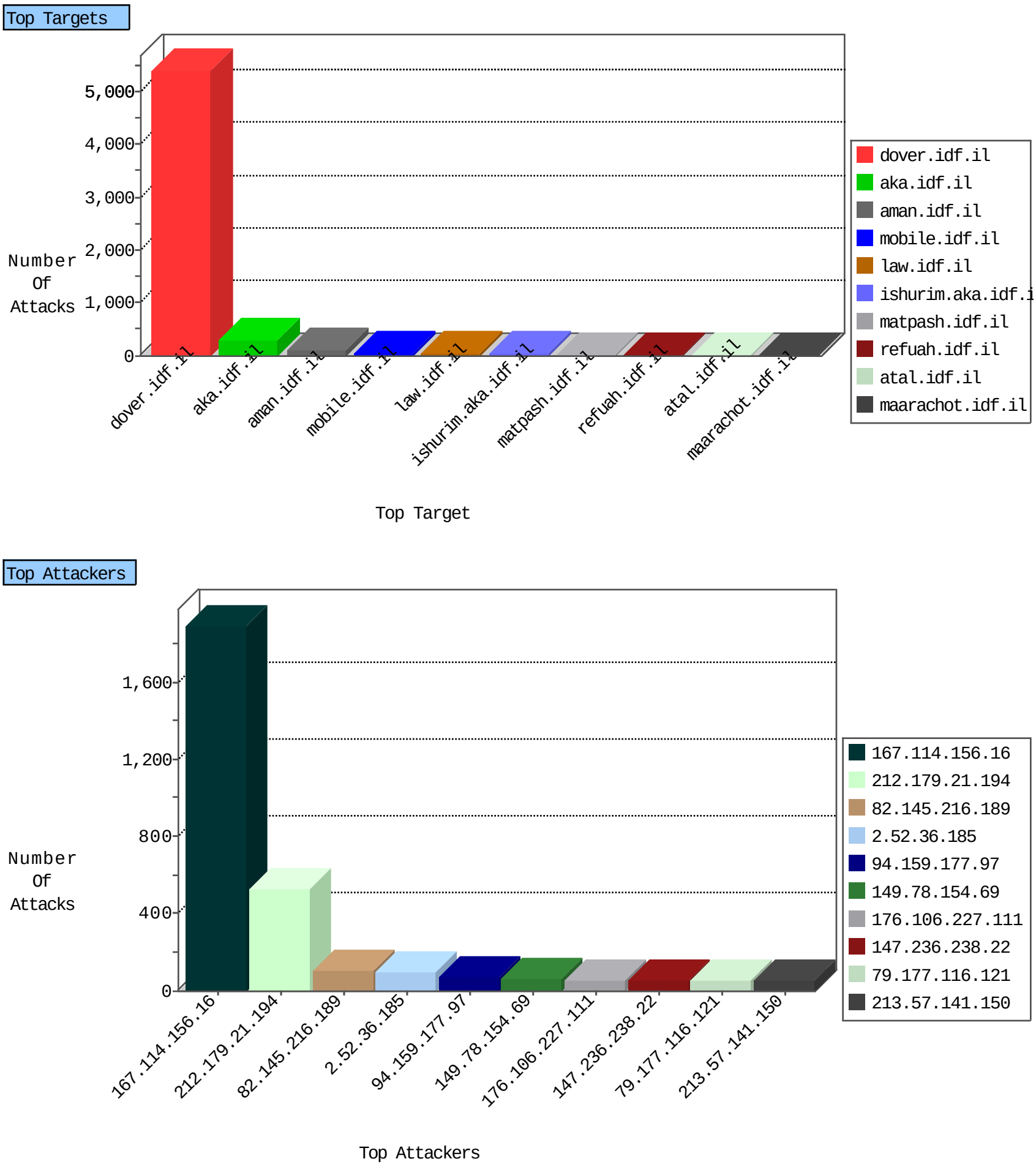
11-04-2015-10:04:00 to 11-04-2015-11:04:00

