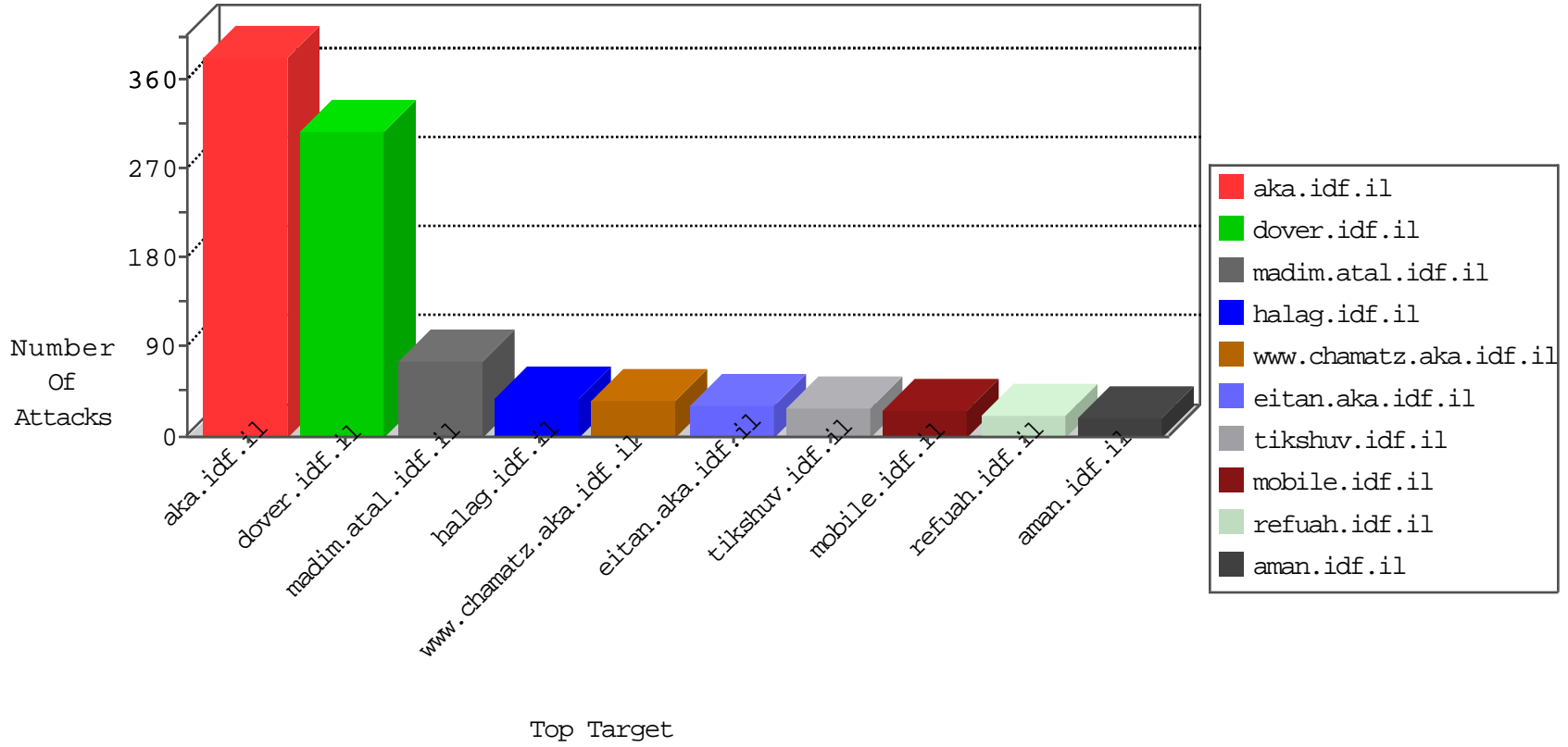


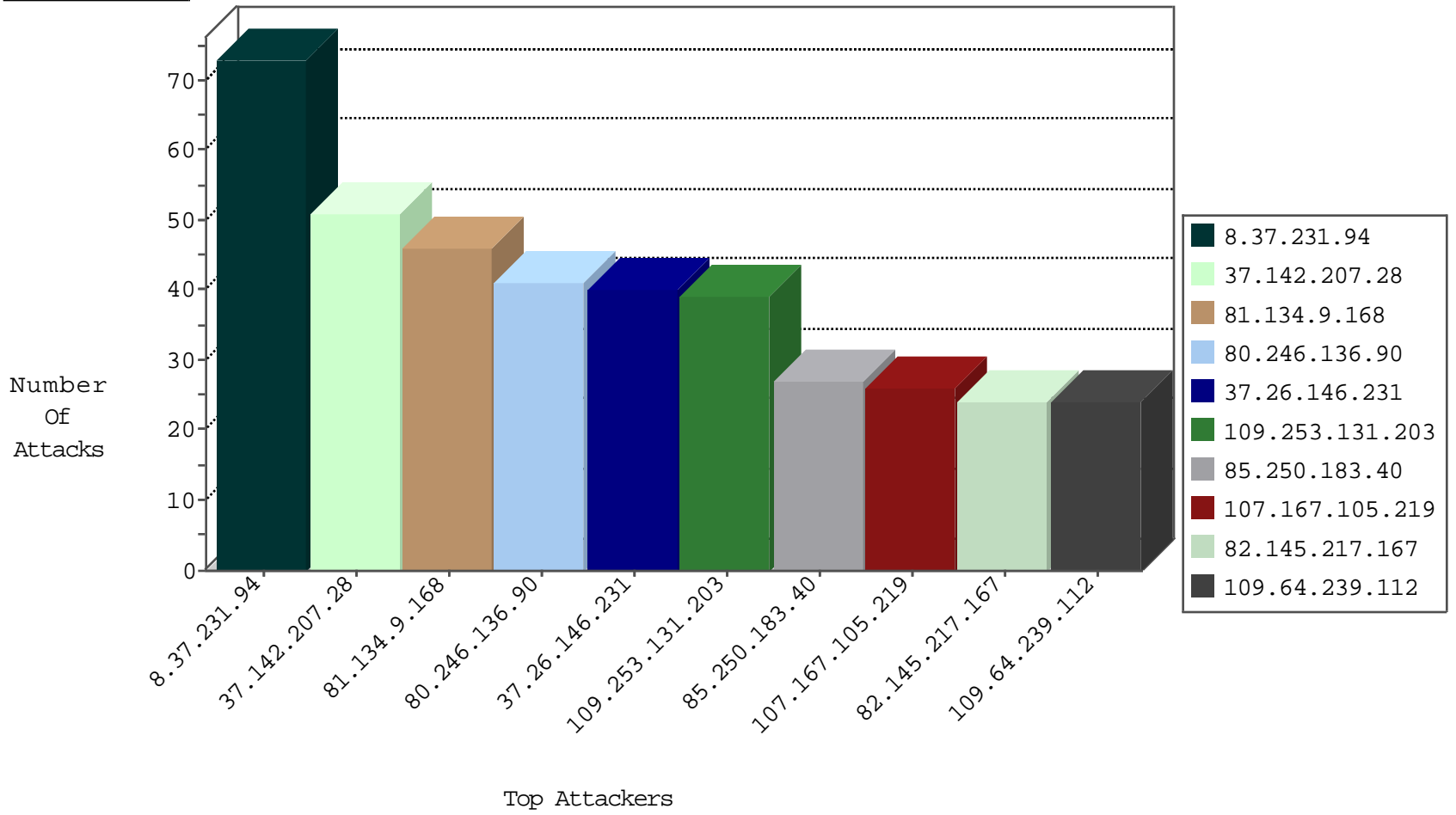
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.217.167	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	24
79.179.31.82	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.176.197.214	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
8.37.231.94	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Purple_Con_Limit_Http	drop	3
8.37.231.94	Anonymous Proxy	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	2
185.130.5.224		147.237.76.198	e.yohanan.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.228		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
118.143.37.71	Hong Kong	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
81.134.9.168	United Kingdom	147.237.77.216	dover.idf.il	I4 Source or Dest Port Zero	drop	1
185.94.111.1		147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.146	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
5.22.130.89	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
37.142.176.73	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.180.171.239	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
31.154.34.190	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
207.46.13.70	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.98	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.102	China	147.237.76.42	refuah.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

## 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
173.236.255.128	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	4
80.82.78.66	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
176.205.244.143	147.237.77.216	United Arab Emirates	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.107.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.65.251.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.50	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.224.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.182.170.38	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
92.13.217.108	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
87.70.52.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.253.48.226	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 2048	1
84.111.20.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.173	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.66	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	1
5.29.26.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.66	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
186.9.133.132	147.237.77.216	Chile	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.78.66	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
79.176.211.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.68.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.244.49.137	147.237.0.200	Hong Kong	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
104.41.169.33	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
61.182.170.38	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
89.138.52.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.253.48.226	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
85.64.125.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
