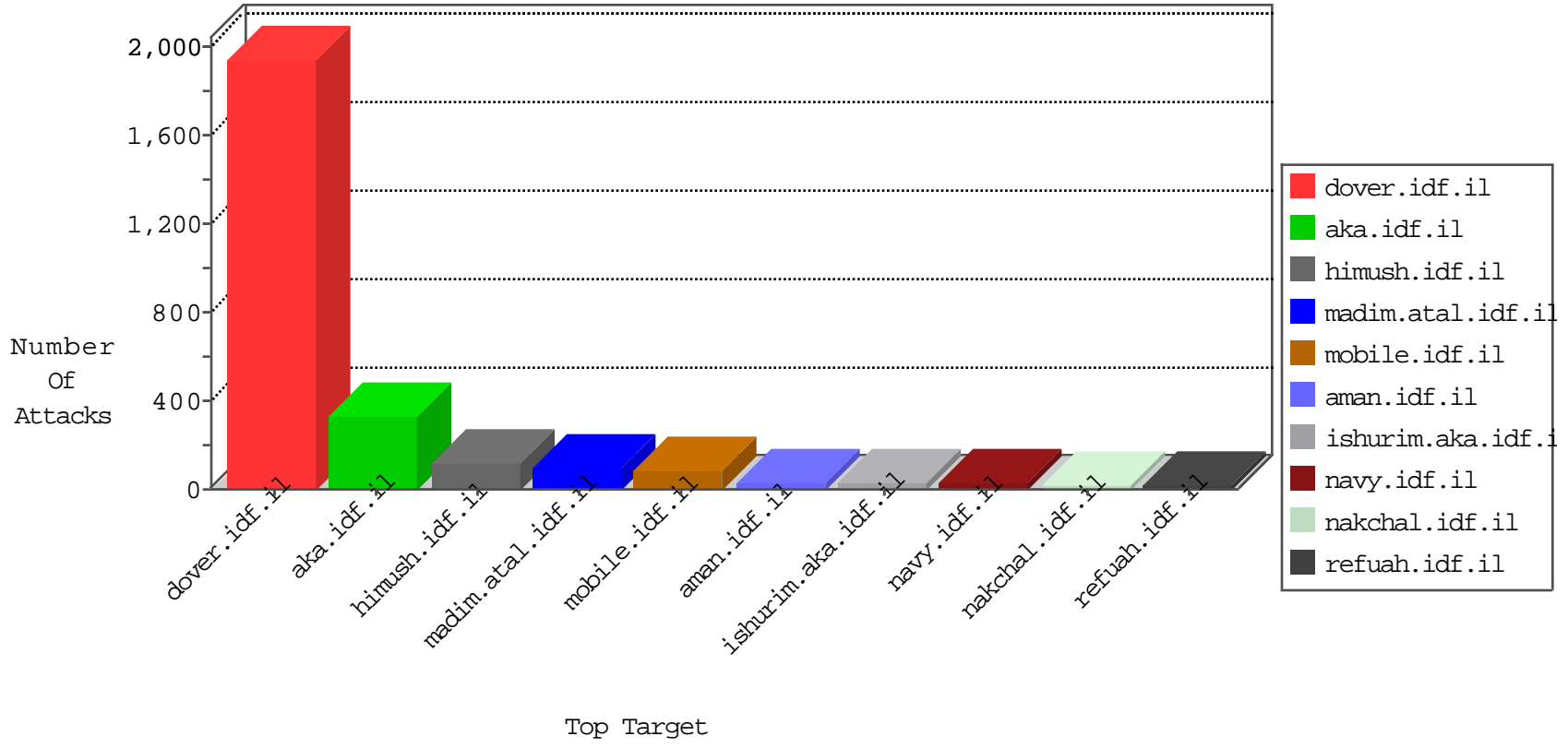


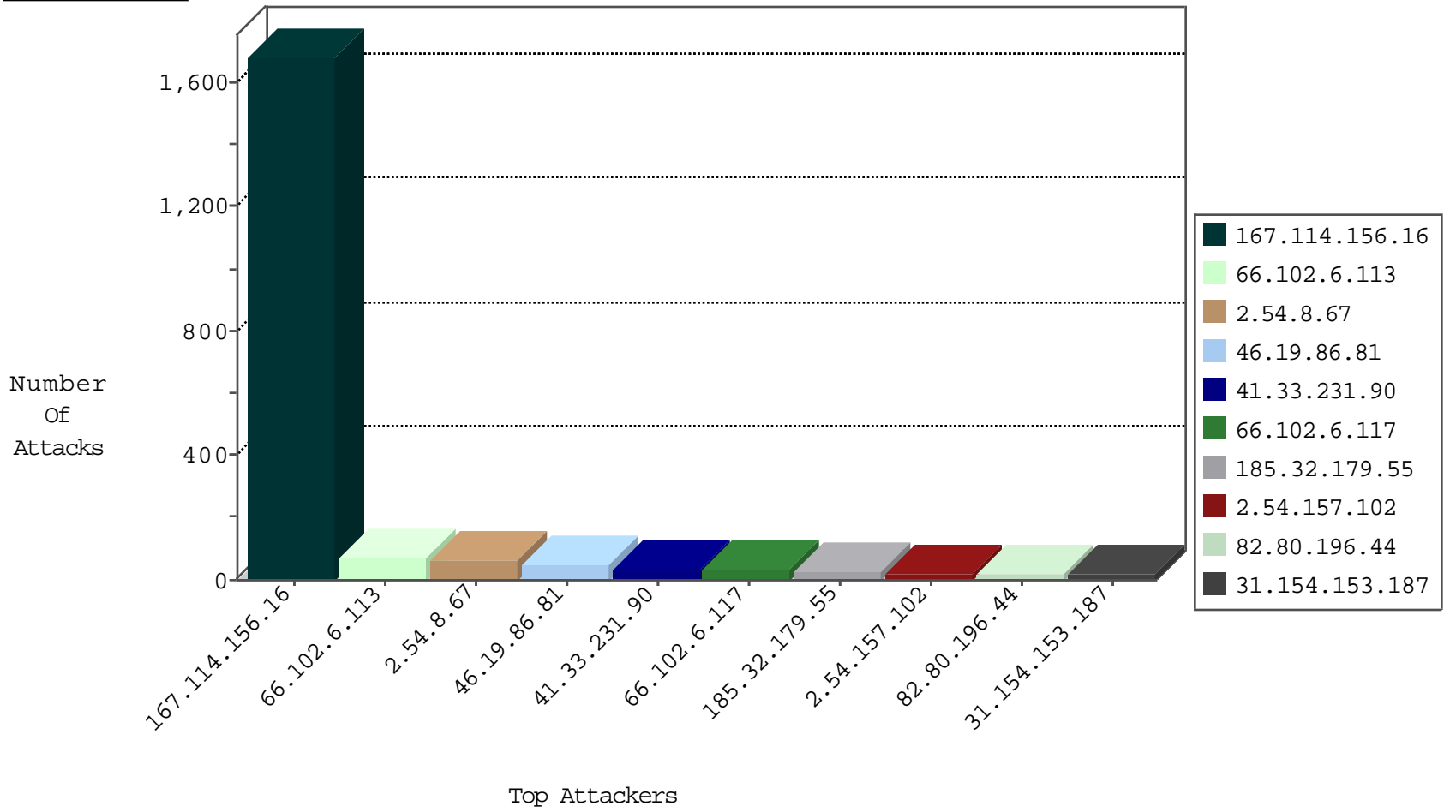
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3116
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	80
66.249.64.153	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
80.246.136.119	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
52.91.59.24	United States	147.237.76.30	himush.idf.il	Invalid L4 Header Length	drop	1
52.91.59.24	United States	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1
52.91.59.24	United States	147.237.0.16	my-kosher-kravi.idf.il	Invalid L4 Header Length	drop	1
52.91.59.24	United States	147.237.76.31	nakchal.idf.il	Invalid L4 Header Length	drop	1
52.91.59.24	United States	147.237.0.16	my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
169.54.233.125	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
52.91.59.24	United States	147.237.76.34	yohalan.idf.il	Invalid L4 Header Length	drop	1
52.91.59.24	United States	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	1
52.91.59.24	United States	147.237.76.38	e.e.meitav.idf.il	Invalid TCP Flags	drop	1

12-24-2015-10:04:00 to 12-24-2015-11:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.46.13.51	United States	147.237.77.216	dover.idf.il	C076: HTTP: Access to - action=... (General)	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.102.48.195	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.168.29	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.210.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.172	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
37.26.148.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.207.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
2.52.59.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
166.63.122.229	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
149.78.249.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.241.70	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.38.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.37.216	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.100.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.140.54	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.30.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
166.63.122.229	147.237.76.199	United States	e.nakchal.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
46.19.86.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.102.6.113	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
66.102.6.113	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid sequence number	monitor	23
66.102.6.113	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
46.19.86.249	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
80.246.136.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.146.221	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
2.54.2.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.120.78.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.102.6.117	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
66.102.6.117	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
66.102.6.117	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
31.154.153.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
31.154.153.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
212.179.220.182	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.145	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.131.154	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
2.54.157.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
2.54.157.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
82.80.196.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	7
2.54.157.102	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.197	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.179.218.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.67.255.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.134.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
