdfצבא-ההצלה	Block	1
109.64.238.226	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.66	Israel	147.237.76.86	navy.idf.il	Malformed URL __atuvc=0	Block	1
212.45.44.1	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
84.111.233.104	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
184.71.156.194	Canada	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.125.167	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
109.186.156.205	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
46.19.85.2	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
223.206.21.149	Thailand	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.93.237.70	Norway	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
79.181.125.167	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.181.125.167	Block	1
31.168.122.81	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
157.55.39.181	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/drushim/misrot.aspx	Block	1