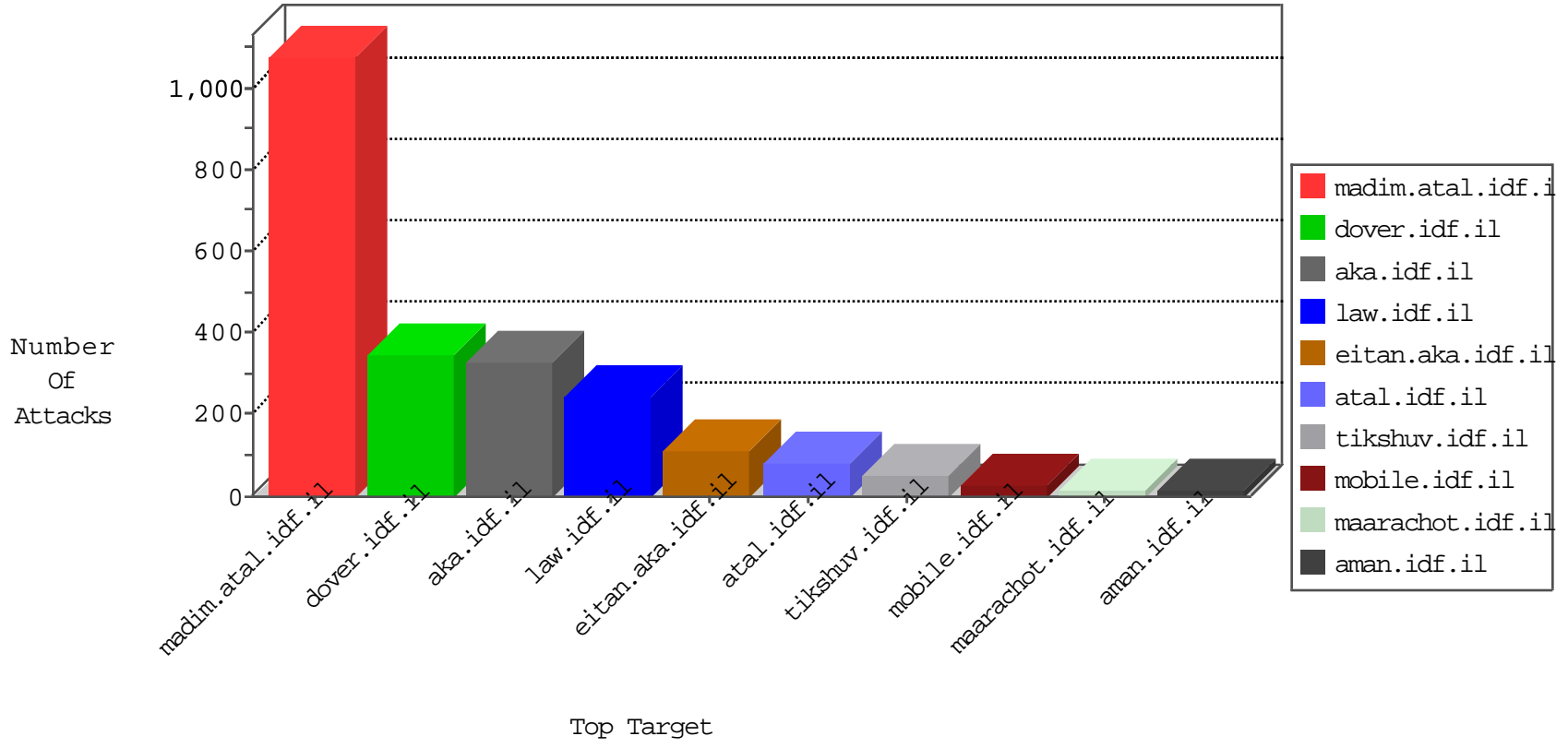


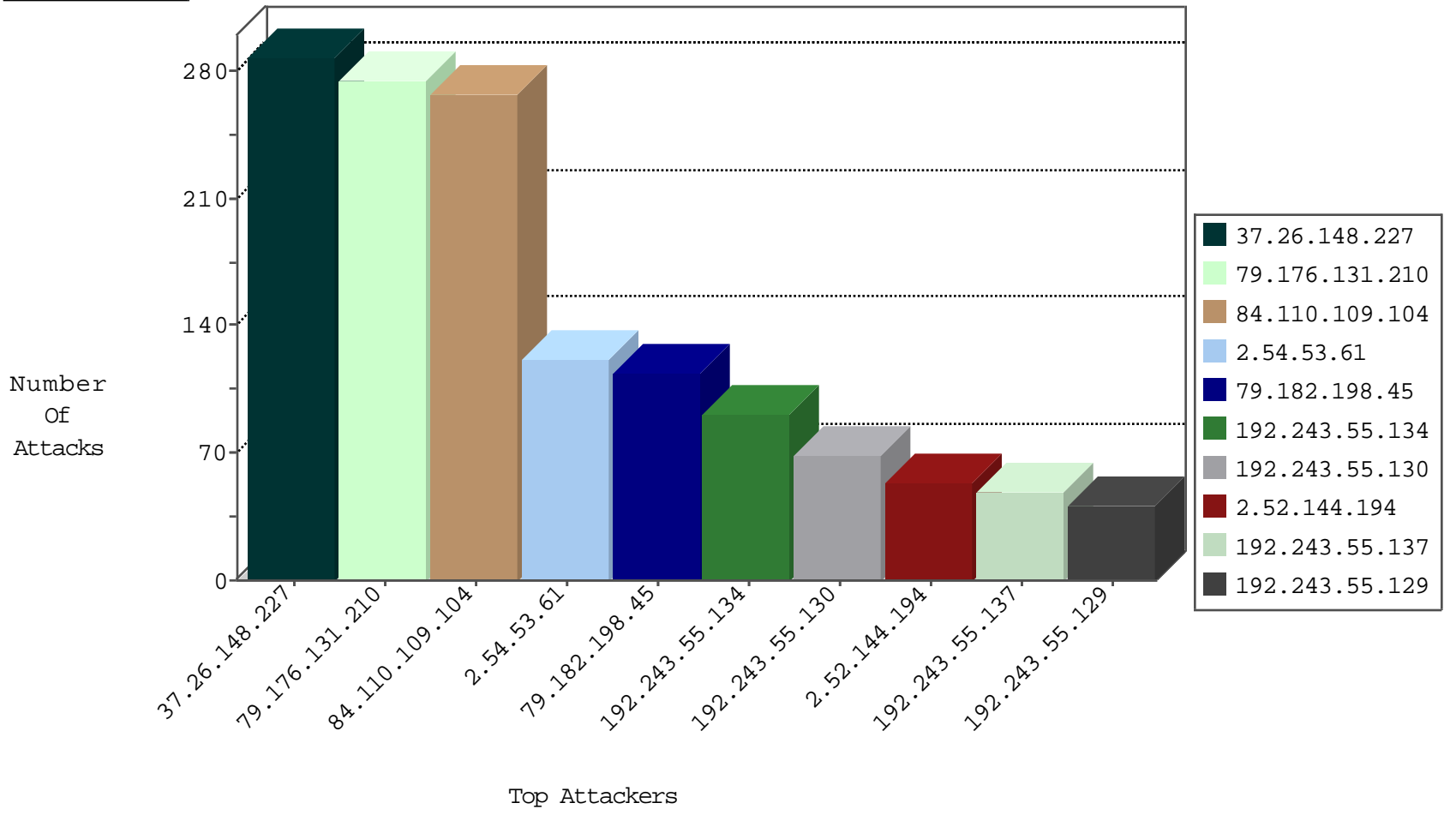
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.199.124.85	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
173.199.124.85	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.81.86	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	13
89.139.147.59	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
177.185.194.47	Brazil	147.237.77.74	law.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
64.87.23.55	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.194.47	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
46.117.156.218	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
195.154.200.93	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000103: HTTP: User Agent Sogou+web+spider	Block	1
178.63.18.196	Germany	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
115.124.70.145	Indonesia	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
188.165.15.224	France	147.237.77.216	dover.idf.il	C1000228: HTTP: AhrefBot crawler	Block	1
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
177.185.194.47	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	10
64.87.23.55	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
37.26.148.227	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.0.35	Turkey	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
218.201.61.82	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.0.35	Turkey	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
91.216.3.106	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
218.201.61.82	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
218.201.61.82	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.144.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
84.108.58.128	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
109.64.11.136	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
79.179.146.120	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	19
79.179.146.120	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
5.28.154.45	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.134	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
192.243.55.137	Dominica	147.237.77.74	law.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	Invalid ACK number	monitor	10
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
188.120.154.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.117.156.218	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
192.243.55.134	Dominica	147.237.77.216	dover.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	Bad TCP sequence	Invalid ACK number	alert	8
46.120.249.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
