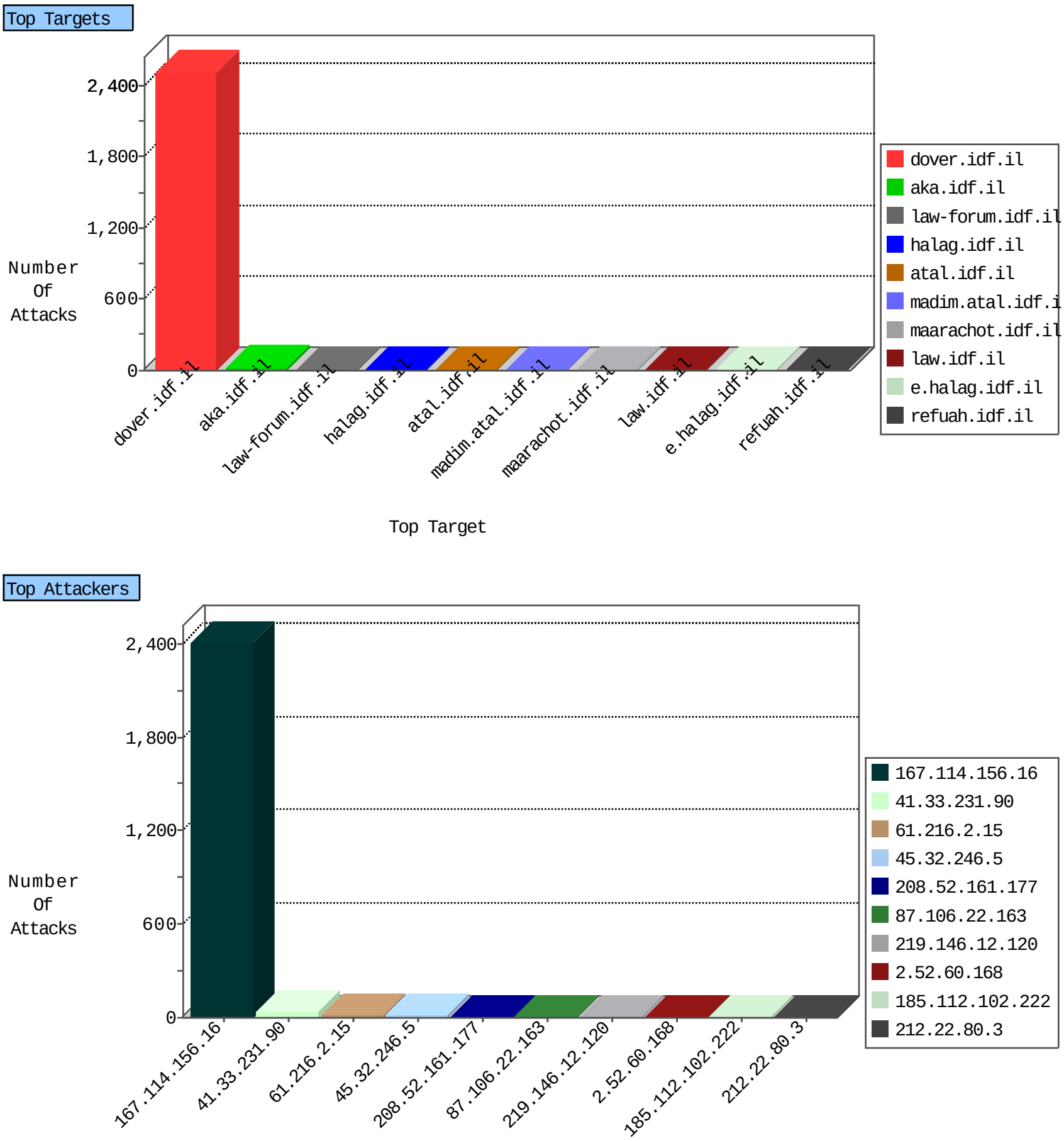
12-10-2015-03:04:03 to 12-10-2015-04:04:03

IDF Under Attack Daily Report



12-10-2015-03:04:03 to 12-10-2015-04:04:03

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	3331
45.32.246.5		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
66.249.64.50	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1

12-10-2015-03:04:03 to 12-10-2015-04:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-10-2015-03:04:03 to 12-10-2015-04:04:03

