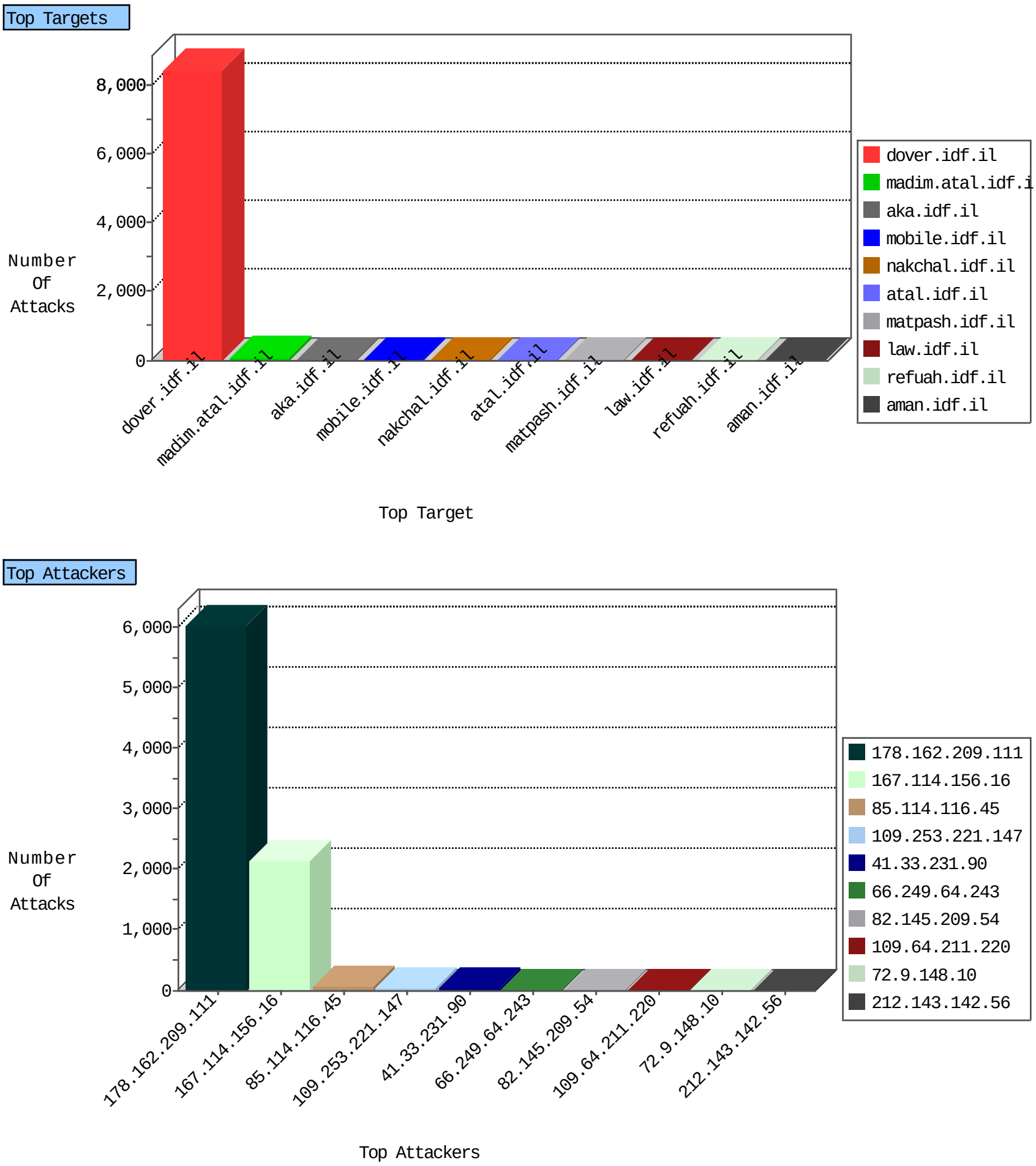
12-26-2015-00:04:07 to 12-26-2015-01:04:07

IDF Under Attack Daily Report



12-26-2015-00:04:07 to 12-26-2015-01:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
178.162.209.111	Germany	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4991
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3406
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	75
82.145.209.54	Europe	147.237.76.31	nakchal.idf.il	Block_Ip_Web_In	drop	13
66.249.64.243	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
178.162.209.111	Germany	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	3
114.113.126.4	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
41.233.27.224	Egypt	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

12-26-2015-00:04:07 to 12-26-2015-01:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-26-2015-00:04:07 to 12-26-2015-01:04:07

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	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
37.143.82.50	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
187.160.131.190	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
131.109.15.15	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
104.219.238.10	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.243	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
37.143.82.50	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
37.143.82.50	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -f -sS	1
131.109.15.15	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
131.109.15.15	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
73.17.14.46	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1

12-26-2015-00:04:07 to 12-26-2015-01:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.162.209.111	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5799
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	206
178.162.209.111	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	76
178.162.209.111	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	76
178.162.209.111	Germany	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	76
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
85.114.116.45	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
85.114.116.45	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
85.114.116.45	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
109.64.211.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
141.0.15.247	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
85.114.116.45	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.181.109.250	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
66.249.78.252	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.114.116.45	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
128.127.107.99	Netherlands	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5
85.114.116.45	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.178.150.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.247.36.71	Netherlands	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
91.200.12.137	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.30.24.192	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.137	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
84.228.22.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.153.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.154.227.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
185.3.146.205	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.142.156.67	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
79.179.52.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.26.180.86	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
109.65.35.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
185.106.92.33		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.66.139.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.233.27.224	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
41.140.48.74	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
41.250.68.33	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
46.19.85.242	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
154.109.133.81	Tunisia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
31.210.186.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
37.46.39.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.181	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.169.113	Israel	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
141.8.183.19	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.221.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
91.228.196.139	Poland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 91.228.196.139	Block	7
40.77.167.5	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 40.77.167.5	Block	5
207.46.13.183	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.183	Block	5
2.54.130.37	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	4
79.181.214.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.211.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.7.11.192	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
91.228.196.139	Poland	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
85.64.16.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.158.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
31.168.208.53	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
200.73.17.115	Chile	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
89.221.250.22	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
186.192.129.73	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
78.47.17.5	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.108	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/2/242.doc	Block	1
149.78.163.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
2.54.169.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.163.220.160	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
178.162.209.111	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/×©×§×•×¤×™×ª 14	Block	1
109.160.209.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
50.62.177.15	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
213.154.242.163	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.122.209.14	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
200.73.17.115	Chile	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
78.47.17.5	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
188.40.0.137	Germany	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.113	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
154.107.1.205	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
41.140.48.74	Morocco	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
207.46.13.183	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-8877-he/~/media/thriving/familyresources.ashx	Block	1
5.61.251.87	Netherlands	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
192.163.220.160	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
185.106.92.36		147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/×–×″	Block	1
54.229.65.238	Ireland	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
216.224.183.129	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
109.253.131.193	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	1
37.122.209.14	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	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
79.134.234.247	Iceland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
188.40.0.137	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19795-he/idfgdover.aspx	Block	1
154.109.133.81	Tunisia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1