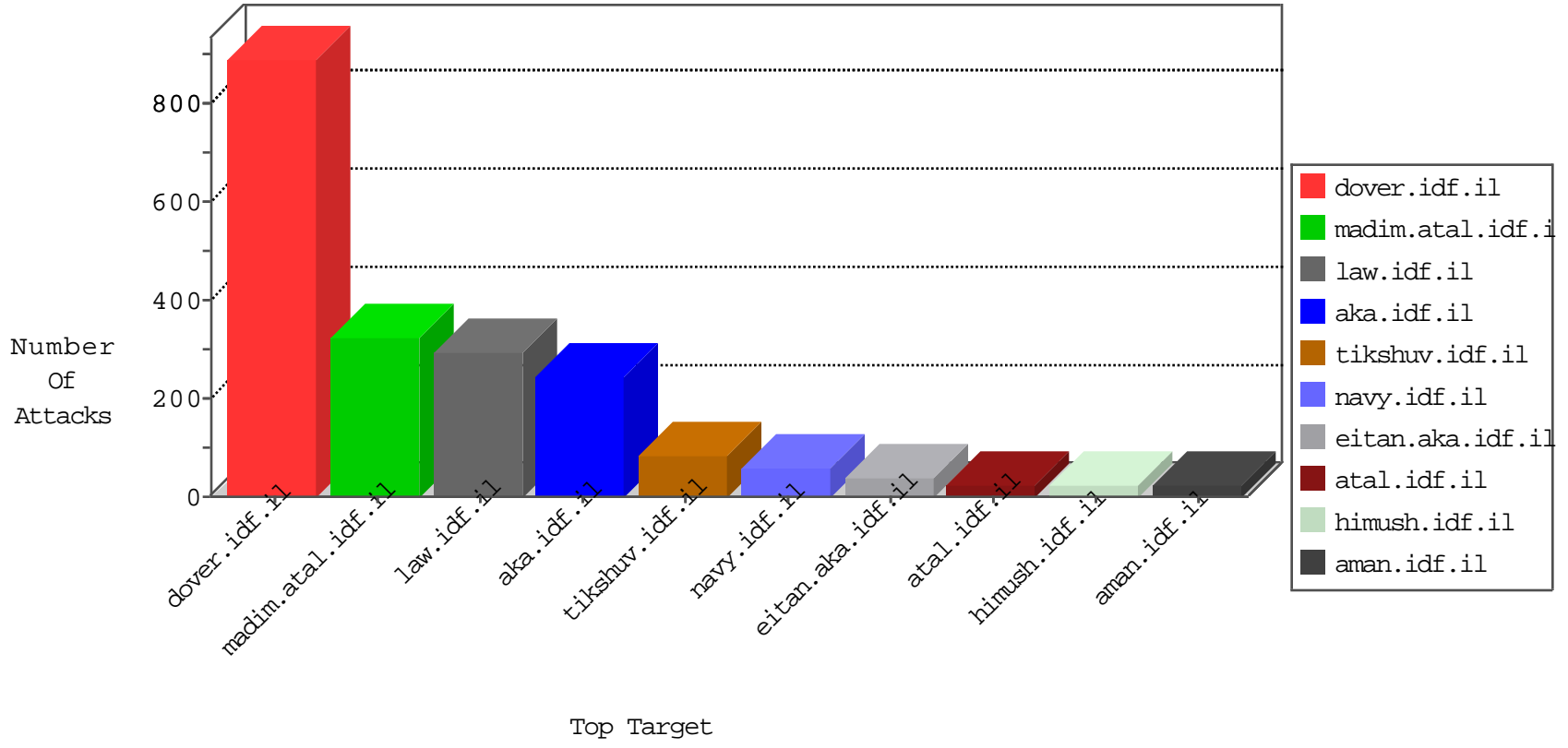


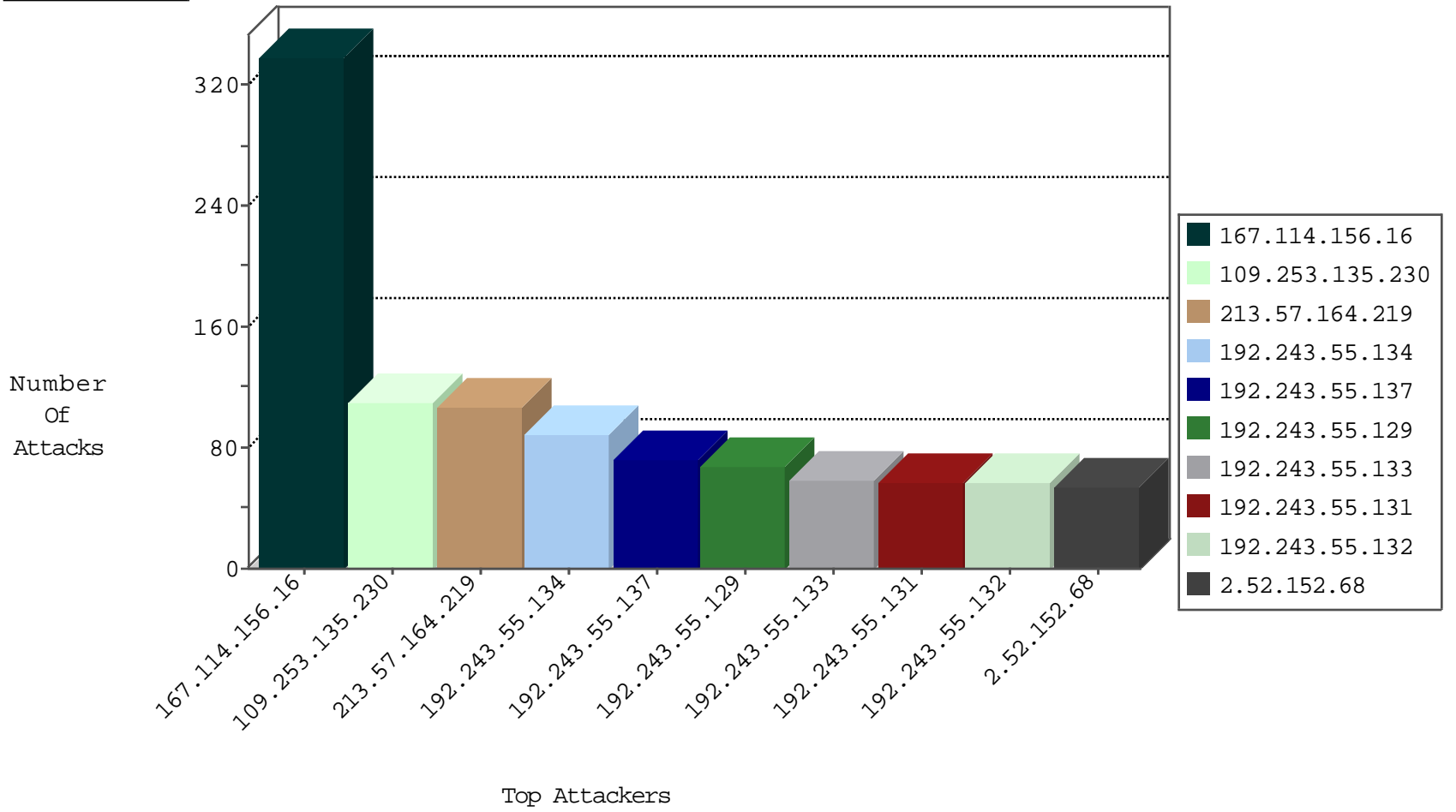
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	2166
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
159.122.254.192	Netherlands	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
198.20.69.98	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1
66.112.192.66	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.207	Netherlands	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
71.6.33.147	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.171.86	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
5.29.120.176	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
176.13.12.107	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
176.13.20.138	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
108.59.8.70	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.93.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.52.7.151	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.85.140	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.65.30	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
37.187.94.50	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
37.187.94.118	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
37.187.95.18	France	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
66.249.93.125	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.139.40.244	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
199.203.215.1	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.77.243	Sweden	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
149.88.248.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.164.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.71.22.133	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.57.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
62.90.100.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.231.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.152.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.124.35.115	147.237.8.24	Nicaragua	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
109.253.145.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.189.26.18	147.237.0.35	Austria	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
89.138.87.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.50	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
218.57.11.7	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
5.29.71.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
132.64.177.72	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
2.54.178.147	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
176.13.9.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.52.152.68	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
66.249.93.117	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	13
66.249.93.121	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	13
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
95.86.105.233	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.52.152.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
212.179.213.153	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
109.253.135.230	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
109.253.136.136	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
109.253.136.136	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.143.169.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
109.253.156.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