80.246.137.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.52.49.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.53	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.138.27	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.3.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.220.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.139.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.160.240.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.59.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
132.70.66.11	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.166.140.117	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
66.102.6.115	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.86.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.209	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.102.6.115	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.102.6.115	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.8.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	58
185.32.179.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
109.253.195.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
192.116.232.69	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	8
109.253.131.154	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.8.67	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.8.67	Block	3
213.8.10.16	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/0/112270/pdf	Block	2
213.57.90.90	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
62.219.99.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.153.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
37.142.190.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.25.84.200	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
95.86.115.169	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
84.94.230.194	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.54.41.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.23.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/adx/bin/clientside/b7181a2fq2fq7bq7bq7bq7bq7bmq7bmq20ydwjwxfq7bq7bq7bq7bq7bq7bmq20wmwydq27fq7bq7bwbbemq7bfkq27	Block	1
66.249.75.46	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.201.154.138	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
2.54.170.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	1
89.138.98.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.7.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.18.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.139.60	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
61.135.190.71	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
149.88.113.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
40.77.167.61	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/captcha.ashx	Block	1
212.25.84.200	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
84.108.147.94	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
2.54.50.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.37.139.65	Portugal	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
2.52.29.158	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
176.13.3.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method oFriend.aspx?&l=he&f=1133&d=23036 in URL	Block	1
2.90.19.38	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/cpanel	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
93.115.95.206	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
80.246.139.60	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
183.79.223.23	Japan	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
61.135.190.200	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
149.202.98.160	Germany	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
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
45.35.71.181		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
212.179.218.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1