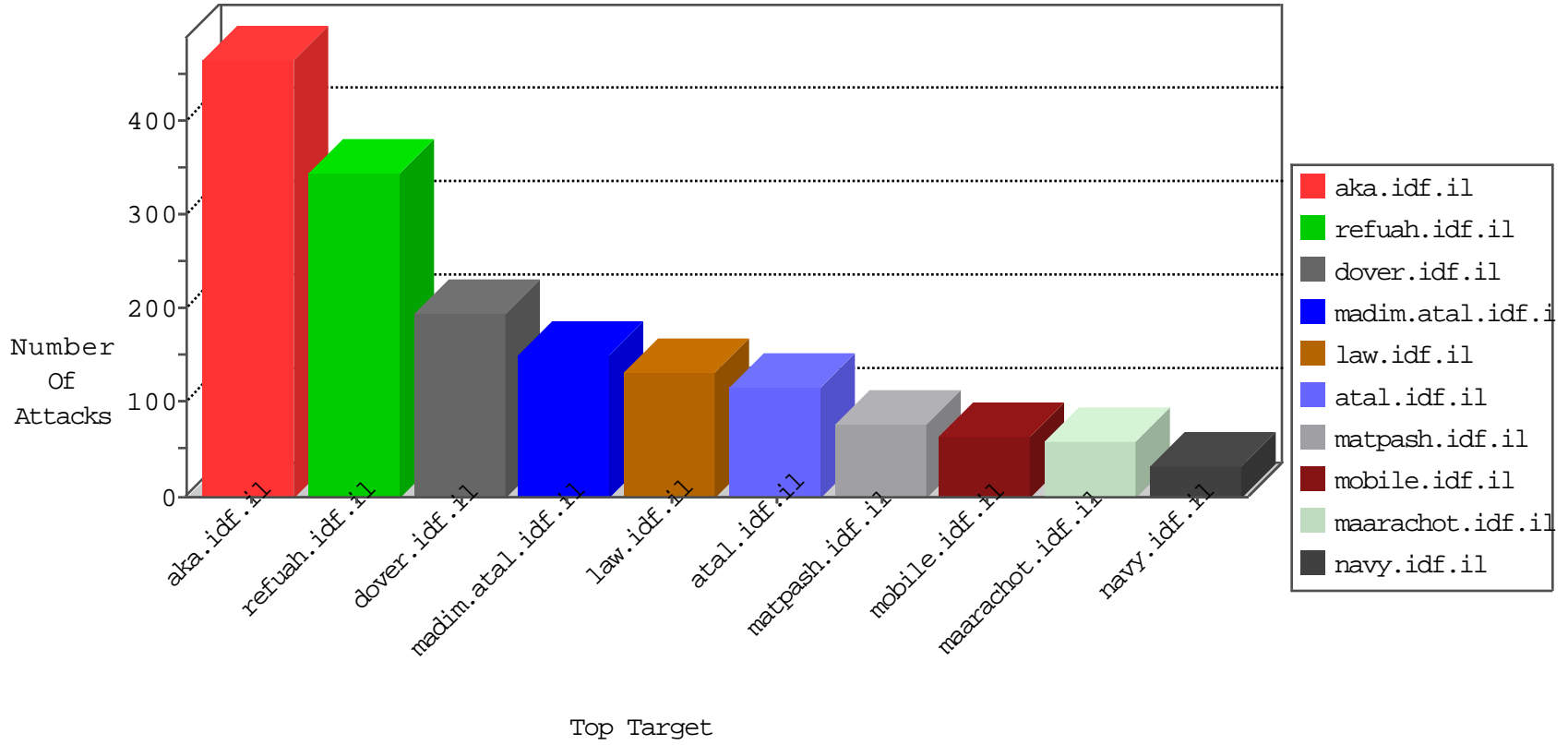


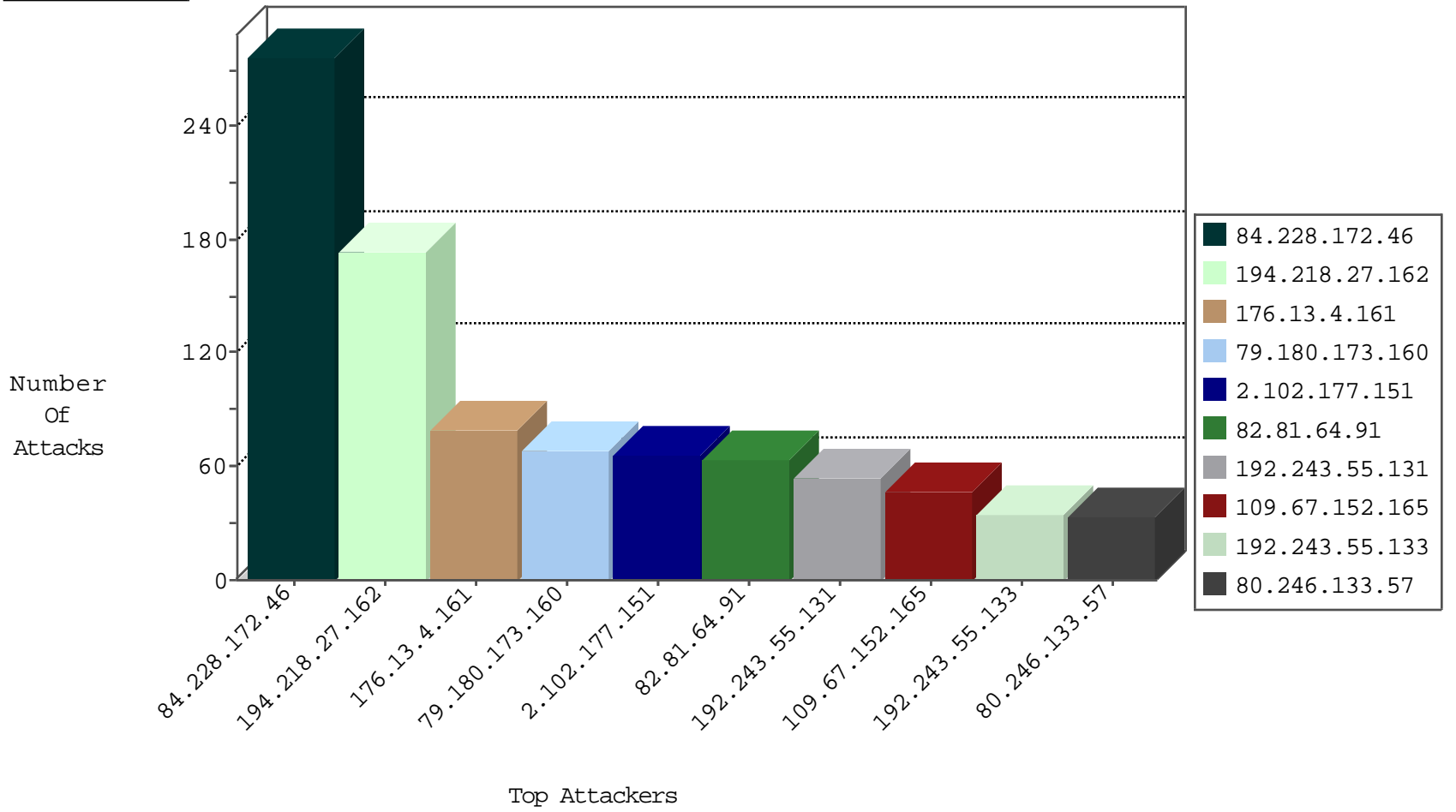
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
47.88.103.153	Canada	147.237.77.233	atal.idf.il	block-sp-trafl	drop	1
208.67.1.70	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.70	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
85.105.13.167	Turkey	147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
208.67.1.70	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.70	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.38.35	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
109.66.166.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.19.85.95	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
106.38.241.107	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
5.9.89.170	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
85.65.214.152	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.30.236	Germany	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Block	2
149.202.54.50	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
158.69.214.109	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
136.243.152.18	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
46.244.74.216	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1
69.30.198.178	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.133.57	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	21
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.246.130.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
195.216.176.244	147.237.77.243	Latvia	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
109.160.167.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.36.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.82.106.200	147.237.76.44	India	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
178.79.130.52	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN Potential SSH Scan	1
46.121.223.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
121.18.74.98	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -sS window 4096	1
113.76.90.199	147.237.77.234	China	halag.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
218.246.0.97	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
110.92.195.112	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.216.176.244	147.237.0.200	Latvia	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 3072	1
183.82.106.200	147.237.76.44	India	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
79.176.16.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
146.185.250.2	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
121.18.74.98	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
119.146.221.68	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -sS window 3072	1
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
112.74.39.155	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.228.172.46	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	276
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	115
79.180.173.160	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	67
2.102.177.151	United Kingdom	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	66
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	57
109.67.152.165	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
89.138.113.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
84.228.33.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.196.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.28.189.195	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
89.138.120.102	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
109.67.152.165	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
80.246.133.57	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.28.189.195	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	7
79.181.178.71	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.176	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.115.25.79	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.171.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.31.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.109.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.205.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.181.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.176	Israel	147.237.77.216	dover.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	monitor	6
