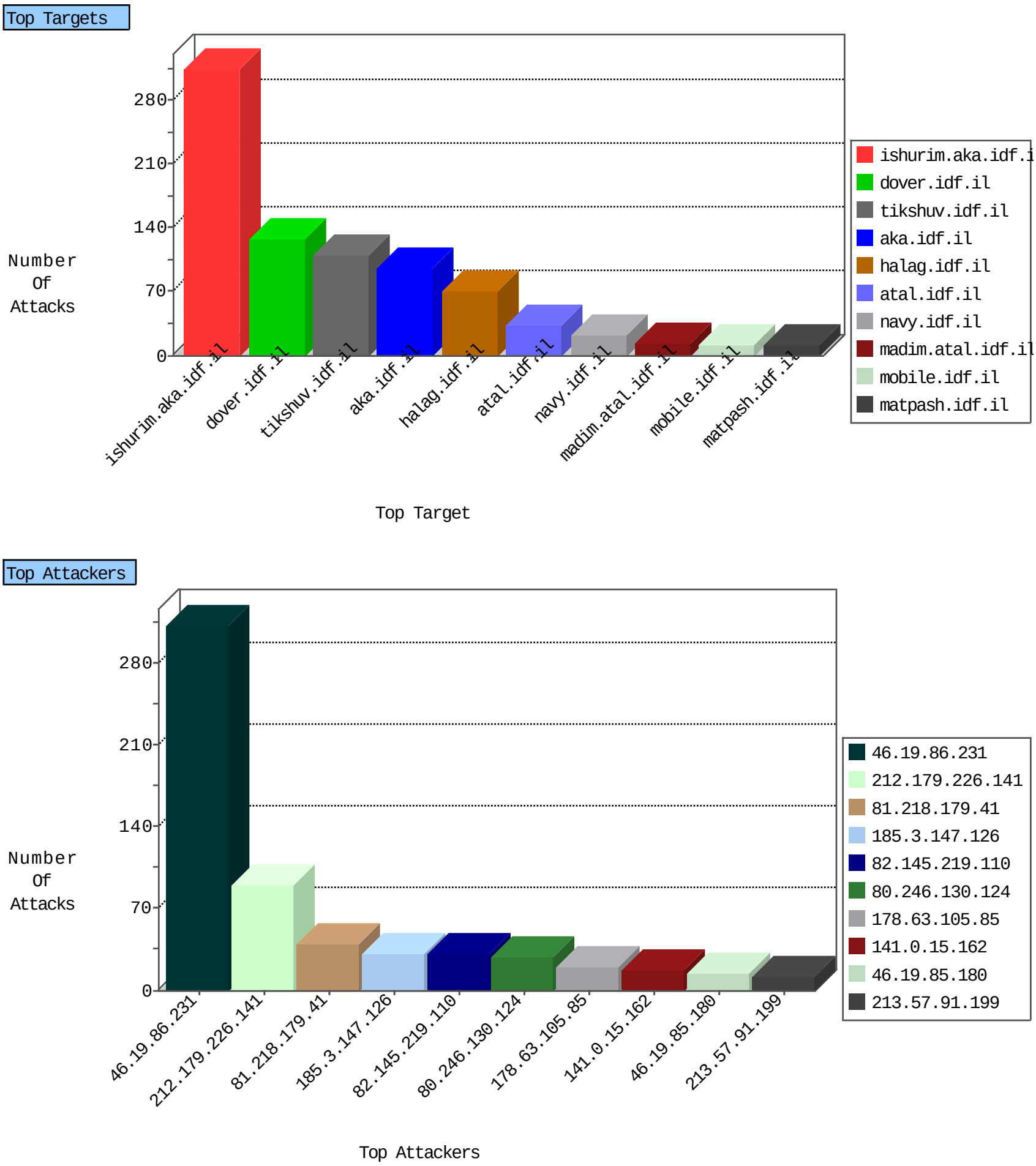
03-07-2016-00:04:01 to 03-07-2016-01:04:01

IDF Under Attack Daily Report



03-07-2016-00:04:01 to 03-07-2016-01:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.219.110	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	31
82.145.209.99	Europe	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	11
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
59.85.121.110	Japan	147.237.77.178	e.matpash.idf.il	Block_Udp_All_Nets	drop	1
85.14.165.7	France	147.237.76.198	e.yohalan.idf.il	JLM_Purple_Con_Limit_Http	drop	1
85.14.165.7	France	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Http	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

03-07-2016-00:04:01 to 03-07-2016-01:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.108	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
85.64.53.238	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
51.254.121.187	United Kingdom	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
79.176.48.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.254.121.187	United Kingdom	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-07-2016-00:04:01 to 03-07-2016-01:04:01

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
66.249.73.198	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
161.10.159.40	147.237.76.30	Colombia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.64	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
95.130.13.220	147.237.72.167	France	ishurim.aka.idf.i	ET SCAN Potential SSH Scan	1
61.240.144.66	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1

03-07-2016-00:04:01 to 03-07-2016-01:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.231	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	312
212.179.226.141	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
81.218.179.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
185.3.147.126	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
80.246.130.124	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
141.0.15.162	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
46.19.85.180	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
73.70.4.100	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
87.68.79.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.169	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.91.199	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.46.41.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.57.91.199	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
79.179.132.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.247.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.91.199	Israel	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	3
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	3
66.249.93.146	United States	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.192.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.27.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.193.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.42.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.120.188.65	Belarus	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.145.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	3
200.161.54.76	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
178.154.149.13	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	3
109.66.49.8	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	3
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	3
109.253.137.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
172.56.19.252	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
207.241.229.225	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	2
46.19.86.32	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
73.70.4.100	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.86.177	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.241.229.222	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.3.147.102	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.131.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.149.169	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence		monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
188.163.78.47	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.163.78.47	Block	3
64.71.32.19	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 64.71.32.19	Block	3
82.102.136.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
160.176.14.107		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 160.176.14.107	Block	2
5.28.157.125	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
68.180.230.240	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/319,	Block	1
185.3.147.251	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
37.26.146.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
151.252.97.204	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.154.201.150	United Kingdom	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
188.252.241.148	Croatia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
185.3.147.126	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.64.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
109.65.67.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.8.204.21	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
86.1.22.98	United Kingdom	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
79.178.175.53	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
160.176.14.107		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
37.237.142.122	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
95.154.201.150	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xyzzy	Block	1
82.102.136.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.3.147.251	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
141.212.122.129	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /x	Block	1
94.230.93.5	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
79.178.175.53	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/xmlrpc.php	Block	1
188.163.78.47	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
95.154.201.150	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
198.58.102.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
83.36.243.152	Spain	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.3.147.251	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
66.249.66.23	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1401-he/atal.aspx	Block	1
141.212.122.129	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to /x	Block	1
94.230.93.5	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
80.246.130.124	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
188.163.78.47	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/xmlrpc.php	Block	1
160.176.14.107		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/electricity	Block	1
64.71.32.19	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
108.26.217.218	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
204.79.180.196	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.14.165.7	France	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /	Block	1
66.249.66.33	United States	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
185.3.147.251	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
141.212.122.129	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /x	Block	1
95.154.201.150	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
81.218.179.41	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
188.252.241.148	Croatia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
64.71.32.31	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/test/wp-admin/	Block	1