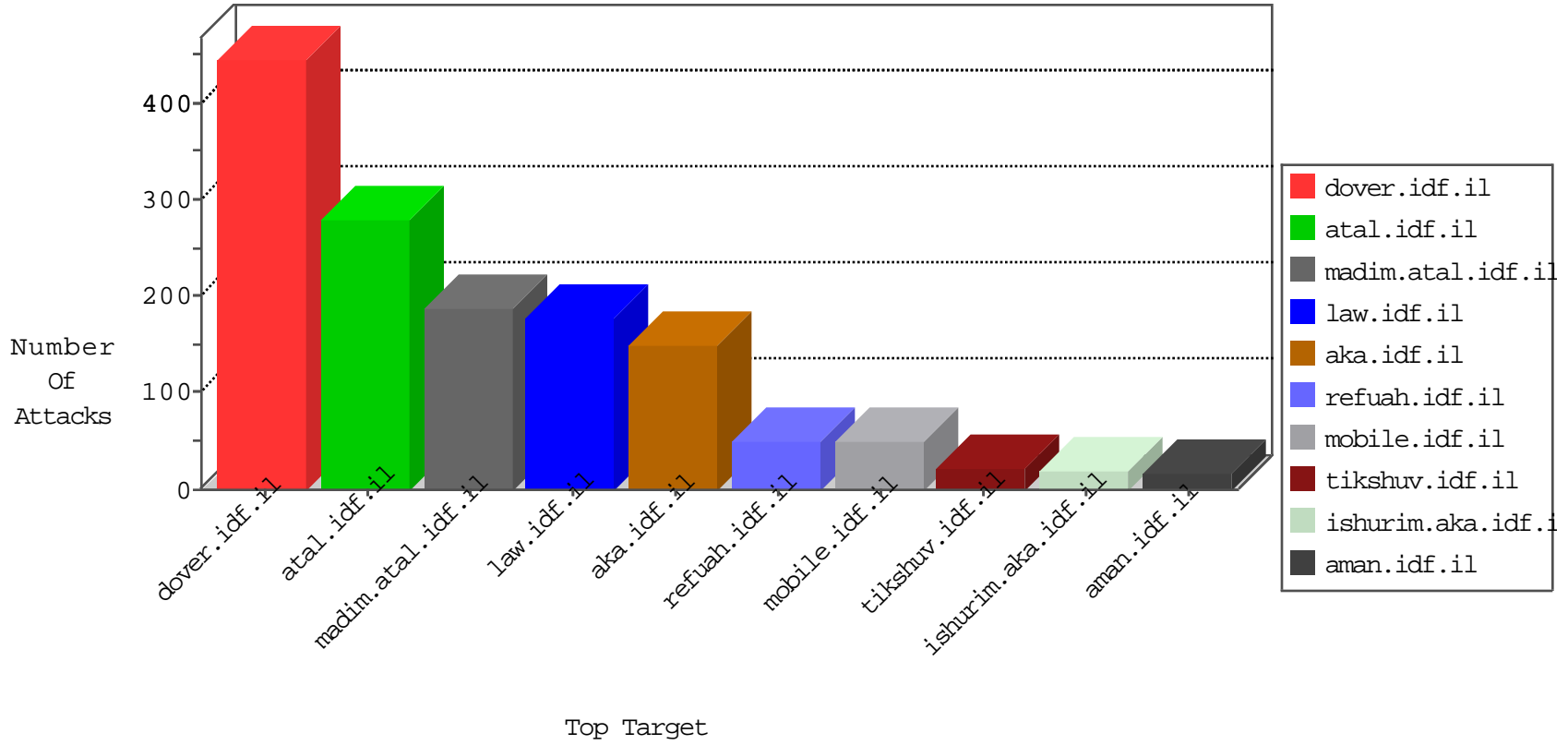


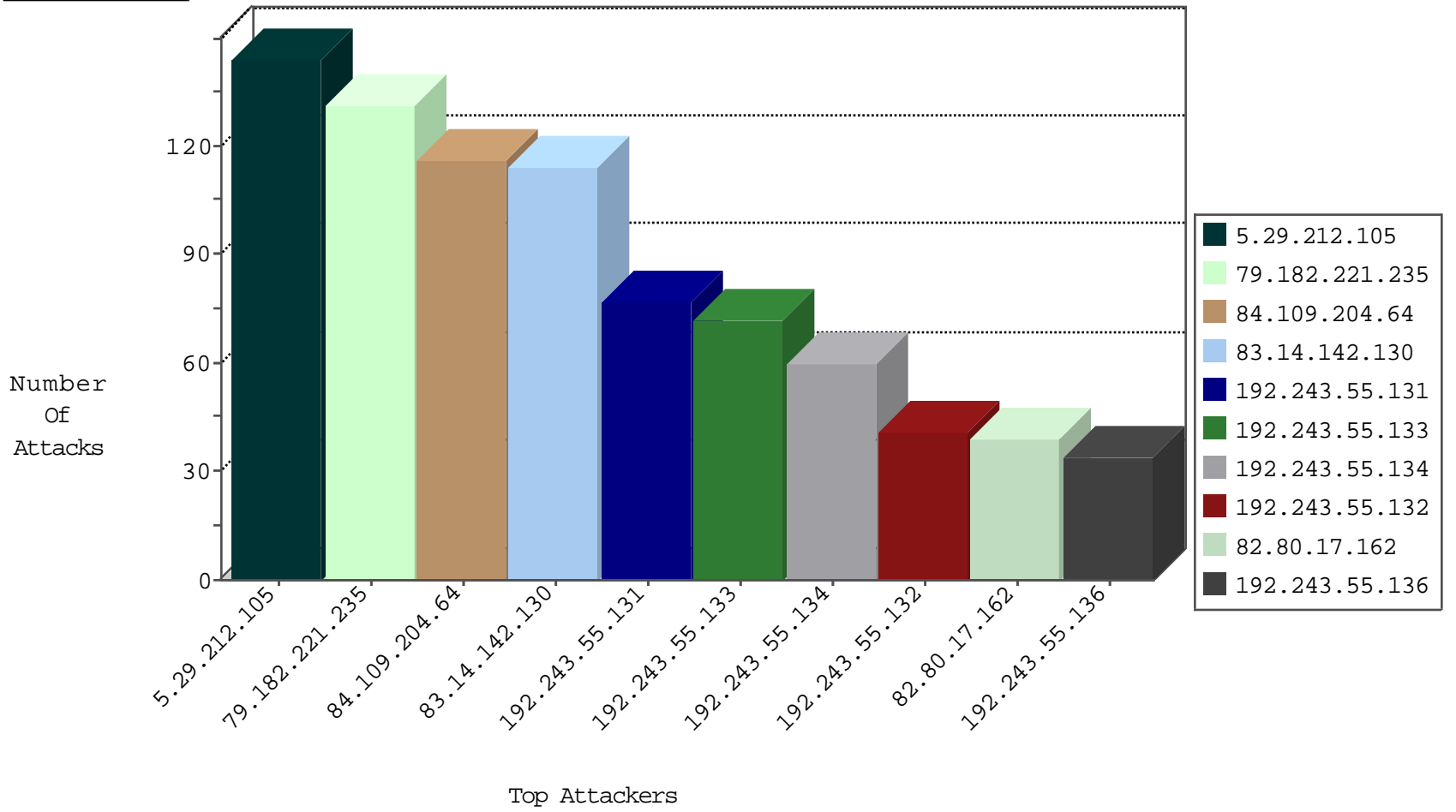
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.198	United States	147.237.77.243	mobile.idf.il	TCP Scan (vertical)	drop	183
79.182.134.79	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	30
82.145.222.24	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
204.42.253.2	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	2
49.151.33.169	Philippines	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
85.10.203.133	Germany	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
85.10.203.133	Germany	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
85.10.203.133	Germany	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.74	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
85.10.203.133	Germany	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.114	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
85.10.203.133	Germany	147.237.77.176	matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.239	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.4.23	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
87.68.251.254	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.65.36.9	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
213.8.204.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
212.129.26.132	France	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

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
198.180.198.185	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
222.186.42.206	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
202.112.51.113	147.237.76.201	China	e.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
198.180.198.185	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -f -sS	1
62.210.69.71	147.237.8.50	France	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
208.80.155.214	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.29.212.105	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	139
84.109.204.64	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	111
83.14.142.130	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
83.14.142.130	Poland	147.237.77.216	dover.idf.il	drop	SAM rule	drop	57
82.80.17.162	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
100.127.18.162		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.55.184.206	Switzerland	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.131	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	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
46.19.86.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.116.89.158	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.201	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
192.243.55.132	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	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.64.80.50	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
2.54.36.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.152	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.250.46.99	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.1.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
88.161.117.91	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.182.221.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.164.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.156.123	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.175.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.131	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
