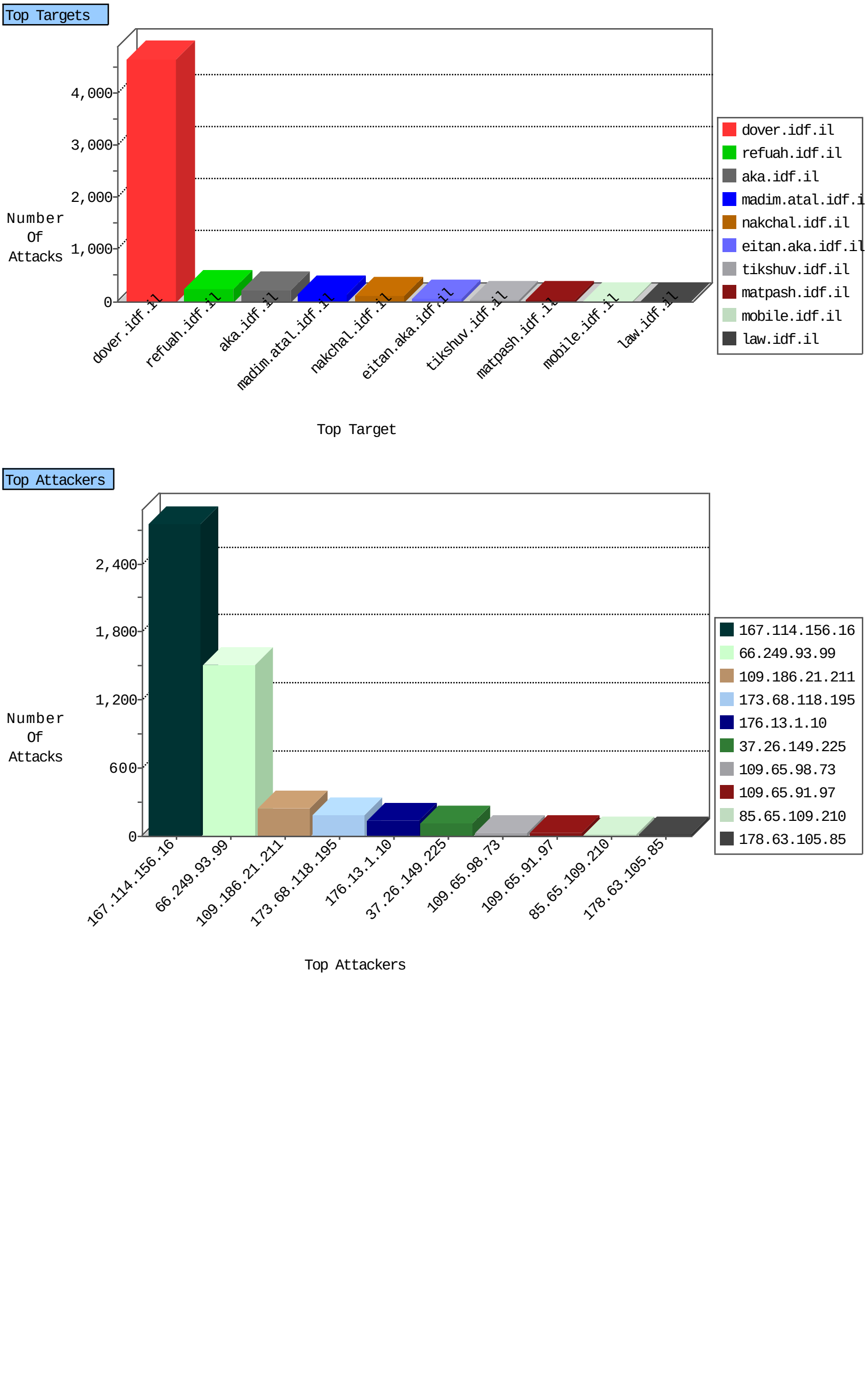
03-13-2016-22:04:04 to 03-13-2016-23:04:04