50.253.48.226	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -f -sS	1
84.108.90.117	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.57.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
80.82.78.66	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
192.116.53.232	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
8.37.231.94	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
81.134.9.168	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	33
37.142.207.28	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
107.167.105.219	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	26
85.250.183.40	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
109.64.239.112	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.142.207.28	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
2.54.13.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.136.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
37.26.146.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
84.94.72.61	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
109.65.48.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.142.213.22	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
37.26.146.231	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
37.142.213.22	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
180.94.48.185	Hong Kong	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.146.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.246.136.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.210.189.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.19.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.136.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.64.176.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.246.137.103	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.125.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.134.9.168	United Kingdom	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
80.246.136.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.177.41.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.69.245.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.22.129.96	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.146.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
84.111.155.155	Israel	147.237.8.50	e.tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
94.159.152.103	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
199.30.25.66	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
81.134.9.168	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	alert	4
2.54.50.223	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.80.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
5.102.254.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
87.71.9.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.131.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.183.114.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.51.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.106.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.8.2	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
109.253.131.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	39
46.19.85.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
2.54.183.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
173.236.255.128	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	4
79.180.102.216	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	3
84.94.72.61	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	3
199.30.24.149	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
173.236.255.128	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 173.236.255.128	Block	3
79.176.132.53	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.136.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.179.241.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.137.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.71.9.229	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 87.71.9.229	Block	2
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.132.230	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.18.88	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
186.9.133.132	Chile	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.225	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in ww.tikshuv.idf.il/site/contactus.aspx	Block	1
37.26.146.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.111.233.25	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyus/forum/asp/	Block	1
185.82.200.91		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
79.180.123.64	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
77.126.29.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
87.69.62.227	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/	Block	1
41.129.3.42	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
80.246.137.103	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.180.123.64	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.180.123.64	Block	1
94.159.152.103	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.146.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.109.208.50	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
185.89.217.226		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.123.64	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php	Block	1
109.253.132.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
87.69.208.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/gyus/	Block	1
5.29.75.126	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/gyus/atuda/asmachta.aspx	None	1
212.76.110.173	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/&sa=u&ved=0ahukewjd9uuzxrhlahwjkiwkhuvsc-gqfggrmai&usg=afqjcned8i jyzkxmvasyx7h7flpeujjow	Block	1
79.180.123.64	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
95.86.86.47	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1361-10653-he/dover.aspx&sa=u&ved=0ahukewjgw8uzwl hlahwcknikhwv2c8eqfggemag&usg=afqjcnqpmhfayeubnu9uob5yavfmo whyiw	Block	1
46.117.63.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.252.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
85.64.156.102	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.180.228.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.51.22.116	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
185.89.217.227		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.176.132.53	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
87.69.208.55	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/kiosk/kiosk.aspx	Block	1