188.120.148.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.200.38	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	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.137	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
80.246.133.57	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
79.181.153.142	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.29.189.81	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	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
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.180.61.36	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
5.22.129.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.187.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.133	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.135	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.135	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
101.227.61.203	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.4.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
82.81.64.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
80.178.207.93	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 80.178.207.93	Block	10
80.178.207.93	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	5
46.19.85.203	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	4
82.166.159.136	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.166.159.136	Block	3
66.249.81.218	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
80.246.137.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.76	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.76	Block	2
82.166.159.136	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
109.253.203.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.115.227	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/size338x0/1584.jpg	Block	2
109.66.196.152	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.176.42.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
148.251.21.227	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	2
82.102.193.178	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/894-ar	Block	2
79.178.171.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.67.152.165	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
40.77.167.81	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
85.64.157.252	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.157.252	Block	1
2.54.23.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19239-en/dover.aspx http://digg.com/submit	Block	1
79.177.28.122	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
148.251.21.227	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/cgi-bin/shitur/bookpage100598/iturfindpageexact.pl	Block	1
109.65.22.235	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
31.154.94.69	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
216.55.143.94	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name Mozilla/5.0 (compatible; spider/2.0; +http	Block	1
180.76.15.26	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1927-en/cogat.aspx gaza semanales	Block	1
79.179.109.253	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.126	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/5/111525.pdf	Block	1
109.160.181.82	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cpMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
40.77.167.94	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
85.64.157.252	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
2.54.179.35	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/main.stm,	Block	1
148.251.21.227	Germany	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 148.251.21.227	Block	1
79.177.28.122	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.177.28.122	Block	1
109.65.22.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.22.235	Block	1
66.249.64.229	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
31.154.94.69	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 31.154.94.69	Block	1
192.115.25.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.180.173.160	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
85.64.157.252	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	1
46.19.85.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.61.10.2	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	1
149.50.76.60	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.65.22.235	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
66.249.66.64	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/108237.pdf	Block	1