192.243.55.137	Dominica	147.237.77.74	law.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	Invalid ACK number	monitor	7
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
188.120.148.165	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
85.65.144.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
37.26.148.227	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
5.102.241.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.128.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.153.148	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.112.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.148.227	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		alert	6
46.19.85.232	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.142.87	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.132	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.121.81.86	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.19.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.232	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.227	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	6
109.253.210.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.230.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.232	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.151.218	Israel	147.237.76.86	navy.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	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	234
84.110.109.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	152
79.176.131.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	142
79.176.131.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
84.110.109.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	79
79.182.198.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
2.54.53.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
79.182.198.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	43
2.54.53.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
79.176.131.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	26
37.26.148.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
2.54.53.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	18
84.110.110.107	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
84.110.109.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	4
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
17.138.56.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templatecontrols/generic/	Block	3
5.29.160.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.81.36.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl100\$ctl100\$cphMain\$TochenPlaceHolder\$ctl113\$ctl101\$ctl103\$cblQuestion\$7 in www.aka.idf.il/main/gyius/questionnaire.aspx	None	2
93.173.135.246	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl100\$ctl100\$cphMain\$TochenPlaceHolder\$ctl113\$ctl101\$ctl103\$cblQuestion\$8 5 in www.aka.idf.il/main/gyius/questionnaire.aspx	None	2
84.94.209.172	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyius/controls/atuda/Å	Block	2
176.106.230.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl100\$ctl100\$cphMain\$TochenPlaceHolder\$ctl113\$ctl101\$ctl103\$cblQuestion\$9 0 in www.aka.idf.il/main/gyius/questionnaire.aspx	None	2
37.26.148.227	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl100\$ContentPlaceHolder1\$txtCity in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
37.26.147.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.50	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
87.71.31.161	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 87.71.31.161	Block	1
173.252.121.116	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.179.146.120	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
116.75.72.23	India	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
109.64.106.129	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl100\$ctl100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/gyius/atuda/asmachta.aspx	None	1
204.79.180.91	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.71.31.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
188.120.154.138	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.51.125	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
149.88.111.32	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.130.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
77.75.77.95	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/31/	Block	1
204.79.180.187	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.120.22.136	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
192.243.55.138	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
8.37.71.69	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/&usg=alkjrhh2auth98ij1a95g6tdpdp7qgybyg	Block	1
176.106.230.44	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl100\$ctl100\$cphMain\$TochenPlaceHolder\$ctl113\$ctl101\$ctl103\$cblQuestion\$1 1 in www.aka.idf.il/main/gyius/questionnaire.aspx	None	1
79.180.125.48	Israel	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
116.75.72.23	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
109.65.201.179	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
204.79.180.100	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.71.31.161	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
192.99.101.171	Canada	147.237.77.216	dover.idf.il	Multiple signatures from 192.99.101.171	Block	1