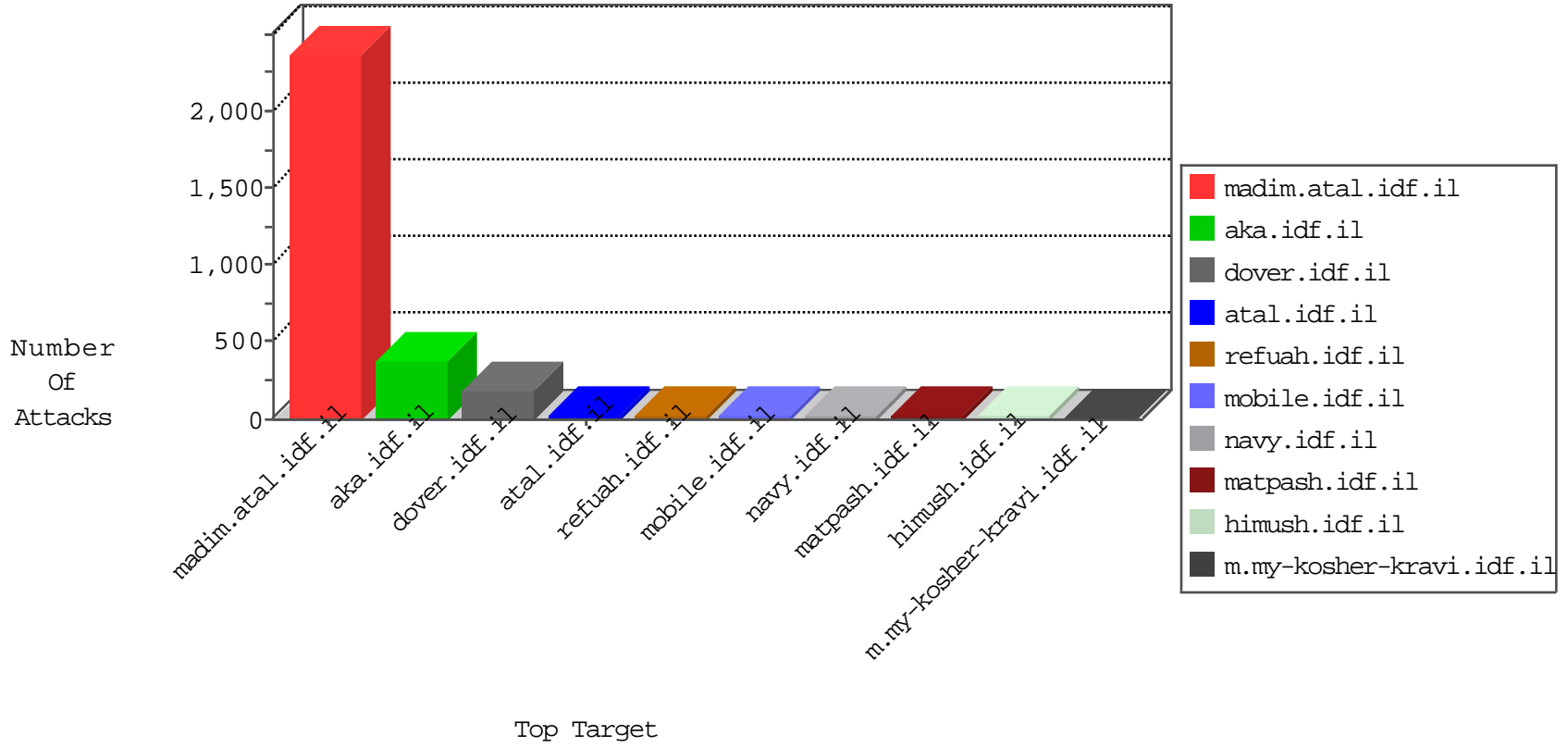


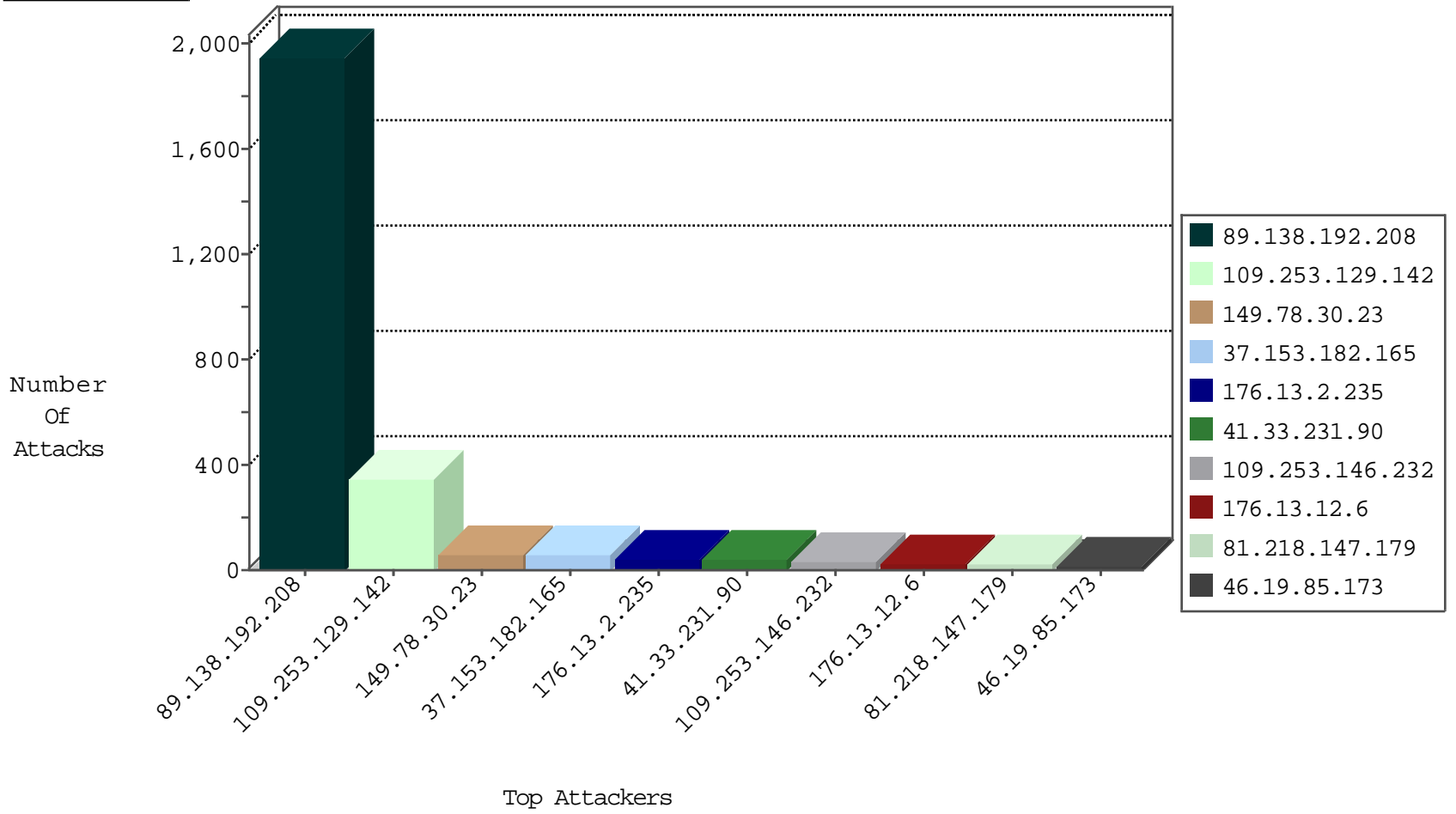
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.136.152	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
74.91.28.59	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
103.21.58.191	India	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
23.91.70.51	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
45.63.97.227		147.237.77.74	law.idf.il	C041: HTTP: Access to - index.php?option=com_jce	Block	1
89.38.209.50	Romania	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
103.21.58.191	147.237.77.233	India	atal.idf.il	SQL Injection - Select From	3
23.91.70.51	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
89.38.209.50	147.237.77.74	Romania	law.idf.il	SQL Injection - Select From	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
109.67.149.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.33.33	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.76.125.229	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
120.24.72.25	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
113.107.169.162	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.182.27.248	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.21.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.61.143.147	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
117.179.120.37	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
149.78.30.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
109.253.146.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
37.153.182.165	Romania	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
37.153.182.165	Romania	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	26
149.78.30.23	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
176.13.12.6	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
81.218.147.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
77.125.78.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.173	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.86.252	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
85.130.206.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.225.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
207.141.36.226	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
149.78.30.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
185.3.144.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.146.148	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
45.55.196.106		147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
109.64.155.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.193.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.175.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.169.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.6.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.192.208	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.116.52.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.138.192.208	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
207.141.36.226	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.249.78.177	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
93.172.21.68	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.182.220.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.140.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.97.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
217.132.31.74	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.17.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.186.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.216.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.203.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.49.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.43.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.194.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.33.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.153.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.147.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-09-2016-22:04:08 to 02-09-2016-23:04:08