IDF Under Attack Daily Report



11-04-2015-10:04:00 to 11-04-2015-11:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.79.43	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7900
66.249.69.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4328
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3090
66.249.67.210	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2194
68.180.228.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2060
66.249.67.235	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1809
66.249.69.26	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1685
66.249.67.73	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1006
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	890
82.145.216.189	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	781
66.249.67.122	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	357
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	239
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	114
176.12.149.228	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	40
213.151.38.107	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	20
132.74.56.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
183.56.172.222	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	11
217.194.194.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
147.236.238.22	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
66.249.67.194	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	9
79.177.116.121	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
194.150.168.95	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
176.12.149.228	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
66.249.67.227	United States	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	6
89.138.222.65	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.106.227.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
109.67.206.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
194.150.168.95	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.162	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
80.246.139.90	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.52.12.76	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
66.249.79.45	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3
37.26.147.244	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
5.22.134.240	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
185.22.32.15	Lebanon	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
79.176.53.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.26.148.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
5.28.189.69	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
192.116.167.41	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
66.249.67.13	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2
176.228.190.5	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
81.89.96.89	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
78.186.62.98	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
37.26.148.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2

11-04-2015-10:04:00 to 11-04-2015-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.251.252	Israel	147.237.77.176	matpash.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
198.20.69.74	United States	147.237.76.38	e.e.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

11-04-2015-10:04:00 to 11-04-2015-11:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.52.36.185	147.237.72.156	Israel	aman.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	42
82.80.176.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.176.127.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.125.82.246	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.11.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.76.38	United States	e.e.meitav.idf.il	ET DROP Dshield Block Listed Source	1
176.13.0.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
111.93.198.54	147.237.77.234	India	halag.idf.il	ET SCAN NMAP -sS window 4096	1
79.182.27.243	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.197.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.79.41	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
213.57.204.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.76.34	Sweden	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.151.149	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-04-2015-10:04:00 to 11-04-2015-11:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	520
82.145.216.189	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	101
94.159.177.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
176.106.227.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
2.52.36.185	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	53
213.57.141.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	53
149.78.15.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
46.19.86.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
62.219.175.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
79.177.116.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
147.236.238.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
84.94.32.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
46.117.199.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
2.54.146.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
212.143.116.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
212.199.242.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
62.219.235.35	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
66.249.69.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.27.105.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
2.52.132.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
46.19.85.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
5.28.189.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
157.55.39.236	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
178.25.3.243	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
176.12.149.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
81.218.208.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
2.54.172.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
87.69.37.129	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
37.26.149.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
212.25.102.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.54.39.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
78.186.62.98	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
87.69.92.239	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
149.78.29.142	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
46.121.244.106	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.86.160	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
66.249.69.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
77.127.197.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
31.154.254.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
82.166.22.3	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
85.250.224.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.58.129		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.15.142	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	9
46.19.85.221	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.19.85.221	Block	3
80.246.136.72	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	3
176.13.1.162	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
176.13.14.175	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
79.180.138.99	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
2.54.50.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
185.120.126.50		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ajax/updatestatus.php	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.248.169.36	Netherlands	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
79.183.169.204	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
2.52.42.146	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.76.105.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
176.13.18.249	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
66.249.69.15	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
141.212.122.64	United States	147.237.76.42	refuah.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
61.135.190.200	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
2.54.145.124	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.81.250.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/	Block	1
79.177.174.157	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
185.120.126.50		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	1
66.249.67.46	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
94.199.238.15	United Kingdom	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.221	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
80.230.38.227	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVEN in www.aka.idf.il/main/sachar/default.aspx	None	1
2.52.132.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.18.249	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.18.249	None	1
66.249.69.34	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17047-h	Block	1
62.219.175.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
141.212.122.64	United States	147.237.77.176	matpash.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
31.168.180.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
85.64.32.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.174.157	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.177.174.157	Block	1
188.165.15.210	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1498-he/atal.aspx Ð¾Ð± Ñ?Ñ‚Ð¾Ñ ÐžÐµ Ð² Ñ?Ð²Ð¾Ð¸Ñ… Ð¸Ñ?Ñ?Ð»ÐµÐ´Ð¾Ð²Ð°Ð½Ð¸ÑÑ… Ð³Ð¾Ð²Ð¾Ñ€Ð¸Ñ‚ Ð³ÐµÐ½ÐµÑ€Ð°Ð»ÑŒÐ½Ñ‹Ð¹ Ð¿Ñ€Ð¾ÐºÑƒÑ€Ð¾Ñ€ Ñ€Ñƒ Ñ‚Ð¾	Block	1
66.249.67.54	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
94.230.93.162	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.27	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/default.aspx'	Block	1
2.52.164.132	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.149	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	1
66.249.69.42	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/3426.jpg	Block	1
141.212.122.64	United States	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
37.26.148.214	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.64.241.236	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	1
176.13.16.98	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.67.190	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
104.236.16.238		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspxshared/usercontrols/headerupper/	Block	1
46.120.223.45	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1