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	4
190.12.107.247	147.237.8.27	Argentina	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.112.102.222	147.237.77.61		e.cogat.idf.il	ET SCAN Potential SSH Scan	1
185.112.102.222	147.237.0.33		idf.il	ET SCAN Potential SSH Scan	1
166.63.125.149	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 3072	1
151.233.164.85	147.237.0.35	Iran, Islamic Republic of	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
219.146.12.120	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
96.94.72.226	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
219.146.12.120	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
219.146.12.120	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
189.220.57.168	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.112.102.222	147.237.72.217		e.idf.il	ET SCAN Potential SSH Scan	1
185.3.95.93	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
166.63.125.149	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
219.146.12.120	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
96.94.72.226	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
219.146.12.120	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
219.146.12.120	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
219.146.12.120	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1

12-10-2015-03:04:03 to 12-10-2015-04:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
45.32.246.5		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
61.216.2.15	Taiwan	147.237.77.19	law-forum.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
2.52.60.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.7.79.82	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.29.46.106	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
208.52.161.177	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
212.22.80.3	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
61.216.2.15	Taiwan	147.237.77.234	halag.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
46.19.85.95	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
213.57.247.100	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
212.22.80.3	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
61.216.2.15	Taiwan	147.237.77.19	law-forum.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
140.113.194.87	Taiwan	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
80.7.79.82	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.142.212.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.141	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
185.112.102.222		147.237.76.34	yohalan.idf.il	drop		drop	1
46.19.86.122	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.146	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
213.57.247.100	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.52.161.177	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
61.216.2.15	Taiwan	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.123	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.142	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
82.166.240.204	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
61.216.2.15	Taiwan	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.112.102.222		147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.182	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.78.6.226	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
139.196.104.39	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
208.52.161.177	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
61.216.2.15	Taiwan	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.123	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
45.32.246.5		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.144	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.65.9.237	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
61.216.2.15	Taiwan	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
208.52.161.177	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.227.69.163	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
149.78.6.226	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
139.196.104.39	China	147.237.76.34	yohalan.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.10.175	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	4
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
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	2
79.178.189.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
87.106.22.163	Germany	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/admin	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8769-he/refuah.aspx	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/main/main.asp	Block	1
95.108.132.166	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
46.121.142.55	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation ReturnUrl in my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
84.111.224.167	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catID in www.aka.idf.il/yohalan/home/home.asp	None	1
52.35.180.120	United States	147.237.77.233	atal.idf.il	NULL Character in Method	Block	1
109.64.131.189	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
87.106.22.163	Germany	147.237.77.170	maarachot.idf.il	Admin Blocking	Block	1
2.54.169.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
104.236.49.184		147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.m.my-kosher-kravi.idf.il/	Block	1
46.227.69.163	Sweden	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
87.106.22.163	Germany	147.237.77.74	law.idf.il	Admin Blocking	Block	1
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	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
61.216.2.15	Taiwan	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Method	Block	1
162.243.188.75	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on /	Block	1
87.106.22.163	Germany	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/admin	Block	1
40.77.167.16	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
77.125.108.229	Israel	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
207.46.13.38	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
52.35.180.120	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method	Block	1
87.106.22.163	Germany	147.237.77.74	law.idf.il	Multiple Admin Blocking from 87.106.22.163	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/3211.jpg	Block	1
61.216.2.15	Taiwan	147.237.77.234	halag.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
178.154.243.114	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
87.106.22.163	Germany	147.237.77.234	halag.idf.il	Multiple Admin Blocking from 87.106.22.163	Block	1
40.77.167.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/counter_term.php	Block	1
77.125.108.229	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/xmlrpc.php	Block	1
207.46.13.90	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/default.asp	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
52.35.180.120	United States	147.237.77.233	atal.idf.il	Multiple Illegal Byte Code Character in Method from 52.35.180.120	Block	1
87.106.22.163	Germany	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 87.106.22.163	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
185.3.95.93	United Kingdom	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /	Block	1
66.249.64.9	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/news/pages/kenessikum2010arbel.aspx	Block	1
87.106.22.163	Germany	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 87.106.22.163	Block	1
40.77.167.66	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
208.52.161.177	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /phpmyadmin/scripts/signon.php	Block	1