23.242.247.235	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.132	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.16	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.253.135.230	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.179.213.153	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.134	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.164.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
109.253.135.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	92
176.13.8.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	39
109.64.218.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
2.54.171.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
80.246.136.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.85.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
2.54.30.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.176.17.161	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 79.176.17.161	Block	3
146.159.132.2	Switzerland	147.237.77.176	matpash.idf.il	Parameter Type Violation SearchText in www.cogat.idf.il/938-en/cogat.aspx	Block	2
46.19.85.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
40.77.167.82	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
94.230.93.60	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/asp/personalentrance.asp	Block	1
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
37.26.148.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
132.64.177.72	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter r in www.eitan.aka.idf.il/templates/opcontactus/govcaptchaimage.axd	None	1
79.181.194.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.218.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Parameter Type Violation on madim.atal.idf.il/mobile/1088-he/meretz.aspx parameter ct100\$ContentPlaceHolder1\$txtMobile	Block	1
77.125.12.177	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
207.46.13.87	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/giyus/qanda/default.asp	None	1
37.26.148.213	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.133.106	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.115.130.253	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/4/109754.pdf	Block	1
2.54.44.8	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
213.57.37.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.46.38.14	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
147.236.38.135	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
46.19.86.27	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.19.86.27	Block	1
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19122-en/dover.aspx http://startowy.com/dodajlink.html	Block	1
79.176.17.161	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/7/size338x0/1877.jpg	Block	1
40.77.167.2	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/home/default.aspx	Block	1
2.49.15.175	United Arab Emirates	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
173.247.228.10	United States	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
94.230.93.57	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
37.26.147.199	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
109.253.135.230	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtMobile in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
79.181.96.11	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/6/486.jpg	Block	1
2.49.15.175	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
173.247.228.10	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1