IDF Under Attack Daily Report



03-13-2016-22:04:04 to 03-13-2016-23:04:04

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	3918
5.22.129.78	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.181.134.55	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
78.152.21.90	Poland	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.206	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

03-13-2016-22:04:04 to 03-13-2016-23:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.82.80	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.177.235.118	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.178.204.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.147.169	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
176.9.131.69	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
84.111.162.192	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
65.55.210.99	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
94.23.214.33	France	147.237.77.216	dover.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
2.54.175.0	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
173.208.145.58	United States	147.237.76.31	nakchal.idf.il	0543: HTTP: php.cgi Access	Block	1
79.179.110.73	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-13-2016-22:04:04 to 03-13-2016-23:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.99	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1514
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
132.74.95.19	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
54.193.115.56	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
54.93.85.231	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
42.116.139.91	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
40.121.136.51	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
40.121.136.51	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
108.59.248.198	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
104.215.89.20	147.237.72.167	United States	ishurim.aka.idf.i	ET SCAN NMAP -sS window 1024	1
54.193.115.56	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
54.193.115.56	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
46.19.85.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
42.116.139.91	147.237.0.19	Vietnam	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.8.14	Cote D'Ivoire	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
40.121.136.51	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
40.117.92.242	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.215.89.20	147.237.72.167	United States	ishurim.aka.idf.i	ET SCAN NMAP -sS window 3072	1
77.44.73.85	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1

03-13-2016-22:04:04 to 03-13-2016-23:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.186.21.211	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	242
173.68.118.195	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	190
109.65.98.73	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.65.91.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
37.26.149.225	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	30
37.26.149.225	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	26
37.26.149.225	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	25
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
85.65.109.210	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
68.196.85.117	United States	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
37.26.149.225	Israel	147.237.76.31	nakchal.idf.il	SYN Attack		reject	13
132.66.236.200	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
37.142.186.11	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
37.142.186.11	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
79.179.48.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
197.46.119.39	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.146.202	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.246	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
79.182.12.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.67.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.136.214	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.33.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.225	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.142.171.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.173	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
31.210.187.94	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.181.111.212	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
197.46.119.39	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	5
213.8.204.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.149.225	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
93.173.139.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.117.227.101	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.142.228.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
108.61.123.86	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
149.88.85.232	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.109.64.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.117.227.101	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.149.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.180.176.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.102.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.46.119.39	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.177.128.160	Israel	147.237.72.166	aka.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
176.13.1.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	140
2.52.184.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.140.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
173.208.145.58	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 173.208.145.58	Block	3
46.19.86.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.64.145	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
185.88.24.137		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
40.77.167.11	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
37.26.148.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
41.238.223.48	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.186.21.211	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
79.181.118.38	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.181.118.38	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/0/size220x0/12380.jpg	Block	1
46.121.121.245	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.146.202	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
149.78.201.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.228.217.1	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.75.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/size100x0/2973.jpg	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
109.253.136.214	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.47.225	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.82.65.82	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/shared/usercontrols/headerupper/	Block	1
208.81.210.240	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
37.26.146.211	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.20	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
85.65.109.210	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
68.180.230.59	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakhal.idf.il/1073-he/nakhal.aspx	Block	1
186.55.181.230	Uruguay	147.237.77.74	law.idf.il	PHP Attempt	Block	1
132.66.236.200	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-7237-he/atal.aspx	Block	1
80.246.136.44	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.37.219	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	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
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
73.182.247.27	United States	147.237.77.176	matpash.idf.il	Multiple NULL Character in Method from 73.182.247.27	Block	1
186.55.181.230	Uruguay	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
141.212.122.64	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /x	Block	1
8.37.230.115	Anonymous Proxy	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.108.58.29	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/size100x0/3295.jpg	Block	1
217.69.133.243	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
37.58.59.88	Germany	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
93.173.139.41	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
73.182.247.27	United States	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
186.204.169.246	Brazil	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.168.118.88	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 31.168.118.88	Block	1
141.212.122.64	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to /x	Block	1
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/3142.jpg	Block	1
37.157.143.2	Bulgaria	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.32.179.65	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1