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.54.166	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.203.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.254.150	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.176.191	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
89.138.192.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1202
89.138.192.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	569
109.253.129.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	238
89.138.192.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	168
109.253.129.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
176.13.2.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
85.250.89.100	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	7
79.170.44.111	United Kingdom	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.170.44.111	Block	5
104.131.214.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 104.131.214.72	Block	4
217.132.57.89	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 217.132.57.89	Block	3
176.13.19.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.3.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.116.12.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.129.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	3
46.117.124.182	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
80.246.137.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.169.63	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
109.253.158.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.87.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
217.132.57.89	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
109.253.200.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.129.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
65.132.59.34	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1283-en/dover.aspx	Block	2
46.117.124.182	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.117.124.182	Block	2
87.69.119.138	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
45.55.196.106		147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 45.55.196.106	Block	2
85.65.117.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatgquantity.aspx	Block	2
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.250.79.124	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.250.79.124	Block	1
46.121.88.224	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cphMain\$TochenPlaceHolder\$ctl113\$ctl101\$ctl103\$cb1Questi on\$78 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
217.126.64.131	Spain	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 217.126.64.131	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
109.67.117.87	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover	Block	1
85.250.79.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/default	Block	1
185.65.252.128	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
50.116.30.23	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
84.108.248.31	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
217.126.64.131	Spain	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
176.13.3.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	1
66.249.69.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.asp	Block	1
46.116.52.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.142	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.170.44.111	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
141.212.122.177	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/	Block	1
40.77.167.80	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/sip_storage/files/5/2495.jpg	Block	1
93.172.172.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ctl00\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/gyus/atuda/asmachta.aspx	None	1
84.111.125.240	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ctl00\$cphMain\$TochenPlaceHolder\$passwordUpdate\$hiddenUpdatePassword in www.aka.idf.il/main/gyus/faq.aspx	None	1
217.126.64.131	Spain	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
176.13.6.47	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.177	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/1028-en/eitan.aspx	None	1