79.180.231.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.221.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
149.78.22.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
2.54.129.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.120.147.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
87.68.240.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.67.3.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
37.115.184.42	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	4
85.250.46.99	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	4
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.118.230.187	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi/	Block	3
77.126.69.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.119.122.177	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/mazi/	Block	3
46.19.85.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.222.252	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/registrationwizard/	Block	2
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.178.39.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
131.253.25.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.178.39.37	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.39.37	Block	2
2.54.49.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.41	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/	Block	1
180.76.15.153	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Malformed URL `1¼	Block	1
31.168.21.81	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.38	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/page.asp	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Distributed Malformed URL	Block	1
66.249.66.69	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/01092010ramtakhevron.aspx	Block	1
40.77.167.92	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.39.58	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.58	Block	1
5.22.135.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishurim.	Block	1
213.55.184.206	Switzerland	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.99.32.3		147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Unknown HTTP Request Method KŠYF' in URL `1¼	Block	1
109.253.206.86	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
207.241.229.224	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
66.249.66.75	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/pages/kenes2009.aspx	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method	Block	1
5.29.212.105	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Distributed Abnormally Long Request	Block	1
37.142.64.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/ain/giyus	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1381-he/dover.aspx	Block	1
82.80.17.162	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
66.249.75.157	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1892	Block	1
174.129.237.157	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
46.19.85.177	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Illegal Byte Code Character in Method KŠYF'	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1